INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

ADMINISTRACION Y CONTROL DE ACCESO A REDES INALAMBRICAS

T É S I S

Q U E P A R A O B T E N E R E L T Í T U L O D E :

INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

P R E S E N T A N

GALVÁN CASTILLO OSCAR HUGO
VALDEZ RAMIREZ ALFREDO

ASESORES: Ing. Ignacio Díaz Sandoval
M. en C. Federico Felipe Duran

MÉXICO, D.F. Noviembre de 2008

INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELECTRICA

UNIDAD PROFESIONAL "ADOLFO LÓPEZ MATEOS"

TEMA DE TESIS

QUE PARA OBTENER EL TITULO DE INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

POR LA OPCIÓN DE TITULACIÓN TESIS COLECTIVA Y EXAMEN ORAL INDIVIDUAL

DEBERA(N) DESARROLLAR OSCAR HUGO GALVÁN CASTILLO
ALFREDO VALDEZ RAMÍREZ

"ADMINISTRACIÓN Y CONTROL DE ACCESO A REDES INALÁMBRICAS"

IMPLEMENTAR UN SISTEMA DE SEGURIDAD QUE ADMINISTRE Y CONTROLE EL ACCESO DE LOS USUARIOS A LA RED INALÁMBRICA DE LA ESIME ZACATENCO.

- INVESTIGACIÓN PREVIA
- IMPLEMENTAR UN SISTEMA DE AUTENTACIÓN DE ACCESO A LA RED INALÁMBRICA DE ESIME , ZACATENCO
- REALIZAR PRUEBAS NECESARIAS
- CONCLUSIONES

MÉXICO D. F., A 18 DE AGOSTO DE 2009.

ASESORES

ING. IGNACIO DÍAZ SANDOVAL

ING. FEDERICO FELIPE DURAN

M. EN C. SALVADOR RICARDO MENESES GONZÁLEZ
JEFE DEL DEPTO. ACADÉMICO DE
INGENIERÍA EN COMUNICACIONES Y ELECTRÓNICA

AGRADECIMIENTO

A mis padres, Rogelio y Lucia. Ejemplo siempre firme de dedicación, comprensión, constancia, cariño y apoyo. Gracias por confiar en la educación como el medio más justo de superación. Y por darme la oportunidad de contar con una profesión.

A mi padre, por ser siempre mi gran ejemplo de responsabilidad, trabajo y constancia.

A mi madre, por no dejarme salir a jugar antes de terminar la tarea y por tantas horas de enseñanza.

A mi país, México por ser mi fuente de inspiración y superación en los momentos difíciles. Y por darme la oportunidad de estudiar en el Instituto Politécnico Nacional.

Oscar Hugo Galván Castillo.

AGRADECIMIENTO

A mi madre por su apoyo incondicional, por su amor interminable y por su ejemplo de valor ante momentos difíciles.

A mi papá, hermanas, tíos, primos… sin su apoyo no lo hubiera logrado y por dejar que mi sueño formará a ser parte del suyo.

A mis amigos de la escuela por su amistad y compartir muchos momentos agradables.

Alfredo Valdez Ramírez.

“ADMINISTRACION Y CONTROL DE ACCESO A REDES INALAMBRICAS”

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Pagina

OBJETIVO GENERAL

Diseñar un sistema de seguridad que administre y controle el acceso de los usuarios a la red inalámbrica de la ESIME Zacatenco.

OBJETIVOS PARTICULARES

- Diseñar un sistema de autenticación de acceso a la red inalámbrica (control y administración).
- Realizar las pruebas necesarias para comprobar su correcto funcionamiento.
- Definir los elementos de seguridad necesarios para la red inalámbrica de la ESIME Zacatenco.

JUSTIFICACIÓN

Actualmente las redes inalámbricas han adquirido mayor importancia para el desarrollo y desempeño de las empresas y de las instituciones, además existen mayores facilidades para adquirir equipos portátiles con su tarjeta de red inalámbrica incluida.

En el caso del IPN esto representará que el número de usuarios de las redes inalámbricas seguirá en aumento, convirtiéndose en un compromiso estratégico por parte del IPN de proveer un servicio de acceso inalámbrico a internet confiable y seguro para toda la comunidad politécnica, sin que esto represente un riesgo para la misma infraestructura de la red del politécnico.

Lo anterior se pone de manifiesto por el creciente número de alumnos y profesores que cuentan con dispositivos capaces de acceder a la Internet, tales como lap Tops, Ipod's, PSP, celulares, etc., mediante los cuales se logra incrementar significativamente el potencial de aprendizaje así como el de la investigación, favoreciendo de manera directa la aplicación del nuevo modelo educativo que el Politécnico ha ofrecido implantar, mismo que difícilmente podrá concretarse si la comunidad institucional carece de los medios para realizar el aprendizaje en línea, así como la incapacidad de apropiarse del cúmulo de conocimientos e información existente en la red de redes. De acuerdo con datos obtenidos en la ESIME Zacatenco, en septiembre de 2008 el 25% de los alumnos ya cuentan con equipos para ingresar en forma inalámbrica al internet.

Actualmente se tienen conectados sin autorización una serie de puntos de acceso que cuentan con mínima seguridad o que simplemente no la tienen, además de que existen programas que son utilizados para eludir la seguridad de bajo nivel.

Por ello es apremiante diseñar un sistema que administre y controle el acceso de los usuarios hacia internet en forma organizada y sistematizada, sin poner en riesgo la integridad de la red del politécnico.

ADMINISTRACIÓN Y CONTOL DE ACCESO A REDES INALAMBRICAS

RESUMEN

En la actualidad en la ESIME Zacatenco no cuenta con una red inalámbrica oficial, confiable y segura que pueda brindar el servicio de acceso a Internet a profesores y alumnos, esto se debe a la falta de un sistema que pueda controlar el acceso de los usuarios a la red de una forma segura, es decir que solo los usuarios autorizados puedan hacer uso de este servicio.

En este trabajo de tesis se presenta una opción de control de acceso que pueda cubrir esta necesidad, presentando el funcionamiento de dicha opción. Asimismo, se describe lo que se necesita en cuanto a dispositivos para poder llevar a cabo la implementación de esta opción de acceso seguro a la red.

METODOLOGIA

- Elección del proyecto:Durante esta etapa se eligió de entre varias opciones este proyecto.

- Etapa de investigación documental: En esta etapa, se llevo a cabo la investigación necesaria sobre redes inalámbricas, en cuanto a los métodos de seguridad y control de acceso existentes.
- Una vez hecha esta investigación se prosiguió a seleccionar la información útil para el proyecto.

- Etapa de investigación de campo: En esta etapa se realizo una investigación acerca de las condiciones actuales de las redes inalámbricas en la dirección de informática de la ESIME Zacatenco y en la dirección de informática ubicada en el edificio inteligente del IPN.

- Etapa de integración de las investigaciones: Una vez conocidas las condiciones actuales del IPN y teniendo la información necesaria, se prosiguió a la elección del método de autenticación que más se adapta a las necesidades del IPN.

- Implementación del sistema de autenticación:En esta etapa se hizo el trabajo necesario para poder configurar los servidores y el AP que nos ayudarían a tener la posibilidad de realizar las pruebas.

- Realización de pruebas: En esta última etapa se llevaron a cabo las pruebas necesarias para lograr el óptimo funcionamiento de este sistema de autenticación.

GLOSARIO DE TERMINOS Y ACRONIMOS

802.11 Protocolo establecido por la IEEE para redes inalámbricas de área local.

802.1x Protocolo de la IEEE que se basa se basa en el control de puerto de conexión, este puerto será abierto una vez que el cliente cumpla de manera satisfactoria un proceso de autentificación.

Acces point (AP) Punto de acceso, un punto de acceso es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

Active Directory Directorio activo, es la base de datos en donde se encuentran registrados todos los usuarios y equipos pertenecientes a un dominio.

Administración Conjunto de procesos de planificación, organización, ejecución, coordinación y control que se ejercen sobre un sistema.

Algoritmo Conjunto de operaciones y procedimientos bien definidos para logra la solución de un problema.

Autoridad Certificadora La autoridad certificadora es un elemento que se encarga de expedir los certificados implementando las directivas adecuadas para evaluar las solicitudes de certificado y denegar el certificado a cualquier entidad que no cumpla con la directiva

Bridge Puente para interconexión de redes.

CHAP Challenge Handshake Authentication Protocol “Protocolo de autenticación por desafío mutuo”.

Certificado Acreditación emitida por una entidad o un particular debidamente autorizados garantizando que determinado dato (por ejemplo, una firma electrónica o una clave pública) pertenece realmente a quien se supone.

Cifrado El proceso de juntar o separar información de manera que se enmascara su significado.

Clave Pieza de información que controla la operación de un algoritmo en este caso de cifrado.

Cobertura El término cobertura se refiere al área geográfica que cubre una estación específica.

Codificación Aplicación de un algoritmo especifico a los datos, de forma que se altere la apariencia de estos.

CRC Algoritmo de chequeo de integridad.

EAP Acrónimo del protocolo de autenticación extensible, asegura la autenticación mutua entre un cliente inalámbrico y un servidor.

EAP-MD5 Acrónimo de protocolo de autenticación extensible de mensaje resumido 5, está basado en nombres de usuario y contraseñas.

IAS Servicio de autenticación de internet.

IEEE Acrónimo de institute of electrical and Electronics Engineers "instituto de ingenieros eléctricos y electrónicos".

IPsec Seguridad del protocolo de internet

NAT Acrónimo de Network Address Translation

PAP Password Authentication Protocol "Protocolo de autenticación por contraseña".

Password Es una contraseña o clave y es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso

PEAP Acrónimo del protocolo de autenticación protegida extensible. Proporciona la autenticación mutua y la generación de claves de manera que la fase de autenticación del usuario está protegida.

PPP Protocolo punto a punto.

Protocolo Descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en que los dispositivos de una red intercambian información.

Proxy RADIUS El término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para

	permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.
RADIUS	Acrónimo de Remote Authentication Dial-In User Server ” servicio de autenticación de usuarios telefónicos remotos” Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red.
RC4.	Algoritmo de cifrado. RC4 es un algoritmo de cifrado de flujo, funciona expandiendo una semilla para generar una secuencia de números pseudoaleatorios
Rendimiento	Hace referencia al resultado obtenido en comparación con el resultado deseado.
UDP	User Datagram Protocol “Protocolo de Datagramas de Usuario”
User name	Suele ser un nombre intelegible que identifica al usuario de un sistema o red
VPN	Red privada virtual
WEP	Es un protocolo de seguridad usado para proteger las comunicaciones inalámbricas de robo de información y de espionaje, además evita el acceso no autorizado a la red inalámbrica.
Wi-Fi	Acrónimo de Wireless fidelity (fidelidad sin cables), hace referencia a los dispositivos de red inalámbricos basados en la norma estándar 802.11. La primera versión fue 802.11b, con una velocidad máxima de 11 Mbps. Actualmente es muy extendida la versión 802.11g, que permite alcanzar los 54 Mbps.
WLAN	Acrónimo de Wireless “red inalámbrica de area local” y es un sistema de comunicación de datos inalámbrico.
WPA	Acrónimo de Wifi Protected Access (acceso sin cables protegido). Al igual que WEP, es un sistema de cifrado para redes inalámbricas, pero más seguro, puesto que cambia el código de manera automática cada cierto intervalo de tiempo y de forma aleatoria.

Capítulo 1

REDES INALÁMBRICAS

1.1 ANTECEDENTES

Las redes inalámbricas son el resultado de la convergencia de 2 tecnologías: redes y radio, lo que a su vez marca un hito en la era de las telecomunicaciones.

El principio básico de las redes inalámbricas nace en el siglo XIX cuando Guillermo Marconi, el padre de la radio, dio inicio al mundo de la tecnología inalámbrica. Cuando Marconi comenzó a experimentar con las ondas hertzianas en 1894 su objetivo era producir y detectar ondas de radio en largas distancias.

1896

Marconi tuvo éxito y obtuvo una patente sobre su invento y estableció la Wireless Telegraph and Signal Company Limited, compañía de telegrafía y señales inalámbricas limitada, la primera empresa de radio en el mundo.

1901

Se realizó la primera transmisión transatlántica.

1905

La primera señal de auxilio enviada por telégrafo inalámbrico fue transmitida utilizando código Morse.

A mediados de la década de los 40 la tecnología inalámbrica eventualmente progresó como una herramienta indispensable para la milicia norteamericana, que utilizó señales inalámbricas para transmitir datos encriptados, lo que hace que un acceso no autorizado al tráfico de la red sea casi imposible.

Este tipo de tecnología se utilizó por primera vez durante la Segunda Guerra Mundial cuando la armada de EE.UU. comenzó a transmitir planes de combate a través de las líneas enemigas y cuando los barcos de la naval instruyeron a sus tropas de costa a costa.

1957

Nace ARPANET, la primera red de computadoras distribuida geográficamente y madre de la actual Internet. La infraestructura es financiada por la Agencia para la Investigación Avanzada de Proyectos (ARPA), creada por el gobierno en plena carrera espacial y a raíz del lanzamiento del Sputnik.

1971

La primera red inalámbrica de datos se integró en cuando las tecnologías de redes se conjugaron con las comunicaciones por radio en la Universidad de Hawai en un proyecto de investigación llamado ALOHANet. La topología en estrella bidireccional del sistema incluyó siete computadoras distribuidas en 4 islas para comunicarse con la computadora central en la Isla Oahu sin utilizar líneas telefónicas, naciendo así la tecnología de redes inalámbricas.

1972

Científicos de Xerox ponen en marcha la primera red de área local (Ethernet) en el centro Xerox Park de Palo Alto (California, EEUU).

Las redes inalámbricas basadas en radiofrecuencia despegaron en la década de los 90 cuando la potencia de procesamiento de los chips llegó a ser suficiente para gestionar los datos transmitidos y recibidos a través de conexiones de radio. Sin embargo estas implementaciones eran caras y eran productos de marca: no se podían usar con otras. Las redes incompatibles están abocadas al fracaso.

Ahora los transmisores son minúsculos chips encapsulados en dispositivos del tamaño de una tarjeta de crédito que se conecta en ordenadores que a su vez no son muchos más grandes que un cuaderno. Estos equipos no transmiten ni reciben voces con ruido, sino pequeños paquetes de ceros y unos: datos informáticos.

1997

El IEEE, organización encargada de la elaboración de normas de carácter técnico para la industria eléctrica y electrónica, publica en junio el estándar 802.11, las normas técnicas que rigen el funcionamiento de las redes inalámbricas.

1999

Nace la Alianza Wi-Fi, una institución financiada por los fabricantes de equipos para redes inalámbricas, encargada de certificar que los productos de esta tecnología cumplen con el estándar IEEE 802.11.

La IEEE finalizó el estándar 802.11b aumentando el rendimiento de las redes inalámbricas a 11 Mbps. El momento decisivo de las redes inalámbricas llegó en julio, con un lanzamiento por parte de Apple de su tecnología Airport.

Está tecnología de Airport era una versión de IEEE 802.11b ajustada al estándar de la industria y Apple la puso en marcha en el mercado cobrando por tarjetas de red inalámbricas y por puntos de acceso (llamadas estación base), estos productos encajaban en distintos modelos de Macintosh. A lo largo de los últimos años sus capacidades han aumentando y los precios han bajado.

2001

Nace en España Redlibre.net, el primer intento de creación de una red inalámbrica ciudadana de acceso libre. La empresa Kubi Wireless instala en pruebas una red inalámbrica en el Hotel Montecarlo de Barcelona.

2003

La empresa Alvarion y la Corporación Espacial Sueca solicitan al Libro Guiness de los Records la inclusión de una nueva marca: la mayor distancia de alcance de una conexión WiFi – 310 kilómetros- gracias a un globo estratosférico equipado con esta tecnología.

A las redes inalámbricas comúnmente se les conoce como redes Wireless, el cual es un término que significa “sin cables”, y que designa a todos aquellos aparatos que, en su funcionamiento no requieren la conexión física entre él y otro.

Otra definición correcta es: cuando los medios de unión entre sus terminales no son los cables, sino un medio inalámbrico, como por ejemplo la radio, los infrarrojos o el láser.

Las más populares en los últimos años son las redes de área local inalámbricas (WLAN, Wireless Local Área Network) que se ven acrecentadas conforme sus ventajas aumentan y se descubren nuevas aplicaciones para ellas. Esta red puede definirse como una red local que utiliza tecnología de radiofrecuencia para enlazar los equipos conectados a la red.

Las WLAN permiten a los usuarios acceder a información y recursos en tiempo real y sin necesidad de estar físicamente conectados a un determinado lugar y lo más importante incrementa la productividad y eficiencia en las empresas donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de los edificios, campus universitarios o inclusive sobre áreas metropolitanas para cubrir zonas de alta densidad de usuarios.

Muchos de los fabricantes de ordenadores y equipos de comunicaciones como los son los PDAs (Personal Digital Assistants), terminales de puntos de ventas y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas.

En la actualidad prácticamente todos los negocios, necesitan de una red de comunicación, por lo tanto parece sencillo comprender que si esta comunicación se realiza sin conexión física, esto hará que compartir información sea mucho más cómodo.

1.2 ASPECTOS IMPORTANTES DE LAS REDES INALAMBRICAS

Las redes inalámbricas presentan las siguientes ventajas:

- La movilidad permite obtener información en tiempo real en cualquier parte de la institución, organización, sitio público o empresa aumentando con esto la productividad.

- La facilidad de la instalación ya que no se requiere realizar obras para tender el cable, muros o techos.

- La flexibilidad ya que nos da la facilidad de conservar la estética de los lugares de trabajo, evitando los cables.

- Reducción de costos a largo plazo y en la instalación.

- Escalabilidad que presentan en cuanto a los cambios en la topología ya que se realizan de manera sencilla.

Aunque como todo, las redes WI-FI también presentan una serie de desventajas:

- Baja o nula capacidad en lugares ruidosos.

- La inseguridad.

- Las velocidades de transmisión relativamente bajas.

1.3 CARACTERÍSTICAS IMPORTANTES DE UNA RED INALÁMBRICA

Las características más importantes de las redes inalámbricas son:

- Cobertura: El rango de cobertura de una WLAN típica permiten de 30m a 100m. Puede extenderse y tener la posibilidad de alto grado de libertad utilizando puntos de acceso, ubicándolos en donde se requiera tener cobertura.

- Rendimiento: El rendimiento de una WLAN va a depender, de una serie de parámetros: Puesta a punto de los productos, del número de usuarios, factores de propagación, tipo de sistema inalámbrico, del retardo de la red y de los cuellos de botella de la parte cableada y aplicaciones utilizadas por el usuario.

- Compatibilidad con las redes existentes: Las WLAN proporcionan un estándar de interconexión con las redes cableadas como Ethernet o Token Ring. La red trata a los nodos inalámbricos igual que cualquier otro componente de la red aunque con los controladores apropiados.

- Interoperabilidad de los dispositivos inalámbricos dentro de la red: Utilizar dispositivos con la misma tecnología y misma banda de frecuencia.

- Simplicidad y facilidad de uso: Simplificación de la configuración de la red ya que únicamente los puntos de acceso de las redes inalámbricas necesitan cable.

- Seguridad en la comunicación: Utilización de técnicas de encriptado y métodos de acceso autorizado a la red, los nodos de la red inalámbrica deben de tener habilitada la seguridad antes de ser utilizadas.

- Seguridad Laboral: Se refiere a cumplir con las normas de seguridad dictadas por la industria.

Para ser considerada una WLAN la red tiene que cumplir con la norma 802.11 establecido por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

La arquitectura de las redes WLAN tienen una estructura celular similar a las redes de telefonía móvil. Cada celda llamada BBS (Basic Service Set) gobernada por una estación base o AP (Access Point), conectados entre sí a través de una red troncal de distribución o DS (Distribution System). Además en algunas ocasiones los DS se agrupan en niveles jerárquicos superiores, formando un ESS (Extended Service Set).

Los IBSS (Isolated BSS) se da cuando no existe un sistema de distribución, sino que el AP únicamente hace de intermediario para la conexión entre dispositivos que se encuentran dentro de su área de cobertura. Una variante del IBBS en la que no existe AP es el modo ad hoc; los dispositivos móviles se comunican directamente entre sí y las funciones de coordinación son asumidas por uno de ellos.

¿Pero que es un protocolo? Los protocolos son reglas y procedimientos para la comunicación, por ejemplo; cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se le denomina protocolo.

1.4 REDES INALAMBRICAS 802.11

Existen diferentes tipos de estándares para las redes inalámbricas de área local. Estos estándares determinan los aspectos físicos de transmisión y recepción, como la velocidad de datos, la frecuencia al a que operan, y las potencias de transmisión.

Para las redes WLAN la IEEE estableció el protocolo 802.11 que presenta las siguientes variantes:

802.11a

Esta variante, a 5 GHz, emplea una modulación 64-QAM y codificación OFDM. Alcanza una velocidad nominal de hasta 54 Mbps con un alcance limitado a 50 metros.

802.11b

Se conoce como Wi-Fi, ofrece velocidades de 11 Mbps, 5.5 Mbps, 2 Mbps y 1 Mbps; y un alcance entre 100 y 300 metros. Trabaja en la banda libre de 2.4 GHz y utiliza una modulación lineal compleja (DSSS).

802.11c

Indica que información se requiere para conectar dos redes entre sí. Únicamente afecta a los fabricantes de puntos de acceso; para el usuario este estándar es transparente.

802.11d

Define los requisitos del nivel físico que garantizan el cumplimiento de las limitaciones regulatorias fuera de Europa, Japón y Estados Unidos.

802.11e

Se encarga de los mecanismos de calidad de servicio; que permiten priorizar diferentes tipos de tráfico, distintas ubicaciones geográficas o departamentos concretos.

802.11f

Especifica un protocolo para el punto de acceso que proporciona la información necesaria para efectuar el roaming entre puntos de acceso de diferentes vendedores.

802.11g

Alcanza las velocidades de 54 Mbps en la banda de 2.4 GHz

802.11h y 802.11j

Interoperación con redes inalámbricas en Europa (802.11h) y en Japón (802.11j).

802.11i

Añade el protocolo de Seguridad AES (Advanced Encryption Standard) al estándar 802.11.

802.11ir

Variante de la 802.11 en la banda infrarroja, que alcanza 1-2 Mbps.

802.11k

Intento de unificar el modo de los estándares a, b y g, que miden las condiciones del entorno radioeléctrico y de la red y las envían a otras partes de la pila de los protocolos. Resulta útil en detección de fallos y otras operaciones de mantenimiento.

802.11m

Conjunto de normas de mantenimiento.

802.11n

Velocidad cercana a los 100 Mbps. Todos los dispositivos 802.11n son compatibles con las normas anteriores.

802.11p

Extiende el estándar 802.11con el fin de soportar comunicaciones inalámbricas a 5.9 GHz.

802.11r

Define un procedimiento de roaming más rápido.

802.11s

Estándar para redes malladas, que no es más que una manera de ruteo de datos.

802.1x

Mecanismos de Autenticación a niveles de puertos.

1.5 RIESGOS DE LAS REDES INALAMBRICAS.

Las redes inalámbricas basadas en el protocolo 802.11 presentan beneficios incuestionables, como son la flexibilidad, reducción de costos de infraestructura, movilidad y una mejor escalabilidad de la red. Sin embargo debido a su medio de transmisión también presentan algunos riegos que pueden afectar directamente algunos factores tales como: la confidencialidad de los usuarios, integridad de la red etc.

Las ondas de radio por sí mismas tienen la posibilidad de propagarse en el medio sin control alguno, por lo tanto es casi imposible controlar su propagación, además la radiación se da en tres dimensiones haciendo que el lóbulo de cobertura pueda incluso pasar a otros plantas dentro de un edificio, el problema de la propagación desmedida de estas ondas es que un intruso podría interceptarlas y acceder a la red sin que tenga autorización.

Existen muchos riesgos que nacen de no tener un sistema de seguridad adecuado para nuestra red:

- Acceso no controlado a la red: En un instante de tiempo dado, un número muy grande de usuarios conectados a la red podría provocar que esta sufra una saturación reflejándose en la disminución del ancho de banda para los usuarios, menor calidad en la intensidad de señal, además de que en cualquier momento un usuario pueda sufrir la perdida de conectividad.

- Intercepción del tráfico en la red: como ya mencionamos las ondas de radio se propagan sin control alguno, esto permite que personas ajenas a ella puedan escuchar el tráfico en la red y poder por ejemplo: capturar contraseñas, leer

información confidencial etc. Existe un cierto nivel de riesgo en caso de ser una red de tipo casera, sin embargo tratándose de una red de tipo empresarial o una red institucional como es el caso de una escuela de nivel superior el riesgo es mucho mayor por obvias razones.

- Acceso no permitido a internet: Un intruso puede ocupar una red inalámbrica con poca o nula seguridad para acceder a internet de forma gratuita atreves de la red sirviendo como entrada a virus o para apoderarse de información confidencial.

1.6 ELEMENTOS DE SEGURIDAD

La seguridad en una red inalámbrica es una característica que nos indica que ese sistema está libre de todo peligro, daño o riesgo; y que es, en cierta manera infalible.

Mantener una red segura consiste en garantizar tres aspectos:

- Confidencialidad. Los objetos de una red han de ser accedidos únicamente por elementos autorizados a ello, y esos elementos no van a convertir esa información en disponible para otras entidades.

- Integridad. Los objetos solo pueden ser modificados por elementos autorizados, y de una manera controlada.

- Disponibilidad. Los objetos del sistema tienen que permanecer accesibles a elementos autorizados.

¿Pero cuáles son las amenazas que se tienen? Los elementos que pueden amenazar un sistema son los siguientes:

- Personas: Las personas que pueden constituir un peligro para la red se dividen en dos grupos: pasivos (aquellos que fisgonean en el sistema pero que no lo destruyen o modifican) y los activos (los modifican y dañan a su objetivo).

- Amenazas lógicas: Son programas que de una forma u otra pueden dañar a nuestra red, ejemplos como los virus, malware, etc.

- Catástrofes: Estas se clasifican en naturales o artificiales.

Bueno ahora se hará mención de los mecanismos de seguridad, el cual es el principal objetivo de este proyecto, ya que con ello controlaremos y administraremos nuestra red de una forma segura.

Los mecanismos de seguridad se dividen en tres grandes grupos: de prevención, de detección y de recuperación.

- Prevención: Son aquellos que aumentan la seguridad de un sistema durante el funcionamiento normal. Por ejemplo el uso de cifrado en las transmisiones, mecanismos de autentificación, control de acceso, etc.
- Detección: Se utilizan para detectar violaciones de seguridad o intentos de violación.

- Recuperación: Son aquellos que se aplican cuando una violación del sistema ha sido detectado, para retornar a éste su funcionamiento correcto. Ejemplo de este punto pueden ser las copias de seguridad o de respaldo.

1.7 SEGURIDAD INALAMBRICA

En las redes inalámbricas cualquiera dentro del radio de cobertura del punto de acceso es un intruso potencial, por este motivo las acreditaciones del usuario se deben de poder intercambiar con seguridad, además de esto se debe de asegurar la conexión con la red de trabajo, los datos se deben de poder transmitir con seguridad a través de la red.

Algunas herramientas de seguridad disponibles son las que a continuación se describen.

1.7.1 WEP

Es el sistema de cifrado incluido dentro del estándar IEEE 802.11 como protocolo para redes Wireless, proporciona cifrado a nivel dos, está basado en el algoritmo de cifrado RC4. Para poder cifrar las tramas de información el protocolo WEP se basa en dos algoritmos:

CRC (algoritmo de chequeo de integridad).

RC4 (algoritmo de cifrado) RC4 es un algoritmo de cifrado de flujo, funciona expandiendo una semilla para generar una secuencia de números pseudoaleatorios. Esta secuencia de números se unifica con el mensaje pasando por una compuerta XOR, de esta manera se obtiene un mensaje cifrado, sin embargo un problema que se presenta aquí es que no se debe usar la misma semilla para cifrar dos mensajes diferentes ya que de esta manera se podría obtener la clave a partir de la obtención de los textos cifrados resultantes. Sin embargo para evitar eso WEP especifica un vector de inicialización de 24 bits que se modifica regularmente y se concatena a la contraseña que se va a cifrar y es a través de la concatenación que se genera la semilla que sirve de entrada al algoritmo RC4, de esta manera se evitan secuencias iguales y se crean semillas nuevas cada vez que el vector varia.

Su principal defecto es que aunque se pueden generar gran variedad de vectores y semillas, en un punto de acceso se conecta un número considerable de usuarios haciendo que la cantidad de tramas que circulan través del sea grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de inicialización y por lo tanto sea relativamente fácil dar con la clave.

1.7.2 WPA

Es un sistema utilizado para proteger las redes inalámbricas (WI-FI), fue creado para corregir los problemas de WEP. Fue diseñado para la utilización de servidor de autentificación, que es generalmente un servidor RADIUS, que distribuye claves diferentes a cada usuario, esto se hace mediante el protocolo 802.1x, como se dijo anteriormente WPA se creo para corregir solventar deficiencias, sin embargo su funcionamiento es el mismo con la diferencia que WPA incorpora claves de 128 bits y el vector de inicializaciones de 48 bits y la información sigue siendo cifrada mediante el algoritmo RC4. una de las mejoras es la implementación del protocolo de integridad de clave temporal TKIP- Temporal Key Integrity Protocol, que tienen la función de cambiar claves dinámicas cada vez que el sistema es utilizado.

Existen dos versiones de WPA

a) Para el uso personal domestico: En esta versión se utiliza el protocolo TKIP, este mecanismo es empleado para crear el cifrado de clave dinámico. TKIP solventa las carencias de WEP ya que las claves son dinámicas aporta un importante nivel de seguridad para la red.

b) Para el uso empresarial: En esta versión de usa el protocolo EAP que se emplea durante el intercambio de mensajes en el proceso de autentificación, mediante un servidor RADIUS que funciona a través del protocolo 802.1x

1.7.3 WPA2

Esta actualmente disponible en los puntos de acceso mas modernos existentes en el mercado, aunque realmente no llego para sustituir a WPA ya que estos dos son totalmente compatibles, la principal diferencia es que WPA2 para el cifrado de los datos necesita el protocolo AES (estándar avanzado de cifrado), mientras que WPA original emplea TKIP. Las ventajas de este tipo de cifrado es que necesita poca memoria lo que lo hace muy rápido tanto en software como en hardware y además es muy fácil de implementar. Cabe mencionar que el tamaño de bloque fijo es de 128 bits y los tamaños de llave son de 128, 192 ó 256 bits, así al incrementar el tamaño de los bloques el número de llaves en uso y al agregar un sistema de verificación de mensajes hace que la entrada no autorizada a redes inalámbricas sea más difícil.

1.7.4 802.1x/EAP

El protocolo IEEE 802.1x se basa se basa en el control de puerto de conexión, este puerto será abierto una vez que el cliente cumpla de manera satisfactoria un proceso de autentificación.

Este protocolo define tres términos importantes:

- ✓ Servidor de Autenticación: Es el responsable de llevar a acabo una buena autenticación.

- ✓ Autenticador: Es el elemento intermedio una vez que el usuario haya sido autentificado.

- ✓ Solicitante: Usuario o cliente que desea ser autentificado.

EAP

(Extensible Authentication Protocol) sirve como soporte a protocolos de autenticación donde administra las contraseñas en mecanismos llamados de desafío-respuesta. Este protocolo se sigue de la siguiente forma:

1. El autenticador envía un paquete “EAP-REQUEST IDENTITY” (Solicitud de Identidad) al usuario tan pronto como detecte que el acoplamiento está activo.

2. El usuario envía un paquete de “EAP-RESPONSE-IDENTITY” al autenticador (Respuesta de Identidad), que pasa directamente al servidor de autenticación.

3. El servidor de la autenticación envía un desafío al autenticador, el autenticador desempaqueta el contenido del paquete IP, lo empaqueta de nuevo en EAPOL (encapsulamiento definido para redes LAN Ethernet cableada o inalámbrica para pasar por EAP) y lo envía al usuario.

4. El usuario responde al desafío vía el autenticador y pasa la respuesta al servidor de autenticación.

5. Si el usuario proporci

6. ona una identidad correcta, el servidor responde con un mensaje de éxito al autenticador, y que es pasado así mismo al usuario. El autenticador permite a partir de ese momento el acceso a la red al usuario.

Aunque existen varios tipos de EAP los cuales se mencionan a continuación:

1. EAP-Cisco Wireless (LEAP): Requiere una infraestructura Cisco Wireless.

2. EAP-MD5: Este es basado principalmente en nombres de usuario y contraseñas.

3. EAP-PEAP: Sin certificados, utiliza también TLS para establecer un túnel de cifrado.

4. EAP-TLS: Requiere la distribución de certificados de autenticación tanto a los usuarios como a los servidores de autenticación.

5. EAP-TTLS: Requiere de la distribución de certificados digitales a todos los servidores de Autenticación pero no a los usuarios, por lo tanto es más flexible.

6. EAP-SIM: Emplea el SIM y el PIN de una tarjeta de teléfono móvil.

1.7.5 FALSOS AP´s Y SEÑUELOS

Esta medida de seguridad consiste principalmente en simular la existencia de un gran número de AP´s (Puntos de Acceso), para así poder distraer a nuestros posibles atacantes, con esto se tardarían mucho tiempo en encontrar el verdadero AP.

Todo este proceso es realizado a través de un programa para GNU/Linux que se encarga de realizar esta actividad. Este programa cuenta con una lista de nombres de las redes inalámbricas más utilizadas normalmente con los nombres que vienen al comprar un AP de las diferentes marcas y también cuenta con una lista de direcciones de MAC congruentes con esos nombres. Además cuenta con el canal con el que queremos que se emitan los falsos AP´s.

1.7.6 VPN´s e IPSEC

Una VPN es una red privada virtual. Se utiliza para interconectar redes dispersas de una organización creando con ello que una red pública como internet pueda ser utilizada como una red privada. Es privada porque se utilizan métodos de cifrado de datos y autenticación de servidores que pretenden entrar a la red. Y es virtual porque la red no está interconectada directamente sino que utilizan túneles cifrados a través de internet. Las VPN´s se utilizan para que un usuario móvil sea capaz de utilizar la red de su empresa desde cualquier punto como puede ser un AP.
Existe un gran número de tecnologías para crear las redes privadas y diversos protocolos como lo puede ser:

- PPT (Point to Point Tunneling Protocol)
- L2TP (Layer 2 Tunneling Protocol)
- IPSEC (Internet Protocol Security)

Hoy en día IPSEC es la tecnología más robusta en cuanto a la solución de autenticación de usuarios y equipos.

1.7.7 PORTALES CAUTIVOS

Es un sistema que permite controlar el acceso a redes inalámbricas. La arquitectura de este sistema consiste en:

1. Un Gateway que encamina las conexiones.
2. Un servidor de autenticación que define el perfil de cada una de las conexiones y que designa las partes de la red que podrá visitar en consecuencia.

Para ello se definen tres tipos de perfiles:

1. Invitado.
2. Miembro.
3. Propietario.

Estos perfiles son ordenados de menor a mayor nivel en cuanto a privilegios de la red. Para implementar este tipo de sistema será necesario un programa como NoCatAuth que es un software de GNU/Linux que sirve para la implementación de portales cautivos.

1.7.8 802.11i

Es un nuevo protocolo de seguridad aún no establecido que define una serie de sistemas de cifrado y autenticación AES “Advanced Encryption Standard” y TKIP “Temporal Key Integrity Protocol” para disminuir la posibilidad de que la clave empleada en el cifrado sea rota por un atacante.

Capítulo 2

ANALISIS DEL PROBLEMA

2.1 ANTECEDENTES

La red del Instituto Politécnico Nacional está conformada principalmente por fibra óptica, enlaces de microondas y enlaces de satélite, ésta consta de tres nodos principales que son: nodo Zacatenco, nodo Santo Tomas y nodo UPIICSA, el tendido de la red de fibra óptica se realizo a través de la red del sistema de transporte colectivo metro y éste enlaza a los tres nodos mencionados, mientras que los enlaces de microondas son fijos entre estos tres nodos, además de sus nodos secundarios; y se tiene una cobertura satelital en toda la república mexicana, algunos de los servicios que se brindan a través de esta red son: telefonía, datos videoconferencia y teleconferencia y por supuesto servicio de internet.

En los diferentes centros y unidades del instituto se cuenta con infraestructura para poder utilizar estos servicios y sin lugar a dudas el más utilizado entre los alumnos y administrativos es el servicio de internet mismo que ha servido como puerta de entrada a una gran cantidad de usuarios maliciosos, principalmente, desde las redes inalámbricas por medio de los puntos de acceso que se encuentran abiertos a todo usuario que cuente con una computadora portátil. La falta de un control de acceso y autenticación ha provocado que el servicio de acceso inalámbrico a la internet no se abra completamente para la utilización por parte de los usuarios que en su mayoría son alumnos.

Hablando específicamente de la ESIME Zacatenco, hasta la fecha no se ha podido brindar el servicio de internet inalámbrico a los alumnos debido al mismo problema; la falta de un control de acceso y autenticación; se dice que la infraestructura física existe, sin embargo por cuestiones de seguridad institucional esta infraestructura no se explota en beneficio de la comunidad de ESIME.

2.2 EL MUNDO MODERNO Y LAS REDES INALÁMBRICAS

Una de las tecnologías que en la actualidad se encuentra en plena expansión es la de poder comunicarnos a través de una computadora por un medio inalámbrico, ya que esto representa muchas ventajas entre las que se encuentran; la movilidad que un usuario puede tener dentro del área de cobertura, ahorro de costos, flexibilidad de crecimiento, entre otras. Esta serie de ventajas ha propiciado que ahora las empresas y diferentes organizaciones prefieran invertir y hacer crecer sus redes por medio de esta tecnología y evitar las modificaciones físicas y estructurales que muchas veces representa la instalación de una red cableada.

Sin lugar a dudas las redes inalámbricas se han expandido de tal manera que ahora estas las podemos encontrar en lugares como: empresas privadas, empresas públicas, hospitales, edificios públicos, parques, escuelas etc. Incluso, actualmente esta tecnología es utilizada como un atractivo extra en algunos centros comerciales y restaurantes en los

que se ofrece el servicio de internet inalámbrico; usted como usuario llega al restaurante y mientras le sirven el desayuno puede sacar su computadora portátil y navegar en la red, revisar correo electrónico, hacer transferencias bancarias etc. Todo esto representa para los usuarios una serie de ventajas por ejemplo, para los estudiantes la misma computadora con la que se conectan a internet en su casa, la pueden trasladar hasta la escuela y utilizarla para el mismo fin sin la necesidad de tener que solicitar un cable para esto.

Pero actualmente la tecnología inalámbrica no se está limitando al uso de laptops, en estos tiempos la tecnología inalámbrica esta abarcando el uso de los llamados Gadgets; un Gadget es un dispositivo que tiene un propósito o función específica, este dispositivo generalmente es de proporciones físicas reducidas y está elaborado a base de un diseño novedoso; algunos ejemplos de estos aparatos son los ipods, PDA, PSP etc., pensados para proporcionar información útil o para mejorar aplicaciones por ejemplo de la web, hoy en día estos dispositivos se han vuelto muy populares entre la gente, principalmente por sus aplicaciones web y sin lugar a dudas esta tecnología va a seguir escalando lugares entre las preferencias de los usuarios ya que estos dispositivos sumados a sus aplicaciones web representan innumerables ventajas, además de no tener que cargar con nuestra laptop, ya que como se dijo anteriormente estos dispositivos son de tamaño reducido y con estos mismos podemos tener acceso a internet a través de una red inalámbrica, descargar archivos, consultar correos electrónicos, intercambiar información con otros usuarios etc.

Hoy en día las redes inalámbricas han abarcado incluso ciudades completas, estas ciudades como: Seúl, Londres, Tokio, entre otras grandes ciudades del mundo cuentan con conexiones de red inalámbrica a través de tecnologías como wi-fi y wi-max, tecnologías que brindan servicio a las poblaciones de dichas ciudades. Sin lugar a dudas las redes inalámbricas es una tecnología en pleno desarrollo ya que poco a poco se están aplicando en diferentes áreas de la vida cotidiana.

- Entretenimiento: ahora con las redes inalámbricas podemos disfrutar de un partido de futbol, ver un concierto o programas de televisión, incluso escuchar estaciones de radio completamente en vivo.

- Negocios: en la actualidad podemos hacer compras y ventas de productos desde internet además podemos hacer transferencias bancarias, consultar cuentas etc.

- Investigación: una de las principales aplicaciones de las redes inalámbricas es la de dar cobertura a centros de investigación por ejemplo las escuelas, hoy en día existen centros de educación superior que están implementando en sus campus la tecnología Wi-Fi, que es una tecnología inalámbrica, esto con la finalidad de brindar el servicio de acceso a internet a sus estudiantes.

- Educación: en la actualidad los centros de educación ofrecen la opción de cursar alguna carrera a través de internet, el llamado modelo de educación a distancia está basado precisamente en esta tecnología y con las redes inalámbricas el alumno puede tener acceso a sus actividades escolares en cualquier zona que cuente con cobertura de red inalámbrica incluso por ejemplo desde un restaurante, un centro comercial etc.

- Foros: Existen muchos foros de discusión o ponencias que se realizan a través de internet, la ventaja que en este sentido proporcionan las redes inalámbricas es que los participantes pueden tener movilidad y no estar precisamente en una oficina fija.

Actualmente en el Instituto Politécnico Nacional se tiene la necesidad de implementar un proyecto de una red inalámbrica institucional, es decir una red inalámbrica que tenga cobertura en cada centro, escuela y unidad. Esto obedece a que del Instituto Politécnico Nacional egresan profesionales de gran calidad, por lo cual el Instituto posee un gran prestigio, prestigio que se debe mantener no solo con su calidad humana si no también con su infraestructura tanto material como tecnológica.

La infraestructura tecnológica es una de las partes más importantes para el desarrollo de investigación dentro del instituto y es precisamente una red inalámbrica eficiente un gran bloque de esta infraestructura tecnológica ya mencionada, sin embargo para que sea eficiente se deben tomar en cuenta varios aspectos tanto en el diseño como en la puesta en operación, y es precisamente esta una parte muy compleja ya que esta red debe funcionar en todas las escuelas centros y unidades del Instituto, un usuario debe poder tener conectividad en cualquier zona de cobertura no importando que esta se encuentre en diferentes centros de estudio del Instituto con la misma contraseña y el mismo nombre de usuario, el uso de contraseña y nombre de usuario posibilita de cierta forma el poder tener un control de acceso a la red, ya que ésta debe brindar el mejor servicio posible pero únicamente a las personas autorizadas para hacer uso de este servicio, esto ayuda a varias cosas por ejemplo: el consumo del ancho de banda beneficia únicamente a la comunidad politécnica mientras que al mismo tiempo impide que usuarios mal intencionados hagan uso de la red para cometer acciones ilegales desde esta.

Una manera eficiente de controlar el acceso a la red es contar con un sistema que permita identificar el propietario de la contraseña y el nombre de usuario, mediante un registro previo de este.

2.3 ESTADO ACTUAL DEL SERVICIO DE CONEXIÓN INALAMBRICA PARA EL USO DE INTERNET EN ESIME ZACATENCO

Dentro de las instalaciones de la ESIME Zacatenco encontramos una serie de problemas que se deben corregir para llevar a cabo una buena administración y control al acceso a la red, y poder dar un servicio de calidad a la comunidad de la ESIME Zacatenco.

- Puntos de acceso abiertos: Los puntos de acceso con los que se cuenta no tienen implementado un sistema de seguridad, esto implica que cualquier persona puede llegar a la zona de cobertura y poder tener el acceso a internet, incluso el radio de cobertura alcanza zonas fuera de las instalaciones de la unidad Zacatenco, por tanto persona ajena al instituto puede hacer uso del servicio utilizando un ancho de banda que podría ser utilizado por algún miembro de la comunidad politécnica.

- Puntos de acceso piratas: Al no contar con el servicio de acceso a internet inalámbrico oficial ha provocado la instalación de puntos de acceso no autorizados,

sin seguridad, y no tomando en cuenta las zonas de mayor demanda por lo que solo cubre necesidades particulares.

- Mala ubicación de los puntos de acceso: se tiene el conocimiento de que se han entregado puntos de acceso a la escuela, pero solo algunos de estos han sido habilitados con una mala ubicación ya que no se toma en cuenta el número de usuarios que requieren del servicio.

- Puntos de acceso insuficientes: El hecho de no contar con un sistema de control de acceso limita la instalación de todos los puntos de acceso, haciendo insuficiente el servicio, esto provoca que en donde hay puntos de acceso abiertos se concentre un mayor número de usuarios, y esto se ve reflejado en una disminución del ancho de banda, haciendo que la red se vuelva lenta

2.4 LA EDUCACION DE LOS INGENIEROS REQUIERE APOYARSE EN LA RED PARA MEJORAR EL APRENDIZAJE

Como sabemos una de las ventajas de las redes inalámbricas es la movilidad, esto nos permite conectarnos a la red desde cualquier punto dentro del área de cobertura, además actualmente los nuevos equipos de cómputo que se venden en el mercado cuentan con tarjetas de red inalámbrica y existen diferentes tipos de dispositivos comúnmente llamados gadgets que ya cuentan con esta tecnología, y que su principal objetivo es la de proveer información haciendo uso del servicio del internet.

Contando con estos equipos que son ahora más accesibles para adquirirlos y con la estructura adecuada para una red inalámbrica, la productividad de los alumnos, profesores y en general de la comunidad politécnica se verá beneficiada, se podrá consultar de manera eficiente y en tiempo real información en el internet que ayude a los profesores impartir de manera más eficaz y dinámica sus clases evitando con esto interrupciones en sus exposiciones por no recordar alguna información u otra situación semejante.

Otro de los beneficios de este servicio es la eliminación de tiempo de espera que los alumnos tienen que tomar para que se les brinde este servicio ya sea que se les proporcione un equipo de un laboratorio o que se tenga que trasladar a un centro como por ejemplo el centro de apoyo polifuncional (CAP) donde se les brinda el servicio pero que en ocasiones los equipos disponibles son insuficientes para cubrir la demanda.

Hay que señalar que actualmente existen profesores que exigen a sus alumnos hacer uso de diferentes herramientas como lo son las páginas virtuales en donde llevan a cabo foros de discusión, entrega de tareas y trabajos, impartición de calificaciones, etc. Facilitando con esto a los profesores para tener una mejor administración de la información de sus alumnos y de sus evaluaciones, y por el otro lado ayuda a los alumnos a realizar sus actividades de manera más productiva desde cualquier equipo de computo portátil o con los dispositivos (gadgets) como lo son los PDA, iPod, etc., aunque estos últimos tienen la limitante de que solo se pueden conectar a redes con baja o nula seguridad

Conjuntando todos estos beneficios visualizamos por poner un ejemplo a un profesor que está impartiendo su clase ya sea en un salón común o en un laboratorio, y que necesita que buscar cierta información para resolver un problema, inmediatamente un alumno con equipo de cómputo portátil busca en internet la información y en cuestión de unos segundos su alumno le proporciona la información solicitada a su profesor, la clase continua y se resuelve el problema por el profesor, sin embargo, ahora es turno de que los alumnos apliquen lo aprendido en clase y el profesor les pide que realicen una serie de ejercicios.

Pero existe un problema el tiempo de clase se ha terminado, por lo que el profesor les pide que le envíen las tareas a una página de una plataforma web evitando con ello las impresiones en hojas de sus trabajos y que las herramientas necesarias para contestar sus ejercicios (archivos de texto, imágenes, software, etc.) las pueden descargar de la misma página, además el profesor les menciona que si tienen dudas acerca de la tarea el profesor se encuentra disponible para aclarar dudas a través de un foro en internet a una hora en especifico.

Sin lugar a dudas el contar con un servicio de red inalámbrica ayuda a potencializar el rendimiento de los usuarios, en este caso principalmente de los profesores y alumnos que se les abre una serie de opciones para hacer uso de muchas herramientas que apoyen el desarrollo académico de las escuelas y acercando aún más todo lo necesario para su formación dentro del instituto.

2.5 LA TECNOLOGIA Y LOS ALUMNOS

Actualmente las aplicaciones de la internet han llegado a la vida cotidiana de los estudiantes de la ESIME Zacatenco ya que muchas investigaciones se realizan a través de ella, el descargar manuales, descargar software libre, subir tareas a la red, mandar correos electrónicos a sus profesores, etc., son solo algunos de los usos que los alumnos le dan a la red, cabe destacar que la puesta en operación de una red inalámbrica en las instalaciones de ESIME no sería algo inútil o algo que tuviera poco uso, ya que como se ha mencionado gran parte de las tareas escolares se realizan a través de la internet, por otra parte hoy en día la tecnología en general ha adquirió costos accesibles para la mayoría de la población estudiantil, y las computadoras personales no son la excepción, hoy en día muchos alumnos tienen una laptop que bien pueden utilizar en caso de que se instalara una red inalámbrica en la ESIME.

2.6 EVALUACION DE LA DEMANDA DEL SERVICIO

Dentro del Instituto Politécnico Nacional la ESIME Zacatenco es una de las escuelas con mayor número de estudiantes, principalmente en la carrera de Ingeniería en Comunicaciones y Electrónica, el reto de proveer el servicio a las instalaciones de la ESIME es complejo, aunque el punto que nosotros vamos a tratar será el de la administración del sistema de autenticación.

Actualmente la ESIME atienda aproximadamente a más de 9,000 alumnos. Hay que agregar también un estimado de los profesores que harían uso de la red. Por lo que la

estructura para dar administración y controlar las redes inalámbricas deberá de cubrir esta demanda.

Otra característica que debemos de tomar en cuenta es el crecimiento estimado del número de nuevos usuarios que demandará este servicio, considerando que hay mayor accesibilidad en los precios de los equipos de cómputo y por tanto el número de usuarios crecerá de manera acelerada, además de que el acceso a internet ya no es solo por medio de los equipos de computo si no también es importante mencionar que los gadgets cuentan con los recursos necesarios para conectarse a internet de forma inalámbrica enlazándose por medio de los puntos de acceso.

Gracias a datos proporcionados por el departamento de control escolar obtuvimos los siguientes datos que se refieren al número de estudiantes que actualmente están inscritos en la ESIME, otro dato importante a considerar es el número de profesores que imparten clases en la unidad y que son usuarios que pueden hacer uso de la red inalámbrica.

Tabla 1
Cantidad de alumnos por carrera y semestre en ESIME Zacatenco [1]

SEMESTRE	ICE	ICA	IE	ISA
1º	1349	299	438	45
2º	746	124	181	0
3º	923	271	362	38
4º	556	142	202	0
5º	638	206	207	0
6º	382	85	96	0
7º	434	147	181	0
8º	242	37	60	0
9º	422	161	206	0
TOTAL	5692	1472	1924	83

Total de alumnos en ESIME Zacatenco: **9171**

Tabla 2
Cantidad de profesores que imparten clases en la ESIME Zacatenco [2]

	ICE	ICA	IE	ISA	SEPI
PROFESORES	458	106	274	26	114

Total de profesores en ESIME Zacatenco: **978**

Para estimar el número de usuarios que requieren el servicio de conexión a internet de forma inalámbrica necesitaremos realizar una encuesta que proporcione estos datos. El primer paso es definir el tamaño de la muestra para ello utilizaremos un método estadístico llamado muestreo aleatorio simple.

Con los datos obtenidos podemos definir que contamos con una población finita, es decir se conoce el total de la población que vamos a analizar y necesitamos conocer cuántos de ellos se deben tomar en cuenta para poder tener un buen nivel de confianza.

[1] Información obtenida de Control escolar ESIME Zacatenco.
[2] Información obtenida del departamento de recursos humanos de ESIME Zacatenco

Para ello haremos uso de la siguiente fórmula que corresponde al muestreo aleatorio simple.

$$n = \frac{N * Z_{\alpha}^{2} * p * q}{d^{2} * (N-1) + Z_{\alpha}^{2} * p * q}$$

Fórmula para calcular el tamaño de una muestra

Donde:

- N = Total de la población.
- Z_{α}^{2} = Nivel de confianza.
- p = Probabilidad de éxito.
- q = Probabilidad de fracaso.
- d = Precisión.

Las recomendaciones para este método de muestreo son:

- Es recomendable utilizar rangos de confianza mayores de 90%; a cada nivel de confianza le corresponde un coeficiente $Z_{\propto}$.

Tabla 3
Porcentajes y coeficientes de confianza para una muestra

Confianza	Coeficiente $Z_{\propto}$
90 %	1.64
95 %	1.96
97.5 %	2.24
99 %	2.57

- Es recomendable utilizar niveles de precisión de entre 1% y 2%

En el caso particular de este análisis se utilizara un nivel de confianza del 95% al cual le corresponde un coeficiente $Z_{\propto}$de 1.96.

Nuestros datos son:

- N = 9171
- Z_{α}^{2} = 1.96^{2}
- p = 95%
- q = 5%
- d = 1% y 2%

Numero de muestras necesarias con una precisión de 1%

$$n = \frac{10149 * 1.96^{2} * 0.95 * 0.05}{0.01^{2} * (10148) + 1.96^{2} * 0.95 * 0.05} = 1546\ muestras$$

Numero de muestras necesarias con una precisión de 2%

$$n = \frac{10149 * 1.96^{2} * 0.95 * 0.05}{0.02^{2} * (10148) + 1.96^{2} * 0.95 * 0.05} = 437\ muestras$$

Como podemos observar en estos resultados calculados la variación del número de muestras de un punto porcentual a otro es muy amplia así que se tomo la decisión de tomar un grado de precisión de 1.5%. De esta manera se tomo la decisión de hacer un total de 878 encuestas.

Para estimar el número de usuarios de la red dentro de la ESIME llevamos a cabo una encuesta en los diferentes semestres de la carrera tomando como muestra a grupos de forma aleatoria, realizamos las siguientes preguntas en forma grupal:

I. ¿Cuántos alumnos del grupo que cuentan con laptop que hacen uso de red inalámbrica?

II. ¿Cuántos de los alumnos que no cuentan con una laptop piensan adquirir un equipo en un lapso de 6 meses?

En la siguiente tabla se muestran los resultados y con estos datos obtendremos un porcentaje del número de usuarios o clientes de la red con respecto al número total de alumnos.

Tabla 4
Muestra de equipos potenciales a utilizar la red

SEMESTRE	I	II	No. De Grupos Muestra	Total Alumnos Inscritos
1º	8	8	3	114
2º	6	7	3	100
3º	10	8	3	109
4º	13	4	3	90
5º	11	9	3	97
6º	12	15	3	93
7º	14	25	3	125
8º	30	10	3	83
9º	28	8	3	67
TOTAL	132	94	27	878

En la siguiente tabla obtenemos los porcentajes para cada pregunta realizada y se realiza el cálculo con respecto al total de alumnos de la muestra.

Tabla 5
Porcentajes de usuarios potenciales con respecto al total de la muestra

I	II	Total
15.03%	10.70%	25.73%

Tabla 6
Número de usuarios estimados para el total de alumnos y maestros

Total de alumnos en ESIME	Total de profesores	Total	Total de usuarios estimados	Total de usuarios estimados a 6 meses
9171	978	10149	1525	2611

Con respecto a la muestra anterior se estima que para la población actual de la ESIME se tengan a más de 1500 usuarios, y se espera que a 6 seis meses sean más de 2000 usuarios.

2.7 ADMINISTRACION ACTUAL DE LA RED INSTITUCIONAL

La red del Instituto Politécnico Nacional está divida en varias subredes y es administrada de forma centralizada desde el DCYC (Dirección de Cómputo y Comunicaciones).

La administración de la red la llevan a cabo por medio de un directorio de usuarios y de equipos que pertenecen a un dominio (Directorio Activo), en el DCYC se encuentran anexados cada uno de los servidores de las escuelas pertenecientes al instituto.

Por medio de este sistema se pueden soportar a miles de usuarios y equipos sin ningún problema y con ello tener la facilidad de implementar varias aplicaciones como la del correo electrónico institucional, manejo de información de las diferentes escuelas (trayectoria académica de sus alumnos, respaldos de información, etc.).

El directorio activo implementado en la red del Instituto Politécnico Nacional esta creado bajo la plataforma de Microsoft a través del Windows Server 2003. Este software le permite al instituto llevar a cabo su administración de forma eficaz utilizando herramientas que pueden ser agregadas al sistema operativo sin costo alguno, una herramienta que utilizaremos para el desarrollo de nuestro proyecto será el IAS (Servicio de Autenticación de Internet) el cuál nos ayudará a implementar un sistema de autenticación que nos servirá para administrar y controlar el acceso a redes inalámbricas.

Capítulo 3

IAS

3.1 INTRODUCCIÓN

El Servicio de autenticación de Internet (IAS, Internet Authentication Service) en Microsoft® Windows Server™ 2003, es la implementación de Microsoft de un servidor RADIUS, IAS se encarga de manera centralizada de la autenticación, autorización y de las cuentas de conexión de muchos tipos de accesos a la red entre ellos el inalámbrico.

Cuando un servidor IAS es miembro de un dominio de Directorio Activo (Active Directory), IAS utiliza el servicio de directorio como su base de datos de cuentas de usuario y forma parte de una solución de inicio de sesión. El mismo conjunto de credenciales se utiliza para controlar (autenticar y autorizar) el acceso a la red.

Las organizaciones y empresas que mantienen el acceso a la red han visto incrementado el reto de administrar todos los tipos de acceso a la red desde un punto de administración único. El estándar RADIUS admite esta funcionalidad en sistemas informáticos que comparten o no la misma arquitectura. RADIUS es un protocolo cliente-servidor que permite que el equipo de acceso a la red (utilizado como clientes RADIUS) envíe solicitudes de administración de cuentas y autenticación a un servidor RADIUS.

Un servidor RADIUS tiene acceso a información de cuentas de usuario y puede comprobar las credenciales de autenticación de acceso a la red. Si las credenciales del usuario son auténticas y se autoriza el intento de conexión, el servidor RADIUS autoriza el acceso del usuario basándose en las condiciones especificadas, y registra la conexión de acceso a la red en un registro de cuentas. El uso de RADIUS permite la recopilación y el mantenimiento de los datos de autenticación, autorización y cuentas de usuario para el acceso a la red en una ubicación central, en lugar de en cada servidor de acceso.

3.2 CARACTERISTICAS DE IAS

El servicio de autenticación de Internet (IAS) es compatible con las características siguientes:

- ✓ **Varios métodos de autenticación:**

IAS es compatible con varios protocolos de autenticación y permite agregar métodos personalizados que cumplan los requisitos de autenticación. Los métodos de autenticación compatibles son:

- Los protocolos de autenticación Punto a punto (PPP, Point-to-Point Protocol) basados en contraseña.

Los protocolos de autenticación PPP basados en contraseña, como Protocolo de autenticación de contraseña (PAP, Password Authentication Protocol), Protocolo de autenticación por desafío mutuo (CHAP, Challenge Handshake Authentication Protocol),

Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP, Microsoft Challenge Handshake Authentication Protocol).

- Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol)

Infraestructura basada en estándares de Internet que permite la incorporación de métodos de autenticación arbitrarios, como tarjetas inteligentes, certificados, contraseñas de un solo uso y tarjetas testigo.

- ✓ **IAS es compatible con**:

- EAP-Síntesis de mensaje 5 (MD5, Message Digest 5), el desafío de síntesis de mensaje 5 (Desafío-MD5) es un tipo de EAP requerido que utiliza el mismo protocolo de desafío mutuo que CHAP basado en PPP, con la diferencia de que los desafíos y las respuestas se envían como mensajes EAP. Desafío-MD5 suele utilizarse para autenticar las credenciales de los clientes de acceso remoto mediante sistemas de seguridad que usan nombres de usuario y contraseñas.

- EAP-Seguridad de nivel de transporte (EAP-TLS, EAP-Transport Level Security), se utiliza en entornos de seguridad basados en certificados. Si está utilizando tarjetas inteligentes para la autenticación de acceso remoto, debe utilizar el método de autenticación EAP-TLS. El intercambio de mensajes EAP-TLS permite la autenticación mutua, la negociación del método de cifrado y la determinación de claves cifradas entre el cliente de acceso remoto y el autenticador. EAP-TLS proporciona el método de determinación de claves y autenticación más eficaz.

- ✓ **Proxy Radius:**

IAS permite que las solicitudes RADIUS entrantes se reenvíen a otro servidor RADIUS para el proceso de autenticación y autorización o cuentas. Como proxy RADIUS, IAS se puede emplear siempre que la solicitud RADIUS se deba enrutar a otro servidor RADIUS. IAS puede reenviar solicitudes basándose en el nombre de usuario, la dirección IP del servidor de acceso, el identificador del servidor de acceso u otras condiciones.

- ✓ **Autenticación y autorización de usuarios centralizadas**

Las directivas de acceso remoto proporcionan una forma más flexible y eficaz de administrar los permisos de acceso remoto. Puede autorizar el acceso a la red basándose en diversas condiciones, por ejemplo:

- La pertenencia de la cuenta de usuario a un grupo.

- La hora o el día de la semana.

- El tipo de medios a través de los que se conecta el usuario (por ejemplo, conexión inalámbrica, conmutador Ethernet, módem o VPN).

- El número de teléfono al que llama el usuario.

- El servidor de acceso desde el cual se recibió la solicitud.

- Si configura perfiles en las directivas de acceso remoto, puede controlar muchos parámetros de conexión, como:

- El uso de métodos de autenticación específicos.

- El tiempo de espera de inactividad.

- El tiempo máximo de una sola sesión.

- El número de vínculos en una sesión multivínculo.

- El uso de cifrado y su seguridad.

- El uso de filtros de paquetes para controlar los elementos a los que puede tener acceso el usuario de acceso remoto cuando se conecta a la red. Por ejemplo, puede utilizar filtros para controlar las direcciones IP, los hosts y los puertos que el usuario puede utilizar para enviar o recibir paquetes.

- La creación de un túnel obligatorio que forzosamente y de forma segura envíe todos los paquetes de dicha conexión a través de Internet de forma que terminen en una red privada.

✓ **Escalabilidad**

IAS puede utilizarse en diversas configuraciones de red de distinto tamaño, desde servidores independientes para redes pequeñas hasta grandes redes de ISP y organizaciones.

✓ **Puntos de acceso inalámbrico**

Mediante las directivas de acceso remoto y la condición del tipo de puerto Wireless-IEEE 802.11, IAS se puede emplear como servidor RADIUS en los puntos de acceso inalámbrico que utilizan RADIUS para la autenticación y autorización de nodos inalámbricos.

3.3 PROTECCION DEL IAS

Secretos compartidos

Un secreto compartido es una cadena de texto que sirve como contraseña entre:

- Un cliente RADIUS y un servidor RADIUS.

- Un cliente RADIUS y un proxy RADIUS.
- Un proxy RADIUS y un servidor RADIUS.

Los secretos compartidos se utilizan para comprobar que los mensajes RADIUS, a excepción del mensaje Access-Request (Petición de acceso), son enviados por un dispositivo compatible con RADIUS que está configurado con el mismo secreto compartido. También comprueban que no se ha modificado el mensaje RADIUS durante la transmisión (integridad del mensaje). Asimismo, se utilizan para cifrar algunos de los atributos RADIUS, como User-Password (Usuario - Contraseña). Para proporcionar confirmación de mensajes Access-Request, puede habilitar el uso del atributo autenticador de mensaje RADIUS tanto en el cliente RADIUS configurado en el servidor IAS como en el servidor de acceso.

Al crear y utilizar un secreto compartido:

- Se debe utilizar el mismo secreto compartido que distingue mayúsculas y minúsculas en ambos dispositivos RADIUS.

- Utilizar un secreto compartido diferente para cada servidor-cliente RADIUS.

- Para asegurarnos de que el secreto compartido es aleatorio, hay que generar una secuencia aleatoria de al menos 22 caracteres.

- Se puede utilizar cualquier carácter alfanumérico o especial estándar.

- Se puede utilizar un secreto compartido de hasta 128 caracteres de longitud. Para proteger el servidor IAS y los clientes RADIUS de ataques violentos, hay que utilizar secretos compartidos largos (más de 22 caracteres).

- Los secretos compartidos deben estar formados por una secuencia aleatoria de letras, números y signos de puntuación y se deben cambiar con frecuencia para proteger el servidor IAS y los clientes RADIUS de ataques de diccionario. Los secretos compartidos deben contener caracteres de cada uno de los tres grupos.

Cuanto más seguro sea el secreto compartido, más seguros serán los atributos (por ejemplo, los utilizados para contraseñas y claves de cifrado). Un ejemplo de secreto compartido seguro es 8d#>9fq4bV)H7%a3-zE13sW.

Protección del Active Directory

Active Directory ofrece a la organización un directorio seguro gracias a que ofrece una autenticación de inicio de sesión y la autorización de usuarios integradas. Para proporcionar aun más protección Active Directory considera las siguientes recomendaciones y precauciones:

- ✓ **Una contraseña segura:**

- ➢ Tiene siete caracteres como mínimo

- ➢ No contiene el nombre del usuario; nombre real o nombre de la empresa

- ➢ Se pueden utilizar caracteres de mayúsculas, minúsculas, numéricos y símbolos del teclado.

- ✓ **Duración máxima de la contraseña:**

- ➢ Es un implemento más de seguridad que ofrece IAS; esta configuración de seguridad, exige al usuario cambiar la contraseña al transcurrir un periodo en días. Puede configurar las contraseñas para que caduquen en un periodo comprendido entre “1 y 999”, de igual manera se puede configurar que nunca caduquen simplemente estableciendo el número de días en “0”.

De igual manera en que se implementan mecanismos de seguridad, IAS ofrece la posibilidad de configurar el tipo de servicios que se van a proporcionar a los usuarios, por ejemplo:

- ➢ Designar derechos de usuario aun grupo en el directorio activo

- ➢ Configurar dos directivas de acceso remoto en servidores de acceso remoto o IAS

- ➢ Agregar un filtro IP de cuarentena

- ➢ Agregar un temporizador de sesión de cuarentena

Protección del trafico Radius con IPsec

La Seguridad del protocolo Internet (IPSec, Internet Protocol security) proporciona la capacidad para proteger a los servidores RADIUS del tráfico no deseado al utilizar filtros en adaptadores de red específicos (que permiten o bloquean protocolos específicos) y al permitirle elegir direcciones IP de origen desde las que se permite el tráfico.

Antes de crear filtros IPSec, se debe determinar el tipo de tráfico que desea permitir en cada servidor RADIUS. Los filtros demasiado estrictos podrían bloquear el tráfico de red y volverlo inaceptable.

Los mensajes RADIUS se envían con el Protocolo de datagramas de usuario (UDP, User Datagram Protocol). El puerto UDP 1812 se utiliza para los mensajes de autenticación RADIUS y el puerto UDP 1813 para los mensajes de cuentas RADIUS. Al crear filtros de entrada y salida con IPSec, en esos puertos se debe permitir el tráfico UDP. Sin embargo, puede que algunos servidores de acceso a la red utilicen el puerto UDP 1645 para mensajes de autenticación RADIUS y el puerto UDP 1646 para los mensajes de cuentas

RADIUS. De manera predeterminada, IAS admite ambos conjuntos de puertos. Si los servidores de acceso a la red utilizan los puertos UDP 1645 y 1646, puede crear filtros IPSec que permitan el tráfico en esos puertos.

Directiva de auditoria

Antes de implementar una directiva de auditoría, se debe decidir qué categorías de sucesos desea auditar. Un registro de auditoría registrará una entrada siempre que los usuarios realicen ciertas acciones específicas. Por ejemplo, la modificación de un archivo o una directiva puede desencadenar una entrada de auditoría que muestra la acción que se ha llevado a cabo, la cuenta de usuario asociada y la fecha y hora de la acción. Puede auditar tanto los intentos correctos como incorrectos en las acciones.

Las categorías de sucesos que puede elegir para auditar son:

- **Auditar sucesos de inicio de sesión de cuenta**

Esta configuración de seguridad determina si hay que auditar cada instancia de inicio o cierre de sesión de usuario. Los sucesos de inicio de sesión de cuenta se generan cuando una cuenta de usuario de dominio se autentica en un controlador de dominio. El suceso se registra en el registro de seguridad del controlador de dominio. Los sucesos de inicio de sesión se generan cuando un usuario local se autentica en un equipo local. El suceso se graba en el registro de seguridad local. Los sucesos de cierre de sesión de cuenta no se generan.

Se puede especificar si se auditan aciertos, errores o si o no se audita el tipo de suceso. Las auditorías de aciertos generan una entrada de auditoría cuando un intento de inicio de sesión en una cuenta tiene éxito. Las auditorías de errores generan una entrada de auditoría cuando un intento de inicio de sesión en la cuenta falla.

- **Auditar sucesos de inicio de sesión**

Esta configuración de seguridad determina si se audita cada instancia de un inicio o cierre de sesión de usuario en un equipo.

- **Auditar la administración de cuentas**

La configuración de seguridad determina si hay que auditar cada suceso de la administración de cuentas en un equipo. Algunos ejemplos de sucesos de la administración de cuentas son:

- Se crea, cambia o elimina una cuenta de usuario o un grupo.
- Se cambia el nombre, se deshabilita o se habilita una cuenta de usuario.
- Se establece o se cambia una contraseña.

- **Auditar el acceso del servicio de directorio**

Esta configuración de seguridad determina si hay que auditar el suceso de un usuario que obtiene acceso a un objeto de Active Directory que tiene especificada su propia lista de control de acceso al sistema (SACL, System Access Control List).

Si define esta opción de configuración de directiva, puede especificar si se auditan aciertos, errores o si o no se audita el tipo de suceso. Las auditorías de aciertos generan una entrada de auditoría cuando un usuario tiene acceso correctamente a un objeto de Active Directory que tiene especificada una SACL. Las auditorías de errores generan una entrada de auditoría cuando un usuario intenta tener acceso, sin lograrlo, a un objeto de Active Directory que tiene especificada una SACL.

- **Auditar el acceso a objetos**

Esta configuración de seguridad determina si se debe auditar el suceso de un usuario que obtiene acceso a un objeto (por ejemplo, un archivo, carpeta, clave del Registro, impresora, etc.) que tiene especificada su propia lista de control de acceso al sistema (SACL).

- **Auditar el uso de privilegios**

Esta configuración de seguridad se determina si se debe auditar cada instancia de un usuario que utiliza un derecho de usuario.

- **Auditar el seguimiento de procesos**

Esta configuración de seguridad determina si se debe auditar de modo detallado la información relacionada con el seguimiento de sucesos, como la activación de programas, salida de procesos, duplicación de identificadores y acceso indirecto a objetos.

- **Auditar sucesos del sistema**

Esta configuración de seguridad determina si se debe auditar cuándo un usuario reinicia o apaga el equipo, o si se produce un suceso que afecta a la seguridad del sistema o al registro de seguridad.

3.4 CUENTAS DE USUARIOS Y EQUIPOS

Las cuentas de usuario y las cuentas de equipo del directorio activo representan una entidad física como una persona o un equipo. Las cuentas de usuario también se pueden utilizar como cuentas de servicio dedicadas para algunas aplicaciones.

Las cuentas de usuario y de equipo (así como los grupos) se denominan también principales de seguridad. Los principales de seguridad son objetos de directorio a los que se asigna automáticamente identificadores de seguridad (SID), que se utilizan para tener acceso a los recursos del dominio. Una cuenta de usuario o de equipo se utiliza para:

- Autenticar la identidad de un usuario o equipo.

- Una cuenta de usuario permite que un usuario inicie una sesión en equipos y dominios con una identidad que puede ser autenticada por el dominio.

- Autorizar o denegar el acceso a los recursos del dominio.

- Después de que el usuario haya sido autenticado, se le autoriza o deniega el acceso a los recursos del dominio según los permisos explícitos asignados a dicho usuario en el recurso.

- Auditar las acciones realizadas con la cuenta de usuario o de equipo.

- La auditoría puede ayudarle a supervisar la seguridad de las cuentas.

Proteger cuentas de usuarios

Si un administrador de red no modifica ni deshabilita los derechos y permisos de las cuentas integradas, cualquier usuario o servicio malintencionado podría usarlos para iniciar una sesión, de manera ilegal, en un dominio mediante la identidad Administrador o Invitado. Una práctica recomendable de seguridad para proteger estas cuentas consiste en cambiar sus nombres o deshabilitarlas. Dado que una cuenta de usuario con el nombre cambiado conserva su identificador de seguridad (SID), conserva también todas las demás propiedades, como su descripción, la contraseña, la pertenencia al grupo, el perfil de usuario, la información de cuenta y todos los permisos y derechos de usuario asignados.

Opciones de cuentas

Cada cuenta de usuario del directorio activo tiene varias opciones de cuenta que determinan cómo se autentica en la red a un usuario que ha iniciado una sesión con esa cuenta de usuario en particular**.**

Tabla 7.

Opciones para configurar los valores de contraseña e información específica de la seguridad para cuentas de usuario.

Opción de cuenta	Descripción
El usuario debe cambiar la contraseña en el siguiente inicio de sesión	Obliga a un usuario a modificar su contraseña la próxima vez que inicie una sesión en la red. Utilice esta opción cuando desee asegurarse de que el usuario va a ser la única persona que va a saber su contraseña.
El usuario no puede cambiar la contraseña	Impide al usuario cambiar su contraseña. Utilice esta opción cuando desee controlar una cuenta de usuario, como una cuenta temporal o una cuenta de invitado.
La contraseña nunca caduca	Impide que caduque una contraseña de usuario. Se recomienda que las cuentas de servicio tengan habilitada esta opción y que se utilicen contraseñas seguras.
Cuenta deshabilitada	Impide que los usuarios inicien una sesión con la cuenta seleccionada.
La cuenta es importante y no se puede delegar	Permite el control sobre una cuenta de usuario, como una cuenta Invitado o temporal. Esta opción se puede utilizar si esta cuenta no puede ser asignada para delegación, es decir que un servicio pueda suplantar una cuenta de usuario o una cuenta de equipo.

3.5 CONSIDERACIONES DE SEGURIDAD DE IAS COMO SERVIDOR RADIUS

Al implementar IAS como servidor RADIUS debemos tener en cuenta las siguientes consideraciones acerca de la seguridad:

- **Secretos compartidos**

Se deben configurar secretos compartidos seguros para evitar los ataques de diccionario y se deben cambiar con frecuencia. Los secretos compartidos seguros son una secuencia larga (más de 22 caracteres) de letras, números y signos de puntuación aleatorios.

- **Protocolos de autenticación**

IAS admite varios protocolos de autenticación diferentes. El orden de los protocolos de autenticación, del más seguro al menos seguro, es: PEAP-EAP-TLS (sólo para clientes inalámbricos y clientes de conmutación autenticados), EAP-TLS, PEAP-EAP-MS-CHAPv2 (sólo para clientes inalámbricos y clientes de conmutación autenticados), MS-CHAP v2, MS-CHAP, EAP-MD5, CHAP y PAP. Microsoft recomienda utilizar sólo los protocolos de autenticación más seguros que exija la configuración. En los protocolos de autenticación basada en contraseñas, deben aplicarse directivas de contraseña segura como protección contra ataques de diccionario.

3.6 DIRECTIVAS DE CUENTAS

3.6.1 DIRECTIVAS DE CONTRASEÑAS

Forzar el historial de contraseñas

Esta configuración de seguridad determina el número de nuevas contraseñas únicas que hay que asociar con una cuenta de usuario para que se pueda volver a utilizar una contraseña antigua.

Esta directiva permite a los administradores mejorar la seguridad, al garantizar que las contraseñas antiguas no se vuelven a utilizar continuamente.

Duración máxima de la contraseña

Esta configuración de seguridad determina el periodo (en días) que puede utilizarse una contraseña antes de que el sistema exija al usuario que la cambie. Puede configurar las contraseñas para que caduquen tras un número de días entre 1 y 999, o puede especificar que las contraseñas nunca caduquen.

Duración mínima de la contraseña

Esta configuración de seguridad determina el periodo (en días) que se debe utilizar una contraseña antes de que el usuario pueda cambiarla. Puede establecer un valor entre 1 y 998 días.

La vigencia mínima de la contraseña debe ser inferior a la Duración máxima de la contraseña, a menos que ésta se establezca en 0, valor que indica que la contraseña nunca caduca. Si la vigencia máxima de la contraseña está establecida en 0, la vigencia mínima puede ser cualquier valor entre 0 y 998.

Longitud mínima de la contraseña

Esta configuración de seguridad determina el número mínimo de caracteres que puede contener la contraseña de un usuario. Podemos establecer un valor entre 1 y 14 caracteres, o que no se requiere contraseña si establece el número de caracteres como 0.

3.6.2 DIRECTIVAS DE BLOQUEO DE CUENTAS

Duración del bloqueo de cuenta

En esta configuración de seguridad determinamos el número de minutos que permanece bloqueada una cuenta antes de que se desbloquee automáticamente. El intervalo disponible es de 0 a 99,999 minutos. Si define la duración del bloqueo de la cuenta como 0, la cuenta quedará bloqueada hasta que un administrador la desbloquee explícitamente.

Umbral de bloqueos de la cuenta

Esta configuración de seguridad determina el número de intentos de inicio de sesión erróneos necesarios para que se bloquee una cuenta de usuario. Una cuenta bloqueada no se puede utilizar hasta que el administrador la restablezca o hasta que caduque la duración del bloqueo de dicha cuenta. Podemos definir un valor entre 0 y 999 intentos de inicio de sesión erróneos. Si se establece el valor en 0, la cuenta nunca se bloqueará.

Establecer la cuenta de bloqueos después de intentos de inicio de sesión erróneos

Esta configuración de seguridad determina el número de minutos que debe transcurrir después de un intento de inicio de sesión erróneo para que el contador correspondiente restablezca a 0 los intentos de inicio de sesión erróneos. El intervalo disponible es de 1 a 99,999 minutos.

3.7 ASIGNACIÓN DE DERECHOS DE USUARIO

En este apartado podemos determinar a que usuarios se le van a asignar los siguientes derechos:

- Tener acceso a este equipo desde la red.
- Actuar como parte del sistema operativo.
- Agregar estaciones de trabajo al dominio.
- Hacer copias de seguridad de archivos y directorios.
- Cambiar la hora del sistema
- Crear un archivo de paginación
- Depurar programas
- Suplantar a un cliente después de la autenticación

- Cargar y descargar controladores de dispositivo
- Administrar los registros de auditoría y seguridad
- Restaurar archivos y directorios
- Apagar el sistema
- Tomar posesión de archivos y otros objetos

3.8 ESTANDAR 802.1x

Compatibilidad con IAS para la autenticación 802.1X

Para mejorar la seguridad y la implementación de redes inalámbricas, se puede utilizar 802.1X con IAS, la implementación de Microsoft de un servidor proxy y un servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). Cuando se implementa RADIUS, los puntos de acceso inalámbrico configurados como clientes RADIUS utilizan el protocolo RADIUS para enviar solicitudes de conexión y mensajes de cuentas a un servidor central RADIUS. El servidor RADIUS tiene acceso a una base de datos de cuentas de usuario y a un conjunto de reglas para conceder autorización, procesa la solicitud de conexión del punto de acceso inalámbrico, y acepta o rechaza dicha solicitud.

Descripción de la autenticación 802.1X para redes inalámbricas

802.1X es un estándar IEEE para un acceso de red autenticado a redes Ethernet por cable y redes 802.11 inalámbricas. IEEE 802.1X mejora la seguridad y la implementación al proporcionar la compatibilidad con la identificación de usuarios, la autenticación, la administración de claves dinámicas y la creación de cuentas de manera centralizada.

Cómo funciona 802.1X en redes inalámbricas 802.11

802.1X implementa el control de acceso a red basado en puertos. El control de acceso a red basado en puertos utiliza las características físicas de una infraestructura de red de área local (LAN) conmutada para autenticar los dispositivos conectados a un puerto de LAN e impedir el acceso a dicho puerto cuando se produzca un error en el proceso de autenticación.

Durante una interacción del control de acceso a red basado en puertos, un puerto de LAN adopta una de dos funciones:

Autenticador o Suplicante.

- En la función de autenticador, un puerto de LAN exige la autenticación antes de permitir el acceso de los usuarios a los servicios a los que se puede tener acceso desde dicho puerto.

- En la función de suplicante, un puerto de LAN solicita acceso a los Servicios a los que se puede tener acceso desde el puerto del autenticador. Un servidor de autenticación, que puede ser una entidad independiente o coincidir con el autenticador, comprueba las credenciales del suplicante en nombre del autenticador. El servidor de autenticación responde entonces al autenticador, indicando si el suplicante tiene autorización o no para el acceso a los servicios del autenticador.

El control de acceso a red basado en puertos del autenticador define dos rutas de acceso lógico a datos para la LAN a través de un puerto de LAN físico. La primera ruta de acceso a datos, el puerto sin controlar, permite el intercambio de datos entre el autenticador y un dispositivo de la LAN, independientemente de cuál sea el estado de autenticación del dispositivo. Esta ruta de acceso es la que utilizarán los mensajes de EAPOL (EAP a través de LAN). La segunda ruta de acceso a datos, el puerto controlado, permite el intercambio de datos entre un usuario de LAN autenticado y el autenticador. Esta ruta de acceso es la que utilizará el resto de tráfico de la red, una vez autenticado el dispositivo.

3.9 802.1X e IAS

Puede utilizarse 802.1X con IAS para permitir la autenticación, autorización y creación de cuentas para conexiones de red inalámbrica. IAS es la implementación de Microsoft de un servidor proxy y un servidor de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS, Remote Authentication Dial-in User Service). Cuando se implementa RADIUS, un punto de acceso inalámbrico impide el reenvío del tráfico de datos a una red por cable o a otro cliente inalámbrico sin una clave de autenticación válida. El proceso para obtener una clave de autenticación válida es el siguiente:

1. Cuando un cliente inalámbrico se encuentra dentro del intervalo de acción de un punto de acceso inalámbrico, éste envía un desafío al cliente.

2. El cliente inalámbrico envía su identidad al punto de acceso inalámbrico, el cual reenvía esta información a un servidor RADIUS.

3. El servidor RADIUS solicita las credenciales del cliente inalámbrico para comprobar su identidad. Como parte de esta solicitud, el servidor RADIUS especifica el tipo de credenciales necesarias.

4. El cliente inalámbrico envía sus credenciales al servidor RADIUS.

5. El servidor RADIUS comprueba las credenciales del cliente inalámbrico. Si las credenciales son válidas, el servidor RADIUS envía una clave de autenticación cifrada al punto de acceso inalámbrico.

6. El punto de acceso inalámbrico utiliza esta clave de autenticación para transmitir de forma segura al cliente inalámbrico claves de autenticación de multidifusión y unidifusión de sesión por cada estación.

3.10 PROTOCOLO RADIUS

RADIUS “Servicio de usuario de acceso telefónico de autenticación remota” (RADIUS, Remote Authentication Dial-In User Service) es un protocolo estándar, RADIUS se utiliza para proporcionar servicios de autenticación, autorización y administración de cuentas. Un cliente RADIUS (en este caso un punto de acceso inalámbrico) envía credenciales de usuario e información de parámetros de conexión en forma de un mensaje RADIUS a un servidor RADIUS. El servidor RADIUS autentica y autoriza la petición del cliente RADIUS y devuelve un mensaje de respuesta RADIUS. Los clientes RADIUS también envían mensajes de administración de cuentas RADIUS a los servidores RADIUS. Además, los estándares RADIUS admiten el uso de proxy RADIUS. Un proxy RADIUS es un equipo que reenvía mensajes RADIUS entre equipos compatibles con RADIUS.

Tipos de mensajes RADIUS

- **Access-Request (solicitud de acceso)**

Enviado por un cliente RADIUS para solicitar autenticación y autorización de un intento de conexión.

- **Access-Accept (aceptación de acceso)**

Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. En él se informa al cliente RADIUS de que se ha autenticado y autorizado el intento de conexión.

- **Access-Reject (rechazo de acceso)**

Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. En él se informa al cliente RADIUS de que se ha rechazado el intento de conexión. Un servidor RADIUS envía este mensaje si las credenciales no son auténticas o si no se ha autorizado el intento de conexión.

- **Access-Challenge (desafío de acceso)**

Enviado por un servidor RADIUS como respuesta a un mensaje Access-Request. Este mensaje es un desafío al cliente RADIUS que exige una respuesta.

- **Accounting-Request (solicitud de administración de cuentas)**

Enviado por un cliente RADIUS para especificar información de administración de cuentas de una conexión que se ha aceptado.

- **Accounting-Response (respuesta de administración de cuentas)**

Enviado por el servidor RADIUS como respuesta a un mensaje de Solicitud de administración de cuentas. En este mensaje se confirman la recepción y el procesamiento correctos del mensaje de Solicitud de administración de cuentas

Componentes de una infraestructura RADIUS

Un sistema IAS-RADIUS esta formado por los siguientes componentes

- Cliente Radius (AP)
- Controlador de Dominio – Directorio Activo
- Servidor IAS-RADIUS
- Autoridad Certificadora (Certification Authority**)**
- Cliente RADIUS(AP)

Fig.1. Componentes de una infraestructura RADIUS.

El cliente RADIUS se va a definir como el punto de acceso que da servicio de conexión a la red. El punto de acceso debe cumplir con las siguientes requisitos:

- ✓ Debe soportar la norma 802.1x (EAP-PEAP).
- ✓ Debe ser registrado por parte del servidor RADIUS.
- Directorio Activo

El Directorio Activo cumple la función de una base de datos donde están registrados cada uno de los usuarios y equipos que son parte de un dominio para controlar sus funciones por medio de directivas.

El Directorio Activo basa su administración en:

- ✓ Creación y configuración de cuentas de usuarios y equipos.
- ✓ Directivas o Políticas para las actividades permitidas para las cuentas.

- ✓ Jerarquización de actividades.

- ➢ Servidor IAS-RADIUS

El servidor IAS – RADIUS cumple con las siguientes funciones:

- ✓ Interacción con el cliente RADIUS (AP) para inicio de Autenticación
- ✓ Interacción con la base de datos donde están registradas las cuentas de usuario.
- ✓ Confirma el conjunto de reglas para conceder autorización.
- ✓ Procesa la solicitud de conexión del AP.
- ✓ Acepta o rechaza la solicitud**.**

- ➢ Autoridad Certificadora

La autoridad certificadora es un elemento que se encarga de expedir los certificados implementando las directivas adecuadas.

Capítulo 4

IMPLEMENTACIÓN DEL IAS

Para el desarrollo de la implementación del sistema de autenticación que proporcionará la seguridad y la administración de la red inalámbrica utilizaremos la aplicación del IAS (Internet Autentication Service).

Este sistema de autenticación requiere contar con los siguientes elementos:

- ✓ Un servidor que dará el servicio de Directorio Activo bajo la plataforma de Windows Server 2003.

- ✓ Un servidor que proporcionará los servicios de un servidor IAS – RADIUS, este mismo servidor contará con la aplicación de unidad certificadora CA, etcétera.

- ✓ Por lo menos un cliente RADIUS que físicamente es nuestro AP.

Hoy en día el hardware se ha visto favorecido por la tecnología que ha logrado muchísimas mejoras en este aspecto. Por ello para poder explotar al máximo el rendimiento de nuestro hardware vamos a utilizar el software VMware para virtualizar nuestros servidores y así tener 2 servidores virtuales dentro de un servidor físico.

El sistema operativo Windows Server 2003 puede desarrollar su funcionamiento de manera normal con 384 MB de memoria RAM cada uno con un procesador Pentium IV como mínimo, este suponiendo que solo está implementación solo servirá como prototipo para la realización de pruebas para la autenticación de usuarios.

Por lo tanto podemos definir los requerimientos mínimos de hardware para nuestro sistema, estas características son las siguientes:

- 2 GB de memoria RAM tomando en cuenta los dos servidores virtuales y el sistema operativo original del servidor.

- Procesador Intel Pentium IV a 3 GHz.

- Disco Duro de 40 GB.

- Tarjetas de red Erthernet de 100 Mbps.

- Lector de disco CD o DVD.

- Entradas USB.

Ahora nos disponemos a crear los dos servidores virtuales dentro del ambiente VMware, cabe señalar que existen diversas ventajas para desarrollar entornos con máquinas virtuales:

- Es la movilidad que podemos tener con las maquinas virtuales, con solo llevarnos los archivos de disco duro y de configuración de la máquina virtual podemos seguir trabajando con el servidor desde otra máquina física siempre y cuando tenga el software de VMware como por ejemplo en una PC portátil.

- Maximiza el rendimiento del hardware de nuestro servidor físico, como la memoria RAM, procesador, etcétera, debido principalmente a que los servidores trabajan bajo demanda y si la demanda del servidor hacia su hardware es poca obviamente no se explota al máximo los recursos que se tienen.

- Pueden albergar varios servidores virtuales que estén en servicio al mismo tiempo compartiendo los recursos de hardware, con esto se pueden implementar varios desarrollos o aplicaciones con diferentes sistemas operativos y programas.

4.1 IMPLEMENTACION DE SERVIDORES VIRTUALES.

Como ya lo habíamos mencionado empezaremos por crear los servidores virtuales con el software VMware, este sistema está representado por el siguiente esquema para entender su funcionamiento.

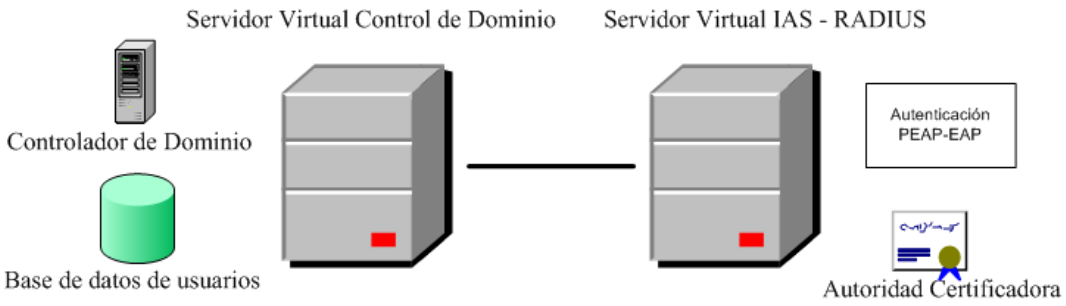

Fig.2. Implementación de Servidores Virtuales.

En este esquema observamos como los servidores virtuales tienen cada uno una función independiente. Cabe señalar que el directorio activo y el controlador de dominio por recomendaciones de Microsoft es necesario que sólo estén instalados en un solo servidor. Con el servidor IAS – RADIUS se realizará el proceso de autenticación y además le agregaremos las herramientas necesarias para que éste también tenga como función la Autoridad Expedidora de Certificados. Hay que mencionar que los servidores necesitan estar en comunicación para que funcione correctamente el sistema. Esto es de vital importancia porque la autenticación es realizada por el servidor RADIUS pero a su vez este servidor realizará consultas de información hacia el servidor del controlador de

dominio, esta información consta básicamente de los usuarios pertenecientes al directorio activo.

Ahora podemos observar en la siguiente imagen como están creados los dos servidores y con cada una de las características con las que cuentan cada uno de ellos.

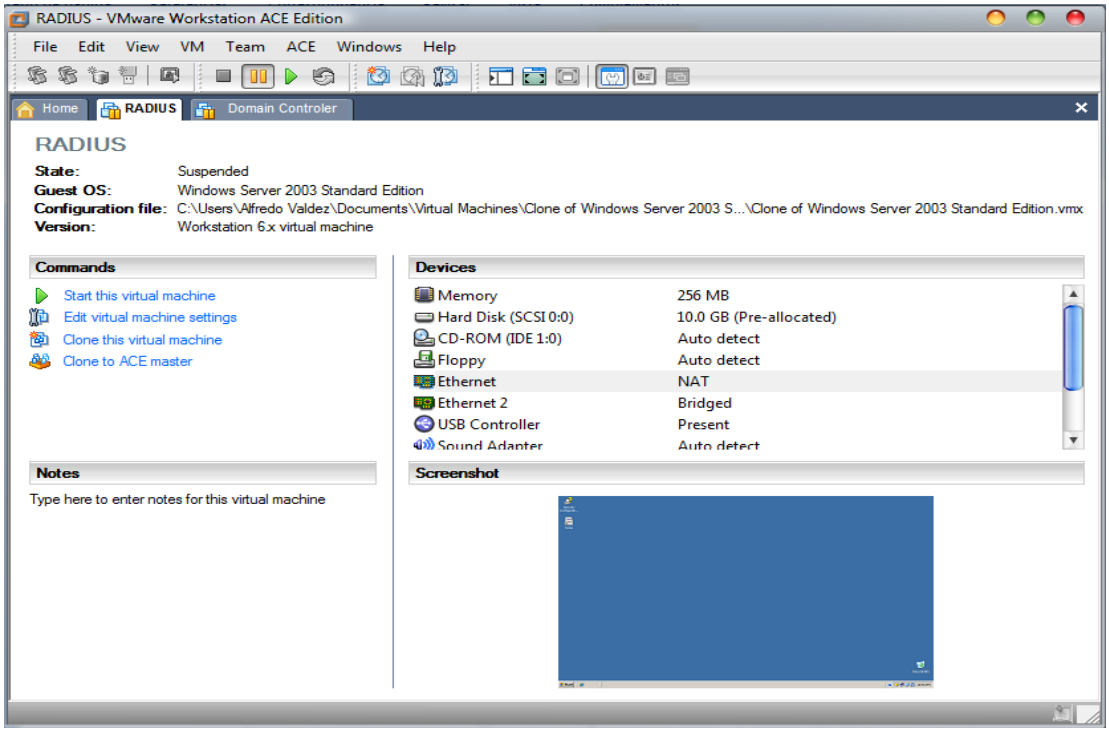

Fig. 3. Servidor Virtual IAS – RADIUS.

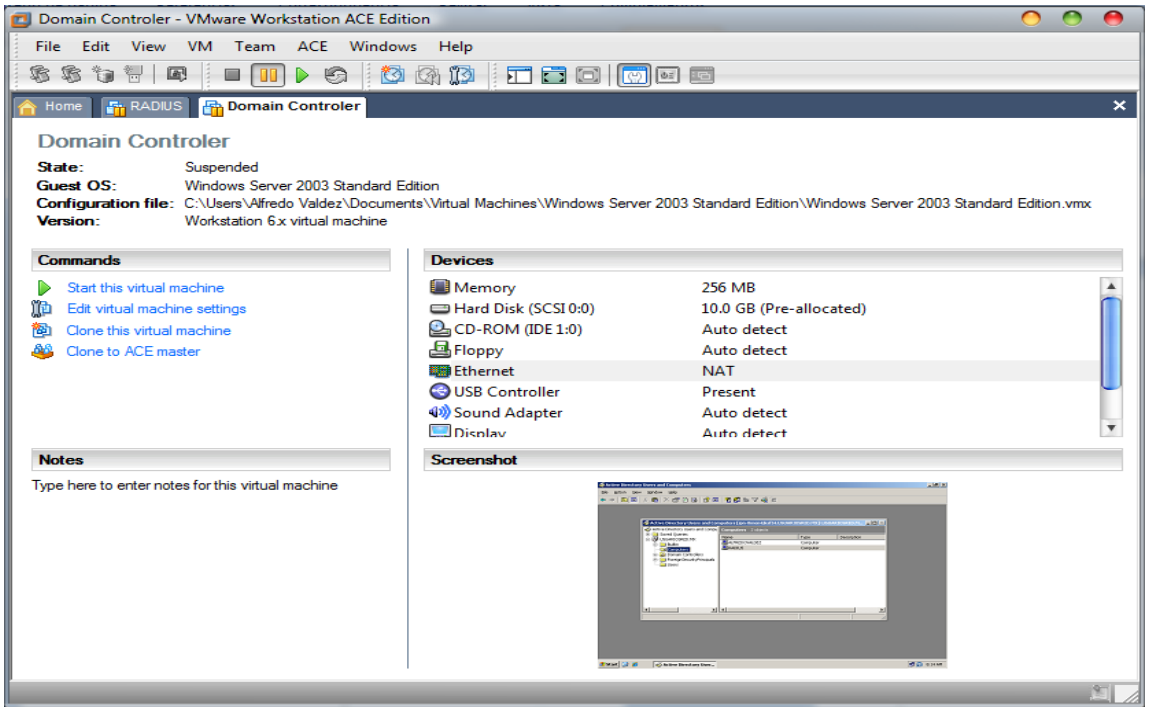

Fig. 4. Servidor Virtual de Controlador de Dominio.

En las imágenes anteriores se observa la configuración para los servidores virtuales:

- Cada uno cuenta con 256 MB de espacio reservado de memoria RAM.

- Cada uno cuenta con 10 GB de disco duro.

- Lector de CD, es compartido dependiendo de que entorno nos encontremos, en los servidores es el que envía la petición del hardware, este mismo caso es para las interfaces USB, floppy, adaptador de sonido, pantalla, y procesador.

- En el caso de las interfaces de red podemos observar en las imágenes la opción de Ethernet que hace referencia a la conexión de red, para su configuración nos proporciona dos opciones:

  I. Nat: Indica que el servidor hará uso de una dirección IP privada proporcionada por el mismo VMware a través del protocolo DHCP.

  II. Bridge: Indica que el servidor hará uso de la dirección IP que le pertenece al equipo físico que alberga al servidor virtual.

Para lograr que estos dos servidores se puedan comunicar necesitamos que las direcciones de IP sean fijas y con esto aseguramos que la comunicación entre los dos servidores no se pierda, para ello ejecutaremos el comando ipconfig en la consola de uno de los servidores y obtendremos la dirección IP que VMware le asigna al servidor. Con los datos proporcionados configuramos la dirección IP de nuestro servidor pero configurando como IP estática.

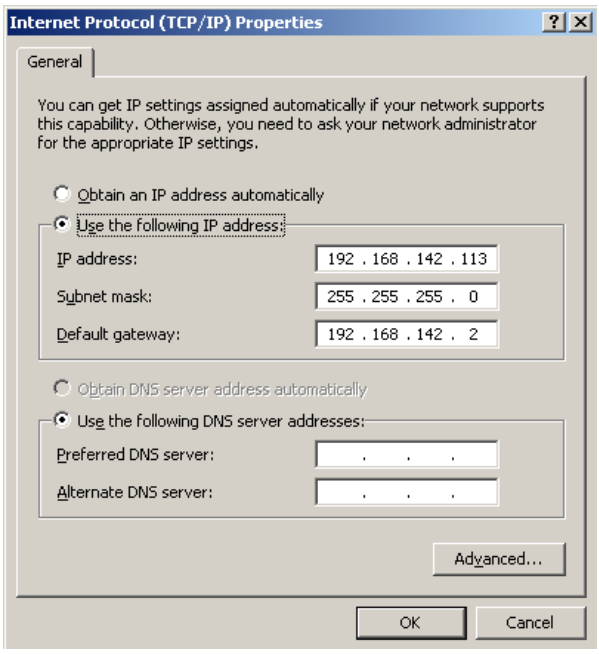

Fig. 5. Configuración de IP (NAT) del Controlador de Dominio.

Para el otro servidor solo llenamos su tabla con la dirección contigua al servidor del directorio activo, pero en el caso del servidor RADIUS agregamos en la opción de DNS la dirección del servidor del controlador de dominio porque este servidor tiene instalados los controladores de DNS.

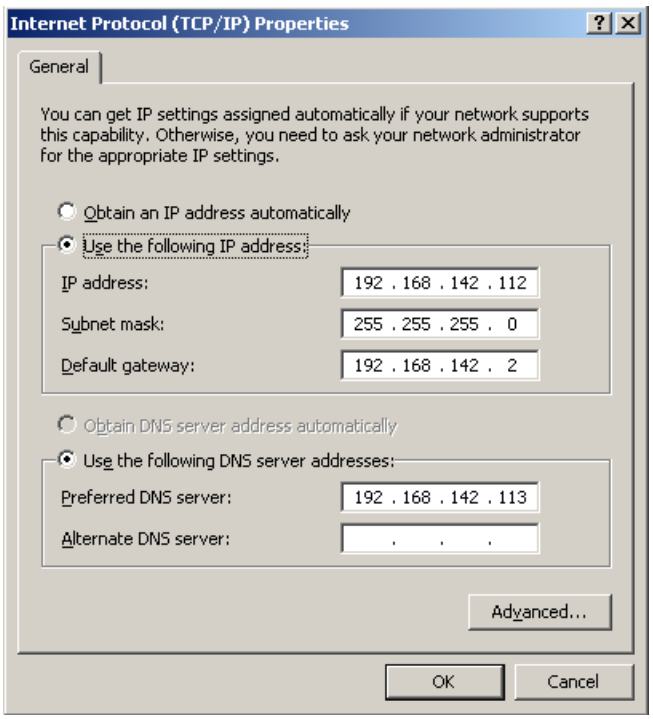

Fig. 6. Configuración de IP (NAT) del servidor IAS - RADIUS.

Para la siguiente configuración, se anexo al servidor virtual otra salida de red, pero en este caso esta salida esta destinada para que el servidor RADIUS este conectado a nuestra red y por medio de esta conexión tener la comunicación con nuestro punto de acceso (AP). Para ello necesitamos tener una dirección IP válida para conectarnos a la red, en este caso utilizamos una dirección de la red privada de DCyC del Instituto Politécnico Nacional.

La configuración en el VMware para esta conexión de red es BRIDGE, esto significa que el servidor IAS utilizará la tarjeta física del servidor en donde se encuentran alojados los servidores virtuales, por tanto también es necesario que la configuración de la IP del servidor físico sea idéntica a la del servidor virtual en modo BRIDGE.

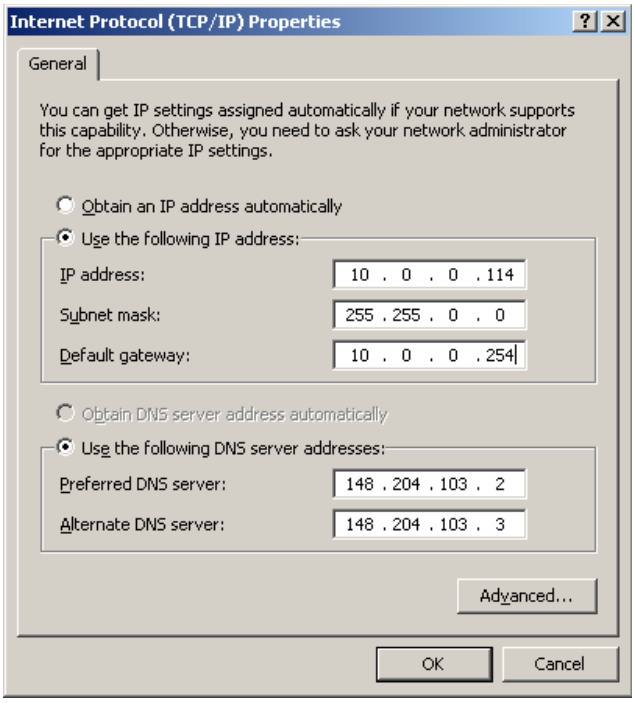

Fig. 7. Configuración de IP (Bridge) del servidor IAS - RADIUS.

Observamos que en la configuración de IP del servidor del controlador de dominio tienen una dirección IP de la red 192.0.0.0 estas direcciones están determinadas por VMware para darle conexión a red a los servidores virtuales.

4.2 CONFIGURACION DEL SERVIDOR DEL CONTROLADOR DE DOMINIO.

Iniciaremos en primer lugar con la creación del dominio, aquí se encontrara la base de datos del directorio activo como son los usuarios, computadoras, grupos y las directivas a las que estarán sujetos cada uno de los usuarios.

Ahora en principio tendremos que crear nuestro dominio para ello en el menú de inicio de Windows se encuentra la aplicación “Manage Your Server” en el cual seleccionaremos la opción de “Add or remove a role”.

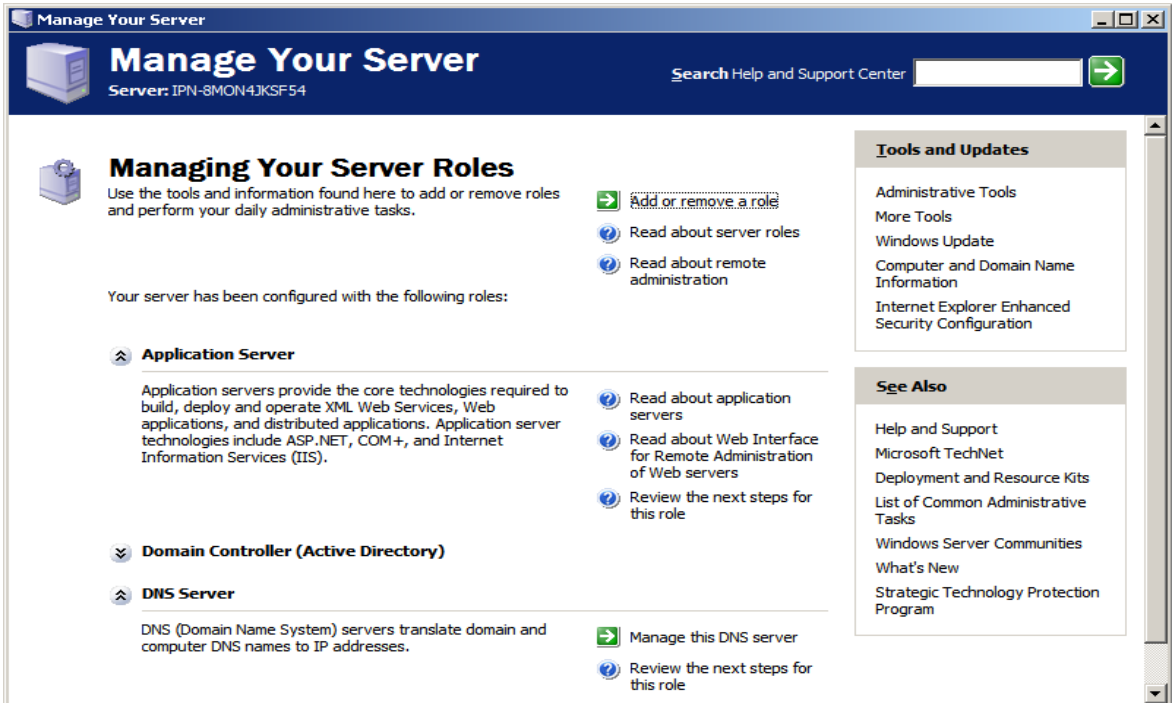

Fig. 8. Aplicación Manage Your Server.

Inmediatamente se realizara una configuración típica para un servidor principal para instalar el directorio activo y además instalar el DNS y el servidor DHCP. Posteriormente se define el nombre del directorio activo o dominio.

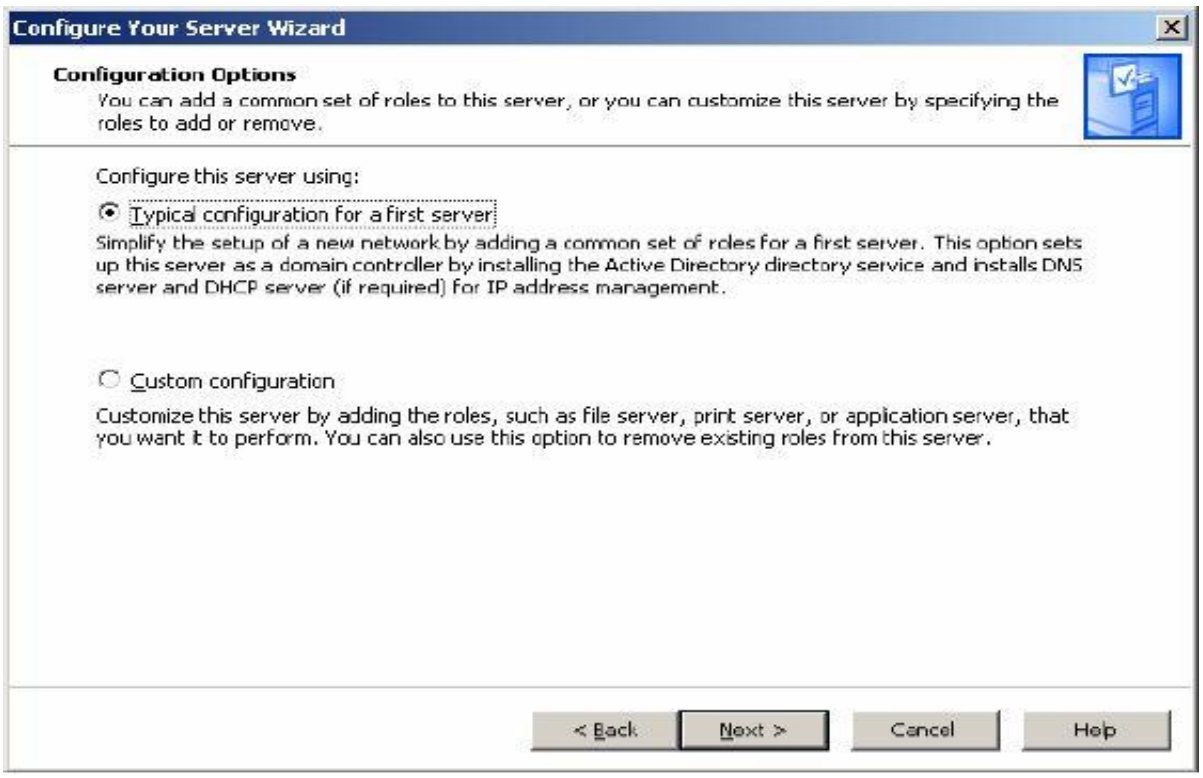

Fig. 9. Selección de la configuración del servidor.

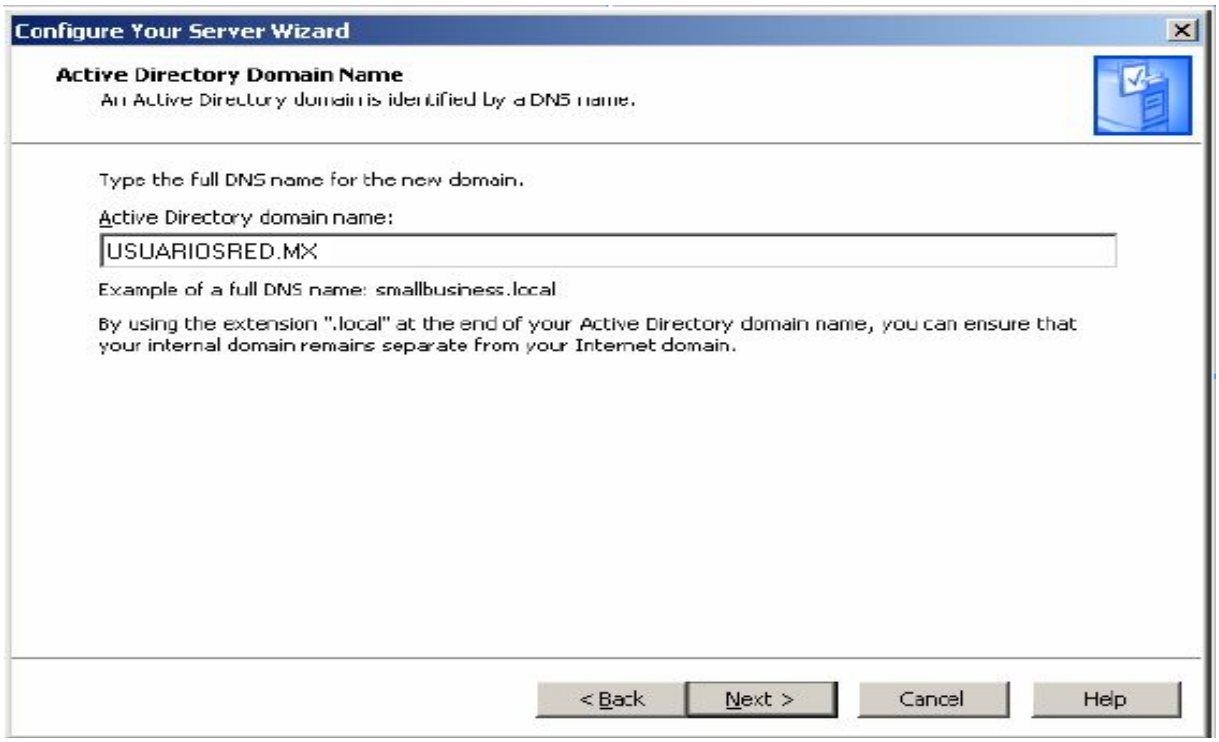

Fig. 10. Asignación del nombre de dominio del directorio activo.

El siguiente paso es seleccionar la opción de crear el control de dominio para un nuevo dominio, esta opción se selecciona porque es el primer dominio que generamos y por tanto no tenemos antecedentes de otro dominio anterior, como se muestra en las siguientes figuras.

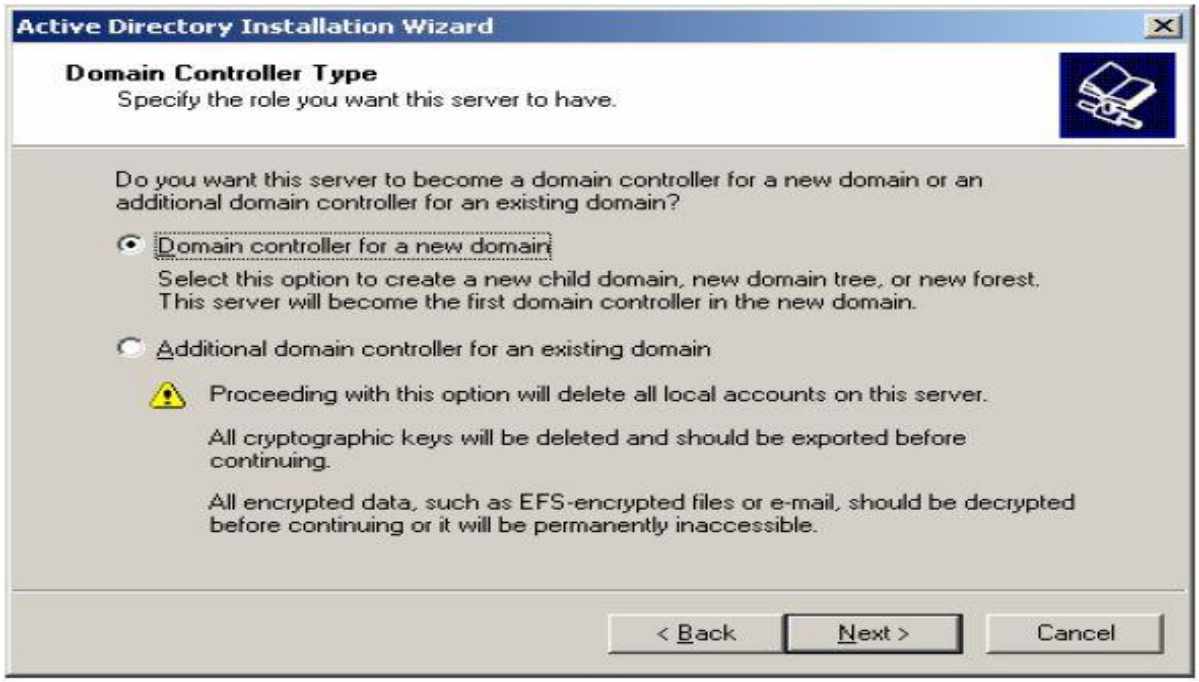

Fig. 11. Tipo de controlador de dominio.

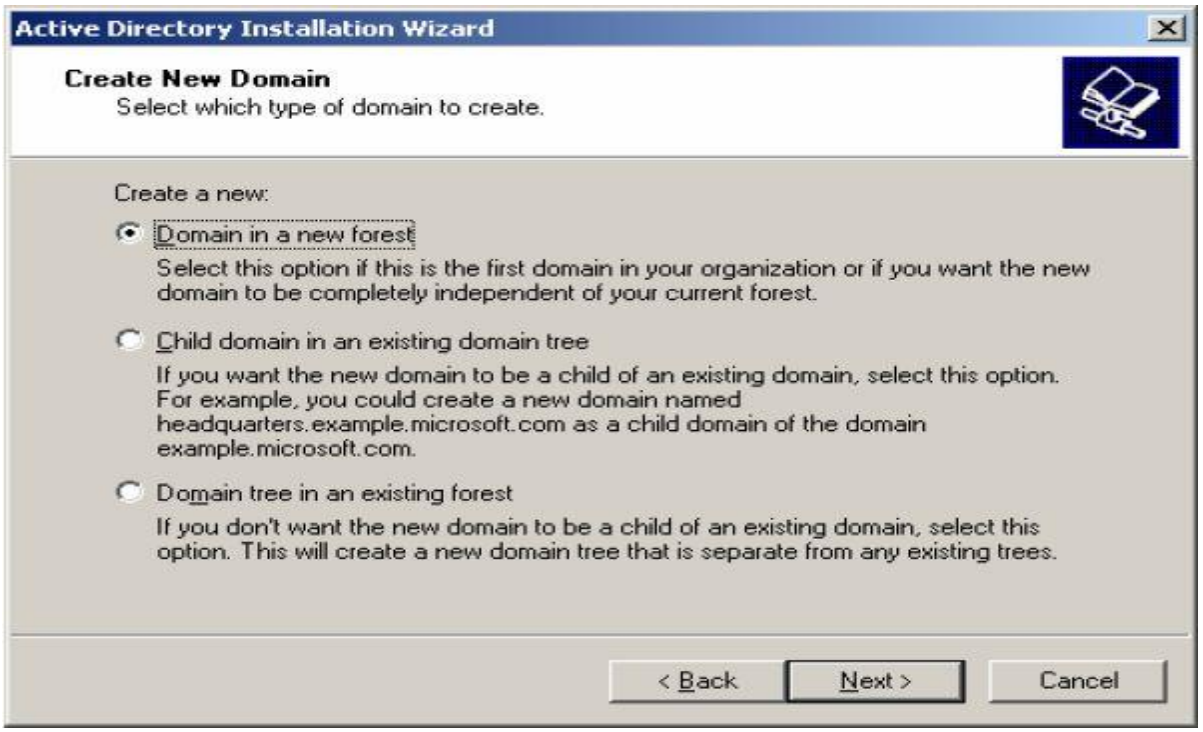

Fig. 12. Creación del nuevo dominio.

El siguiente paso es el registro de los usuarios y de las computadoras, para este caso solo haremos nuestros registros ya que somos los administradores del sistema y además hay que registrar los equipos en donde están instalados tanto el servidor de control de dominio y el servidor del IAS – RADIUS.

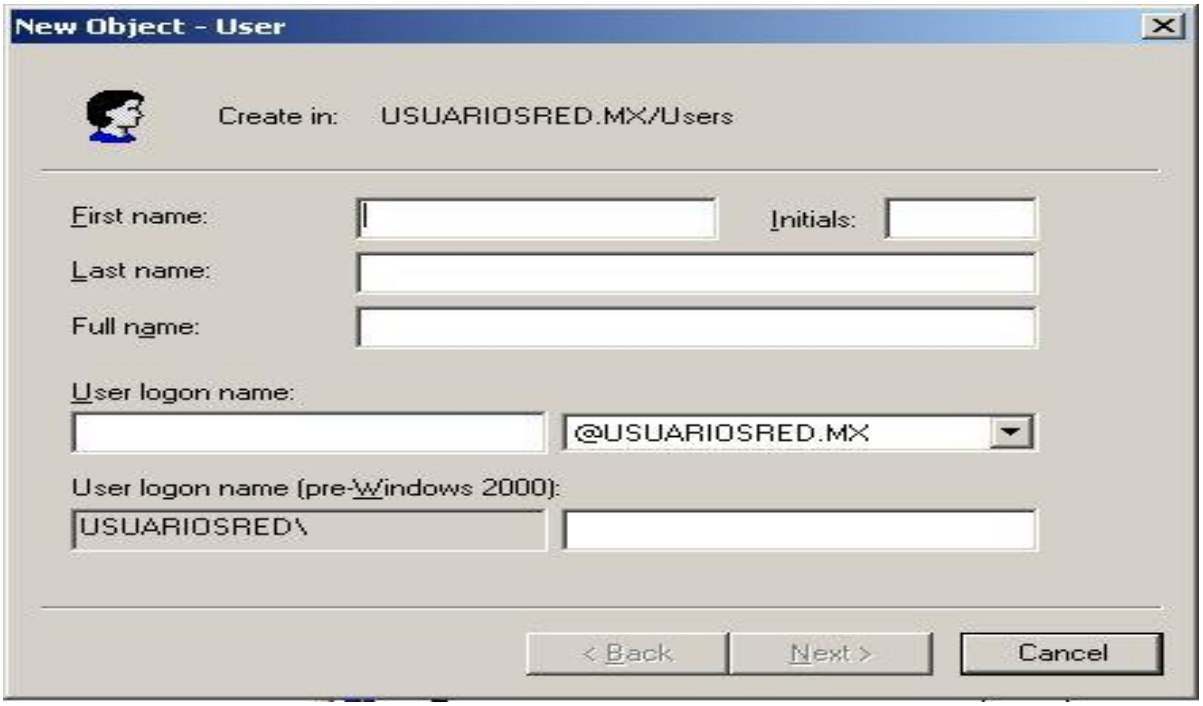

Fig. 13. Plantilla de registros de usuarios.

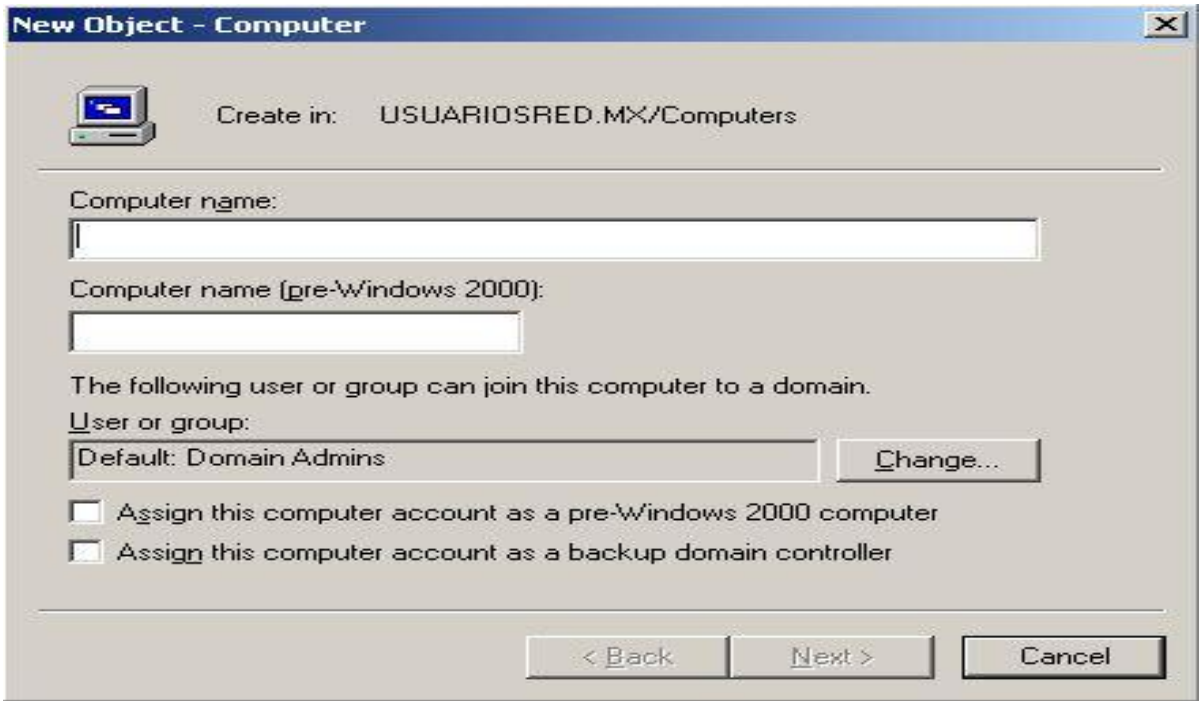

Fig. 14. Plantilla de registros de equipos o computadoras.

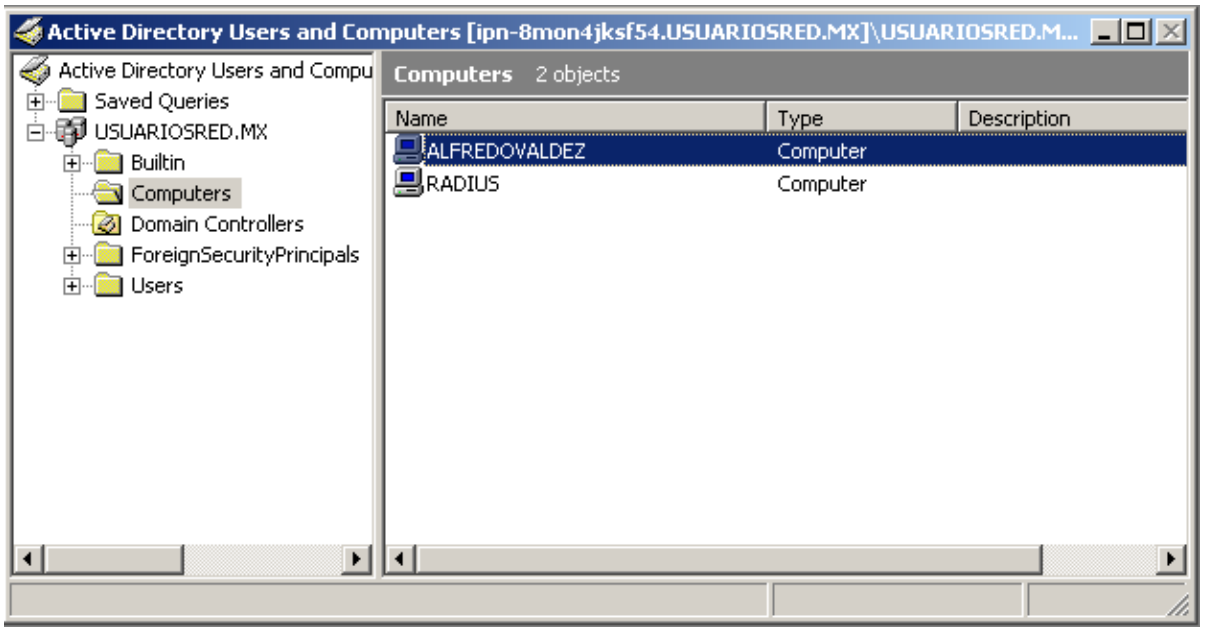

Fig. 15. Equipos ya registrados.

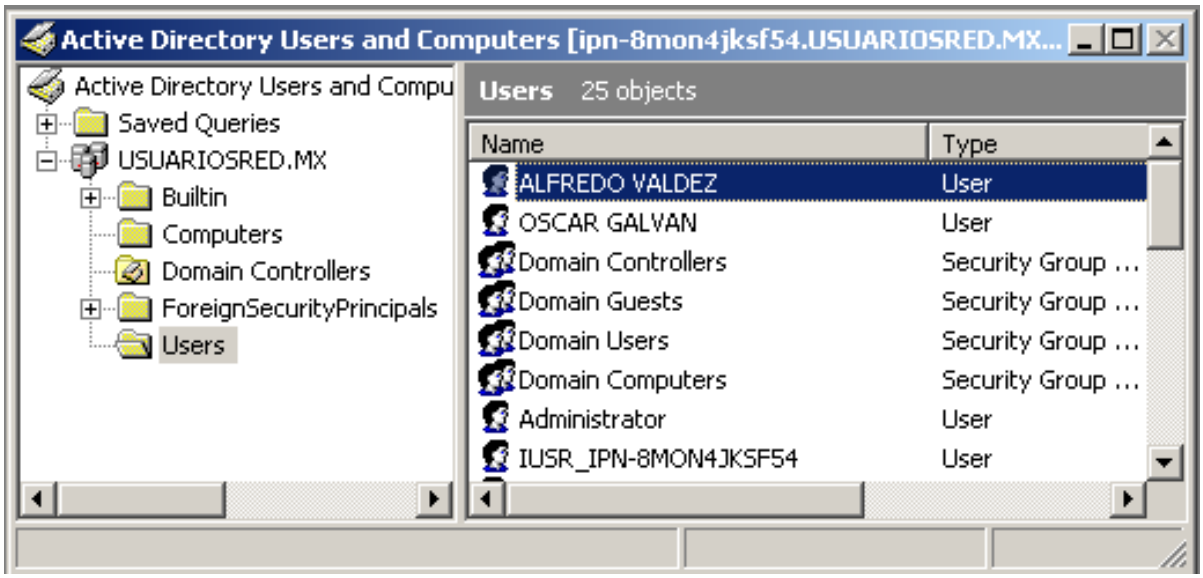

Fig. 16. Usuarios ya Registrados.

En las imágenes anteriores podemos darnos cuenta de cómo se llevan a cabo los registros y como se quedan guardados dentro del dominio cada uno dentro del grupo correspondiente. Para este prototipo recordemos que le creamos su propio controlador de dominio y a este servidor de dominio se le implemento su servidor RADIUS que también pertenece al dominio, en conclusión cada servidor RADIUS debe pertenecer a un dominio y el registro de cada uno de los usuarios tendrá que ser llevada a cabo por los administradores del sistema o en el caso de que se desee se puede migrar al servidor la base de datos del controlador de dominio del Instituto.

Otra opción es que al dominio Institucional se le implemente su propio servidor RADIUS.

4.3 CONFIGURACION DEL SERVIDOR IAS – RADIUS.

Para llevar a cabo la configuración de este servidor es necesario instalar los servicios de CA o Autoridad Certificadora y posteriormente los servicios y herramientas del IAS, hay que mencionar que la instalación de estos componentes es necesarios tener el disco de instalación y la versión Enterprise 2003 y que se debe de respetar el orden de la instalación mencionado anteriormente.

Cabe señalar que es importante que los dos equipos registrados anteriormente en el directorio activo también necesitan que se les instale un certificado de seguridad, por lo que al término de la instalación de la CA inmediatamente realizaremos la expedición de certificados para estos dos equipos.

Ahora empezaremos a crear nuestra Autoridad Certificadora pero es importante señalar que a partir de este momento los dos servidores deben de estar en estado encendido y en comunicación, esto es importante para que la configuración del equipo se establezca para el directorio activo. Para checar que los dos servidores están dentro del directorio activo es importante entrar con las cuentas de directorio activo hacia los dos servidores, para asegurarnos de la conectividad y de la comunicación entre los dos servidores podemos hacerlo por comandos de consola con ping de una IP de un servidor a otro.

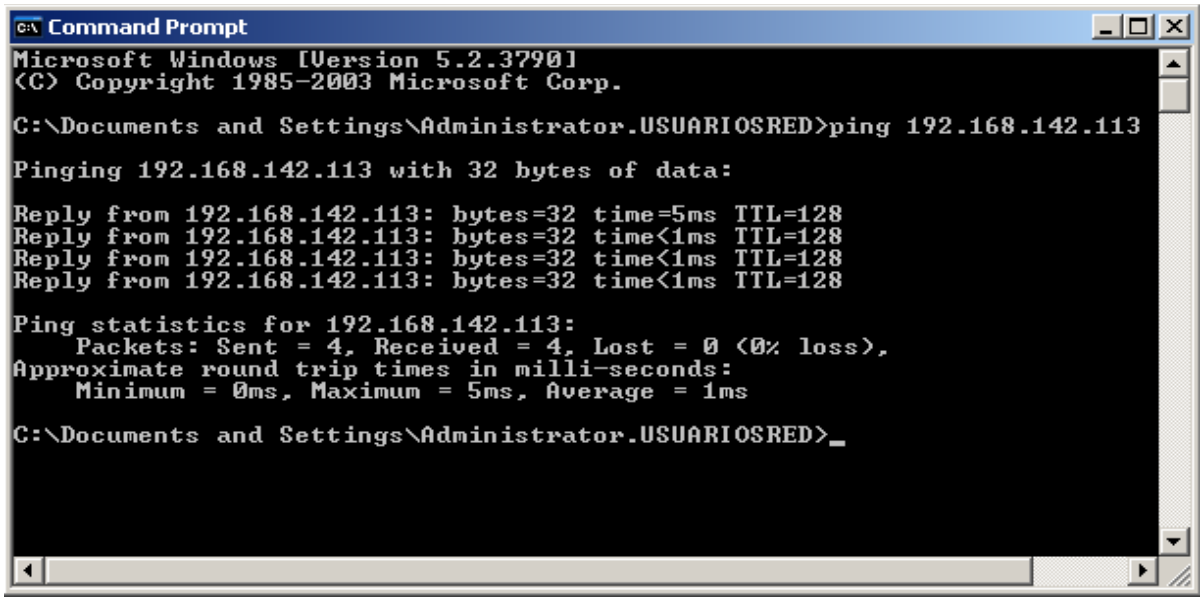

Fig. 17. Ping del servidor RADIUS hacia el servidor de controlador de dominio.

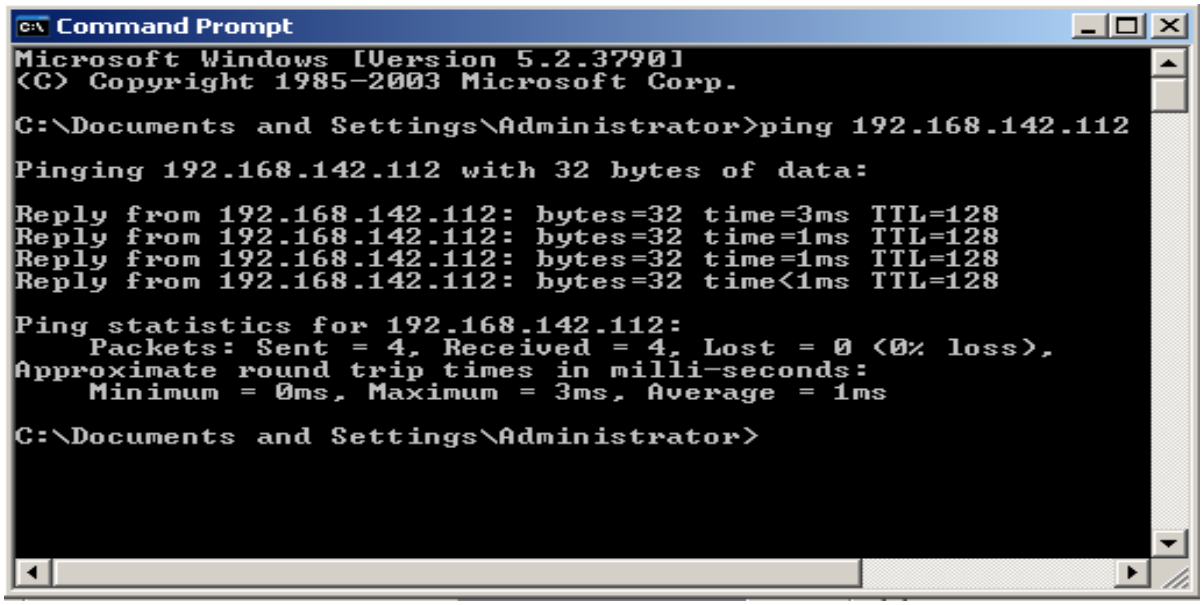

Fig. 18. Ping del servidor del controlador de dominio hacia el servidor RADIUS.

Después de asegurarnos de la conectividad entre los dos servidores instalamos la herramienta de Autoridad Certificadora, en el menú de inicio de Windows seleccionamos panel de control, agregar o quitar programas, agregar o quitar componentes de Windows, ahí seleccionamos servicios de certificación. Es importante tener el disco de instalación de Windows Server 2003 dentro de la unidad lectora de discos para instalar los componentes.

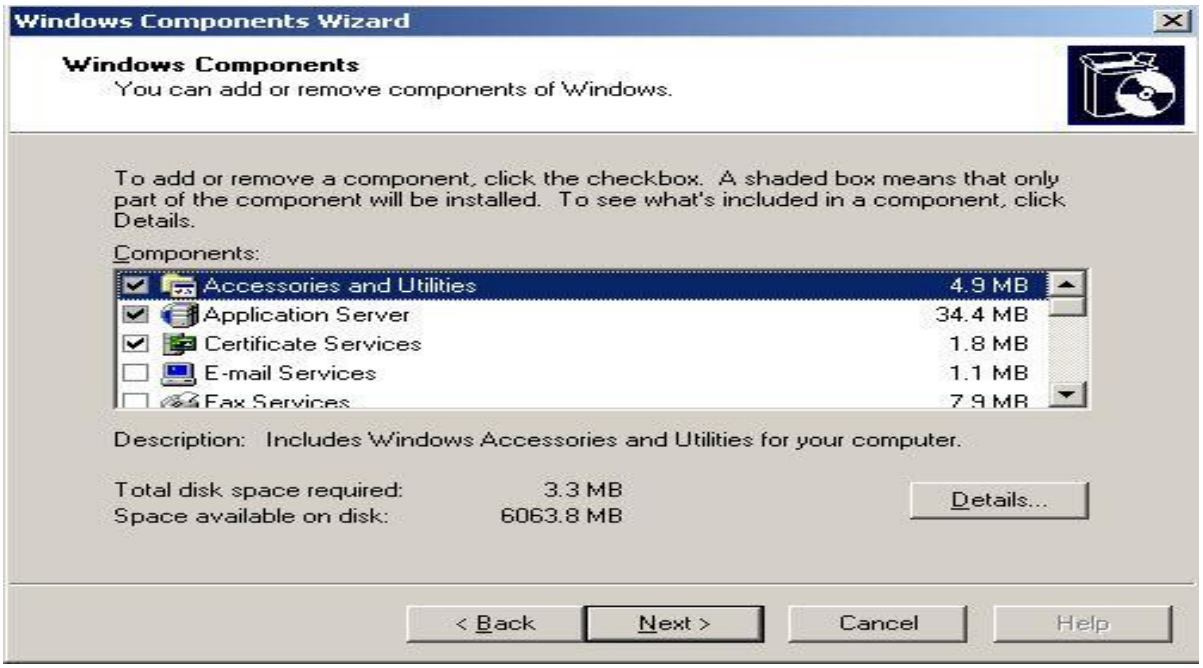

Fig. 19. Selección de Servicios de Certificación.

De aquí seleccionamos el tipo de Autoridad Certificadora, con la opción de Root CA creamos la unidad certificadora principal de nuestro sistema.

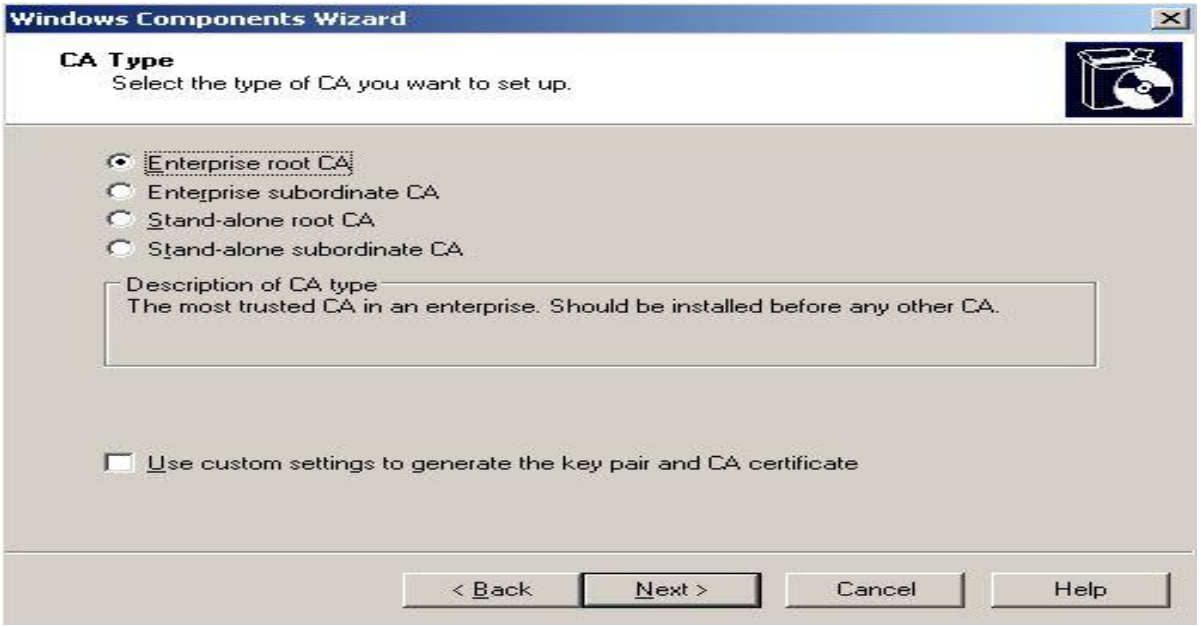

Fig. 20. Crear CA principal.

Posteriormente le asignamos un nombre a nuestra unidad certificadora y le damos el tiempo de validación, podemos observar que nuestra Autoridad Certificadora está unida a nuestro dominio. La última parte de nuestra instalación de nuestro componente es darle la dirección en donde queremos que guarde toda la documentación de la unidad certificadora.

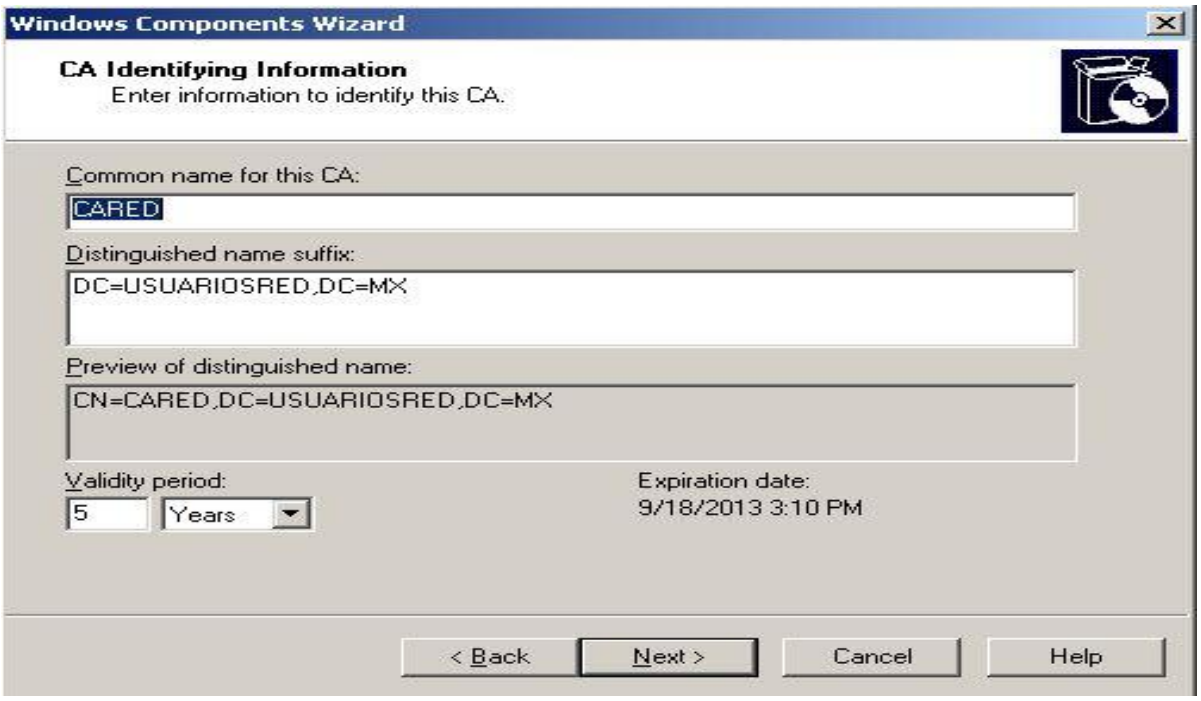

Fig. 21. Nombre de la CA.

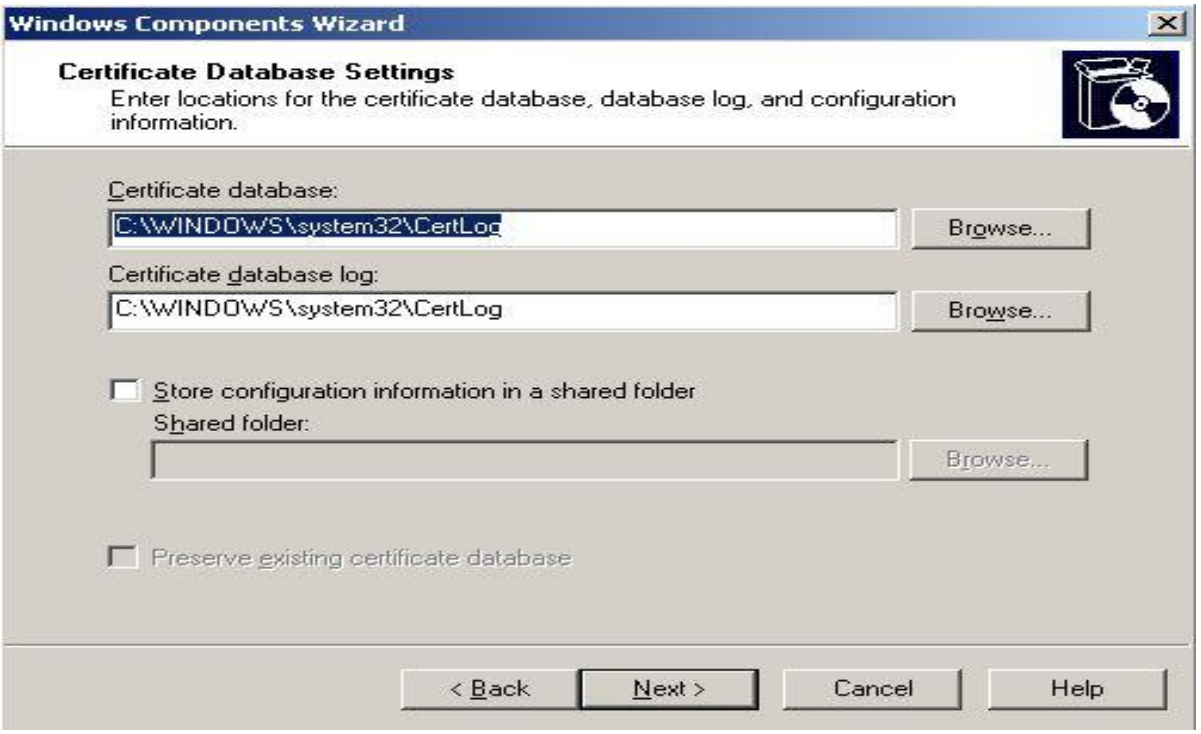

Fig. 22. Ruta de la base de datos de la CA.

Ahora al contar ya con nuestras CA es importante que a nuestros dos servidores se les expida el certificado para que el IAS – RADIUS reconozca a las máquinas como parte del sistema. En primera instancia hay que crear el certificado para expedirlos a los equipos. Iniciamos el asistente desde el panel de control, en la opción de políticas de seguridad del controlador de dominio así como se muestra en la figura siguiente. En esta opción vamos

a especificar una política para crear el certificado para las computadoras o equipos que pertenecen al directorio activo.

Fig. 23. Ruta de Inicio de asistente para asignación de certificado.

Al dar clic derecho sobre la carpeta seleccionamos la opción de nuevo para iniciar con el asistente de la política de certificado.

Fig. 24. Inicio de asistente para asignación de certificado de equipo.

Vamos a seleccionar en la siguiente como tipo de certificado el de computadoras o equipos, así como se muestra en la siguiente figura.

Fig. 25. Tipo de certificado a seleccionar.

Por último podemos observar como genera un tipo de certificados para todos los equipos que pertenecen al directorio activo.

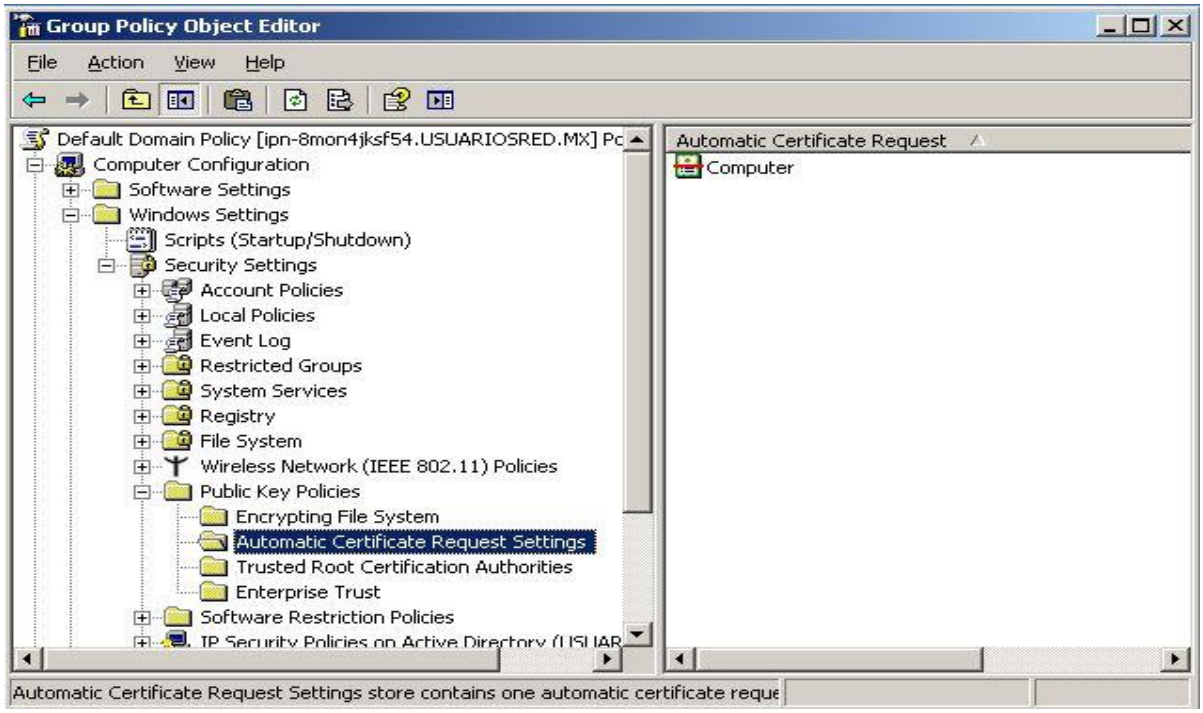

Fig. 26. Certificados para equipos.

Ahora para asignar el certificado ya creado para el servidor de control de dominio utilizaremos el comando mmc en la herramienta de ejecutar. Posteriormente seleccionamos en el menú en la pestaña de archivo agregar o quitar Snap-in.

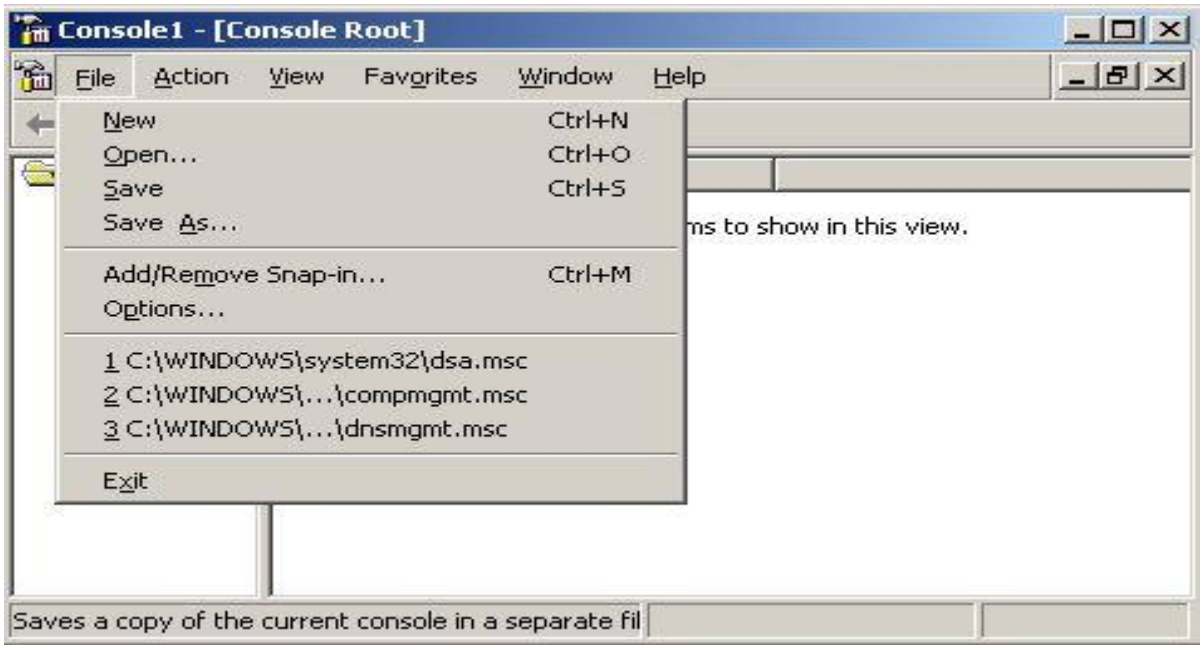

Fig. 27. Agregar o quitar elementos

Seleccionamos la opción de certificados, después la opción de computadoras y por último tomamos la opción de computadora local.

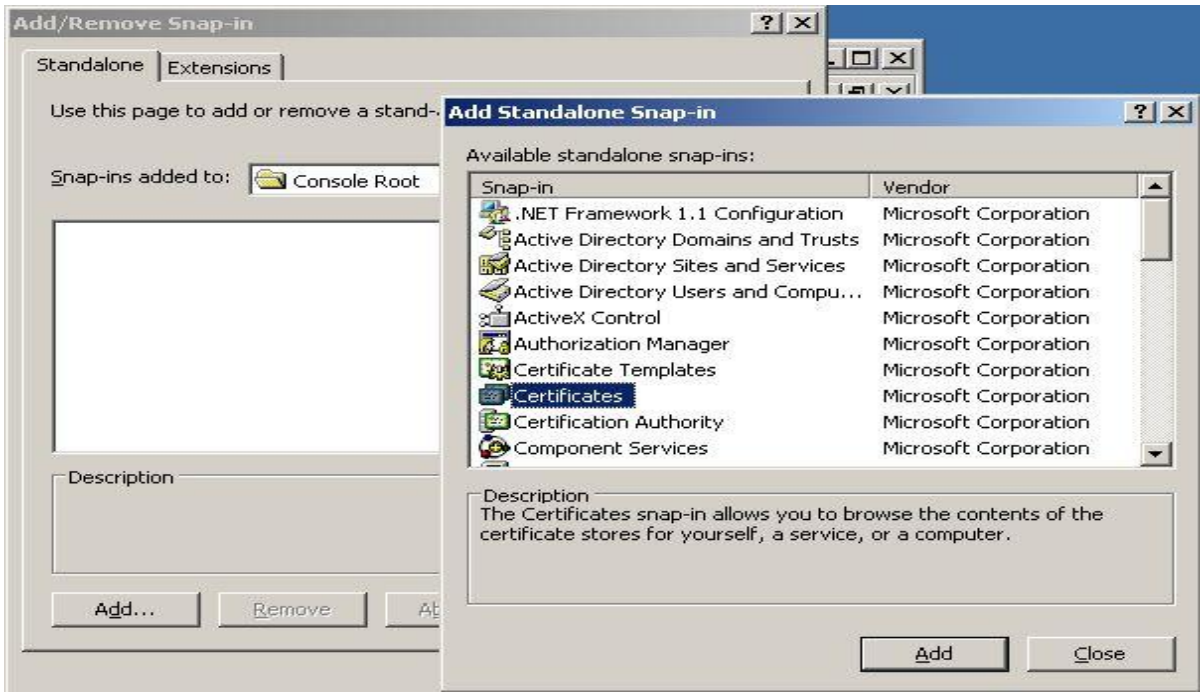

Fig. 28. Selección de certificados.

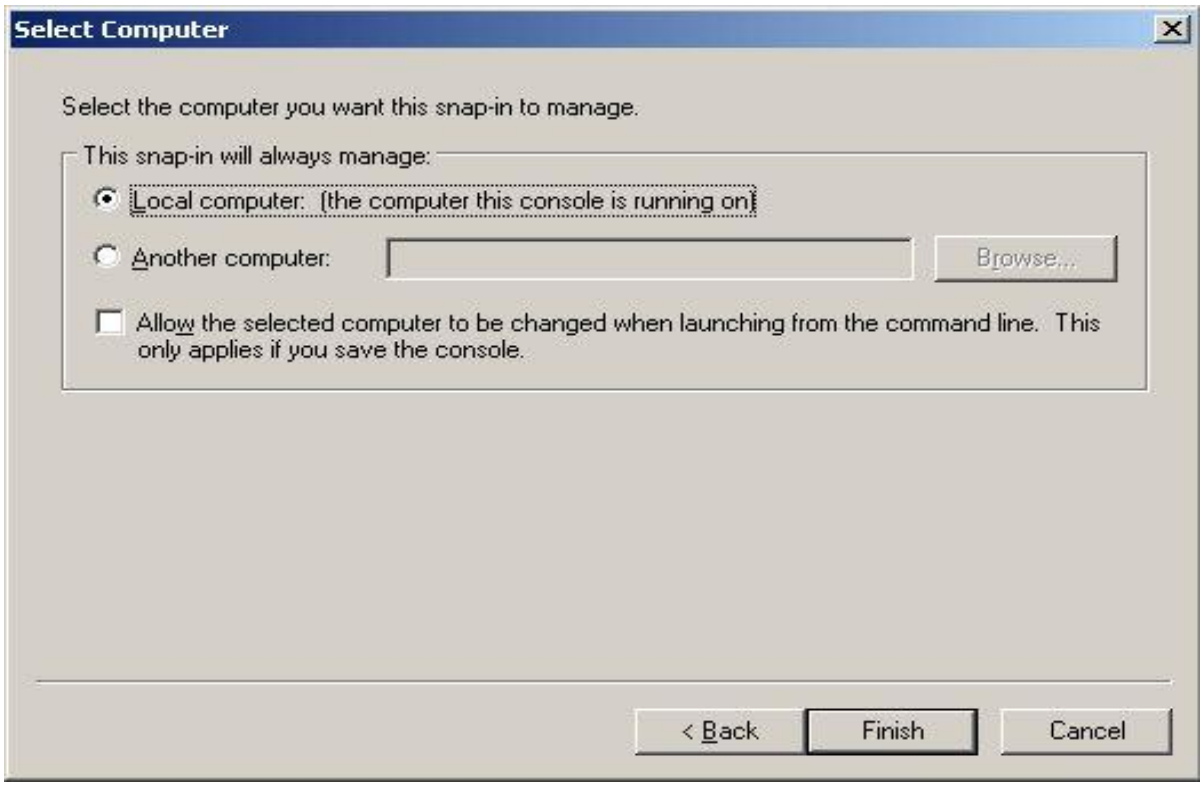

Fig. 29. Certificados para equipo local.

Ya que instalamos el certificado en servidor de controlador de dominio nos disponemos a realizar el mismo procedimiento para el servidor de IAS – RADIUS. Al terminar de instalar el certificado para el servidor IAS – RADIUS seguiremos ahora con su configuración.

Recordemos que hay ciertos elementos dentro del mismo servidor que inicialmente no están instalados con la paquetería del sistema operativo de Windows Servers 2003, el IAS es uno de estos elementos y el siguiente paso es la instalación de este complemento.

Por lo tanto siguiendo la ruta panel de control, agregar o quitar programas, agregar o quitar componentes de Windows, vamos a seleccionar el componente servicios de red y posterior a esto seleccionamos IAS.

Al seleccionar IAS como opción damos aceptar es importante seguir dentro de una cuenta de directorio activo y que los servidores estén en comunicación sin excepción.

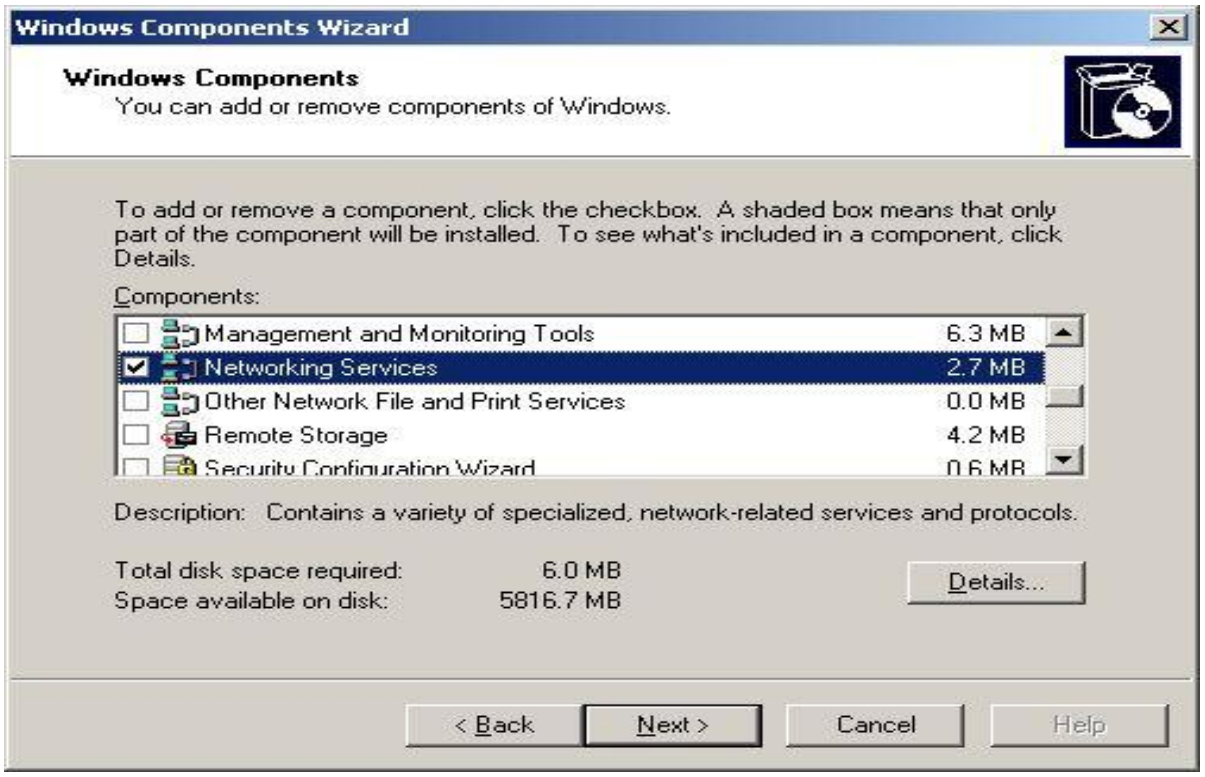

Fig. 30. Selección de servicios de red.

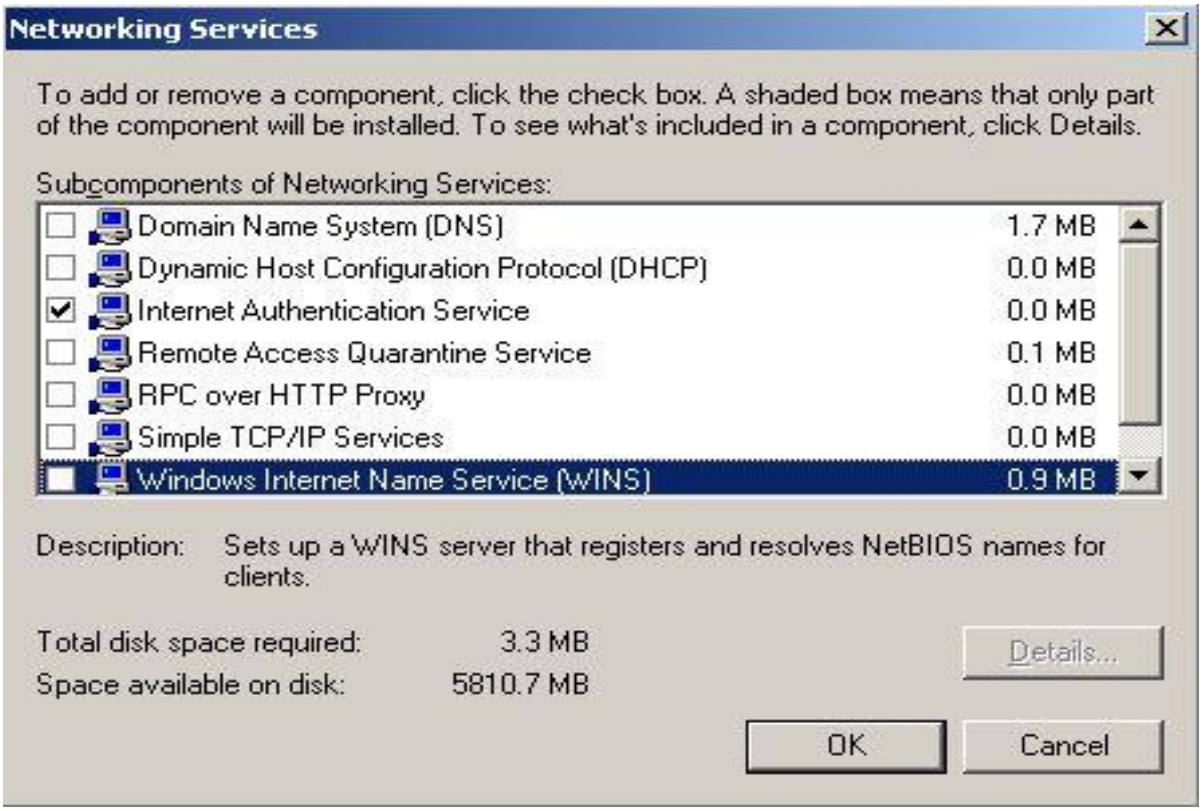

Fig. 31. Selección de IAS para instalación.

Ahora que IAS ya está instalado en nuestro servidor hay que configurar sus puertos de entrada y salida de datos. Los puertos que le corresponden son 1812 y 1645 que son usados para mensaje de autenticación, 1813 y 1646 que es utilizado para mensajes de cuentas RADIUS, como lo observamos en la siguiente figura, estos puertos están definidos por el RFC 2138.

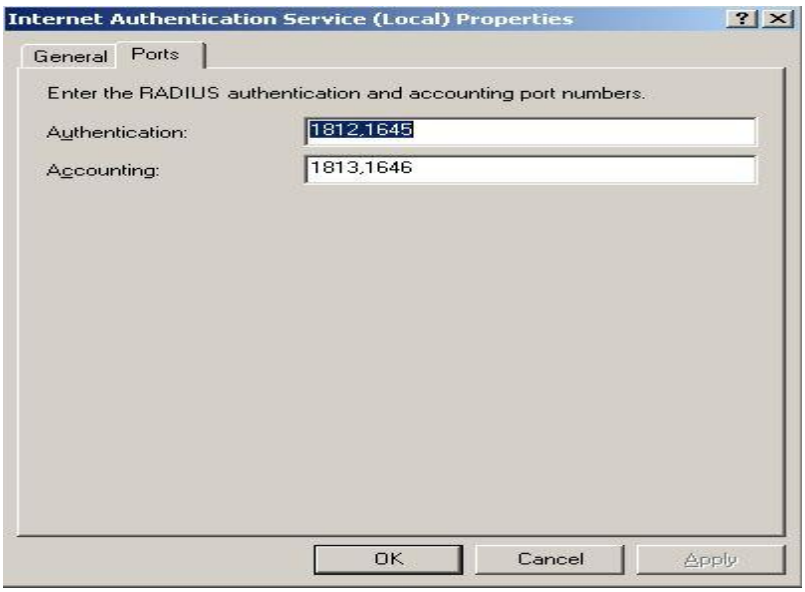

Fig. 32. Puertos del IAS.

Otro punto de la configuración es saber donde va a guardar la documentación sobre solicitudes de cuentas o solicitudes para entrar a una cuenta, etcétera. Por lo que este aspecto también se configura, se recomienda seleccionar todas las opciones y solo se designa la ruta de donde hay que guardar toda la documentación de los reportes o avisos que va generando el programa.

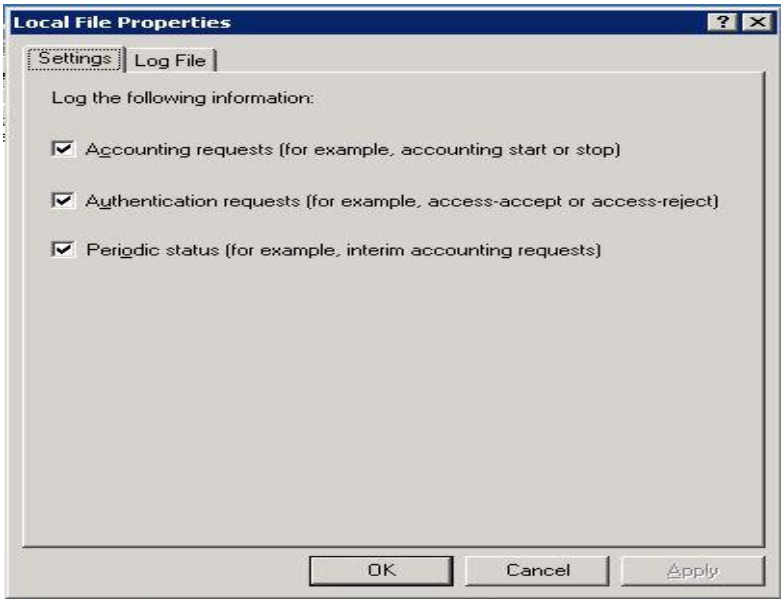

Fig. 33. Configuración de solicitudes que se van a registrar.

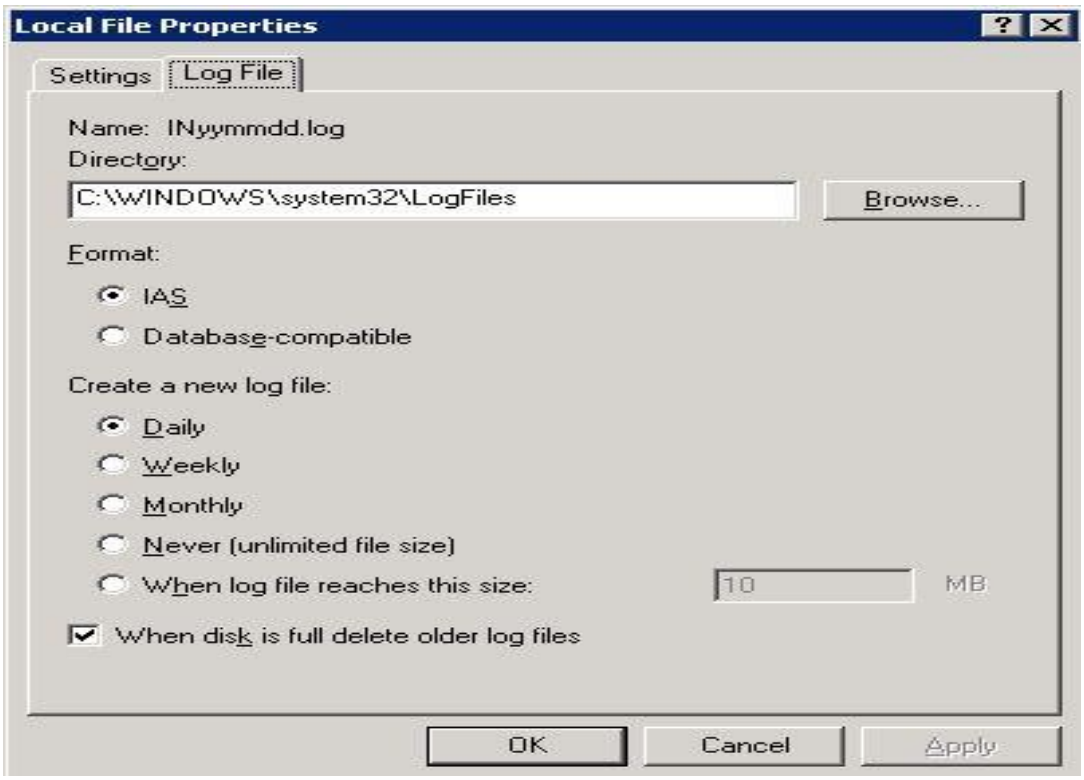

Fig. 34. Ruta de la documentación de las solicitudes.

Ahora para poder realizar la autenticación vía inalámbrica necesitamos configurar al cliente RADIUS que es nuestro equipo de acceso a la red o Access Point.

Para ello hemos elegido la marca Linksys como la marca de nuestro punto de acceso ya que la configuración de este dispositivo es muy sencilla, la serie del AP que vamos a utilizar es de la serie WRT54G, una de las características principales que debe cumplir el AP es que tiene que soportar el protocolo de seguridad 802.1x ya que este protocolo hace referencia al método de seguridad utilizado por un servidor RADIUS.

Para agregar nuestro AP en nuestro servidor RADIUS desde el panel de control seleccionamos IAS y en la carpeta de clientes RADIUS seleccionamos la opción nuevo cliente.

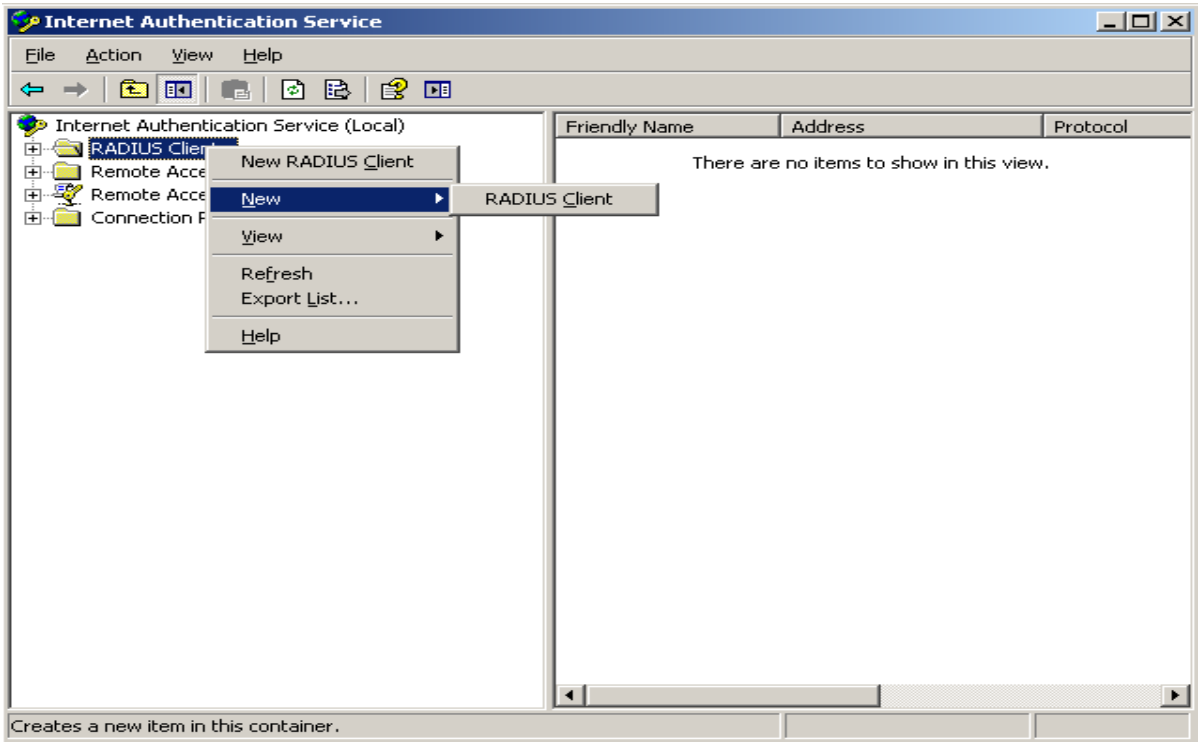

Fig. 35. Agregando clientes RADIUS.

En la siguiente configuración solo tenemos que ponerle nombre a nuestra AP y asignarle una dirección IP.

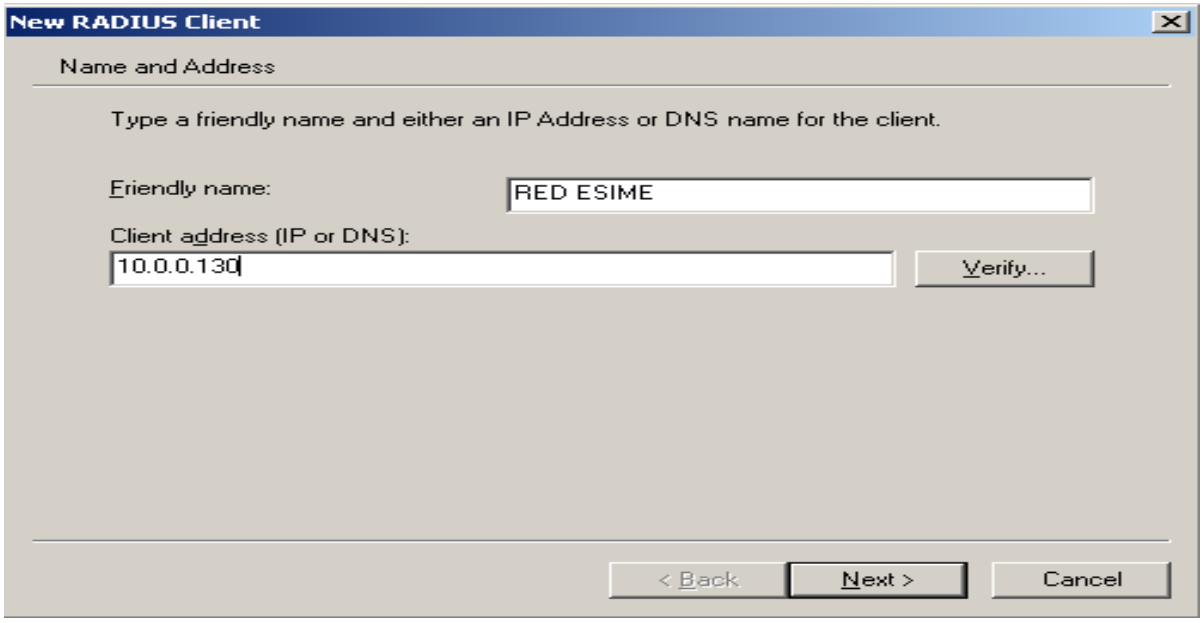

Fig. 36. Nombre de AP y dirección IP.

Posteriormente en la casilla de la configuración en vendedor de cliente hay que seleccionar la marca del AP que estamos agregando, en caso de no estar en la lista se selecciona RADIUS Estándar y por último se coloca la clave de secreto compartido el cual

tiene que coincidir con el con la clave del AP para la comunicación segura entre el AP y el servidor RADIUS.

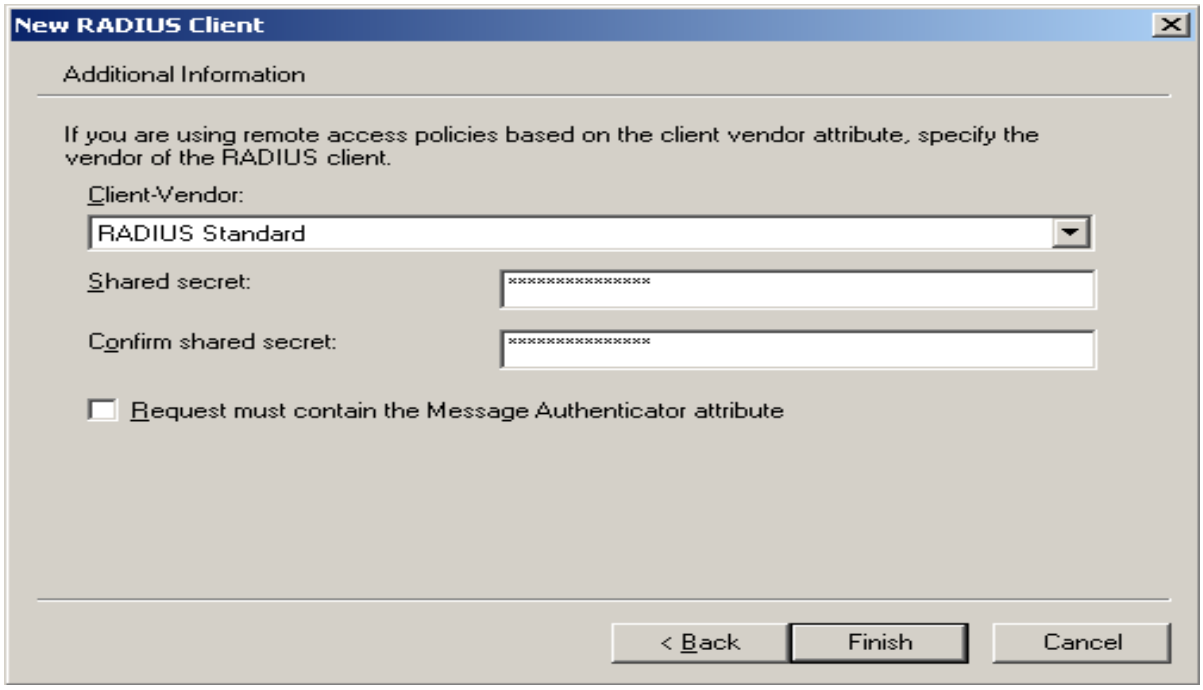

Fig. 37. Marca de AP y clave de secreto compartidos.

Por último para este punto podemos observar como queda agregado nuestro AP para la aplicación del método de autenticación.

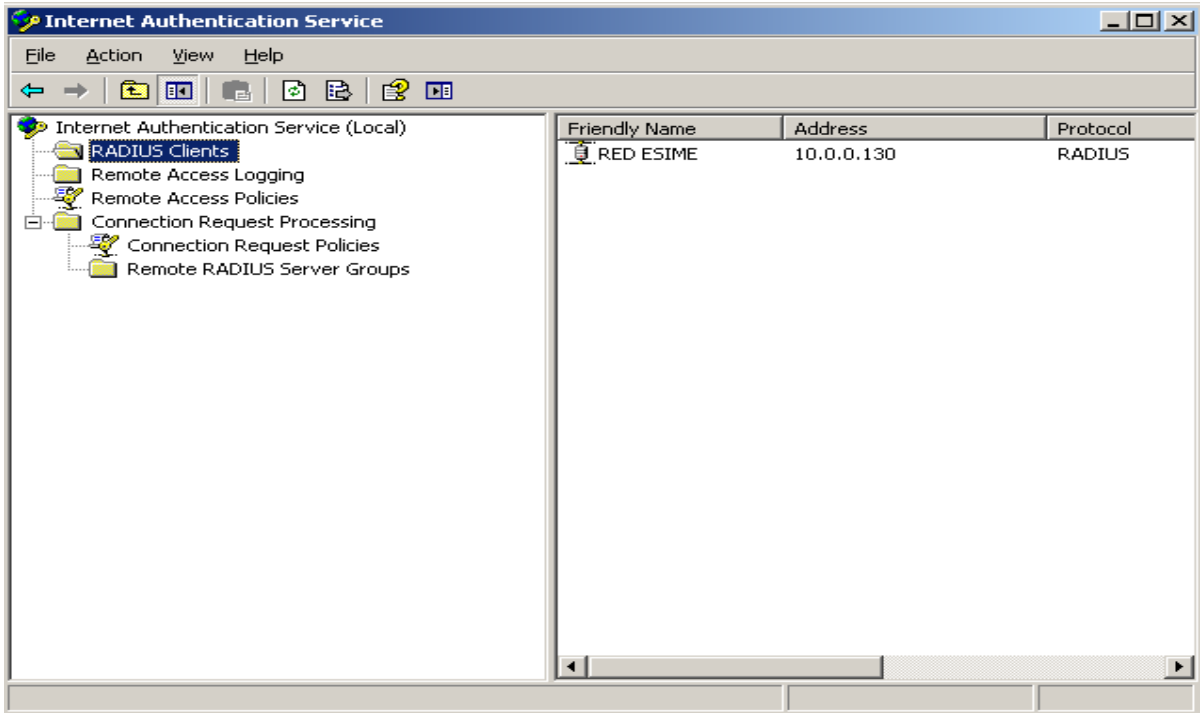

Fig. 38. Cliente RADIUS agregado.

Ahora el siguiente paso de la implementación es la configuración interna del AP la cual podemos observar es muy sencilla y sin complicaciones solo hay que recordar que la clave del secreto compartido debe serla misma que en la configuración.

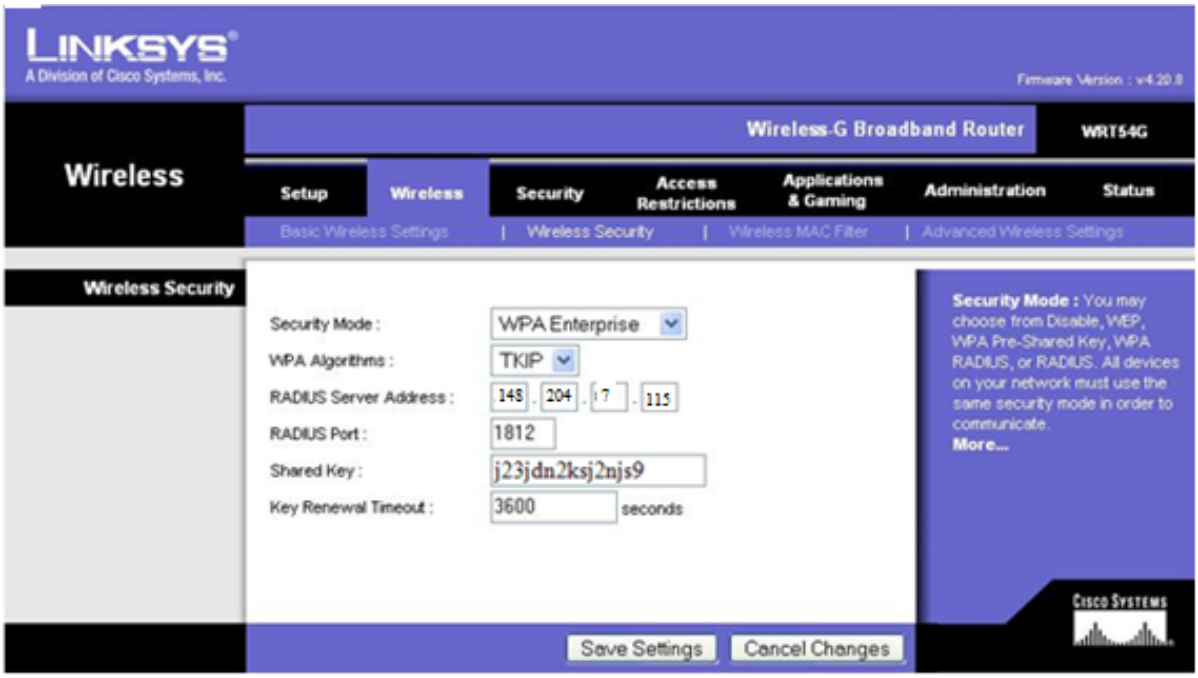

Fig. 39. Configuración del AP.

Nuestro siguiente paso para la configuración del sistema es la implementación de la política para la comunicación de acceso remoto como en este caso vía inalámbrica.

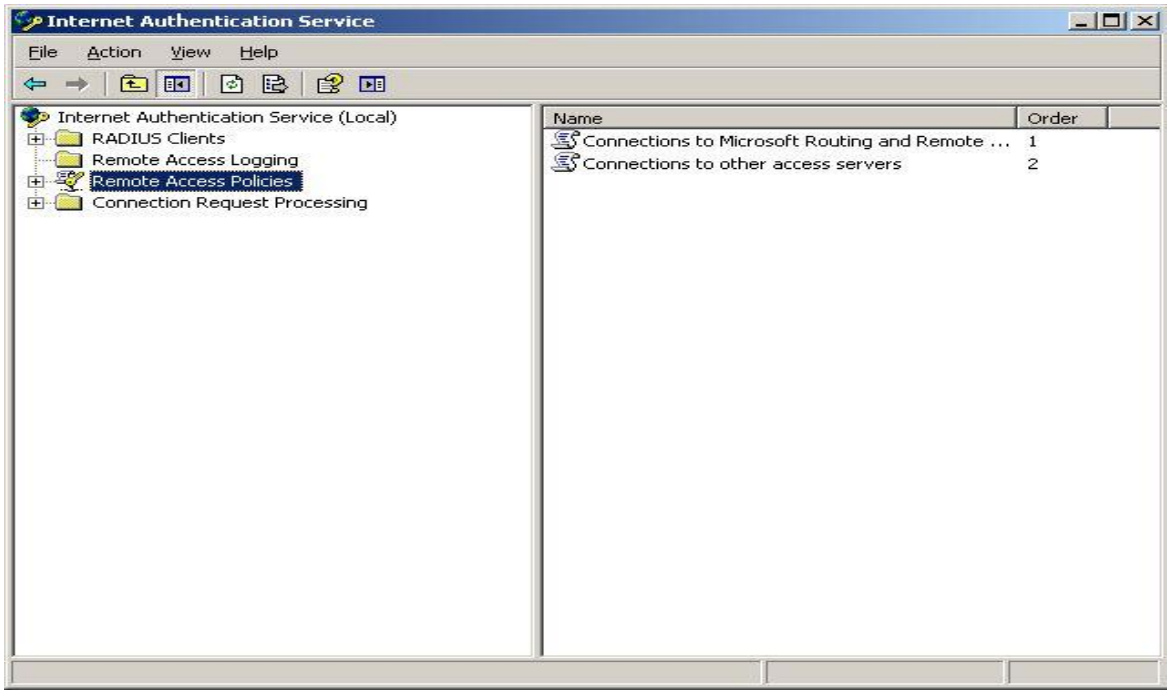

Fig. 40. Políticas de Acceso Remoto.

Fig. 41. Inicio del asistente para nueva política de acceso remoto.

Le indicamos en los campos el nombre de la política que estamos generando y le damos en **aceptar**. Enseguida hay que seleccionar el tipo de conexión en este caso es la opción Wireless lo que significa conexión inalámbrica.

Fig. 42. Tipo de conexión para la política.

En la siguiente pantalla nos proporcionará dos opciones aquí tenemos que definir hacia quién es aplicable la política, en este caso tenemos que elegir la opción de grupos, ya que

por medio de un grupo de directorio activo vamos hacer valido esta directiva, esto creara al grupo que le apliquemos la política.

Fig. 43. Aplicando a un grupo la política o directiva.

Inmediatamente le damos la ubicación donde se generará al grupo y con esto estaremos adjuntando al grupo de usuarios como pertenecientes al directorio activo del controlador de dominio.

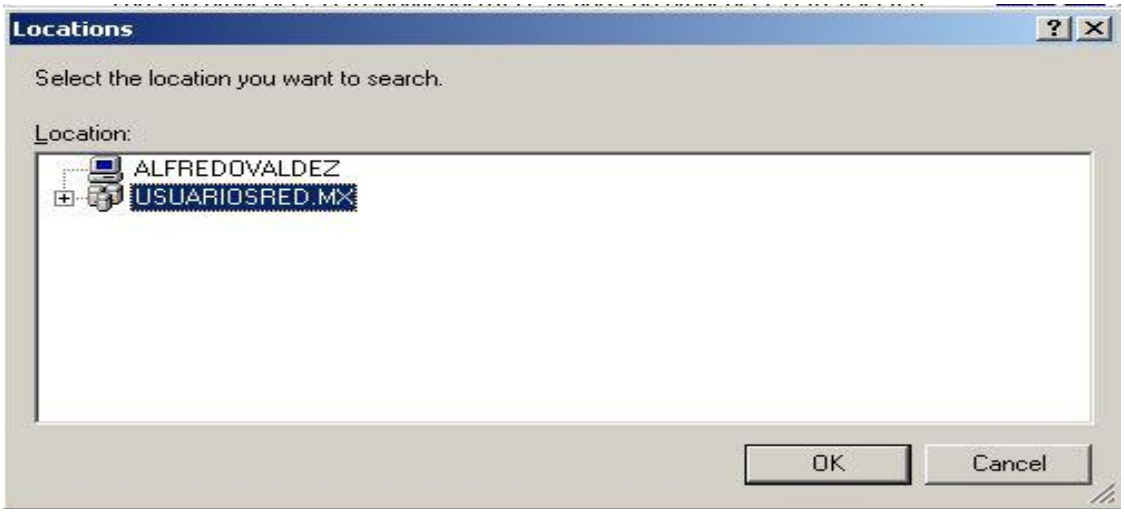

Fig. 44. Ubicación del grupo de usuarios.

Y por último le damos el nombre al grupo donde registremos a nuestros usuarios y sobre el cual la política le va ser aplicada.

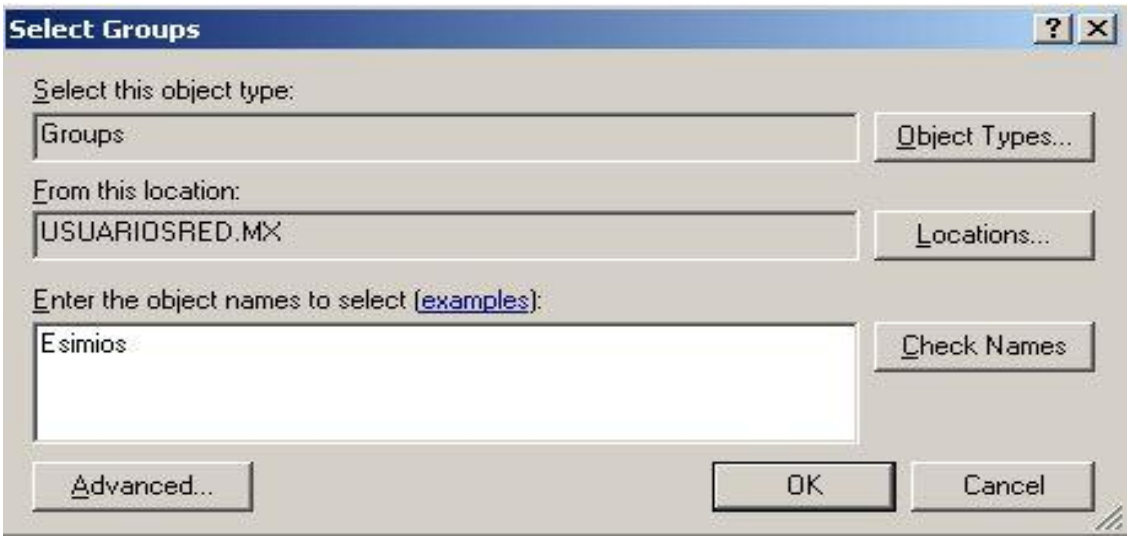

Fig. 45. Nombre del grupo al que se le aplicará la política.

Inmediatamente en la siguiente ventana nos desplegará el tipo de método de seguridad para aplicarle al grupo y al tipo de conexión en este caso seleccionaremos el método EAP-PEAP, el cual consiste en certificados y en mensajes de desafío respuesta.

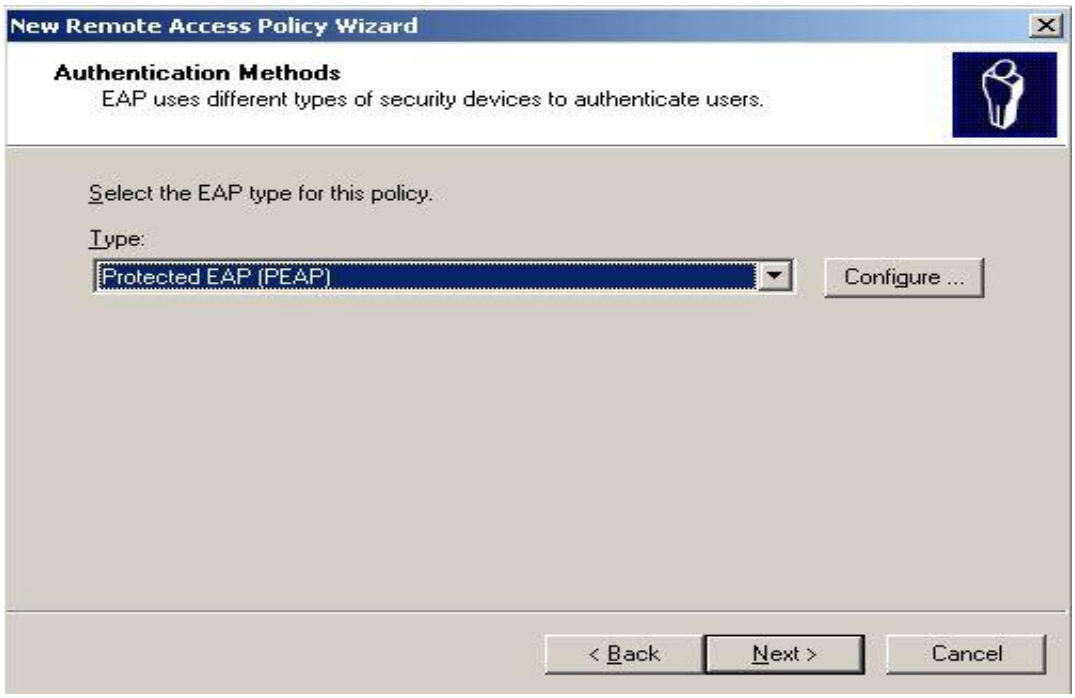

Fig. 46. Selección de método de seguridad.

Por último finalizamos con la configuración de la política. Como lo muestra la siguiente figura.

Fig. 47. Termino de la creación de la política de acceso remoto.

Para concretar con este punto es importante checar el registro de las políticas y las especificaciones guardadas en la configuración. Podemos observar en la siguiente como las políticas siguen dentro del mismo directorio activo y que nuestra política fue creada con éxito.

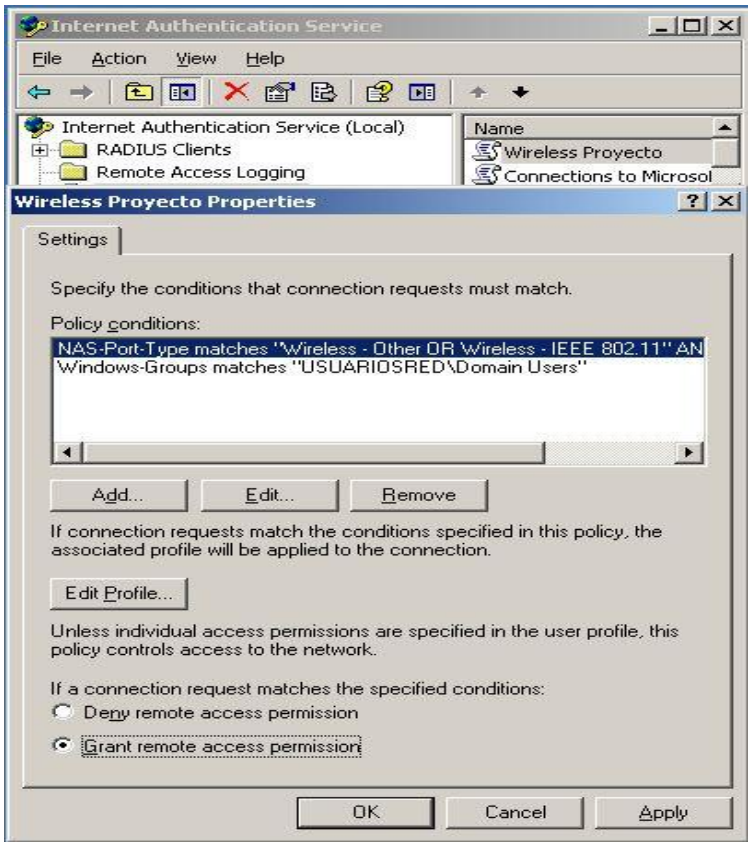

Fig. 48. Registro de la política de acceso remoto.

Para concluir con las configuraciones del servidor IAS – RADIUS vamos a configurar el método de autenticación el cual estará definido por EAP-PEAP con MS-CHAP$_{v2.}$ Así como se muestra en la imagen se realiza la configuración.

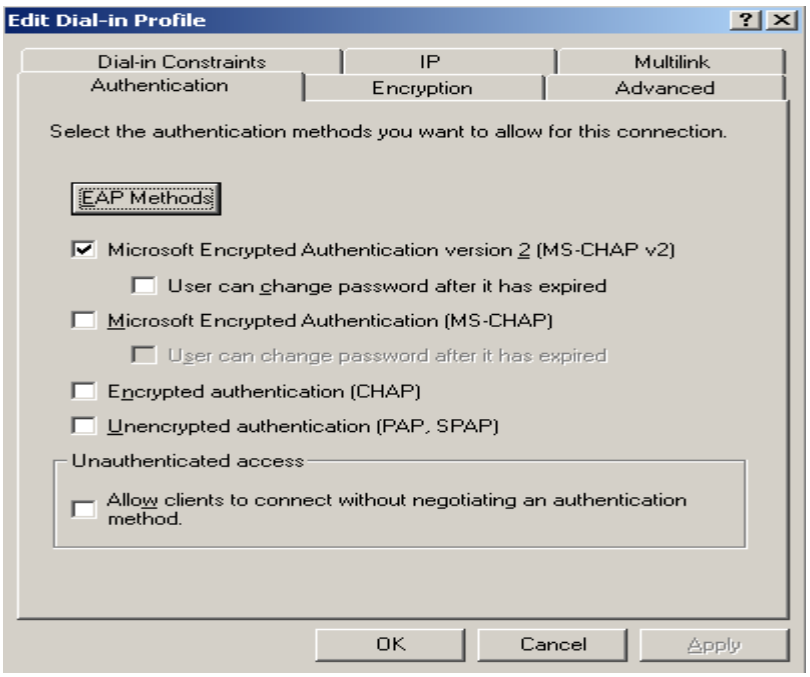

Fig. 49. Activación del método de seguridad EAP.

Ahora disponemos a seleccionar el tipo de método para la autenticación.

Fig. 50. Tipo autenticación seleccionado.

Y por último seleccionamos el certificado que servirá para realizar la autenticación para iniciar la intercomunicación entre el AP y el cliente inalámbrico.

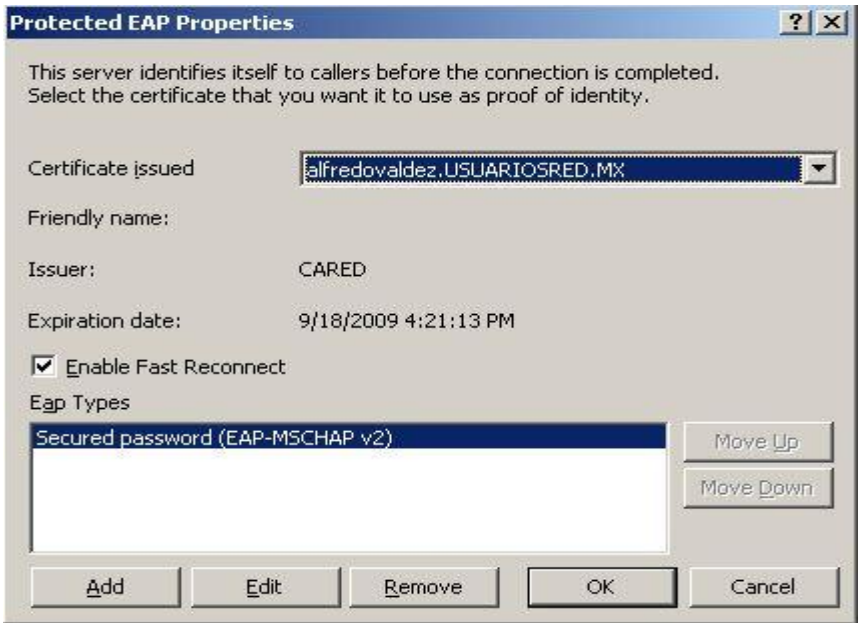

Fig. 51. Definición del certificado que utilizara para la autenticación.

Para poder obtener el certificado necesitamos instalar en el servidor RADIUS la herramienta IIS de Windows, esto para que a través de un programa de explorador de internet y el IP del servidor nos genere una página con una plantilla predeterminada donde podamos adquirir el certificado y bajarlo por una unidad flash.

La plantilla se muestra en la siguiente figura y seleccionamos la opción descargar un certificado de la Autoridad Certificadora. La ruta para bajar el archivo se recomienda que sea en una memoria flash USB en caso de que se necesite para varios equipos. El archivo al ser copiado en el equipo será necesario instalarlo.

Fig. 52. Plantilla de descarga del certificado.

Al descargar el archivo en la memoria flash o en el equipo se verá de la siguiente manera en el explorador de archivos.

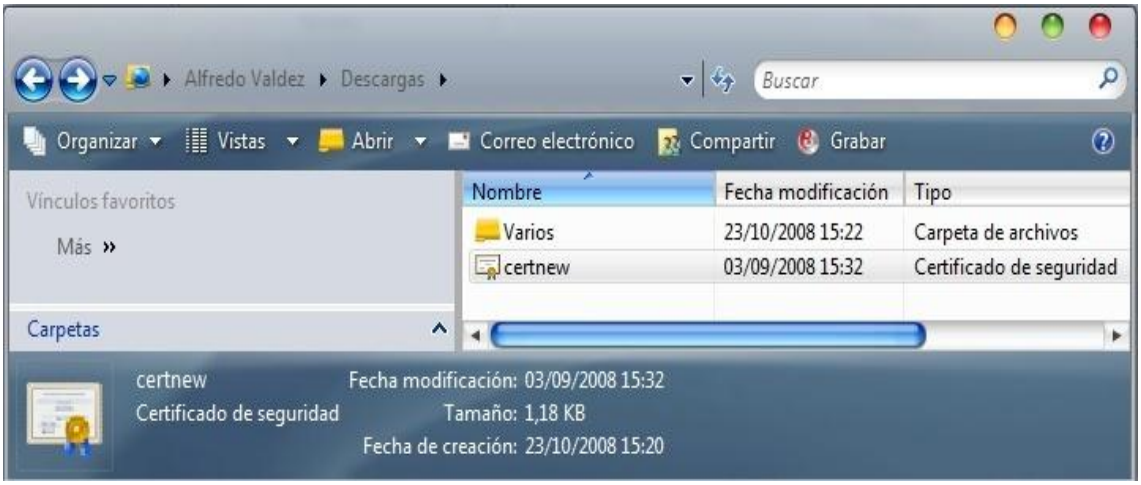

Fig. 53. Archivo de certificado descargado.

Para instalar el certificado hay que dar doble clic sobre el archivo del certificado, y nos aparecerá la ventana en donde seleccionaremos la opción de instalar certificado.

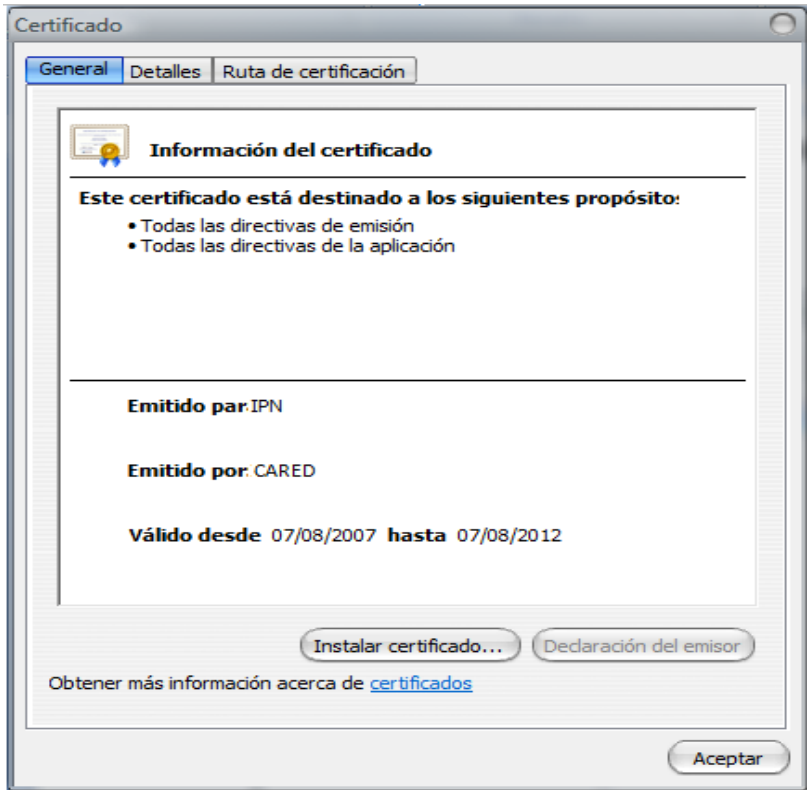

Fig. 54. Menú y presentación del certificado.

Después de instalar el certificado podemos asegurarnos de la ruta de la instalación del certificado en el equipo cliente.

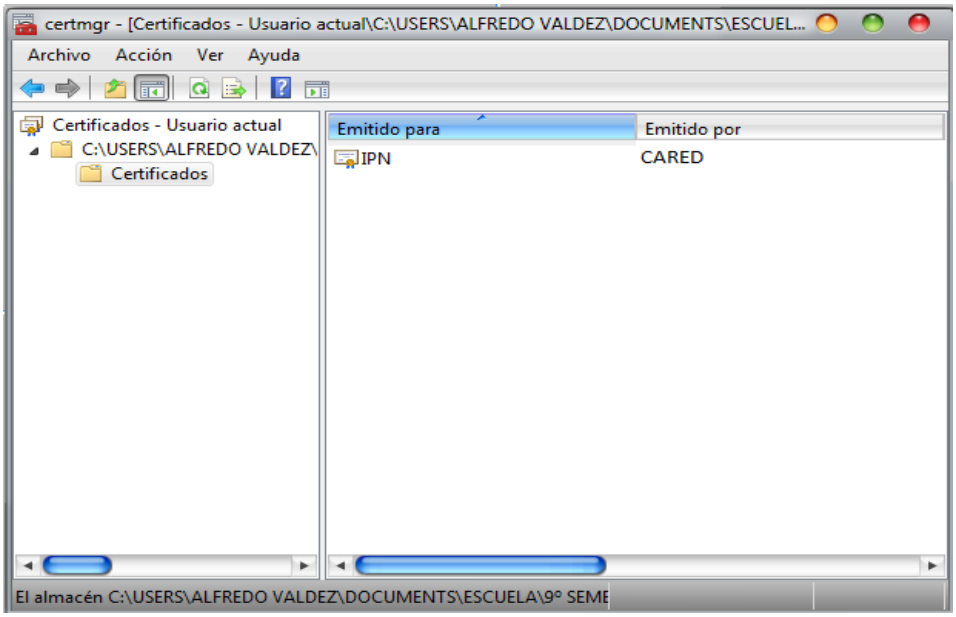

Fig. 55. Certificado instalado en el equipo.

4.4 PRUEBA DEL FUNCIONAMIENTO DEL SISTEMA DE AUTENTICACION

Para comprobar un óptimo funcionamiento del sistema de autentificación hemos definido las siguientes pruebas:

- Realizar la conexión con equipos con sus certificados instalados pero con sistemas proporcionando el nombre de usuario y contraseñas correctas.

- Intentar la conexión pero sin la instalación de certificados en los equipos.

- Realizar la conexión con equipos con sus certificados instalados pero proporcionando el nombre de usuario incorrecto, contraseña incorrecta o ambas.

- Realizar el proceso de autentificación con diferentes cuentas de usuario de nuestro directorio activo.

El primer punto que decidimos probar fue el intento de conexión con el AP sin tener en el equipo de computo el certificado instalado, la prueba fue realizada con dos equipos, en los dos casos intentamos conectarnos a la red inalámbrica pero no fue posible. El siguiente paso a seguir fue la instalación de los certificados en los equipos, una vez instalados intentamos conectarnos a la red inalámbrica, al hacer la petición el AP envía una plantilla requiriendo un nombre de usuario y su contraseña como se muestra en la siguiente figura.

Fig. 56. Plantilla de desafió para la autenticación de usuario.

En este punto se decidió en primera instancia proporcionar los nombres de usuario y contraseñas correctos, al apretar aceptar (OK) observamos que la conexión era exitosa al comprobar que teníamos el servicio de internet en los equipos. Estas pruebas posteriormente se realizaron con varias cuentas creadas con anterioridad y como resultado observamos que en ocasiones la conexión con la red fallaba, pero al intentar de nuevo el procedimiento obteníamos una conexión exitosa.

Este último procedimiento se realizo con 10 cuentas de directorio activo y por cada cuenta se realizaron 10 pruebas de conexión en donde el único problema que observamos es que en ciertas ocasiones no se lograba la conexión en el primer intento.

Por último realizamos el procedimiento para cada una de las cuentas pero proporcionando el nombre de usuario y contraseña de manera incorrecta y observamos que al oprimir aceptar (OK) la plantilla nuevamente hacia la petición de nombre de usuario y contraseña, pero al tercer intento fallado ya no se volvían a solicitar nuevamente los datos hasta realizar nuevamente la petición de conexión a la red.

4.5 ADMINISTRACION DE LA RED

Para llevar a cabo una buena administración y un correcto funcionamiento del sistema de autenticación será necesario tomar en cuenta que se requiere de personal capacitado que cuente con conocimientos de informática, sistemas, redes, para cubrir con las siguientes necesidades satisfactoriamente:

- ✓ **Mantenimiento al hardware del equipo de cómputo:** Es importante que el equipo reciba mantenimiento cuando el equipo sufra de alguna descompostura o que necesite cambio de algún dispositivo.

- ✓ **Actualizaciones del software:** Para tener nuestro sistema con un optimo desempeño es necesario tener actualizados nuestros sistemas operativos, programas antivirus, VMware para el soporte de los servidores virtuales, etc.

- ✓ **Administración del servidor del controlador de dominio:** Las actividades que se requieren para llevar a cabo la administración de este servidor son: Registro de usuarios en el directorio activo, revisión de políticas o directivas de grupo, baja de usuarios o bloqueos de cuentas.

- ✓ **Administración del servidor IAS-RADIUS:** El servidor RADIUS requerirá de que los administradores registren nuevos clientes RADIUS (nuevos puntos de acceso) en caso de ser necesario, para ello administrará las claves de seguridad de secretos compartidos y en cuanto a la unidad certificadora el usuario creara los nuevos certificados con los nuevos tiempos de validación e instalara los certificados en los equipos de los usuarios.

Es necesario que los administradores del sistema implementen la organización como según les convenga, ya sea para el método de registro de los usuarios, expedición e instalación de certificados en los equipos de los usuarios y tiempos de atención a usuarios para resolución de problemas. Como el servicio esta planeado para ofrecerlo a los alumnos y profesores de la ESIME Zacatenco el personal deberá cubrir los horarios más convenientes para la comunidad escolar.

4.6 EVALUACIÓN ECONÓMICA

La evaluación económica de este proyecto esta dividido en dos aspectos importantes, que son: las inversiones requeridas y los costos directos e indirectos.

- Resumen de inversiones requeridas

Para poder llevar a cabo este proyecto, son necesarios ciertos dispositivos, estos dispositivos tienen un precio variable de acuerdo al proveedor que se consulte sin embargo, la tabla que a continuación se presenta esta basada en un promedio, tomando en cuenta varios proveedores y el tipo de cambio peso-dólar que a la fecha se encuentra vigente, además de que se toma en cuenta el costo de instalación.

Tabla 8
Inversiones Requeridas

Descripción	**Precio**
Router inalámbrico de la marca Linksys modelo WRT54G	$ 1,000.00
Licencia de Windows Server 2003 para dos equipos	$ 800.00
Servidor DELL poweredge T605	$ 23,000.00
Costos de instalación	$ 96,000.00
SUB TOTAL	**$ 120,800.00**

Entre las inversiones requeridas y los costos de instalación tenemos un total de:

$ 120,800.00

CONCLUSIONES

Conclusiones respecto al proyecto desarrollado

Con base en las pruebas realizadas, podemos concluir que el sistema de autenticación para el acceso a redes inalámbricas que estamos aplicando es compatible con el tipo de administración que se lleva a cabo en el IPN, utilizando las herramientas del Windows Server 2003.

Este sistema es viable en su instalación ya sea a nivel local; en ESIME o a nivel institucional IPN, ya que este sistema puede ajustarse al tamaño de red que se requiera.

La utilización de servidores virtuales disminuye el costo de esta aplicación, además de que se obtiene un mejor aprovechamiento de los recursos disponibles, en lugar de hacer uso de un solo servidor físico.

Conclusiones respecto al logro de los objetivos

El sistema de autenticación que proponemos cumple con la premisa de que solo los usuarios autorizados pueden hacer uso de la red teniendo la certeza de que su información viaja de manera segura. Esto se pudo comprobar con los resultados obtenidos en las pruebas realizadas con el sistema de autenticación. Este hecho permite superar la restricción impuesta por las autoridades de la escuela para poner al alcance de nuestra comunidad los beneficios de la red, sobre todo para el acceso a Internet.

Por esta razón, podemos concluir que el proyecto ha alcanzado plenamente los objetivos planteados, quedando disponible para que las instancias responsables de la escuela procedan a su aplicación y puesta en operación.

Este sistema cumple con elementos de seguridad necesarios para garantizar la seguridad de nuestra red estos elementos necesarios son los siguientes:

El protocolo EAP-PEAP que nos permite una conexión segura entre el usuario y el AP y la clave de secretos compartidos que nos permite seguridad de conexión entre el AP y el servidor RADIUS, por ultimo tenemos IPSEC que nos permite comunicación segura entre los servidores de nuestro sistema.

Conclusiones respecto a la forma en que se realizo el trabajo

Durante la realización de este proyecto se encontraron diferentes obstáculos, principalmente por las limitantes existentes en la propia escuela en cuanto al uso de los recursos y la disponibilidad de información sobre la infraestructura de redes en la ESIME Zacatenco. Esta situación obligó a buscar la información y las tecnologías necesarias en otras instancias del IPN.

El desarrollo de este proyecto se llevo a cabo en la Dirección de Computo y Comunicaciones, teniendo las limitantes de tiempo de estancia a si como de espacio, por lo que solo se realizaron las pruebas que estuvieran al alcance de los recursos disponibles es por eso que las personas que deseen continuar o retomar este proyecto deberán tener en cuenta que se deben realizar pruebas que proporcionen un mayor nivel de confianza, tales como incrementar la demanda de peticiones para poder saber el rendimiento del sistema, otra recomendación es poner a prueba los protocolos de seguridad utilizando métodos de ataque a estos protocolos, como por ejemplo software que realice criptoanálisis para descifrar llaves de seguridad, contraseñas, nombres de usuario o cualquier paquete de información.

FUENTES DE INFORMACIÓN

- Andreu Fernando, “Fundamentos y aplicaciones de seguridad en redes WLAN”, Marcombo.

- Huidobro Moya José M, “Comunicaciones en redes WLAN”, creaciones copyright

- Mitch Tulloch, “Microsoft Encyclopedia of Security”, Microsoft Press, 2003.

- http://www.microsoft.com/latam/technet/seguridad/

- http://technet.microsoft.com/en-us/library/cc779009.aspx

- http://technet.microsoft.com/en-us/library/cc787275.aspx

- http://articles.techrepublic.com.com/5100-10878_11-6148579.html

- Mejía Nogales J Luis ”Sistema de Acceso Seguro a Recursos de Información para Redes Inalámbricas 802.11”, México DF 2006