UNIVERSIDAD TECNICA DE
COTOPAXI
ECUADOR

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL SAN FRANCISCO
ARGENTINA

UNIVERSIDAD TECNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERIA Y APLICADAS

TESIS DE GRADO PREVIA LA OBTENCION DEL TITULO DE INGENIERO EN INFORMATICA Y SISTEMAS COMPUTACIONALES

TEMA*: ANÁLISIS Y DISEÑO DE UNA WIRELESS LAN SEGURA PARA EL ENLACE ENTRE DOS O MAS EDIFICIOS EN LA MUNICIPALIDAD DE LA CIUDAD DE SAN FRANCISCO.*

AUTOR:

RAMIRO MENA.

DIRECTOR DE TESIS:

ING. JUAN CARLOS CALLONI

SAN FRANCISCO, CORDOBA, ARGENTINA

2007

AUTORIA

El presente trabajo de investigación, es original, auténtico y personal. En tal virtud declaro que el contenido es de mi absoluta responsabilidad legal y académica.

_____

Ramiro Esteban Mena Delgado

C.I. 050258952-6

CERTIFICACION DIRECTOR DE TESIS

Por medio de la presente, yo Juan Carlos Calloni, en calidad de docente en la cátedra de Redes, de la Universidad Tecnológica Nacional Regional San Francisco certifico haber dirigido el presente proyecto de tesis dirigido por el Sr. Ramiro Mena con el tema *ANÁLISIS Y DISEÑO DE UNA WIRELESS LAN SEGURA PARA EL ENLACE ENTRE DOS O MAS EDIFICIOS DE LA MUNICIPALIDAD DE LA CIUDAD DE SAN FRANCISCO.*

Es todo lo que puedo mencionar en honor a la verdad.

Atentamente

_____

Ing. Juan Carlos Calloni

PAGINA DE APROBACION DEL TUTOR

Tesis de grado previa a la obtención del título de Ingeniero en Sistemas

DIRECTOR DE TESIS

Calificación _____ _____

Número Letras

PAGINA DE APROBACION DEL TRIBUNAL DE GRADO

ANÁLISIS Y DISEÑO DE UNA WIRELESS LAN SEGURA PARA EL ENLACE ENTRE DOS O MAS EDIFICIOS DE LA MUNICIPALIDAD DE LA CIUDAD DE SAN FRANCISCO.

APROBADO POR LOS MIEMBROS DEL TRIBUNAL DE GRADO

FECHA _____

_____ _____

_____ _____

_____ _____

DEDICATORIA

En especial quiero dedicar este trabajo a mi adorada madre una gran mujer, a mi familia y amigos. A mis seres queridos que ya no se encuentran entre nosotros que me dan fuerza para continuar día a día.

Ramiro.

AGRADECIMIENTOS

Doy gracias a Dios por haberme permitido culminar una de mis metas en la vida.

Un agradecimiento a la Universidad Técnica de Cotopaxi, a la Carrera de Ciencias de la Ingeniería y Aplicadas y todas las personas que impartieron sus conocimientos académicos.

Agradezco a la Universidad Tecnológica Nacional facultad regional de San Francisco por abrirme sus puertas, de igual manera a toda la gente de esta hermosa ciudad en especial a quienes se preocuparon por mí desde el inicio.

Mi agradecimiento a Tamboroses S.A. a todo el personal que trabaja en esta empresa por haberme permitido ser parte del equipo de trabajo, por darme la experiencia, por su apoyo y por confiar en mí.

Agradezco a mi familia, a todos mis amigos que siempre estuvieron pendientes en todo momento, a mis compañeros de viaje y convivencia, fueron 6 meses inolvidables.

Ramiro Mena.

INDICE GENERAL

CAPITULO I

MARCO TEORICO

INDICE DE GRAFICOS

RESUMEN

El presente trabajo se realizó mediante la gentil colaboración tanto de la Universidad Tecnológica Nacional UTN Regional San Francisco y la Municipalidad de dicha ciudad.

La necesidad de la Municipalidad en contar con un enlace para la actualización de datos oportunos, confiables y seguros llevó a la presente investigación con la que se buscó una solución para agilizar una parte del trámite burocrático en beneficio de todas personas inmersas en los procesos informáticos así como de la comunidad tomando en cuenta la importancia de brindar un servicio oportuno. Pudimos comprobar la fiabilidad del proyecto y todos los beneficios que generaría el tener dicho enlace.

Espero que esta propuesta pueda aportar a la búsqueda y desarrollo de nuevas soluciones en el área de redes en especial a las inalámbricas que pienso en un futuro serán el principal canal para recibir conocimiento.

INTRODUCCION

Hoy en día el avance científico se ha desarrollado en todos los campos y las necesidades del hombre cada vez son mayores, esto ha obligado a buscar nuevas y mejores formas de Tecnología. Una de ellas es la comunicación entre computadoras, ya sea en áreas locales o zonas con mayor distancia.

La comunicación se fundamenta específicamente en la transmisión de datos por medio de líneas físicas o conexión inalámbrica (sin cables); permitiendo al usuario transferir datos de cualquier tipo incluyendo la utilización del Internet.

Las redes han constituido un factor primordial en la transferencia de cualquier tipo de datos, tanto para el uso educativo, así como en el uso industrial, ya que facilitan y economizan gastos en una empresa.

Por esta razón con esta tesis he previsto un Análisis y Diseño de una Wireless Lan segura para el enlace entre dos o más edificios, mejorando la calidad de transmisión de datos de una manera fácil y sobre todo con mayor seguridad.

El proyecto está estructurado en tres capítulos, el cuál consta de un teórico uno práctico y el último de conclusiones y recomendaciones.

En el primer capítulo doy conceptos básicos de red, estándares inalámbricos, topologías, protocolos, configuración de equipos y tarjetas inalámbricas, clases de antenas, y lo más importante, la seguridad que se manejará para la utilización del enlace.

En el segundo capítulo me voy a enfocar en el análisis de la empresa a la cual sería dirigida la posible implementación.

En el tercer capítulo me basaré específicamente en la práctica; en el cuál explico detalladamente el diseño lógico, físico y la tecnología a ser determinada.

OBJETIVOS

GENERALES.

- Analizar y diseñar una Wireless LAN segura para el enlace entre dos o más edificios de la municipalidad de la ciudad de San Francisco para centralizar y compartir información.

ESPECÍFICOS.

- Determinar la situación actual de la forma de comunicación entre los edificios de la municipalidad.

- Emplear estándares inalámbricos de calidad necesarios para el correcto manejo y uso de esta tecnología.

- Determinar un óptimo esquema de seguridad Wireless LAN para el funcionamiento confiable.

- Estructurar los diferentes parámetros de acuerdo a la necesidad de funcionamiento para el enlace de los edificios.

HIPOTESIS

UNA WIRELESS LAN SEGURA PARA EL ENLACE ENTRE DOS O MAS EDIFICIOS DE LA MUNICIPALIDAD DE LA CIUDAD DE SAN FRANCISCO, nos garantizará que la producción de información generada sea mas eficiente, eficaz, confiable, consistente y nos permitirá actualizarla en tiempo real.

CAPITULO I

1.1 INTRODUCCION

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología. El siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial. El siglo XIX fue la época de la máquina de vapor. Durante el siglo XX, la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de los ordenadores (computadores), así como a la puesta en orbita de los satélites de comunicación.

A medida que avanzamos hacia los últimos años de este siglo, se ha dado una rápida convergencia de estas áreas, y también las diferencias entre la captura, transporte almacenamiento y procesamiento de información están desapareciendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, simplemente oprimiendo una tecla. A medida que crece nuestra habilidad para recolectar procesar y distribuir información, la demanda de mas sofisticados procesamientos de información crece todavía con mayor rapidez.

1.2 DEFINICION

Definición de rede locales inalámbricas.

Una red local inalámbrica (Wireless LAN o WLAN es un sistema de comunicación flexible implementado como una extensión o alternativa para las redes cableadas. Usan tecnología de radiofrecuencias RF, transmiten y reciben datos a través del aire minimizando la necesidad de conexiones cableadas. Son tecnologías que combinan la conectividad de datos con la movilidad del usuario.

Hay dos componentes básicos en una red inalámbrica un punto de acceso y un cliente con una tarjeta de red inalámbrica.

Tarjeta de red inalámbrica (Wireless Adapter Cards).- Es un dispositivo que sirve para realizar la comunicación inalámbrica con el punto de acceso o con otra tarjeta de red inalámbrica, intercambiar datos y compartir recursos.

Punto de acceso (Access Point o AP).- Es el que crea la red de radio y la comunica con la red local alámbrica, el AP contiene un puerto 10BaseT con el cual se puede conectar a la red alámbrica por medio de un dispositivo de conexión LAN el cual puede ser un swith o un hub

Wireless Local Area Network.

Abreviatura de una red local que utiliza ondas de radio. A ella se pueden conectar ordenadores inalámbricos estableciendo la comunicación recíproca mediante ondas de radio (gama de microonda) o rayos infrarrojos. Especialmente los ordenadores portátiles son los que se conectan sin cables (wireless) a la red de Internet. Estos puntos de acceso son denominados Hotspots.[1]

Llamamos red inalámbrica a aquella que posibilita la unión de dos o más dispositivos sin la mediación de cables.

Principales ventajas:

- Permiten la movilidad.
- Facilitan la reubicación de las estaciones de trabajo evitando la necesidad de tirar cableado.
- Rapidez en la instalación.
- Menores costes de mantenimiento.

[1] Diccionario de Wi Fi http://wifi.lycos.es/info/lexicon

1.3 ESTANDARES INLAMBRICOS

El Institute of Electrical and Electronics Engineers (IEEE) fomenta el desarrollo de estándares que suelen convertirse en normas nacionales e internacionales. Lo mismo que el estándar 802.3 que define Ethernet en el entorno cableado, el IEEE ha definido un conjunto de estándares para el entorno de la gestión de las redes inalámbricas, bajo la denominación 802.11[2]

1.3.1 ESTANDAR 802.11

Ancho de banda máximo de hasta 2 Mbps

Opera en el espectro de 2.4 Ghz sin necesidad de licencia.

Posible interferencia con hornos microondas, dispositivos bluetooth, y teléfonos DECT, puesto que operan en el mismo espectro de frecuencias.

Sistemas de modulación FHSS (Espectro Distribuido con Saltos de Frecuencias) y DSSS (Espectro Ensanchado de Secuencia Directa).

1.3.2 ESTANDAR 802.11b

Ancho de banda máximo de hasta 11Mbps

Opera en el espectro de 2.4 Ghz sin necesidad de licencia.

Las mismas interferencias que para 802.11

Conocido como WIFI

Modulación DSSS es necesario

[2] Wikipedia estándares inalámbricos
http://es.wikipedia.org/wiki/Est%C3%A1ndares_inal%C3%A1mbricos#802.11

Compatible con los equipos DSSS del estándar 802.11.

1.3.3 ESTANDAR 802.11g

Ancho de banda máximo de hasta 54 Mbps

Opera en el espectro de 2.4 Ghz sin necesidad de licencia.

Compatible con 802.11b.

Modulación DSSS y OFDM.

1.3.4 ESTANDAR 802.11a

Ancho de banda máximo de hasta 54 Mbps

Opera en el espectro de 5 Ghz sin necesidad de licencia. Menos saturado

No es compatible con 802.11b y 802.11g

Modulación de OFDM.

1.3.5 ESTANDAR 802.15

1.3.6 HIPERLAN

Es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz. HIPERLAN/2 es una solución estándar para un rango de comunicación corto que permite una alta transferencia de datos y Calidad de Servicio del tráfico entre estaciones base WLAN y terminales de

usuarios. La seguridad esta provista por lo último en técnicas de cifrado y protocolos de autenticación.

HIPERLAN/1

Hiper Lan es similar a 802.11a (5 GHz) y es diferente de 802.11b/g (2,4 GHz). HIPERLAN/1, HIgh Performance Radio LAN version 1 es un estándar del ETSI (European Telecomunications Standards Institute).

El plan empezó en 1991. El objetivo de HIPERLAN era la alta velocidad de transmisión, más alta que la del 802.11. El estándar se aprobó en 1996.

El estándar cubre las capas física y MAC como el 802.11. Hay una nueva subcapa llamada Channel Access and Control sublayer (CAC). Esta subcapa maneja las peticiones de acceso a los canales. La aceptación de la petición depende del uso del canal y de la prioridad de la petición. La capa CAC proporciona independencia jerárquica con un mecanismo de Elimination-Yield Non-Preemptive Multiple Access.(EY-NPMA). EY-NPMA codifica las prioridades y demás funciones en un pulso de radio de longitud variable que precede a los datos.

EY-NPMA permite trabajar a la red con pocas colisiones aunque halla un gran número de usuarios. Las aplicaciones multimedia funcionan en HIPERLAN gracias al mecanismo de prioridades del EY-NPMA. La capa MAC define protocolos para enrutado, seguridad y ahorro de energía y proporciona una transferencia de datos natural a las capas superiores.

En la capa física se usan modulaciones FSK y GMSK.

Características de HIPERLAN :

- rango 50 m
- baja movilidad (1.4 m/s)
- soporta tráfico asíncrono y síncrono.
- sonido 32 Kbps, latencia de 10 ns
- vídeo 2 Mbit/s, latencia de 100 ns
- datos a 10 Mbps

HIPERLAN no interfiere con hornos microondas y otros aparatos del hogar, que trabajan a 2.4 GHz.

HIPERLAN/2

Las especificaciones funcionales de HIPERLAN/2 se completaron en el mes de Febrero de 2000. La versión 2 fue diseñada como una conexión inalámbrica rápida para muchos tipos de redes. Por ejemplo: red back bone UMTS, redes ATM e IP. También funciona como una red doméstica como HIPERLAN/1. HIPERLAN/2 usa la banda de 5 GHz y una velocidad de transmisión de hasta 54 Mbps.

Los servicios básicos son transmisión de datos, sonido, y vídeo. Se hace énfasis en la calidad de esos servicios.(QoS).

El estándar cubre las capas Física, Data Link Control y Convergencia. La capa de Convergencia se ocupa de la funcionalidad de la dependencia de servicios entre las capas DLC y Red (OSI 3). Las subcapas de Convergencia se pueden usar también en la capa física para conectar las redes IP, ATM o UMTS. Esta característica hace HIPERLAN/2 disponible para la conexión inalámbrica de varias redes.

En la capa física se emplean modulaciones BPSK, QPSK, 16QAM o 64QAM.

HIPERLAN/2 ofrece unas medidas de seguridad aceptables. Los datos son codificados con los algoritmos DES o 3DES. El punto de acceso y el terminal inalámbrico se pueden autenticar mutuamente.

1.4 TOPOLOGIAS Y PROTOCOLOS INALAMBRICOS

Las redes LAN 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". En este sitio web se utilizarán los términos "infraestructura" y "ad hoc". Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

1.4.1 Redes Ad-Hoc

Las redes ad-hoc son un conjunto autónomo y espontáneo de routers móviles, conectados por enlaces inalámbricos que no precisan de una infraestructura fija. Se proyectan para operar en ambientes hostiles e irregulares, y sus aplicaciones son extensas tales como redes de área personal, entornos militares, entornos ciudadanos y operaciones de emergencia. Estas redes plantean grandes retos técnicos y funcionales debido a la hostilidad del medio inalámbrico. Estas redes fueron inicialmente diseñadas para antenas omnidireccionales. Sin embargo, recientemente, se ha estudiado que las antenas direccionales pueden ser beneficiosas para este tipo de redes. Al direccionar las transmisiones se puede incrementar el rehúso espacial ya que dos nodos vecinos podrían comunicarse a la vez en diferentes direcciones. Desafortunadamente, las transmisiones direccionales incrementan los problemas de nodos ocultos, deafness, y la localización

de los nodos vecinos. De esta manera, para utilizar las antenas direccionales se debe diseñar un protocolo específico ya que el protocolo MAC 802.11 fue diseñado para antenas omnidireccionales. El objetivo de este proyecto es el estudio de los protocolos MAC 802.11 con antenas direccionales de cara a diseñar uno nuevo que mejore el rendimiento del protocolo MAC 802.11 con antenas omnidireccionales. En el estudio de los protocolos MAC 802.11 para antenas direccionales se explican las diferentes propuestas que existen hasta ahora para solucionar problemas relacionados con localización de los nodos, nodos expuestos, nodos ocultos y deafness. El nuevo protocolo se compara con el protocolo MAC 802.11 con antenas omnidireccionales. Para ello se diseña un simulador escalable y se obtienen resultados del rendimiento dado por los dos protocolos en diferentes topologías.[3]

En una topología ad hoc, 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.

[3] Biblioteca Universitaria Redes Ad-hoc http://bibliotecnica.upc.es/pfc/mostrar_dades_PFC.asp?id=4079

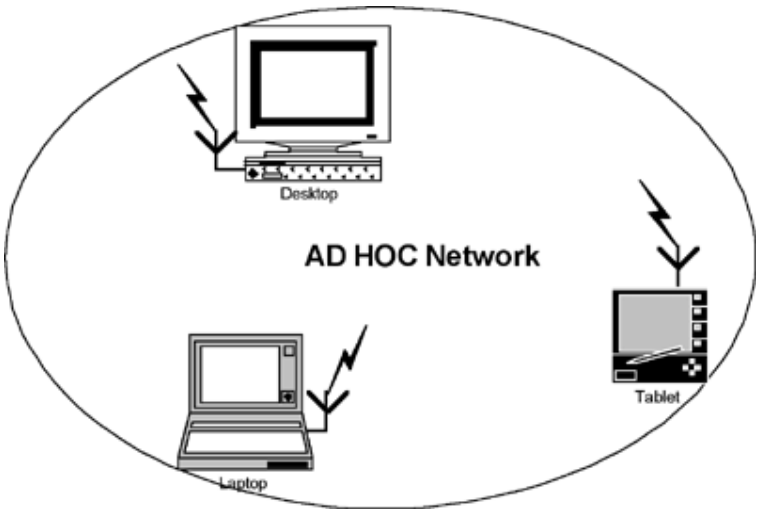


Fig 1. Red ad hoc

Por ejemplo, cuando se combinan con la nueva generación de software y soluciones par a par inteligentes actuales, estas redes inalámbricas ad hoc pueden permitir a los usuarios móviles colaborar, participar en juegos de equipo, transferir archivos o comunicarse de algún otro modo mediante sus PC o dispositivos inteligentes sin cables.

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.

1.4.2 Redes de infraestructura

Una 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.

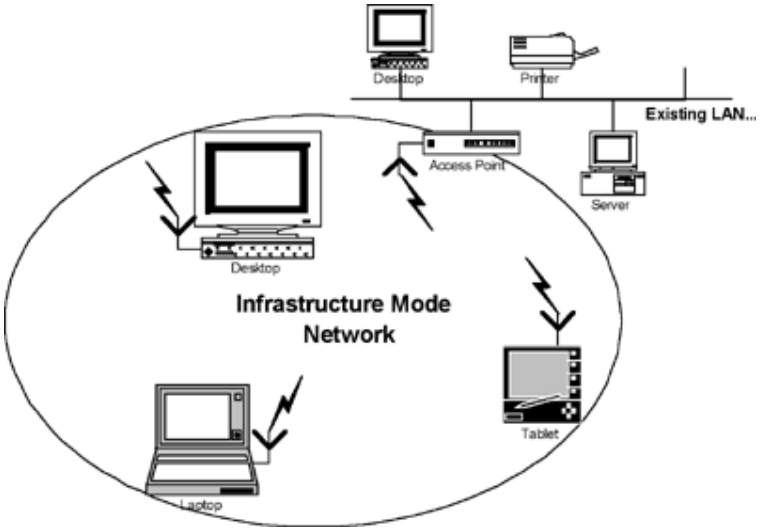


Fig 2 Red de la modalidad de infraestructura

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 está 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 CONFIGURACION DE ACCESS POINTS.

1.5.1 Modos de Operación.

Para maximizar el retorno total de la inversión, el DWL-3200AP puede ser configurado para optimizar el desempeño de la red basándose en alguno de sus múltiples modos de operación: Access Point, Sistema de Distribución Inalámbrica (WDS) con Access Point, y WDS (Sin difusión de AP). Con soporte WDS, los administradores de la red pueden también configurar varios DWL-3200AP por medio de un dispositivo y configurarlos para hacer un puente entre ellos para distribuir de manera efectiva el tráfico entre la red y sus respectivas fuentes. En el modo WDS, el DWL-3200AP incluye el protocolo Spanning Tree Protocol, el cual proporciona redundancia de rutas mientras previene loops indeseables en la red. Además, soporta bitácoras de sistema (syslog) proporcionando un estándar de la industria para capturar información de la bitácora para los dispositivos conectados a la red.

1.5.1.1 Punto de acceso (Access Point AP)

Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso - se convierten en una red **ad-hoc**). Los

puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalambrica.

1.5.1.2 Cliente inalámbrico

Una red local (LAN) es una red ubicada en un lugar. Los usuarios en dicho lugar puede compartir archivos, impresoras y otros servicios de la red. En una LAN, un ordenador conectado a la red que solicita servicios se denomina cliente. Una red local inalámbrica (WLAN) es un tipo de LAN que utiliza ondas de radiofrecuencia alta en vez de cables para comunicar y transmitir datos entre los clientes y dispositivos de la red. Se trata de un sistema flexible de comunicación implementado como una ampliación o como alternativa a una red local cableada.

En una WLAN, los adaptadores inalámbricos se instalan en los clientes, también conocidos como "clientes inalámbricos". El adaptador permite al cliente inalámbrico comunicarse con la WLAN sin necesidad de cables. En vez de ello, los clientes inalámbricos envían y reciben información a través de una ruta (ondas) denominada canal.

Un cliente inalámbrico opera en modo de infraestructura o en modo distribuido (peer-to-peer).

Modo infraestructura: WLAN con routers de banda ancha inalámbricos

En el modo de infraestructura, los clientes inalámbricos envían y reciben información a través de uno o más routers de banda ancha inalámbricos. Los routers de banda ancha inalámbricos están colocados estratégicamente en una zona determinada para proporcionar una cobertura óptima a los clientes inalámbricos. Los routers de banda ancha inalámbricos y los clientes inalámbricos constituyen una WLAN.

Los routers de banda ancha inalámbricos pueden conectarse a una red local de clientes cableados o inalámbricos. Los routers de banda ancha inalámbricos envían y reciben información desde la LAN mediante esta conexión.

Se utiliza un ESSID (Identificador del conjunto de servicios ampliado) para identificar a los clientes inalámbricos y los routers de banda ancha inalámbricos en una WLAN. Todos los clientes inalámbricos y los routers de banda ancha inalámbricos conectados en una WLAN deben tener el misma ESSID. Se utiliza un BSSID (Identificador del conjunto de servicios básico) para definir de forma exclusiva cada uno de los clientes inalámbricos y router de banda ancha inalámbrico.

Modo distribuido **(Peer-to-Peer o modo Ad Hoc): WLAN sin routers de banda ancha inalámbricos**

En el modo distribuido, los clientes inalámbricos envían y reciben directamente información a otros clientes inalámbricos sin utilizar routers de banda ancha inalámbricos.

Identificación de una WLAN

Los ESSID y BSSID son identificadores de conjuntos de servicios (SSID) que identifican y controlan el acceso al cliente inalámbrico a una determinada WLAN. El SSID se conoce a veces como el nombre de red. El SSID indica a qué WLAN se está haciendo referencia. En la mayoría de los casos, la interfaz de usuario muestra el SSID.

Cuando se instala un router de banda ancha inalámbrico o un adaptador inalámbrico en un cliente inalámbrico, el programa de instalación pide que se introduzca el SSID.

Todos los clientes inalámbricos y los routers de banda ancha inalámbricos de una WLAN deben utilizar el mismo nombre.

1.5.1.3 Puente inalámbrico

Conocido también como Wireless Bridge, una de las aplicaciones más habituales en redes inalámbricas es como unión de redes remotas. Esta funcionalidad se denomina "Bridge" y supone importantes ahorros respecto a sistemas alternativos como las líneas punto-a-punto o las VPNs a través de Internet. Los smartBridges permiten transmisiones efectivas (throughoutput) entre las dos redes de entre 7Mbps y 9 Mbps,

que en términos práctico es una velocidad de red normal, y es una 36 veces más rápido que una unión por ADSL de 256 Kbps. El único requisito es que los edificios/redes a unir tengan línea visual entre si y distancias inferiores a los 40 km. Si las distancias son mayores de 40 km. harán falta dispositivos adicionales y si no hay línea visual entre los puntos podríamos también recurrir a poner dispositivos intermedios que fuesen visible por los todos los puntos a unir.

Union Bridge Ad-hoc

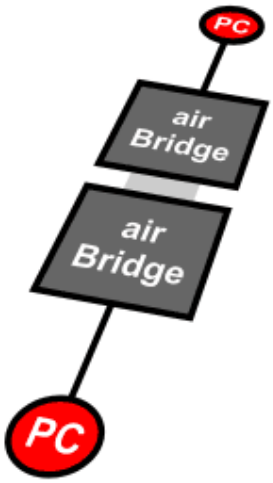


Fig 3. Puente Inalámbrico

Para la unión inalámbrica de dos PCs en modo punto-a-punto, es decir, conectados entre si exclusivamente y sin dar servicio a terceros, la solución más económica es el modo "Bridge Ad-Hoc" de smartBridges. Tan solo hacen falta dos airBridge Total, ni un solo accesorio ni elemento más, y los dos PCs quedan unidos como si lo estuviesen por cable.

Union estandar bridge con visibilidad

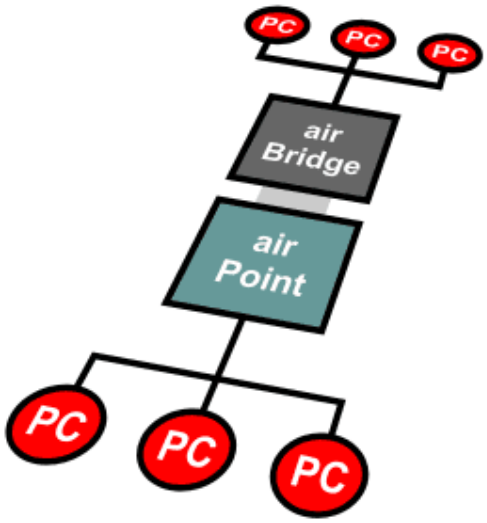


Fig.4 Bridge con visibilidad

Para la unión inalámbrica de dos redes de PCs, o de una red de PCs con un PC, se utilizará una configuración Bridge estándar, en la que deberemos situar un airPoint Pro Total en un extremo (puede ser cualquiera de los dos extremos) y un airBridge Total en el otro. Las dos redes quedarán unidas como si fuesen una sola con visibilidad total entre los PCs.

Union bridge estandar sin visibilidad

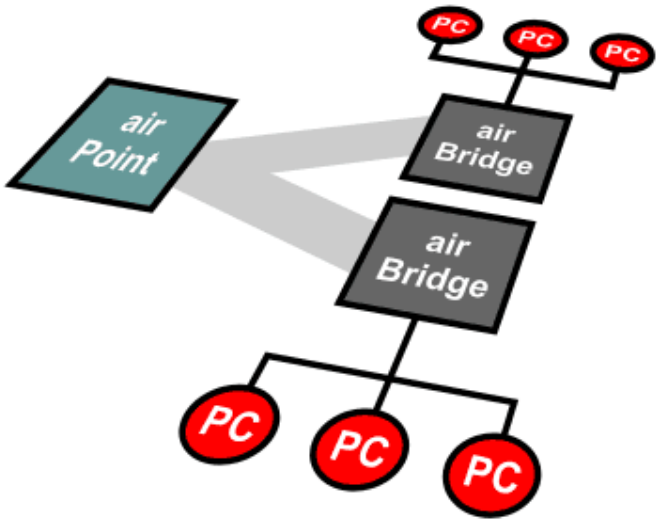


Fig.5 Bridge sin visibilidad

Si entre las dos redes a unir no hay visibilidad porque hay un obstáculo podemos solucionar la conexión instalando un airPoint en algún punto que sea visible por las dos redes a unir, y, al ser el punto intermedio un airPoint podremos reducir costes instalando airBridges en las dos redes. El único requisito del punto intermedio es que tenga corriente eléctrica.

Union multi bridge con visibilidad

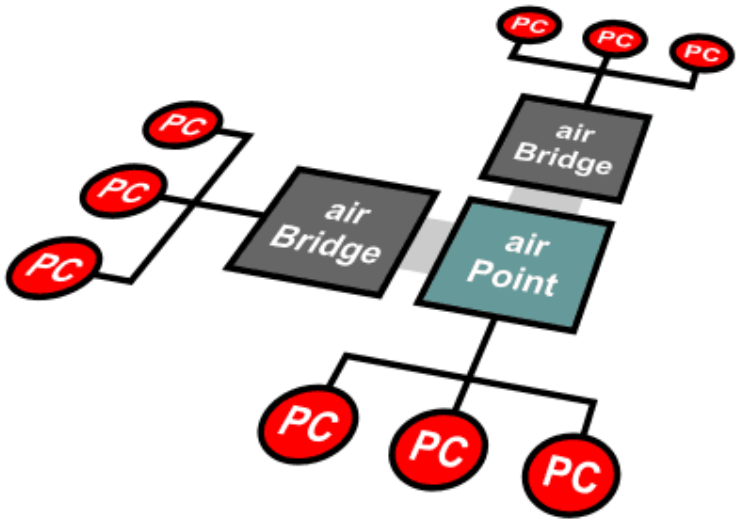


Fig. 6 Multi Bridge con visibilidad

En una unión MultiBridge uniremos más de una red. A diferencia de in Bridge estándar, deberemos situar el airPoint en un punto visible por las demás redes. Las dos redes quedarán unidas como si fuesen una sola con visibilidad total entre los PCs.

Union multi bridge sin visibilidad

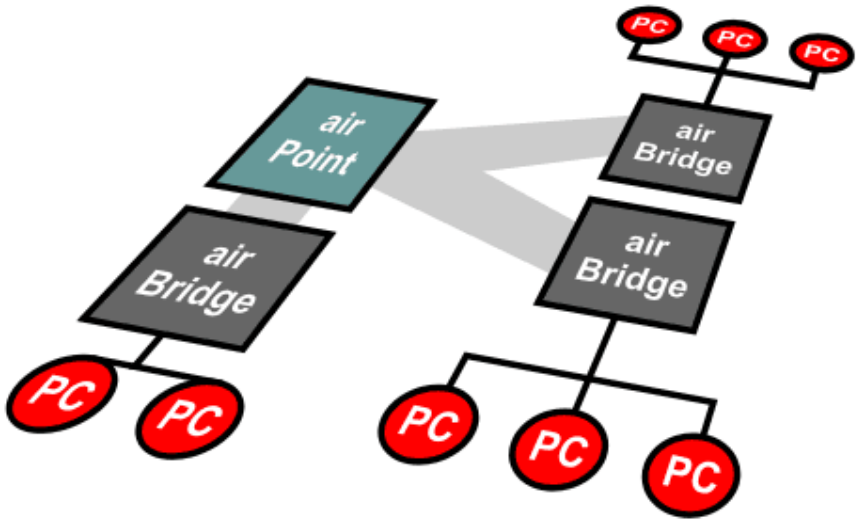


Fig. 7 Multi Bridge sin visibilidad

Si entre las diversas redes a unir no hay visibilidad directa, también podemos hacer un MultiBridge instalando un airPoint en algún punto visible por todas las redes a unir. El único requisito para instalar este "Hub inalámbrico" es una toma de corriente, es decir, podremos poner ese airBridge en cualquier lugar que se vea por todos los puntos a unir y que tenga corriente eléctrica.Mod

1.5.1.4 Puente multi-punto

1.5.1.5 Repetidor

Un repetido**r** es un dispositivo electrónico que recibe una señal débil o de bajo nivel y la retransmite a una potencia o nivel más alto, de tal modo que se puedan cubrir distancias más largas sin degradación o con una degradación tolerable.

En el modelo de referencia OSI el repetidor opera en el nivel físico.

Un repetidor (o generador) es un dispositivo electrónico &uacute que opera sólo en la Capa Física del modelo OSI (capa 1). Un repetidor permite sólo extender la cobertura física de una red, pero no cambia la funcionalidad de la misma. Un repetidor regenera una señal a niveles más óptimos. Es decir, cuando un repetidor recibe una señal muy debil o corrompida, crea una copia bit por bit de la señal original. La posición de un repetidor es vital, éste debe poner antes de que la señal se debilite. En el caso de una red local (LAN) la cobertura máxima del cable UTP es 100 metros; pues el repetidor debe ponerse unos metros antes de esta distancia y poner extender la distancia otros 100 metros o mas.

Existen también regeneradores ópticos conocidos como EDFA (Erbium-Doped Fiber Amplifier) los cuales permiten extender la distancia de un haz de luz sobre una fibra óptica hasta 125 millas.

1.6 TIPOS DE ANTENAS Y SU ESTANDARES DE INSTALACIÓN

1.6.1 Antenas direccionales o (directivas).

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz concreto y estrecho pero de forma intensa (más alcance).

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

1.6.2 Antenas omni-direccionales

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance.

Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que

se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

1.6.2 Antenas sectoriales

Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con un haz de luz más ancho de lo normal.

Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120º ó 4 antenas sectoriales de 80º. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

Selección de antenas a utilizarse.

Las antenas direccionales se suelen utilizar para unir dos puntos a largas distancias mientras que las antenas omnidireccionales se suelen utilizar para dar señal extensa en los alrededores. Las antenas sectoriales se suelen utilizan cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa.

Si necesita dar cobertura de red inalámbrica en toda un área próxima (una planta de un edificio o un parque por ejemplo) lo más probable es que utilice una antena omnidireccional. Si tiene que dar cobertura de red inalámbrica en un punto muy concreto (por ejemplo un PC que está bastante lejos) utilizará una antena direccional, finalmente, si necesita dar cobertura amplia y a la vez a larga distancia, utilizará antenas sectoriales.

Apertura vertical y apertura horizontal de una antena

La apertura es cuanto se "abre" el haz de la antena. El haz emitido o recibido por una antena tiene una abertura determinada verticalmente y otra apertura determinada horizontalmente.

En lo que respecta a la apertura horizontal, una antena omnidireccional trabajará horizontalmente en todas direcciones, es decir, su apertura será de 360º. Una antena direccional oscilará entre los 4º y los 40º y una antena sectorial oscilará entre los 90º y los 180º.

La apertura vertical debe ser tenida en cuenta si existe mucho desnivel entre los puntos a unir inalámbricamente. Si el desnivel es importante, la antena deberá tener mucha apertura vertical. Por lo general las antenas, a más ganancia (potencia por decirlo de

algún modo) menos apertura vertical. En las antenas direccionales, por lo general, suelen tener las mismas aperturas verticales y horizontales.

1.7 INSTALACIÓN Y CONFIGURACION DE LAS TARJETAS DE RED INALAMBRICA

Instalación de la tarjeta de red inalámbrica.

En este paso se explica cómo instalar la tarjeta PCMCIA 3Com modelo "OfficeConnect Wireless 11g PC Card". Si dispone de otro modelo de tarjeta, consulte su manual, el procedimiento debe ser parecido.

Si no tenemos instalada la tarjeta de red inalámbrica, al pincharla el sistemas la detectará automáticamente. Si no es así nos iremos a inicio ?configuración ? Panel de control ? Agregar hardware. En este caso lo que haremos será elegir la tarjeta de red e introducir el CD que acompaña a la tarjeta para la instalación de los drivers.

- Inserte el CD-ROM que acompaña a la tarjeta.
- Inserte la tarjeta PCMCIA en la ranura de su ordenador portátil.
- En la ventana que aparece, elija "Instalar automáticamente el software (recomendado)" y pulse el botón "Siguiente >":

Asistente para la instalación de nuevo hardware.

- En la siguiente ventana, elija la primera opción y pulse el botón "Siguiente >":

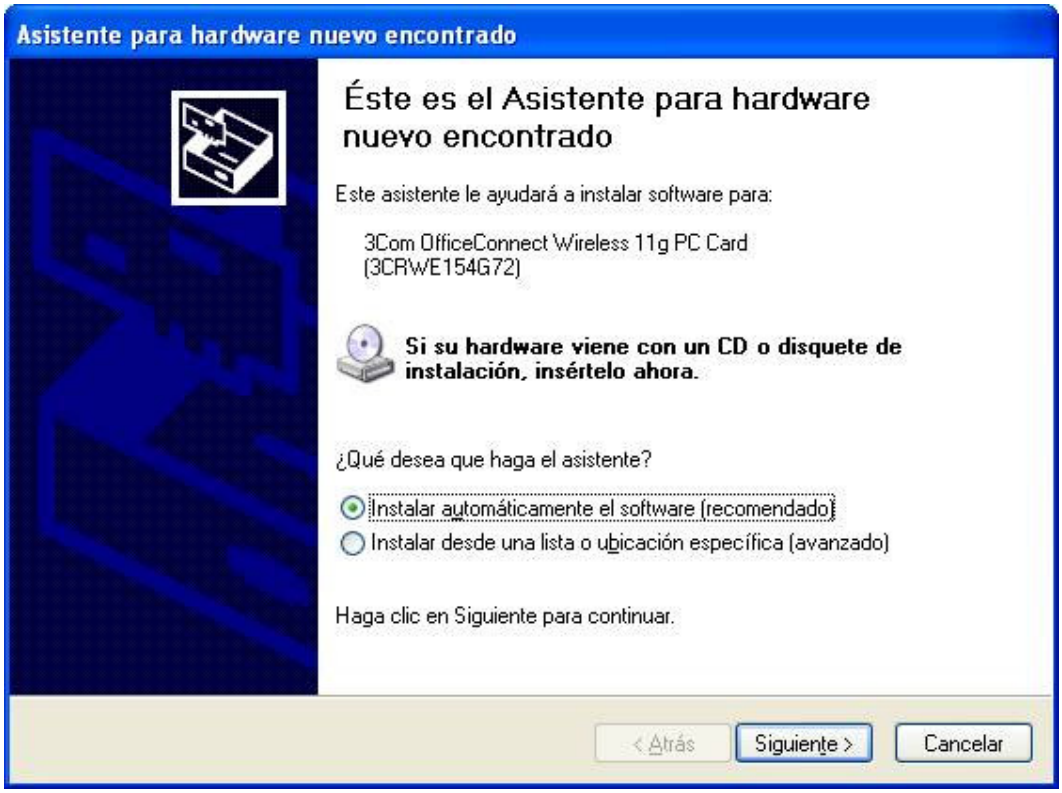


Fig 8 Inicio del asistente para instalacion

Asistente para la instalación de nuevo hardware.

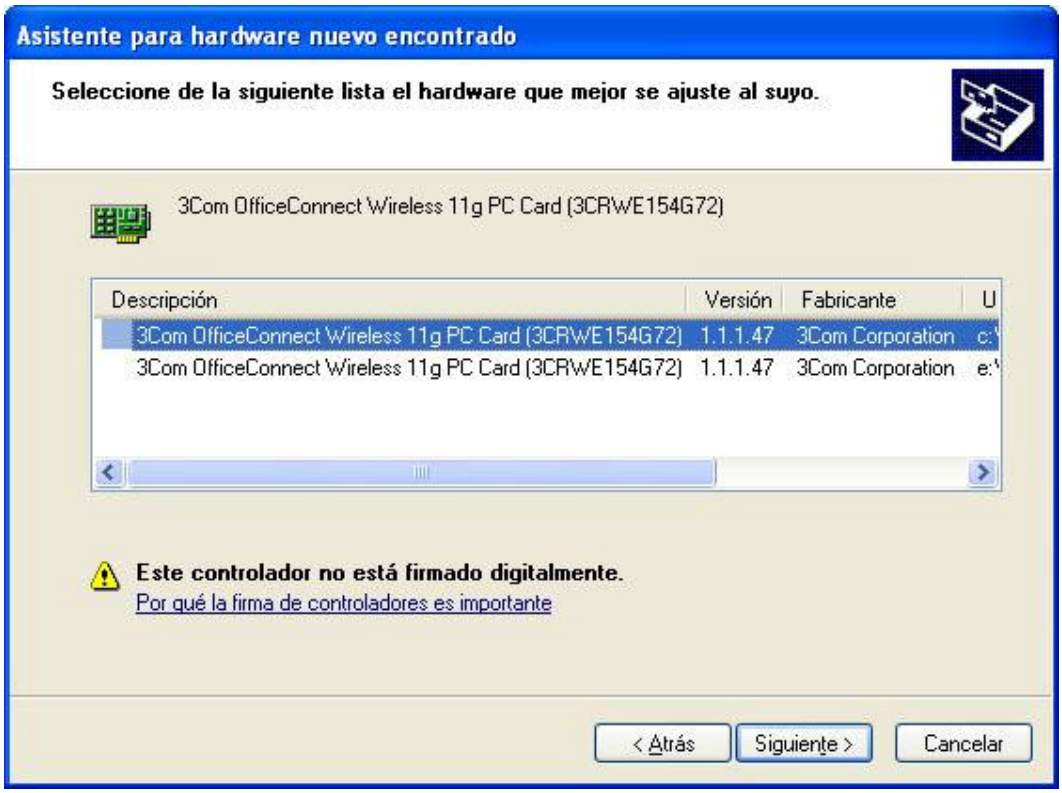


Fig 9 Asistente para instalación de nuevo hardware

- Cuando Windows le advierta sobre la firma del controlador, elija "Continuar":

Pantalla del certificado de red.

Fig 10 Certificado de red

- En la siguiente ventana se le pedirá que elija su país. Seleccione "Spain" y pulse el botón "OK":

Pantalla de selección de idioma.

Fig. 11 Selección de idioma

- Para terminar con éxito la instalación, pulse el botón "Finalizar":

Pantalla de finalización de instalación de hardware.

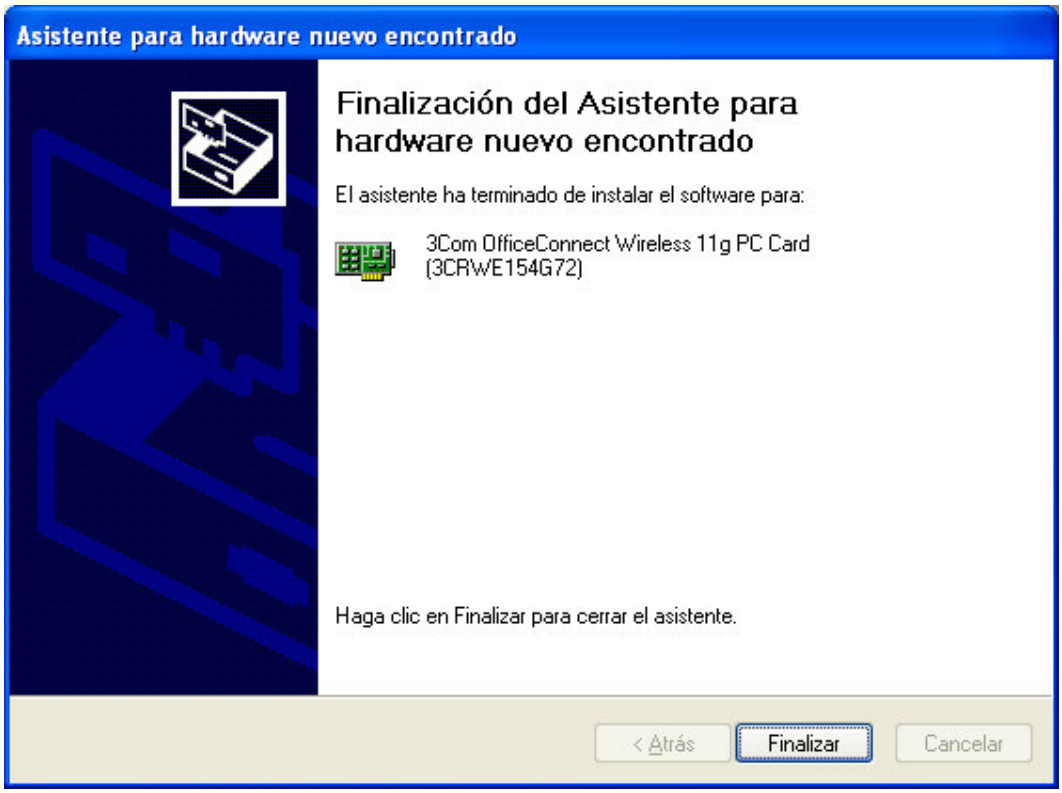


Fig. 12 Finalizacion de instalacion

Instalación de la tarjeta de red inalámbrica.

Este paso sólo es necesario si es la primera vez que accedemos a la red inalámbrica o si hemos cambiado la configuración.

En la barra de tareas de nuestro escritorio podemos pulsar con el botón derecho sobre el icono de red inalámbrica y pulsar sobre ver redes inalámbricas disponibles.

Pantalla de finalización de instalación de hardware.

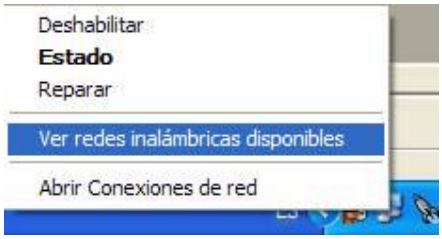


Fig. 13 Finalización de la instalación

A continuación veremos las redes que ha detectado la tarjeta de red, en caso de no ser alguna de las redes detectadas la que nos interesa o en caso de no haber detectado ninguna red inalámbrica, lo que haremos será pulsar en el botón de Opciones avanzadas... para pasar a configurar la nuestra red.

Pantalla donde podemos ver las redes disponibles.

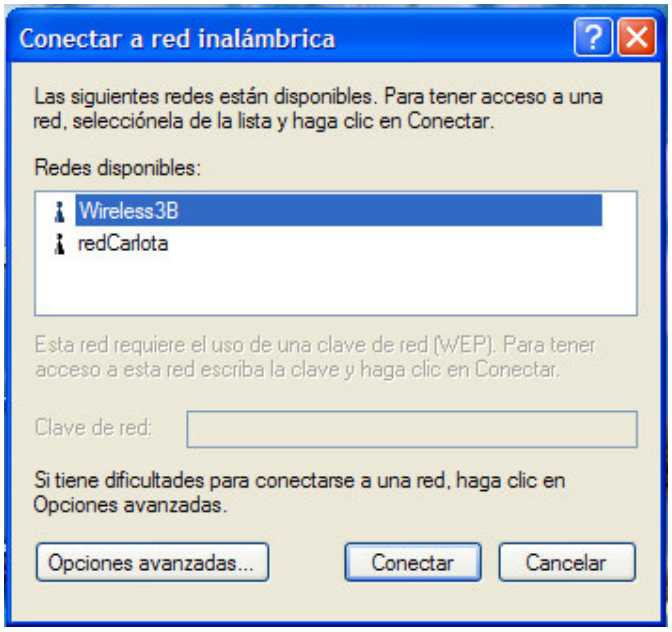


Fig 14 Pantalla de redes inlambricas

En la pantalla siguiente pulsaremos la opción de Usar Windows para establecer mi conf. de red inalámbrica.

Pantalla de configuración y selección de nuestra red.

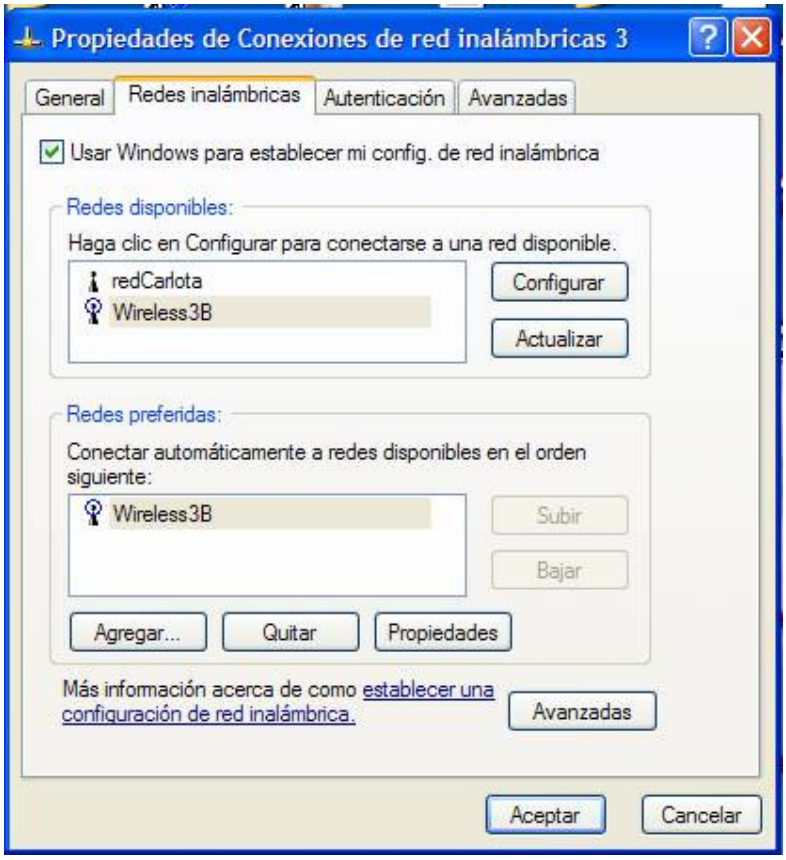


Fig 15 Selección de la red

Si ninguna de las redes detectadas es la correcta lo que haremos será quitar estas redes y pulsando en el botón quitar tras seleccionar la red adecuada posteriormente lo que haremos será agregar nuestra red, pulsando en el botón agregar.

Pantalla de configuración de red.

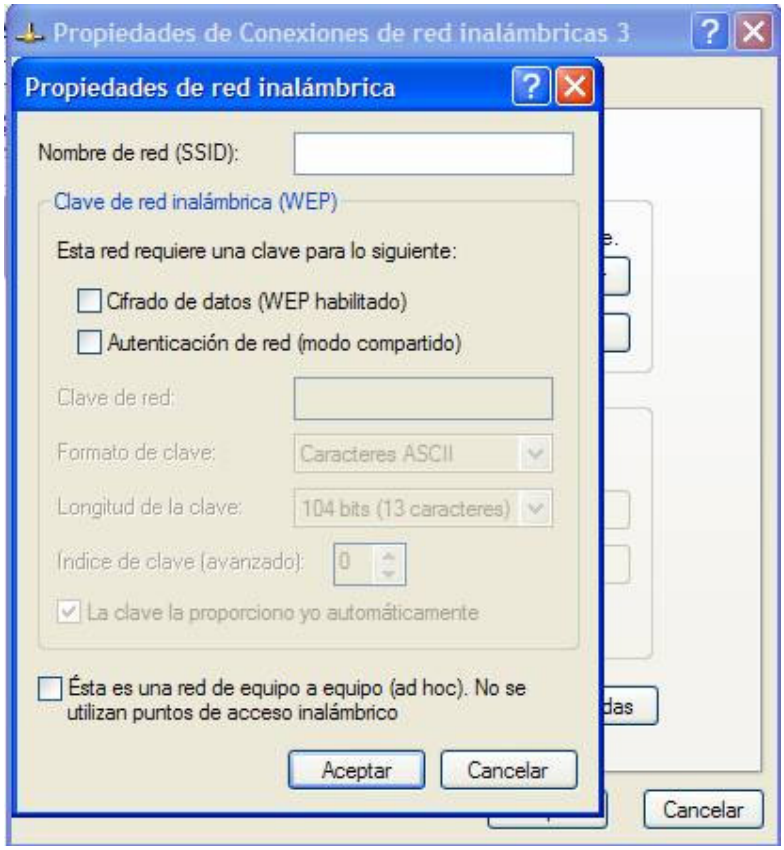


Fig. 16 Pantalla configuración de la red

A continuación escribiremos el nombre de la red que queremos instalar en el campo SSID, en nuestro caso escribiremos ESI2 como nombre de nuestra red.

El resto de campos lo utilizaremos para asignar una clave WEP para no permitir que usuarios no autorizados se puedan conectar a nuestra red. Pulsaremos en el botón de opción Cifrado de datos (WEP habilitado) y escribiremos la contraseña de cifrado, en nuestro caso escribiremos ?administrador2?.

Pantalla de configuración de red.

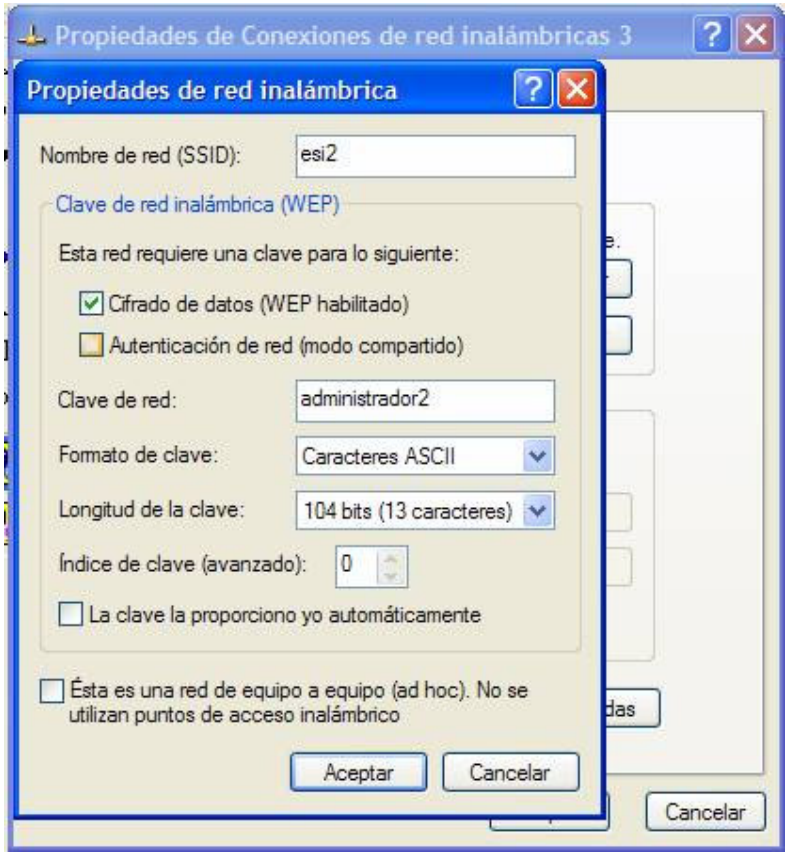


Fig. 17 Configuración de la red (1)

No es necesario marcar las demás opciones, simplemente pulsaremos aceptar y ya nos aparecerá la red que queremos utilizar.

Pantalla de configuración de red.

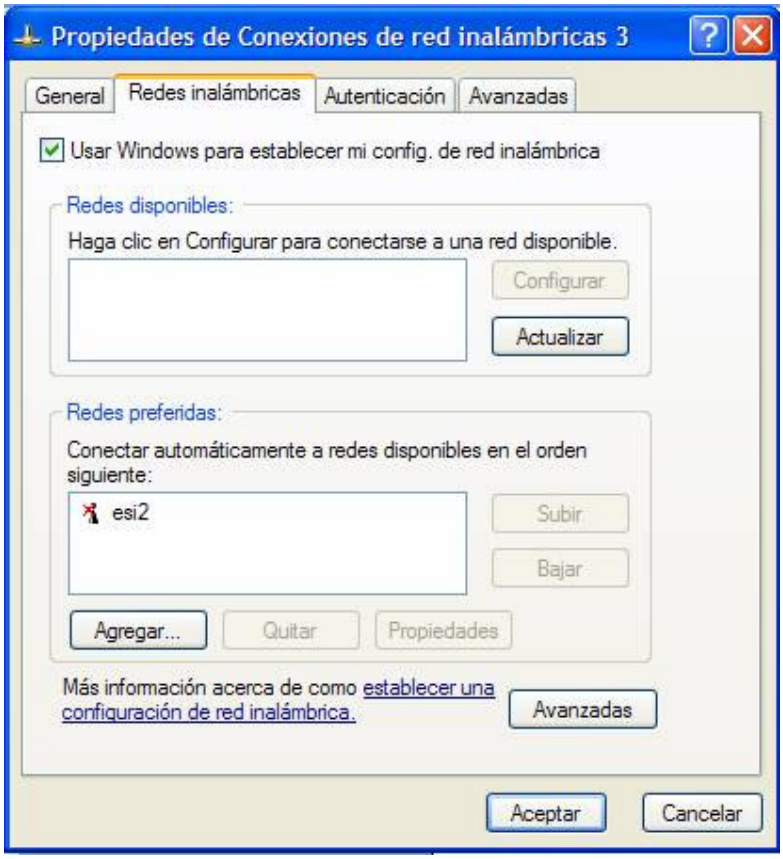


Fig 18 Propiedades de la conexión

En este momento nos aparecerá nuestra red dentro de redes preferidas, de no ser así habrá que pulsar en el botón actualizar para que recargue la red y pueda detectar nuestra red.

El resto de pestañas que tenemos las utilizaremos para la configuración de la tarjeta de red en sus opciones avanzadas:

Pantalla de Autenticación de la red inalámbrica.

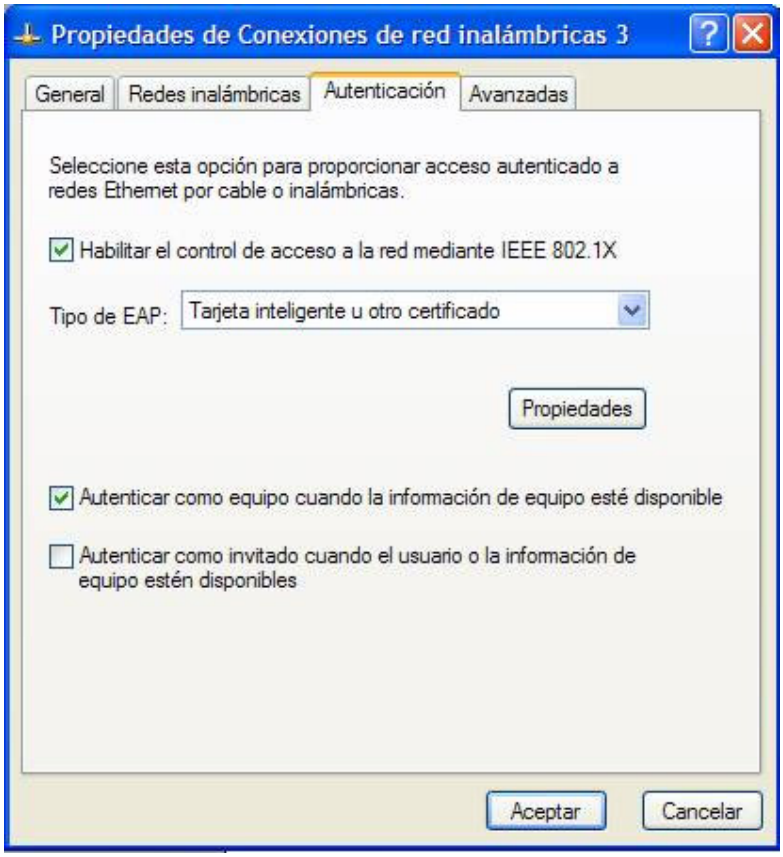


Fig. 19 Pantalla de autenticación de la red

La pestaña de autenticación la utilizaremos para indicar que el equipo se autentique en la red y pulsando en el botón de propiedades nos pedirá si queremos usar el certificado de red o si queremos conectarnos a una red en particular. Estas opciones las dejaremos por defecto como las detecte la red.

Pantalla de opciones avanzadas de la red inalámbrica.

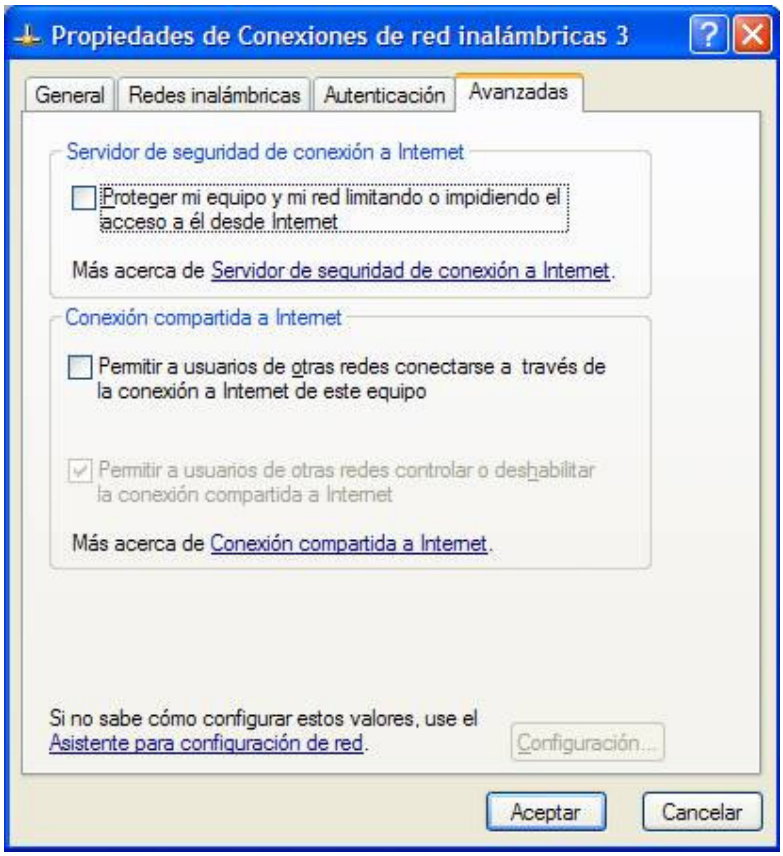


Fig. 20 Propiedades inalambricas

La pestaña Avanzada la utilizaremos para indicar si queremos proteger el equipo impidiendo el acceso desde Internet a él.

Además podemos permitir a otros usuarios conectarse a través de él por Internet.

1.8 VENTAJAS Y DESVENTAJAS DEL USO DE TARJETAS INALAMBRICAS.

Una de las desventajas que tiene el sistema Wi-Fi es la pérdida de velocidad en relación a la misma conexión utilizando cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan

calcular la contraseña de la red y de esta forma acceder a ella, las claves de tipo WEP son relativamente *fáciles de conseguir* para cualquier persona con un conocimiento medio de informática. La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad.

Los dispositivos Wi-Fi ofrecen gran comodidad en relación a la movilidad que ofrece esta tecnología, sobre los contras que tiene Wi-Fi es la capacidad de terceras personas para conectarse a redes ajenas si la red no está bien configurada y la falta de seguridad que esto trae consigo.

Cabe aclarar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.[4]

Ventajas: No hay que pasar cables por dentro de las paredes o por los pasillos; puede usar su portátil para navegar por la Web. Desventajas: Más costosa que la tecnología alambrada. Deber configurarse con cuidado para aumentar el alcance y la seguridad. La evolución de las normas puede causar confusión e incompatibilidades. La velocidad disminuye a medida que aumenta la distancia.

Movilidad**:** las redes inalámbricas proporcionan a los usuarios de una LAN 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. Simplicidad y rapidez en la instalación: la instalación de una

[4] http://es.wikipedia.org/wiki/Wi-Fi

WLAN es rápida y fácil y elimina la necesidad de tirar cables a través de paredes y techos. Flexibilidad en la instalación: La tecnología inalámbrica permite a la red llegar a puntos de difícil acceso para una LAN cableada.

Costo de propiedad reducido: mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN, 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.

Escalabilidad: los sistemas de WLAN 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.

1.9 MANEJO DE LAS SEGURIDADES EN LAS REDES INALAMBRICAS.

1.9.1 Radius

RADIUS (acrónimo en inglés de *Remote Authentication Dial-In User Server*). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red) *sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor* RADIUS comprueba que la información es correcta utilizando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores de Acceso a la Red (NAS), más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes).

RADIUS es extensible; la mayoría de fabricantes de software y hardware RADIUS implementan sus propios dialectos.

1.9.2 Seguridad en WLAN

Las redes inalámbricas requieren nuevos conceptos de seguridad que se obvian en las redes cableadas. Un intruso que busque acceso a una LAN cableada se enfrenta irremediablemente con el problema del acceso físico a la misma. El villano necesita conectar su cable al switch. En una WLAN el problema del intruso se torna etéreo. Le basta permanecer en el área de cobertura –que puede ser muy extensa- para estar en contacto con la red local. Puede incluso estar en movimiento.

Esta nueva situación obliga a la búsqueda de nuevas soluciones para garantizar la seguridad de los usuarios. Vamos a procurar hacer una exposición simple y rápida.

¿Qué es seguridad?

Autenticidad: El usuario es quien dice ser.
Privacidad: La información no es legible por terceros.
Integridad: La información no puede ser alterada en tránsito.

Al principio fue el WEP.

Primer intento. Fallido. WEP (Wired Equivalent Privacy) Privacidad equivalente a red cableada. Es -o mejor dicho, era- el primer estándar de seguridad. Con este estándar el usuario debía introducir un juego de claves, que podían ser de 40 o de 104 bits, coincidente con las configuradas en el punto de acceso. Un sistema de clave compartida (PSK, Pre-Shared Key).

Primer problema. Todos los usuarios deben usar las mismas claves. No es necesario describir los inconvenientes que tiene este sistema.

Segundo problema: Se reservan 24 bits para lo que se conoce como "Vector de inicialización" (IV) Una especie de clave de sesión que varía de manera periódica y automática y que se añade a las claves configuradas por el usuario. Este IV se transmite en claro, sin encriptar y es muy pequeño. Un atacante puede sin demasiada dificultad determinar el IV por fuerza bruta y desencriptar el tráfico o inyectar paquetes válidos en la red. Además, el algoritmo que sirve para determinar estos 24 bits adolece de cierta predictibilidad que hace más eficaz a la fuerza bruta.

Nótese que el que logre romper la clave habrá roto también los tres conceptos que definíamos como seguridad: Puede acceder como usuario legítmo y puede observar y modificar el tráfico del resto.

WPA (Wi-Fi Protected Access)

Este estándar desarrollado por la Wi-Fi alliance trata de ser el sustituto de WEP. A la hora de diseñarlo se trató de que fuera compatible con la mayor cantidad de dispositivos ya presentes en el mercado. WPA puede ser incorporado en muchos sistemas diseñados para WEP sin más que una actualización de firmware.

TKIP (Temporal Key Integrity Protocol)

Al contrario que WEP, utiliza claves de sesión dinámicas de 128 bits, para cada usuario, cada sesión y cada paquete. Los usuarios deben acceder a través de un servidor de autentificación, típicamente un RADIUS. Una vez autentificados mutuamente el

servidor genera una clave “master” que transmite de manera segura al cliente y que será utilizada para enviar el resto de claves auxiliares que serán utilizadas durante esa sesión.

MIC (Message Integrity Check)

Se trata de un sistema que garantiza que un paquete no ha sido modificado en tránsito.

Con WPA desaparece el problema de las claves compartidas, ya que una clave “master” distinta es recibida por cada usuario cada vez que RADIUS acepta sus credenciales. Con este sistema el administrador puede aceptar o eliminar usuarios del sistema sin necesidad de cambiar todas las claves.

Con WPA tenemos las tres cuestiones que definen la seguridad resueltas de manera robusta:

RADIUS provee la autentificación.
TKIP la privacidad.
MIC la integridad.

En el GUI hemos conseguido establecer una WLAN con WPA utilizando FreeRADIUS y clientes WindowsXP y Linux con xsupplicant satisfactoriamente con varios puntos de acceso: D-Link 900AP+, Linksys WRT54G y Cisco Aironet 1200+IOS.

SOHO (Small Office and Home Office)

Los usuarios que no deseen usar un servidor de acceso pueden seguir utilizando el sistema de clave compartida, ya que WPA lo permite, aunque sin necesiad de preocuparse por los problemas de seguridad de WEP.

Hasta la fecha la única vulnerabilidad que se ha descrito referente a WPA se refiere a sistemas que han sido establecidos con SOHO y claves PSK demasiado cortas y/o vulnerables a ataques por diccionario.

No dispongo de WPA ¿Cómo puedo asegurar mi red?

Se pueden utilizar un conjunto de medidas que reducen las posibilidades de ver la red comprometida:

Deshabilitar la difusión del SSID: No llamar la atención.

Habilitar WEP.

Habilitar el filtrado por MAC: Es un método de autentificación muy débil. Una vez roto el WEP las MAC's de los usuarios legítimos son visibles. Muchos adaptadores Wi-Fi permiten cambiar la MAC de fábrica por otra cualquiera.

Utilizar encriptación en capas superiores: HTTPS, POP3S, SSH siempre que sea posible.

Sistema abierto:

Cualquier cliente puede asociarse a la red sin autentificarse. En este caso podría establecerse un filtro que confinara el tráfico a la red del GUI. El tráfico va sin encriptar. La autentificación abierta es el sistema que utilizan los AP's de gama baja. Es posible restringir el acceso y encriptar estableciendo un WEP estático, en cuyo caso el cliente que no conoce el WEP puede asociarse pero no pasar tráfico a través del AP. El WEP es un método muy frágil. Existe software capaz de romper un WEP con facilidad. Los clientes que conocen el WEP pueden escucharse mutuamente. Si se me permite la fivolidad el WEP es un mecanismo de seguridad de "Todo a 100".

- Autentificación por MAC.

El AP comprueba la MAC del cliente antes de permitir el acceso. Las MAC pueden configurarse tanto tanto en el AP como en un ACS. En este momento el Aironet utiliza un servidor RADIUS para autentificar las MAC de los clientes en los SSID's correspondientes. En este apartado procede hacer los mismos comentarios respecto al WEP y a la encriptación que en el apartado anterior. La dirección MAC de un cliente legítimo puede ser capturada por un atacante. Las tarjetas Orinoco (y todas las que tienen un chipset prism) permiten la modificación de su MAC. Con este sistema se podría establecer un filtro que obligase a utilizar encriptación en SSL o a nivel de aplicación (pop3s, imaps, SSH, HTTPS) y HTTP.

-Autentificación_EAP

Protocolo extensible de autentificación. Es un protocolo que sirve para adaptar a las redes inalámbricas protocolos ya establecidos y otros nuevos. Este sistema requiere siempre un ACS. EAP utiliza dos WEP comos claves de sesión que las partes implicadas acuerdan durante la autentificación y que se cambia con una frecuencia que determina el administrador del AP. Un WEP es para el tráfico broadcast y otro se establece para cada cliente de manera que los clientes no pueden escucharse mutuamente. Yo considero que este mecanismo es muy seguro. La política de filtros para esta autentificación podría ser completamente abierta.

EAP-MD5

Mediante EAP se autentifica realizando un intercambio de claves "cifradas" por MD5. El autentificador puede ser nombre de usuario y contraseña o una dirección MAC. Linux y WinXP pueden asociarse por este método. Con WinXPSP1 desaparece la

autentificación EAP-MD5 que es sustituida por EAP-MS-CHAPv2 que freeradius aún no soporta.

EAP-TLS

TLS: Seguridad en la capa de transporte. La autentificación se realiza mutuamente mediante certificados. Con este sistema tanto el ACS como el cliente deben demostrar su identidad. Sólo WinXPSP1 soporta este método. WinXP lo hace defectuosamente. Esta configuración es para el AP "raíz". La red se extiende fácilmente manteniendo estas configuraciones sin mas requerimientos que asociar correctamente los puntos de acceso que funcionan como repetidores.

1.9.3 Mecanismo WEP (wired equivalent privacy)

WEP (Wired Equivalent Privacy, privacidad equivalente al cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11 . Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autentificación y control de acceso en redes WLAN . Estudiamos a continuación las principales características de WEP.

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 red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. 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 de encriptación utilizado es RC4 con claves (seed), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama. El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero sabemos ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Observemos que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, Integrity Check Value).
2. Se concatena la clave secreta a continuación del IV formado el seed.
3. El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream), a partir del seed, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.

5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (frame body) de la trama IEEE 802.11.

El algoritmo para descifrar es similar al anterior. Debido a que el otro extremo conocerá el IV y la clave secreta, tendrá entonces el seed y con ello podrá generar el keystream. Realizando el XOR entre los datos recibidos y el keystream se obtendrá el mensaje sin cifrar (datos y CRC-32). A continuación se comprobara que el CRC-32 es correcto.

Debilidad del vector de inicialización

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Recordemos que el IV es la parte que varía de la clave (seed) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica cómo manejar el IV. Según se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello. Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama. Y esto ocasiona que los primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si tenemos en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de IVs diferentes no es demasiado elevado (2^24=16 millones aprox.), por lo que terminarán repitiéndose en cuestión de minutos u horas [6]. El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se

repitiese nunca, pero como vemos, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red. Observemos que es trivial saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática.

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Bien es cierto que existen implementaciones con claves de 128 bits (lo que se conoce como WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

¿Qué podemos hacer una vez hemos capturado varias tramas con igual IV, es decir, con igual keystream? Necesitamos conocer el mensaje sin cifrar de una de ellas. Haciendo el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV. Conociendo el keystream asociado a un IV, podremos descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no es tan complicado, porque existen tráficos predecibles o bien, podemos provocarlos nosotros (mensajes ICMP de solicitud y respuesta de eco, confirmaciones de TCP, etc.)

Con lo que hemos descrito no podemos deducir la clave secreta, aunque sí es posible generar una tabla con los IVs de los que sabemos su keystream, la cual permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla.

Sin embargo, podemos llegar a más y deducir la clave secreta. Una nueva vulnerabilidad del protocolo WEP permite deducir la clave total conociendo parte de la clave (justamente, el IV que es conocido). Para ello necesitamos recopilar suficientes IVs y sus keystreams asociados obtenidos por el procedimiento anterior.

Otras debilidades de WEP

WEP también adolece de otros problemas además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Entre los objetivos de WEP, como comentamos más arriba, se encuentra proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, por ejemplo, modificar algún número de la trama sin que el destino se percatara de ello. En lugar del algoritmo de CRC se recomienda como ICV (Integrity Check Value) un algoritmo diseñado para tal fin como SHA1-HMAC

El estándar IEEE 802.11 incluye un mecanismo de autentificación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que describimos a continuación. Una estación que quiere unirse a una red, solicita al punto de acceso autentificación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de autentificación de secreto compartido tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino, el mecanismo ofrece

información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización explicadas más arriba.

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (podrán entrar aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso tendríamos una autentificación de sistema abierto, es decir, sin autentificación.

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (replay). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica

Alternativas a WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64 bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como WEP2. Sin embargo, debemos observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar

el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es WEP dinámico. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de autentificación (RADIUS normalmente) funcionando en la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN. Tiene como inconveniente la falta de interoperatibilidad entre dispositivos de distintos fabricantes.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA y WPA2 (IEEE 802.11i). El primero es de 2003 y el segundo se espera para 2004. Se estudian a continuación.

.9.4 Mecanismo WAP (Wi-Fi Protected Access)

WPA (Wi-Fi Protected Access, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicarán en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaban suficientemente maduras y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible.

Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

WPA incluye las siguientes tecnologías:

- IEEE 802.1X. Estándar del IEEE de 2001 para proporcionar un control de acceso en redes basadas en puertos. El concepto de puerto, en un principio pensado para las ramas de un switch, también se puede aplicar a las distintas conexiones de un punto de acceso con las estaciones. Las estaciones tratarán

entonces de conectarse a un puerto del punto de acceso. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique. Con este fin se utiliza el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS (Remote Authentication Dial-In User Service). Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

- EAP. EAP, definido en la RFC 2284, es el protocolo de autentificación extensible para llevar a cabo las tareas de autentificación, autorización y contabilidad. EAP fue diseñado originalmente para el protocolo PPP (Point-to-Point Protocol), aunque WPA lo utiliza entre la estación y el servidor RADIUS. Esta forma de encapsulación de EAP está definida en el estándar 802.1X bajo el nombre de EAPOL (EAP over LAN).
- TKIP (Temporal Key Integrity Protocol). Según indica Wi-Fi, es el protocolo encargado de la generación de la clave para cada trama.
- MIC (Message Integrity Code) o Michael. Código que verifica la integridad de los datos de las tramas.

3.2 Mejoras de WPA respecto a WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48

combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados. El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (replay).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

Modos de funcionamiento de WPA

WPA puede funcionar en dos modos:

- Con servidor AAA, RADIUS normalmente. Este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- Con clave inicial compartida (PSK). Este modo está orientado para usuarios domésticos o pequeñas redes. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en

WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de los datos.

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.

WPA2 incluye el nuevo algoritmo de cifrado AES (Advanced Encryption Standard), desarrollado por el NIS . 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 (Counter-Mode / Cipher Block Chaining / 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).[5]

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

1.9.5 Amenazas

Una diferencia esencial entre las redes Ehernet y las inalámbricas es que estas últimas se construyen en un medio compartido. Se parecen más a los viejos concentradores de red que a los conmutadores modernos, en ellas cada computadora conectada a la red puede "ver" el tráfico de todos los otros usuarios. Para monitorear todo el tráfico de la red en un punto de acceso, uno puede simplemente sintonizar el canal que se está utilizando, colocar la tarjeta de red en el modo de monitoreo, y registrar cada paquete. Estos datos pueden ser de mucho valor para alguien que los escucha a escondidas (incluyendo datos como el correo electrónico, datos de voz o registros de conversaciones en línea). Esto también puede proveer contraseñas y otros datos de gran valor, posibilitando que la red se vea comprometida en el futuro. Como veremos más adelante en este capítulo, este problema puede mitigarse con el uso de la encriptación.

Otro problema serio de las redes inalámbricas es que los usuarios son relativamente anónimos. Todos los dispositivos inalámbricos incluyen una dirección MAC única, la cual es asignada por el fabricante, pero esas direcciones a menudo pueden ser modificadas con ciertos programas. Aún teniendo la dirección MAC, puede ser muy difícil identificar donde está localizado físicamente un usuario inalámbrico. Los efectos del eco, las antenas de gran ganancia, y una amplia variedad de características de los transmisores de radio, pueden hacer que sea imposible determinar si un usuario malintencionado está en el cuarto de al lado o en un lujar muy alejado.

Si bien el espectro sin licenciamiento implica grandes ahorros económicos para el usuario, por otro lado tiene el desafortunado efecto colateral de que los ataques de denegación del servicio (DoS por su sigla en inglés) son extremadamente simples. Simplemente con encender un punto de acceso

de alta potencia, un teléfono inalámbrico, un transmisor de video, o cualquier otro dispositivo de 2.4 GHz, una persona con malas intenciones puede causar problemas significativos a la red. Muchos dispositivos de red son vulnerables también a otras formas de ataques de denegación del servicio, tales como una avalancha de desasociaciones (disassociation flooding) y el desborde de las tablas ARP.

Les presentamos varias categorías de personas que pueden causar problemas a una red inalámbrica:

- Usuarios involuntarios. Como la mayoría de las redes inalámbricas están instaladas en áreas muy pobladas, es común que los usuarios de computadoras portátiles se asocien accidentalmente a la red equivocada. La mayoría de los clientes va a elegir cualquier red disponible si la de su preferencia no lo está. Los usuarios pueden hacer uso de esta red como lo hacen habitualmente, ignorando completamente que pueden estar transmitiendo datos importantes en la red de alguien más. Las personas malintencionadas pueden aprovechar esta situación instalando puntos de acceso en lugares estratégicos, para intentar atacar usuarios desprevenidos y capturar sus datos. El primer paso para evitar este problema es educar a sus usuarios, y subrayar la importancia de conectarse solamente a redes conocidas y de confianza. Muchos clientes inalámbricos pueden configurarse para conectarse solamente a redes confiables, o para pedir permiso antes de incorporarse a una nueva red. Como veremos más adelante en este capítulo los usuarios pueden conectarse de forma segura a redes públicas abiertas utilizando una encriptación fuerte.

- War drivers. El fenómeno de los “war drivers” (buscadores de redes) basa su nombre en la famosa película sobre piratas informáticos de 1983, “Juegos de Guerra” (War Games). Ellos están interesados en encontrar la ubicación física de las redes inalámbricas. En general se mueven por la ciudad equipados con una computadora portátil, un GPS, y una antena omnidireccional, registrando el nombre y la ubicación de cada red que localizan. Luego se combinan esos registros con los de otros buscadores de redes transformándose en mapas gráficos describiendo las “huellas” inalámbricas de una ciudad. La amplia mayoría de los buscadores de redes no representa una amenaza directa a la red, pero los datos que recolectan pueden ser de interés para aquellos que se dedican a atacar redes. Por ejemplo, un punto de acceso desprotegido detectado de esta manera, puede estar ubicado en un edificio importante, como una oficina de gobierno o de una empresa. Una persona con malas intenciones puede utilizar esta información para acceder a esa red ilegalmente. La instalación de ese AP nunca debió haber sucedido en primer lugar, pero los buscadores de redes hacen más urgente la solución de este problema. Como veremos más adelante en este capítulo, los buscadores de redes que utilizan el famoso programa NetStumbler pueden ser detectados con otros programas como el Kismet.

- Puntos de acceso deshonestos. Hay dos clases generales de puntos de acceso deshonestos: aquellos instalados incorrectamente por usuarios legítimos, y los instalados por gente malintencionada que piensa en recolectar datos o dañar la red. En el caso más sencillo, un usuario legítimo de la red, puede querer una mejor cobertura inalámbrica en su oficina, o puede que encuentre demasiado difíciles de cumplir las restricciones de seguridad de la red inalámbrica

corporativa. Al instalar un punto de acceso sin autorización, el usuario abre la red desde el interior de la misma a los ataques potenciales. Si bien existe la posibilidad de rastrear a través de la red puntos de acceso no autorizados, es muy importante tener una política clara que los prohíba. Puede que sea muy difícil lidiar con la segunda clase. Al instalar un AP de gran potencia que utilice el mismo ESSID de la red, una persona puede engañar a la gente para que use este equipo y registrar o manipular todos los datos que pasan por él. Repetimos, si sus usuarios están entrenados para usar una fuerte encriptación, este problema se va a deducir de forma significativa.

- Escuchas Subrepticias. Como mencionamos antes, este es un problema muy difícil de manejar en las redes inalámbricas. Utilizando una herramienta de monitoreo pasiva (como Kismet), un fisgón puede registrar todos los datos de la red desde lejos sin que ni siquiera se note su presencia. Los datos encriptados pobremente simplemente pueden registrarse y luego descifrarse, mientras que los datos sin encriptación se pueden leer fácilmente en tiempo real. Si a usted le es difícil convencer a otros de este problema, puede realizar una demostración con herramientas como Etherpeg o Driftnet. Estas herramientas buscan datos gráficos en redes inalámbricas, tales como archivos GIF y JPEG. Mientras que los usuarios están navegando en Internet, estas herramientas despliegan todos los gráficos encontrados en un collage. A menudo utilizo estas herramientas cuando estoy dando una charla de seguridad inalámbrica. Usted le puede decir a un usuario que su correo electrónico es vulnerable si no tiene encriptación, pero nada les hace llegar mejor el mensaje que mostrarles las imágenes que están

buscando en su navegador web. Si bien no puede ser prevenido por completo, el uso de una fuerte encriptación va a desalentar las escuchas subrepticias.[6]

- ORIGEN

  Cuando las primeras empresas comenzaron a implementar la tecnología inalámbrica, aquellas que las siguieron lo hicieron guiadas por los grandes beneficios que ésta ofrecía, se introdujeron entonces estándares para la interoperabilidad entre las diferentes marcas de equipos y dispositivos, lo cual facilitó la penetración de dichas soluciones en el mercado y su uso en zonas donde era costoso o difícil mantener o instalar el cableado para una red.

  Pero sucedió que entre el frenesí por implementarlas se pasaron por alto los riesgos en seguridad que venían implícitos y poco tiempo después comenzaron a hacerse notar las amenazas inherentes a una red de este tipo.

  Y es que los problemas de seguridad en cuanto al protocolo IEEE 802.11 o Wi-Fi (un grupo de estándares desarrollados por el grupo 11 del IEEE LAN/MAN Standards Committee (IEEE 802 http://www.ieee802.org/) existen de forma implícita en éste debido a su diseño y a que los mecanismos de seguridad propuestos no fueron lo suficientemente fuertes, para no entorpecer su difusión internacional.

[6] http://www.montevideolibre.org/manuales:libros:wndw:capitulo_6:amenazas

Que són?

Wi-Fi Tretas son las amenazas que afectan a una red inalámbrica, como: acceso fácil y anónimo, autenticación a nivel dispositivo más que a nivel usuario, lo cual hace aún más difícil el control y auditoría de la entrada a la infraestructura y a la información.

Otra es que una persona puede fácilmente conectar un dispositivo GPS a su laptop, manejar por la ciudad y guardar un registro de las redes inalámbricas, el nombre y el tipo de seguridad de cada una junto con las coordenadas que indica el GPS al momento de la detección, si la persona encuentra un nombre llamativo pude regresar a la dirección indicada en el mapa y tratar de comprometer la seguridad de la red para su propio beneficio, a lo cual se le conoce como WarDrinving.

ARMAS DE PROTECCIÓN

El documento 802.11 define servicios de autenticación, que se dividen en dos: Open System y Shared Key; para apoyar estos mecanismos se definió un método de encripción de datos, el Wired Equivalent Privacy (WEP) que soporta 64 y 128 bits como llave para el cifrado, aunque algunos fabricantes ofrecen 256 bits.

No obstante, cuando se mencionó por primera vez de forma oficial las vulnerabilidades relacionadas al WEP, sin importar el tamaño de la llave de cifrado, se hizo evidente la necesidad de un mecanismo más seguro de autenticación sin esperar a que el estándar 802.11i estuviese listo. Así se desarrolló el WPA (Wi-Fi Protected Access), que evolucionó después al WPA2, sin embargo no todos los fabricantes lo soportan.

Más tarde se definió el nuevo estándar 802.11i, en el cual se estructuraron nuevos

métodos de protección para la autenticación, los más significativos y sencillos de entender son el Temporal Key Integrity Protocol (TKIP) y el Counter-Mode/CBC-MAC Protocol (CCMP).

Además de estos estándares existen una serie de mejores prácticas que pueden aplicarse para robustecer la seguridad de una red inalámbrica, entre éstas: evaluar bien las soluciones ofrecidas por algunos fabricantes, usar soluciones VPN/SLAN e IPSec, implementar sistemas de autenticación 802.1x / RADIUS y diseñar de forma adecuada la arquitectura y topología de las redes considerando el alcance de la señal, a fin de llevar un control de qué personas podrían tener acceso a ésta.

Aunque también conviene utilizar access points con firewall integrado, implementar sistemas de detección de intrusos vía inalámbrica (AirDefense—www.airdefense.net), desarrollar políticas de seguridad en cuanto al uso de la red y educar al personal de la empresa en el cumplimiento de estas normas.

1.9.6 Spoofing

Spoofing, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque - al menos la idea - es muy sencilla: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Y como los anillos de confianza basados en estas

características tan fácilmente falsificables son aún demasiado abundantes (no tenemos más que pensar en los comandos r-, los accesos NFS, o la protección de servicios de red mediante TCP Wrapper), el spoofing sigue siendo en la actualidad un ataque no trivial, pero factible contra cualquier tipo de organización.

Como hemos visto, en el spoofing entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo, y por otro evitar que el equipo suplantado interfiera en el ataque ([HB96]). Probablemente esto último no le sea muy difícil de conseguir: a pesar de que existen múltiples formas de dejar fuera de juego al sistema suplantado - al menos a los ojos del atacado - que no son triviales (modificar rutas de red, ubicar un filtrado de paquetes entre ambos sistemas...), lo más fácil en la mayoría de ocasiones es simplemente lanzar una negación de servicio contra el sistema en cuestión. Aunque en el punto siguiente hablaremos con más detalle de estos ataques, no suele ser difícil `tumbar', o al menos bloquear parcialmente, un sistema medio; si a pesar de todo el atacante no lo consigue, simplemente puede esperar a que desconecten de la red a la máquina a la que desea suplantar (por ejemplo, por cuestiones de puro mantenimiento).

El otro punto importante del ataque, la comunicación falseada entre dos equipos, no es tan inmediato como el anterior y es donde reside la principal dificultad del spoofing. En un escenario típico del ataque, un pirata envía una trama SYN a su objetivo indicando como dirección origen la de esa tercera máquina que está fuera de servicio y que mantiene algún tipo de relación de confianza con la atacada. El host objetivo responde

con un SYN+ACK a la tercera máquina, que simplemente lo ignorará por estar fuera de servicio (si no lo hiciera, la conexión se resetearía y el ataque no sería posible), y el atacante enviará ahora una trama ACK a su objetivo, también con la dirección origen de la tercera máquina. Para que la conexión llegue a establecerse, esta última trama deberá enviarse con el número de secuencia adecuado; el pirata ha de predecir correctamente este número: si no lo hace, la trama será descartada), y si lo consigue la conexión se establecerá y podrá comenzar a enviar datos a su objetivo, generalmente para tratar de insertar una puerta trasera que permita una conexión normal entre las dos máquinas.

Podemos comprobar que el spoofing no es inmediato; de entrada, el atacante ha de hacerse una idea de cómo son generados e incrementados los números de secuencia TCP, y una vez que lo sepa ha de conseguir `engañar' a su objetivo utilizando estos números para establecer la comunicación; cuanto más robusta sea esta generación por parte del objetivo, más difícil lo tendrá el pirata para realizar el ataque con éxito. Además, es necesario recordar que el spoofing es un ataque ciego: el atacante no ve en ningún momento las respuestas que emite su objetivo, ya que estas van dirigidas a la máquina que previamente ha sido deshabilitada, por lo que debe presuponer qué está sucediendo en cada momento y responder de forma adecuada en base a esas suposiciones. Sería imposible tratar con el detenimiento que merecen todos los detalles relativos al spoofing por lo que para obtener información adicional es necesario dirigirse a excelentes artículos que estudian todos los pormenores del ataque, como [Dae96] o [HB96]; de la misma forma, para conocer con detalle el funcionamiento del protocolo TCP/IP y sus problemas podemos consultar [Ste94], [Tan96], [Bel89] y [Mor85].

Para evitar ataques de spoofing exitosos contra nuestros sistemas podemos tomar diferentes medidas preventivas; en primer lugar, parece evidente que una gran ayuda es reforzar la secuencia de predicción de números de secuencia TCP: un esquema de generación robusto puede ser el basado en [Bel96], que la mayoría de Unices son capaces de implantar (aunque muchos de ellos no lo hagan por defecto). Otra medida sencilla es eliminar las relaciones de confianza basadas en la dirección IP o el nombre de las máquinas, sustituyéndolas por relaciones basadas en claves criptográficas; el cifrado y el filtrado de las conexiones que pueden aceptar nuestras máquinas también son unas medidas de seguridad importantes de cara a evitar el spoofing.

Hasta ahora hemos hablado del ataque genérico contra un host denominado spoofing o, para ser más exactos, IP Spoofing; existen otros ataques de falseamiento relacionados en mayor o menor medida con este, entre los que destacan el DNS Spoofing, el ARP Spoofing y el Web Spoofing ([Ris01]).

Existen diferentes tipos de spoofing dependiendo de la tecnología a la que nos refiramos, los cuales se describirán más adelante, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

TIPOS DE SPOOFING

- IP SPOOFING: Suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las respuestas del host que reciba los paquetes irán dirigidas a la IP falsificada. Por ejemplo si enviamos un ping (paquete icmp "echo request") spoofeado, la respuesta será recibida por el host al que pertenece la IP legalmente. Este tipo de spooofing unido al uso de peticiones broadcast a diferentes redes es usado en un tipo de ataque de flood conocido como smurf ataque. Para poder realizar IP SPOOFING en sesiones TCP, se debe tener en cuenta el comportamiento de dicho protocolo con el envío de paquetes SYN y ACK con su ISN específico y teniendo en cuenta que el propietario real de la IP podría (si no se le impide de alguna manera) cortar la conexión en cualquier momento al recibir paquetes sin haberlos solicitado. También hay que tener en cuenta que los routers actuales no admiten el envío de paquetes con IP origen no perteneciente a una de las redes que administra (los paquetes spoofeados no sobrepasarán el router).

- ARP SPOOFING: Suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. Explicándolo de una manera más sencilla: El protocolo Ethernet

trabaja mediante direcciones MAC, no mediante direcciones IP. ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC para que la comunicación pueda establecerse; para ello cuando un host quiere comunicarse con una IP emite una trama ARP-Request a la dirección de Broadcast pidiendo la MAC del host poseedor la IP con la que desea comunicarse. El ordenador con la IP solicitada responde con un ARP-Reply indicando su MAC. Los Switches y los hosts guardan una tabla local con la relación IP-MAC llamada "tabla ARP". Dicha tabla ARP puede ser falseada por un ordenador atacante que emita tramas ARP-REPLY indicando su MAC como destino válido para una IP específica, como por ejemplo la un router, de esta manera la información dirigida al router pasaría por el ordenador atacante quien podrá sniffar dicha información y redirigirla si así lo desea. El protocolo ARP trabaja a nivel de enlace de datos de OSI, por lo que esta técnica sólo puede ser utilizada en redes LAN o en cualquier caso en la parte de la red que queda antes del primer Router. Una manera de protegerse de esta técnica es mediante tablas ARP estáticas (simpre que las ips de red sean fijas), lo cual puede ser difícil en redes grandes. Para convertir una tabla ARP estática se tendría que ejecutar el comando:

FORMULA # arp -s [IP] [MAC]

EJEMPLO # arp -s 192.168.85.212 00-aa-00-62-c6-09

Otras formas de protegerse incluyen el usar programas de detección de cambios de las tablas ARP (como Arpwatch) y el usar la seguridad de puerto de los switches para evitar cambios en las direcciones MAC.

- DNS SPOOFING: Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa. Esto se consigue falseando las entradas de la relación Nombre de dominio-IP de un servidor DNS, mediante alguna vulnerabilidad del servidor en concreto o por su confianza hacia servidores poco fiables. Las entradas falseadas de un servidor DNS son susceptibles de infectar (envenenar) el caché DNS de otro servidor diferente (DNS Poisoning).

- WEB SPOOFING: Suplantación de una página web real (no confundir con phising). Enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima (páginas WEB visitas, información de formularios, contraseñas etc.). La página WEB falsa actúa a modo de proxy solicitando la información requerida por la víctima a cada servidor original y saltándose incluso la protección SSL. El atacante puede modificar cualquier información desde y hacia cualquier servidor que la víctima visite. La víctima puede abrir la página web falsa mediante cualquier tipo de engaño, incluso abriendo un simple LINK. El WEB SPOOFING es difícilmente detectable, quizá la mejor medida es algún plugin del navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas WEB significará que probablemente estemos sufriendo este tipo de ataque.

- MAIL SPOOFING: Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de

e-mails hoax como suplemento perfecto para el uso de phising y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin. Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa ip pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Otra técnica de protección es el uso de firmas digitales.[7]

1.9.7 Suplantación

Uno de los delitos que está obteniendo importantes índices de crecimiento en la red, es el de la suplantación de sitios de Internet (PHISHING) y el posterior robo de identidades, con el ánimo de obtener datos sensibles, tales como números de tarjetas de crédito y claves de acceso.

Estas estafas, usualmente, se inician mediante un correo electrónico indicando que nuestra cuenta o usuario está por ser deshabilitado y se deben reingresar los datos, o en caso contrario se dará de baja o alguna excusa similar. Se nos facilita un enlace obviamente falso en el mensaje, remitiéndonos así, a un sitio malicioso creado para hurtar nuestra información personal, al intentar autenticarnos.

Induciendo a un visitante a dichos sitios, en lugar de los verdaderos, se pueden obtener números de tarjetas de crédito, claves de acceso, número de cuenta, números personales de identificación, etc., que luego serán usados en forma fraudulenta, suplantando a los verdaderos usuarios.

[7] http://es.wikipedia.org/wiki/Spoofing

Esta clase de delitos se ven beneficiados también, por fallas en los navegadores, que permiten visualizar cierta URL, cuando en realidad se esta visitando un sitio diferente.

1.9.8 Filtrado MAC

Un filtrado MAC hace que solo se conecten al router las direcciones MAC que se desea, una MAC es una dirección física de una tarjeta de red, con lo cual con el filtrado mas impides que ordenadores que no se desea que se conecten al router.

Usuarios con Win XP debéis dirigiros a inicio/ejecutar/cmd y ejecutar el comando **IPCONFIG**

Fig 21 Pantalla de IP Config

La dirección IP se corresponde con vuestra IP privada (marcado en amarillo) y la puerta de enlace para acceder al router marcada en verde.

Para usuarios con Win 98 dirigiros a inicio/ejecutar/winipcfg señalad vuestro adaptador (NO PPP adapter) y allí veréis vuestra IP privada y puerta de enlace.

En este ejemplo tomaremos como datos:

Dirección IP: 192.168.0.2

Puerta de enlace: 192.168.0.1

Una vez que conocemos estos datos estamos en disposición de entrar por web a la configuración de nuestro Router.
Marcamos la opción Wireless y después pinchamos en Wireless MAC Filter

una vez que tengamos seleccionada esa opción veremos lo siguiente:

Fig. 22 Pantalla de Linksys para filtrado MAC

En esta pantalla activaremos el filtro Mac y para eso marcamos en Wireless MAC Filter **enable** y luego marcamos **Permit only** para así añadir nosotros el listado de direcciones MAC que queremos que conecten a nuestra red Wi Fi.

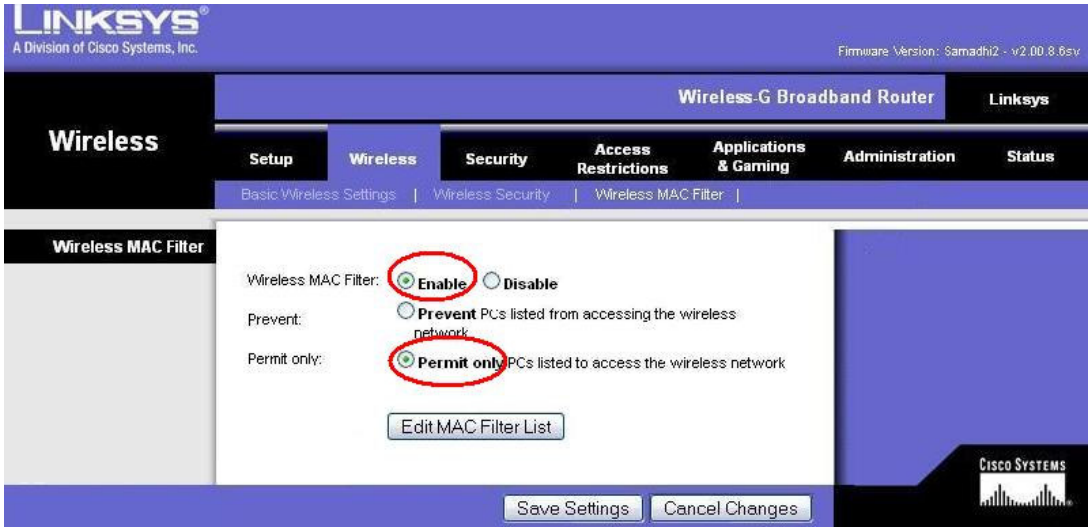


Fig. 23 Habilitar filtro MAC

El siguiente paso será pulsar sobre el botón **Edit MAC Filter List** y nos saldrá lo siguiente en otra ventana:

Fig.24 Listado direcciones MAC

En este paso introduciremos la dirección **MAC** de nuestro ordenador y de los ordenadores que queramos que tenga acceso a nuestra red inalámbrica . Para saber nuestra dirección MAC iremos a Inicio/ejecutar y pulsaremos **cmd** y se nos abrirá una ventana de símbolo de sistema, en ella escribiremos **IPCONFIG/ALL** y apuntaremos donde pone "dirección física"

Importante: Si la dirección por ejemplo es **00-0E-A6-70-00-9D** tenemos que añadirla sin guiones. Quedería en este ejemplo **000EA670009D**

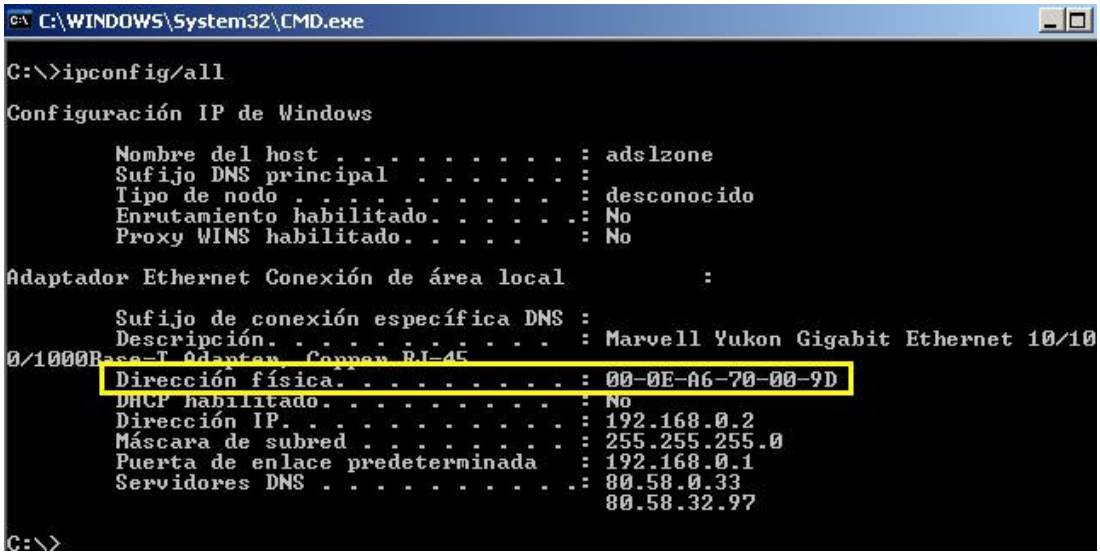


Fig.25 Pantalla IP config all

Ahora para guardar los vcambios pulsamos sobre "save settings" y se nos reiniciara la red y después para guardar y resetear volvemos a pulsar en save settings. Si todo ha ido bien ya estarán filtradas las direcciones MAC que hayamos puesto.

1.9.9 Activación WEP

Si bien este protocolo ha sido vulnerado, muchos dispositivos y placas sólo admiten este tipo de encriptación como el mayor grado de seguridad otorgado, por lo que su activación se vuelve obligatoria. Para redes hogareñas puede ser suficiente, ya que vulnerar WEP no está al alcance de cualquier persona active la WEP: Los protocolos 802.11b y 802.11a incluyen un elemento de seguridad optativo llamado Privacidad Inalámbrica Equivalente (Wireless Equivalent Privacy o WEP) que autentica a todos los que quieran entrar a la red inalámbrica y que cifra todo el tráfico. La WEP tiene debilidades que pudieran exasperar a cualquier experto en criptografía (el profesor de ciencias de computación de la Universidad de Maryland, William A. Arbaugh, ha

reunido evidencia irrefutable en find.pcworld.com/ 30332). Pese a esto, tener un poco de seguridad es mejor que nada. Su manual de hardware de Wi-Fi le indicará cómo activar la WEP.

Use la WEP de 128 bits: Los equipos de Wi-Fi son capaces de funcionar con un cifrado WEP de 40 o de 128 bits. El cifrado WEP más débil de 40 bits, combinado con los otros defectos documentados de la WEP, hacen que un sistema sea fácil de penetrar. Pero debemos mencionar que para usar la WEP de 128 bits, primero hay que asegurarse de que todos los dispositivos inalámbricos en la red sean compatibles con esa tecnología. La activación de la WEP de 128 bits en toda su red podría justificar el costo de reemplazar aquellas tarjetas que son incompatibles con esta seguridad más estricta.

Escoja buenas frases de contraseña, o use números hexadecimales: Parte del proceso de activar la WEP es escoger una frase de contraseña. Desafortunadamente, la WEP es aun más ineficaz si se utiliza una frase fácil de adivinar. Mezcle las letras mayúsculas y minúsculas con caracteres que no sean alfanuméricos, no use palabras reales (aunque se trate de otro idioma) y evite aquellos trucos demasiado transparentes como los de desplazar sus dedos una tecla hacia arriba, hacia abajo o lateralmente antes de escribir una contraseña obvia (como la propia palabra ‘contraseña’), o las sustituciones de caracteres predecibles (como pa55w0rd en lugar de paSSwOrd). Los manejadores bélicos experimentados tienen diccionarios y otras herramientas que prueban todos estos trucos y permutaciones en poco tiempo.

Por suerte, la frase de contraseña es una conveniencia que usted puede pasar por alto si lo desea. Simplemente cree su clave WEP hexadecimal (una serie de números decimales de dos dígitos) y escríbala en las pantallas de configuración de su enrutador y tarjeta

inalámbrica (vea la Figura 1). Los números hexadecimales (de base 16) comienzan con el cero y usan las letras de la A a la F para reemplazar con un solo dígito los números decimales (de base 10) del 10 al 15. Así se pueden producir cantidades de dos dígitos como 0B (decimal 11) y FF (decimal 255). Evite las claves memorizables con homónimos hexadecimales como A1, 3D, 4F, 2B, B4 porque los piratas ya pensaron en eso y están buscando esas combinaciones.

Cifrado WEP (Wired Equivalent Privacy)

El modelo 5430 es compatible con la seguridad WEP de 64 y 128 bits. Si su router lo permite, le recomendamos que active el sistema de seguridad de mayor nivel (número de bits más alto). Cuando se activa el método WEP, se utiliza una clave para cifrar los datos, lo que significa que adquieren un formato específico que sólo puede interpretar otro dispositivo inalámbrico que conozca esa clave. Dado que en los dos extremos se utiliza la misma clave, los usuarios que no la conozcan no podrán conectarse a la red ni utilizar su conexión a Internet.

Filtrado de direcciones MAC

Muchos routers inalámbricos disponen de un mecanismo para crear una lista de dispositivos que pueden formar parte de su red inalámbrica. Consulte la documentación relacionada con el punto de acceso o el router inalámbrico para averiguar si es posible el filtrado de direcciones MAC.

Cómo activar la seguridad en el dispositivo 5430

Activación de WEP

Después de obtener el nombre de red (SSID configurado en el router o punto de acceso inalámbricos y sus parámetros de seguridad), puede utilizar el menú Security

(Seguridad) que se encuentra en las páginas de interfaz Web del usuario para programar la seguridad WEP del dispositivo 5430.

Si selecciona WEP, tiene la opción de aplicar Shared Key Authentication (Autenticación de clave compartida) (forzada) o permitir que el modelo 5430 sólo la envíe cuando la solicite un router inalámbrico (Open System, Sistema abierto).

Es importante que las claves de red coincidan con las de los routers inalámbricos. Si dispone de varias claves de red, puede especificar hasta cuatro.

Nota: Para las claves de red se distingue entre mayúsculas y minúsculas. Cuando introduzca una clave de red, escríbala tal como aparece en el router o punto de acceso inalámbricos.

Filtrado inalámbrico de direcciones MAC

Puede utilizar la función de filtrado de direcciones MAC para conectarse a un router o un punto de acceso inalámbricos determinados. Puede añadir la dirección MAC del router o punto de acceso inalámbricos y cambiar el criterio del campo “Wireless MAC address filtering” (Filtrado de direcciones MAC) a Allow (Activar). Al realizar esta operación, el dispositivo 5430 sólo se comunicará con su router o punto de acceso inalámbricos y no será posible el acceso al dispositivo a través de otros.

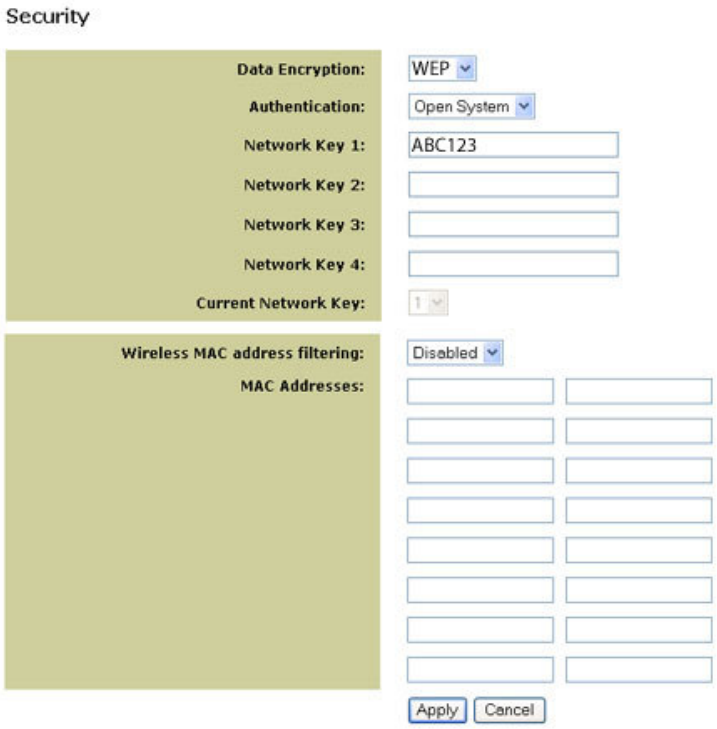


Fig. 26 Seguridad WEP

Opciones del menú Advanced (Opciones avanzadas)

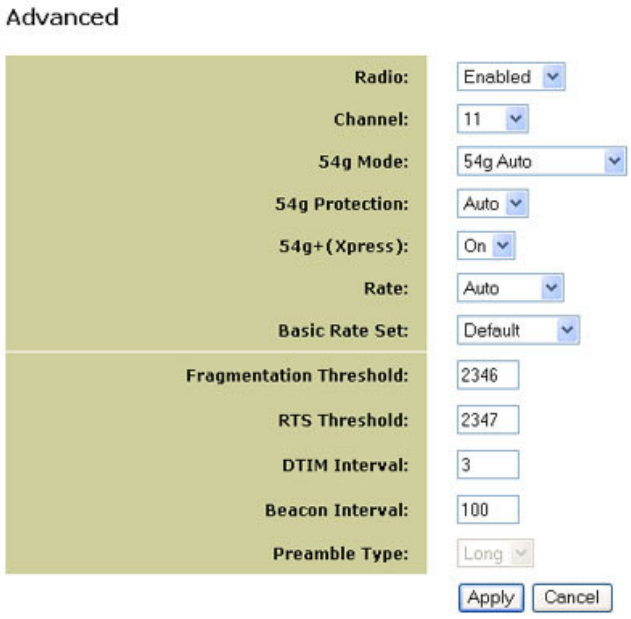


Fig. 27 Seguridades avanzadas WEP

1.9.10 VPN

La Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Los ejemplos más comunes es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo esto utilizando la infraestructura de Internet.

En pocas palabras una VPN es una red virtual que se crea "dentro" de otra red, como por ejemplo Internet. Generalmente las redes privadas se crean en redes públicas, en las que se quiere crear un entorno confidencial y privado. La VPN nos permitirá trabajar como si estuviésemos en la red local, es totalmente transparente para el usuario.

Una vez establecida la conexión de la red privada virtual los datos viajan encriptados de forma que sólo el emisor y el receptor son capaces de leerlos.

Para poder realizar una VPN se necesita un servidor (o host) que espera conexiones entrantes, y uno o varios clientes, que se conectan al servidor para formar la red privada.

¿Qué podemos hacer con una VPN?

Al permitirnos establecer conexiones seguras entre otros equipos podremos acceder a los recursos del otro equipo de forma segura y confidencial, por ejemplo a impresoras, documentos, servidores de base de datos, aplicaciones específicas, etc.

¿Cómo funciona una VPN?

Como ya se ha dicho anteriormente se trata de un proceso totalmente transparente para el usuario y para la mayoría de las aplicaciones. Funciona exactamente igual que cualquier otra conexión de red, es decir, dentro de la VPN cada equipo tendrá una IP, todas las conexiones usando esa IP estarán funcionando dentro de la VPN y serán encriptadas, el usuario simplemente tendrá que usar las IPs de la VPN, y no preocuparse de nada más, el resto ya lo hace el cliente VPN y el servidor VPN.

Cultura general sobre VPN's

Antes de comenzar a trabajar con VPN's es bueno poseer unas nociones básicas del mundo en el que nos estamos metiendo.

Son dos las tecnologías más utilizadas para crear VPN's, en realidad son diferentes protocolos o conjuntos de protocolos, PPTP y L2TP.

PPTP: Point to Point Tunneling Protocol

PPTP es un protocolo desarrollado por Microsoft y disponible en todas las plataformas Windows. Es sencillo y fácil de implementar pero ofrece menor seguridad que L2TP. En este artículo implementaremos una conexión VPN mediante PPTP usando MS-CHAP v2. También es posible usar PPTP con EAP-TLS para soportar certificados de

seguridad.

L2TP: Layer Two Tunneling Protocol

Se trata de un estándar abierto y disponible en la mayoría de plataformas Windows, Linux, Mac, etc. Se implementa sobre IPSec y proporciona altos niveles de seguridad. Se pueden usar certificados de seguridad de clave pública para cifrar los datos y garantizar la identidad de los usuarios de la VPN.

Comparativa entre PPTP y L2TP

- Con PPTP, el cifrado de datos comienza después de que la conexión se procese (y, por supuesto, después de la autentificación PPP). Con L2TP/IPSec, el cifrado de datos empieza antes de la conexión PPP negociando una asociación de seguridad IPSec.
- Las conexiones PPTP usan MPPE, un método de cifrado basado en el algoritmo de encriptación Rivest-Shamir-Aldeman (RSA) RC-4, y usa llaves de 40, 56 o 128 bits. Las conexiones L2TP/IPSec usan Data Encryption Standard (DES), con llaves de 56 bits para DES o tres llaves de 56 bits para 3-DES. Los datos se cifran en bloques (bloques de 64 bits para el caso de DES).
- Las conexiones PPTP requieren sólo autentificación a nivel de usuario a través de un protocolo de autentificación basado en PPP. Las conexiones L2TP/IPSec requieren el mismo nivel de autentificación a nivel de usuario y, además nivel de autentificación de máquina usando certificados digitales.

Existen más diferencias, pero hacer un estudio más pormenorizado se saldría de la idea inicial de este artículo por lo que lo dejaremos en estas tres diferencias fundamentales.

Caso práctico

La mejor forma de entender y ver como funciona es implementándolo, y eso es lo que haremos a continuación.

- Escenario: Dos (o más) equipos distantes y conectados a Internet quieren compartir sus recursos (ficheros, impresoras, etc.) entre ellos de forma privada y sencilla.
- Software: Windows XP o 2000, también es posible realizar la conexión con equipos con Windows 98 y 95 descargando los ficheros de actualización de la web de Microsoft.
- Solución: Montar una VPN a través de Internet entre estos equipos.

Necesitamos establecer un equipo como servidor, éste será el encargado de la autenticación, el resto de equipos establecerán la conexión con él.

Servidor VPN

- Vamos al Panel de control, y abrimos la carpeta de "Conexiones de red" y en el menú Archivo seleccionamos "Nueva conexión".

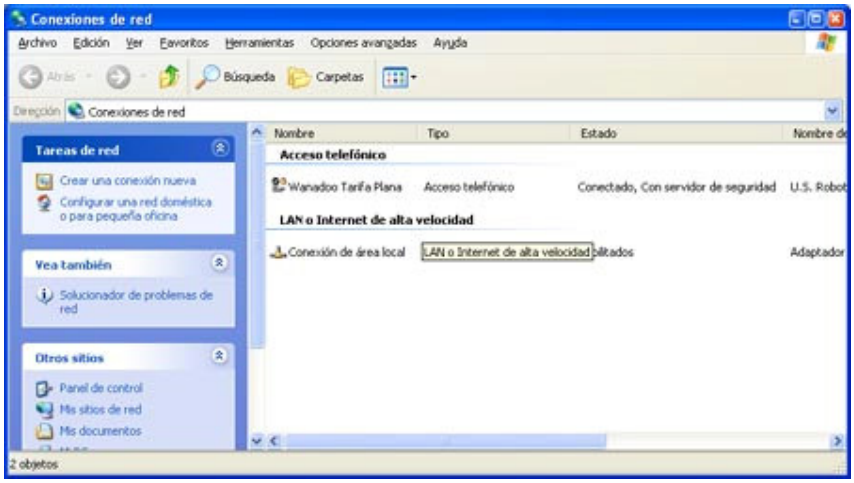


Fig. 28 Conexión VPN

- Ahora estamos en el "Asistente para conexión nueva". Pulsamos en el botón "Siguiente" para continuar.

Fig. 29 Pantalla inicial de la configuración VPN

- Entre las opciones disponibles seleccionamos "Configurar una conexión avanzada", y pulsamos en "Siguiente".

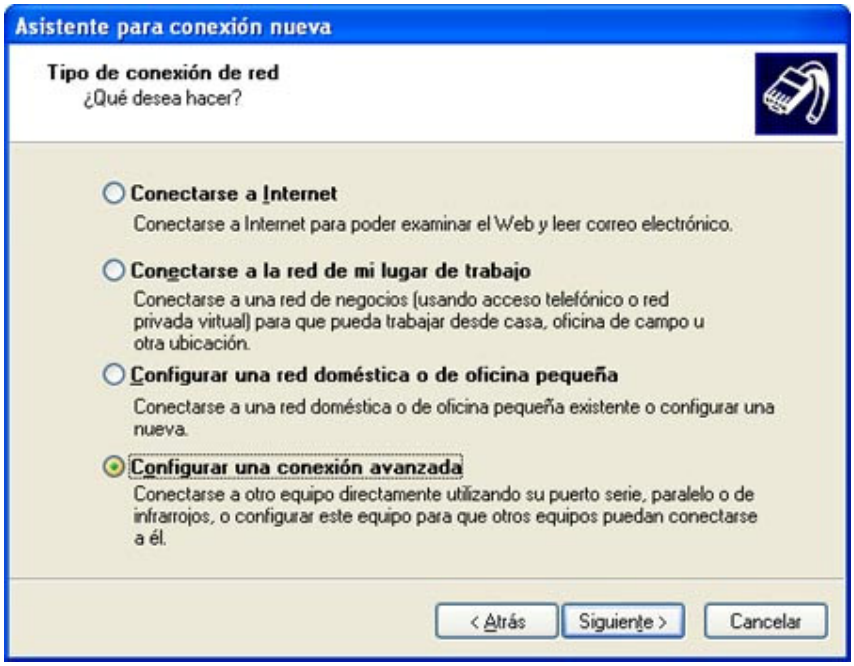


Fig. 30 Asistente para la conexión VPN

- Ahora seleccionamos "Aceptar conexiones entrantes" y pulsamos "Siguiente" para continuar.

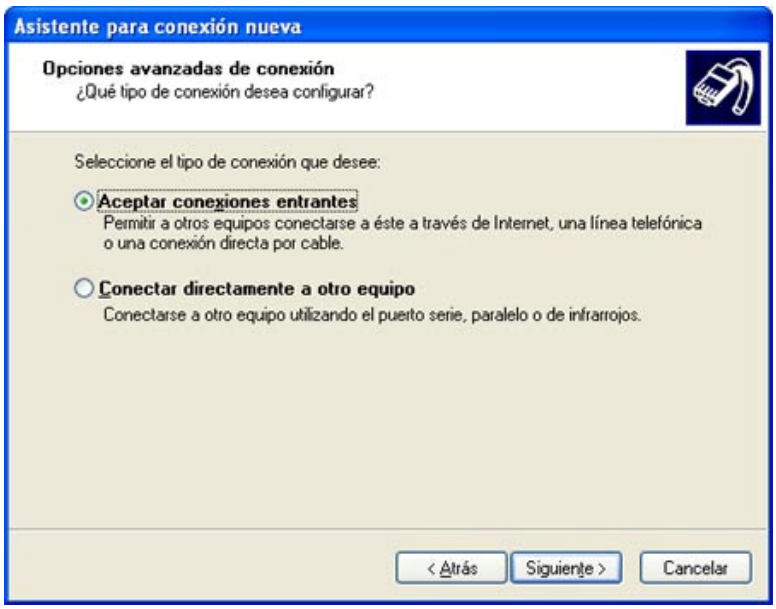


Fig. 31 Asistente para conexción VPN (1)

- En la pantalla "Dispositivos de conexiones entrantes" no seleccionamos ninguno, pues no queremos que se conecten a este equipo haciendo una llamada o usando el puerto paralelo. Pulsamos en "Siguiente".

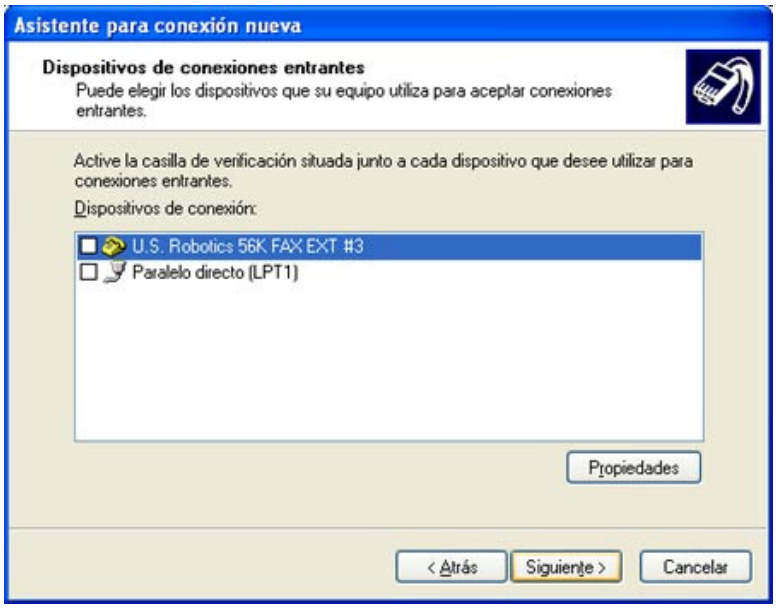


Fig. 32 Pantalla elegir dispositivos a utilizar en la VPN

- En la pantalla "Conexión de red privada virtual (VPN) entrante" debemos seleccionar "Permitir conexiones virtuales privadas". Pulsamos en "Siguiente".

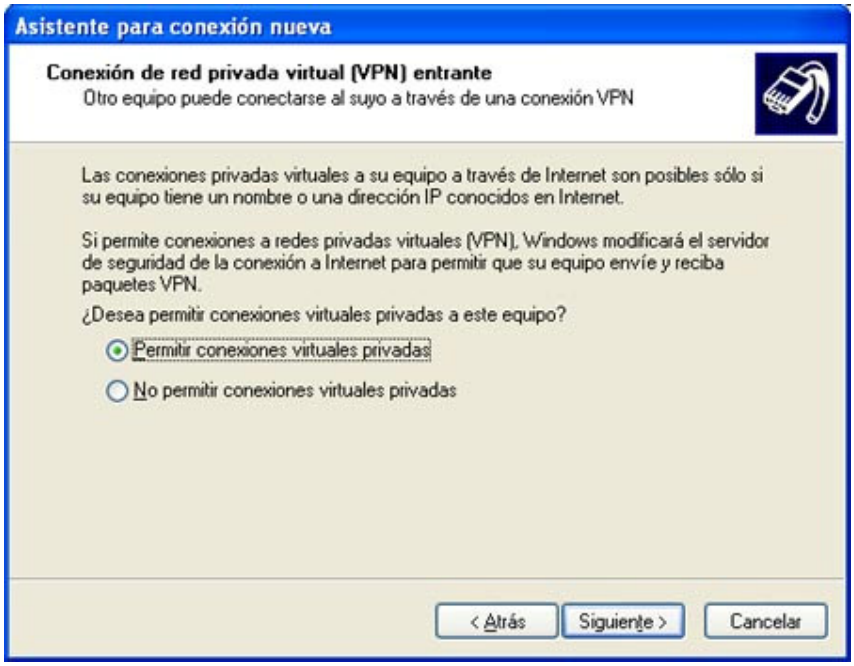


Fig. 33 Asistente para conexion a VPN

- En la pantalla "Permisos de usuarios" seleccionamos los usuarios que podrán conectarse a nuestro equipo usando la VPN. Desde esta misma pantalla podremos crear nuevos usuarios. Pulsamos en "Siguiente".

Fig. 34 Selección de los usuarios de la VPN

- Ahora debemos seleccionar los protocolos que habilitaremos en la VPN. Como queremos compartir ficheros e impresoras marcaremos "Protocolo Internet (TCP/IP)", "Compartir impresoras y archivos para redes Microsoft". Podremos agregar los protocolos que queramos usando el botón Instalar. Seleccionamos el protocolo "Protocolo Internet (TCP/IP)" y pulsamos en el botón Propiedades para proceder a configurarlo.

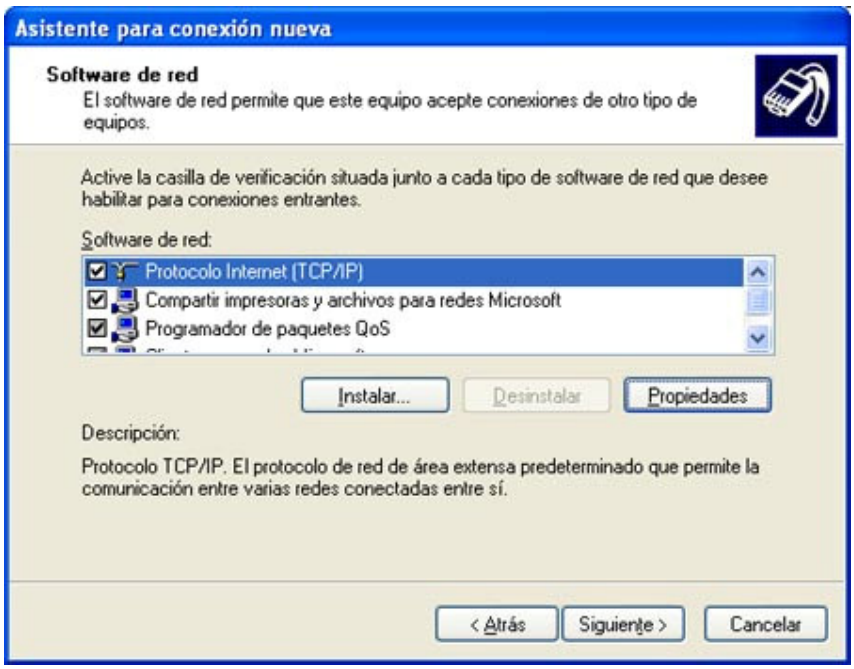


Fig. 35 Asistente para conexión

- Ahora podemos configurar las propiedades del protocolo TCP/IP. Si queremos que los clientes que se conectan a nosotros puedan acceder a la red local en la que tenemos nuestro servidor deberemos activar la primera casilla. Además podemos dejar que el servidor asigne las IPs de los clientes o establecer un intervalo de IPs, o incluso permitir que los clientes especifiquen su IP.

Fig. 36 Propiedades TCP de la VPN

- Guardamos la configuración de TCP/IP y pulsamos en el botón siguiente del asistente y ya habremos terminado. En este momento tendremos una nueva conexión en la carpeta de Conexiones de red. Seleccionando la nueva conexión podremos ver el estado de ésta, los clientes conectados, cambiar las opciones de configuración, etc.

Ahora ya tenemos configurado el servidor VPN y ya está listo para aceptar clientes VPN.

A continuación configuraremos una conexión VPN para que se conecte al servidor.

Cliente VPN

- Abrimos la carpeta de "Conexiones de red" y en el menú Archivo seleccionamos "Nueva conexión". En el asistente para conexión nueva seleccionamos "Conectarse a la red de mi lugar de trabajo", y pulsamos siguiente.

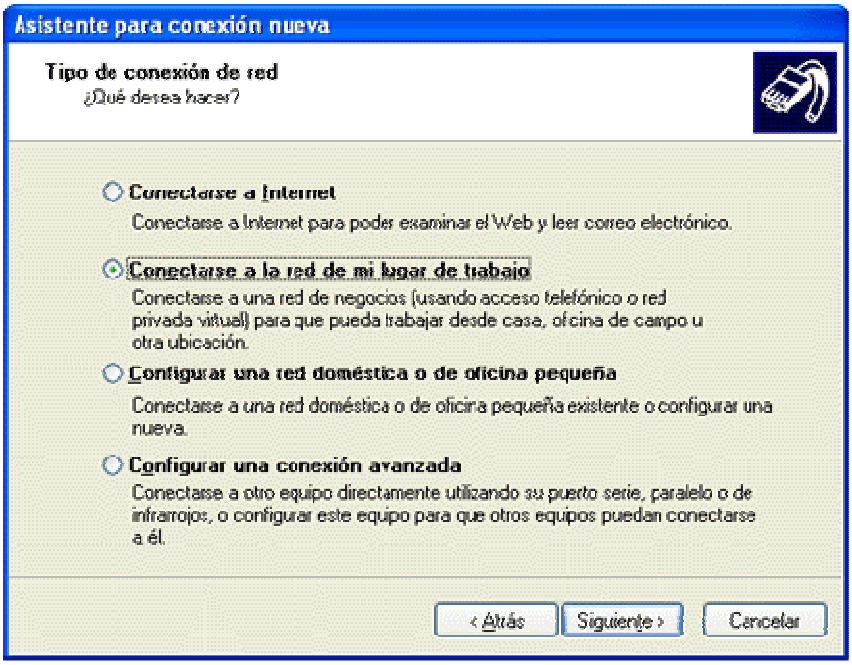


Fig. 37 Cliente VPN

- Seleccionamos "Conexión de red privada virtual", y pulsamos siguiente.

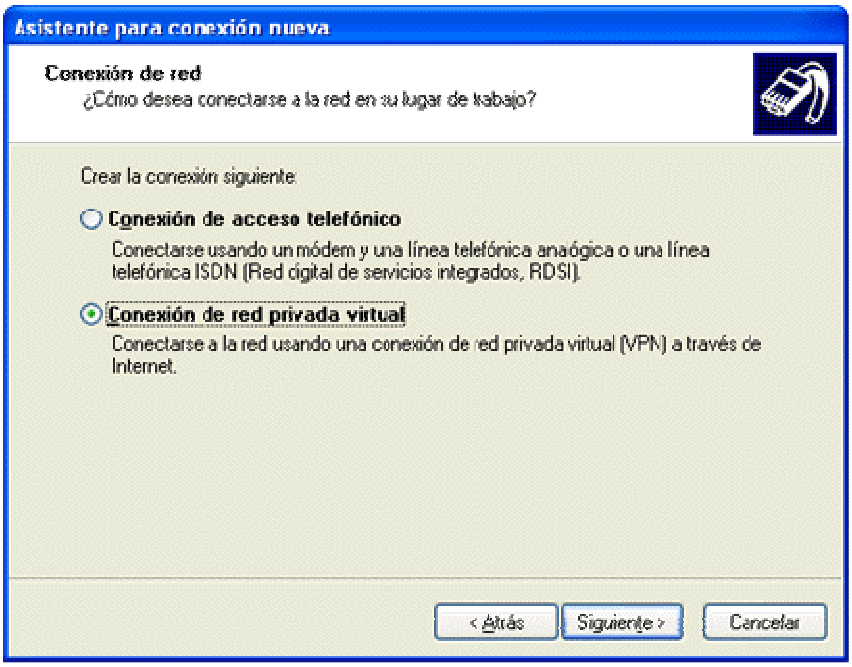


Fig. 38 Conexión VPN

En la siguiente ventana, marcaremos la opción "no usar conexion inicial" a menos que queramos que con la vpn se utilice otra de nuestras conexiones a internet, si indicamos que al activar esta conexión se active antes otra conexión, por ejemplo una conexión telefónica, se conectará primero a Internet y luego se establecerá la VPN. Si disponemos de cable o ADSL no es necesario activar ninguna de estas conexiones. Tampoco lo es si estamos conectados a Internet cuando activamos la conexión VPN o no queremos que ésta marque ninguna conexión. Por último indicamos la dirección IP del servidor VPN, esta es la dirección IP pública, es decir, la que tiene en Internet en el momento de establecer la conexión entre los clientes y el servidor.

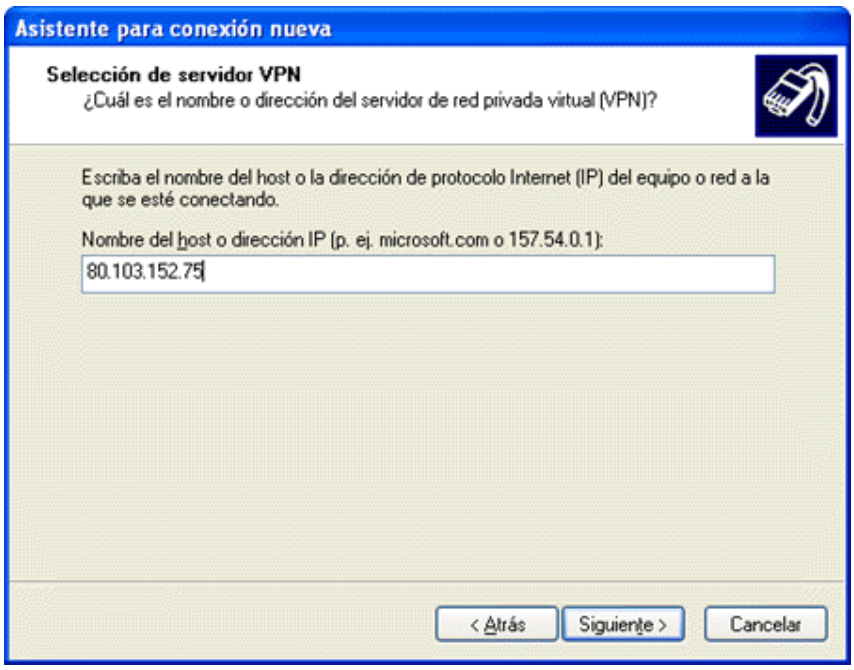


Fig. 39 Conexión al Servidor

- Al finalizar el asistente ya tendremos la conexión lista para activarse. Ahora debemos indicar el usuario y las password que hemos activado en el servidor y ya podremos conectarnos con el servidor.
  Si el servidor VPN se conecta a Internet usando un modem o Cable la IP puede cambiar (IPs dinámicas) por lo que será necesario indicarle la IP que tiene en cada momento.

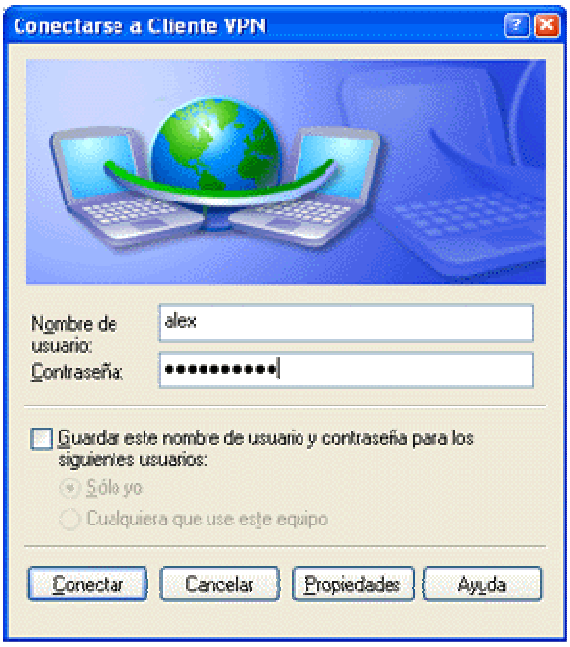


Fig. 40 Acceso al Servidor

Ya tenemos la conexión VPN lista para funcionar.
Si trabajamos con conexiones lentas (móden o similar) la VPN también irá lenta. Es recomendable disponer de conexiones de banda ancha para sacarle todo el rendimiento a este tipo de conexiones.

Para realizar las comunicaciones usando la VPN deberemos usar las IPs de la VPN. Es decir, además de la IP de Internet que tiene el servidor y los clientes se han generado otras IPs internas de la VPN, pues esas deberemos usar para comunicarnos con los equipos de la VPN, estas se obtendrán como las habituales, pero en el icono de la nueva conexión que aparece en la barra de notificación (junto al reloj).

En conexiones lentas, el Explorador de Windows no será capaz de mostrar los otros

equipos de la red, o le llevará mucho tiempo, en ese caso, podremos acceder a ellos escribiendo en la barra de direcciones del Explorardor de Windows "\\ip_en_la_VPN" o "\\nombre_maquina" de la máquina a la que queremos acceder, por ejemplo, si la IP (en la VPN) de la otra máquina es 169.254.3.117 pondremos \\169.254.3.117 en la barra de direcciones del Explorador de Windows y de esta forma ya tendremos acceso a los ficheros e impresoras de la máquina indicada.
Para usar otros recursos, como servidores de base de datos, etc. simplemente usamos la IP en la VPN de la máquina destino.

Además, si los equipos no tienen realizada la configuración de red adecuadamente, o tienen mal asignados los permisos puede ocurrir que no se pueda acceder a recursos. Esto no es un problema de la VPN sino de cómo se tienen establecidos los permisos en cada ordenador, al igual que pasa en una red local.

Por último, y como recomendación final, es aconsejable mantener el equipo actualizado e instalar los parches y services packs que va publicando Microsoft. Al tratarse de un servicio de red es muy vulnerable a ser atacado y si no está convenientemente actualizado podemos ser víctimas de ataques, o nuestros datos quizás no viajen lo suficientemente seguros como esperábamos.[8]

[8] http://www.elrincondelprogramador.com/default.asp?pag=articulos/leer.asp&id=55

CAPITULO II

DISEÑO DE LA WLAN PARA EL ENLACE ENTRE DOS O MAS EDIFICIOS PERTENECIENTES A LA MUNICIPALIDAD DE LA CIUDAD DE SAN FRANCISCO

San Francisco fue fundada el 9 de septiembre de 1886 por José Bernardo Iturraspe, en el marco de un plan de colonización que había puesto en marcha en esa época el gobierno de la provincia de Córdoba.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL PARA MEJORAR LA TOMA DE DECISIONES EN LA MUNICIPALIDAD.

La municipalidad como tal en la actualidad trabaja en diferentes sectores de la ciudad uno de ellos está ubicado a un kilómetro y medio de distancia de la matriz, es con este punto donde se necesita un enlace para centralizar la información de manera segura, en este punto se concentra el área de tránsito de la ciudad, es aquí donde llegan todas las multas e infracciones recolectadas por los agentes de tránsito, una vez recolectadas se las procesa ahí mismo pero a la vez deben ser cargadas en la base de datos principal de la municipalidad, la falta del enlace hace que a diario una persona se deba movilizar de un punto al otro llevando consigo la información en medio magnético para ser cargada en la municipalidad, esto conlleva a la pérdida de tiempo en la actualización de información en ocasiones por razones ajenas a la voluntad humana no llega a su destino y debe ser cargada con mayor retraso aún, esto también hace sentir malestar a los

usuarios que se acercan a la municipalidad a pagar su multa al día siguiente de haber cometido la infracción y se encuentran con que no hay ningún reporte y por no regresar al día siguiente no pagan las multas.

Si bien la información que se moviliza en el medio magnético no puede ser alterada en el trayecto, no es la mejor manera de manejar datos y más aún cuando deben ser actualizados en un tiempo prudente.

A continuación se describe un gráfico de las redes actuales

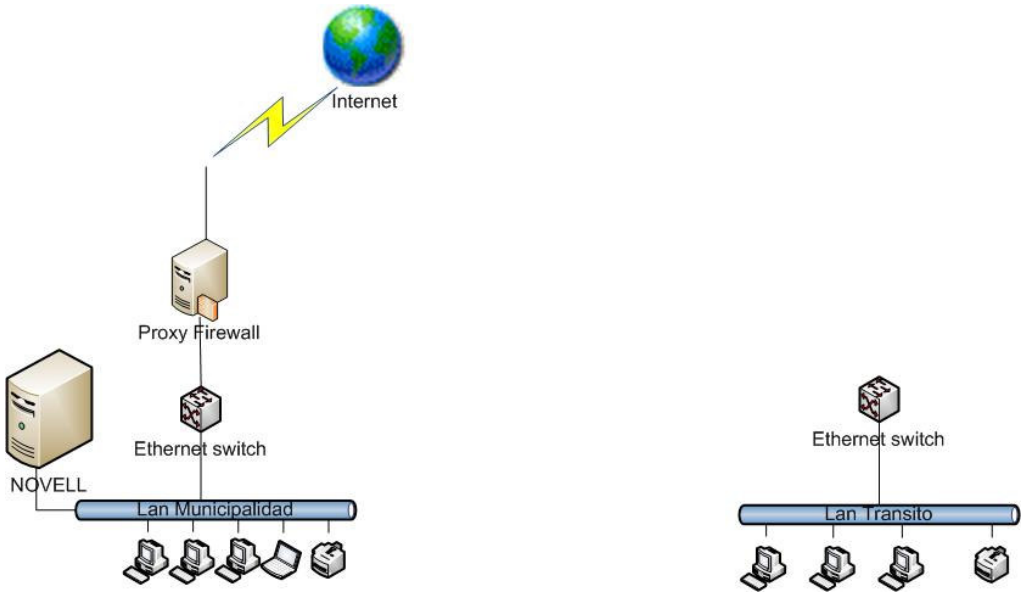


Fig 41 Gráfico estructura actual de las redes

Dirección de Informática Municipal

Nuestra Visión:

Ser un área de planeamiento y proveedora de sistemas de calidad y justo a tiempo, estando al servicio de los clientes internos y externos para satisfacer toda sus necesidades.

Nuestra Misión:

Confeccionar los mejores sistemas posibles, logrando no solo calidad, sino también integridad, en el tiempo justo y la satisfacción de nuestros clientes internos.

Atender a nuestros clientes internos con la mejor buena predisposición respetando sus opiniones y necesidades y concensuando cada cambio.

Pensar cada trabajo no sólo en los clientes internos, sino también en los clientes externos (contribuyentes), solicitando opiniones cuando sea necesario.

Cumplir con nuestros objetivos respetando siempre las leyes, ordenanzas, decretos, y normas que los gobernantes dispongan.

Contribuir en mejorar la economía de nuestro municipio realizando los gastos mínimos necesarios y suficientes, haciendo los ahorros que las necesidades nos permitan.

FODA

Nuestras fortalezas:

- La capacidad del personal.
- El grupo humano formado con una buena capacidad de trabajo en equipo, importante para llevar adelante cualquier proyecto.
- La buena relación que existe con las demás áreas para consensuar cambios sin que haya resistencia.
- Los sistemas existentes son propios, cuentan con más de 10 años de desarrollo y funcionamiento y solo habría que agregar nuevos o actualizarlos.
- Los datos en soporte magnético se encuentran todos en la municipalidad y la mayoría en el área informática lo que facilita cualquier cambio.

Nuestras Oportunidades:

- La disponibilidad económica para la modernización del equipamiento y el software.
- La decisión a niveles superiores de la necesidad de un cambio.
- Los lineamientos políticos que produjo una necesidad de mostrar cambios para mejorar.

Nuestras Debilidades:

- La escasa cantidad de RRHH para afrontar los cambios necesarios para la modernización total del municipio.
- Escaso equipamiento para poder afrontar dicho cambio.
- Equipamiento desactualizado que NO permitiría empezar el cambio.
- Lenguajes y Herramientas de desarrollo adquiridas en el año 1995, hoy totalmente obsoletas para los requerimientos de las nuevas tecnologías.
- Backups descentralizados que terminan en muchos casos por no ser seguros.
- Espacio físico insuficiente para el correcto desarrollo de las distintas funciones de la dirección informática.

Nuestras Amenazas:

- Terceras empresa que ofrecen sistemas modernos que serían difícil de aplicar.

Que Hacemos

- Diseño, desarrollo, implementación y mantenimiento de los Sistemas Informáticos Municipales:
  1. Catastro y Obras privadas
  2. Contribución por Mejoras.
  3. Tesorería
  4. Inmuebles
  5. Cementerio
  6. Comercio
  7. Automotores
  8. Guías de Hacienda.
  9. Fiscalización.
  10. AMOS: SS y Red Cloacas
  11. Contaduría.
  12. Tribunal de Faltas
  13. Tránsito.
  14. Desarrollo Comunitario
  15. Mesa de Entradas
  16. Sistema de seguimiento de Expedientes.
  17. Librería.
  18. Imprenta.
  19. Stock de depósito de Mercadería.
  20. Salud Pública

21. Bromatología
22. Procuración Fiscal y Gestión Judicial
23. Registro Civil.
24. Contrataciones.
25. Diseño del Sistema para la Farmacia Municipal
26. Sistema Gestión de Grandes deudores
27. Sistema Gestión deuda de AMOS
28. Sistemas de Caja Chicas
29. Sistemas de Gestión de llamadas a deudores de todas las contribuciones
30. Sistema de Registro de Bicicletas
31. Sistema de Patrimonio Municipal
32. Sistema del CEDEM
33. Sistemas de Liquidación de Sueldos.
34. Rediseño, desarrollo, implementación y mantenimiento de los Siguientes Sistemas Informáticos a partir del año 2000
    - Inmuebles
    - Comercio
    - Automotores
    - Iluminación.
35. Generación e Impresión de Cedulones de las siguientes áreas:
    - Inmuebles
    - Cementerio
    - Comercio
    - Automotores

- AMOS y Red Cloacas

36. Sistema Gestión de Grandes deudores
37. Sistema Gestión deuda de AMOS
38. Contribución por Mejoras.
39. Sistema de Laboratorio de Análisis.

- Amortización de todos los impuestos cobrados por la municipalidad. Carga complementaria de datos de los archivos maestros de cada área. Control de las impresoras en las emisiones generales de cedulones. Recepción, control, clasificación y carga de los partes diarios de la recaudación de los bancos (trabajo que hasta el año pasado realizaba "contaduría").
- Asistencia técnica y reparaciones primarias en los 120 equipos de la Municipalidad. Las tareas comprenden: Asistencia operativa personal, reparaciones de CPU, impresoras, modem, teclados y mouses sobre 51 equipos 486, 386 y 286; 22 equipos Pentium I; 7 equipos Pentium II; 40 equipos Pentium III. Totalizando unas 400 asistencias aproximadamente distribuida en todas las áreas Municipales.
- Mantenimiento y asistencia técnica en el Sistema de Sueldos
- Instalación y configuración de equipos, Sistemas Operativos y software varios, Actualización de Antivirus, recupero de información y limpieza de sistemas infectados por virus.
- Mantenimiento de la Red Informática Municipal: 91 equipos en la Red Principal, 8 equipos en el TAF, 5 equipos en el Registro Civil, 3 equipos en Tránsito.
- Implementación y mantenimiento de Nodo de Internet.
- Mantenimiento de la página Municipal y correos.

2.2 DISEÑO DEL SISTEMA DE RED.

2.2.1 Diseño Lógico

Hay diversos puntos débiles graves en la seguridad inherentes a las redes inalámbricas. En el mejor de los casos, estos puntos débiles se solucionan parcialmente mediante el uso de la privacidad equivalente por cable (WEP, Wired Equivalent Privacy), como se especifica en el estándar 802.11 del IEEE. La solución propuesta en esta guía se ocupa del problema de cómo mejorar la seguridad de las comunicaciones mediante redes inalámbricas. La solución ideal necesita contar con las características siguientes:

Autenticación sólida de cliente inalámbrico. Esto debe incluir la autenticación mutua del cliente, el punto de acceso (PA) inalámbrico y el servidor RADIUS.

Un proceso de autorización para determinar quién tendrá o no tendrá acceso a la red inalámbrica.

Control de acceso que solamente permita el acceso de red a clientes autorizados.

Cifrado eficaz del tráfico de la red inalámbrica.

Una administración segura de las claves de cifrado.

Una resistencia a los ataques de denegación de servicio.

El estándar del protocolo 802.1X para control de acceso a la red, en combinación con un método de autenticación segura como EAP-TLS, cumple con algunos de estos requisitos. La WEP de alta potencia brinda un cifrado seguro del tráfico de red pero ofrece un nivel de administración de claves deficiente. Los métodos para administrar claves de cifrado WEP inherentes a 802.1X y EAP son mucho más seguros que lo permitido por los estándares básicos de 802.11. El estándar de acceso protegido WiFi (WPA, WiFi Protected Access) es un grupo de normas basadas en el sector que incluye

802.1X y EAP (entre otras mejoras) y un protocolo estandarizado para la administración de claves conocido como Protocolo de integridad de claves temporales (TKIP, Temporal Key Integrity Protocol). El estándar WPA representa un paso considerable hacia la seguridad de WLAN y cuenta con el respaldo de la mayoría de los analistas y proveedores.

Nota: ninguna de las mejoras de WPA se ocupa de los problemas de denegación de servicio inherentes a 802.11 y 802.1X. Estas debilidades no representan un problema tan grave como los otros fallos de WEP, y la mayoría de los ataques de denegación de servicio demostrados causan únicamente una disrupción temporal en la red. Sin embargo, la amenaza de los ataques de denegación de servicio continúa siendo un tema preocupante para algunas empresas. La solución debería estar disponible tras la publicación del estándar IEEE 802.11i.

Aunque la compatibilidad con WPA ya está bastante extendida, todavía hay muchos dispositivos y sistemas incapaces de acomodar este estándar. Por esta razón, la solución en esta guía está diseñada para funcionar con WPA y WEP dinámica. La mayoría de los proveedores de hardware de red venden productos compatibles con 802.1X con claves WEP dinámicas y WPA. La finalidad de esto ofrecer la posibilidad de tratar los dos métodos indistintamente; el uso de uno u otro no influye significativamente en el diseño.

La figura siguiente muestra un diagrama conceptual de la solución (autenticación de 802.1X EAP-TLS).

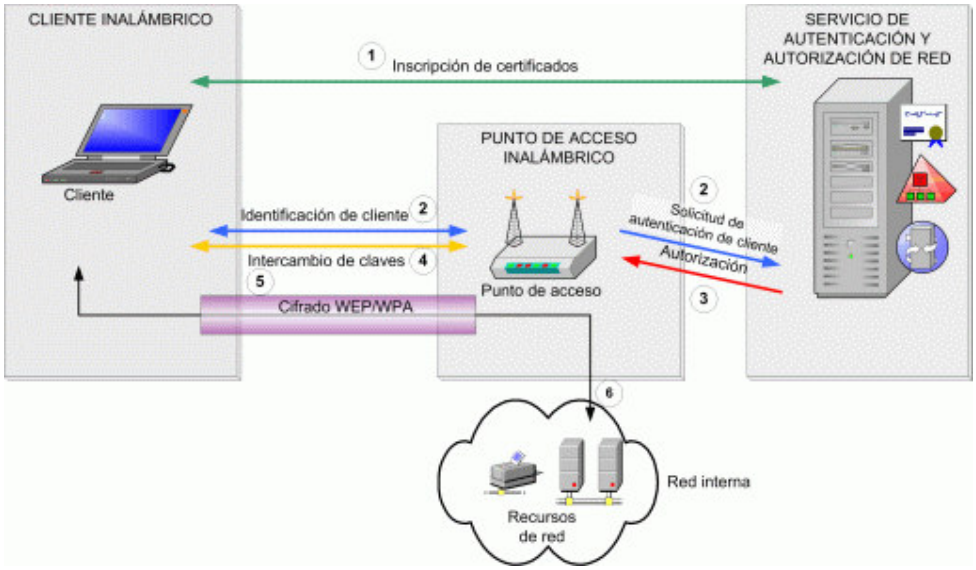


Figura 42 Concepto de la solución basado en la autenticación de 802.1X EAP-TLS

2.2.1.1 Selección de la Tecnología de Red.

Para este enlace he creído conveniente utilizar antenas parabólicas grilladas para enlace via microonda con equipos ruteadores Linksys, a pesar que su costo es mayor la fiabilidad que brindan es superior en muchos aspectos, integrando las mayores seguridades posibles como servidor Radius, y protocolos WEP y WPA.

2.2.1.3 Gestión de la red

El cliente inalámbrico. Se trata de un equipo o dispositivo que ejecuta una aplicación que requiere acceso a los recursos de red. El cliente tiene la capacidad de cifrar su tráfico de red, además de guardar e intercambiar credenciales de manera segura (como claves o contraseñas).

El AP inalámbrico. En términos de redes más generales se conoce como "servicio de acceso a la red" (NAS, Network Access Service) pero en los estándares inalámbricos se

hace referencia a este componente como "AP" o "punto de acceso". El punto de acceso inalámbrico implementa funciones de control de acceso para permitir o denegar el acceso a la red y ofrece la capacidad de cifrar el tráfico inalámbrico. También cuenta con los medios para intercambiar claves de cifrado de manera segura con el cliente a fin de asegurar el tráfico de red. Finalmente, puede consultar un servicio de autenticación y autorización para tomar decisiones de autorización.

Servicio de autenticación (AS, Authentication Service). Guarda y comprueba las credenciales de los usuarios válidos y toma decisiones de autorización basándose en una directiva de acceso. También puede recopilar información contable y de auditoría sobre el acceso de los clientes a la red. El servidor RADIUS es el componente principal de este servicio pero el directorio y la entidad emisora también contribuyen a esta función.

La red interna. Se trata de un área segura de servicios conectados a la red a los que la aplicación cliente inalámbrica debe obtener acceso.

Los números del diagrama ilustran el proceso de acceso a la red, que se describe con más detalle en los pasos siguientes:

1.- El cliente inalámbrico es decir el departamento de tránsito debe establecer credenciales con el servicio de autenticación antes de que se establezca el acceso a la red inalámbrica. (Esto podría realizarse con algunos medios fuera de banda como, por ejemplo, mediante un intercambio de disquetes, o bien podría realizarse en una red segura por cable o de otro tipo.)

Cuando se encuentra al alcance del punto de acceso inalámbrico, el equipo cliente intenta conectarse a la WLAN activa en el punto de acceso. Para su identificación, la WLAN cuenta con un identificador del conjunto de servicios (SSID, Service Set Identifier). El cliente detecta el SSID de la WLAN y lo usa para determinar la

configuración correcta y el tipo de credencial que debe utilizarse para esta WLAN específica.

El punto de acceso inalámbrico se configura para permitir únicamente conexiones seguras (autenticadas de 802.1X). Cuando el cliente intenta conectarse a él, el punto de acceso envía un desafío al cliente. A continuación, el punto de acceso configura un canal restringido que permite al cliente comunicarse sólo con el servidor RADIUS. Este canal bloquea el acceso al resto de la red. El servidor RADIUS solamente aceptará una conexión de un punto de acceso inalámbrico de confianza o de uno que haya sido configurado como cliente RADIUS en el servicio de autenticación de Internet (IAS, Internet Authentication Service) de Microsoft y que proporcione el secreto compartido para dicho cliente RADIUS.

El cliente intenta realizar la autenticación con el servidor RADIUS a través del canal restringido por medio de 802.1X. Como parte de la negociación EAP-TLS, el cliente establece una sesión de seguridad de la capa de transporte (TLS, Transport Layer Security) con el servidor RADIUS. El uso de una sesión de TLS tiene las finalidades siguientes:

- permite al cliente llevar a cabo la autenticación del servidor RADIUS, lo que significa que el cliente solamente establecerá la sesión con un servidor que cuente con un certificado de confianza.
- permite al cliente suministrar sus credenciales de certificado al servidor RADIUS.
- protege el intercambio de autenticación frente a intrusiones contra paquetes.

- la negociación de la sesión de TLS genera una clave que el cliente y el servidor RADIUS pueden utilizar para establecer claves maestras comunes. Estas claves se usan para derivar las claves utilizadas en el cifrado de tráfico de WLAN.

Durante este intercambio, solamente el cliente y el servidor RADIUS pueden ver el tráfico en el túnel de TLS y no queda nunca expuesto al punto de acceso inalámbrico.

3.- El servidor RADIUS valida las credenciales de cliente con el directorio. Si la autenticación del cliente se lleva a cabo de forma satisfactoria, el servidor RADIUS reunirá la información que le permitirá decidir si debe autorizarse el uso de la WLAN al cliente. Utiliza información del directorio (por ejemplo, sobre la pertenencia a grupos) y las restricciones definidas en su directiva de acceso (por ejemplo, los períodos de tiempo en que se permite el acceso a la WLAN) para conceder o denegar el acceso del cliente. Seguidamente, el servidor RADIUS transmite la decisión al punto de acceso.

4.- Si se concede acceso al cliente, RADIUS transmitirá la clave maestra del cliente al punto de acceso inalámbrico. Con ello, el cliente y el punto de acceso comparten información de clave común que pueden utilizar para cifrar y descifrar el tráfico de WLAN que se desplaza entre ellos.

Cuando se utiliza WEP dinámica para cifrar el tráfico, las claves maestras deben cambiarse periódicamente para evitar ataques de recuperación de claves WEP. El servidor RADIUS realiza este proceso de forma regular, lo que obliga al cliente a repetir la autenticación y generar un conjunto de claves nuevo.

Si se utiliza WPA para proteger la comunicación, la información de la clave maestra se usa para derivar las claves de cifrado de datos, que cambian para cada paquete transmitido. WPA no necesita exigir la repetición frecuente de la autenticación para garantizar la seguridad de las claves.

5.- A continuación, el punto de acceso establece la conexión de WLAN del cliente con la LAN interna, lo que ofrece al cliente un acceso sin restricciones a los sistemas de la red interna. Ahora, el tráfico transmitido entre el cliente y el punto de acceso está cifrado.

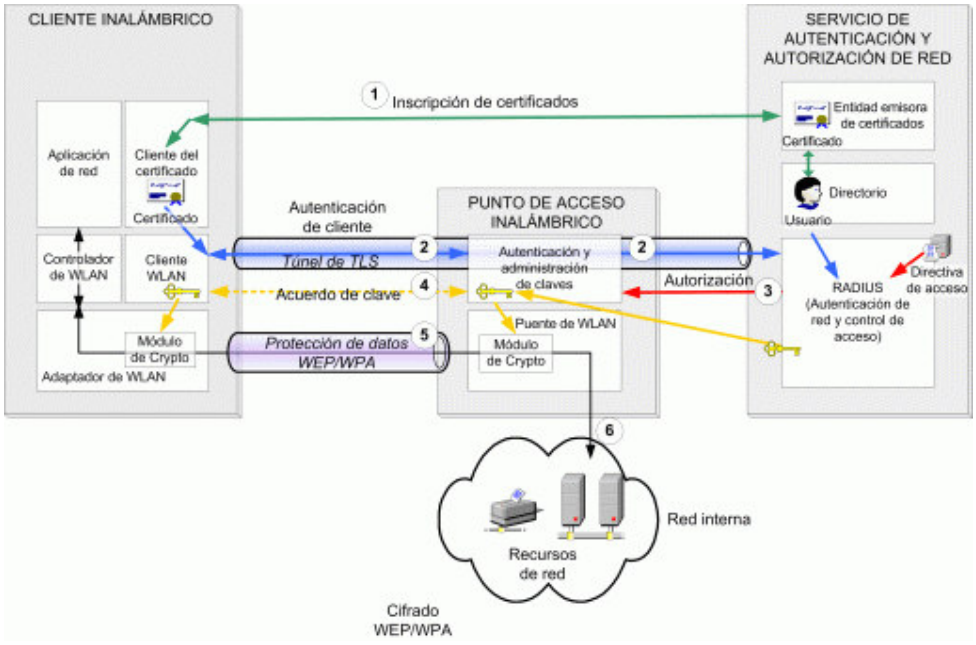


Fig. 43 Punte inalámbrico cifrado

2.2.2 Diseño Físico.

En el nivel físico, el diseño muestra cómo se implementarán estos componentes como servidores físicos, cómo se vincularán y cómo se distribuirán entre los diferentes sitios de la Municipalidad y las oficinas de Tránsito.

El diagrama ilustra los edificios los cuales hay que enlazar y la distancia entre ellos, en la parte de la municipalidad existen dos servidores, el de aplicaciones que es un Solaris y el Proxy Server para Internet y 120 equipos para usuarios por otro lado en el área de tránsito existe un Servidor y 2 equipos para usuarios.

Las antenas a utilizar serán una antena de grilla sólida en cada lado, la cuales tienen una frecuencia de 2.4 a 2.8 Ghz, estas antenas están diseñadas para baja resistencia al viento, su tamaño y versatilidad hace de esta antena muy aceptada.

(cablearemos mediante fibra óptica los tramos entre la antena ubicada en el exterior hasta un transeiver esto nos brinda mayor seguridad en caso de algún rayo pegue la antena, y desde el mismo hacia el router utilizaremos cable ethernet y hasta llegar a la placa de red en el servidor. Del otro lado de igual manera pero hasta llegar al router firewall.

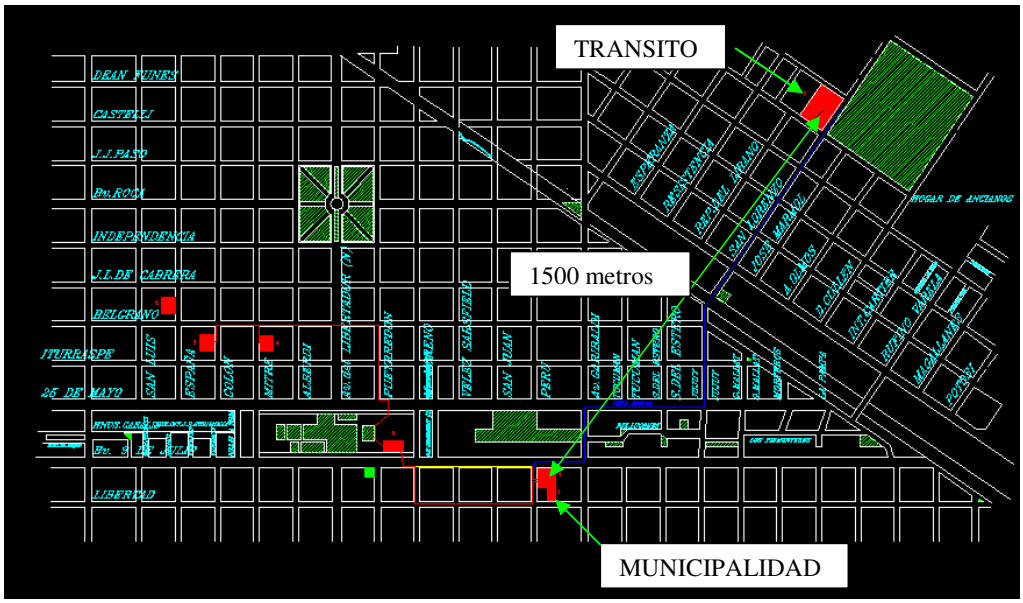


Fig. 44 Ubicación geográfica de los edificios de la Municipalidad

22.1 Diagramación del diseño físico.

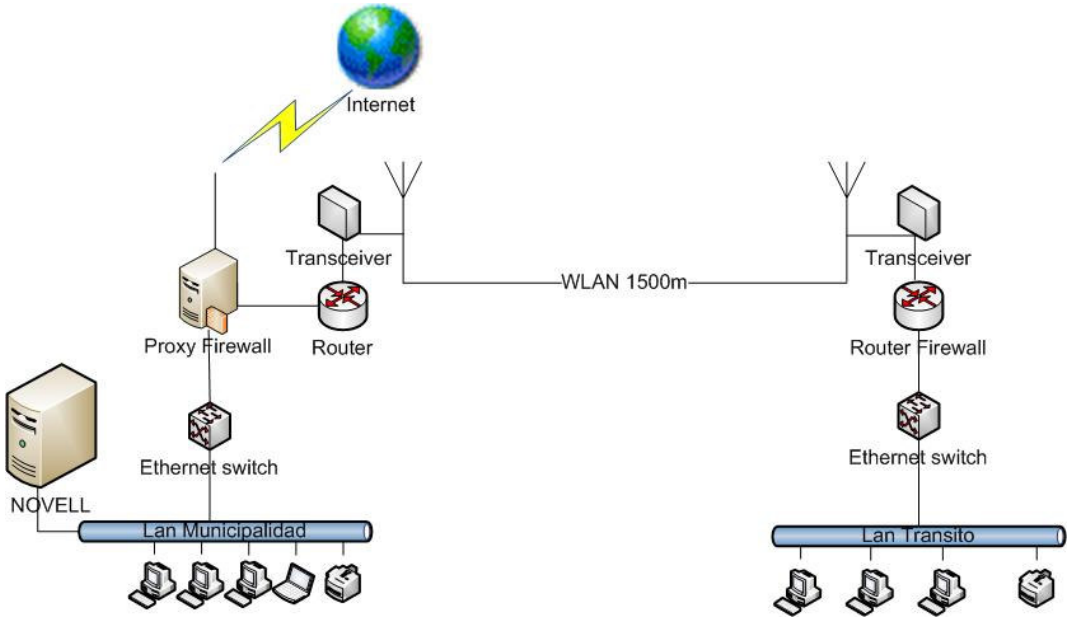


Fig. 45 Diseño Físico de la WLAN

2.2.2.2 Direccionamiento y Ruteo.

El ruteo de los paquetes lo realizará directamente el servidor Proxy el mismo que tiene instalado tres placas de red, la una para la entrada de Internet, otra para la conexión al switch de la Lan y la otra para el enlace WLAN, de el otro lado está el Access Point (AP) conectado al switch de la Lan de Tránsito los datos que provengan de los usuarios de tránsito saldrán por el AP ubicado en la misma oficina cruzarán por la WLAN hasta el otro AP ubicado en la Municipalidad ingresarán al Proxy luego en la Lan y finalmente llegarán hasta su destino en el servidor, este ruteo se lo hará asignando direcciones IP fijas para un direccionamiento directo.

En la Municipalidad se utilizará desde la IP 192.168.0.2 con máscara 255.255.255.0 y en Tránsito desde la IP 10.0.0.2 con mascara igual 255.255.255.0 de esta manera tendremos dos redes diferentes e independientes.

2.3 IDENTIFICACIÓN Y ESTIMACIÓN DE COSTO BENEFICIO.

2.3.1 Costos.

Para el diseño de este proyecto se ha tenido en consideración los siguientes equipos:

Antena parabólica grillada de 2.4 Ghz x 2 WIMO	466.00 USD
Torres para antena x 2	200.00 USD
Firewall Router Linksys AP Serie BEFVP41	185.00 USD
Router Linksys AP Serie BEFSR41	109.00 USD
Fibra óptica 8 metros	64.00 USD
Transceiver Mini-gbic 3Com x 2	788.00 USD
Cable UTP y conectores	50.00 USD
TOTAL	1862.00 USD

Este es el costo únicamente de los equipos y materiales, sin la instalación.

Mano de obra:

El recurso humano que se requiere en cuanto a construcción y levantamiento de las torres, instalación del cable de fibra óptica y pacheo de cables es algo que se debe contratar por separado, para las torres he considerado el costo de 100 usd por torre el costo de la hora es de 2.50 usd y aproximadamente tomaría una semana la instalación para los dos puntos.

Según estimaciones se prevee que el armado completo estaría en aproximadamente dos meses.

2.3.2 Beneficios.

Los beneficios de tener un enlace inalámbrico entre estos dos edificios se hace cada vez más necesario por un lado y lo más importante se tendría la información centralizada y actualizada en tiempo real, se optimizaría el tiempo y los recursos de la Municipalidad.

2.3.3 Comparación costo beneficio

Al contar con un enlace que permita mantener actualizados los datos en la municipalidad permitiría a los usuarios poder pagar sus faltas en forma oportuna es decir podrían acercarse al día siguiente de haber cometido la infracción y pagar la multa correspondiente evitando tener que regresar otro día o peor el caso por no pagar ese momento ya no regresar más. Las recaudaciones se incrementarían de un 20 a 25% mas o menos esto como una estimación.

El costo de la instalación estaría cubierto en su totalidad en muy poco tiempo y sería un alivio para todas las personas inmersas en el tema.

CAPITULO III

CONCLUSIONES Y RECOMENDACIONES

3.1 Verificación de Objetivos

OBJETIVOS ESPECÍFICOS.

- Determinar la situación actual de la forma de comunicación entre los edificios de la municipalidad.

Mediante el análisis previo realizado conocí el manejo de la información la comunicación aislada prácticamente inexistente se logrará corregir mediante el enlace.

- Emplear estándares inalámbricos de calidad necesarios para el correcto manejo y uso de esta tecnología.

Los estándares inalámbricos utilizados y los equipos nos garantizan un enlace permanente, estable y sin pérdidas en la conexión.

- Determinar un óptimo esquema de seguridad Wireless LAN para el funcionamiento confiable.

Las normas de seguridad utilizadas permiten un enlace lo suficientemente robusto, confiable e íntegro, para salvaguardar la información que fluye en el canal.

- Estructurar los diferentes parámetros de acuerdo a la necesidad de funcionamiento para el enlace de los edificios.

Tanto el software y hardware principalmente está diseñado para ser ampliado en un futuro, en el caso que se desee agregar un nuevo punto de acceso remoto la tecnología presta las facilidades para hacerlo.

3.2 Comprobación de la Hipótesis

HIPOTESIS

UNA WIRELESS LAN SEGURA PARA EL ENLACE ENTRE DOS O MAS EDIFICIOS DE LA MUNICIPALIDAD DE LA CIUDAD DE SAN FRANCISCO, nos garantizará que la producción de información generada sea mas eficiente, eficaz, confiable, consistente y nos permitirá actualizarla en tiempo real.

Por lo anteriormente mencionado puedo decir que la hipótesis se cumple, el enlace cumple con la eficacia y eficiencia, cumple con la actualización en tiempo real, cumple con la consistencia de los datos y desde luego con la seguridad de dicha información, contamos con cifrado de datos, seguridades en la red, codificación, es decir un conjunto de herramientas muy completo, con un servidor Proxy y un Firewall muy robustos que pueden mantener el canal libre de intrusos o escuchas.

3.3 Conclusiones

- En base al análisis y diseño planteado de una WLAN para en enlace de dos o mas edificios de la Municipalidad de San Francisco llegamos a la conclusión que tenemos el 100% de accesibilidad para desarrollar el proyecto.
- Implementar un programa de capacitación al personal del departamento de sistemas.
- La necesidad de la implementación está latente, para el beneficio de la comunidad.
- Las condiciones físicas y geográficas no presentan mayor inconveniente y el coste de implementación no es exagerado.
- En lo personal este proyecto ah sido muy enriquecedor para mi vida personal y profesional, adquirí muchos conocimientos útiles para mi futuro.

3.4 Recomendaciones

- Desarrollar un programa de capacitación para el personal de sistemas de la Municipalidad.
- Se recomienda mantenimiento de claves periódicamente en cada uno de los equipos.
- Recomendaría un estudio paralelo a esta investigación en lo relacionado al tema de seguridades.
- Se recomienda mantener el software de antivirus y anti spyware actualizados así como el sistema operativo.

BIBLIOGRAFIA

http://www.monografias.com/trabajos12/quimi/quimi.shtml#def (Sep-2007)

http://es.wikipedia.org/wiki/Dise%C3%B1o (Sep-2007)

http://wifi.lycos.es/info/lexicon (Oct-2007)

http://es.wikipedia.org/wiki/Est%C3%A1ndares_inal%C3%A1mbricos#802.11 (Oct-2007)

http://bibliotecnica.upc.es/pfc/mostrar_dades_PFC.asp?id=4079 (Dic-2007)

http://es.wikipedia.org/wiki/Wi-Fi (Dic-2007)

http://www.saulo.net/pub/inv/SegWiFi-art.htm (Oct-2007)

http://www.montevideolibre.org/manuales:libros:wndw:capitulo_6:amenazas (Nov-2007)

http://es.wikipedia.org/wiki/Spoofing (Sep-2007)

http://www.elrincondelprogramador.com/default.asp?pag=articulos/leer.asp&id=55 (Dic-2007)

http://www.timagazine.net/magazine/0798/wireless.cfm (Dic-2007)

http://www.iec.uia.mx/proy/titulacion/proy14/vpnprin.htm (Nov-2007)

http://www.gobernabilidad.cl/modules.php?name=News&file=article&sid=419 (Nov-2007)

http://www.ieee802.org/ (Sep-2007)

CURSO POLITECNICA NACIONAL, Wireless & Wirelan 2004.

ORIENTE, 1990; Diccionario Enciclopédico Ilustrado, Primera Edición, Buenos Aires.

GLOSARIO DE TERMINOS

ACCESS POINT (PUNTO DE ACCESO).- Son los equipos que permiten la comunicación entre dispositivos inalámbricos y las redes cableadas (WireLAN o wireline).

ANTENAS.- Las antenas son elementos que aumentan el nivel de transmisión y de recepción de la señal en el medio.

ATENUACION.- La atenuación es la fuerza de la señal sobre la distancia también conocida como pérdida de propagación.

CLIENTE INALAMBRICO.- Comunica a cualquier dispositivo con una interfaz de red Ethernet con una red inalámbrica, se necesita de la dirección MAC del punto de acceso.

REDES AD-HOC.- Son aquellas que están formadas por estaciones que se comunican mutuamente por un medio inalámbrico.

REDES DE INFRAESTRUCTURA.- Son aquellas que contienen uno o más puntos de acceso y tienen un sistema de distribución que permite la comunicación con redes cableadas.

REPETIDOR.- Extiende el rango o cobertura de una red inalámbrica.

RED PRIVADA.- Redes privadas son aquellas utilizadas por personas naturales o jurídicas exclusivamente, con el propósito de conectar distintas instalaciones de su propiedad que se hallen bajo su control. Su operación requiere de un permiso.

Una red privada puede estar compuesta de uno o más circuitos arrendados, líneas privadas virtuales, infraestructura propia o una combinación de éstos. Dichas redes pueden abarcar puntos en el territorio nacional y en el extranjero. Una red privada puede ser utilizada para la transmisión de voz, datos, sonidos, imágenes o cualquier combinación de éstos.

SERVIDOR.- Ordenador que se encarga de la distribución del servicio de aplicaciones que se encuentran en el mismo.

PUENTE INALAMBRICO.- Conecta inalámbricamente dos redes. Para este caso, los dos equipos deben tener el mismo modo de operación.

TERMINAL PORTATIL.- Es un cliente que se conecta a la red de forma inalámbrica a través de un dispositivo.

ANEXOS

Anexo 1 Modelos de antenas.

PA-3500 WiMAX antena direccional


wimo

Antena plana de panel para punto a punto o puntos multiples. Incluye el montaje universal para abatir, para la pared o el montaje del mástil, todo el hardware incluido.

	PA-3500-12	PA-3500-18	
Frecuencia	3400-3600	3400-3600	MHz
Ganancia	12	18	dBi
HPBW horizontal	ca. 35°	ca. 30°	mm
HPBW vertical	ca. 30°	ca. 25°	mm
SWR max.	<1:2	<1:2	
Max. poténcia	10	10	Watt
Conector	N jack	N jack	
Max. Mast diametro	55	55	mm
Size	140x166	290x330	mm
Peso			Kg
Artículo No.	18850.12 **113.41 usd** Comprar	18850.18 **204 usd** Comprar	

Detalles PA-3500-12 para Descargar (inglés/alemán, PDF, 130kb)
Detalles PA-3500-18 para Descargar (inglés/alemán, PDF, 120kb)

http://www.wimo.com/cgi-bin/verteiler.pl?url=overview-wifi-antennas_s.html

Wifi solid Grid Dish 5

Info freight charges

18685.x

The Wifi grid dishes are made from casted aluminium and combine a high stability and low wind load for a long endurance of the antennas. The carefully designed parabolic dish offer a gain of 26dBi on 2.4GHz and 31dBi on 5GHz. In contrast to other parabolic dishes these antennas are designed for best performance also on 5GHz.
Due to the split construction of the reflector (90x70cm) the shipping size is very small, very facorable for the shipping ost. A tilt/swivel mount for mast mounting is included. Connector N female.

Technical data

Frequency range	2.4-2.8	5.1-5.85	GHz
Gain	26-27	31	dBi
HPBW	8/11°	12°	
Wind speed	160	160	km/h max.
Price	**223.88 usd**	**257.75 usd**	
Comprar	Comprar		

Download: Datasheet 18685.24 (PDF, EN, 450KB)
Download: Datasheet 18685.5 (PDF, EN, 590KB)

Anexo 2 Modelos de Routers

Paga ahora con MercadoPago en un solo paso

Puedes pagar hasta en 24 cuotas con tarjeta de crédito
Ver formas de pago con MercadoPago

Pagar ahora

Computación › Redes › Routers No Inalámbricos

Artículo: #31773974

[3 Fotos]

Haz clic en la foto para ampliarla

Precio Final: U$S 184.99 c/u

Compra Inmediata

o 6 cuotas de U$S 36.38

Paga en cuotas | Ver formas de pago

Vendedor: QUICK INFORMÁTICA (5287)

Puntaje del vendedor: 5287

99% calificaciones positivas (1% negativas)

Miembro desde: 20/05/2004 | Ver reputación

Ver artículos del vendedor | Ver eShop

Tipo de producto: Nuevo

Ubicación: CAPITAL FEDERAL

Finaliza en: 12d 9h (17/12/2007 11:28)

Cant. de ofertas: 1 Ver compradores Visitas: 145

Cantidad: 1 **de 4 disponibles**

Tu Oferta: U$S 184.99 c/u

Comprar

Programa de Protección al Comprador (Ver requisitos)

Regístrate gratis aquí | ¿Cómo Comprar? | ¿Cómo Vender? | Ver preguntas al Vendedor | Seguir de cerca este artículo | Envíale este artículo a un amigo

Descripción

Garantía: **Garantia directa por 3 años con Quick Informática S.A. presentando factura de compra.**

Quick Informática

Router Linksys Etherfast Cable/DSL VPN 50 tuneles con Switch 10/100 de 4 Ports Lan + 1 port Wan Server Modelo BEFVP41

LINKSYS
A Division of Cisco Systems, Inc.

- ☑ Nuevos, en caja
- ☑ Fácil de instalar
- ☑ Con Fuente 220v
- ☑ Garantía de 3 años

PRECIO OFERTA EFECTIVO: U$S 184.99 final (incluye IVA)

Cotización del dolar U$S 1 = $3.16, el tipo de cambio se tomará al día de efectivizado el pago

¡Compre Tranquilo, somos MercadoLider "Platinum" (los más distinguidos y selectos usuarios de Mercadolibre!

Los MercadoLideres son aquellos miembros de la comunidad que por su trayectoria, seriedad y continuidad, MercadoLibre los distingue con medallas especiales. Puedes verificar que "QUICK INFORMATICA S.A." es MercadoLider Platinum porque tiene las medallas distintivas al lado de su apodo.

¡Mi reputación es de 100% calificaciones positivas!

Mi reputación al 01-11-2007. Puntaje 5084. Con un 100% de calificaciones positivas (0% negativas). Soy miembro de MercadoLibre desde el 20-05-2004 y estoy registrado en Micro Centro, CAPITAL FEDERAL.

COSTOS DE ENVIO

NUESTRO LOCAL

Cable/ DSL VPN Router

With 4-port 10/100 switch

FEATURES

-Full IPSec Virtual Private Network
(VPN) Capability
-Supports DES and 3DES Encryption Algorithms
-Supports MD5 and SHA Authentications Algorithms
-Supports IKE Key Management
-Supports Up to 50 IPSec Tunnels
Simultaneously
-Compatible with Other IPSec
VPN Products
-Acts as a DHCP Server for Your
Existing Network
-Hardware Security Co-Processor
by Hifn Inside
-NAT, PPPoE, IP Filter, and MAC
Filter Support
-Built-in 4-Port 10/100 Switch for
Sharing Broadband

SPECIFICATIONS

Model: BEFVP41
Standards: IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX)
Ports: One 10/100 RJ-45 Port (Internet)
Four 10/100 RJ-45 Ports (Ethernet)
Cabling Type: 10BaseT, 100BaseTX: UTP Category 5 or better
LEDs: Power, Internet, Ethernet (1-4)
Security Features: DES (56-bit), 3DES (168-bit), MD5, SHA
Warranty:1 Years

Minimum Requirements	Package Contents
• Broadband connection and Cable/DSL modem • TCP/IP Protocol • CD-ROM Drive • Internet Explorer 5.0 or Netscape 6 for webbased configuration • Network adapter • Network cable	• Cable/DSL VPN Router • AC Power Adapter • User Guide (PDF on CD) • Quick Install

Router Linksys BEFSR41 4 Port Switch

Publicación # 16687486

Foto 1

Precio fijo:
US$ 109.00
o 6 cuotas sin interés de $57.46con DEPAGOS
Cantidad:
1 (1 artículos disponibles)
Tipo de publicación:
compra inmediata
La Compra Inmediata es una compra a precio fijo.
Al comprar el producto se accede a los datos del vendedor para concretar la transacción y a diferencia de otros tipos de venta no es necesario esperar a que finalice la publicación para obtenerlos.
El producto se vende al precio publicado al momento en que lo compras.

Tipo de producto:
Nuevo
Cantidad vendida:
1 Ver listado de compradores
Cantidad de visitas:
222
Finaliza en:
26d 23h (09/01/2008 16:22)
Vendedor:
abeyoglo
Calificaciones:
745 100% (+)
Otros productos del vendedor | Reputación | Preguntas al vendedor
Ubicación:
Parque Chacabuco, Capital Federal
Métodos de envío | Métodos de pago | Descripción del producto Enviar a un amigo Imprimir Seguir este producto Reportar al detective deRemate

Anexo 3 Modelos de Transceivers

Mini-gbic 3Com® 1000 BASE-SX SFP Transceiver

Publicación # 17765805

Foto 1

Precio fijo:
US$ 394.00
o 6 cuotas sin interés de $207.70con DEPAGOS
Cantidad:
1 (10 artículos disponibles)
Tipo de publicación:
compra inmediata
La Compra Inmediata es una compra a precio fijo.
Al comprar el producto se accede a los datos del vendedor para concretar la transacción y a diferencia de otros tipos de venta no es necesario esperar a que finalice la publicación para obtenerlos.
El producto se vende al precio publicado al momento en que lo compras.

Tipo de producto:
Nuevo
Finaliza en:
1d 4h (14/12/2007 21:29)
Vendedor:
EBayer
Calificaciones:
1293 97% (+)
Otros productos del vendedor | Reputación | Preguntas al vendedor
Ubicación:
Turdera, Gran Buenos Aires
Métodos de envío | Métodos de pago | Descripción del producto
Enviar a un amigo Imprimir Seguir este producto Reportar al detective deRemate Como comprar en deRemate

Descripción del producto

Mini-gbic 3Com® 1000 BASE-SX SFP Transceiver

CODIGO DEL FABRICANTE: 3CSFP91
CODIGO INTERNO: 3C0617

Características y ventajas

Flexibilidad en Conexiones Gigabit Ethernet
Este transceptor SFP (Pequeño Factor de Forma Enchufable) permite una conexión 1000BASE-SX. Los SFPs tienen un factor de forma de la mitad del tamaño de los estándares actuales de la industria.

Este transceptor SFP puede usarse en aquellos conmutadores y módulos 3Com que soporten módulos SFP. Los SFPs pueden combinarse en un determinado conmutador para maximizar la flexibilidad. Sin embargo, la conexión y el puerto asociado en el extremo remoto deben acoplarse con el tipo de conexión elegido.

Encontrará una lista actual de estos productos en el apartado Especificaciones de producto, sección Este producto soporta...

La simplicidad del diseño del SFP crea una nueva definición de la facilidad de uso con un excepcional rendimiento mecánico y óptico

Permite una conexión 1000BASE-SX

Especificaciones de producto

Interfaces con los medios: LC
Tipo de conector: LC
Tipo de fibra: Multi-modo

3Com® 1000BASE-SX GBIC Transceiver 3CGBIC91
Publicación # 18340811

Foto 1

Precio fijo:
US$ 549.00
o 6 cuotas sin interés de $289.41con DEPAGOS
Cantidad:
1 (1 artículos disponibles)
Tipo de publicación:
compra inmediata
La Compra Inmediata es una compra a precio fijo.
Al comprar el producto se accede a los datos del vendedor para concretar la transacción y a diferencia de otros tipos de venta no es necesario esperar a que finalice la publicación para obtenerlos.
El producto se vende al precio publicado al momento en que lo compras.

Vendedor:
abeyoglo
Calificaciones:
745 100% (+)
Otros productos del vendedor | Reputación | Preguntas al vendedor
Ubicación:
Parque Chacabuco, Capital Federal
Métodos de envío | Métodos de pago | Descripción del producto Enviar a un amigo Imprimir Seguir este producto Reportar al detective deRemate Como comprar en deRemate

Descripción del producto

Consultar Stock antes de ofertar

El Stock es Figurativo

SIEMPRE CONSULTAR STOCK ANTES DE OFERTAR

3Com® 1000BASE-SX GBIC Transceiver

Características y ventajas

Flexible Gigabit Ethernet Connections
Un Gigabit Interface Converter (GBIC) es un transceptor modular estándar que ofrece una mayor flexibilidad para conexiones Gigabit Ethernet.

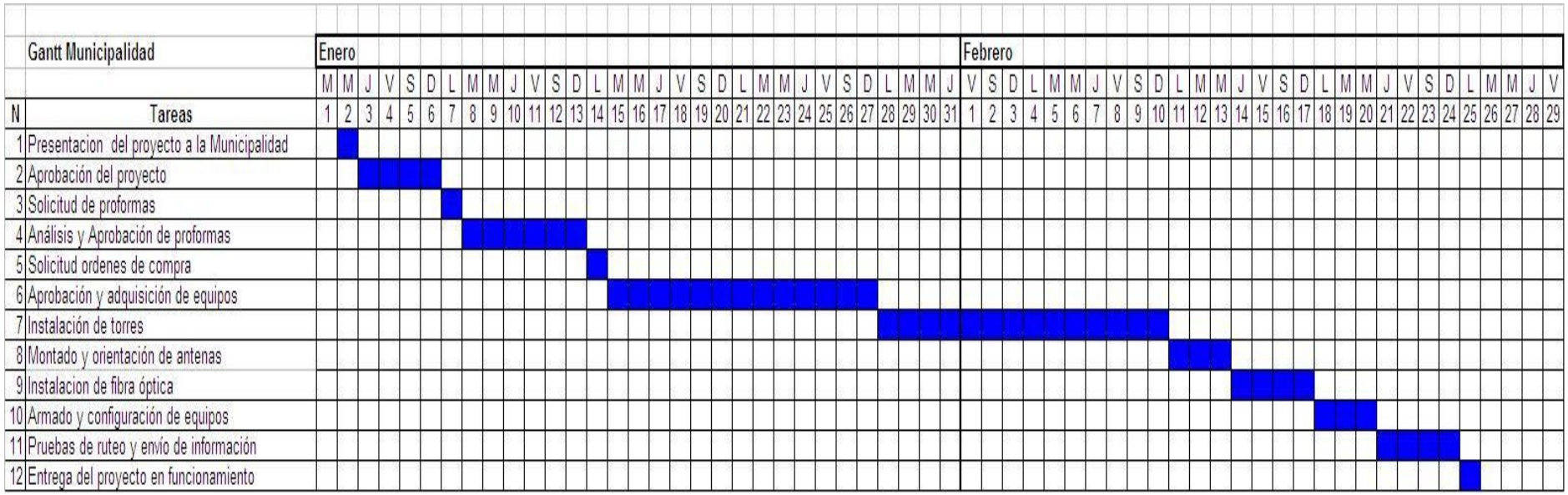
Este transceptor GBIC puede utilizarse en aquellos switches y módulos 3Com que soporten módulos GBIC. Los GBICs pueden mezclarse y combinarse en un determinado switch para maximizar la flexibilidad.

Puede encontrarse una lista actual de estos productos en la sección "Especificaciones de producto" bajo el epígrafe "Este producto soporta".

Especificaciones de producto

- **Tipo de conector:** Fibra SC
- **Tipo de fibra:** Multi-modo

Contenidos del paquete
- GBIC



Anexo 4 Cronograma de Gantt para implementación.