ESCUELA POLITÉCNICA DEL EJÉRCITO
SEDE LATACUNGA

CARRERA DE INGENIERIA EN SISTEMAS E INFORMÁTICA

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TITULO DE:
INGENIERA EN SISTEMAS E INFORMÁTICA

DISEÑO E IMPLEMENTACIÓN DE SEGURIDADES LÓGICAS EN REDES INALÁMBRICAS DE DATOS FIJAS EN LOS LABORATORIOS DE LA FACULTAD DE SISTEMAS E INFORMÁTICA DE LA ESPE-L

MARIA DEL CARMEN ERAZO CAJAS

LATACUNGA – ECUADOR

2007

CERTIFICACIÓN

SE CERTIFICA QUE EL PRESENTE TRABAJO FUE DESARROLLADO POR MARIA DEL CARMEN ERAZO CAJAS, BAJO NUESTRA SUPERVISIÓN.

_____

ING. SANTIAGO JÁCOME
DIRECTOR DE PROYECTO

_____

ING. RAÚL CAJAS
CODIRECTOR DE PROYECTO

AGRADECIMIENTO

Mi profundo agradecimiento y gratitud, por los conocimientos impartidos a quienes aportaron su sabia experiencia, de manera desinteresada e incondicional, para la culminación del presente trabajo de investigación ya que sin su ayuda no hubiese sido posible llegar a feliz término.

De manera especial no quiero dejar de reconocer su labor fecunda y próspera por el apoyo recibido de mis queridos maestros Ing. Santiago Jácome e Ing. Raúl Cajas, quienes en su destacada labor docente han formado personas y profesionales con espíritu emprendedor.

A mi noble Institución ESPE Sede Latacunga, en sus aulas adquirí la sapiencia impartida por tan notable cuerpo docente que de igual manera aportaron en mi formación estudiantil y profesional, infinitas gracias por haberme dado la posibilidad de formarme íntegramente como persona adquiriendo valores y virtudes humanas que solo allí pude encontrar.

DEDICATORIA

Éste trabajo lo dedico con todo mi amor a ti DIOS que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

De manera especial y con todo cariño a mis padres que me dieron la vida y que han estado conmigo en todo momento. Gracias por todo papá y mamá por darme una carrera para mi futuro y por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón, también agradezco a mis hermanos quienes han estado a mi lado impulsándome a seguir adelante, sin ellos nada de esto fuera posible.

María del Carmen

PRESENTACIÓN

EL SIGUIENTE PROYECTO ESTA ORIENTADO HACIA LA NUEVA TECNOLOGÍA COMO LO ES LA TECNOLOGÍA INALÁMBRICA CON SUS SEGURIDADES CORRESPONDIENTES, UN TEMA MUY INTERESANTE E INDISPENSABLE EN EL CAMPO PROFESIONAL, Y DE GRAN AYUDA A ESTUDIANTES, PROFESIONALES SIRVIENDO COMO FUENTE DE CONSULTA.

Latacunga, octubre del 2007.

_____

María del Carmen Erazo Cajas

AUTORA

_____

Ing. Edison Espinosa

CORDINADOR DE LA CARRERA DE INGENIERIA EN SISTEMAS E INFORMÁTICA

_____

Dr. Eduardo Vázquez Alcázar

SECRETARÍA ACADÉMICA ESPE-L

CAPITULO I

1.1 INTRODUCCIÓN A LAS REDES INALÁMBRICAS DE DATOS FIJAS

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica, debido a que facilita la operación en lugares donde las computadoras no pueden permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos, además permiten a sus usuarios acceder a la información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Una red inalámbrica es un sistema de comunicación de datos flexible, donde la información viaja por medio de ondas de radio frecuencia o luz infrarroja, manteniendo conexión con una red de computadoras en la cual un usuario dentro de esta red puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios.

Las conexiones inalámbricas pueden ampliar o reemplazar una infraestructura cableada en situaciones en donde resulta costoso o está prohibido tender cables. Las instalaciones temporales son un ejemplo de cuándo una red inalámbrica puede tener sentido o hasta ser requerida ya que en algunos tipos de edificios o códigos de construcción pueden prohibir el uso de cables, haciendo de las redes inalámbricas una alternativa importante. Y, por supuesto, el fenómeno asociado al término "inalámbrico", es decir, no tener que instalar más cables además de los de la red de telefonía y la red de alimentación eléctrica, ha pasado a ser el principal catalizador para las redes domésticas y la experiencia de conexión desde el hogar.

Si nos basamos en el gran y continuo crecimiento que tiene la informática y la telecomunicación, podemos asegurar que los PC tendrán cada vez mayor importancia en el mundo laboral, es necesario la utilización de redes inalámbricas para un desplazamiento ágil, cómodo, rápido y confiable de los usuarios en el entorno de su trabajo, este principio básico es cada vez mas reconocido como parte fundamental de la productividad y competitividad de la empresa.

El atractivo de las redes inalámbricas de datos fijas está en la combinación de flexibilidad, ubicación de la red y distancia entre nodos de red que hace que las redes inalámbricas superen al trivial mundo cableado, ofreciendo a los usuarios de la red resolver varios problemas asociados a las redes con cableado fijo y, en algunos casos, incluso reducir los gastos de implementación de las redes.

1.2 ENTORNO EN REDES INALÁMBRICAS DE DATOS FIJAS

Las empresas han reconocido la necesidad de convergencia de voz, video y datos sobre la red, y así explotar al máximo el potencial de sus redes de datos y maximizar el retorno de sus inversiones en infraestructura. En este entorno la **movilidad** se convierte en un requerimiento clave. Los usuarios de la empresa requieren acceso a los datos y aplicaciones almacenados en sus servidores, o el acceso a Internet, en cualquier momento, sin tener en cuenta donde están ubicados.

Para poder llenar los requerimientos de movilidad, el uso de redes inalámbricas se vuelve un componente clave dentro de la infraestructura empresarial. Además las redes inalámbricas ayudan a reducir costos de planificación e implementación de cableado estructurado y a optimizar tiempos de instalación en las empresas, ya que son cómodos de instalar, son escalables y fáciles de administrar, los movimientos, los cambios y el agregado de clientes a la red son simples de implementar.

Los requerimientos son mínimos, lo único que se necesita es:

- Contar con un Access Point (AP), que funciona como antena receptora y es el corazón de una red Wireless. Si lo vemos como el esquema tradicional de su red cableada, el AP reemplaza a su HUB (concentrador) o su Switch.
- Que cada computadora o laptop tenga una tarjeta Wireless instalada, ya que esta tarjeta es la que le permite al equipo enviar su señal al AP. Esta tarjeta reemplaza a su tarjeta de red tradicional.

Este es el único equipo necesario para contar con una red Wireless en su casa, oficina o negocio. El número de AP's necesarios varia según la distancia en metros de los equipos o el tamaño de la oficina o negocio. Normalmente, un AP puede dar servicio a un radio de 50 metros de forma óptima.

Además en una implementación wireless se deben realizar pruebas de distancias e interferencia, en la cual, nuestros consultores realizan pruebas con AP's y laptops con el fin de determinar la viabilidad de la distancia entre sus equipos, identificar la localización física óptima para los AP's y analizar si no hay radio frecuencias que puedan degradar la señal.

Las redes inalámbricas no solo tienen su centro de introducción en entornos en los que es mandatorio una solución inalámbrica. Contrariamente a lo que se piensa, una de sus grandes ventajas radica en su empleo como red fija, pues son múltiples los beneficios que ofrecen frente a la instalación de cableado estructurado convencional. Es esta una faceta todavía relativamente desconocida pero que puede reportar un fuerte impulso a su introducción en el ambiente empresarial y residencial. Se puede aplicar tanto a redes de Área local (LANs) dentro de la empresa como en

la interconexión de redes de edificios próximos, en la que la solución cableada requiere complejas tramitaciones o es obligada la contratación de la línea de datos a un operador de red con licencia para operar públicamente.

1.3 MODELOS DE REDES INALÁMBRICAS DE DATOS FIJAS

1.3.1 CONEXIÓN PUNTO A PUNTO

El enlace punto a punto proporciona soluciones de conectividad para empresas con centros de trabajo múltiples que necesiten de una gran coordinación y trabajo compartido. Este enlace proporciona a la empresa un entorno de intercambio de información con un coste periódico de cero. Es el complemento exterior perfecto a una instalación interior de red local estándar o inalámbrica.

Efectivamente, todos los centros conectados por el enlace punto a punto formarán parte de una única red local, exactamente como si estuvieran en el mismo edificio, pero con la flexibilidad que proporciona la distribución multicentro, imprescindible en el entorno empresarial cambiante de hoy en día.

Gracias a la potente antena de emisión / recepción con un alcance extendido; pueden unirse mediante el enlace punto a punto centros situados hasta a 15 kilómetros. Esto nos proporciona los beneficios que supone compartir una red local con una velocidad de transferencia de 10 megabytes por segundo, sin ninguno de los costes ni problemas asociados a una interconexión estándar, que pueden ser la diferencia entre una instalación eficiente y con beneficios y una instalación caótica y en números desordenados.

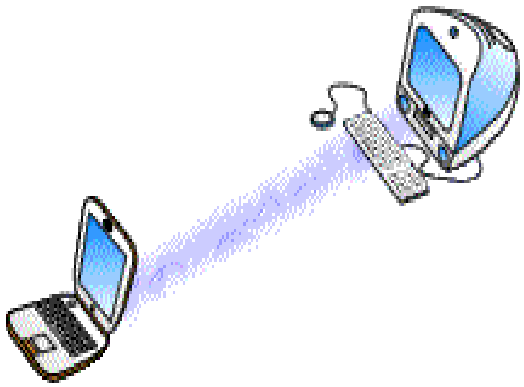


Figura 1.1 Ejemplo de conexión punto a punto

1.3.2 CONEXIÓN PUNTO A MULTIPUNTO

El enlace punto a multipunto es la versión del punto a punto para la conexión rápida y fiable de más de dos instalaciones.

Para reducir costes, este sistema consta de una instalación central dotada de una antena multidireccional, a la que apuntan las antenas direccionales del resto de centros. Esto nos da una capacidad igual a la del punto a punto, pero extensible hasta a 16 centros (incluso con instalaciones replicadas).

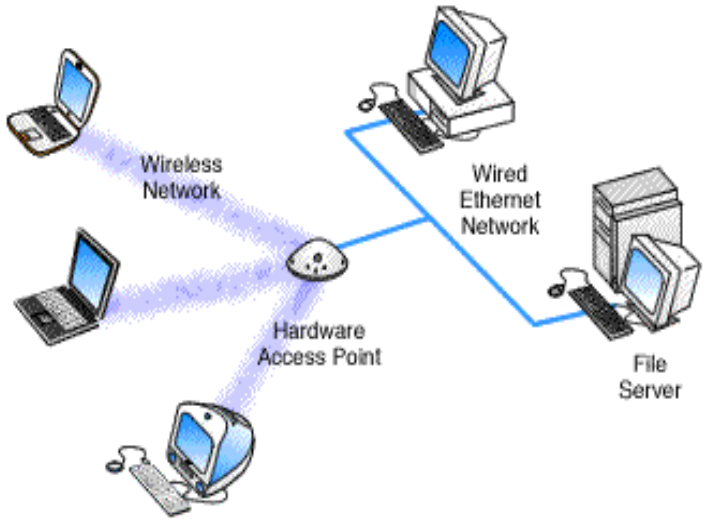


Figura 1.2 Ejemplo de conexión punto a multipunto

1.4 HARDWARE RECOMENDADO

Debemos recordar que el término “Inalámbrico” que ya de por sí es nuevo, puede usarse para incentivar a un usuario, que al saber que no depende de cables para trabajar, puede incrementar su productividad. Con los últimos productos de LAN que operan con ondas de Radio esto es más sencillo.

Para la elección de los productos inalámbricos se deben de considerar ciertos detalles como: costo, rendimiento y facilidad de uso. Aunque los sistemas inalámbricos no son tan veloces si son fáciles de instalar. Usando los puntos de acceso o los adaptadores inalámbricos que se instalan en un servidor, los usuarios pueden comunicarse con las redes alambradas existentes. Todos los productos exponen buenos resultados, de 400 pies (122 mts) a más de 1.000 pies (305 m) sin perder conexión en la prueba de distancia en exteriores.

1.4.1 MARCAS RECOMENDADAS

A continuación se presenta los diferentes tipos de marcas existentes en el mercado de las redes inalámbricas:

IMAGEN	MARCA	DESCRIPCIÓN
 Punto de Acceso	WIFI	Es un punto de acceso de 54 Mbits para redes inalámbricas que permite enlazar los dispositivos inalámbricos con la red cableada tradicional.
 Adaptador Tarjeta de Red Inalámbrica	D-LINK	La tarjeta **DWL-G650** es un adaptador PCMCIA que le permitirá disponer rápidamente de una red inalámbrica en su ordenador portátil. Son equivalentes a una tarjeta de red normal, sólo que sin cables.
 Tarjeta de Red Inalámbrica	LINKSYS	Es una tarjeta PCI inalámbrica **G WMP54G-FR** que soporta velocidades de hasta 54 Mbit/s y es compatible con la mayoría de los ordenadores de sobremesa
 Antena Omnidereccional	TRENDNET	-Potencia: 100 Watts -Frecuencia:2400-2500MHz - Impedancia: 50 Ohms - Ganancia: 15 dBi - VSRW:1:1.5 max - Conector: N Hembra - W.Survival: >150 MHP - Polarización: Vertical - Dimensiones: 1,52 mts - Peso: 1,160 kgs
	TRENDNET	Características: -Potencia: 50 Watts -Frecuencia:2400-500MHz - Impedancia: 50 Ohms - VSWR: < 1.5:1 avg. avg - Ganancia: 19 dBi - Conector: N Hembra - Polarización: Vertical u horizontal - Dimensiones: 16,7 x 23,5 pulgadas

 Antena Direccional		- Peso: 3,9 libras - Color: blanco
 Cables para Antenas Inalámbricas	NETGEAR	Cable de 3 metros HDF-400 con conectores tipo N cable de prolongación de 9 metros para antena wireless, conectores N macho a N hembra.

Tabla 1.1 Marcas Recomendadas

1.4.2 AMPLIFICADORES

A continuación se presenta los tipos de amplificadores más recomendados para la implementación de una red inalámbrica:

IMAGEN	MARCA	DESCRIPCIÓN
 Amplificador Bi-direccional de RF 2.4 Ghz. 1 Watt. - Para exteriores.	SMARTAMP	- Rango de operación: 2.4 - 2.5 Ghz. - Modo de operación: Bi-direccional. - Respuesta en frecuencia: ± 1 dB - Temp. de operación: -40 a +70 °C - Potencia de salida: 1 Watt. (+30 dBm) - Excitación: +23 dBm max. - Ganancia en recepción: 16 db. - Ruido: 3.5 db. - Conectores: "N" Hembra - 50 Ohms. - Protección c/descargas: 1/4 onda. - TX: 1.2 Amp.

 Amplificador Bi-direccional de 5.8 Ghz. 1 Watt. – Uso exteriores.	SMARTAMP	- Rango de operación: 5.7 - 5.8 Ghz. - Modo de operación: Bi-direccional. -TTD - Respuesta en frecuencia: ± 1 dB - Temp. de operación: -30 a +70 °C - Potencia de salida: 1 Watt. (+30 dBm) - Excitación: 1 mW a 100 mW.max. - Ganancia en recepción: 16 db. - Ruido: 3.5 db. - Conectores: "N" Hembra - 50 Ohms. - Protección c/descargas: 1/4 onda. - Consumo sobre 12 VDC.: RX 600 mA. - TX: 4 Amp.
 Amplificador Bi-direccional Uso Exteriores/Interiores 802.11g 250 mW.	SMARTAMP	- Rango de operación: 2.4 - 2.5 Ghz. - Modo de operación: Bi-direccional. TTD - Respuesta en frecuencia: ± 1 dB - Temp. de operación: -40 a +70 °C - Potencia de salida: 250 mW. (+24 dBm) - Excitación: +7 dBm max. - Ganancia en recepción: 16 db. - Ruido: 3.5 db. - Conectores: "N" Hembra - 50 Ohms. - Protección c/descargas: 1/4 onda. - Consumo sobre 9 v. DC.: RX 130 mA. - TX: 900 mA.

Tabla 1.2 Amplificadores

1.5 TOPOLOGÍA EN REDES INALÁMBRICAS DE DATOS FIJAS

Las redes inalámbricas se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y ad hoc. Para nuestro caso utilizaremos los términos “infraestructura” y “ad hoc”. Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

1.5.1 TOPOLOGÍA DE INFRAESTRUCTURA

Es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

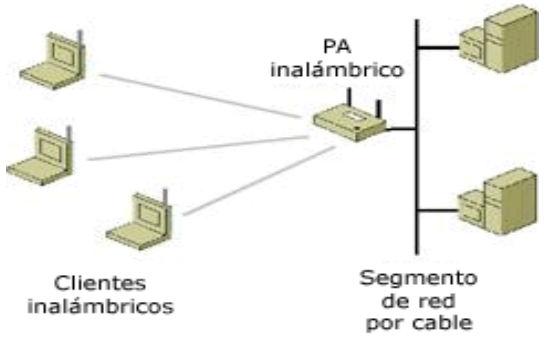


Figura 1.3 Red inalámbrica en modo de infraestructura

DESCRIPCIÓN GENERAL DEL FUNCIONAMIENTO DE LA MODALIDAD DE INFRAESTRUCTURA

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico

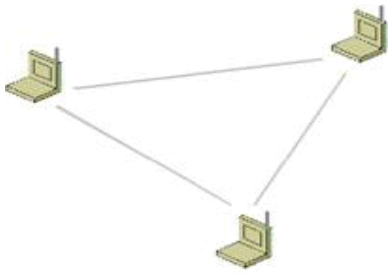
después de que la red esté despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representan la parte del protocolo que evita las colisiones. Observe que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso. Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

1.5.2 TOPOLOGÍA AD HOC

En esta topología los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.



Clientes inalámbricos

Figura 1.4 Red inalámbrica en modo ad hoc

DESCRIPCIÓN GENERAL DEL FUNCIONAMIENTO DE LA MODALIDAD AD HOC

Después de explicar el funcionamiento básico de la modalidad de infraestructura, del modo ad hoc se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

1.6 ESTÁNDARES DE LAS REDES INALÁMBRICAS DE DATOS FIJAS

Las redes inalámbricas se han extendido rápida y ampliamente a pesar de la recesión en la economía de las telecomunicaciones. En sus inicios, las aplicaciones fueron limitadas a industrias y grandes almacenes. Hoy en día, las redes inalámbricas son instaladas en universidades, oficinas, hogares y hasta en espacios públicos.

Otra atracción importante de los productos inalámbricos es la interoperatibilidad. Gracias al desarrollo de estándares, pueden mezclarse dispositivos inalámbricos de diversos fabricantes haciendo un acceso más directo y transparente con la tecnología.

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE (Institute of Electrical and Electronics Engineers) y la ETSI (European Telecommunications Standards Institute). Una vez desarrollados se convierten en la base de los fabricantes para desarrollar sus productos.

Entre los principales estándares se encuentran:

- **IEEE 802.11**: Es el estándar original de las WLANs que soporta velocidades entre 1 y 2 Mbps.
- **IEEE 802.11a**: Es un estándar de alta velocidad que soporta velocidades de hasta 54 Mbps en la banda de 5 GHz.
- **IEEE 802.11b**: Es un estándar dominante de WLAN (conocido también como Wi-Fi) que soporta velocidades de hasta 11 Mbps en la banda de 2.4 GHz.

- **IEEE 802.11g**: Estándar compatible con el 802.11b capaz de alcanzar velocidades de hasta 54 Mbps en la banda de 2.4 GHz.
- **HiperLAN2**: Estándar que compite con IEEE 802.11a al soportar velocidades de hasta 54 Mbps en la banda de 5 GHz.
- **HomeRF**: Estándar que compite con el IEEE 802.11b que soporta velocidades de hasta 10 Mbps en la banda de 2.4 GHz.

Estándar	Velocidad máxima	Interfase de aire	Ancho de banda de canal	Frecuencia	Disponibilidad
IEEE 802.11b	11 Mbps	DSSS	25 MHz	2.4 GHz	Ahora
IEEE 802.11a	54 Mbps	OFDM	25 MHz	5.0 GHz	Ahora
IEEE 802.11g	54 Mbps	OFDM/DSSS	25 MHz	2.4 GHz	Finales 2002
HomeRF2	10 Mbps	FHSS	5 MHz	2.4 GHz	Ahora
HiperLAN2	54 Mbps	OFDM	25 MHz	5.0 GHz	2003
5-UP	108 Mbps	OFDM	50 MHz	5.0 GHz	2003

Tabla 1.3: Principales Estándares de las Redes Inalámbricas

DSSS: Direct Sequence Spread Spectrum
OFDM: Orthogonal Frequency Division Multiplexing
FHSS: Frequency Hopping Spread Spectrum
5-UP: Protocolo Unificado de 5 GHz propuesto por Atheros Communications

El gran éxito de las WLANs es que utilizan frecuencias de uso libre, es decir no es necesario pedir autorización o algún permiso para utilizarlas. Aunque hay que tener en mente, que la normatividad acerca de la administración del espectro varia de país a país. La desventaja de utilizar este tipo de bandas de frecuencias es que las comunicaciones son propensas a interferencias y errores de transmisión. Para reducir estos errores, el 802.11a y el 802.11b automáticamente reducen la velocidad de información de la capa física. Así por ejemplo, el 802.11b tiene tres velocidades de información (5.5, 2 y 1 Mbps) y el 802.11a tiene siete (48, 36, 24, 18, 12, 9 y 6 Mbps).

La transmisión a mayor velocidad del 802.11a no es la única ventaja con respecto al 802.11b. También utiliza un intervalo de frecuencia más alto de 5 GHz. Esta banda es más ancha y menos saturada que la banda de 2.4 GHz que el 802.11b comparte con teléfonos inalámbricos, hornos de microondas, etc. Una banda más ancha significa que más canales de radio pueden coexistir sin interferencia. Si bien, la banda de 5 GHz tiene muchas ventajas, también tiene sus problemas. Las

diferentes frecuencias que utilizan ambos sistemas significan que los productos basados en 802.11a son no interoperables con los 802.11b. Esto significa que aunque no se interfieran entre sí, por estar en diferentes bandas de frecuencias, los dispositivos no pueden comunicarse entre ellos. Para evitar esto, la IEEE desarrolló un nuevo estándar conocido como 802.11g, el cual extenderá la velocidad y el intervalo de frecuencias del 802.11b para así hacerlo totalmente compatible con los sistemas anteriores. Sin embargo, no será más rápido que el estándar 802.11a.

Como otro intento de permitir la interoperatibilidad entre los dispositivos de bajas y altas velocidades, la compañía Atheros Comunications propuso unas mejoras a los estándares de WLANs de la IEEE y la ETSI. Este nuevo estándar conocido como 5-UP (5 GHz Unified Protocol) permitirá la comunicación entre dispositivos mediante un protocolo unificado a velocidades de hasta 108 Mbps.

Ambas especificaciones, la 802.11a (IEEE) y la HiperLAN2 (ETSI) son para WLANs de alta velocidad que operan en el intervalo de frecuencias de 5.15 a 5.35 GHz. El radioespectro asignado para el 802.11a y el HiperLAN2 es dividido en 8 segmentos o canales de 20 MHz cada uno. Cada canal soporta un cierto número de dispositivos individuales pueden transitar a través de segmentos de red como si fueran teléfonos móviles de una estación a otra. Este espectro de 20 MHz para un segmento de red soporta 54 Mbps de caudal eficaz compartido entre los dispositivos en el segmento en un tiempo dado.

Además de las mencionadas existen otras tecnologías que detallamos a continuación:

HomeRF, otra tecnología más de WLANs

HomeRF es otra organización que ha desarrollado sus propios estándares para entrar de lleno al mundo de las redes inalámbricas. HomeRF ha sido desarrollado por el grupo de trabajo Home Radio Frequency, el cual está conformado por más de 50 compañías lideres en el ámbito mundial en las áreas de redes, periféricos, comunicaciones, software, semiconductores, etc. Este grupo fue fundado en marzo de 1988 para promover de manera masiva dispositivos de voz, datos y video alrededor de los hogares de manera inalámbrica. HomeRF es la tecnología que compite directamente con los productos de la IEEE 802.11b. La velocidad máxima de HomeRF es 10 Mbps, ideal para las aplicaciones caseras, aunque se manejan otras velocidades de 5, 1.6 y 0.8 Mbps. Según el grupo de trabajo, HomeRF ofrece más seguridad, los dispositivos consumen menos potencia que los productos de las tecnologías competidoras, además de permitir aplicaciones para telefonía y video.

Bluetooth

La tecnología inalámbrica Bluetooth es un estándar global abierto para enlaces de radio, que ofrece conexiones inalámbricas económicas entre computadoras portátiles, dispositivos de mano, teléfonos celulares y varios aparatos más; así como acceso a otros recursos en la red. La especificación Bluetooth define un enlace de radio de baja potencia, optimizado para conexiones

seguras de corto alcance a velocidades de transmisión de datos de 1 Mbps, y define los pasos estándares para la conexión de varios aparatos. Los radios Bluetooth, que pueden ser incorporados en la mayoría de los aparatos electrónicos, ofrecen un enlace inalámbrico de comunicación universal que facilita una interoperabilidad confiable entre dispositivos de diferentes fabricantes.

Los principales objetivos que se pretende conseguir con esta tecnología son:

- Facilitar las comunicaciones entre equipos móviles y fijos
- Eliminar cables y conectores entre éstos
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

Las soluciones a las redes inalámbricas están disponibles hoy en día y es sólo el principio de una tendencia creciente. El estándar 802.11a, HiperLAN2 así como el 802.11g prometen un gran ancho de banda para permitir un sinfín de nuevas aplicaciones. Aunque todavía existen varios obstáculos que hay que vencer como la seguridad e interferencia, las redes inalámbricas ofrecen por lo pronto una comunicación eficiente tanto en interiores como exteriores. Cuando se evalúa una solución inalámbrica que satisfaga nuestras necesidades de comunicación es muy importante tener en cuenta los estándares y tecnologías de más penetración. Esta sabia decisión ahorrará dinero, tiempo y problemas de incompatibilidad y nos brindará comunicación rápida, eficiente y transparente.

1.7 PROTOCOLOS DE REDES INALÁMBRICAS DE DATOS FIJAS

1.7.1 PROTOCOLO IP

Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes. Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes (llamados *datagramas IP*) que tiene las siguientes características:

- Es **no orientado a conexión** debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.
- Es **no fiable** porque los paquetes pueden perderse, dañarse o llegar retrasados.

Formato del datagrama IP

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas de las distintas redes que va atravesando. Cada vez que un datagrama tiene que atravesar un router, el datagrama *saldrá* de la trama física de la red que abandona y se *acomodará* en el campo de datos de una trama física de la siguiente red. Este

mecanismo permite que un mismo datagrama IP pueda atravesar distintas redes. El propio datagrama IP tiene también un campo de datos será aquí donde viajen los paquetes de las capas superiores.

1.7.2 PROTOCOLO TCP

El protocolo TCP (Protocolo de Control de Transmisión) está basado en IP que es no fiable y no orientado a conexión. Este protocolo permite una comunicación fiable entre dos aplicaciones. De esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información dan por hecho que todo lo que reciben es correcto.

El protocolo TCP envía un *flujo de información no estructurado*. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra.

Formato del segmento TCP

Ya hemos comentado que el flujo de bytes que produce una determinada aplicación se divide en uno o más segmentos TCP para su transmisión. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Para facilitar el control de flujo de la información los bytes de la aplicación se numeran. De esta manera, cada segmento indica en su cabecera el primer byte que transporta. Las confirmaciones o acuses de recibo (ACK) representan el siguiente byte que se espera recibir (y no el número de segmento recibido, ya que éste no existe).

1.7.3 PROTOCOLO ICMP

El protocolo ICMP (Protocolo de Mensajes de Control y Error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Los mensajes ICMP viajan en el campo de datos de un datagrama IP. Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará.

Los mensajes de solicitud y respuesta se utilizan para comprobar si existe comunicación entre 2 hosts a nivel de la capa de red. Estos mensajes comprueban que las capas física, acceso al medio y red estén correctos. Sin embargo, no dicen nada de las capas de transporte y de aplicación las cuales podrían estar mal configuradas; por ejemplo, la recepción de mensajes de correo electrónico puede fallar aunque exista comunicación IP con el servidor de correo.

1.7.4 PROTOCOLO UDP

El protocolo UDP (Protocolo de Datagramas de Usuario) proporciona una comunicación muy sencilla entre las aplicaciones de dos ordenadores. Al igual que el protocolo IP, UDP es:

- **No orientado a conexión:** No se establece una conexión previa con el otro extremo para transmitir un mensaje UDP. Los mensajes se envían sin más y éstos pueden duplicarse o llegar desordenados al destino.
- **No fiable:** Los mensajes UDP se pueden perder o llegar dañados.

UDP utiliza el protocolo IP para transportar sus mensajes. Como vemos, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta.

1.7.5 PROTOCOLO CSMA/CA

En redes informáticas, CSMA/CA (Detección de Portadora con Detección de Colisiones) es un protocolo de control de redes utilizado para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuenta con un modo práctico para transmitir y recibir simultáneamente). Es un método de acceso de red en el cual cada dispositivo señala su intento para transmitir antes de que lo haga realmente. Esto evita que otros dispositivos envíen la información, así evitando que las colisiones ocurran entre las señales a partir de dos o más dispositivos. De esta forma permite a un emisor transmitir en cualquier momento en que el medio no esté ocupado.

Este protocolo impone a una estación que desee transmitir que previamente escuche el medio para detectar si otro emisor está realizando esta función. Si es así, esperará un tiempo aleatorio para sondear de nuevo el medio. Cuando detecte que el medio está libre, emitirá una solicitud de ocupación que será escuchada por el sistema que gestione los permisos (el punto de acceso). Si se le concede el acceso, podrá realizar la emisión. De esta forma también se evita un conocido problema denominado del “nodo oculto”, donde dos nodos dentro de una celda gobernada por un punto de acceso tienen cobertura suficiente para acceder a él, pero están entre sí lo suficientemente alejados para no detectar sus respectivas peticiones disminuyendo así la posibilidad de colisiones.

1.8 VENTAJAS DE UNA RED INALÁMBRICA DE DATOS FIJA SOBRE UNA RED NORMAL

En la actualidad, prácticamente todas las empresas necesitan de una red de comunicación, por lo tanto parece sencillo comprender que si esta comunicación se realiza sin una conexión física, esto hará que compartir información sea mucho más cómodo y además nos permita una mayor movilidad de los equipos. Esta movilidad se observa claramente cuando se desea cambiar la colocación de los equipos en una oficina conectada a una red por medio de cables. Este cambio provocaría tener que redistribuir la colocación de los cables en dicha oficina. Sin embargo con una red inalámbrica este trabajo no sería necesario realizarlo.

A continuación se analizarán en detalle los aspectos en las que las redes inalámbricas aventajan a las redes cableadas:

- **Costo de propiedad reducido:** Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que en una red cableada, la inversión de toda la instalación y el costo durante el ciclo de vida puede ser significativamente inferior. Los beneficios a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

- **Poca planificación:** Con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.
- **Rapidez de implantación:** Por lo general la tarea que suele consumir mayor tiempo en la instalación de una red inalámbrica es paradójicamente la parte cableada que se emplea para enlazar los puntos de acceso con la red local de la empresa. Aún así se mide en días la duración de este proyecto, siempre dependiendo de su extensión. En cambio con las redes cableadas, no son días sino habitualmente semanas. Esto resulta en muchos casos un factor decisivo para trabajar con redes inalámbricas.
- **Movilidad:** Es evidente que este es el punto fuerte de las redes inalámbricas, inalcanzable para las cableadas. Es especialmente interesante para cubrir salas de reunión, laboratorios, centros de alta itinerancia, donde haya portátiles y en general para facilitar reuniones de trabajo en cualquier punto proporcionando a los usuarios acceso a la información en tiempo real en cualquier lugar dentro de la organización o el entorno público (zona limitada) en el que están desplegadas.
- **Estética:** Las instalaciones de redes locales se caracterizan por la existencia de infinidad de cajas de conexiones próximas a cada puesto de trabajo, canalizaciones generalmente visibles y cables desde los PCs hasta el punto de conexión más próximo. Todo ello y debido a la mayor densidad de equipos, impacta de forma muy negativa en la estética del entorno de trabajo. Como contrapartida, en una instalación inalámbrica desaparecen los cables de los PCs y cajas de conexiones, así como se reducen al mínimo las canalizaciones visibles. Este factor, siempre bien valorado, en ocasiones se convierte en fundamental, decidiendo la tecnología de red a implantar.
- **Provisionalidad:** Las redes inalámbricas tienen una gran utilidad en instalaciones que tienen carácter de provisionalidad. Ejemplos de ello son infraestructuras itinerantes (ferias, congresos, demostradores), despliegues cortos o limitados en el tiempo (oficinas temporales). Las redes inalámbricas pueden soportar un número elevado de usuarios transitorios, mientras que las tradicionales están limitadas a las conexiones ya cableadas.
- **Diseño:** Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.
- **Robustez:** Las redes basadas en cableado estructurado son por lo general más robustas frente a interferencias y condiciones adversas que las inalámbricas. Sin embargo en ciertos entornos en fábricas con elevada humedad, agentes químicos agresivos, calor, etc. las instalaciones cableadas pueden sufrir una rápida degradación o ser inviables. Una instalación inalámbrica adecuadamente ubicada para resguardarse de dichas inclemencias puede ser la alternativa idónea y eficaz.
- **Escalabilidad:** los sistemas de redes inalámbricas pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las

configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red.

Las redes inalámbricas también están implantándose en la industria y alcanzando grandes éxitos en los siguientes campos:

- **Corporaciones:** Con el uso de las redes inalámbricas los empleados pueden beneficiarse de una red móvil para el correo electrónico, compartición de ficheros y visualización de web's, independientemente de dónde se encuentren en la oficina.
- **Educación:** Las instituciones académicas que permiten este tipo de conexión permiten a los usuarios la utilización de ordenadores para conectarse a la red para realizar tutorías con profesores, intercambio de materiales entre los alumnos, etc.
- **Finanzas:** Mediante un PC portable y un adaptador a la red inalámbrica, los representantes pueden recibir información desde una base de datos en tiempo real y mejorar la velocidad y calidad de los negocios.
- **Manufacturación**: Las redes inalámbricas ayudan al enlace entre las estaciones de trabajo de los pisos de la fábrica con los dispositivos de adquisición de datos de la red de la compañía.
- **Almacenes:** En los almacenes de ventas al por menor una red inalámbrica se puede usar para actualizar temporalmente registros para eventos especiales.

CAPITULO II

2.1 TIPO DE ATAQUES

De la misma manera como existen un sin número de aplicaciones que permiten el total funcionamiento de los dispositivos inalámbricos, existe una gran cantidad de personas maliciosas que se preocupan únicamente por probar su influencia al tratar de violar la seguridad de la información. Es justo en este momento cuando surgen los diferentes ataques para este cometido.

Dentro de las redes inalámbricas se pueden identificar los siguientes tipos de ataques:

- **Espionaje**

Consiste en observar el entorno al que pertenece la red y para esto no se necesita ningún tipo de “Hardware” o “Software” especial.

Que Observar	Localización
Antenas	muros, techos, tejidos, pasillos, ventanas, entradas
Puntos de Acceso	muros, techos falsos
Cables de Red	atraviesan techos, muros, paredes
Dispositivos-scanners/PDAs	personal de la empresa

Tabla 2.1: Entorno de Espionaje

- **Interceptar una señal**

El atacante intenta identificar el origen y el destino que posee la información. Tras haber interceptado la señal, el atacante intentará recopilar información sensible del sistema.

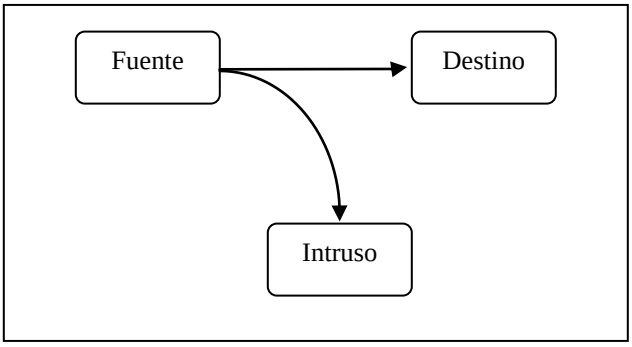


FIGURA 2.1: INTERCEPTACIÓN DE UNA SEÑAL

- **Suplantar una fuente real**

Esta técnica de ataque se engloba dentro de los ataques activos, donde un intruso pretende ser la fuente real u original.

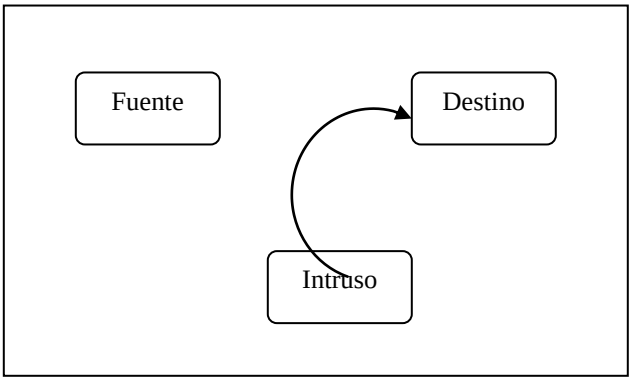


FIGURA 2.2: SUPLANTACIÓN DE UNA FUENTE REAL

- **“Sniffing” y “eavesdropping” (escuchas - interceptación)**

El programa monitoriza los datos y determina hacia donde van, de donde vienen y qué son y consiste en alterar la configuración de un ordenador para que acceda a todos los datos que pasen por él, aunque no estén destinados a dicho ordenador, capturando o enviando al atacante aquellos que resulten de interés. Los datos objeto de fisgoneo suelen ser principalmente datos de acceso a sistemas (nombres de usuario y contraseñas) y datos financieros (información de tarjetas de crédito o números de cuentas bancarias).

- **“Spoofing” (burla) y “hijacking” (secuestro)**

Consiste en utilizar una clave de acceso válida obtenida en un ataque de monitorización para acceder al sistema suplantando a un usuario y realizar acciones en nombre de dicho usuario. Existe una variedad de este ataque denominada “looping” en la que el atacante encadena accesos falsos en varios sistemas, para hacer más difícil su localización. En cambio “hijacking” asocia una dirección IP válida del sistema atacado.

- **Denegación de Servicio (DoS) o ataques por inundación (flooding attacks)**

La denegación de servicio sucede cuando un atacante intenta ocupar la mayoría de los recursos disponibles de una red inalámbrica lo cual impide a los usuarios legítimos de esta disponer de dichos servicios o recursos.

2.2 ATAQUES A LOS PROTOCOLOS Y PUERTOS

2.2.1 SPAM (CORREO ELECTRÓNICO NO DESEADO)

SPAM es la palabra que se utiliza para calificar al **correo no solicitado** enviado por Internet. La mayor razón para ser indeseable es que la mayoría de las personas conectadas a Internet no gozan de una conexión que no les cueste, y adicionalmente reciben un cobro por uso del buzón. Por lo tanto el envío indiscriminado de este tipo de correo ocasiona costos al lector y más aún cuando el recibo de correo se hace por medio de la red el costo es tanto en la conexión como en el uso de la red misma.

Algunas buenas prácticas personales pueden aplicarse para prevenir el spam.

1. Utilice una dirección de correo pública (gratuita) para suscribirse a todos aquellos productos, concursos, o para dar a conocer en grupos de interés y de noticias. De esta manera mantendrá privada su dirección primaria de correo Electrónico.

2. No participe en cadenas de correo por más noble que la causa aparente ser.

Por supuesto estas 2 medidas no serán suficientes contra el flagelo del Spam, ya que cada día los spammers (encargado de enviar el correo SPAM) son más creativos en la forma de conseguir direcciones.

Tipos de detección de SPAM

Los productos para servidor tienen varias formas de detectar el SPAM.

1. Detección por lista negra: Las listas negras son bases de datos que contienen las direcciones IP de spammers identificados utilizado por proveedores de servicio de Internet y redes corporativas de todo el mundo, gracias a las cuales los administradores pueden comprobar si un servidor de e-mail entrante se utiliza habitualmente para el envío de spam.

2. Listas Blancas: Una solución más sofisticada e ingeniosa es permitir que se reciba correo sólo de tus colegas o personas que están en tu directorio, es decir, crear una lista blanca. El resto de las personas reciben un email explicando que su correo ha sido filtrado e invitándoles a que vuelvan a enviarlo pero incluyendo una palabra "secreta".

2.2.2 LOS HACKERS DE REDES INALÁMBRICAS

Con frecuencia la señal inalámbrica no se queda entre las cuatro paredes de la oficina, sino que puede ser detectada, utilizada y/o explotada por aquellos atacantes conocidos como hackers de redes inalámbricas (War Drivers) y hackers de señales inalámbricas (War Chalkers). Con la ayuda de un equipo sencillo y un software "rastreador" de los puntos de acceso inalámbrico que está listo para su descarga de Internet, estos individuos recorrerán ciudades y pueblos en busca de puntos inseguros de acceso inalámbrico.

Los hackers de redes inalámbricas tienen mucha práctica y han dedicado muchos sitios Web y carteleras de anuncios para mejorar sus actividades y compartir sus ideas. Los hackers de redes inalámbricas consiguen la ayuda del equipo más sofisticado, como antenas que ayudan a recoger las señales y receptores del Sistema de Posicionamiento Global (GPS) que se utilizan para obtener las coordenadas exactas (longitud y latitud) de un punto de acceso inalámbrico detectado con fines de mapeo.

Otro creciente fenómeno es el ataque a señales inalámbricas (War Chalking), derivado de la práctica de los vagabundos que consiste en señalar los hogares y empresas amigables marcando sus aceras y cercas. En el caso del ataque a señales inalámbricas, se pintan los símbolos en el edificio o en el pavimento para indicar que hay un punto de acceso para que otros puedan aprovechar la señal. Siempre existe el peligro de que estos grupos clandestinos puedan detectar y vulnerar los puntos de acceso desprotegidos de su empresa.

Si un hacker de redes inalámbricas (War Driver) intercepta la red inalámbrica de una empresa, la pone en grave peligro. Un punto de acceso abierto puede exponer toda la red a la actividad de los hackers. El problema no es únicamente la destrucción que pueden ocasionar a una red empresarial,

sino también el gran potencial del robo de información. Con el software adecuado, un hacker sería capaz de ver los contenidos de todo el tráfico de la red incluyendo detalles específicos como los nombres de usuario y de archivo.

2.3 ESTANDARES DE SEGURIDAD INALAMBRICA

La seguridad es un aspecto que cobra especial relevancia cuando hablamos de redes inalámbricas, debido a la naturaleza del medio de transmisión “el aire”. Las características de seguridad se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlando el ingreso a la red y protegiendo al sistema de administración de accesos no autorizado.

Ante la existencia de dispositivos WLAN de diferentes fabricantes, se hizo necesaria la presencia de recomendaciones contenidas en los estándares, para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades.

802.11 es una familia de especificaciones para redes inalámbricas de área local (WLANs) desarrolladas por un grupo de trabajo del instituto de ingenieros eléctricos y electrónicos (IEEE) el cual aprobó los siguientes estándares: **802.11** es el estándar original de las WLANs que soporta velocidades entre 1 y 2 Mbps, **802.11a** define la operación en la banda de los 5 GHz con velocidades de hasta 54 Mbps, **802.11b** opera en la banda de los 2.4 GHz con velocidades de hasta 11 Mbps, y el estándar **802.11g** funciona en la misma banda de frecuencia del 802.11b pero con velocidades de transmisión de datos del estándar 802.11a.

Para seguridad en redes inalámbricas también existen una multitud de estándares definidos o en proceso de definición que es necesario dar a conocer para una correcta interpretación de seguridad en la información los cuales detallamos a continuación:

- **802.11c** Estándar que define las características que necesitan los APs para actuar como puentes (bridges). Ya está aprobado y se implementa en algunos productos.
- **802.11d** Estándar que permite el uso de la comunicación mediante el protocolo 802.11 en países que tienen restricciones sobre el uso de las frecuencias que éste es capaz de utilizar. De esta forma se puede usar en cualquier parte del mundo.
- **802.11e** Estándar sobre la introducción de calidad de servicio (QoS) en la comunicación entre Puntos de Acceso(APs) y Tarjetas de Red(TR). Actúa como árbitro de la comunicación, esto

permitirá el envío de vídeo y de voz sobre IP. Esta especificación, que está haciendo el IEEE será aplicable tanto a 802.11b como a 802.11a.

- **802.11f** Estándar que define una práctica recomendada de uso sobre el intercambio de información entre el AP y TR en el momento del registro a la red y la información que intercambian los APs para permitir la interportabilidad. La adopción de esta práctica permitirá el Roamming entre diferentes redes, básicamente esta especificación funciona bajo el estándar 802.11g y se aplica a la intercomunicación entre APs de distintos fabricantes.
- **802.11h** Estándar que sobrepasa al 802.11a al permitir la asignación dinámica de canales para permitir la coexistencia de éste con el HyperLAN. Además define el TCP (Protocolo de Control de Transmisión) según el cual la potencia de transmisión se adecúa a la distancia a la que se encuentra el destinatario de la comunicación.
- **802.11i** Estándar de seguridad para redes 802.11 que surgió a raíz de las vulnerabilidades 802.11b y será aplicable a redes 802.11a (54Mbps), 802.11b (11Mbps) y 802.11g (22Mbps). Define la encriptación y la autentificación para complementar, completar y mejorar al WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Protocolo de integridad de clave temporal (TKIP), ofrece una solución interoperable y un patrón robusto para asegurar datos.
- **802.11j** Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.
- **802.11m** Propuesto para mantenimiento de redes inalámbricas.

2.4 PROTOCOLOS Y PUERTOS

2.4.1 PROTOCOLOS

Para considerarse una red inalámbrica como segura se debe requerir de ciertos métodos que logren un nivel diferente de seguridad alcanzando así la confidencialidad y autenticidad de la información.

WEP (PROTOCOLO EQUIVALENTE AL CABLE)

Es un sistema de encriptación estándar propuesto por el comité 802.11, fue diseñado con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado y su objetivo principal es proporcionar confidencialidad, autentificación y control de acceso en redes inalámbricas.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de la red. Esto genera varios

inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea complicada. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

El algoritmo WEP cifra de la siguiente manera:

- A la trama se le computa un código de integridad (ICV) mediante el algoritmo CRC-32. Dicho código de integridad se concatena con la trama, y es empleado más tarde por el receptor para comprobar si la trama ha sido alterada durante el transporte.
- Se escoge una clave secreta compartida entre emisor y receptor. Esta clave puede poseer 40 ó 128 bits.
- Si se empleara siempre la misma clave secreta para cifrar todas las tramas, dos tramas iguales producirían tramas cifradas similares.

Para evitar esta eventualidad, se concatena la clave secreta con un número aleatorio llamado vector de inicialización (IV) de 24 bits, el cual se cambia con cada trama.

- La concatenación de la clave secreta y el vector de inicialización (conocida como semilla) se emplea como entrada de un generador RC4 de números seudo- aleatorios. El generador RC4 es capaz de generar una secuencia seudo-aleatoria (o cifra de flujo) tan larga como se desee a partir de la semilla.
- El generador RC4 genera una cifra de flujo, del mismo tamaño de la trama a cifrar más 32 bits (para cubrir la longitud de la trama y el código de integridad).
- Se hace un XOR bit por bit de la trama con la secuencia de clave, obteniéndose como resultado la trama cifrada.
- El vector de inicialización y la trama se transmiten juntos.

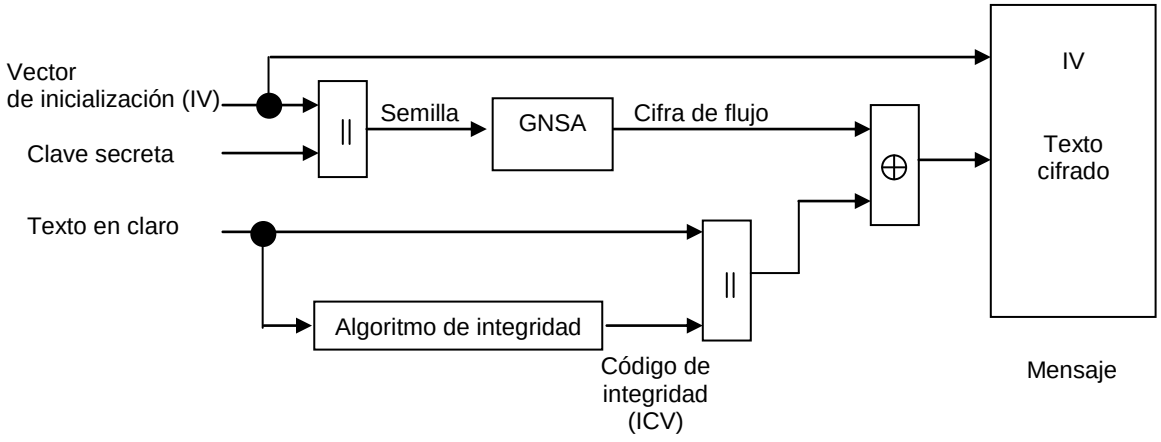


Figura 2.3: Funcionamiento del algoritmo WEP en modalidad de cifrado.

En el receptor se lleva a cabo el proceso de descifrado:

- Se emplean el vector de inicialización recibido y la clave secreta compartida para generar la semilla que se utilizó en el transmisor.
- Un generador RC4 produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será idéntica a la usada en la transmisión.
- Se efectúa un XOR bit por bit de la cifra de flujo y la trama cifrado, obteniéndose de esta manera la trama y el código de integridad.
- A la trama se le aplica el algoritmo CRC-32 para obtener un segundo código de integridad, que se compara con el recibido.
- Si los dos códigos de integridad son iguales, la trama se acepta; en caso contrario se rechaza.

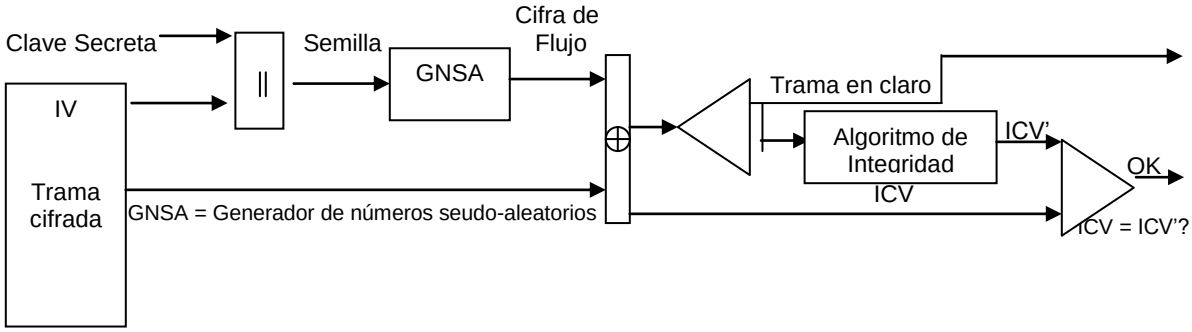


Figura 2.4: Funcionamiento del algoritmo WEP en modalidad de descifrado.

En definitiva el protocolo WEP es un leve intento al tratar de generar una privacidad y seguridad de los datos que se transmiten de manera inalámbrica, establecida por el IEEE en el 802.11; y como idea principal, la seguridad es directamente proporcional a la eficiencia que adopte el administrador de la red; lastimosamente, la carga administrativa y de gestión que se debe asumir al emplear este protocolo, es exagerada; por consiguiente es de notar, que el protocolo WEP, no debe ser la única herramienta para asegurar la confidencialidad, integridad y demás características de seguridad.

WPA (ACCESO PROTEGIDO WI-FI)

El protocolo WPA tiene varios objetivos de diseño, como son robustez, interoperabilidad, sustituir al WEP en cuestiones de seguridad, ser actualizable mediante software en los productos existentes con el certificado Wi-Fi, ser aplicable tanto para hogares como para grandes empresas y estar disponible inmediatamente.

Para conseguir estos objetivos, es necesario realizar dos mejoras primarias de la seguridad. WPA está construido para proveer una encriptación de datos mejorada, la cual era débil en WEP, y proveer autenticación de usuarios que estaba muy perdido.

Mejorando la encriptación de datos a través de TKIP

Para mejorar la encriptación, WPA utiliza su protocolo de integridad de clave temporal o TKIP. TKIP provee importantes mejoras de encriptación de datos, incluyendo una función de mezcla de clave por paquete, un chequeo de integridad de mensaje (MIC), un vector de iniciación (IV) extendido con reglas de secuenciamiento y un mecanismo de reintroducción. A través de estas mejoras, TKIP soluciona todas las vulnerabilidades conocidas del WEP.

Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los vectores de inicialización con respecto a WEP.

Autenticación de usuario a nivel empresarial vía 802.1x y EAP

WEP no tiene ningún mecanismo de autenticación de usuarios. Para realizar la autenticación, WAP implementa el 802.1x y el protocolo de autenticación extensible o EAP. Juntos, estas implementaciones proveen de un marco de trabajo para una rígida autenticación de usuarios. Este marco de trabajo utiliza un servidor central de autenticación, como por ejemplo RADIUS, para autenticar a cada usuario en la red antes de permitirle unirse a ella. Además, también emplea “autenticación mutua”, por lo que un usuario de red inalámbrica no puede unirse accidentalmente a una “red infiltrada” donde podría ser robada.

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- **Modalidad de red empresarial:** Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

- **Modalidad de red casera:** WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

WPA2 (IEEE 802.11i)

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2. Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (*Estándar de Encriptación Avanzada*). Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (*Message Authentication Code Protocol*) en lugar de los códigos MIC. Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

2.4.2 PUERTOS (GATEWAYS)

Cuando un ordenador se conecta a internet, éste pasa a ser un elemento más dentro de la Red, es decir, forma parte de toda la Red y como tal se tiene que comunicar con el resto. Para poder comunicarse, lo primero que necesita es tener una dirección electrónica y poder identificarse con los demás. Si se realiza una petición, por ejemplo de una página web, el servidor tiene que saber a quien se la envía. Esa dirección electrónica es la dirección IP, qué es un número de 4 grupos de cifras de la forma **xxx.xxx.xxx.xxx**. Pero eso no es suficiente, ya que en internet se pueden utilizar muchos y diversos servicios y es necesario poder diferenciarlos. La forma de "diferenciarlos" es mediante los puertos.

Los puertos son los puntos de enganche para cada conexión de red que realizamos. El protocolo TCP (el utilizado en internet) identifica los extremos de una conexión por las direcciones IP de los dos nodos (ordenadores) implicados (servidor y cliente) y el número de los puertos de cada nodo.

Cuando conectamos a Internet nuestro proveedor nos da, para esa conexión, una dirección IP para poder comunicarnos con el resto de Internet. Cuando solicitas un servicio de internet, por ejemplo una pagina web, haces tu solicitud de la página mediante un puerto de tu ordenador a un puerto del servidor web.

Existen mas de 65.000 puertos diferentes, usados para las conexiones de Red. Los siguientes enlaces son una relación de puertos y los servicios a los que corresponden, así como un listado de puertos más utilizados por los troyanos.

Nombre de Servicio	**Número de Puerto**
echo	7/tcp
echo	7/udp
discard	9/tcp
discard	9/udp
systat	11/tcp
daytime	13/tcp
daytime	13/udp
qotd	17/tcp
qotd	17/udp
chargen	19/tcp
chargen	19/udp
ftp-data	20/tcp
ftp	21/tcp
telnet	23/tcp
smtp	25/tcp
time	37/tcp
time	37/udp
rlp	39/udp
nameserver	42/tcp
nameserver	42/udp
nicname	43/tcp
domain	53/tcp
domain	53/udp
bootps	67/udp
bootpc	68/udp
tftp	69/udp
finger	79/tcp
http	80/tcp
kerberos-sec	88/tcp
kerberos-sec	88/udp
hostname	101/tcp
iso-tsap	102/tcp
rtelnet	107/tcp

pop2	109/tcp
pop3	110/tcp
sunrpc	111/tcp
sunrpc	111/udp
auth	113/tcp
uucp-path	117/tcp
nntp	119/tcp
ntp	123/udp
epmap	135/tcp
epmap	135/udp
netbios-ns	137/tcp
netbios-ns	137/udp
netbios-dgm	138/udp
netbios-ssn	139/tcp
imap	143/tcp
pcmail-srv	158/tcp
snmp	161/udp
snmptrap	162/udp
print-srv	170/tcp
bgp	179/tcp
irc	194/tcp
ipx	213/udp
ldap	389/tcp
https	443/tcp
https	443/udp
microsoft-ds	445/tcp
microsoft-ds	445/udp
#? kpasswd	464/tcp
#? kpasswd	464/udp
isakmp	500/udp
exec	512/tcp
biff	512/udp
login	513/tcp
who	513/udp
cmd	514/tcp
syslog	514/udp
printer	515/tcp
talk	517/udp
ntalk	518/udp
efs	520/tcp
router	520/udp
timed	525/udp
tempo	526/tcp
courier	530/tcp
conference	531/tcp
netnews	532/tcp
netwall	533/udp
uucp	540/tcp
klogin	543/tcp
kshell	544/tcp
new-rwho	550/udp
remotefs	556/tcp
rmonitor	560/udp
monitor	561/udp

ldaps	636/tcp
doom	666/tcp
doom	666/udp
kerberos-adm	749/tcp
kerberos-adm	749/udp
kpop	1109/tcp

TABLA 2.2: PUERTOS

2.5 MEDIDAS DE PREVENCIÓN

A continuación se indican cuatro medidas básicas que le ayudarán a reducir sus temores de seguridad de red inalámbrica.

1. Utilice un firewall

Un firewall o servidor de seguridad controla el acceso a la red. Puede impedir que los intrusos de Internet sondeen los datos de su red privada. Y puede controlar a los empleados que tienen acceso fuera de la red.

Existen dos tipos básicos de firewalls: de hardware y de software. Ambos examinan los datos que circulan por la red y descartan los que no cumplen determinados criterios. Los servidores de seguridad de hardware resultan más adecuados para una red ya que pueden proteger todos los equipos de la misma. También ofrecen un nivel adicional de defensa ya que pueden "ocultar" de forma efectiva todos los equipos de red al mundo exterior. Los servidores de seguridad de software, como Firewall de Windows sólo protegen el equipo en el que se ejecutan y proporcionan una buena defensa de reserva a los servidores de seguridad de hardware.

2. Utilice contraseñas seguras.

La mayoría de las pequeñas empresas utilizan contraseñas para autenticar la identidad, tanto en equipos o cajas registradoras como en sistemas de alarma. Aunque hay sistemas de autenticación más sofisticados, como tarjetas inteligentes y analizadores de huellas digitales o iris, las contraseñas son más habituales porque son fáciles de utilizar. Pero también es muy fácil que se utilicen de un modo incorrecto. Los piratas informáticos disponen de herramientas automatizadas que les ayudan a descubrir contraseñas simples en pocos minutos.

Y con demasiada frecuencia las contraseñas no son eficaces por tres motivos:

- Los documentos confidenciales no se han protegido con contraseña, lo que permite que cualquier persona acceda a un equipo no seguro e inicie la sesión.
- Las contraseñas no son seguras o nunca se han cambiado.
- Las contraseñas están anotadas a simple vista junto al equipo.

Informar a los empleados de la importancia de las contraseñas es el primer paso para convertir las contraseñas en una valiosa herramienta de seguridad de la red inalámbrica. Los empleados deben considerar su contraseña del mismo modo que si fuera una llave de la oficina. Es decir, no se debe dejar en cualquier parte ni se debe compartir. También deben evitar las contraseñas no seguras y fáciles de adivinar que incluyan:

- Su nombre real, nombre de usuario o nombre de la compañía.
- Una palabra de diccionario común que les haga vulnerables ante "ataques de diccionario".
- Contraseñas comunes, como "contraseña", "entrar" o "1,2,3,4".
- Sustituciones de letras conocidas, como reemplazar "i" por "!" o "s" por "$".
- Una contraseña que conozca alguien.

¿Cómo es una contraseña "segura"? Debe tener las siguientes características:

- Una longitud de ocho caracteres como mínimo; cuanto más larga, mejor.
- Una combinación de letras mayúsculas y minúsculas, números y símbolos.
- Se debe cambiar cada 90 días como mínimo y, al cambiarla, debe ser muy distinta de las contraseñas anteriores.

3. Utilice las funciones de seguridad inalámbrica.

Las redes inalámbricas utilizan un vínculo de radio frecuencia en vez de cables para conectar los equipos. Por lo tanto, cualquiera dentro del alcance puede, en teoría, recibir o transmitir datos en la red. Existen herramientas gratuitas que permiten a los intrusos "rastrear" redes no seguras. Aunque la vulnerabilidad aumenta con una red inalámbrica, los criminales informáticos disponen de herramientas para acceder a cualquier tipo de sistema informático.

Existen funciones de seguridad integradas en los productos Wi-Fi, pero los fabricantes normalmente las desactivan de forma predeterminada porque así se facilita la configuración de la red. Si utiliza una red inalámbrica, asegúrese de activarlas y de utilizar las funciones de cifrado configurable y de control de acceso que contribuirán a que su red sea más segura.

Tenga en cuenta también lo siguiente:

- Restringir el acceso inalámbrico, si el punto de acceso lo permite, al horario de oficina o cuando piense utilizar la red.
- Filtrar los intrusos ocasionales mediante la configuración de puntos de acceso para restringir el acceso a la red únicamente a las direcciones de control de acceso a los medios (MAC, Control de Acceso al Medio) que sean de confianza.
- Actualizar a un cifrado de acceso protegido (WPA) más sólido si su equipo es antiguo.

4. Cierre los puertos de red innecesarios.

Los puertos de red permiten la comunicación entre los equipos cliente y los servidores. Para reforzar la seguridad de la red y frustrar el acceso no autorizado, deben cerrar los puertos de red que no utilice o sean innecesarios mediante servidores de seguridad dedicados, servidores de seguridad basados en host o filtros de seguridad de protocolo Internet. Se debe tener precaución: los productos de servidor de Microsoft utilizan varios puertos y protocolos de red numerados para establecer comunicación con los sistemas cliente y servidor. Al bloquear los puertos que utiliza Windows Server System se puede impedir que un servidor responda a solicitudes de cliente legítimas, lo que puede implicar que el servidor no funcione correctamente o deje de hacerlo.

CAPITULO III

ESCENARIOS DE FUNCIONAMIENTO DE SEGURIDAD MÁS COMUNES

3.1 MODELO DE SEGURIDAD

3.1.1 INTRODUCCIÓN

En las redes wireless los datos circulan a través del aire, con lo que pueden ser fácilmente interceptados sin necesidad de estar en el interior de las instalaciones de la empresa. Esto provoca un riesgo en la transmisión de datos “sensibles” a través de una red wireless. Para ello existen diferentes soluciones para evitar la interceptación. Todas ellas, de una manera o de otra, se basan en la encriptación de los datos que circulan por la red, de manera que aunque sean interceptados, no puedan ser descifrados, proporcionando, además, de manera implícita, un control de acceso a la red.

Entre los métodos de encriptación que el Access Point nos brinda tenemos la protección WEP y protección WPA.

Si se utiliza el método de protección WEP los datos viajan cifrados y por lo tanto este método es más seguro. Sin embargo he de decir que el uso de este método tampoco es suficiente, ya que el cifrado WEP se ha demostrado inseguro y es posible descifrar los datos que hayan sido cifrados con este protocolo y por consiguiente se puede averiguar la clave WEP y los parámetros necesarios para poder acceder a una red protegida con este método.

El otro método que hemos mencionado es la protección basada en WPA. Al igual que ocurre con WEP se trata de un método que utiliza la criptografía para cifrar

los paquetes que viajan por la red. Sin embargo este método es más seguro, ya que se ha demostrado que es menos vulnerable.

De forma generar podemos decir que WPA es mucho más robusto y seguro que WEP; sin embargo WPA es más difícil de configurar y no todos los dispositivos inalámbricos permiten su uso, por lo que la mayoría de las redes protegidas usan WEP.

Para complementar la seguridad tanto en la plataforma de Linux como en la de Windows independientemente del tipo de red tengamos se puede implementar lo siguiente:

SISTEMA OPERATIVO LINUX

Bajo la plataforma de Linux para la implementación de seguridad se puede utilizar lo siguiente:

- Iptables
- Servidor Proxy

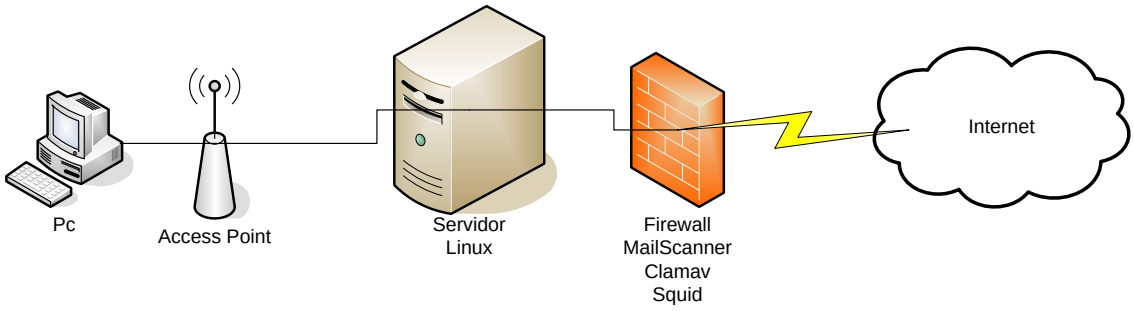


Figura 3.1: Modelo de seguridad bajo la plataforma LINUX

SISTEMA OPERATIVO WINDOWS

En cambio bajo la plataforma de Windows se puede utilizar lo siguiente:

- Active Directory
- Isa Server

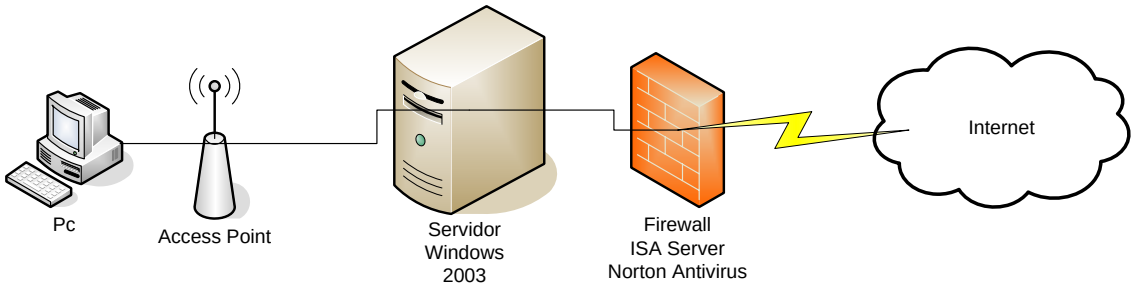


Figura 3.2: Modelo de seguridad bajo la plataforma WINDOWS 2003

3.1.2 ÁMBITO DESIGNADO A ESTUDIAR

La institución educativa ESPE sede Latacunga a demostrado ser un establecimiento líder, integrado al desarrollo científico, educativo y productivo a nivel provincial.

Los servicios que presta el laboratorio de la ESPEL son de Internet, enviar y recibir mail, los mismos que están expuestos a posibles ataques a los cuales debemos brindar la seguridad necesaria, ya que actualmente existe una gran variedad de métodos para proteger una red inalámbrica.

3.2 SOFTWARE PARA SEGURIDAD

3.2.1 LINUX

NOCIONES DE SISTEMA OPERATIVO LINUX

Linux es un sistema operativo basado en Unix que se distribuye bajo licencia GNU. Este sistema operativo ha sido diseñado y programado por una multitud de programadores alrededor del mundo y su núcleo sigue en continuo desarrollo.

ARQUITECTURA DE GNU/LINUX

- Linux no es un bloque monolítico
- Varios componentes trabajan en conjunto, diseñados por personas diferentes y conjuntados en distribuciones
- Solo del exterior el núcleo Linux parece una unidad
- Existe una diferencia entre el núcleo y las aplicaciones

El sistema de archivos de Linux tiene una estructura definida según su propósito:

/etc	Archivos de configuración

/var	Datos volátiles y directorios de spooling
/usr	Programa y librerías accesibles por el usuario
/usr/bin	Herramientas de uso general (editores, correos, compiladores)
/usr/sbin	Utilizado para herramientas de administración que no sean esenciales (cron, lpd)
/usr/local	Contiene la mayor parte de elementos de software que se añade de forma no estándar (bin, lib, etc, man)
/usr/share/man	Páginas manuales
/usr/share/doc	Documentos variados sobre el software instalado
/mnt	Punto de montaje temporal de dispositivos
/tmp	Archivos temporales del sistema
/home	(creado por defecto) Directorios de todos los usuarios
/dev	Archivos de interfaz de dispositivos
/boot	Archivos estáticos para el arranque del sistema
/lib	Compartidas esenciales. Módulos de núcleo
/bin	Comandos básicos
/root	Directorio de la cuenta de administrador
/proc	Información asociada con el núcleo que se está ejecutando
/sbin	Comandos básicos para la administración del sistema

Tabla 3.1: Estructura de directorios**.**

COMPONENTES DEL NÚCLEO

- Administración memoria principal
- Acceso a los periféricos
- Administración del espacio en disco duro
- Administración de los programas y los procesos
- Administración de los derechos de acceso

3.2.2 WINDOWS SERVER 2003

Windows Server 2003 es la versión de Windows para servidores lanzada por Microsoft en el año 2003. Está basada en el núcleo de Windows XP, al que se le han añadido una serie de servicios, y se le han bloqueado algunas características (para mejorar el rendimiento, o simplemente porque no serán usadas). En términos generales, Windows Server 2003 es un Windows XP simplificado, no con menos funciones, sino que estas se encuentran deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor.

Funciones del Servidor

Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar una gran gama de funciones de servidor, en base a sus necesidades, tanto de manera centralizada como distribuida. Algunas de estas funciones del servidor son:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

Windows Server 2003 contiene varias herramientas importantes de administración automatizada como Microsoft Software Update Services (SUS) y asistentes de configuración de servidor para ayudar a automatizar la implementación. La Administración de Políticas de Grupo se hace más fácil con la nueva Consola para Administración de Políticas de Grupo (GPMC), permitiendo que más organizaciones utilicen mejor el servicio Active Directory para sacar beneficio de sus poderosas características de administración.

Active Directory, es un servicio de directorio de la familia de Windows Server 2003. Esto almacena información acerca de objetos en la red y hace que esta información sea fácil de encontrar por los administradores y usuarios proporcionando una organización lógica y jerárquica de información en el directorio. Windows Server 2003 trae muchas mejoras para Active Directory, haciéndolo más versátil, fiable y económico de usar. En Windows Server 2003, Active Directory ofrece una escalabilidad y rendimiento elevado. Esto también le permite mayor flexibilidad para diseñar, implementar y administrar el directorio de su organización.

3.3 IMPLEMENTACIÓN DE SEGURIDAD

3.3.1 FIREWALL

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra, funciona como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

En el caso de las redes wireless los firewalls se establecen como barrera de separación entre los dispositivos wireless y el resto de la red cableada, para evitar accesos no autorizados a zonas comprometedoras de la red, como se muestra en la siguiente figura.

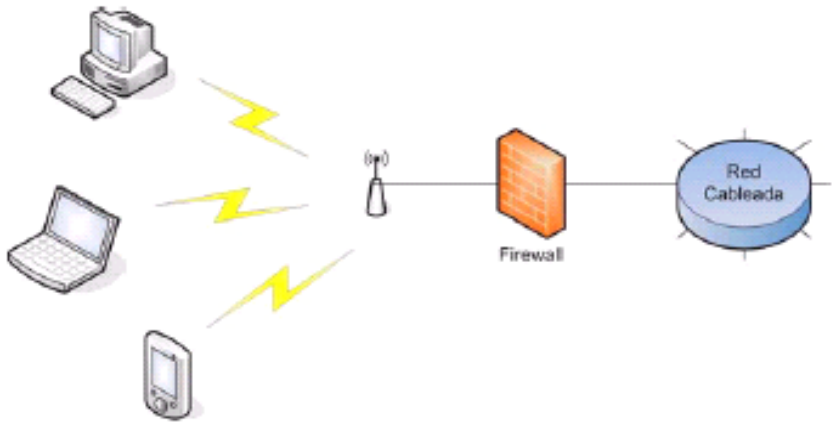


Figura 3.3: Uso de un firewall en la red wireless.

Un firewall es un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sea permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y ftp, también podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, ya que son muchas personas que hoy en día que se conectan, de una manera u otra, a Internet, desde empresas que operan en la red hasta personas en sus casas que pasan un rato divertido navegando por sus páginas preferidas sin saber el riesgo que con esto conllevan ya que el bien que obtenemos de Internet tiene un precio: **Internet no es un lugar seguro**.

La función del firewall, por tanto, es bloquear el tráfico no autorizado entre un sistema de confianza y un sistema de dudosa confianza. Lo cual nos da una idea del

peligro que corre un usuario cualquiera de Internet que no tome las precauciones mínimas.

Eso quiere decir que, mediante un firewall, podemos detectar el tráfico no deseado hacia nuestros sistemas, y en general, los posibles ataques de que seamos objeto. De esta manera podremos **aislar** nuestros equipos del exterior, permitiendo nuestro uso al Internet de manera absolutamente normal pero minimizando en lo posible la probabilidad de padecer las consecuencias de un ataque.

Un firewall es a menudo, instalado en el punto donde una red interna se conecta con Internet. Todo tráfico externo de Internet hacia la red interna pasa a través del firewall, así puede determinar si dicho tráfico es aceptable de acuerdo a sus políticas de seguridad.

Aunque el propósito principal de los firewall es mantener a los intrusos fuera del alcance de la información que es propiedad de un ente determinado, ya sea un usuario, una empresa o un gobierno, su posición dentro del acceso a distintas redes lo vuelve muy útil para controlar estadísticas de situaciones como usuarios que intentaron conectarse y no lo consiguieron, tráfico que atravesó la misma, etc. Esto proporciona un sistema muy cómodo de auditar la red. Algunas de sus funciones son las siguientes:

- Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- Prevenir los ataques
- Dividir una red en zonas con distintas necesidades de seguridad
- Auditar el acceso a la red.

Algunos firewall solamente permiten tráfico de correo a través de ellos, de modo que protegen de cualquier ataque sobre la red distinto de un servicio de correo electrónico. Otros firewall proporcionan menos restricciones y bloquean servicios que son conocidos por sus constantes problemas de intrusión. Generalmente, los firewalls están configurados para proteger contra "logins" sin autorización. Esto ayuda principalmente a prevenir actos de vandalismos en máquinas y software de nuestra red. Redes firewalls más elaboradas bloquean el tráfico de fuera a dentro, permitiendo a los usuarios del interior comunicarse libremente con los usuarios del

exterior. Los firewall pueden protegernos de cualquier tipo de ataque a la red, siempre y cuando se configuren para ello.

Hay tres formas de operar los firewalls (se pueden usar una o varias de ellas):

1. Filtrado de paquetes. Cada paquete de información se analiza con respecto a una serie de filtros. Los paquetes que logran pasar los filtros se envían al sistema que los solicitó y todos los demás se descartan.
2. Servicio Proxy. La información solicitada del exterior es recuperada por el firewall y después enviada al sistema que la requirió originalmente.
3. Inspección estática. No se examinan los paquetes de la información, pero se comparan ciertas partes clave de cada paquete en búsqueda de datos confiables. Los datos que salen de la red local se analizan registrando patrones específicos, de tal manera que la información entrante debe cumplir con esos patrones. Si hay un cierto margen de coincidencia, el material entrante pasa sin problema; en otro caso, se descarta.

Los filtros de un firewall se definen a partir de ciertos criterios, tales como:

- **Direcciones IP.** Se puede bloquear el acceso desde una IP específica, evitando ataques o consultas masivas a equipos, servidores y clientes.
- **Nombres de dominio.** Consiste en tablas con nombres de computadoras vinculadas al DNS a donde no se permite el acceso de los usuarios locales.
- **Palabras clave.** Programas detective (sniffer) en los firewalls revisan el contenido de la información en búsqueda de palabras vinculadas con información o sitios no permitidos.
- **Puertos.** Cada aplicación o servicio que usa la red IP, genera una conexión hacia un puerto. El 80 es el común para los servidores WWW y el 21 para las transferencias de archivos. Un firewall registra estos servicios y determina que computadoras pueden acceder a ellos y cuáles no.
- **Protocolos.** Es factible restringir el uso de algunos protocolos, como HTTP (el que sirve las páginas WWW) o Telnet (para sesiones remotas). Así se evita que usuarios mal intencionados del exterior de la red, intenten acceder a un equipo local mediante un protocolo específico.

Para un administrador de firewall es mucho más sencillo aplicar el filtrado por puertos o protocolos que los anteriores, ya que requerirían de más vigilancia y administración del firewall, aunque ninguno método excluye a los demás de ser empleados.

3.3.2 IMPLEMENTACIÓN DE SEGURIDAD UTILIZANDO EL SISTEMA OPERATIVO LINUX

3.3.2.1 IPTABLES

En Linux para implementar el firewall vamos a utilizar Iptables.

Iptables es la herramienta que nos permite configurar las reglas del sistema de filtrado de paquetes del kernel de Linux. Con esta herramienta, podremos crearnos un firewall adaptado a nuestras necesidades.

Un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación, iptables esta integrado con el kernel, es parte del sistema operativo.

Iptables maneja las reglas de filtrado de forma dinámica. Esto significa que cada vez que la máquina sea reiniciada, las reglas se borrarán. Por este motivo, se recomienda crear un script que se ejecute al iniciar el sistema para que éstas vuelvan a ser definidas.

Dado que el soporte para el firewall está integrado en el kernel de Linux (**Netfilter**), para poder usar iptables tendremos que asegurarnos que nuestro núcleo admite el uso de iptables y que añadimos a la configuración del núcleo todos aquellos *targets o acción* que vayamos a necesitar.

Su funcionamiento es simple: a iptables se le proporcionan unas *reglas*, especificando a cada una de ellas unas determinadas características que debe cumplir un paquete. Además, se especifica para esa regla una *acción*. Las reglas tienen un orden, y cuando se recibe o se envía un paquete, las reglas se recorren en orden hasta que las condiciones que pide una de ellas se cumplen en el paquete, y la regla se activa realizando sobre el paquete la acción que le haya sido especificada.

Estas acciones se plasman en los que se denominan ***targets***, que indican lo que se debe hacer con el paquete. Los más usados son bastante explícitos: **ACCEPT**, **DROP** y **REJECT.**

En cuanto a los paquetes, el total del sistema de filtrado de paquetes del kernel se divide en tres *tablas*, cada una con varias **chains** a las que puede *pertenecer* un paquete, de la siguiente manera.

- **filter**: Tabla por defecto, para los paquetes que se refieran a nuestra máquina
  - **INPUT**: Paquetes recibidos para nuestro sistema
  - **FORWARD**: Paquetes enrutados a través de nuestro sistema

- **OUTPUT**: Paquetes generados en nuestro sistema y que son enviados

- **nat**: Tabla referida a los paquetes enrutados en un sistema con Masquerading
  - **PREROUTING**: Para alterar los paquetes según entren
  - **OUTPUT**: Para alterar paquetes generados localmente antes de enrutar
  - **POSTROUTING**: Para alterar los paquetes cuando están a punto para salir
- **mangle**: Alteraciones más *especiales* de paquetes
  - **PREROUTING**: Para alterar los paquetes entrantes antes de enrutar
  - **OUTPUT**: Para alterar los paquetes generados localmente antes de enrutar.

Cuando un paquete es recibido, el sistema utiliza en primer lugar las reglas de la lista INPUT para decidir si la acepta o no. Si las reglas definidas en esta lista indican que el paquete puede ser aceptado, se comprueba dónde debe ser enrutado. Si el destino es una máquina diferente a firewall, se aplican las reglas de la lista FORWARD para reenviarlo a su destino.

La lista OUTPUT se utiliza antes de enviar un paquete por una interfaz de red, para decidir si el tráfico de salida es permitido o no.

Si el paquete no cumple ninguna de las reglas de la lista, puede ser aceptado o rechazado según haya sido configurado el iptables. Para lograr mantener un nivel óptimo de seguridad, se recomienda que sea configurado para que rechace el paquete.

Cuando un paquete cumple con una determinada regla de una lista, se define qué hacer con éste mediante una acción (Target). Las acciones utilizadas en iptables son: ACCEPT, que permite el paso del paquete. DROP, que lo bloquea, QUEUE y RETURN.

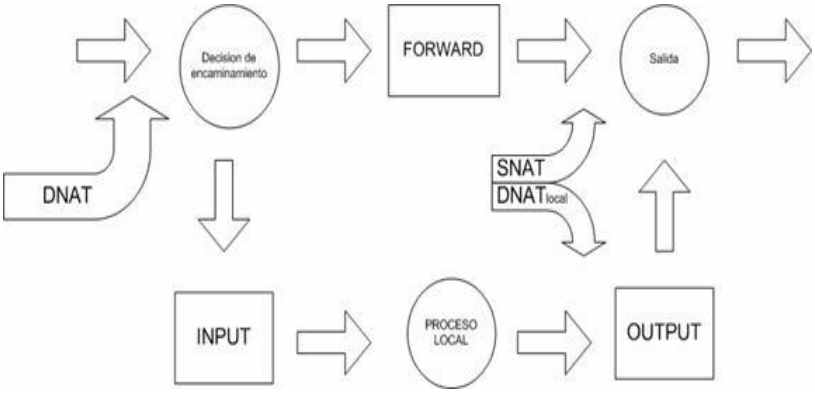


Figura 3.4: Función de Iptables

Como se ve en el gráfico, básicamente se mira si el paquete esta destinado a la propia máquina o si va a otra. Para los paquetes (o datagramas, según el protocolo) que van a la propia maquina se aplican las reglas INPUT y OUTPUT, y

para filtrar paquetes que van a otras redes o máquinas se aplican simplemente reglas FORWARD.

INPUT, OUTPUT y FORWARD son los tres tipos de reglas de filtrado. Pero antes de aplicar esas reglas es posible aplicar reglas de NAT: estas se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino

- **CREACIÓN DE UNA POLÍTICA DE SEGURIDAD USANDO IPTABLES**

Se definirá una política de seguridad básica para demostrar el funcionamiento del firewall, para lo cual señalamos algunas órdenes básicas:

- **iptables -F :** borrado de reglas
- **iptables -L :** listado de reglas que se están aplicando
- **iptables -A :** append, añadir regla
- **iptables -D :** borrar una regla

EJEMPLO DE UNA REGLA

#Aceptar conexiones al puerto 80 (www)

iptables -A INPUT -s 0.0.0.0/0 -p TCP --dport 80 -j ACCEPT

Nomenclatura:

iptables: comando iptables

-A: añadir una regla

INPUT: estado del paquete *(al entrar es input).*

-s source address **0.0.0.0/0:** dirección de acceso *(cualquiera en este caso)*

-p TCP: tipo de puerto

--dport : puerto de destino

-j ACCEPT: destino del paquete *(se acepta, podrá ser DROP, LOG, REJECT, ...)*

Visto esto, y dado que tenemos multitud de conexiones, más aún si estamos ofreciendo servicios, deberemos introducir una multitud de comandos al iptables cada vez que arranque el núcleo, un trabajo laborioso, de ahí que se opte por la automatización.

Por ello se crea un **script**, *un simple archivo de texto,* en el que ponemos todo lo que queramos que ejecute nuestro cortafuegos durante la carga del sistema, y programamos el Linux para que cargue el script durante arranque.

3.3.2.2 SQUID

Squid es un programa que hace caché de datos obtenidos en Internet. Realiza este trabajo aceptando peticiones de los objetos que los usuarios quieren descargar y realizando estas peticiones a la red en su nombre. Squid se conecta con el servidor correspondiente, pide el objeto. De forma transparente, este objeto se entrega a la máquina cliente, pero al mismo tiempo, guarda una copia. La próxima vez que alguna máquina cliente de squid solicite la misma página, squid simplemente le transfiere su copia almacenada en memoria o disco, acelerando considerablemente la transferencia y ahorrando ancho de banda en la conexión a Internet.

Squid también soporta SSL (Secure Socket Layer) con lo que también acelera las transacciones cifradas, y es capaz de ser configurado con amplios controles de acceso sobre las peticiones de usuarios, lo que es muy útil, para permitir/denegar acceso al servidor a diferentes grupos de usuarios. Al utilizar el protocolo de cache de Internet, *squid* puede ahorrar un considerable ancho de banda.

Para que se observe de forma más ilustrativa veámoslo en una imagen:

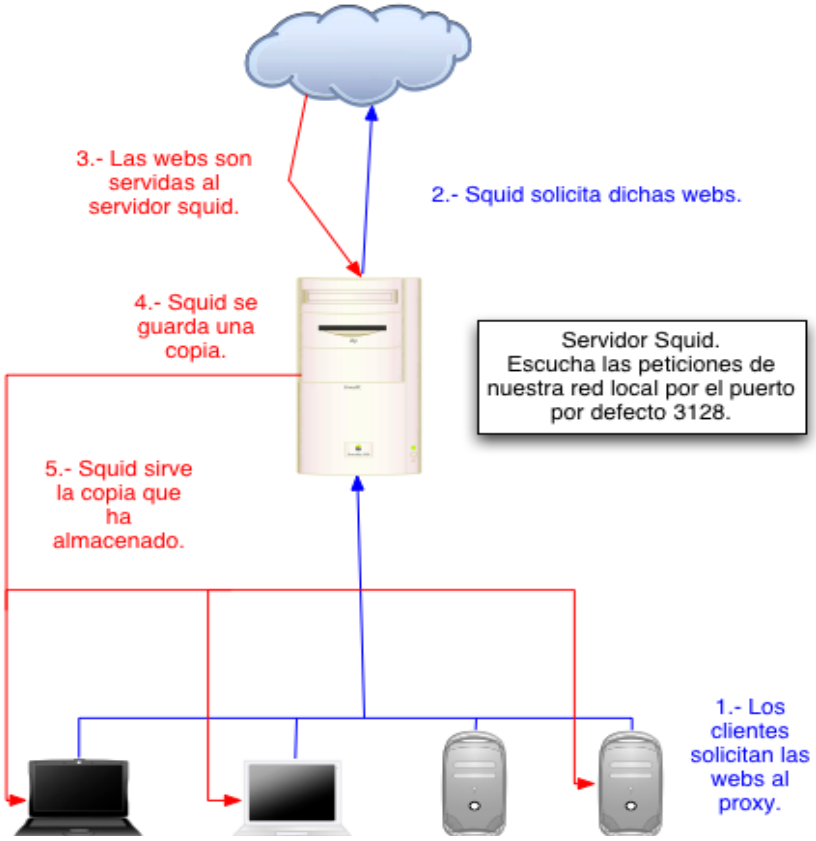


Figura 3.5: Función del Servidor Proxy (Squid)

3.3.3 IMPLEMENTACIÓN DE SEGURIDAD UTILIZANDO EL SISTEMA OPERATIVO WINDOWS SERVER 2003

Microsoft y la Seguridad

- Originalmente Windows fue diseñados como SO para PC's de usuario y no como SO de Red.
- En este escenario la seguridad era menos importante que las funcionalidades o facilidades para los usuarios.
- Con los problemas de seguridad crecientes, Microsoft tiene que cambiar la filosofía de sus productos.
- Productos específicos para la seguridad (ISA Server)
- Cualquier Firewall sobre plataforma Windows es inseguro.
- ISA Server es una buena solución como Proxy.

3.3.3.1 ISA SERVER

3.3.3.1.1 INTRODUCCIÓN

Microsoft Internet Security and Acceleration (ISA) Server 2004 es la solución de caché Web, servidor de seguridad avanzado en el nivel de aplicación y red privada virtual que permite a los clientes obtener el máximo provecho de las inversiones en tecnología de la información existente al mejorar la seguridad de la red y el rendimiento.

ISA Server ofrece un acceso rápido y seguro a todo tipo de redes. El firewall de ISA Server 2004 protege a la empresa frente a amenazas tanto externas como internas. ISA Server 2004 realiza una exploración detallada de los protocolos de Internet, como HTTP, que le permite detectar muchas de las amenazas pasadas por alto por los firewall tradicionales. La arquitectura integrada de firewall ofrece prestaciones de filtrado e inspección de todo el tráfico, protegiendo la red de amenazas que intentan entrar a través de una conexión de red.

Al iniciar Isa Server ya tiene configurado una regla por defecto en la cual se deniega todo, eso deja aislado todo el tráfico, pues si necesitamos navegar desde el servidor, tenemos que crear una regla para que desde el host local se pueda acceder a la red externa mediante protocolo HTTP. ISA Server, puede hacer reglas diferentes para diferentes usuarios, o permitir una regla a unos y a otros denegarla.

3.3.3.1.2 REGLAS DEL ISA SERVER 2004

Existen 3 tipos de reglas que permiten la comunicación entre las redes manejadas por el ISA Server estas son:

Reglas de Redes:

Estas reglas definen la topología de red en donde se encuentra el ISA Server. Las reglas de red definen como es la relación entre la red. El tipo de relación posible es Ruteo o NAT. Si no existe la relación entre las redes, el ISA Server bloquea el tráfico. En el caso de la relación de ruteo, es bi-direccional y permite el trafico ambas direcciones y en cambio en la relación de NAT es el trafico permito es unidireccional. Si bien son simples de configurar, son muy importante su Buena definición.

Reglas de Sistema:

Son un conjunto de 30 reglas incorporadas que se aplican al propio ISA Server (localhost), Estas controlan la comunicación del ISA Server con todas las redes. Por defecto están ocultadas. Y tiene prioridad ante cualquier otra regla ya que son aplicadas primero que cualquier otra.

Reglas de Firewall:

Son todas las reglas definidas por el administrador. Hay 3 tipos de estas, reglas de acceso, regla de publicación de Web y regla de publicación de servidor. También incluye una regla especia que no puede ser borrada ni modificada que deniega todo y siempre se aplica en ultimo orden. Con lo cual todo tráfico que no esta explícitamente permitido se deniega.

Orden de Aplicación

Para el orden de aplicación el ISA chequea primero la existencia de las redes y la relación entre estas, si no esta definida una relación entre redes de donde viene el tráfico y el destino. El ISA bloquea el tráfico.

Luego el ISA Server chequea en orden las políticas del sistema y luego las políticas de firewall. Si alguna regla concuerda con la petición de tráfico el ISA Server aplica la regla y no sigue buscando en otras reglas.

Si no hay regla que concuerde con la petición, el ISA recorre todas las reglas hasta llegar a la última que siempre concuerda y que deniega todo el tráfico.

Criterio de concordancia

La pregunta es, que parámetros usa el ISA Server para aplicar una regla a un tráfico. El ISA Server usa los siguientes parámetros de las reglas para ver si la aplica o no.

Protocolo: Definidos en las reglas de firewall, son tomados en cuenta el tipo de protocolo y puerto

Origen: Las redes de origen u objeto origen de donde viene el tráfico, estos objetos pueden ser "Network, Network Sets, Computers, Computer Sets, Address Ranges y Subnets."

Horario: Cualquier horario definido.

Destino: La red destino a donde va dirigido el tráfico u objetos como "Network, Network Sets, Computers, Computer Sets, Address Ranges, Subnets, Domain Name Sets y URL Sets."

Usuarios: Uno o más objetos que pueden ser "All Users, All Authenticated Users, System and Network Service" o cualquier grupo o usuario definido

Contenido: Cualquier tipo de contenido definido en las reglas.

CAPITULO IV

IMPLEMENTACIÓN DE SEGURIDADES EN REDES INALÁMBRICAS DE DATOS FIJAS EN LOS LABORATORIOS DE LA FACULTAD DE SISTEMAS E INFORMÁTICA DE LA ESPEL

4.1 CONTROL DE SERVICIOS

4.1.1 CONTROL DE SERVICIOS BAJO LA PLATAFORMA LINUX

El mantenimiento de la seguridad en su sistema Red Hat Linux es extremadamente importante. Una forma de administrar la seguridad en el sistema es mediante una gestión minuciosa del acceso a los servicios del sistema. Probablemente su sistema deberá proporcionar acceso a determinados servicios (por ejemplo, httpd si ejecuta un servidor Web). Sin embargo, si no necesita proveer este servicio, debería desactivar esta función para que de este modo se minimice la exposición a potenciales fallos.

Hay diferentes métodos de administrar el acceso a los servicios del sistema. Debe decidir qué método le gustaría usar en función del servicio, la configuración del sistema y el nivel de conocimientos que tenga de Linux.

La forma más fácil de denegar el acceso a un servicio es desactivándolo. Tanto los servicios administrados con xinetd y los servicios en la jerarquía /etc/rc.d se pueden configurar para iniciarse o detenerse con tres aplicaciones diferentes:

- **Herramienta de configuración de servicios**: Es una aplicación gráfica que muestra una descripción de cada servicio, indica si los servicios se han iniciado en el momento del arranque y permite que los servicios sean arrancados, detenidos o reiniciados.
- **Ntsysv**: Es una aplicación basada en texto que permite configurar cuáles servicios son arrancados al momento de arranque para cada nivel de ejecución. Los cambios no toman efecto de inmediato para los servicios no xinetd. Los

servicios que no son xinetd no pueden ser arrancados, detenidos o reiniciados usando este programa.

- **Chkconfig:** Es una utilidad de línea de comandos permite activar o desactivar servicios para los diferentes niveles de ejecución. Los cambios no toman efecto de inmediato para los servicios no xinetd. Los servicios no xinetd no pueden ser arrancados, detenidos o reiniciados usando esta utilidad.

4.1.1.1 CONECTIVIDAD

Para elaborar la conexión del servidor Linux Red Hat 9.0 con el cliente windows 2000 professional utilizando redes inalámbricas realizamos los siguientes pasos:

1. Materiales

- AP o Router Wireless que será necesario ya que vamos a utilizar la topología de infraestructura.
- Tarjeta de red para el PC que actúe como servidor y tarjetas Wireless para los PCs clientes o PCMCIA para los posibles portátiles.

2. Pasos previos

Lo primero que se debe tomar en cuenta antes de comprar todo el material, será hacer una planificación de la futura red, algo como esto:

Figura 4.1: Ejemplo de planificación para una Red Wireless.

También se debe tener en cuenta los muebles, las paredes, aparatos que puedan “interferir” en la red, además recordar que en las redes Wireless, cuantos más obstáculos haya peor llegará la señal.

3. Instalación del hardware

Instalación del servidor.

Vamos a instalar el hardware en el PC servidor (el que distribuirá la señal a los demás PCs).

- Tarjeta de red: Lo primero será instalar la correspondiente tarjeta (Ethernet con puerto RJ45 ya que vamos a conectar un AP).
- AP o Router Wireless: Una vez instalado una tarjeta de red Ethernet se deberá conectar el AP mediante el cable RJ45.

Instalación de los clientes.

Ahora vamos a instalar el hardware en los PCs clientes (a los que llegará la señal que transmita el servidor).

El hardware que se tendrá que instalar será una tarjeta de red Wireless (PC sobremesa) o una tarjeta PCMCIA (portátil).

4. Configuración del software

PC servidor.

Este es el PC que enviará la señal a los demás PCs de la red, así que será el primero que configuremos,

- **Configuración de la tarjeta ethernet**

Lo primero que hay que configurar es la tarjeta de red. En el Panel de control seleccionamos el protocolo TCP/IP para ello configuraremos lo siguiente:

Dirección IP: Aquí pondremos la dirección del PC (cada PC de la red tendrá una dirección IP distinta, siendo siempre del mismo rango, por ejemplo, si ponemos 192.168.0.1, los demás PCs de la red serán siempre 192.168.0.xxx).

Máscara de subred: Tiene que ser la misma en todos los PCs de la red. Por ejemplo, si ponemos 255.255.255.0, los demás PCs de la red serán siempre 255.255.255.0

Puerta de enlace predeterminada: Esto es a la IP que tiene que conectar un PC cliente (la IP del servidor), como estamos configurando el PC servidor, y esta es la que va ha estar conectado al AP ponemos la IP que corresponda al AP como es 192.168.0.50.

Servidores DNS: Será la dirección IP con la que tendremos salida a Internet desde la red.

- **Configuración del Access Point**

Ahora hay que configurar el AP o Router. La interfaz de configuración del dispositivo variará dependiendo del AP o Router que se disponga, pero las opciones son las mismas que a continuación se detalla:

Dirección IP: No puede ser la misma que de la tarjeta de red, la dirección que pongamos aquí es la que viene por defecto pero que este dentro del rango de la red.

Máscara de subred: Tiene que ser la misma que hemos puesto en la configuración de la tarjeta de red.

Gateway: Pondremos la IP del Servidor 192.168.0.1.

SSID: Será el nombre de nuestra red, tiene que ser el mismo en el AP o Router y todas las tarjetas de la red Wireless.

Canal: Es el canal por el que se transmitirán los datos, normalmente se usa el 6, ya que es el que soportan todos los dispositivos.

Admin y clave de acceso: Son los que el sistema te preguntará las próximas veces que intentes configurar el AP o Router.

Con esto es suficiente, las demás opciones van a gusto del usuario, ya que son velocidades de transmisión, modos del dispositivo, etc.

PC cliente

La configuración de los PCs clientes es la misma que el PC servidor, variando algunas cosillas como:

La dirección IP: Tendrá que estar dentro del mismo rango (por ejemplo: 192.168.0.xxx).

Puerta de enlace predeterminada: Aquí ahora sí pondremos una dirección IP (la del PC servidor, 192.168.0.1).

5. Establecer la conexión

Una vez configurados todos los PCs (servidor y clientes), vamos a conectar los clientes a la red.

Lo primero que se debe hacer es asegurar que el PC servidor y el AP o Router estén funcionando correctamente.

Una forma de comprobar si existe conexión a la red es haciendo un ping desde el PC cliente al servidor. Estos pasos los repetiremos con todos los PCs cliente de la red y también desde el PC servidor a todos los clientes y de clientes a clientes, para comprobar que todo estén conectados entre sí.

4.1.1.2 FIREWALL (CODIGO DE IPTABLES)

```
#activa el ruteo hacia internet
echo 1 > /proc/sys/net/ipv4/ip_forward
#asigna comando a variable
REGLA="/sbin/iptables"
#definimos variables de tarjetas
INTERNET=eth0
LAN=eth1
#borrando reglas
$REGLA -F
$REGLA -F INPUT
```

```
$REGLA -F OUTPUT
$REGLA -F FORWARD
$REGLA -F -t mangle
$REGLA -F -t nat
$REGLA -X
#aceptando reglas
$REGLA -P INPUT ACCEPT
$REGLA -P OUTPUT ACCEPT
$REGLA -P FORWARD ACCEPT
#la siguiente linea permite a la LAN navegar en internet
$REGLA -t nat -A POSTROUTING -o $INTERNET -j MASQUERADE
#acepto que la LAN navege el puerto 80
$REGLA -A INPUT -d 0.0.0.0 -p tcp --dport 80 -j ACCEPT
$REGLA -A INPUT -d 0.0.0.0 -p tcp --dport 25 -j ACCEPT
$REGLA -A INPUT -d 0.0.0.0 -p tcp --dport 143 -j ACCEPT
$REGLA -A INPUT -d 0.0.0.0 -p tcp --dport 53 -j ACCEPT
$REGLA -A INPUT -d 0.0.0.0 -p udp --dport 53 -j ACCEPT
$REGLA -A INPUT -d 0.0.0.0 -p tcp --dport 110 -j ACCEPT
$REGLA -A INPUT -d 0.0.0.0 -j DROP
$REGLA -A INPUT -s 0.0.0.0 -j DROP
$REGLA -A OUTPUT -d 0.0.0.0 -j DROP
$REGLA -A OUTPUT -s 0.0.0.0 -j DROP
$REGLA -A FORWARD -d 0.0.0.0 -j DROP
$REGLA -A FORWARD -s 0.0.0.0 -j DROP
```

4.1.1.3 SERVIDOR PROXY (SQUID)

El fichero de configuración de SQUID se halla en /etc/squid/squid.conf y hemos de editarlo con nuestra herramienta favorita para realizar los cambios adecuados y conseguir su labor con cierta seguridad para nuestro sistema.

Este fichero de configuración consta de una multitud de parámetros configurables que ajustan el servidor a nuestras necesidades. Trataremos de reflejar aquellos indispensables para un óptimo funcionamiento.

4.1.1.3.1 CONFIGURACION DE LOS PARAMETROS DE SQUID

Puerto para SQUID

Por defecto, SQUID utilizará el puerto 3128, aunque puede configurarse para que use cualquier otro, incluso varios puertos simultáneamente, dependiendo de nuestras necesidades. La línea correspondiente quedará:

```
http_port 3128
```

Parámetro cache_mem.

El parámetro cache_mem establece la cantidad ideal de memoria para lo siguiente:

• Objetos en tránsito.

• Objetos frecuentemente utilizados (Hot).

• Objetos negativamente almacenados en el caché.

Los datos de estos objetos se almacenan en bloques de 4 Kb. El parámetro cache_mem especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad. Sin embargo los objetos Hot y aquellos negativamente almacenados en el caché podrán utilizar la memoria no empleada hasta que esta sea requerida. De ser necesario, si un objeto en tránsito es mayor a la cantidad de memoria especificada, Squid excederá lo que sea necesario para satisfacer la petición.

De modo predefinido se establecen 8 MB. Puede especificarse una cantidad mayor si así se considera necesario, dependiendo esto de los hábitos de los usuarios o necesidades establecidas por el administrador.

Si se posee un servidor con al menos 128 MB de RAM, establezca 16 MB como valor para este parámetro, para nuestro caso utilizaremos 64 MB:

cache_mem 64 MB

4.1.1.3.2 LISTAS DE CONTROL DE ACCESO

Una de las características más interesantes de este servidor proxy es la posibilidad de establecer unas reglas de control de acceso que pueden complementar perfectamente nuestro objetivo de filtrado de paquetes.

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

acl [nombre de la lista] src [lo que compone a la lista]

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la sub-red. Por ejemplo, si se tiene una red donde las máquinas tienen direcciones IP 192.168.0.**n** con máscara de sub-red 255.255.255.0, podemos utilizar lo siguiente:

```
acl mired src 192.168.0.1/255.255.255.0
```

También puede definirse una Lista de Control de Acceso especificando un fichero localizado en cualquier parte del disco duro, y la cual contiene una lista de direcciones IP. Ejemplo:

```
acl permitidos src "/etc/squid/permitidos"
```

El fichero **/etc/squid/permitidos** contendría algo como siguiente:

```
192.168.0.1
192.168.0.15
192.168.0.40
```

Lo anterior estaría definiendo que la Lista de Control de Acceso denominada permitidos estaría compuesta por las direcciones IP incluidas en el fichero **/etc/squid/permitidos**.

4.1.1.3.3 REGLAS DE CONTROL DE ACCESO.

Estas reglas definen si se permite o no el acceso hacia **Squid**. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador.

La sintaxis básica es la siguiente:

```
http_access [deny o allow] [lista de control de acceso]
```

En el siguiente ejemplo consideramos una regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada permitidos:

```
http_access allow permitidos
```

- **Cómo configurar Squid: Restricción de acceso a sitios Web.**

Denegar el acceso a ciertos Sitios de Red permite hacer un uso más racional del ancho de banda con el que se dispone. El funcionamiento es verdaderamente simple, y consiste en denegar el acceso a nombres de dominio o direcciones Web que contengan patrones en común.

Definiendo patrones comunes.

Lo primero será generar una lista la cual contendrá direcciones Web y palabras usualmente utilizadas en nombres de ciertos dominios. Ejemplos:

```
www.sitioporno.com
www.otrositioporno.com
sitioindeseable.com
otrositioindeseable.com
xxx
sex
porn
```

Esta lista, la cual deberá ser completada con todas las palabras (muchas de está son palabras obscenas en distintos idiomas) y direcciones Web que el administrador considere pertinentes, la guardaremos como */etc/squid/sitios-denegados*.

Parámetros en /etc/squid/squid.conf

Debemos definir una Lista de Control de Acceso que a la vez defina al fichero /etc/squid/sitios-denegados. Esta lista la denominaremos como denegados. De modo tal, la línea correspondiente quedaría del siguiente modo:

```
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
```

A continuación especificaremos una regla de control de acceso para dicha Lista de Control de Acceso*:*

```
http_access allow mired !sitiosdenegados
```

Note que esta debe ir antes de cualquier otra regla que permita el acceso a cualquier otra lista. Ejemplo:

Si por ejemplo el incluir una palabra en particular afecta el acceso a un sitio Web, puede generarse una lista de dominios o palabras que contengan un patrón pero que consideraremos como apropiados.

Como ejemplo: vamos a suponer que en la lista de sitios denegados está la palabra *sex*. esta denegaría el acceso a cualquier nombre de dominio que incluya dicha cadena de caracteres, como extremesex.com. Sin embargo también estaría bloqueando a sitios como sexualidadjoven.cl, el cual no tiene que ver en lo absoluto con pornografía, sino orientación sexual para la juventud. Podemos añadir este nombre de dominio en un ficheros que denominaremos */etc/squid/sitios-inocentes*. Este fichero será definido en una Lista de Control de Acceso del mismo modo en que se hizo anteriormente con el fichero que contiene dominios y palabras denegadas.

```
acl inocentes url_regex "/etc/squid/sitios-inocentes"
```

Para hacer uso del fichero, solo bastará utilizar la expresión ! en la misma línea utilizada para la *Regla de Control de Acceso* establecida para denegar el mismo.

```
http_access deny negados !inocentes
```

La regla anterior especifica que se denegará el acceso a todo lo que comprenda la *Lista de Control de Acceso* denominada *denegados* excepto lo que comprenda la *Lista de Control de Acceso* denominada *inocentes*. Es decir, se podrá acceder sin dificultad a www.sexualidadjoven.cl manteniendo la restricción para la cadena de caracteres *sex*.

Finalmente, solo bastará reiniciar Squid para que tomen efecto los cambios y podamos hacer pruebas.

- **Cómo configurar Squid: Restricción de acceso a contenido por extensión**

Denegar el acceso a ciertos tipos de extensiones de fichero permite hacer un uso más racional del ancho de banda con el que se dispone. Su funcionamiento consiste en denegar el acceso a ciertos tipos de extensiones que coincidan con lo establecido en una Lista de Control de Acceso.

Definiendo elementos de la Lista de Control de Acceso.

Lo primero será generar una lista la cual contendrá la lista de extensiones a la cual denegaremos el acceso. Ejemplos:

```
\.avi$
\.mp4$
\.mp3$
\.mpg$
\.mov$
\.doc$
\.exe$
\.xls$
```

Esta lista, la cual deberá ser completada con todas las extensiones de fichero que el administrador considere pertinentes, la guardaremos como /etc/squid/listaextensiones.

Parámetros en /etc/squid/squid.conf

Debemos definir una Lista de Control de Acceso que a su vez defina al fichero /etc/squid/listaextensiones. Esta lista la denominaremos como "listaextensiones". De modo tal, la línea correspondiente quedaría del siguiente modo:

```
acl listaextensiones urlpath_regex "/etc/squid/listaextensiones"
```

A continuación especificaremos modificaremos una Regla de Control de Acceso existente agregando con un símbolo de !que se denegará el acceso a la Lista de Control de Acceso denominada listaextensiones:

```
http_access allow mired !listaextensiones
```

La regla anterior permite el acceso a la Lista de Control de Acceso denominada mired, pero le niega el acceso a todo lo que coincida con lo especificado en la Lista de Control de Acceso denominada listaextensiones.

4.1.1.4 SERVICIO DE MAIL (CORREO ELECTRÓNICO)

4.1.1.4.1 DESCRIPCION

Un **servidor de correo** es una aplicación que nos permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando.

4.1.1.4.2 PROTOCOLOS DE CORREO ELECTRÓNICO

Hoy día, el correo electrónico es entregado usando una arquitectura cliente/servidor. Un mensaje de correo electrónico es creado usando un programa de correo cliente. Este programa luego envía el mensaje a un servidor. El servidor luego lo redirige al servidor de correo del recipiente y allí se le suministra al cliente de correo del recipiente.

Para permitir todo este proceso, existe una variedad de protocolos de red estándar que permiten que diferentes máquinas, a menudo ejecutando sistemas operativos diferentes y usando diferentes programas de correo, envíen y reciban correo electrónico o email.

- **Protocolos de transporte de correo**

La entrega de correo desde una aplicación cliente a un servidor, y desde un servidor origen al servidor destino es manejada por el *Protocolo simple de transferencia de correo* (*Simple Mail Transfer Protocol* o *SMTP*).

- **SMTP**

El objetivo principal del protocolo simple de transferencia de correo, SMTP, es transmitir correo entre servidores de correo. Sin embargo, es crítico para los clientes de correo también. Para poder enviar correo, el cliente envía el mensaje a un

servidor de correo saliente, el cual luego contacta al servidor de correo de destino para la entrega. Por esta razón, es necesario especificar un servidor SMTP cuando se esté configurando un cliente de correo.

En Red Hat Enterprise Linux, un usuario puede configurar un servidor SMTP en la máquina local para manejar la entrega de correo. Sin embargo, también es posible configurar servidores remotos SMTP para el correo saliente.

Un punto importante sobre el protocolo SMTP es que no requiere autenticación. Esto permite que cualquiera en la Internet puede enviar correo a cualquiera otra persona o a grandes grupos de personas. Esta característica de SMTP es lo que hace posible el correo basura o *spam*. Los servidores SMTP modernos intentan minimizar este comportamiento permitiendo que sólo los hosts conocidos accedan al servidor SMTP. Los servidores que no ponen tales restricciones son llamados servidores *open relay*.

Red Hat Enterprise Linux utiliza Sendmail (/usr/sbin/sendmail) como su programa SMTP por defecto. Sin embargo, también está disponible una aplicación más simple de servidor de correo llamada Postfix (/usr/sbin/postfix).

- ***Protocolos de acceso a correo***

Hay dos protocolos principales usados por las aplicaciones de correo cliente para recuperar correo desde los servidores de correo: el *Post Office Protocol* (*POP*) y el *Internet Message Access Protocol* (*IMAP*).

A diferencia de SMTP, estos protocolos requieren autenticación de los clientes usando un nombre de usuario y una contraseña. Por defecto, las contraseñas para ambos protocolos son pasadas a través de la red sin encriptar.

- **POP**

El servidor por defecto POP bajo Red Hat Enterprise Linux es /usr/sbin/ipop3d y es proporcionado por el paquete imap. Cuando se utiliza POP, los mensajes de

correo son descargados a través de las aplicaciones de correo cliente. Por defecto, la mayoría de los clientes de correo POP son configurados para borrar automáticamente el mensaje en el servidor de correo después que éste ha sido transferido exitosamente.

POP es completamente compatible con estándares importantes de mensajería de Internet, tales como *Multipurpose Internet Mail Extensions* (*MIME*), el cual permite los anexos de correo.

POP funciona mejor para usuarios que tienen un sistema en el cual leer correo. También funciona bien para usuarios que no tienen una conexión permanente a la Internet o a la red que contiene el servidor de correo.

Desafortunadamente para aquellos con conexiones lentas, POP requiere que luego de la autenticación los programas cliente descarguen el contenido completo de cada mensaje. Esto puede tomar un buen tiempo si algún mensaje tiene anexos grandes.

- **IMAP**

El servidor por defecto IMAP bajo Red Hat Enterprise Linux es /usr/sbin/imapd y es proporcionado por el paquete imap. Cuando utilice un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios pueden leerlos o borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo.

IMAP lo utilizan principalmente los usuarios que acceden a su correo desde varias máquinas. El protocolo es conveniente también para usuarios que se estén conectando al servidor de correo a través de una conexión lenta, porque sólo la información de la cabecera del correo es descargada para los mensajes, hasta que son abiertos, ahorrando de esta forma ancho de banda. El usuario también tiene la habilidad de eliminar mensajes sin verlos o descargarlos.

Por conveniencia, las aplicaciones cliente IMAP son capaces de hacer caché de los mensajes localmente, para que el usuario pueda hojear los mensajes previamente leídos cuando no se esté conectado directamente al servidor IMAP.

IMAP, como POP, es completamente compatible con estándares de mensajería de Internet, tales como MIME, que permite los anexos de correo.

4.1.1.4.3 CONFIGURACIÓN SENDMAIL

Sendmail es el agente de transporte de correo (MTA). La responsabilidad de **sendmail** consiste en aceptar correo de agentes de correo de usuario (MUA) y en entregar dichos correos al agente de transporte de correo apropiado, según se especifique en su archivo de configuración.

SendMail funciona con el protocolo SMTP (Simple Mail Transfer Protocol), el cual es utilizado para comunicarse con otros servidores SendMail, manteniéndose a la escucha de posibles comunicaciones por el socket 25 (Se puede comprobar si un MTA está activo haciendo un Telnet al puerto 25 de una máquina). Este programa abre una conexión contra el mail server remoto. Lo que hace es enviar su nombre de máquina local, así como el nombre del emisor, el buzón de destino y un comando

diciendo que empieza el texto del mensaje. En este punto el servidor finaliza el tratamiento de lo que ha asumido como comandos y comienza a aceptar el mensaje hasta que recibe una marca especial (sencillamente, un punto como principio de línea). Después de esto, ambos programas entienden que el envío de comandos ha sido retomado.

Sendmail utiliza los siguientes ficheros de configuración:

Filename	Function
/etc/mail/access	Base de datos de accesos de **sendmail**
/etc/mail/aliases	Carpeta de alias
/etc/mail/aliases	Listados de máquinas para las que **sendmail** acepta correo
/etc/mail/mailer.conf	Configuración del programa de correo
/etc/mail/mailertable	Tabla de entregas de correo
/etc/mail/sendmail.cf	Archivo de configuración principal de **sendmail**
/etc/mail/virtusertable	Usuarios virtuales y tablas de dominio

Tabla 4.1: Ficheros de configuración del Sendmail

¿Por qué es importante tener un Servidor de Correo?

Su empresa encontrará conveniente el poder contar con un Servidor de Correo electrónico con capacidad de recuperar mensajes por medio de los protocolos IMAP, POP3 e interfaz Web. Sus usuarios podrán acceder fácilmente a sus mensajes ya sea desde su cliente de correo electrónico favorito o bien desde el navegador Web de su elección.

Pasos a seguir

1.- En el fichero /etc/mail/local-host-names editamos el dominio al cual estaremos recibiendo correo en el cual ponemos lo siguiente:

192.168.0.1
labsistemas.net

2.- En el fichero /etc/mail/access habilitamos a alguna red para que sea capaz de controlar las máquinas que pueden usar nuestro servidor de correo. Por defecto sendmail solo dejará enviar correo

desde si mismo, para evitar el SPAM. Si queremos usar el servidor de correo para mandar, debemos especificar la ip desde la que accederemos, generalmente la red local en la que se encuentra el servidor o una lista de ips de confianza. La configuración es la siguiente:

localhost.localdomain	RELAY
localhost	RELAY
127.0.0.1	RELAY
192.168.0.1	RELAY
192.168.0	RELAY
labsistemas.net	RELAY
spam.com	REJECT

3.- Hay que asegurarse de que sendmail escucha en el puerto 25 y que no tiene al puerto asociado a localhost. Para verificarlo hacemos netstat -ln y veremos los puertos en escucha que hay en el sistema. Si sale algo como:

tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN

Entonces es correcto.

El fichero sendmail.mc es un fichero de macros, una vez modificado debemos ejecutar un comando que se especifica al principio del propio fichero, normalmente:

m4 /etc/mail/sendmail.mc > /etc/sendmail.cf

También al modificar los otros ficheros que se encuentran en /etc/mail hay que moverse ahí y ejecutar "make".

Cada vez que se metan cambios en estos ficheros, hay que aplicar make o m4 y **además reiniciar el sendmail**.

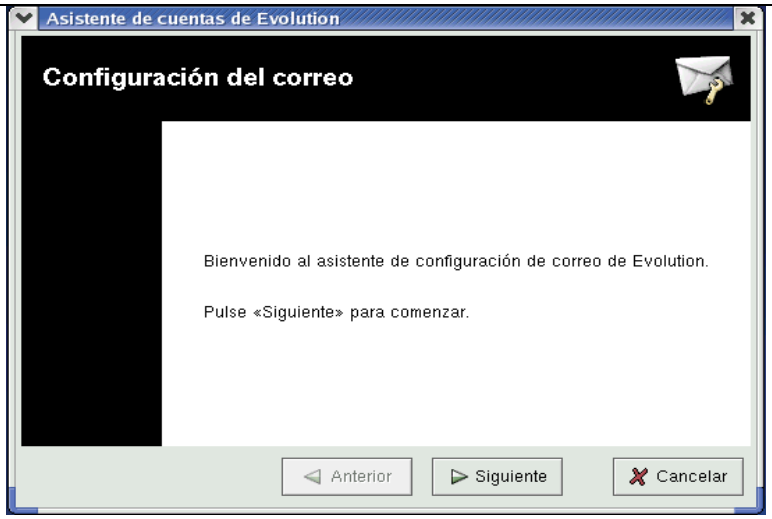
- **PRUEBA**

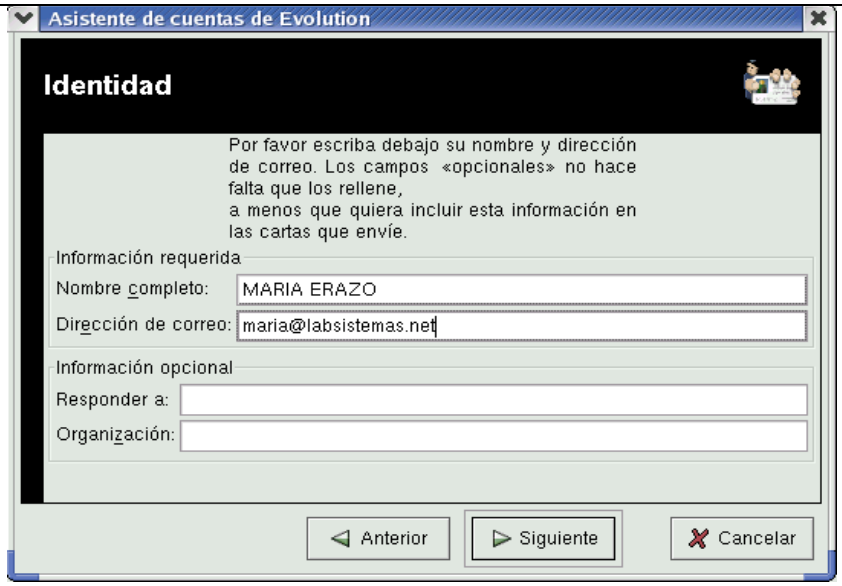
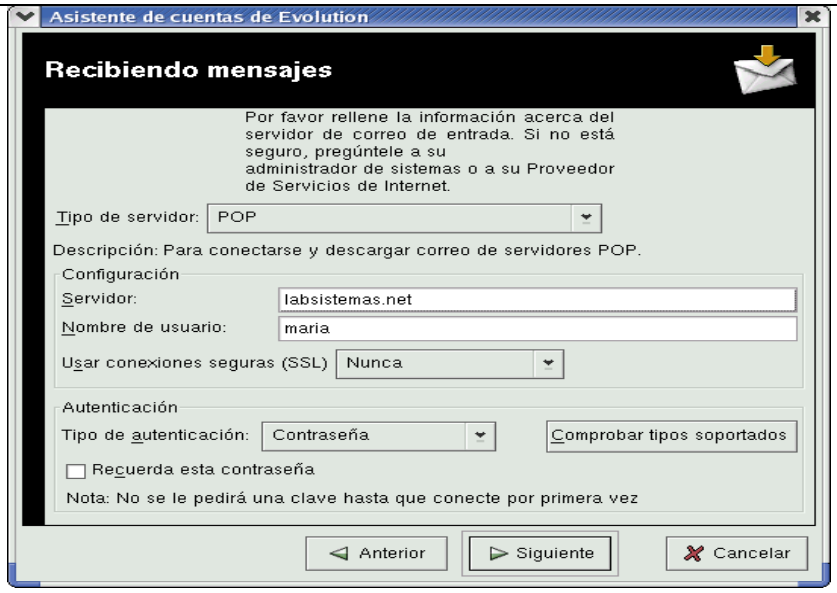
Una forma de comprobar que el Servidor de correo esta funcionando es crear dos cuentas de mail y procedemos a enviar y recibir mensajes.

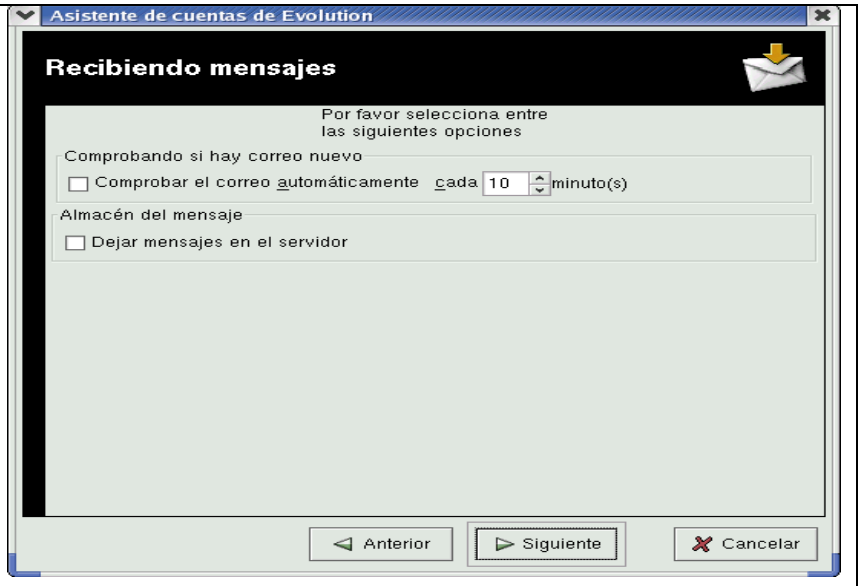
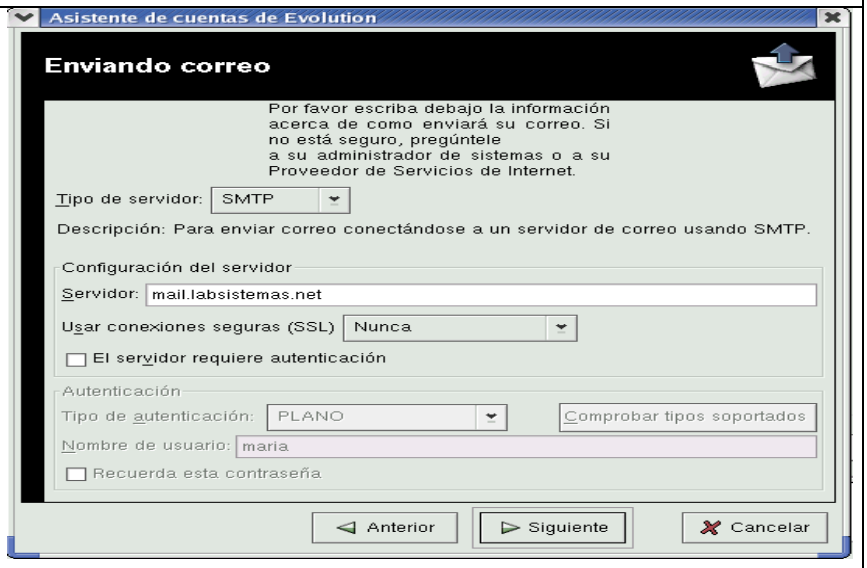
- Creamos dos usuarios de la siguiente manera:

[root@servidor root]# adduser maria [root@servidor root]# passwd maria Changing password for user maria. New password: BAD PASSWORD: it is too short Retype new password: passwd: all authentication tokens updated successfully.	[root@servidor root]# adduser cristian [root@servidor root]# passwd cristian Changing password for user cristian New password: BAD PASSWORD: it is too short Retype new password: passwd: all authentication tokens updated successfully.

- Para crear una cuenta de correo en el Servidor, utilizaremos el usuario maria.

PASOS A SEGUIR	**GRAFICOS DE LA CREACIÓN DE CUENTAS DE CORREO EN EL SERVIDOR UTILIZANDO SENDMAIL**
▪ Damos clic en el icono Correo electrónico Evolution => elegimos Herramientas => Configuración => Añadir y obtendremos la siguiente pantalla:	

▪ Damos clic en siguiente y obtendremos una ventana en la que llenamos la siguiente información. Nombre del usuario y la Dirección de correo como se muestra en la siguiente figura	
▪ En la ventana de Recibiendo mensajes . En Tipo de Servidor elegimos POP. En Servidor ponemos el nombre del dominio o su respectiva dirección IP y en nombre de usuario el respectivo que fue creado y el que estamos usando en el Servidor.	

▪ En la siguiente pantalla de Recibiendo mensajes no llenamos ningún dato y damos clic en siguiente.	
▪ En la ventana Enviando correo en Tipo de Servidor dejamos la que está por defecto SMTP en Servidor llenamos como muestra la figura y damos clic en siguiente.	

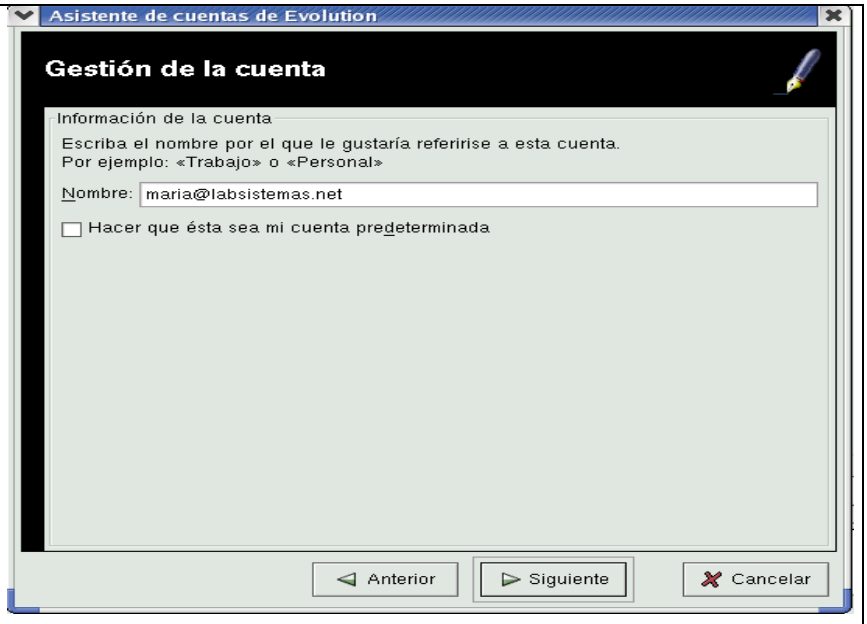
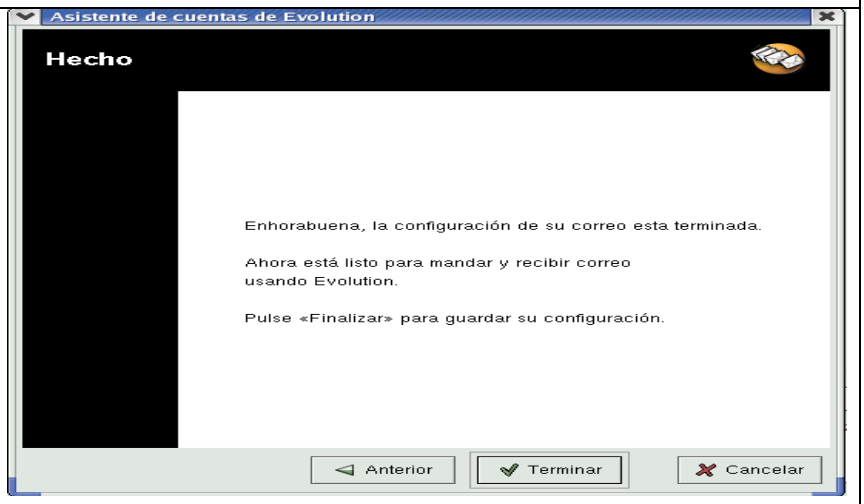
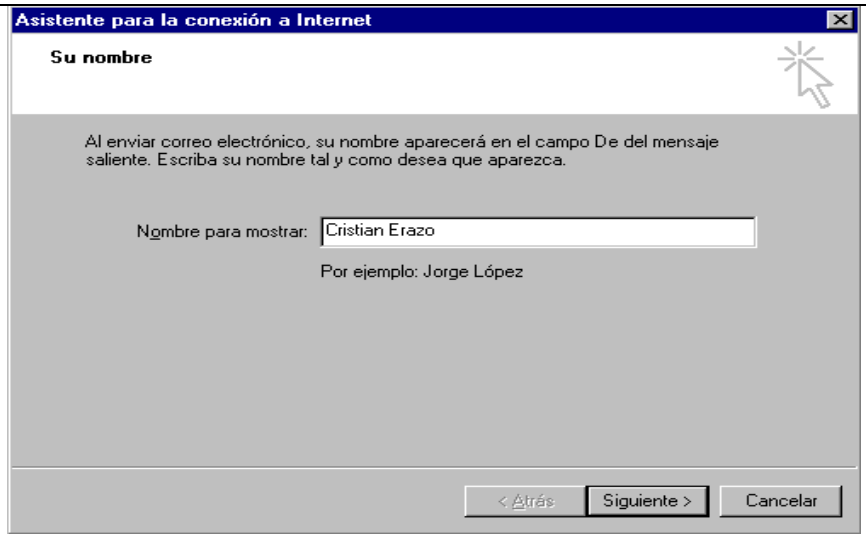
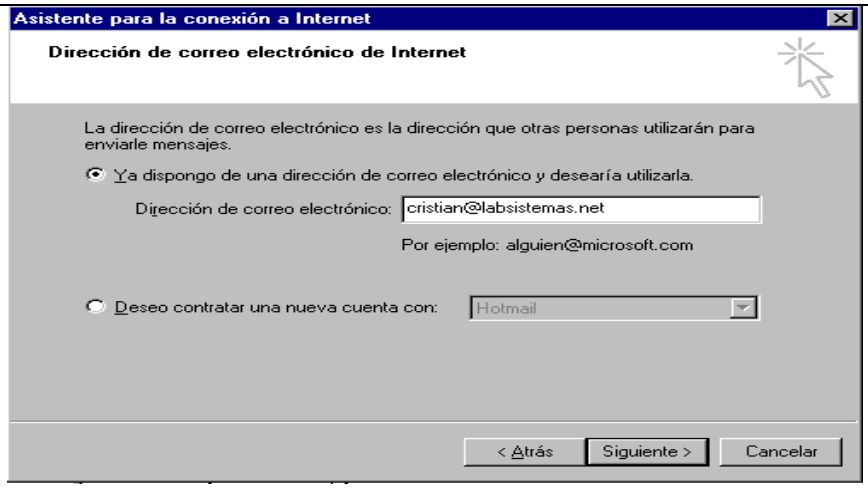
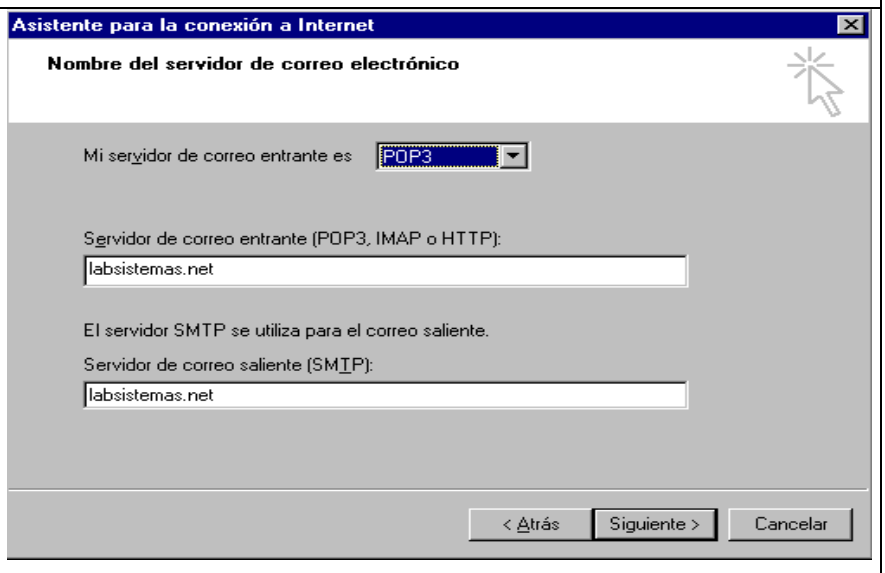
▪ En la ventana de Gestión de Cuenta podremos observar en nombre de la cuenta con el que se va ha enviar el correo y damos clic en siguente	
▪ Por último podemos ver la ventana de finalización indicando que esta listo para enviar y recibir correo.	

Figura 4.2: Configuración de la cuenta de correo en el Servidor en Linux

- Para crear una cuenta de correo en el Cliente, utilizaremos el usuario cristian.

PASOS A SEGUIR	GRAFICOS DE LA CREACIÓN DE CUENTAS DE CORREO EN EL CLIENTE UTILIZANDO SENDMAIL

▪ Damos clic en el icono Outlook Express => elegimos Herramientas => Cuentas => Agregar => Correo y obtendremos la siguiente pantalla en donde editamos el nombre del usuario que se creo anteriormente	
▪ En la siguiente pantalla editamos la dirección de correo electrónico por el que vamos a enviar y recibir mensajes	
▪ En Servidor de correo entrante dejamos la que coje por defecto POP3 y en el Servidor de correo entrante y saliente ponemos el nombre del dominio o su respectiva dirección Ip la que usamos anteriormente en el Servidor.	

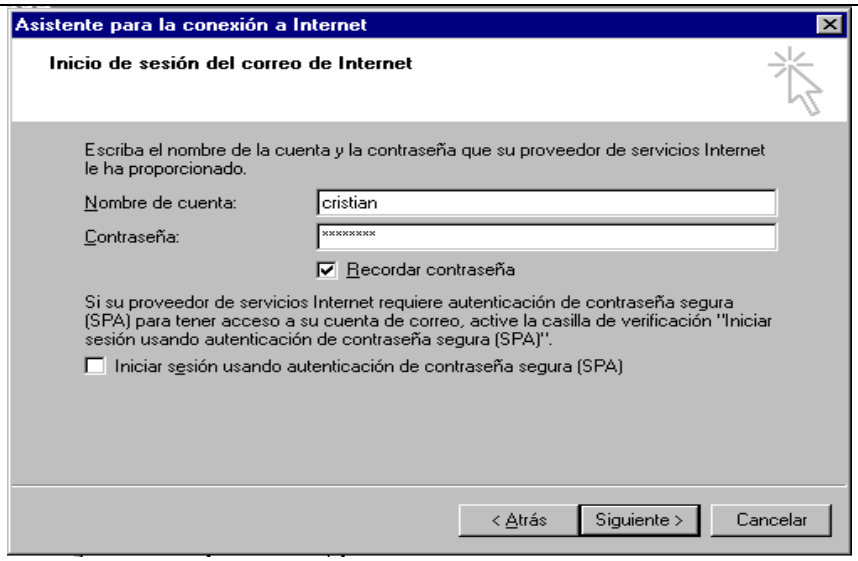
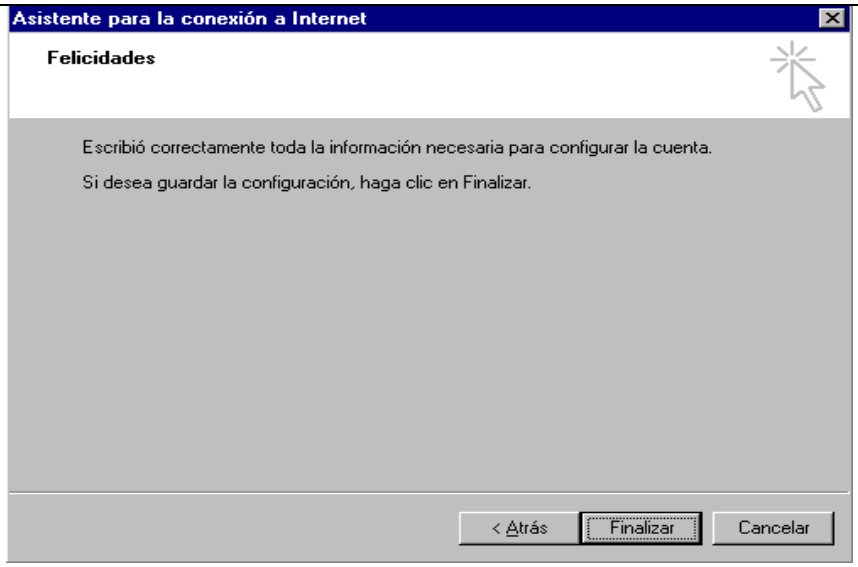
▪ En la ventana de inicio de sesión editamos la respectiva contraseña del usuario que estamos utilizando y damos clic en siguiente	
▪ Por último podemos ver la ventana de finalización indicando que esta listo para enviar y recibir correo.	

Figura 4.3: Configuración de la cuenta de correo en el Cliente en Linux

4.1.2 CONTROL DE SERVICIOS BAJO LA PLATAFORMA WINDOWS

Los servicios de Microsoft Windows, antes conocidos como servicios NT, permiten crear aplicaciones fáciles de ejecución larga que se ejecutan en sus propias sesiones de Windows. Estos servicios pueden iniciarse automáticamente cuando se inicia el sistema, se pueden pausar y reiniciar, y no muestran ninguna interfaz de usuario. Esto hace que los servicios resulten perfectos para ejecutarse en un servidor donde se necesite una funcionalidad de ejecución larga que no interfiera con los demás usuarios que trabajen en el mismo equipo. También puede ejecutar servicios en el contexto de seguridad de una cuenta de usuario específica, diferente de la del usuario que inició la sesión o de la cuenta predeterminada del equipo.

El desarrollo de Microsoft Windows Server 2003 proporcionan experiencia práctica para muchas configuraciones de sistemas operativos.

Para iniciar se establece una infraestructura de red común a través de la instalación y conexión de Windows Server 2003, la configuración de Active Directory, la instalación de una estación de trabajo Windows 2000 Professional y, por último, la incorporación de esta estación de trabajo a un dominio.

4.1.2.1 CONECTIVIDAD

Para elaborar la conexión del servidor windows server 2003 con el cliente windows 2000 professional utilizando redes inalámbricas los pasos son iguales que los configurados antes con la utilización de Linux.

Configuración de la tarjeta Wireless sin la utilización de un AP.

Si se desea configurar el servidor y el cliente sin la utilización del AP mediante la topología Ad -hoc los pasos a seguir son los siguientes:

Pc. Servidor

La siguiente configuración es la misma que la anteriormente descrita:

Dirección IP, Máscara de subred, Puerta de enlace predeterminada, Servidores DNS.

Además de esto, tendremos que configurar algunos parámetros de la tarjeta de red como son:

Authentication mode: Shared Authentication.

Desired BSS Type: Infrastructure.

Desired SSID: El nombre que se le pondrá a la red (tendrá que ser el mismo en todos los PCs).

WEP Option: WEP Enabled.

Bien, ya tenemos configurado el PC servidor con tarjeta wireless.

PC cliente.

La configuración de los PC cliente es la misma que el PC servidor con tarjeta Wireless, variando algunas cosas como:

La dirección IP: Tendrá que estar dentro del mismo rango

Puerta de enlace predeterminada: Aquí ahora sí pondremos una dirección IP (la el PC servidor).

Todos los demás PCs se configurarán de la misma forma, cambiando la dirección IP y así sucesivamente.

4.1.2.2 ACTIVE DIRECTORY

Microsoft® Windows 2003 presenta Active Directory, un servicio de directorio ampliable y escalable que habilita la seguridad y la administración distribuidas y sirve como un almacén de información de red que se puede consultar de manera eficaz. La base de datos Active Directory se almacena y duplica en servidores que se designan como controladores de dominio.

Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

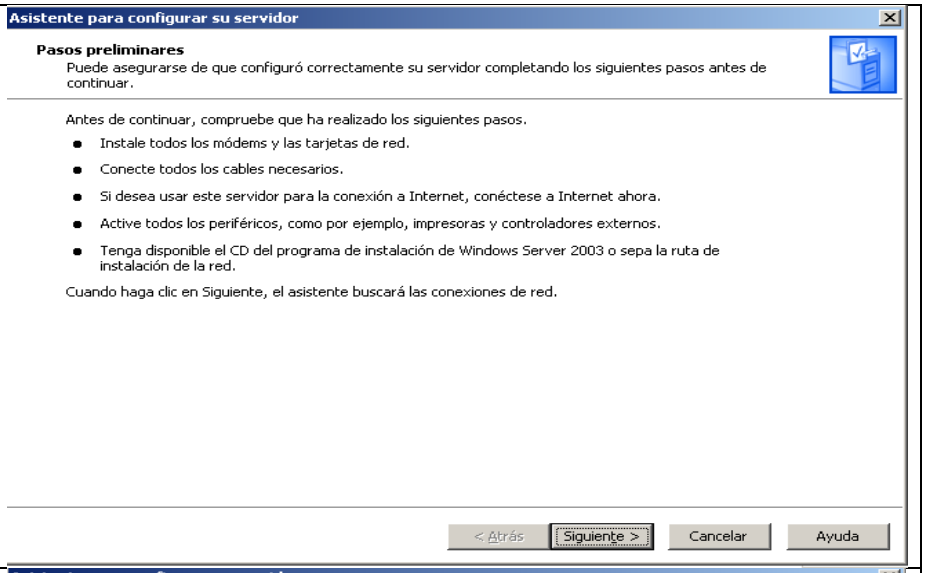
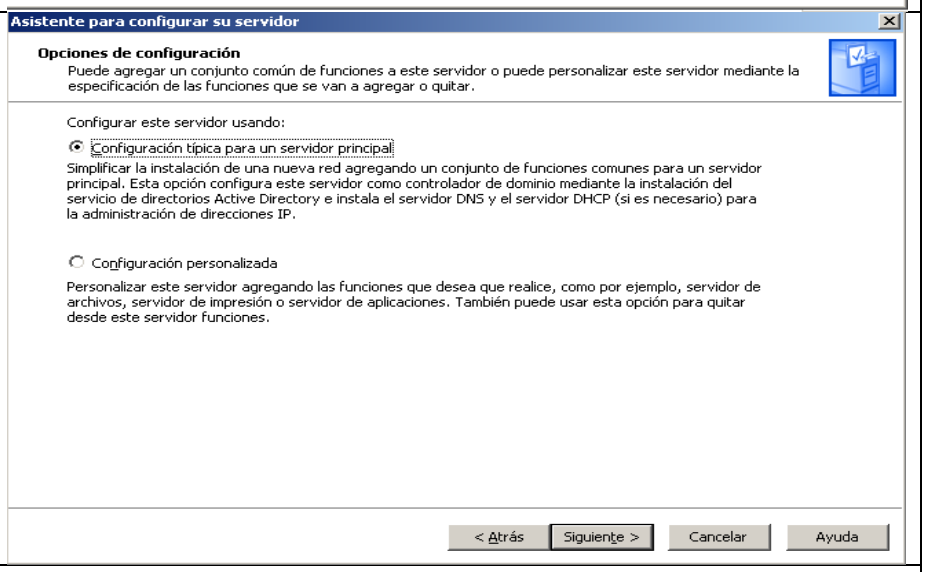
Los requisitos básicos para iniciar la instalación del Active Directory son los siguientes:

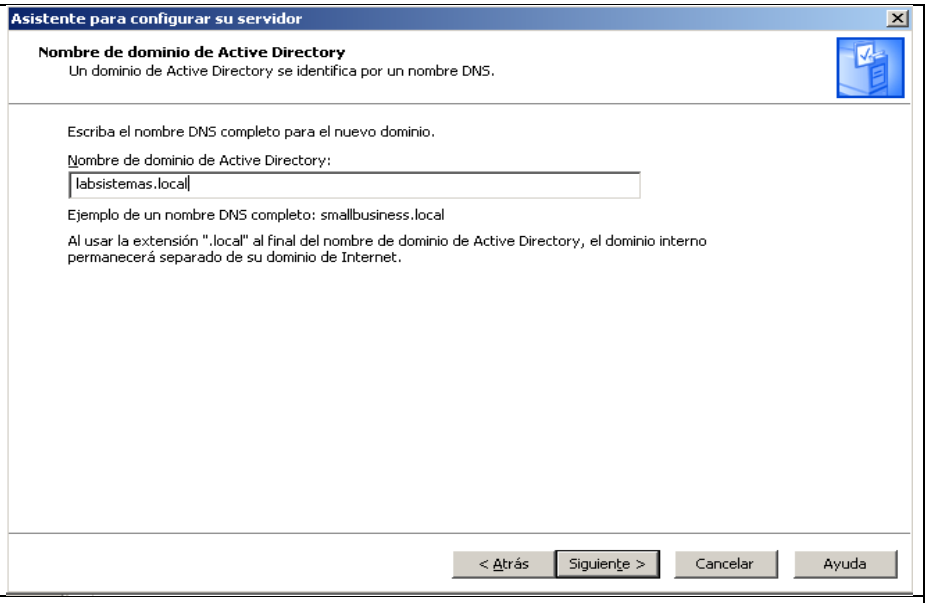
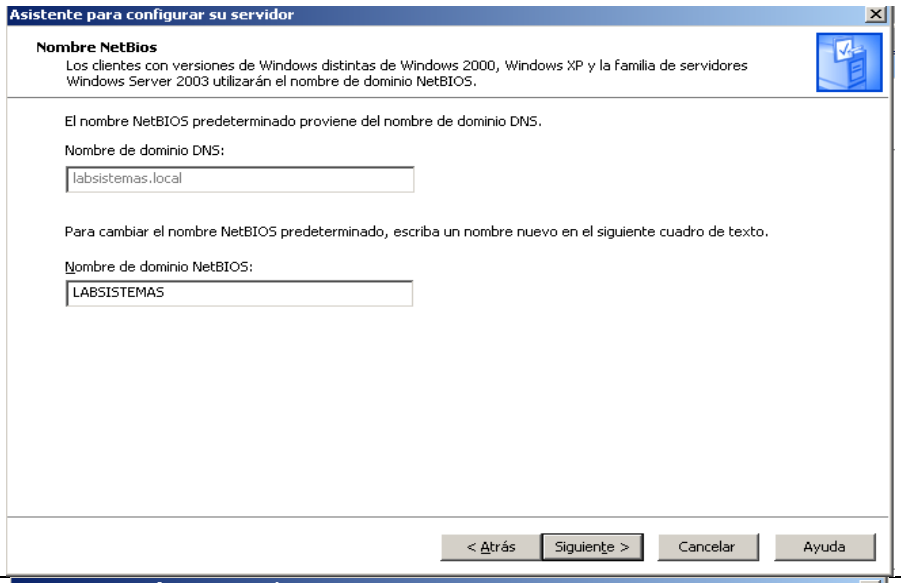
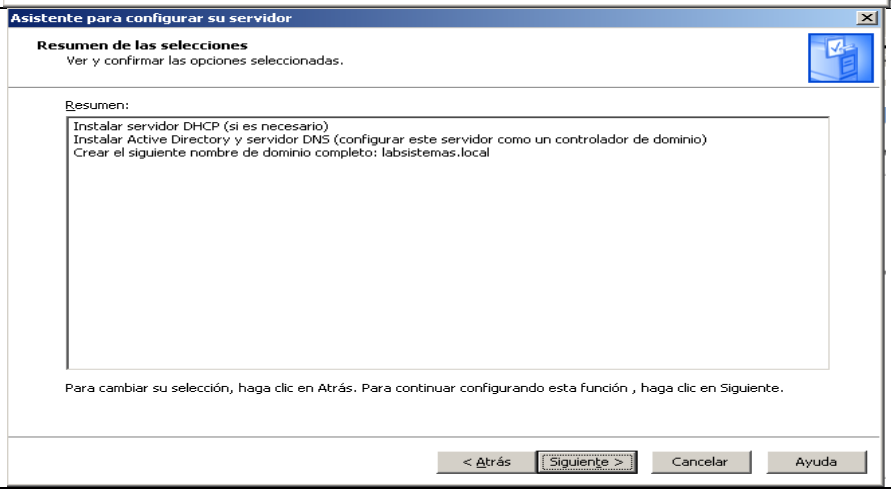
- Tener instalado Windows Server 2003 y disponer del CD de instalación ya que durante la instalación del Active Directory será necesario para la instalación de algunos componentes.
- Disponer de una buena capacidad de memoria y procesador
- Establecer conexión de red wireless entre el servidor y el cliente

Una vez realizado estos pasos básicos procedemos a la instalación del Active Directory.

4.1.2.2.1 INSTALACION Y CONFIGURACIÓN DEL ACTIVE DIRECTORY

PASOS A SEGUIR	GRAFICOS DE LA INSTALACION Y CONFIGURACION DEL ACTIVE DIRECTORY
▪ En el menú inicio elegimos la opción Administre su servidor y obtendremos una pantalla como la siguiente:	
▪ Elegimos la opción Agregar o quitar función y obtendremos una pantalla en la que se mostrará los pasos previos que se deberá disponer, seleccionamos siguiente.	

<table>
<tr>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>▪ En la ventana opciones de configuración elegimos la primera opción en la que directamente se instalara el Sistema de Nombres de Dominio DNS y damos clic en el botón siguiente.</td>
<td> 
</td>
</tr>
<tr>
<td>▪ En la ventana nombre de dominio de Active Directory escribimos el nombre de dominio del DNS que para nuestro caso utilizaremos labsistemas.local y damos clic en el botón siguiente.</td>
<td></td>
</tr>
</table>

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>▪ En la próxima ventana aparece “Nombre NetBIOS” por default nos muestra el nombre que escribimos en la ventana anterior para el nombre DNS, dejamos tal como muestra y damos clic en el botón siguiente.</td><td> 
</td></tr>
<tr><td>▪ En esta pantalla observamos que nos muestra las opciones extras que se van ha instalar y damos clic en siguiente</td><td> 
</td></tr>
<tr><td></td><td></td></tr>
</table>

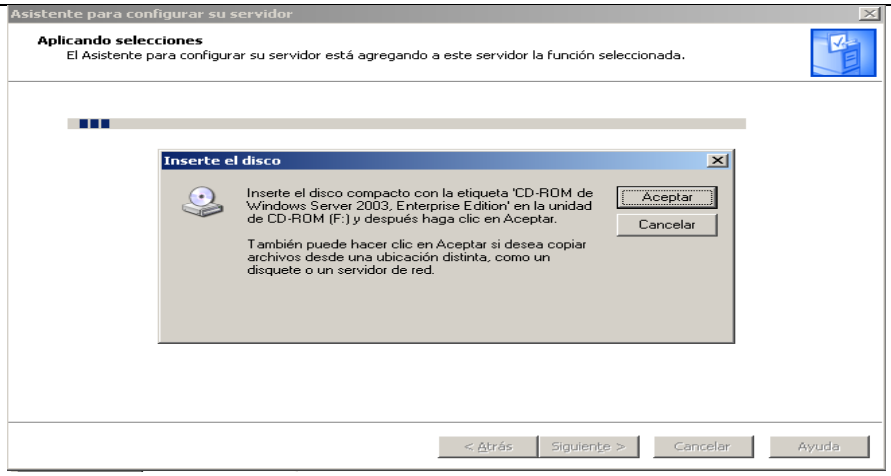
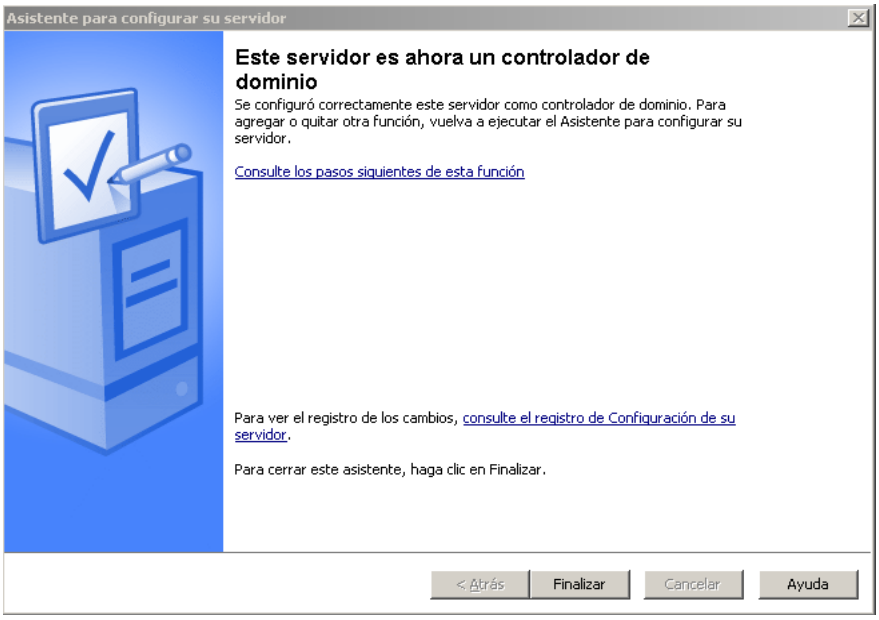
▪ En la siguiente pantalla observamos como inicia la instalación en la misma que se nos muestra que debe estar en el disco extraíble el CDROM de Windows 2003	
▪ Por último nos muestra la ventana que nos indica que la instalación ha terminado, es importante no cancelar la operación ni apagar el servidor y cuando termine de configurarse damos clic en la última ventana en el botón finalizar como se puede apreciar en la siguiente pantalla.	

Figura 4.4: Instalación y Configuración del Active Directory

Durante la instalación del Active Directory se crean los siguientes objetos que a continuación se describen:

Icono	Carpeta	Descripción
	Dominio	El nodo raíz del complemento representa el dominio que se va a administrar.
	Equipos	Contiene todos los equipos con Windows NT, Windows 2000, Windows XP y Windows Server 2003 que se unen a un dominio. Entre éstos se incluyen los equipos que ejecutan Windows NT

Icono	Carpeta	Descripción
		versiones 3.51 y 4.0. Si actualiza de una versión anterior, Active Directory migra la cuenta de equipo a esta carpeta. Es posible mover estos objetos.
	Sistema	Contiene información de sistemas y servicios de Active Directory.
	Usuarios	Contiene todos los usuarios del dominio. En una actualización, se migran todos los usuarios del dominio anterior. Al igual que los equipos, es posible mover los objetos de usuario.

Se puede usar Active Directory para crear los siguientes objetos.

Icono	Objeto	Descripción
	Usuario	Un objeto de usuario es un objeto que es un principal de seguridad en el directorio. Un usuario puede iniciar sesión en la red con estas credenciales y a los usuarios se les puede conceder permisos de acceso.
	Contacto	Un objeto de contacto es una cuenta que no tiene ningún permiso de seguridad. No se puede iniciar sesión como contacto. Los contactos se suelen utilizar para representar a usuarios externos con fines relacionados con el correo electrónico.
	Equipo	Objeto que representa un equipo en la red. Para las estaciones de trabajo y servidores con Windows NT, ésta es la cuenta de equipo.
	Unidad organizativa	Las unidades organizativas se utilizan como contenedores para organizar de manera lógica objetos de directorio tales como usuarios, grupos y equipos, de forma muy parecida a como se utilizan las carpetas para organizar archivos en el disco duro.
	Grupo	Los grupos pueden contener usuarios, equipos y otros grupos. Los grupos simplifican la administración de cantidades grandes de objetos.
	Carpeta compartida	Una carpeta compartida es un recurso compartido de red que se ha publicado en el directorio.
	Impresora	Una impresora compartida es una impresora de red que se ha

Icono	Objeto	Descripción
	compartida	publicado en el directorio.

Tabla 4.2: Objetos del Active Directory

4.1.2.2.2 CREACIÓN DE USUARIOS Y GRUPOS EN ACTIVE DIRECTORY

Un servicio de directorio como Active Directory proporciona métodos para almacenar los datos del directorio, poniéndolos a disposición de los administradores y los usuarios de la red. Por ejemplo, Active Directory almacena información acerca de las cuentas de usuario de dominio (nombres, contraseñas, números de teléfono, etc.) y permite que otros usuarios autorizados de la misma red tengan acceso a esa información.

Creación de cuentas de usuarios

Esta tarea se puede realizar sobre un controlador de dominio, un servidor o estaciones de trabajo miembros de un mismo dominio que tengan las Herramientas Administrativas instaladas.

Antes de crear el usuario creamos una **unidad organizativa** para organizar de manera lógica a los usuarios.

- Damos clic en **Inicio**, **Herramientas Administrativas** y seleccionamos **Usuarios y equipos de Active Directory**.

- Damos clic con el botón secundario del mouse (ratón) sobre el controlador de dominio (Domain Controllers), elegimos nuevo y seleccionamos Unidad Organizativa (OU) o contenedor, escribimos el nombre, aceptamos y obtendremos una pantalla como la siguiente:

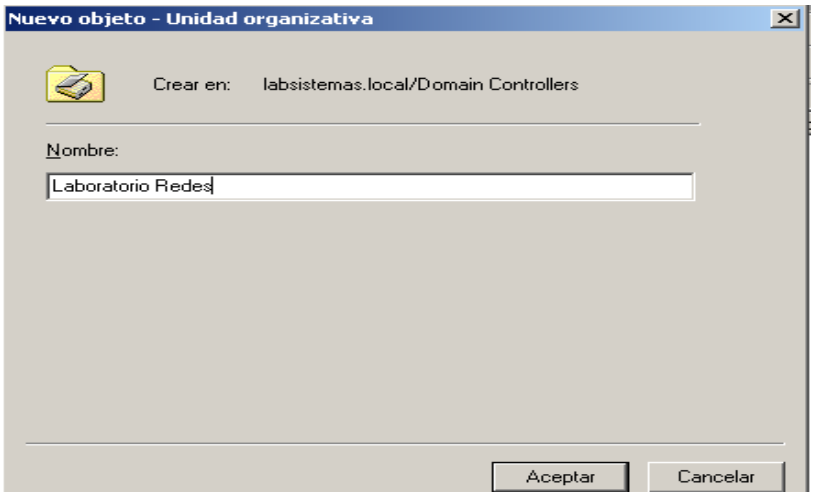
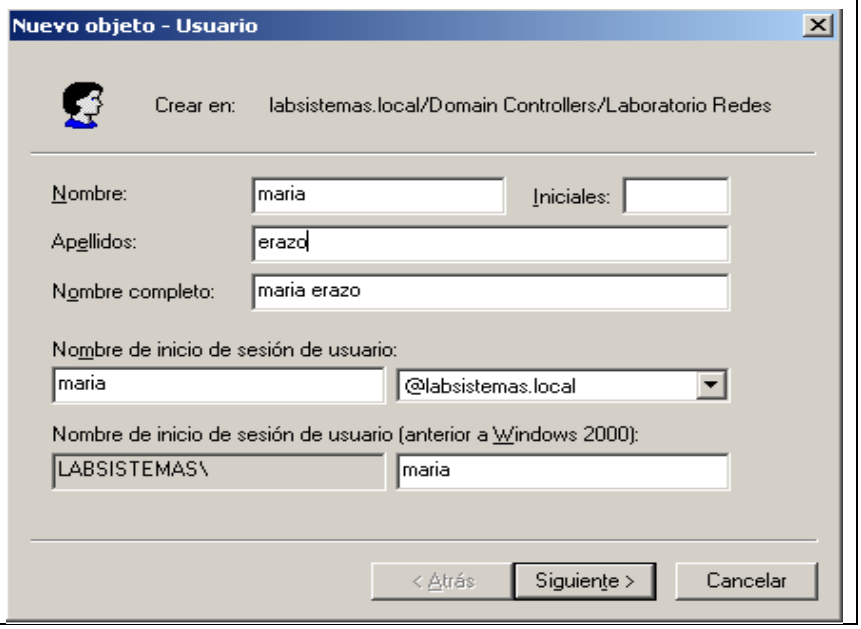


Figura 4.5: Creación de una Unidad Organizativa

PASOS A SEGUIR	GRAFICOS DE LA CREACIÓN DE UN USUARIO
• Una vez creado la Unidad Organizativa damos clic derecho sobre la misma seleccionamos Nuevo y luego hacemos clic en Usuario. En donde editamos el nombre y si desea el apellido así como también el nombre de inicio de sesión y damos clic en siguiente.	

• Escribimos la contraseña con el que el usuario va ha tener acceso a un inicio de sesión y damos clic en siguiente.	

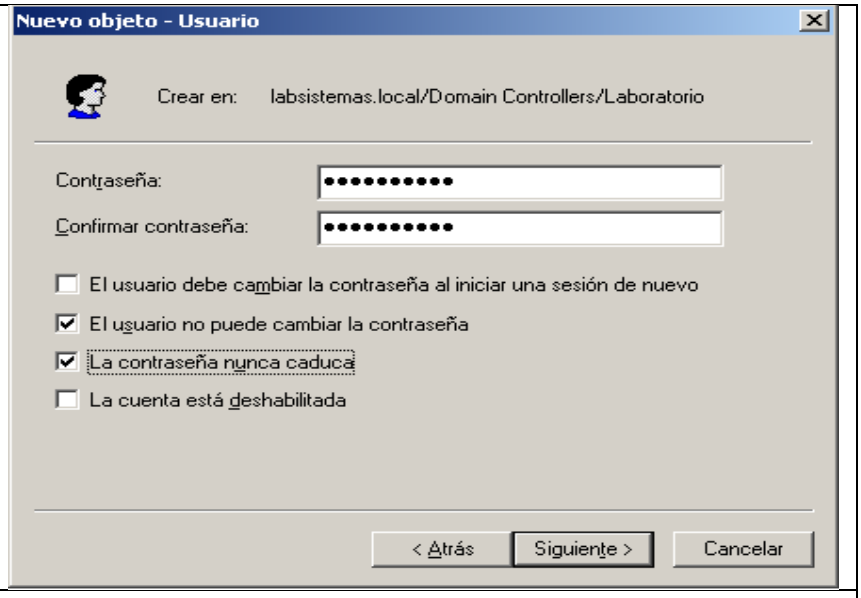
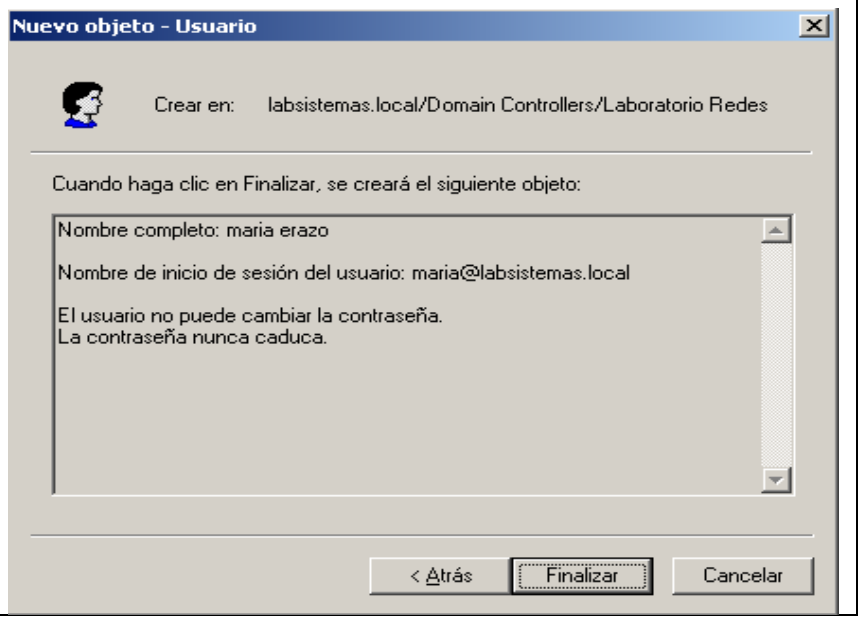
<table>
<tr>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>• Leemos la descripción del objeto y damos clic en Finalizar y nos quedara algo como lo siguiente.</td>
<td> 
</td>
</tr>
</table>

Figura 4.6: Creación de un Usuario

Creación de grupos

- Damos clic en **Inicio**, **Herramientas Administrativas** y seleccionamos **Usuarios y equipos de Active Directory**.
- Damos clic con el botón secundario del mouse sobre el dominio, la Unidad Organizatival (OU) o contenedor donde se va a crear el grupo.
- Seleccionamos **Nuevo** y luego hacemos clic en **Grupo**, escribimos el nombre del grupo y seleccionamos el Ámbito de Grupo y el Tipo de Grupo y hacer clic en **Aceptar**.

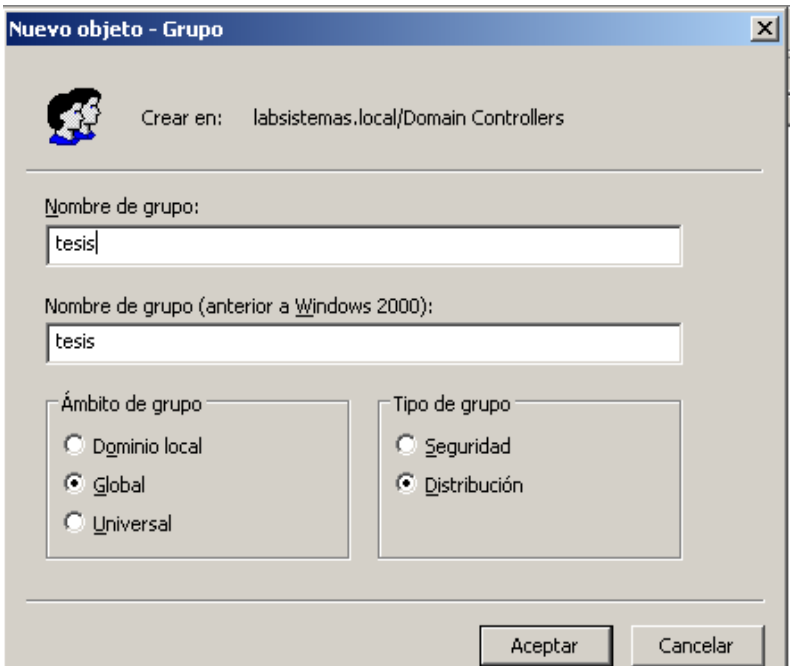


Figura 4.7: Creación de un Grupo

El **Tipo de grupo** indica si se puede utilizar el grupo para asignar permisos a otros recursos de la red. Tanto los grupos de seguridad como los de distribución se pueden utilizar para confeccionar listas de distribución de correo electrónico.

El **Ámbito de grupo** determina la visibilidad del grupo y qué tipo de objetos puede contener el grupo.

Ámbito	Visibilidad	Puede contener
Dominio local	Dominio	Grupos Usuario, Dominio local, Global o Universal
Global	Bosque	Grupos Usuarios o Global
Universal	Bosque	Grupos Usuarios, Global o Universal

Tabla 4.3 Ámbito de un Grupo

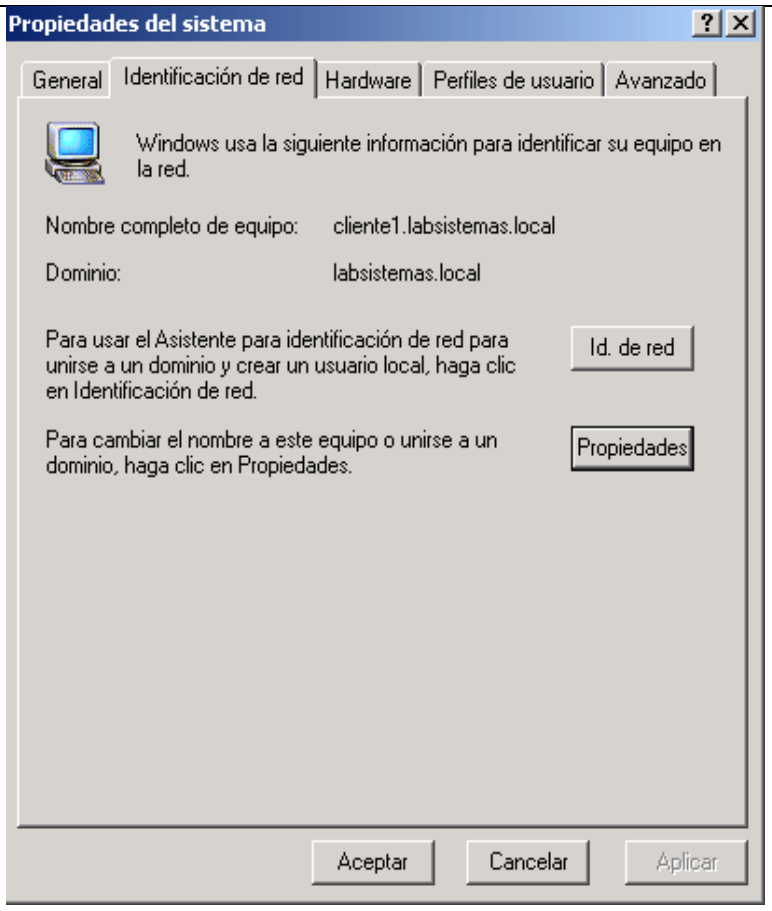
4.1.2.3 INCORPORACIÓN DE LA ESTACIÓN DE TRABAJO A UN DOMINIO

- **DESCRIPCIÓN**

Los usuarios pueden acceder en forma segura a los recursos de otros dominios sin sacrificar el único inicio de sesión y los beneficios administrativos de tener una sola identidad de usuario y contraseña albergada en el dominio principal. Esto provee la flexibilidad para darnos cuenta de la necesidad de tener nuestro propio dominio, y aun conservar los beneficios de Active Directory.

- **PASOS A SEGUIR**

Para incorporar a una maquina (usuario) dentro de un dominio del servidor se debe realizar lo siguiente:

PASOS A SEGUIR	**GRÁFICOS DE LA INCORPORACIÓN A UN DOMINIO**
▪ En Mi PC => propiedades => identificación de red => Propiedades.	
▪ En miembro de dominio escribimos "**labsistemas.local"**	

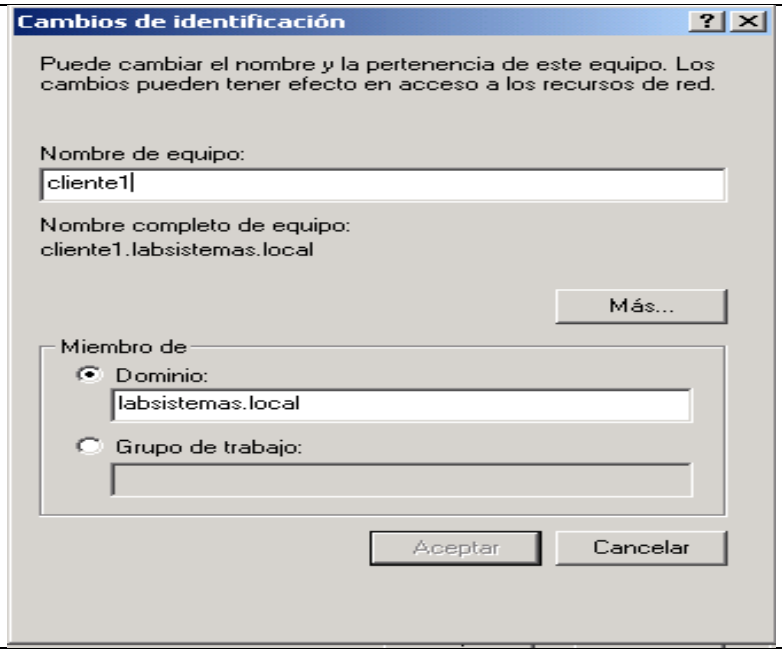
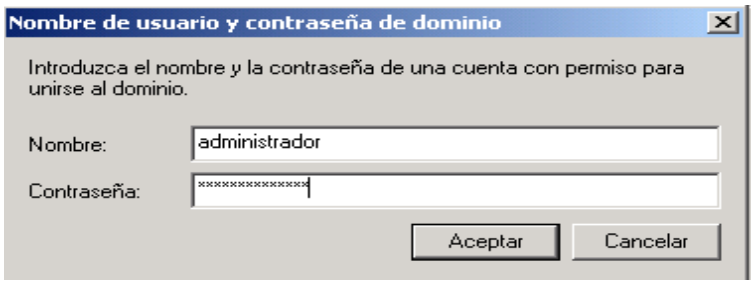
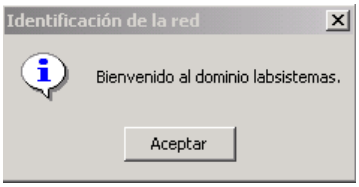
	
▪ Sale una ventana en la que ingresamos Administrador y la contraseña del Servidor como nos muestra la siguiente pantalla.	
▪ Esperamos un momento hasta que nos salga un mensaje de bienvenida al dominio **labsistemas** como a continuación se puede observar y mandamos a reiniciar para que inicie con la nueva configuración.	

Figura 4.8: Incorporación a un Dominio

4.1.2.4 ADMINISTRACIÓN DE LA DIRECTIVA DE GRUPO

- **DESCRIPCIÓN**

Las directivas de grupo permiten la sencilla determinación de directivas para equipos de escritorio y servidores que pueden ser aplicadas automáticamente a tantos equipos de escritorio y servidores como sea necesario vía Active Directory.

Las directivas de Grupo en Windows Server 2003 provee beneficios en las siguientes áreas:

Mayor Seguridad. Los administradores pueden fácilmente definir y hacer cumplir en forma automática las directivas de seguridad del software.

Mayor Satisfacción del Cliente y Reducción de Costos de Servicios de Soporte. Los administradores pueden poner en funcionamiento entornos estandarizados de equipos de escritorio y servidor. Esta capacidad disminuye los riesgos de configuraciones de software dañadas y errores del usuario, al mismo tiempo que mejora la capacidad informática de la empresa para solucionar problemas.

Un Control Flexible sobre el Entorno Informático. Los administradores pueden definir e implementar estándares organizacionales mediante Directivas de Grupo, y pueden rápidamente reconfigurar los parámetros para adaptarse a requerimientos comerciales cambiantes. Las implementaciones de Directivas de Grupo se adaptan fácilmente desde un entorno de grupo pequeño de trabajo hasta los centros de datos de prestigio, simular y validar el impacto de cualquier tipo de cambios antes de aplicarlos a los entornos de producción.

Mayor Productividad. Los administradores pueden manejar un grupo completo de usuarios y haberes informáticos tan fácilmente como manejarían una única entidad.

Las directivas de grupo les permite a los administradores responder rápidamente a los cambios requeridos en las configuraciones de grupo o en las aplicaciones de directivas; una ventaja que ayuda a las organizaciones a dirigir sus operaciones informáticas con mas eficacia. Además de que la programación de operaciones de directivas de grupo puede proporcionar mayor rentabilidad en el volumen de trabajo de informática.

- **CONFIGURACIÓN**

Una vez que la máquina (cliente) esta dentro del dominio, el Servidor tiene control y puede asignar ciertas directivas de seguridad las cuales se elaboran de la siguiente manera:

- Damos clic derecho sobre Domain Controllers o sobre la Unidad Organizativa en la cual deseemos asignar la política => Propiedades en la cual obtendremos la ventana de Directiva de grupo.
- En Directiva de Grupo seleccionamos => Nuevo => “Nombre de la directiva” y obtendremos la siguiente pantalla:

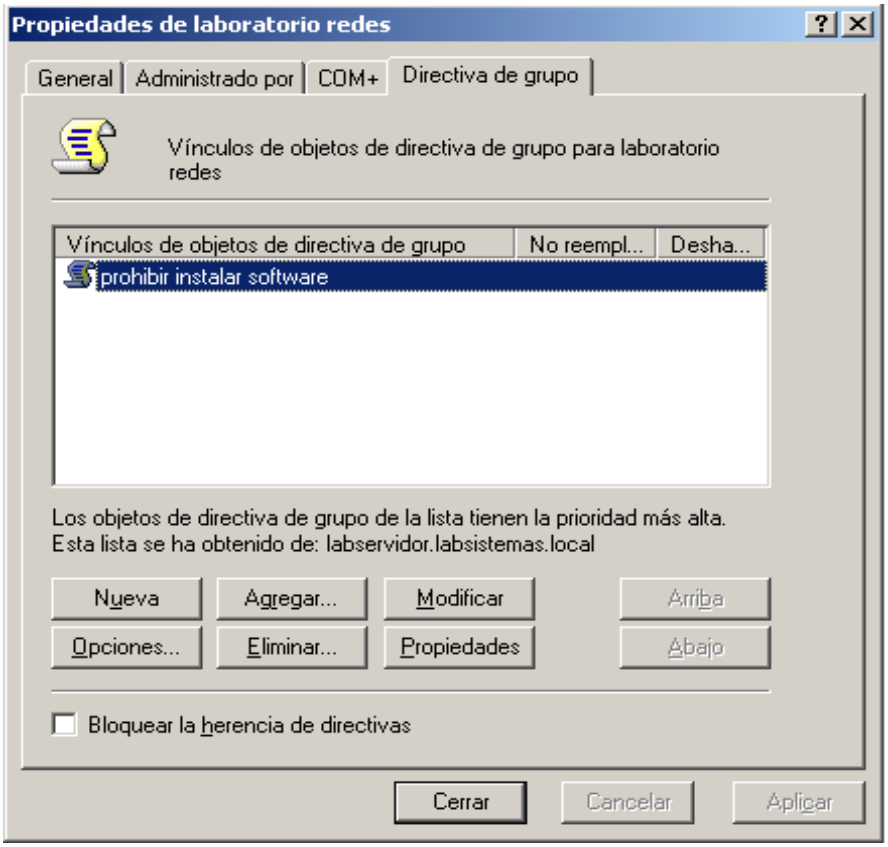


Figura 4.9: Creación de una Directiva de Grupo

Una vez que tenemos listo seleccionamos Modificar y nos mostrará la ventana de Editor de Objetos como se puede observar en la siguiente pantalla:

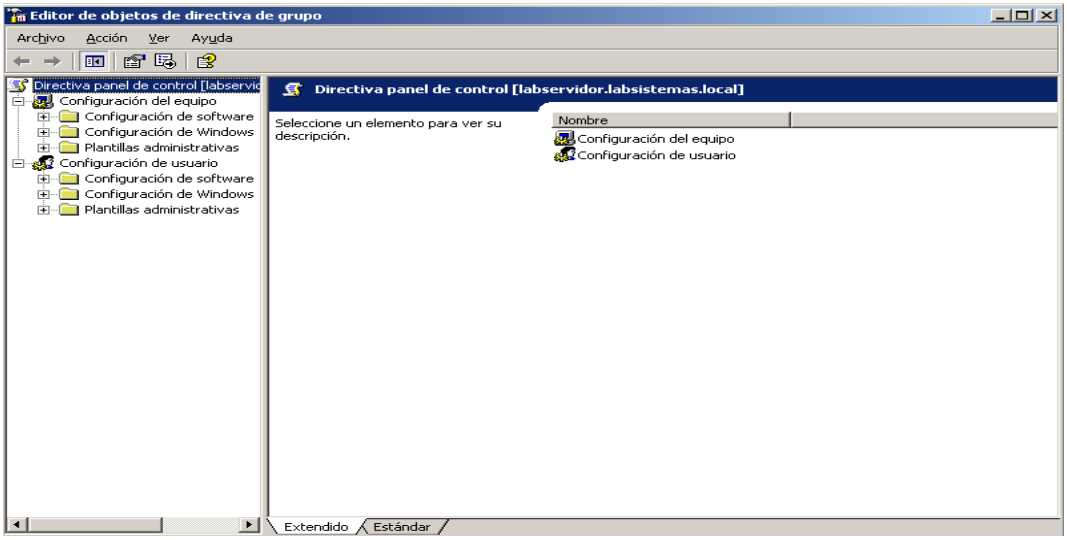


Figura 4.10: Editor de Objetos de una Directiva de Grupo

- Tenemos una lista de directivas en las cuales elegiremos según nuestras necesidades como por ejemplo denegar a los usuarios el acceso a instalación de software, buscamos en el editor y obtenemos la directiva que deseamos como muestra la siguiente pantalla:

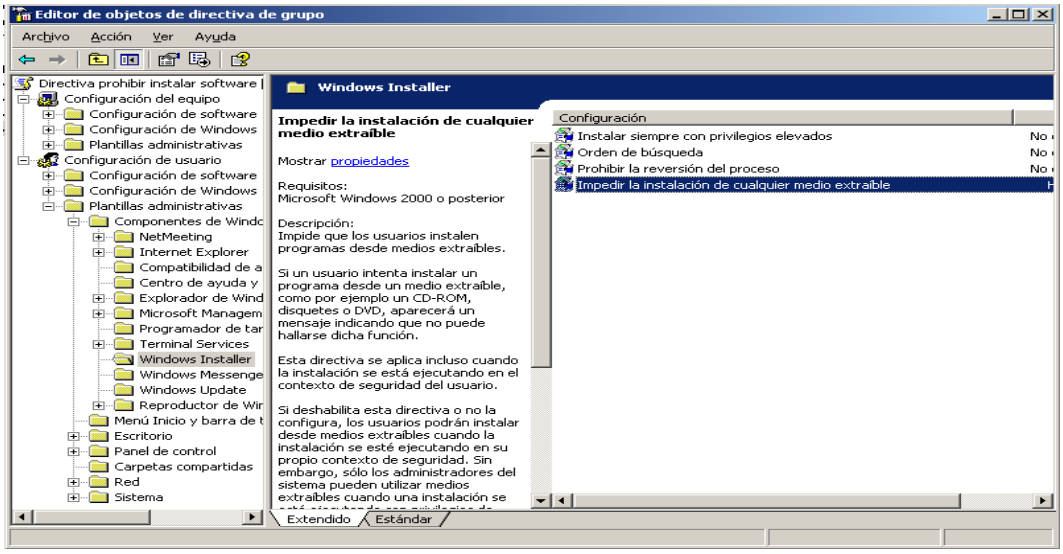


Figura 4.11: Elegir una Directiva de Grupo

- **PRUEBA**

Una vez que hemos asignado la directiva en la máquina (cliente) entramos en modo de usuario y podemos observar que al querer realizar la instalación nos sale un mensaje indicando que los permisos han sido denegados como podemos observar en la siguiente pantalla:

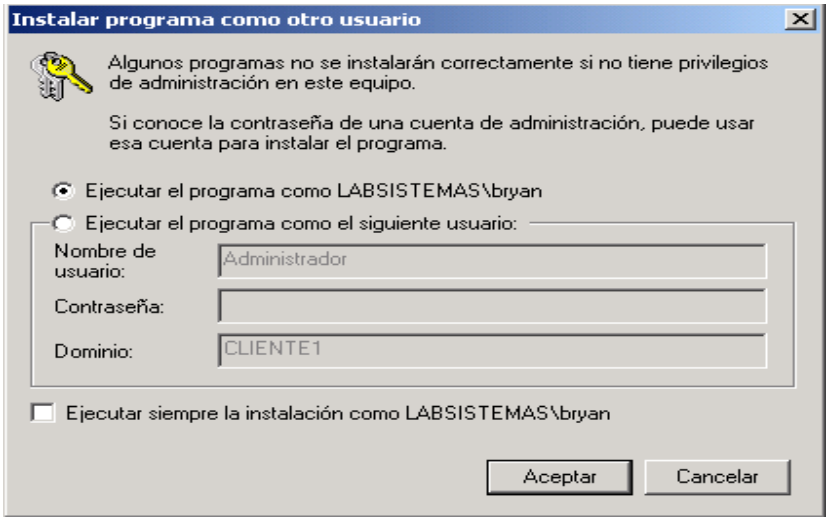


Figura 4.12: Funcionamiento de una Directiva de Grupo

4.1.2.5 SERVICIO DE MAIL (CORREO ELECTRÓNICO)

4.1.2.5.1 DESCRIPCIÓN

Para muchas personas, el envío de mensajes de correo electrónico es lo más importante que hacen en un equipo. A medida que la popularidad e importancia del correo electrónico fue creciendo con el transcurso de los años, han surgido también ciertos inconvenientes y riegos. El correo de Windows está diseñado para ayudarte a vencer estos retos y que el uso del correo electrónico sea lo más productivo y divertido posible. El correo de Windows incluye características que ayudan a reducir los riesgos a la vez que puedes disfrutar de muchos beneficios del correo electrónico.

El correo de Windows está diseñado para que el uso del correo electrónico sea lo más productivo y divertido posible. El correo de Windows incluye características que ayudan a reducir los riesgos a la vez que puedes disfrutar de muchos beneficios del correo electrónico.

La instalación de este servicio es fácil siguiendo las instrucciones, hay que instalar previamente el servicio IIS y dentro de este servicio el servicio SMTP y NNTP. Los servicios de Exchange son varios nos vamos a centrar en el Servidor de Correo POP3 (correo entrante), SMTP (correo saliente).

4.1.2.5.2 EXCHANGE SERVER

El Servidor de Microsoft® Exchange Server 2003, es un producto software basado en mensajería y e-mail, está diseñado específicamente para ayudar a dirigir los requisitos empresariales hacia una mayor seguridad en los entornos informáticos actuales. De acuerdo con la iniciativa de Microsoft Informática de Confianza, Exchange 2003 corriendo sobre Microsoft Windows Server™ 2003 proporciona muchas características nuevas y avances para mejorar la fiabilidad, la manejabilidad y la seguridad.

Al diseñar los nuevos lanzamientos de productos, Microsoft combina las nuevas características y la funcionalidad para dar a nuestros clientes el mayor nivel posible de interoperabilidad y/o coexistencia con las versiones anteriores del producto. Microsoft hace todo lo posible para garantizar que los clientes puedan ampliar las inversiones actuales en infraestructura y tengan la oportunidad de incorporar nuevas tecnologías a sus entornos informáticos. Este documento proporciona una visión general de la compatibilidad de Windows Server 2003 con Exchange 2003, Exchange 2000 Server y Exchange Server 5.5, además de las configuraciones soportadas en un entorno mixto de Exchange y Windows

Outlook es el cliente de correo y colaboración más importante de Microsoft. Con Outlook los usuarios pueden administrar su correo, calendario personal, planificar reuniones con otros usuarios y administrar los contactos. Además, las funcionalidades de administración de tareas y colaboración mejoran la productividad individual por medio de una mejor gestión de la información.

Outlook es también el cliente de referencia para usuarios que disponen de Microsoft Exchange Server para correo electrónico avanzado, calendario y aplicaciones de colaboración a medida dentro de las organizaciones.

PASOS PREVIOS

En el panel de control => Agregar o quitar componentes de Windows => Servidor de aplicaciones habilitar:

- ASP.NET
- Internet Information Services (IIS)
  - NNTP
  - SMTP

INSTALACION

- En la ventana de instalación elegimos Exchange Deployment Tools:

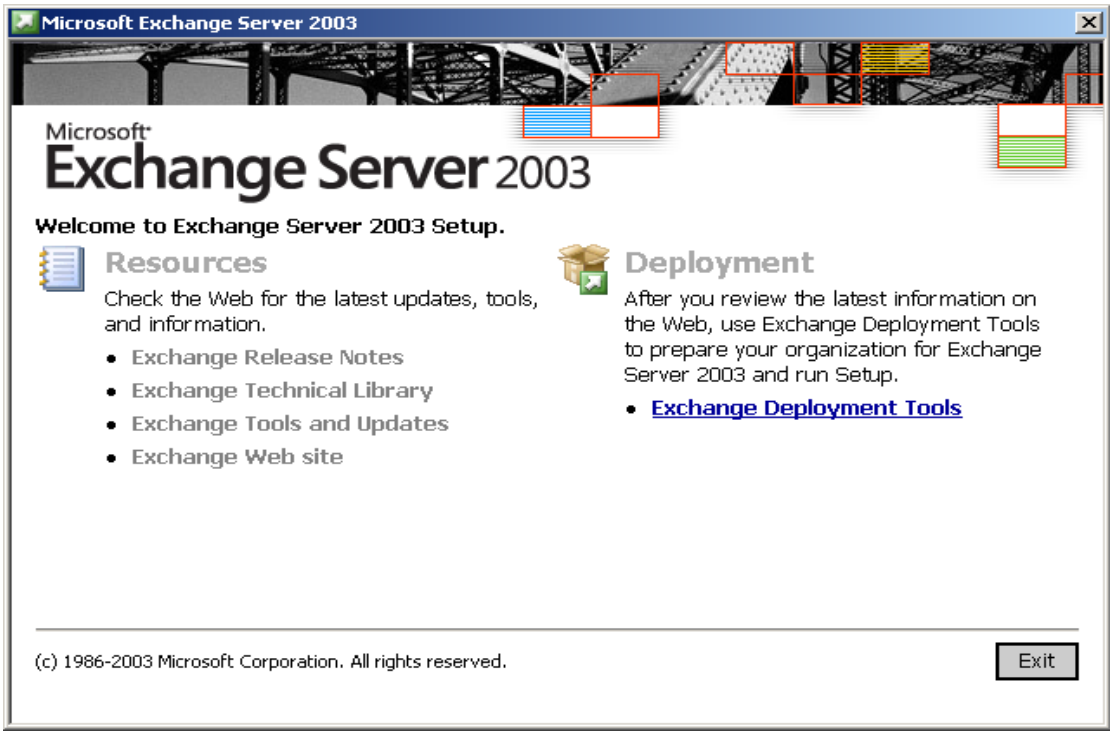


Figura 4.13: Opciones de Instalación del Exchange Server

- En la siguiente ventana elegimos Deploy the first Exchange 2003 server que nos indica que es la primera instalación.
- En la siguiente ventana elegimos New Exchange 2003 Installation
- En la siguiente ventana en donde nos muestra un cierto numero de pasos elegimos el numero 6 en examinar buscamos el path de instalación que se encuentra en SETUP => I386 => Setup, elegimos Run ForestPrep new.
- Nos muestra la siguiente pantalla en ForestPrep elegimos Install.

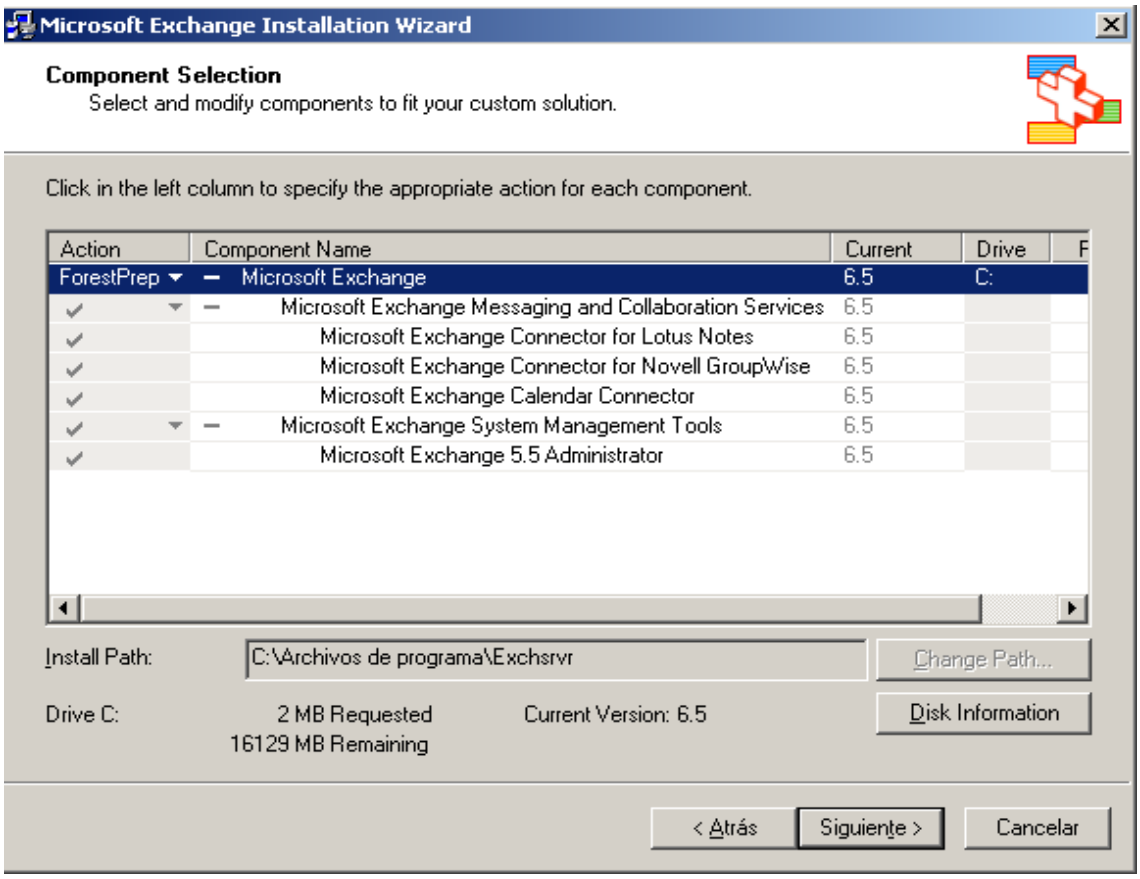


Figura 4.14: Pasos para la Instalación del Exchange Server

- Volvemos a la pantalla anterior en donde nos mostraba un número de pasos y ahora elegimos el número 7 de igual manera elegimos el path y seleccionamos Run DomainPrep new.
- Nos muestra la siguiente pantalla y en DomainPrep elegimos Install.

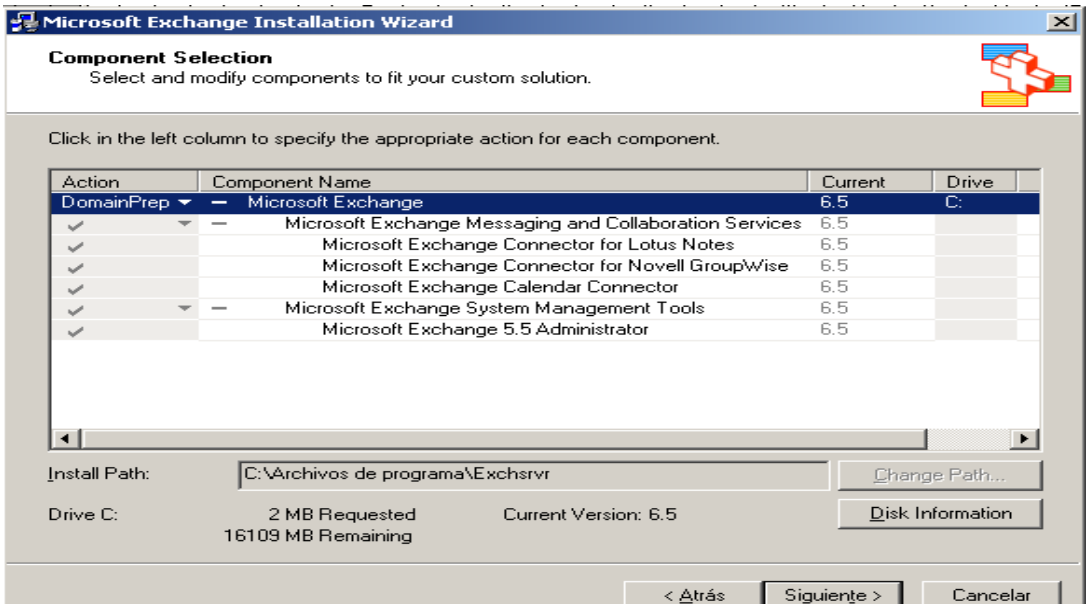


Figura 4.15: Seguimiento de los Pasos del Exchange Server

- Nuevamente volvemos a la ventana en donde nos muestra los pasos y elegimos el número 8, elegimos el path, seleccionamos Run Setup new
- De igual Manera nos muestra la siguiente ventana en la que elegimos Istall

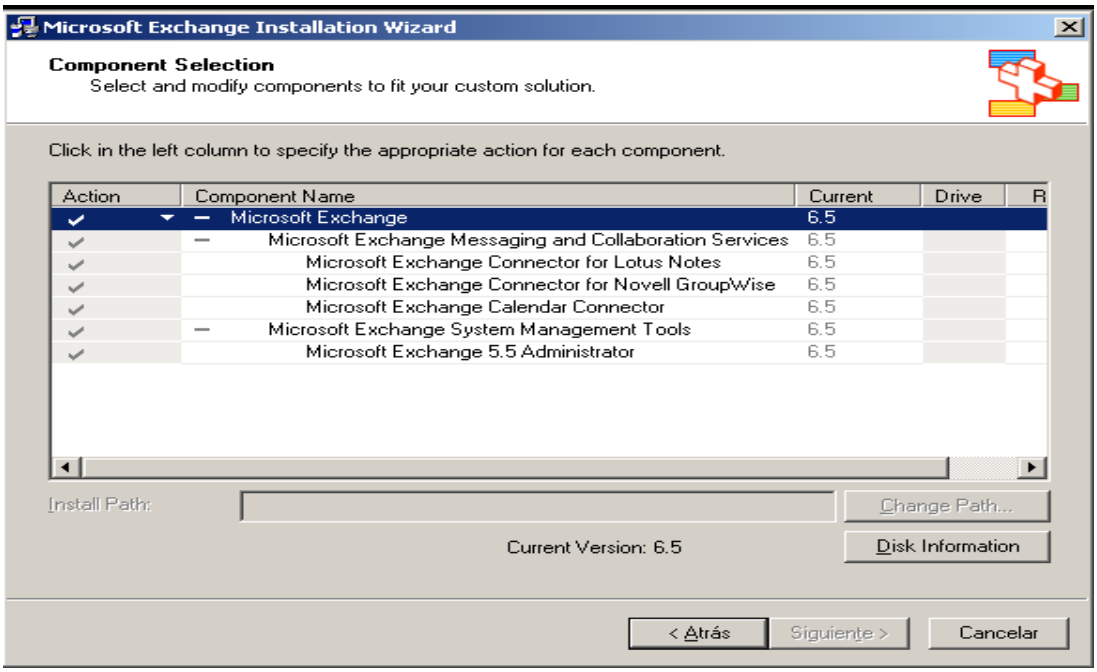
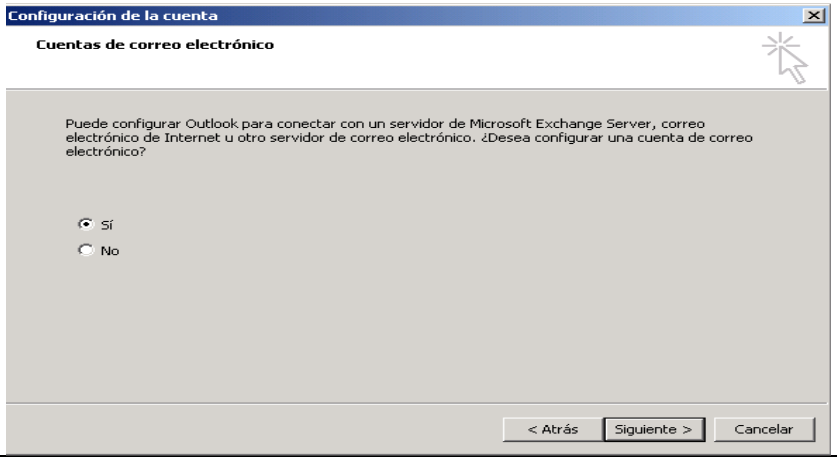
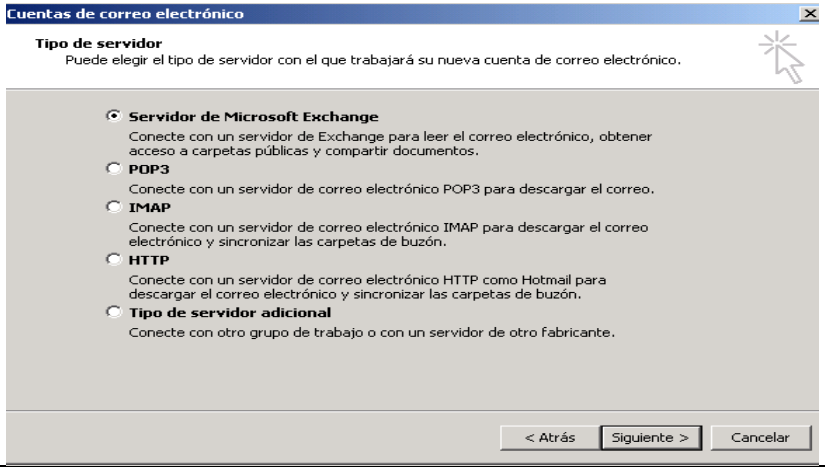


Figura 4.16: Instalación del Exchange Server

- Mandamos a reiniciar y esta listo para utilizar el Exhage Server 2003

4.1.2.5.3 CREACIÓN DE CUENTAS UTILIZANDO EXCHANGE SERVER

PASOS A SEGUIR	GRÁFICOS DE LA CREACIÓN DE CUENTAS UTILIZANDO EXCHANGE SERVER
▪ Por el panel de control elegimos **correo** nos sale una ventana en la que seleccionamos cuentas de correo electrónico y tendremos una pantalla de inicio de Outlook en la que damos clic en siguiente.	
▪ En la ventana cuentas de correo electrónico elegimos que **Si** deseamos configurar una cuenta y damos clic en siguiente.	
▪ En la ventana Tipo de Servidor elegimos **Servidor de Microsoft Exchange** y damos clic en siguiente.	

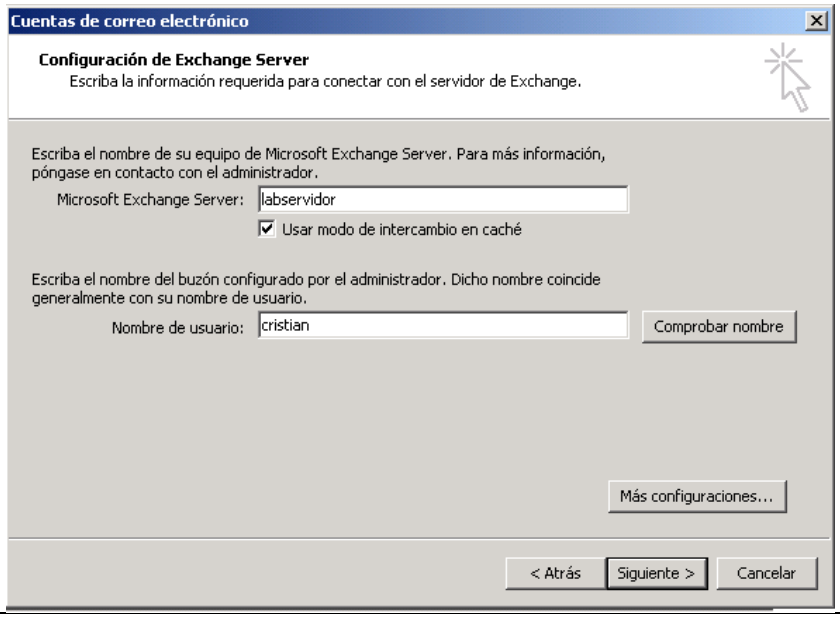
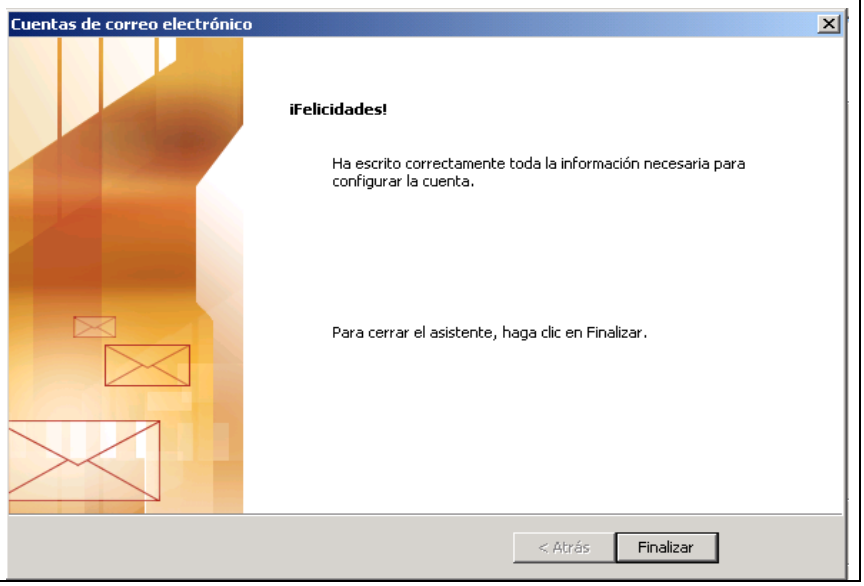
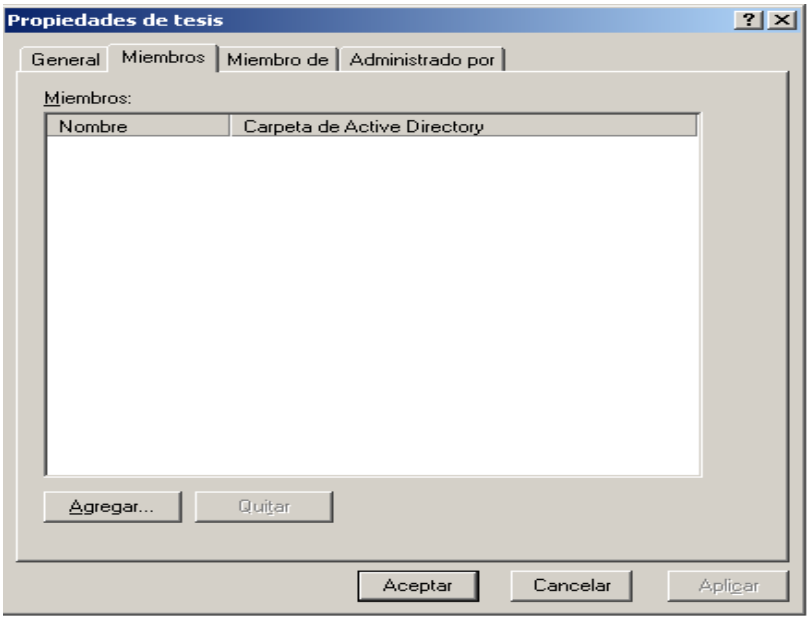
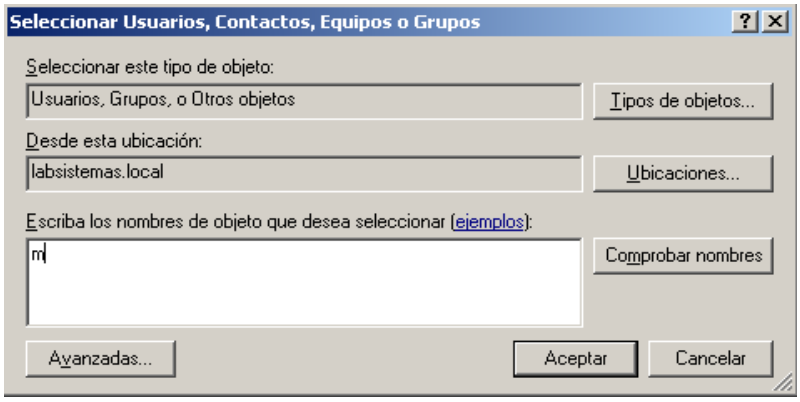
▪ En la ventana Configuración de Exchange Server llenamos el nombre del equipo y el nombre del usuario respectivamente como podemos observar en la siguiente pantalla y damos clic en siguiente.	
▪ Por último nos muestra la ventana de finalización de la cuenta de correo y damos clic en finalizar como nos muestra la siguiente pantalla.	

Figura 4.17: Configuración de la cuenta de correo en Windows

Listas de Distribución

Las listas de distribución son de mucha utilidad ya que hace que el correo electrónico se pueda utilizar de una manera eficaz y se procede de la siguiente manera:

PASOS A SEGUIR	CREACIÓN DE LISTAS DE DISTRIBUCIÓN
• Damos clic derecho sobre el grupo => Propiedades, seleccionamos Miembros y damos clic en Agregar.	
• Editamos la inicial del usuario que vamos a buscar y ponemos Comprobar Nombres para comprobar que es un miembro del Grupo de Seguridad	
• Sale una lista con los nombres de la inicial que editamos en la cual elegiremos el usuario que deseamos.	

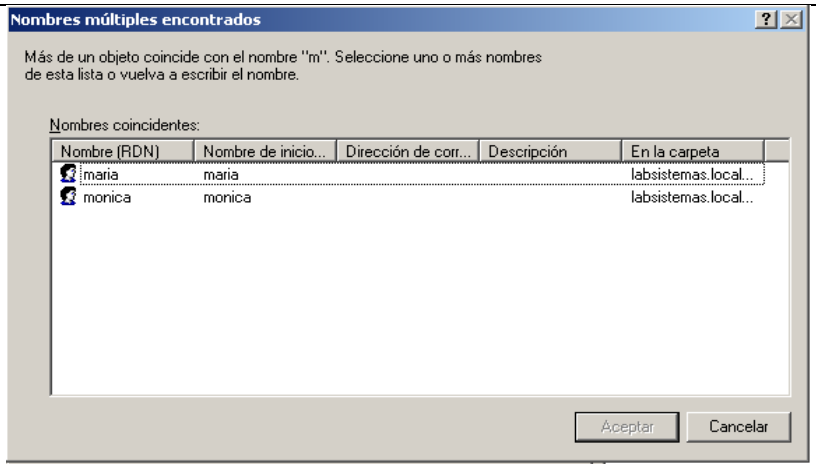
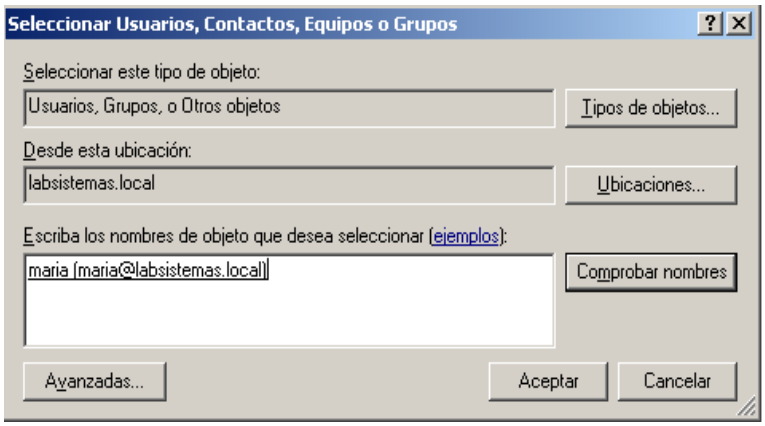
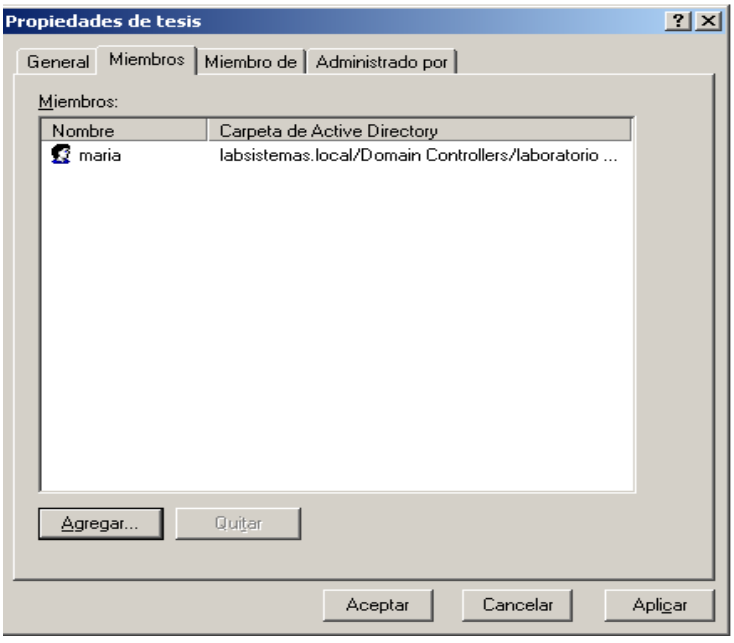
	
• Podemos observar el nombre del usuario seguido del dominio	
• Observaremos que el usuario maria pertenece al grupo tesis, así seguimos sucesivamente con los usuarios que deseemos, en la utilización del correo seleccionamos el grupo al que deseemos enviar el mismo mensaje.	

Figura 4.18: Creación de una Lista de Distribución

4.1.2.5 ISA SERVER

- **CREACIÓN DE POLÍTICAS**

Para la creación de políticas dentro del ámbito de Windows usamos el software isa Server y los pasos a seguir son los siguientes:

1. Damos clic en Create New Access Rule que tenemos a lado derecho de la ventana de Isa Server, obtendremos una pantalla como la siguiente en la cual escribiremos el nombre de la regla que vamos a utilizar como por ejemplo e-mail elegimos siguiente:

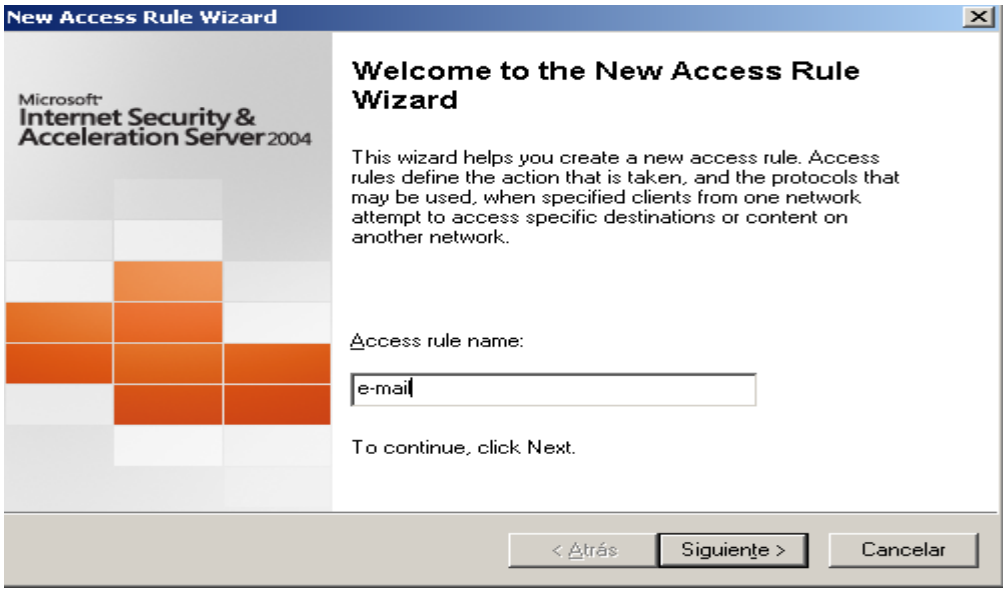


Figura 4.19: Ejemplo de la creación de una regla utilizando ISA SERVER

2. En la siguiente pantalla nos aparece la acción de la regla si permitimos o denegamos elegimos según nuestra conveniencia y seleccionamos siguiente:

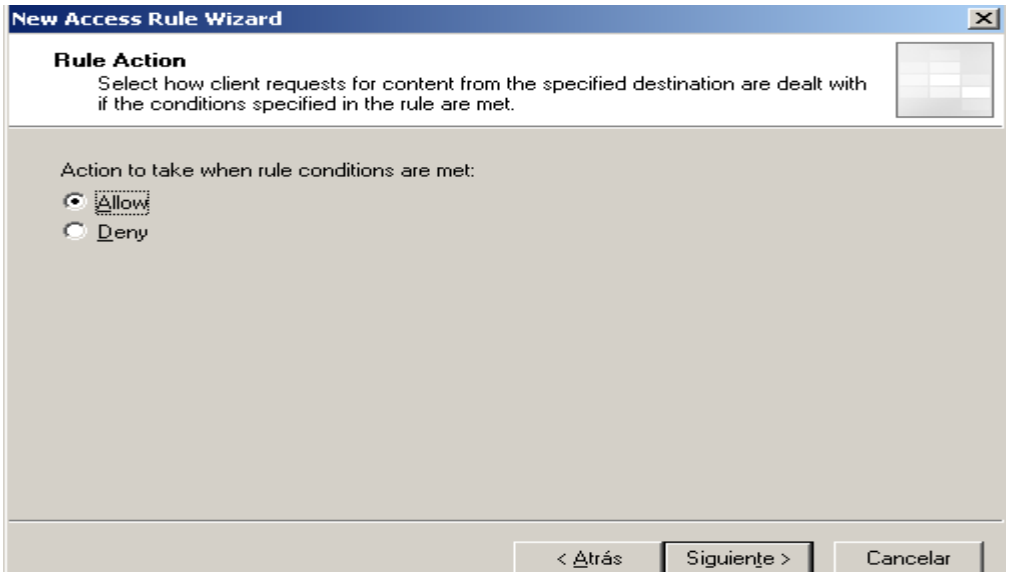


Figura 4.20: Ejemplo de la creación de una regla utilizando ISA SERVER

3. En la ventana de protocolos elegimos los protocolos que se van ha utilizar para el funcionamiento de la regla que estamos creando como podemos observar en la pantalla y damos clic en siguiente:

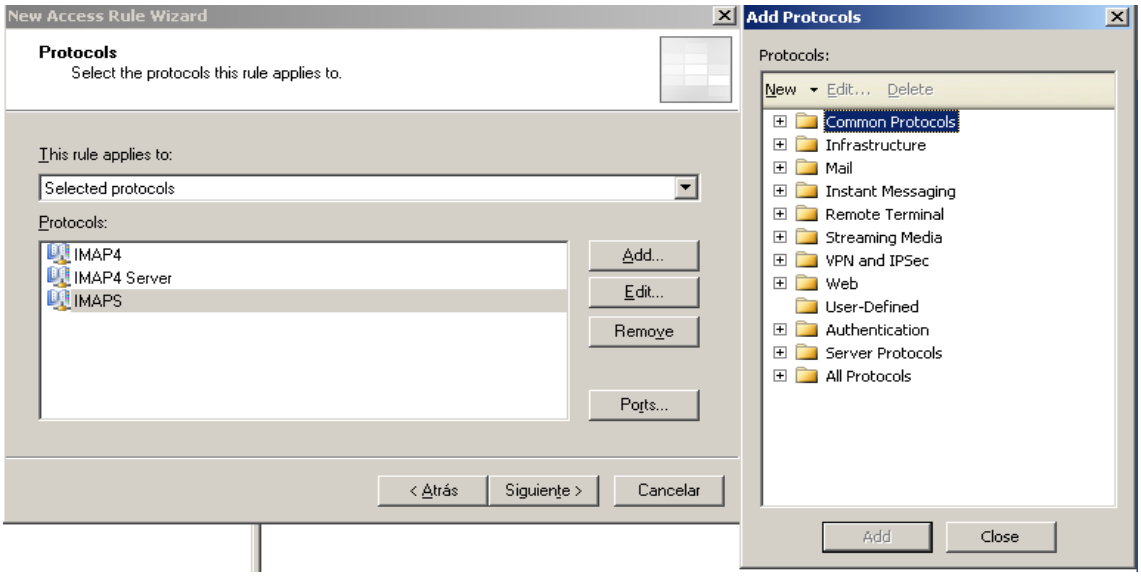


Figura 4.21: Ejemplo de la creación de una regla utilizando ISA SERVER

4. Seguidamente elegimos las redes de origen u objeto origen de donde viene el tráfico, estos objetos pueden ser “Network, Network Sets, Computers, Computer Sets, Address Ranges y Subnets.” Como nos muestra la pantalla y damos clic en siguiente:

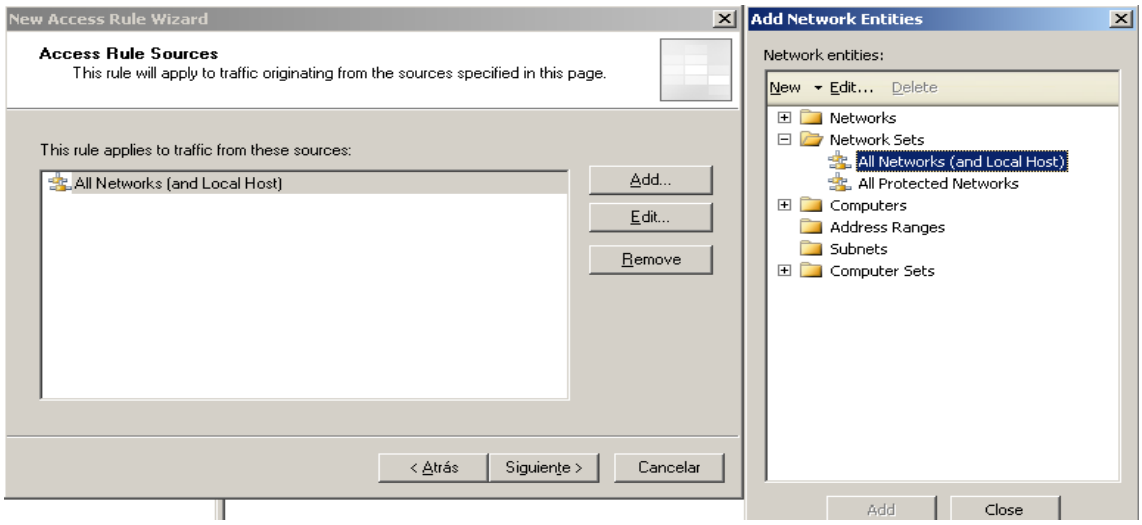


Figura 4.22: Ejemplo de la creación de una regla utilizando ISA SERVER

5. En la próxima ventana seleccionamos la red destino a donde va dirigido el tráfico u objetos como “Network, Network Sets, Computers, Computer Sets, Address Ranges, Subnets, Domain Name Sets y URL Sets.” Como podemos observar en la pantalla y damos clic en siguiente:

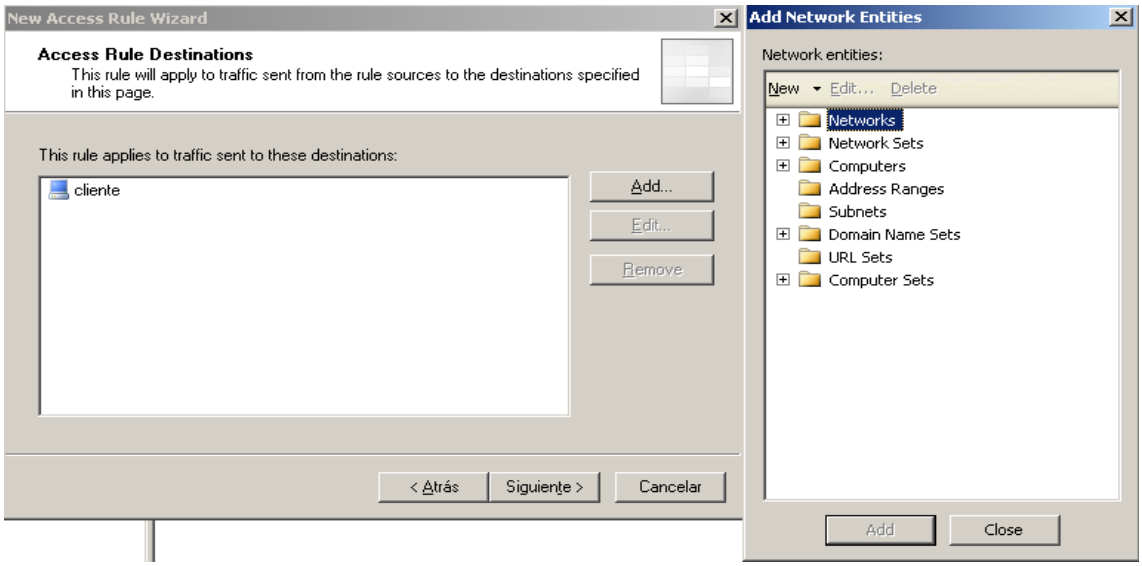


Figura 4.23: Ejemplo de la creación de una regla utilizando ISA SERVER

6. En la siguiente ventana seleccionamos uno o más objetos que pueden ser “All Users, All Authenticated Users, System and Network Service” o cualquier grupo o usuario definido, como muestra la pantalla y damos clic en siguiente:

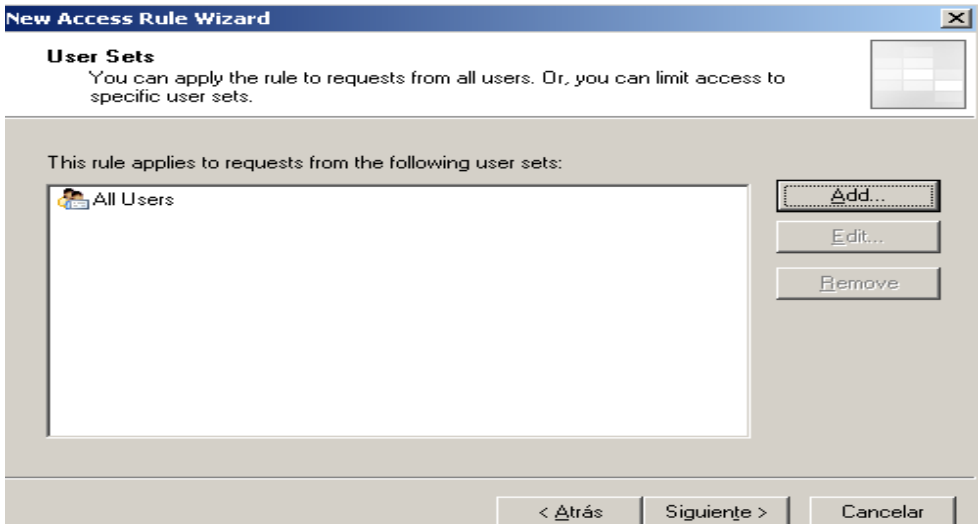


Figura 4.24: Ejemplo de la creación de una regla utilizando ISA SERVER

7. Una vez terminada la configuración nos muestra la ventana de finalización como podemos observar en la siguiente pantalla y damos clic en finalizar.

Figura 4.25: Ejemplo de la creación de una regla utilizando ISA SERVER

8. Finalmente podemos observar en la ventana del Isa Server que la regla ya esta creada damos clic en Aplicar y ya esta listo como nos muestra la siguiente pantalla.

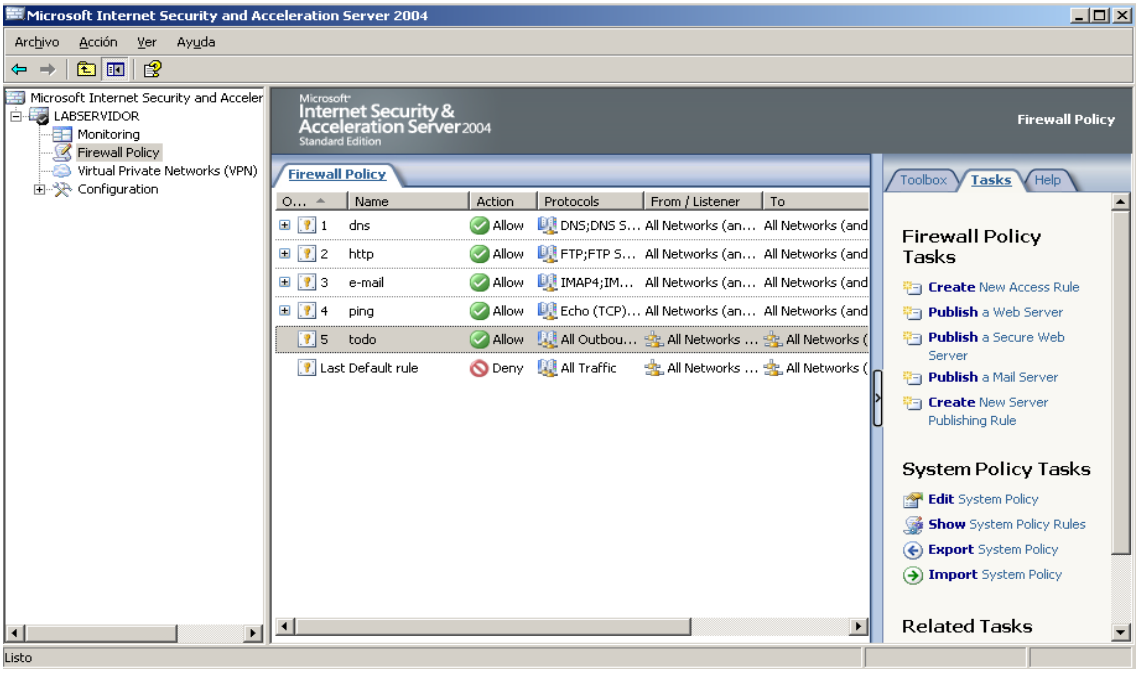


Figura 4.26: Ejemplo de la creación de una regla utilizando ISA SERVER

4.2 CONTROL DE ANCHO DE BANDA

El control ancho de banda se lo hace a través de squid en el parámetro disponible para acceso a Internet.

cache_dir (Cuanto almacenar Internet en el disco duro)

Este parámetro se utiliza para establecer que tamaño se desea que tenga él cache en el disco duro para Squid. Para entender esto un poco mejor, responda a esta pregunta: ¿Cuánto desea almacenar de Internet en el disco duro? Por defecto Squid utilizará un cache de 100 MB, de modo tal que encontrará la siguiente línea:

cache_dir ufs /var/spool/squid **100** 16 256

Se puede incrementar el tamaño del cache hasta donde lo desee el administrador. Mientras más grande el cache, más objetos de almacenarán en éste y por lo tanto se utilizará menos el *ancho de banda*. La siguiente línea establece un cache de 700 MB:

cache_dir ufs /var/spool/squid **700** 16 256

Los números 16 y 256 significan que el directorio del caché contendrá 16 subdirectorios con 256 niveles cada uno. No modifique esto números, no hay necesidad de hacerlo.

Es muy importante considerar que si se especifica un determinado tamaño de caché y este excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente. Sea cauteloso con el tamaño de caché especificado.

4.3 CONTROL DE CORREO

4.3.1 CONTROL DE CORREO BAJO LA PLATAFORMA LINUX

Para asegurar la integridad del correo que se envía y recibe; se ha considerado las utilidades que brindan los siguientes componentes:

- **CLAMAV:** Es un Antivirus que trabaja con el correo.
- **MAILSCANNER:** Este permite evitar el ingreso de Spam.

4.3.1.1 CLAMAV

Clam AntiVirus es un conjunto de herramientas GPL anti-virus para Linux. El principal objetivo de este software es la integración con servidores de correo (análisis de adjuntos). El paquete dispone de un demonio multi-hilo flexible y escalable, un escáner de línea de comando, y una herramienta para actualización automática a través de Internet. Los programas se basan en una librería compartida distribuida con el paquete de Clam AntiVirus, que puede utilizar con su software. Aun más importante, la base de datos de virus se mantiene actualizada.

- **REQUISITOS PREVIOS:**

- Se requiere un servidor de correo con **Sendmail**, previamente configurado y funcionando para enviar y recibir correo electrónico.
- Crear un usuario con su nombre: adduser CLAMAV

- **INSTALACIÓN**:

- Descomprimir las fuentes: tar zxpvf clamav-x.yz.tar.gz
- # cd /usr/local/src/clamav-0.88.7/
- # ./configure

- make
- make check
- make install

- **PRUEBA:**

Para probarlo ejecutamos una búsqueda de virus a través del directorio de las fuentes:

clamscan -r -l scan.txt /usr/src/clamav-0.88.7/

Y el archivo resultante **scan.txt** debe contener algo como lo siguiente:

Scan started: Mon Sep 10 19:23:42 2007
/usr/local/src/clamav-0.88.7/test/clam.cab: ClamAV-Test-File FOUND
/usr/local/src/clamav-0.88.7/test/clam.exe: ClamAV-Test-File FOUND
/usr/local/src/clamav-0.88.7/test/clam.rar: ClamAV-Test-File FOUND
/usr/local/src/clamav-0.88.7/test/clam.zip: ClamAV-Test-File FOUND
/usr/local/src/clamav-0.88.7/test/clam.exe.bz2: ClamAV-Test-File FOUND
-- summary --
Known viruses: 80498
Engine version: 0.88.7
Scanned directories: 44
Scanned files: 753
Infected files: 5
Data scanned: 27.03 MB
Time: 20.237 sec (0 m 20 s)

De esta forma se verá que se testean todos los ficheros de este directorio. Se puede añadirle a **clamscan** parámetros como ***-r* ó *-l*** que pueden ser interesantes (usar **man clamscan** para conocer las demás opciones).

Verá que al menos se encuentra 5 ficheros infectados; pero no se asuste, estos ficheros vienen a modo de ejemplo para comprobar el correcto funcionamiento de **ClamAV** y no son realmente virus.

4.3.1.2 MAILSCANNER

Es un servicio que se encarga de examinar el correo electrónico e identificar y etiquetar correo masivo no solicitado (**Spam**), así como también los fraudes electrónicos (**Phishing**). Combinado con ClamAV, un poderoso y versátil anti-virus libre para GNU/Linux, resultan una de las soluciones más robustas para la protección contra correo masivo no solicitado, fraudes electrónicos, virus, gusanos y troyanos desde el servidor de correo electrónico.

- **INSTALACIÓN**

- # cd/usr/local/src/MailScanner-4.57.6-1/
- # ./install.sh

- **CONFIGURACIÓN**

La siguiente configuración la realizamos en el archivo MailScanner.conf :

- Para configurar los mensajes en español editamos lo siguiente:
  %report-dir% = /etc/MailScanner/reports/es

- Para poner el de la máquina donde ejecutamos (que así aparecerá en los correos salientes, mensajes de error, etc):
  %org-name% = LABSISTEMAS

- Para definir que mostrar en la firma localizada al final de los reportes enviados por MailScanner:
  %org-longname% = LABORATORIO DE SISTEMAS ESPE

- Para definir el URL de la empresa, mismo que también se incluye en la firma al final de los reportes que envía MailScanner:
  %website%= www.labsistemas.net

- Para definir los antivirus necesario

Virus Scanners= clamav

- Para poner los mensajes infectados en cuarentena:
  Quarantine Infections= yes

- Para dar soporte de exploración en busca de correo no solicitado(Spam): Spam Checks= yes

Listas negras.

MailScanner permite también realizar filtrado de correo contra listas negras como SpamCop y Spamhaus. Para ello es necesario modificar el fichero /etc/MailScanner/spam.lists.conf:

```
#
# spamhaus.org sbl.spamhaus.org.
# spamhaus-XBL xbl.spamhaus.org.
# combinación de las dos anteriores:
SBL+XBL sblxbl.spamhaus.org.
#
spamcop.net bl.spamcop.net.
NJABL dnsbl.njabl.org.
SORBS dnsbl.sorbs.net.
```

Luego se tendrá que localizar en el fichero /etc/MailScanner/MailScanner.conf lo siguiente:

Spam List = ORDB-RBL SBL+XBL # MAPSRBL+ costs money (except .ac.uk)

Y cambiar por lo siguiente para que los cambios tengan efecto:

Spam List = ORDB-RBL SBL+XBL spamcop.net NJABL SORBS

Listas Blancas.

Pueden especificarse listas blancas de direcciones o nombres de dominio que no se desee etiqueten como correo masivo no solicitado (Spam) en el fichero /etc/MailScanner/rules/spam.whitelist.rules del siguiente modo, donde dice **yes** significará que el correo proveniente de dichas direcciones nunca se etiquetará como correo masivo no solicitado (Spam):

```
# This is where you can build a Spam WhiteList
# Addresses matching in here, with the value
# "yes" will never be marked as spam.
#From: 152.78. yes
#From: 130.246. yes
FromOrTo: default no
From: 192.168.0. yes
```

En el ejemplo anterior, cualquier dirección IP de la red 192.168.0.0/24 quedará exento de etiquetarse como correo masivo no solicitado (Spam).

4.4 PREVENCIÓN DE FALLAS

El riesgo que implica el despliegue de una red inalámbrica consiste en que la información viaja en un medio que no es limitable a un espacio determinado, surge el peligro de que cualquier persona no autorizada conozca datos sensibles de la empresa comprometiendo su activo más importante: la información.

- Calidad de Servicio. Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps, frente a los 100 que puede alcanzar una red normal y corriente.
- Si dos Access Point (AP) cuentan con el mismo canal de comunicación produce ruido, para lo cual será necesario asignar a cada Access Point con un canal de comunicación diferente.
- Si las antenas están cerca de un generador eléctrico produce ruido e interferencia, esta se puede situar alrededor de 10-4 frente a las 10-10 de las redes cableadas. Esto significa que hay 6 órdenes de magnitud de diferencia y eso es mucho. Estamos hablando de 1 bit erróneo cada 10.000 bits o lo que es lo mismo, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo. Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.
- Ataques continuos de virus, troyanos, gusanos, etc. Para no estar expuestos a este tipo de problemas será necesario disponer de un antivirus Clamav y MailScanner.
- No existe control de ancho de banda, para tener control de ancho de banda se lo realizará a través del proxy Squid.
- No existen seguridades que garanticen la integridad de la red, para solucionar este problema se han implementado reglas que permiten establecer seguridades a través del firewall, esto es habilitando servicios y puertos necesarios.
- Riesgo en la pérdida de información o configuraciones.
- No cuenta con políticas de seguridad (básicas)

4.5 APLICABILIDAD DE LOS ESTÁNDARES DEFINIDOS

La aplicabilidad de los estándares la aplicamos en el Access Point y en la tarjeta inalámbrica:

4.5.1 CONFIGURACIÓN DEL ACCESS POINT

1. Conexión del Punto de Acceso inalámbrico

A. Primero, conectar el adaptador de alimentación al receptor situado en el adaptador trasero del AP y después conectar el otro extremo del adaptador de alimentación en una base de pared o regleta de alimentación.
B. Introducir un extremo del cable en el puerto ethernet del panel trasero del AP, y el otro extremo del cable en el tarjeta ethernet del servidor.
C. El adaptador inalámbrico se conectará directamente con el AP usando sus parámetros inalámbricos por defecto.

2. Uso del Asistente de Configuración

A. Abrir el navegador Web y teclear “http://192.168.0.50” en la barra de direcciones URL y dar enter.
B. Teclear “admin” en el campo de usuario y dejar el campo de la contraseña en blanco y dar clic en OK.

4.5.2 IMPLEMENTACIÓN DE SEGURIDAD EN EL ACCESS POINT

1. Cambiar la contraseña por defecto.

Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso.

Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que *el observador* la conozca.

2. Usar encriptación WEP/WPA.

Activa en el Punto de Acceso la encriptación **WEP**. Mejor de 128 bits que de 64 bits cuanto mayor sea el número de bits mejor.

Los Puntos de Acceso más recientes permiten escribir una *frase* a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercales mayúsculas con minúsculas y números, evites utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").

También se tendrá que establecer en la configuración WEP la clave que se utilizará de las cuatro generadas (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

Después de configurar el AP tendrás que configurar los accesorios o dispositivos Wi-Fi de tu red. En éstos se tendrá que marcar la misma clave WEP (posiblemente puedas utilizar la *frase* anterior) que has establecido para el AP y la misma clave a utilizar (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

Algunos Puntos de Acceso más recientes soportan también encriptación **WPA** (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.
Si se activa WPA en el Punto de Acceso, tanto los accesorios y dispositivos inalámbricos se tendrá que configurar con los mismos datos.

3. Cambia el SSID por defecto.

Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID".
En vez de "MiAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para *el observador*, como puede ser "Broken", "Down" o "Desconectado".

Si no llamamos la atención del *observador* hay menos posibilidades de que éste intente entrar en nuestra red.

4. Desactiva el broadcasting SSID.

El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual.

Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

5. Activa el filtrado de direcciones MAC.

Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a tu red Wi-Fi.

6. Desconecta el AP cuando no lo uses.

Es importante desconectar el AP cuando no se este utilizando ya que si la contraseña sigue siendo la por defecto será muy fácil ingresar a la configuración.

4.5.2 APLICABILIDAD DEL ESTÁNDAR

El Access Point que se esta utilizando es **D-Link *Air*Plus Xtreme G DWL-2100AP** que utiliza el estándar **802.11g** Wireless que alcanza 108Mbps.

Se esta utilizando el protocolo **WPA** con el método de Encriptación **TKIP** el que se encarga de cambiar la clave compartida entre el punto de acceso y cliente cada cierto tiempo para evitar ataques que permitan revelar la clave.

A continuación podemos observar la pantalla en la que se resumen los cambios que hemos realizado:

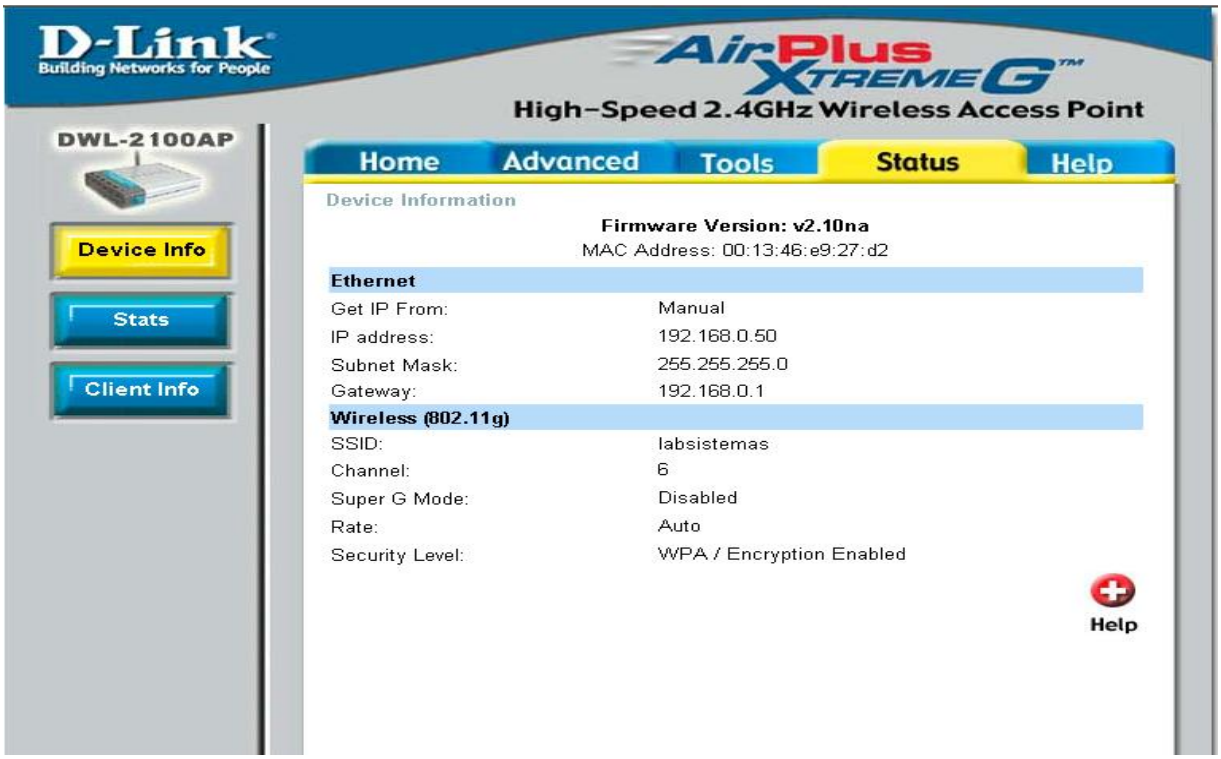


Figura 4.27: Configuración del Access Point

Luego procedemos a configurar la tarjeta inalámbrica del cliente aplicando la misma seguridad que aplicamos en el AP, en la siguiente pantalla podemos observar la configuración:

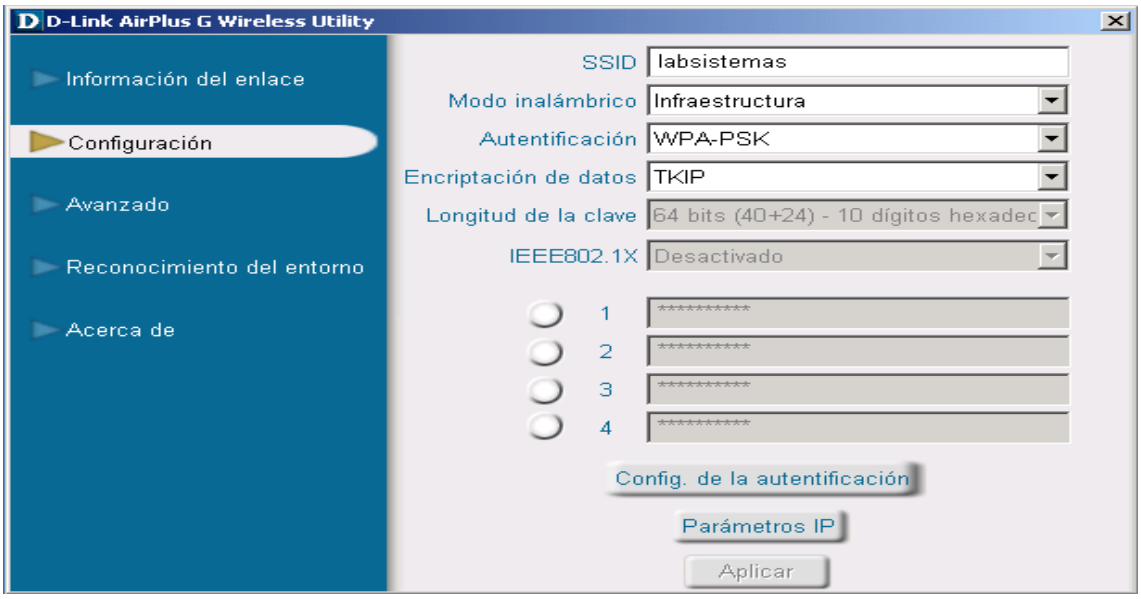


Figura 4.28: Configuración de la Tarjeta Wireless

De igual manera configuramos la clave de autenticación la misma del AP.

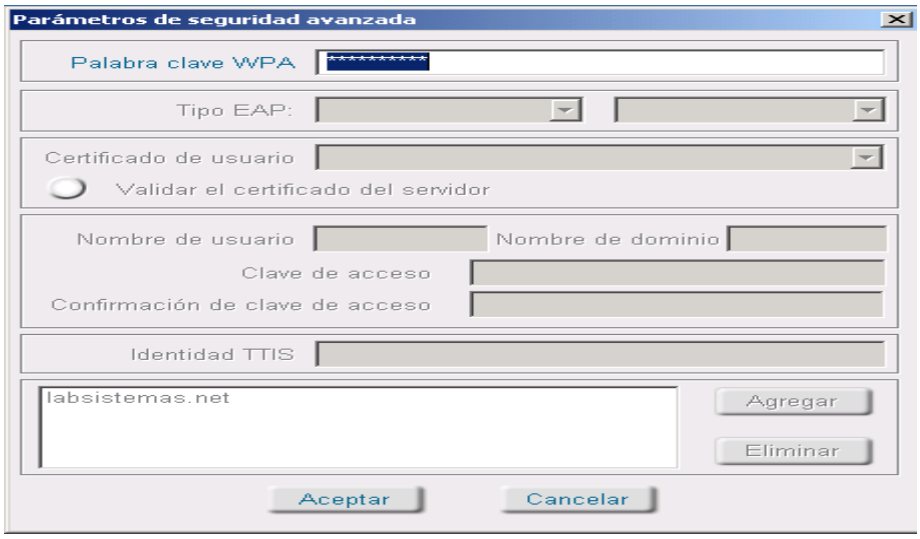


Figura 4.29: Parámetros de Seguridad de la Tarjeta Wireless

Finalmente podemos observar que la conexión a funcionado y se encuentra conectado.

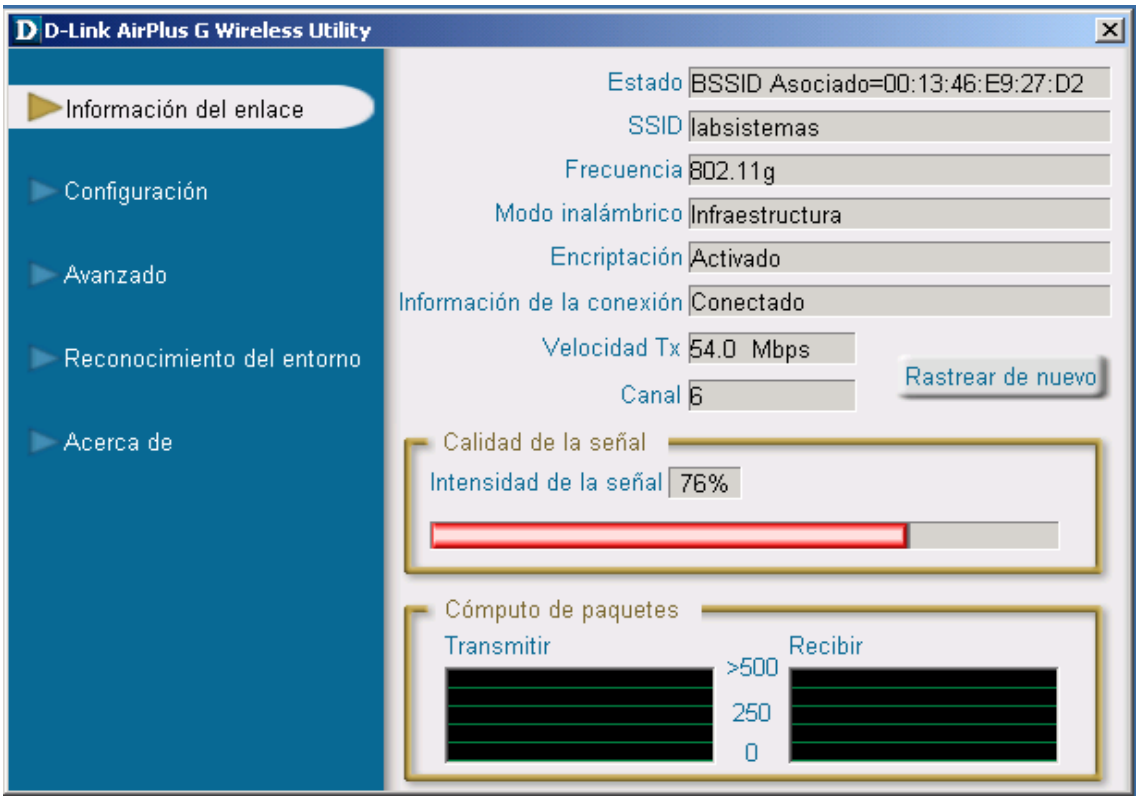


Figura 4.30: Información de Conectividad del Access Point

CAPITULO V

5.1 CONCLUSIONES

- La seguridad en redes inalámbricas es una necesidad, dadas las características de la información que por ellas se transmite, para ello se puede utilizar el método de encriptación WPA, así como la utilización del firewall ya que es de gran ayuda porque permite prevenir ataques informáticos y por ende pérdida de información.
- En este trabajo se ha abordado la aplicación de mecanismos de seguridad tanto en el Sistema Operativo de Linux con la utilización de Iptables y Squid como de Windows a través del ISA Server.
- Mediante el desarrollo de éste trabajo podemos apreciar el costo beneficio que representa cada uno de los sistemas operativos utilizados, así Linux ofrece un software libre lo cual es mucho más fácil el adquirirlo, en cambio con Windows 2003 se ha encontrado muchas limitaciones respecto al costo pues es necesario adquirir el software con licenciamiento lo que representa una mayor inversión.
- La implementación de políticas de seguridad ayuda a las organizaciones a dar un valor agregado a los servicios que presta, así como también crear un ambiente de confianza entre sus clientes.
- Se ha considerado un escenario real de pruebas con las ventajas inherentes de experimentar en un ambiente real, e interactuar directamente con otras nuevas tecnologías, los resultados obtenidos han contribuido a la consideración del Firewall, como una alternativa para brindar servicios de seguridad en el Internet en nuestro medio.
- Este trabajo de tesis representa un fuerte crecimiento profesional y personal al abordar uno de los temas que representan la Seguridad en redes.
- Finalmente, todo mecanismo de protección en una red debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual con los sistemas de información, y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa.

5.2 RECOMENDACIONES

- Crear una Política de Seguridad donde se contemplen todos los usuarios, recursos de una red, instalar un Firewall como apoyo al control de acceso, monitoreo de la red y de bitácoras (loggs de transacciones) de sistemas.
- Los usuarios por su parte, deben proteger sus archivos sensibles de confidencialidad, aplicar candados o seguridades, claves para inicializar su computadora, claves robustas de usuario.
- Fomentar en los estudiantes el uso y propagación del Software Libre, ya que ello ayudará a disminuir costos y dejar de ser dependientes del software propietario.

BIBLIOGRAFÍA

- BORGHELLO, Cristian F. Seguridad Informática sus Implicaciones e Implementación. Buenos Aires 2001.292p
- LINUX-Máxima Seguridad. Prentice-Hall. Madrid 776p
- MCCLURE, Stuart, SCAMBRAY, Joel y KURTZ George. Hackers, Secretos y soluciones para la seguridad de sedes. Madrid McGraw-Hill Osborne Media -2002.854p
- RUDDER, David. Cortafuegos Como-1996.14p.
- TANENBAUM, Adrews. Redes de Computadoras México D.F. Prentice- Hall. 1997.812p.
- VILLALN HUERTA, Antonio. Seguridad en Unix y Redes. Madrid 2002-485p
- Introducción A Las Redes Inalámbricas: 802.11A, 802.11B, AIRPORT Y AIRPORT EXTREME DE APPLE (WINDOWS Y MACINTOSH) de ENGST, ADAM y FLEISHMAN, GLENN

DIRECCIONES WEB

http://www.saulo.net/pub/inv/SegWiFi-art.htm

http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml

http://www.arturosoria.com/eprofecias/art/wireless_seguridad.asp

http://multingles.net/docs/alezito/alezito_inalamb.htm

http://www.zonagratuita.com/servicios/seguridad/wireles.html

http://es.wikipedia.org/wiki/Sendmail

http://www.linuxparatodos.net/portal/staticpages/index.php?page=15-como-sendmail-apendice-01

http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-sendmail.html

http://es.tldp.org/Tutoriales/doc-guia-sendmail/doc-guia-sendmail-html/

http://www.microsoft.com/spain/isaserver/default.mspx

http://technet.microsoft.com/es-es/library/aa997148.aspx

http://es.wikipedia.org/wiki/Microsoft_Internet_Security_and_Acceleration_Server

http://www.microsoft.com/latam/exchange/default.mspx

http://technet.microsoft.com/es-es/library/aa996058.aspx

http://es.wikipedia.org/wiki/Microsoft_Exchange_Server

http://www.emagister.com/introduccion-microsoft-exchange-server-2003-cursos-345308.htm

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS