REDES INALAMBRICAS (WIRELESS LAN)

Otra Posibilidad para la Conexión y Distribución de Datos

CARLOS ALBERTO VANEGAS[@]

Resumen

La flexibilidad y movilidad hacen que las redes sin cable sean muy efectivas para extensiones y una atractiva alternativa a las redes cableadas, puesto que proporcionan la misma funcionalidad sin las restricciones del cable en sí mismo. Las redes inalámbricas permiten topologías desde las más simples hasta las más complejas las cuales ofrecen conexión y distribución de datos y permiten "roaming" (navegar). Además de ofrecer al usuario final movilidad en un entorno de red, habilitan redes portátiles permitiendo a las LAN movimientos con el conocimiento de los usuarios que las utilizan.

Palabras Clave: Red Inalámbrica, Capa Física, Capa de Enlace de Datos, Lan, Infrarrojos, Ondas de Radio, Frecuencia, Cliente, Estaciones (STA), Punto de Acceso (AP), Redes Privadas Virtuales (VPN), Cortafuegos, Protocolo de Seguridad IP(IPSec).

Abstract

The flexibility and mobility make the wireless networks effective for extensions and an attractive alternative to the wired networks, since they provide the same functionality without the restrictions of the cable. Wireless networks allow topology from the simplest until complex that offer connection and distribution of data and they allow " roaming ". Besides offering to the user final mobility in a networks environment, they enable portability allowing to the LAN knowledge with the movements of the users that use them.

[@] Ingeniero de Sistemas. Especialista de Ingeniería de Software de la Universidad Distrital. Estudiante (Ultimo Semestre) Maestría de Ingeniería de Sistemas de la Universidad Nacional. Docente Universidad Distrital adscrito a la Facultad Tecnológica. cavm10@hotmail.com

Key Words: Wireless Network, Physical Layer, Data Link Layer, LAN, Infrared, Radio Wave, Frequency, Client, Stations (STA), Access Point (AP), Virtual Private Networks (VPN), Fire-break, IP Security Protocol.

1. INTRODUCCIÓN

El simple hecho de ser seres humanos nos hace desenvolvernos en medios donde tenemos que estar comunicados. Por eso la gran importancia de la transmisión y la recepción de información, y en la época actual donde los computadores hacen parte de la cotidianidad, es necesario establecer medios de comunicación eficaces entre ellos.

Las Redes Inalámbricas brindan la facilidad de conectar entre sí computadores de una red sin utilizar cables, ya que utilizan ondas de radio para transmitir la información de un punto a otro. Esto se consigue instalando en cada equipo a conectar una tarjeta de recepción/transmisión; y equipos de repetición para ampliar cobertura.

Son utilizadas con frecuencia en lugares donde el computador no puede permanecer en un sólo lugar (por ejemplo: almacenes, oficinas, fábricas, etc.); y en lugares donde se requiere conectividad móvil para un computador portátil. En ellas se pueden llegar a alcanzar velocidades (ancho de banda) de 100 Mbps[1].

No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps.

2. ANTECEDENTES

Una de las áreas de mayor potencial en la evolución futura de las telecomunicaciones es la

transmisión inalámbrica digital de banda ancha. Idealmente, un sistema inalámbrico de banda ancha permitiría la transmisión de cualquier tipo de información digitalizada (audio, vídeo, datos) desde cualquier lugar y en cualquier momento, con posibilidad de transmitir en tiempo real de ser necesario. Entre las ventajas de un sistema inalámbrico sobre uno cableado podemos mencionar: la movilidad y el menor tiempo de instalación y puesta en marcha del sistema.

WLAN son las siglas en inglés de Wireless Local Área Network. Es un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Utiliza tecnología de radio frecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas.
Ejemplos de uso: ventas al por menor, almacenes, manufacturación, etc., casos en que se transmite la información en tiempo real a un procesador central. Cada día se reconocen más este tipo de redes en un amplio número de negocios y se augura una gran extensión de las mismas y altas ganancias.

3. RED INALÁMBRICA

¿ Qué es una red inalámbrica (WLAN)?.

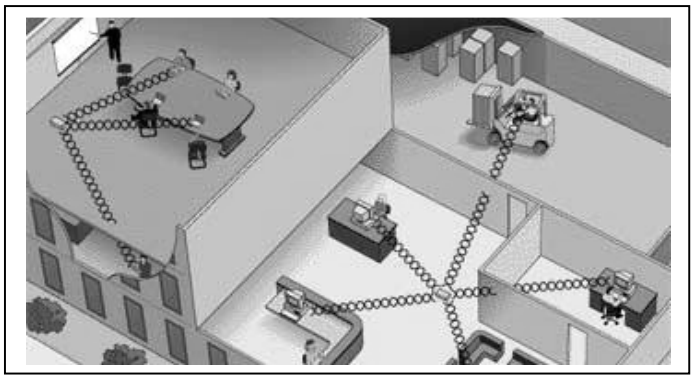

Figura No. 1. Red Inalámbrica

Una red de área local inalámbrica o WLAN (Wireless LAN) puede definirse como una red local que utiliza tecnología de radiofrecuencia para enlazar los equipos conectados a la red en

[1] Megabit por segundo.

lugar de los cables coaxiales o de fibra óptica que se utilizan en las LAN convencionales cableadas. Estos enlaces se implementan mediante tecnología basada en microondas o bien en infrarrojos.

La tecnología basada en microondas se puede considerar como la más desarrollada, dado que es donde se han conseguido los resultados más claros. La tecnología basada en infrarrojos, actualmente es la menos desarrollada, porque las distancias que cubren son cortas y aún existen una serie de problemas técnicos por resolver[2]. A pesar de todo, presenta la ventaja frente a las microondas de que no existe el problema de la saturación del espectro de frecuencias, lo que la hace llamativa.

Las redes inalámbricas, traspasan edificios, paredes, sin correr peligro, están listas para la acción en pocos minutos, permiten a sus usuarios trabajar en redes de equipos portátiles.

La primera empresa que desarrolló y comercializó un sistema inalámbrico de conexión a redes fue NCR, cuando a finales de 1990 lanzó un sistema que utilizaba ondas de radio para interconectar computadores. Desde entonces, la comunicación por redes inalámbricas ha dejado de ser experimental, para convertirse en una solución real a problemas concretos.

¿Por qué utilizar WLAN's?

Es clara la alta dependencia en los negocios de las redes de comunicación; por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad.

Así mismo la red puede ser más extensa sin tener que mover o instalar cables.

Respecto a la red tradicional la red inalámbrica ofrece las siguientes ventajas:

1) **Movilidad**: Información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. Lo cual supone mayor productividad y posibilidades de servicio.

2) **Facilidad de instalación**: Evita obras para extender cable por muros y techos.

3) **Flexibilidad**: Permite llegar adonde el cable no puede.

4) **Reducción de costos**: Cuando se dan cambios frecuentes o el entorno es muy dinámico el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.

[2] Richard Allen, fundador de Photonics Corp., en 1985, el cual desarrolló un "Transreceptor Infrarrojo".

5) **Escalabilidad**: El cambio de topología de red es sencillo y da igual trato a pequeñas y grandes redes.

4. TIPOS DE REDES INALÁMBRICAS

4.1 De larga distancia

Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps[3]. Existen dos tipos de redes de larga distancia:

4.1.1 Redes telefónicas celulares

Son un medio para transmitir información de alto precio, debido a que los módems celulares actualmente son más caros y delicados que los convencionales, ya que requieren circuiteria especial, que permite evitar la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos. Otras desventajas de la transmisión celular son:

- La carga de la batería se termina fácilmente.
- La transmisión celular tradicional se intercepta fácilmente (factor importante en lo relacionado con la seguridad).
- Las velocidades de transmisión a pesar de las nuevas tecnologías aun son bajas.

Todas estas desventajas hacen que la comunicación celular se utilice poco en el envío de *grandes cantidades* de información (voz, datos, video).

4.1.2 Red pública de conmutación de paquetes por radio

Estas redes no tienen problemas de pérdida de señal debido a que su arquitectura está

diseñada para soportar paquetes de datos en lugar de comunicaciones de voz. Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radio frecuencia restringidas por la propia organización de sus sistemas de cómputo [1].

4.2 De corta distancia

Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

5. TECNOLOGÍA WLAN

Según el diseño requerido se tienen distintas tecnologías aplicables:

5.1 Banda estrecha

Se transmite y recibe en una banda específica de frecuencia lo más estrecha posible para el paso de información. Los usuarios tienen distintas frecuencias de comunicación de modo que se evitan las interferencias. Así mismo un filtro en el receptor de radio se encarga de dejar pasar únicamente la señal esperada en la frecuencia asignada.

5.2 Banda ancha

Es el usado por la mayor parte de los sistemas sin cable. Fue desarrollado por los militares para una comunicación segura, fiable y en misiones críticas. Se consume más ancho de banda pero la señal es más fácil de detectar. El receptor conoce los parámetros de la señal que se ha difundido. En caso del receptor no estar en la correcta frecuencia, la señal aparece como ruido de fondo. Hay dos tipos de tecnología en banda ancha:

---

[3] Kilobit por segundo

5.2.1 Salto de frecuencia(FHSS: Frecuency-Hopping Spread Spectrum)

Utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Convenientemente sincronizado es como tener un único canal lógico. Para un receptor no sincronizado FHSS es como un ruido de impulsos de corta duración.

5.2.2 Secuencia directa (DSSS: Direct-Sequence Spread Spectrum)

Se genera un bit redundante por cada bit transmitido. Estos bits redundantes son llamados "chipping code". Cuanto mayor sea esta secuencia mayor es la probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda). Incluso si uno o más bits son perturbados en la transmisión las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado.

Las redes inalámbricas se diferencian de las convencionales principalmente en la "Capa Física" y la "Capa de Enlace de Datos", según el modelo de referencia OSI. La capa física indica cómo son enviados los bits de una estación a otra. La capa de Enlace de Datos (denominada MAC), se encarga de describir cómo se empacan y verifican los bits de modo que no tengan errores. Las demás capas forman los protocolos o utilizan puentes, enrutadores o compuertas para conectarse. Los dos métodos para aplicar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

Transmisión de radio frecuencia (incluye microondas): Algunas de las principales características de las conexiones basadas en radio frecuencia son:

- Permite traspasar la mayoría de los objetos (depende de la frecuencia) y es recomendada para cubrir áreas grandes.
- Las frecuencias que pueden ser utilizadas son restringidas debido a que la mayoría de ellas son utilizadas por otros sistemas, por ejemplo: radio aficionados, radio celular, sistemas de radar.

Algunos problemas que presenta la radio frecuencia son: interferencia (incluyendo dispersión y cruce de comunicaciones entre sí) y poca seguridad (la idea en las redes es que la señal sea transmitida y recibida con un mínimo de alteraciones).
Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente.

Transmisión de luz infrarroja: Las redes de luz infrarroja están limitadas por el espacio y casi generalmente la utilizan redes en las que las estaciones se encuentran en un solo cuarto o piso, algunas compañías que tienen sus oficinas en varios edificios realizan la comunicación colocando los receptores-emisores en las ventanas de los edificios. El principio de la comunicación de datos es una tecnología que se ha estudiado desde los 70´s, Hewlett-Packard desarrolló su calculadora HP-41 que utilizaba un transmisor infrarrojo para enviar la información a una impresora térmica portátil, actualmente esta tecnología es la que utilizan los controles remotos de las televisiones o aparatos eléctricos que se usan en el hogar. El mismo principio se usa para la comunicación de Redes, se utiliza un "*transreceptor*" que envía un haz de Luz Infrarroja, hacia otro que la recibe. La transmisión de luz se codifica y decodifica en el envío y recepción en un protocolo de red existente. Uno de los pioneros en esta área es Richard Allen, que fundó Photonics Corp., en 1985 y desarrolló un "Transreceptor Infrarrojo". Los primeros transreceptores dirigían el haz infrarrojo de luz a una superficie pasiva, generalmente el techo, donde otro transreceptor recibía la señal. Se pueden instalar varias estaciones en una sola habitación utilizando un área pasiva para cada transreceptor.

Transmisión Infrarroja WLAN's: Las principales características de las conexiones basadas en la transmisión infrarroja son:

- El rango de trabajo va entre 700nm y 1500nm, proporciona teóricamente un ancho de banda de 300THz.
- La radiación infrarroja no puede traspasar las paredes. Esto permite construir fácilmente una red basada en celdas. Por ejemplo en un edificio de oficinas, cada oficina podría tener una celda y así no habría problemas de interferencia entre dos celdas.
- El material de los objetos en un ambiente de oficinas tiene buenas propiedades de

reflexión (40%-90%). Esto es bueno porque existe un mejor intercambio de energía óptica entre transmisores-receptores.

Algunos de los problemas que se pueden presentar con esta tecnología son: dispersión y poca seguridad.

Radio Frecuencia vs. Comunicaciones Infrarrojas: Las WLAN's basadas en Radio Frecuencia son utilizadas en áreas donde las distancias entre el transmisor y el receptor son grandes y no se requieren altas velocidades en las comunicaciones. Las Comunicaciones Infrarrojas se utilizan en áreas donde existe ruido, por ejemplo fábricas o donde la arquitectura de la celda es fácil de diseñar como en un edificio de oficinas donde cada celda ocupará una pequeña sala. La seguridad es un problema en ambos tipos de tecnologías debido a que la señal puede ser interceptada, por lo que debe usarse la encriptación de los datos. Las comunicaciones infrarrojas proporcionan altas velocidades de transmisión debido al gran ancho de banda utilizado.

El IEEE 802.11 define opciones de la capa física para la transmisión inalámbrica y la capa de protocolos MAC.

Capa Física Infrarroja: Se soporta un standard infrarroja, que opera en la banda 850nM a 950nM, con un poder máximo de 2 W. La modulación para el infrarrojo se logra usando 4 o 16 niveles de modulación "posicionamiento por pulsos". La capa física soporta dos tasas de datos: 1 y 2Mbps.

Capa física DSSS: utiliza una Secuencia Barker de 11 bits para extender los datos antes de que se transmitan. Cada bit transmitido se modula por la secuencia de 11 bits. Este proceso extiende la energía de RF por un ancho de banda más extenso que el que se requeriría para transmitir los datos en bruto.

Capa física FHSS: tiene 22 modelos de espera para escoger. La capa física en Saltos de Frecuencia se exige para saltar por la banda ISM 2.4GHz cubriendo 79 canales. Cada canal ocupa un ancho de banda de 1Mhz y debe brincar a la tasa mínima especificada por los cuerpos reguladores del país pretendido. Para los Estados Unidos se define una tasa de salto

mínima de 2.5 saltos por segundo.

Cada una de las capas físicas utiliza su propio encabezado único para sincronizar al receptor y determinar el formato de la señal de modulación y la longitud del paquete de datos. Los encabezamientos de las capas físicas siempre se transmiten a 1Mbps. Los campos predefinidos en los títulos proporcionan la opción para aumentar la tasa de datos a 2 Mbps para el paquete de los datos existente.

La Capa MAC para la 802.11 tiene similitudes a la de Ethernet cableada de línea normal 802.3. El protocolo para 802.11 utiliza un tipo de protocolo conocido como CSMA/CA (Carrier-Sense, Múltiple Access, Collision Avoidance). Este protocolo evita colisiones en lugar de descubrir una colisión, como el algoritmo usado en la 802.3. Es difícil descubrir colisiones en una red de transmisión RF y es por esta razón por la que se usa la anulación de colisión. La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. Utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple midiendo la energía RF de la antena y determinando la potencia de la señal recibida. Esta señal medida es normalmente conocida como RSSI[4]. Si la potencia de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares. El Standard proporciona otra opción CCA que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible. Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802.11. El mejor método a utilizar depende de los niveles de interferencia en el entorno operativo. El protocolo CSMA/CA permite opciones que pueden minimizar colisiones utilizando "peticiones de envío" (RTS), "listo para enviar" (CTS), datos y tramas de transmisión de reconocimientos (ACK), de una forma secuencial. Las comunicaciones se establecen cuando uno de los nodos inalámbricos envía una trama RTS. La trama RTS incluye el destino y la longitud del mensaje. La duración del mensaje es conocida como el vector de asignación de red (NAV). El NAV alerta a todos los otros en el medio, para retirarse durante la duración de la transmisión. Las estaciones receptoras emiten una trama CTS, que hace eco a los remitentes y al vector NAV. Si no se recibe la trama CTS, se supone que ocurrió una colisión y los procesos RTS

empiezan de nuevo. Después de que se recibe la trama de los datos, se devuelve una trama ACK, que verifica una transmisión de datos exitosa.

6. FUNCIONAMIENTO DE UNA RED INALÁMBRICA

Cada puerto de acceso tiene una lista de los clientes inalámbricos con los que puede asociarse. Cuando un cliente inalámbrico, por ejemplo un computador, está listo para comunicarse con la red, su tarjeta de red inalámbrica difunde una señal de radio. Cuando el punto de acceso detecta una señal de un cliente inalámbrico asociado, la señal es contestada y se establece una conexión con la red. Un cliente inalámbrico puede estar asociado con varios puntos de acceso diferentes, bien sea por una mayor cobertura mediante puntos de acceso situados en una área de servicio específica o porque el cliente inalámbrico se está desplazando de un punto de acceso a otro punto que está dentro del área de cobertura extendida.

Por ejemplo, al llevar un sistema portátil desde una oficina a una sala de conferencias, la señal entre su cliente inalámbrico y el punto de acceso actual puede debilitarse. El cliente inalámbrico busca automáticamente la señal más intensa de otro punto de acceso y realiza una nueva conexión con el segundo punto de acceso a medida que se incrementa la intensidad de la señal. El cliente inalámbrico se puede conectar automáticamente a varios puntos de acceso a través de la ruta sin tener que interrumpir la conexión con la red. Esta técnica se denomina "roaming" ('desplazamiento automático').

La técnica de desplazamiento automático garantiza un servicio de red estable e ininterrumpido incluso cuando el sistema está en movimiento.

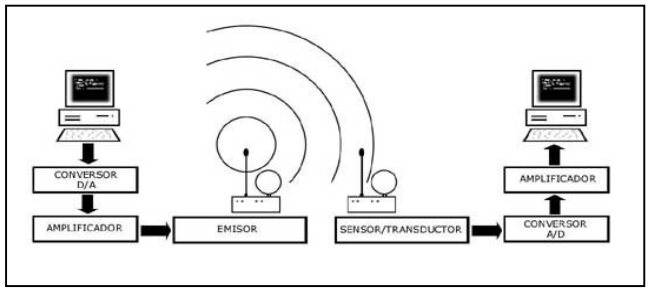

Figura No. 2. Funcionamiento Red Inalámbrica

[4] Intensidad de señal de Radio Frecuencia de entrada.

7. CONFIGURACIONES DE LA WLAN

Las configuraciones de la WLAN pueden ser simples o complejas. La más básica, se da entre dos computadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Se llama Red igual a igual o Red peer to peer.

Figura No. 3. Red igual a igual

Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración.

Instalando un Punto de Acceso (APs) se puede doblar el rango al cuál los dispositivos pueden comunicarse, pues actúan como repetidores. Desde que el punto de acceso se conecta a la red cableada, cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso.

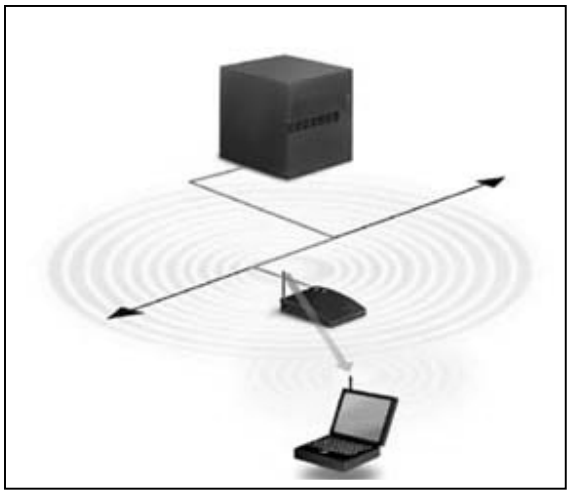

Figura No. 4. Cliente y punto de acceso

Los puntos de acceso tienen un rango finito, del orden de 150m en lugares cerrados y 300m en zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de

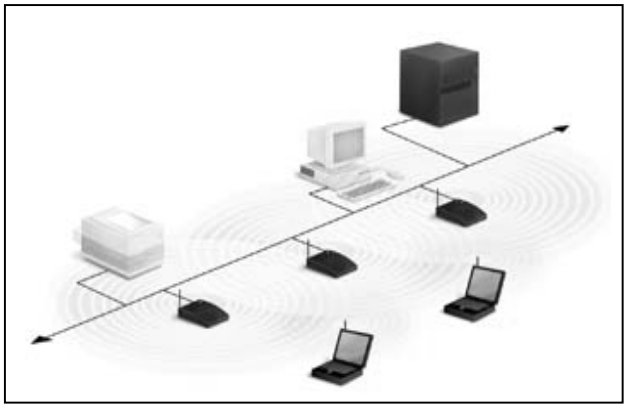

Figura No. 5. Múltiples punto de acceso y roaming

acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso.

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso. Los puntos de extensión funcionan como su nombre indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos.

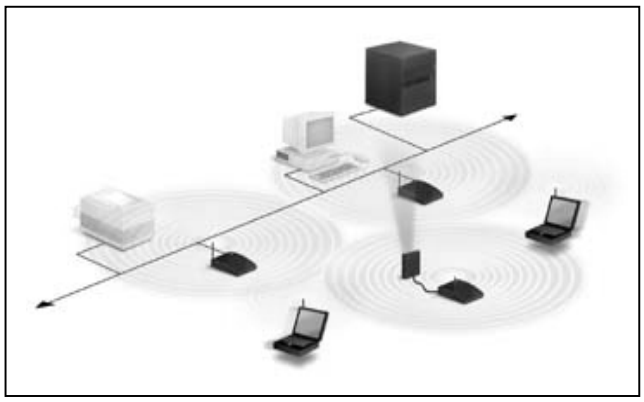

Figura No. 6. Uso de un punto de extensión

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: se quiere una LAN sin cable a otro edificio a 1Km de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cuál permite una conexión sin cable en esta aplicación.

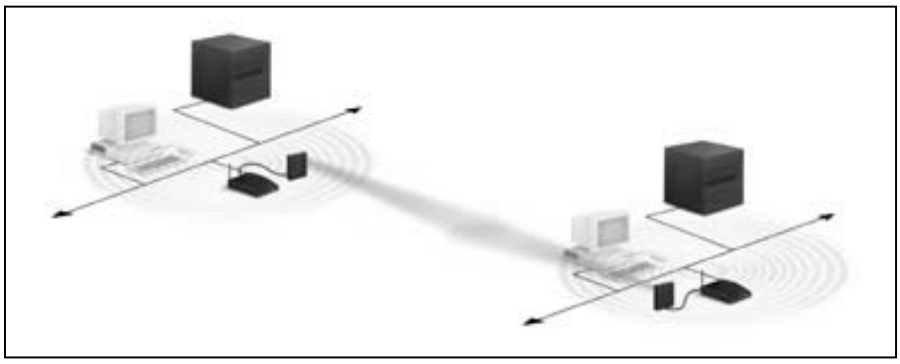

Figura No. 7. Utilización de Antenas direccionales

8. SEGURIDAD EN LAS COMUNICACIONES INALÁMBRICAS

El estándar 802.11 establece diversos mecanismos para conseguir entornos de redes

inalámbricas seguras. Los mecanismos utilizados habitualmente son:

8.1 Wired Equivalent Protocol (WEP)

Se trata del primer mecanismo implementado y fue diseñado para ofrecer un cierto grado de privacidad, pero no puede equiparse (como a veces se hace) con protocolos de redes tales como IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio.
WEP utiliza una clave secreta, utilizada para la encriptación de los paquetes antes de su retransmisión. Por defecto, WEP está deshabilitado.
WEP2 Es una modificación del protocolo WEP realizada en el año 2001, como consecuencia de una serie de vulnerabilidades que se descubrieron. No obstante, todavía hoy no existe ninguna implementación completa de WEP2.

8.2 Open system authentication

Es el mecanismo de autenticación definido por el estándar 802.11 y consiste en autenticar todas las peticiones que reciben. El principal problema de este mecanismo es que no realiza ninguna comprobación y, además, todas las tramas de gestión son enviadas sin ningún tipo de encriptación, incluso cuando se ha activado WEP.

8.3 Access Control List (ACL)

Si bien no es parte del estándar, la mayoría de productos dan soporte al mismo. Se utiliza como mecanismo de autenticación la dirección MAC de cada STA, permitiendo el acceso únicamente a aquellas estaciones cuya MAC figura en la lista de control de acceso (ACL).

8.4 Closed network access control

Sólo se permite el acceso a la red a aquellos que conozcan el nombre de la red, o SSID. Éste nombre viene a actuar como contraseña.

8.5 Acceso no autorizado

Se pueden considerar los siguientes tipos de seguridad:

8.5.1 Identificación de redes

La identificación de redes es el método para detectar la existencia de un PA a una red inalámbrica. Para ello, se utiliza una WNIC (tarjeta de red inalámbrica) funcionando en modo promiscuo conjuntamente con un software que permite verificar la existencia de puntos de acceso. En el momento en que se detecta la existencia de una red abierta, habitualmente se dibuja una marca en el suelo donde se anotan las características de la misma. Esto se conoce como Wardriving y, una vez realizado, permite disponer de un autentico mapa donde se anotan todos los puntos de acceso con sus datos (SSID, WEP, direcciones MAC, etc.)**.**

8.5.2 Wardriving

Es el método más conocido para detectar las redes inalámbricas inseguras. Se realiza habitualmente con un dispositivo móvil, como un ordenador portátil o un PDA. El método es realmente simple: el atacante simplemente pasea con el dispositivo móvil y en el momento en que detecta la existencia de la red, se realiza una análisis de la misma. Para realizar el Wardriving se necesitan realmente pocos recursos. Los más habituales son un ordenador portátil con una tarjeta inalámbrica, un dispositivo GPS para ubicar el PA en un mapa y el software apropiado (AirSnort para Linux, BSD- AriTools para BSD o NetStumbler para Windows).

8.5.3 WarChalking

Se trata de un lenguaje de símbolos utilizado para marcar sobre el terreno la existencia de las redes inalámbricas, de forma que puedan ser utilizadas por aquellos que 'pasen por allí'. El lenguaje como tal es realmente simple:
Por ejemplo, el símbolo

Retina) (
1.5
identifica a un nodo abierto, que utiliza el SSID "Retina" y dispone de un ancho de banda de 1.5 Mbps.

9. PROTECCIÓN DE LAS REDES INALÁMBRICAS

Existen una serie básica de medidas para la protección de las redes inalámbricas. Ninguna de ellas, por si sola, impide el acceso no autorizado a la red por lo que será necesario utilizar una combinación de todas ellas:

9.1 Filtrado de direcciones MAC

Los puntos de acceso deben tener una relación de las direcciones MAC que pueden conectarse. No es un método que ofrezca un alto grado de seguridad, pero es una medida básica para evitar que el primero que pase por la calle pueda acceder a la red.
WEP ofrece un cierto grado de protección por lo que, a pesar de que el mecanismo de cifrado es relativamente simple y la existencia de programas para determinar cual es la clave de encriptación utilizada, es necesario que esté siempre activado.

9.2 SSID (identificador de red)

Este identificador es necesario para permitir a las STA comunicarse con el PA. Puede verse como si se tratara de una contraseña de acceso. El SSID se transmite en claro por la red, excepto si se ha activado la encriptación mediante WEP. No obstante, en los diversos dispositivos, el SSID se almacena sin cifrar, por lo que un atacante con acceso físico a una STA puede acceder a él.

10. CONSIDERACIONES DE DISEÑO

Como paso previo a la aplicación de medidas de protección de una red inalámbrica, es importante diseñar la red de forma correcta. Algunas medidas básicas a implementar son:

- Establecer redes privadas virtuales (VPN), a nivel de cortafuegos, para la encriptación del tráfico de la red inalámbrica.
- No deben conectarse directamente los PA a la red interna 'clásica' de la empresa. Las redes inalámbricas deben recibir el mismo trato que cualquier otra red insegura, como puede ser la conexión a Internet. Por tanto, entre la red inalámbrica y la red 'clásica' deberá existir un cortafuegos[5] y mecanismos de autenticación. Como ampliación del punto anterior, no deben colocarse los PA detrás del cortafuegos.

Los clientes de las redes inalámbricas deben acceder a la red utilizando mecanismos tales como: Secure Shell (SSH), redes privadas virtuales (VPN) o IPSec. Estos mecanismos facilitan los mínimos necesarios en lo referente a la autorización, autenticación y encriptación del tráfico.

11. CONCLUSIONES

El principal objetivo de una red es lograr la comunicación y el entendimiento entre varios computadores, en un espacio determinado, para cumplir con las tareas que sean propuestas. A partir de la incorporación de una red, los usuarios de ésta pueden tener acceso a diversos servicios, como correo electrónico y conexión corporativa a Internet, al igual que podrán compartir equipos, como impresoras y toda clase de información.

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadores mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde el computador no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

No se espera que las redes inalámbricas lleguen a reemplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica.

[5] Es un dispositivo lógico que protege una red privada del resto de la red (pública).

Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de solo 22 Mbps. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida" y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

La flexibilidad y movilidad hace de las redes sin cable que sean muy efectivas para extensiones y que sean una atractiva alternativa a las redes cableadas, puesto que proporcionan la misma funcionalidad sin las restricciones del cable en sí mismo. Las redes sin cable permiten topologías desde las más simples hasta complejas redes que ofrecen conexión y distribución de datos y permiten "roaming" (navegar). Además de ofrecer al usuario final movilidad en un entorno de red.

La instalación inalámbrica trae dos beneficios obvios, la flexibilidad de cambiar la configuración de la red y la anulación del costo por cableado. También nos ofrece la posibilidad de unir un grupo que trabajo de forma inalámbrica, con una red existente ya cableada, actualmente los costos de estas redes están bajando y sus velocidades se incrementan, pero aún estos costos se pueden considerar altos tomando en cuenta que el equipo de comunicación para una red inalámbrica depende del número de nodos.

Las redes inalámbricas pueden usarse en la elaboración de redes temporales (exposiciones) o para enlazar edificios cercanos. Igualmente, son útiles en el control de procesos en compañías como actualizar inventarios desde la misma planta de producción en la creación de puntos móviles de ventas y atención al cliente. Pero a pesar de estas referencias, la velocidad usada en la transmisión y recepción de datos podría generar problemas en el desarrollo de difíciles tareas de red, como la transmisión de archivos multimedia.

Referencias Bibliográficas

[1] AGUIRRE, José Eduardo. “Redes inalámbricas”, http://www.monografias.com/trabajos/redesinalam/redesinalam.shtml

[2] DAVIS et al. Computer Networks and their Protocols. John Wiley & Sons, 1979.

[3] SCHWARTZ, Mischa. Redes de Telecomunicaciones. Addison-Wesley Iberoamericana, 1994.

[4] SHELDON, Tom. LAN Times. Enciclopedia de Redes NetWorking. Osborne/McGraw Hill, 1994.

[5] SHELDON, Tom. LAN Times. Guía de Interoperabilidad. Osborne/McGraw Hill, 1995.

[6] STALLINGS, William. Comunicaciones y redes de Computadores. Prentice Hall, 1997. 75 págs.

[7] TANENBAUM, Andrew. Redes de Ordenadores. Prentice may, 1991.

Infografía

Wi-fi (802.11) Alliance
http://www.wi-fi.com
Standards IEEE "Get IEEE 802": Wireless (IEEE 802.11)

http://standards.ieee.org/getieee802/802.11.html
Best Practices for Deploying Wireless LANs

http://www.ebcvg.com/download.php?id=1160
Warchalking

http://www.warchalking.com
Símbolos utilizados en Warchalking

http://notabug.com/warchalking/card300.png
Wireless Security: Thoughts on Risks and Solutions

http://www.ebcvg.com/download.php?id=1371
Documentos varios sobre seguridad en redes inalámbricas

http://www.ebcvg.com/category.php?cat=11&p=1

http://www.hispasec.com/unaaldia.asp?id=1243