WIRELESS 2

1 OBJETIVO

El objetivo de esta clase es realizar un relevamiento de las distintas tecnologías utilizadas por Wireless, como la transmisión, las distintas configuraciones que se pueden implementar de acuerdo los posibles entornos de trabajo sea por cuestiones de infraestructura, rendimiento o seguridad.

Sobre esta última analizaremos las distintas estrategias que se encuentran disponibles para mejorar a las redes ya instaladas y las actuales, de esta forma podremos ajustar la convivencia entre estas y planificar redes que prevean la incorporación de nuevas tecnologías.

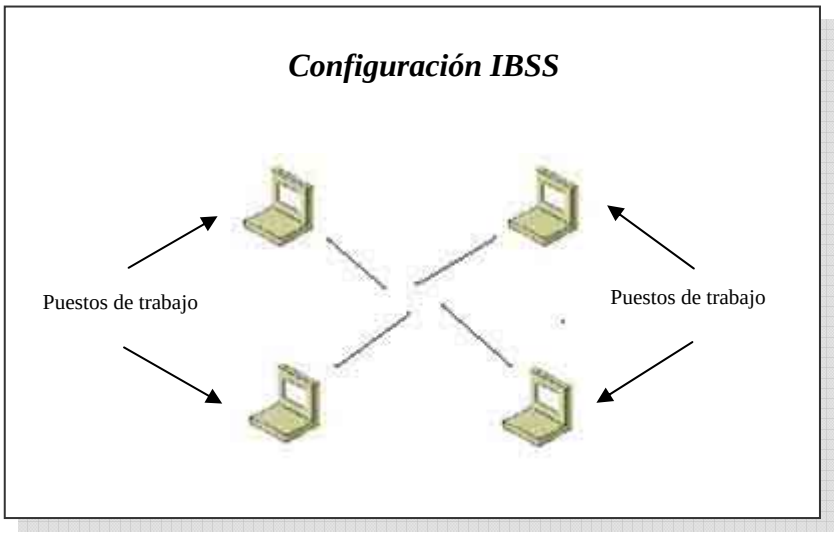
2 TIPOS DE ENLACES

En la siguiente sección nos abocaremos a realizar una breve reseña de los tipos de configuraciones que se pueden llegar a utilizar, cual es su objetivo y aplicabilidad.

2.1 ENLACES IBSS

Como ya hemos visto la configuración básica de una red con tecnología wireless (de PC a PC) que nosotros conocemos como Ad – Hoc lleva el nombre de ***IBSS*** (Independent Basic Service Set – Conjunto de Servicios Básicos Independientes).

La característica que posee esta configuración es que puede estar constituida por dos o más PC que tienen en la habilidad de comunicarse entre ellas sin la intervención de un Access Point.



2.2 ENLACES BSS

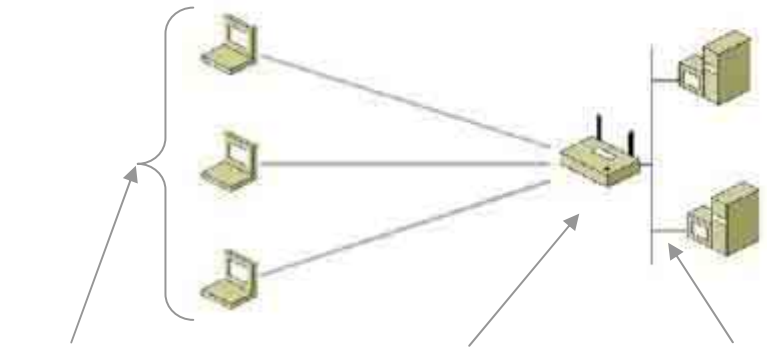
Como vimos anteriormente, las redes Ad - Hoc son muy prácticas por la movilidad en entornos de trabajo donde las distancias y las estructuras edilicias dificultan la instalación de las cableadas.

Pero estas bondades que acabamos de detallar también son requeridas en entornos de trabajo empresariales, donde se requiere que todos sus integrantes tengan acceso a los recursos que se encuentran en la red LAN cableada, por este último motivo es que este tipo de red no es la adecuada ya que no posee ningún mecanismo para poder unirse a una red LAN.

La solución a este problema se llama Access Point (Punto de Acceso), este es un dispositivo que básicamente se encarga de administrar las comunicaciones y permite a los puestos de trabajo el acceder a los recursos que residen en la red LAN cableada.

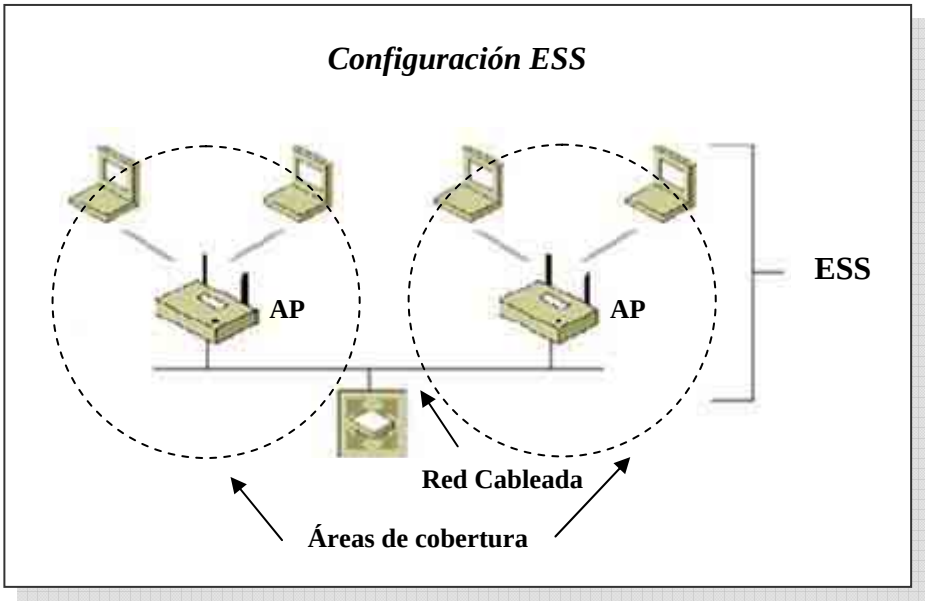
La configuración que utiliza este dispositivo la podemos ver en la próxima figura y se la denomina ***BSS*** (Basic Service Set – Conjunto de Configuración Básico) y también se la suele llamar ***Infrastructure*** (infraestructura).

Configuración BSS



2.3 ENLACES EES

Otra configuración menos conocida es la ***ESS*** (Extended Service Set – Conjunto de Servicios Extendidos), el objetivo básico de esta es prolongar el área de cobertura utilizando una estructura BSS ya existente a la cual se le agregan otros AP que se conectan a la misma red física.



De esta forma no sólo podemos expandirnos físicamente, sino también podemos dotar de movilidad a los usuarios del sistema que tengan necesidades especiales tales como ubicaciones semi permanentes.

Esta configuración también posee una característica poco difundida, que consiste en poder realizar una configuración capaz de aumentar el de ancho de banda disponible en una red con bajas prestaciones, o dicho de otra forma tratar de mantener el rendimiento ante el incremento en la cantidad de usuarios.

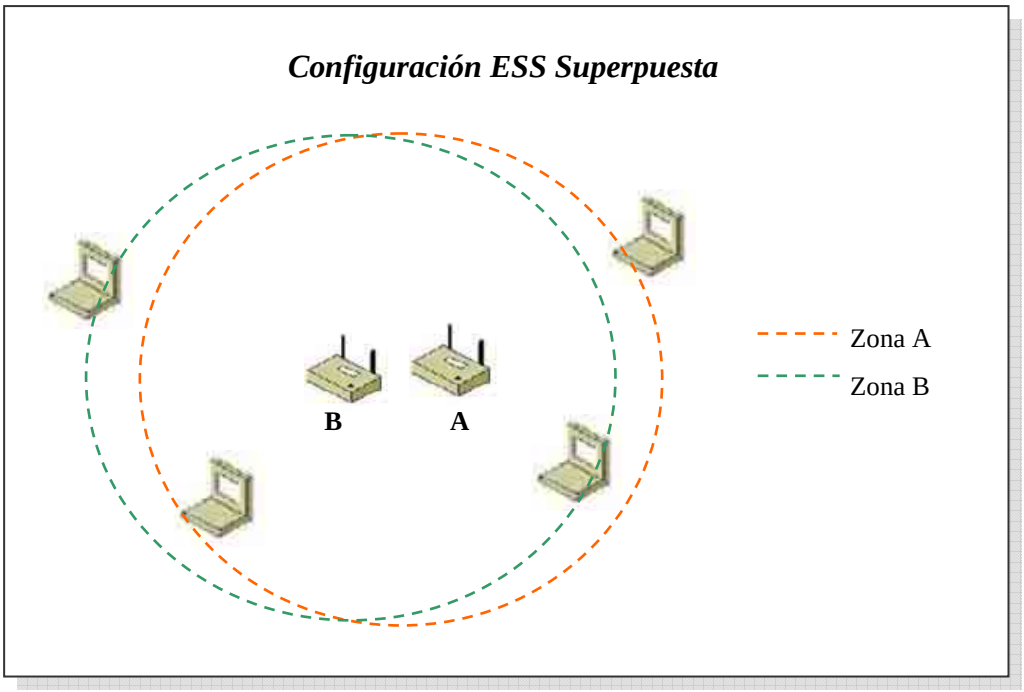
Esto se logra superponiendo las áreas de cobertura de por lo menos dos AP y se los hace transmitir en canales distintos que no se encuentren solapados (superposición de la frecuencia de transmisión y recepción).

Debido a que cada canal de transmisión es posible verlo como un vínculo de conexión independiente, es que podemos implementar una configuración como en el ejemplo, donde cada AP mantiene su propia zona y comparte un mismo espacio físico.

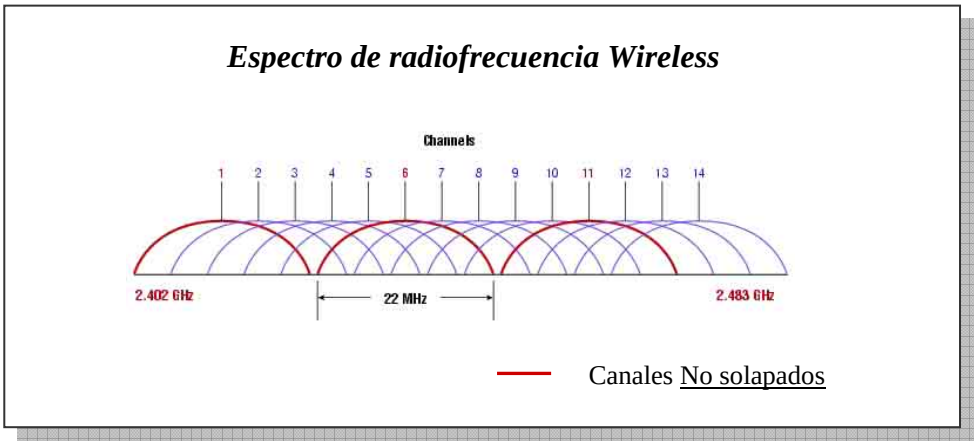
Estos AP controlarán las comunicaciones con sus respectivos clientes en la forma habitual y solo se diferencian por el número de canal que utilizan en la transmisión.

La cantidad máxima de AP que podemos colocar en una misma zona física es de tres unidades y está determinada por la cantidad de canales disponibles en la Argentina (de acuerdo a las regulaciones de la CNC), estos son 11, pero sólo los canales 1, 6 y 11 son los factibles de utilizar.

En la siguiente figura podemos ver una configuración ESS realizada con dos AP y sus correspondientes zonas (Ay B).



Respecto a los canales que se pueden utilizar o no, es que a continuación y con la ayuda de la figura que contiene el diagrama de distribución de frecuencias de wireless, es que trataremos de arrojar luz sobre este tema.



Como podemos ver los canales que están disponibles en esta tecnología son 14 en total, los mismos se encuentran dentro de un rango de frecuencias de uso libre conocidas como ISM, estas comienzan en la frecuencia de 2,402 GHz y terminan en los 2,483 GHz, esto significa que el rango de frecuencia total asignado a las es de 81 MHz. Estas regulaciones también especifican cuantas frecuencias (canales) y que rango tendrán cada una de ellas para realizar las transmisiones, algo similar a lo que ocurre con las frecuencias de la s radioemisoras de AM o FM.

El punto a tener en cuenta es que el rango asignado para estas frecuencias es de 22 MHz, con estos datos disponibles si multiplicamos los 22 MHz x 14 canales, obtendremos como resultado 308 MHz (el rango total que hace falta para poder contener los 14 canales).

Como podemos apreciar existe una diferencia entre los 81 MHz disponibles y los 308 necesarios para albergar os 14 canales en cuestión. La solución a este problema es superponer los canales para que puedan entrar en el rango disponible, tal como se puede ver en la figura anterior.

Si ahora analizamos este resultado funcionalmente podremos observar que tendríamos inconvenientes si en forma simultánea el canal 1 y el 2 quisieran transmitir, si observamos en la figura la posición de los canales, claramente podemos ver que transmiten casi en la misma frecuencia y esto no puede suceder.

Debido a esta forma de distribución de frecuencias es que a la hora de implementar una red Wireless, se tendrá que tener en cuenta que no existan otras redes vecinas operando en algún canal que pueda llegar a degradar el rendimiento de la nuestra. La metodología para seleccionar el canal para red es la siguiente:

- En el lugar de instalación, escanear mediante un software para tal fin, verificar si existen redes en las vecindades y de ser positiva la búsqueda tomar nota del canal en el cual está transmitiendo.
- Configurar la red Wireless utilizado un canal 5 posiciones hacia adelante o atrás, para evitar el solapamiento. Ejemplo: si detecto una red transmitiendo en el canal 5, no podemos seleccionar a un canal inferior ya que no tenemos la separación suficiente, pero sí podríamos seleccionar el canal 10 o superior (en nuestra legislación hasta el 11).

El software para analizar la presencia puede ser cualquiera que como información arroje el canal de transmisión, por ejemplo el NetStubler. Link http://www.netstumbler.com/downloads/

3 SEGURIDAD

En las redes cableadas existe una seguridad que es propio de estas, esto significa que alguien ajeno a la red que desee leer o tomar datos de la misma el primer paso que tiene que dar es lograr acceder físicamente a la misma. De acuerdo a lo planteado el intruso solo podrá tener acceso si es un integrante de la misma red.

En las redes wireless esto es sustancialmente distinto ya que la tecnología involucrada hace que cualquiera que este dentro del área de cobertura de esta red podrá escuchar toda la actividad de la misma, recordemos que las redes wireless funcionan en forma similar a una emisora de radio, y por lo tanto todos los que se encuentren en las vecindades están en condiciones de poder ingresar a la misma.

Con este panorama es que se implementan una serie de mecanismos orientados a disminuir el potencial acceso de usuarios desconocidos.

Siguiendo con el tema de seguridad debemos decir que el Service Pack 2 de Microsoft para Windows XP, incorpora nuevas características acorde a las nuevas medidas de seguridad y una configuración simplificada, por lo que recomendamos fuertemente su utilización. Las características sobresalientes son:

- Compatibilidad integrada con el nuevo sistema de seguridad WPA (Wi-Fi Protected Access - Acceso protegido de fidelidad inalámbrica).
- Asistente para la configuración de una red inalámbrica.
- Mejoramiento de la funcionalidad de reparación para conexiones inalámbricas.
- Nuevo cuadro de diálogo Conexión de red inalámbrica, el cual permite tener acceso a los nuevos asistentes, monitores de estado y configuraciones.

El ingreso a una red sin seguridad es extremadamente fácil, se accede desde el nuevo cuadro de dialogo de Conexión de red inalámbrica del Windows XP donde se puede iniciar una búsqueda de nuevas redes mediante la opción ***Actualizar lista de redes***, obteniendo como resultado el nombre de las mismas. El último paso sería conectarnos a la misma y comenzar a utilizarla.

Obviamente que se necesitaran mecanismos que impidan esto, para lograrlo existen una variedad de estrategias para evitar los ingresos no deseados a nuestra red y son los siguientes:

- Utilizar un nombre de identificación única de red que sea solo conocido por los integrantes de la red.
- Tener un sistema de control de acceso que autentifique quien desee ingresar a nuestra red.
- Proveer de confidencialidad al canal transmisión para impedir la lectura de la información transportada.

SSID

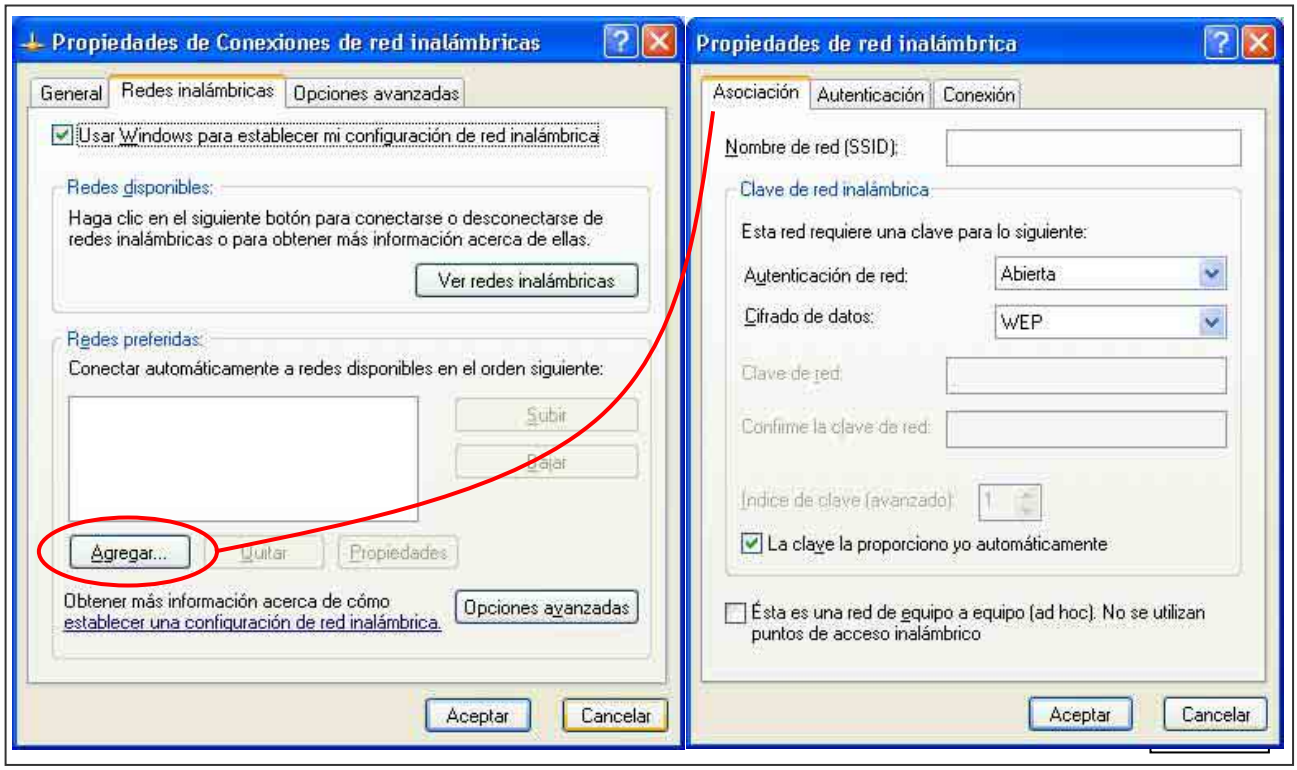
***S**ervice **S**et **Id**entifier* - Identificador de Conjunto de Servicio, es el nombre que identifica a la red, puede tener hasta 32 caracteres alfanuméricos incluyendo letras mayúsculas y es la primera barrera que se debe cruzar si se desea ingresar a una red wireless.

Al SSID también se lo conoce como identificador de área en una clara alusión a los grupos de máquinas formados por las configuraciones topológicas IBSS o BSS, esto significa que este será el nombre de la red.

El SSID es primer dato con que debemos contar cuando crea una red, este procedimiento puede ser iniciado desde una estación cuando se configure una red Ad-Hoc o desde el Access Point en caso de ser una red Infraestructura.

En las redes Ad-Hoc este identificador puede ser visto por cualquier equipo próximo a nuestra red, pero en el caso de tener un Access Point, este puede no mostrar su nombre y así ocultar su existencia.

El primer paso para configurar una red wireless luego de haber instalado la correspondiente placa de red con su correspondiente driver, será necesario seleccionar el nombre con que identificará la red y luego realizar el siguiente procedimiento:



Dentro de las Propiedades de Conexiones de red inalámbrica, seleccionamos la solapa Redes inalámbricas, dentro de este se encuentra una de las novedades del SP2, se de la opción trata de la opción Usar Windows para establecer mi configuración de red inalámbrica.

Si la tildamos desactiva la aplicación provista por el fabricante y permite a Windows realizar la configuración automática de los parámetros de la placa de red. y dentro de esta el espacio para ingresar el nombre del SSID.

Para crear nuestra red presionamos el botón el Agregar..., el cual nos derivará a la próxima pantalla en la solapa Asociación, donde podremos asignarle el nombre de nuestra red (SSID).

En el caso de que la red sea del tipo Ad Hoc, se tendrá que tildar la opción **"Esta es una red de equipo a equipo (ad hoc). No se utilizan puntos de acceso inalámbricos"**, esto significa que se deberán revisar los parámetros de configuración de la placa de red (canal de transmisión, velocidades de transmisión y recepción, etc.) y hacerlos coincidir con los de las máquinas restantes de la red.

3.1 AUTENTIFICACIÓN Y ASOCIACIÓN

Dentro de la solapa asociación se encuentran una serie de datos que son imprescindibles a la hora de implementar seguridad a una red, todas ellas están relacionadas entre si, por lo tanto las desarrollaremos una a una.

Anteriormente dijimos que necesitaríamos una red que tenga la capacidad de controlar el acceso a la red y que pueda verificar la identidad de quien lo intente, mediante una clave.

El tipo de seguridad que se implementa en la actualidad esta sujeta directamente a las tecnologías de la placa de red y estas son dos, WI-FI 802.11b (11Mbps) y 802.11g (54Mbps) que incorpora también a la 802.11i (implementación de seguridad).

El proceso de autentificación de red tiene una particularidad que debe quedar en claro, esta preparado para poder identificar placas de red que se encuentran en máquinas y no usuarios.

Si se utiliza tecnología 802.11b las opciones de configuración son dos:

- **Abierta**: no utiliza ninguna identificación.
- **Compartida**: utiliza una clave que debe ser la misma en todas las otras máquinas.

En caso de utilizar la tecnología 802.11i a las opciones anteriores se les agregan dos más, las cuales son de uso avanzado y serán tratadas con posterioridad.

- **WPA**
- **WPA – PSK**

Al seleccionar la opción Compartida, automáticamente queda disponible el espacio para asignar la clave de red y su confirmación. De esta forma todo aquel que quiera ingresar a la red le será solicitada previamente la clave de la red para poder ser autentificado.

La forma en la cual se completara la clave, la abordaremos en la próxima sección ya que se encuentran ambas sumamente relacionadas.

Una vez cumplimentada esta etapa le sigue el último paso que se llama asociación, este mecanismo es el encargado de proveer los medios necesarios para que dos estaciones o una máquina y un Access Point queden comunicados.

3.2 CIFRADO DE DATOS

El objetivo es proveer de confidencialidad al canal transmisión para impedir la lectura de la información transportada, esto se logra encriptando los mensajes que viajan entre las estaciones con una clave del tipo simétrica que se utiliza en ambas estaciones para decodificar la información en destino, el tipo de calve mas conocida es la WEP (Wired Equivalent Privacy – Privacidad Equivalente a la red Cableada).

WEP es utilizada por los sistemas con tecnología 802.11b y es el más difundido hasta el momento, sin embargo este es débil y puede ser vulnerado, como paliativo a este inconveniente hoy se puede encontrar al sistema WPA (Wi-Fi Protected Access – Acceso Protegido Wi-Fi) que gradualmente suplantara a WEP por ser más robusto.

Cuando se utiliza WEP en su versión original utiliza un código de 64 bits para realizar la encriptación, mientras que la segunda versión utiliza 128 bit. Sin embargo algunos fabricantes ofrecen hasta 256 bits para mejorar sus productos, en este punto debemos tener en cuenta que a raíz de esto solo los productos de este fabricante podrán comprender los datos encriptados y los otras marcas quedaran fuera del sistema, ya que esta modificación no es contemplada en WI FI.

Utilizando a WEP como ejemplo, de los 64 bits nombrados, en realidad solo se utilizan 40 para encriptar la información (datos), estos 40 bit provienen de la clave compartida que como vemos tiene un doble propósito (clave de autentificación y encriptación).

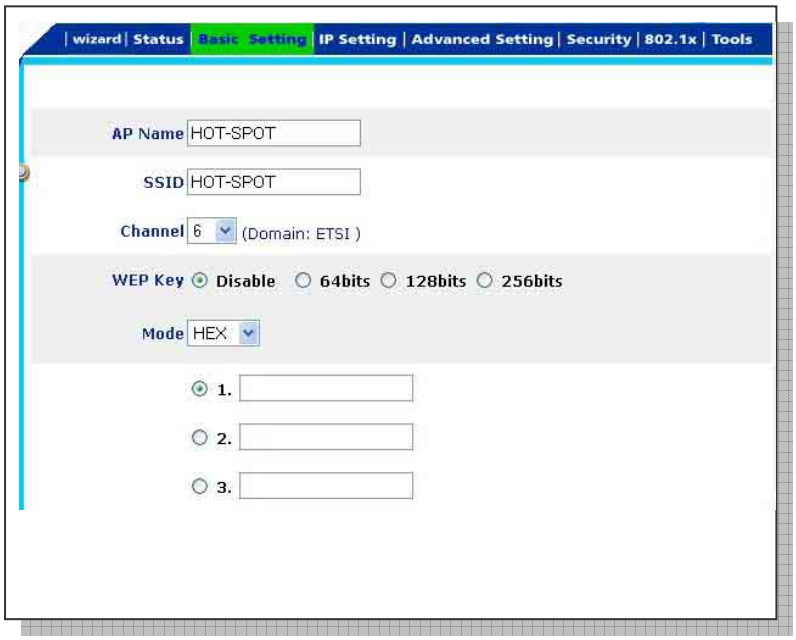
Los otros 24 bits restantes son utilizados para encriptar a los frames enviados con una clave distinta en cada envío, reforzando de esta forma la seguridad existente. Estos 24 bits son aportados por la placa de red y el usuario no tiene ingerencia alguna.

De esto se desprende que, en le caso de utilizar un sistema de 128 bit, solo se utilizaran 104 para la clave compartida.

Técnicamente esto significa que no podremos utilizar cualquier longitud de texto para la clave, y además debemos sumarle que se utilizan dos formas de escritura:

- Formato SCII (Caracteres alfanuméricos) en este sólo se pueden utilizar 5 caracteres en caso de de utilizar 40 bits para encriptar y 13 si utilizamos 104. Esto se debe a que un caracter utiliza 8 bits para ser representado en forma binaria. De no cumplirse estas condiciones la clave es rechazada
- Formato Hexadecimal (Letras desde la A hasta la F inclusive y números desde el 0 hasta el 9 inclusive) en este caso se emplean 10 caracteres si s utilizan claves de 40 bits y 26 caracteres en caso utilizar 128.

En el caso de querer implementar una red wireless con Access Point, el procedimiento es el mismo y solo se requiere de la información con la cual se denominará a la red (SIDD), la clave compartida y la cantidad de bits para la encriptación. En la próxima figura vemos la interfaz administrativa correspondiente a un Access Point, en el cual salvando algunas diferencias encontramos las mismas opciones para completar, tales como el SIDD, la cantidad de bits que se utilizaran para la encriptación WEP, el modo de clave Hexadecimal o ASCII y en este caso particular la posibilidad de tener mas de una clave disponible para utilizar.



3.3 SEGURIDAD AVANZADA

Luego del lanzamiento de wireless con la seguridad de tipo WEP, los usuarios corporativos entre ellos organismos gubernamentales (en EE.UU.) vieron las ventajas del sistema, pero surgieron debilidades con respecto a la seguridad.

El IEEE se dedicó inmediatamente a la solución de este problema la llamó IEEE 802.11i, la cual implementa una solución integral al problema de la seguridad.

Desgraciadamente los extensos tiempos de desarrollo, obligó a los fabricantes de esta tecnología que trataran de implementar soluciones propietarias tal como la utilización de 256 bits para la encriptación y tratar así de mejorar la imagen de sus productos. Esto provocó obviamente que sólo los productos de este fabricante se pudiesen comunicar, perdiendo así la compatibilidad con el resto.

WI FI conociendo la problemática, promovió una salida adelantada de productos con parte de estas soluciones con el apoyo de la IEEE y la llamo WPA (Wi-Fi Protected Access – Acceso Protegido Wi-Fi), en la actualidad también se la llama WPA1 debido a que no es la versión final y como imaginaran WPA2 es la versión final, al cual cumple con el estándar IEEE 802.11i.

Este tipo de seguridad ya se está implementada y se encuentra disponible desde octubre del año 2004 y depende de la aprobación de los productos respecto al estándar.

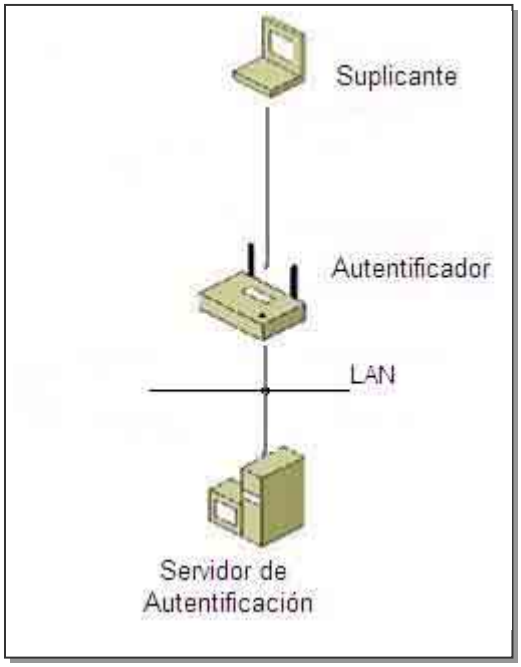
Una empresa que se adelanto a los acontecimientos fue Microsoft, implementando esta tecnología en su Service Pack2 para Windows XP, de esta forma estos sistemas operativos están en condiciones poder manejar la nueva seguridad avanzada.

3.3.1 WPA 1

Esta nueva propuesta de seguridad propone nuevos métodos para implementar seguridad, pero al mismo tiempo brindar momentáneamente soporte para la tecnología anterior.

La solución es radical y propone utilizar un mecanismo para poder autentificar en forma fehaciente la identidad de quien quiere unirse a la red, esto lo hace implementado una máquina servidor que tiene como misión almacenar las identidades de los integrantes de la red. También incorpora otra maquina que cumple la función de intermediaria entre el usuario y la base de datos en la cual se tendrá que validar, esta función es cumplida por una nueva generación de Access Point que tienen esta nueva capacidad.

En la siguiente figura podemos observar un diagrama básico de esta nueva estructura propuesta por WPA.



En la parte superior se encuentra la estación de trabajo en la red wireless, a la cual se la denomina Suplicante o Solicitante debido a que tiene que pedir la autorización para ingresar a la red.

En la parte inferior se encuentra el Servidor de Autentificación o servidor AAA (Authentication, Authorization and Accounting –Autentificación Autorización e Informes), cuya misión es administrar una base de datos que contiene a todos los integrantes de la red para, Autentificar la identidad, Autorizar el ingreso la red y llevar un Informe detallado de las actividades del usuario suplicante.

En el centro se encuentra el Access Point el cual cumple la misión de Autentificador, este actúa como intermediario o delegado entre el Servidor de autentificación y la estación suplicante. Esto significa que en ningún momento se realiza un contacto directo entre la estación de trabajo y la red LAN cableada, asegurándose que toda la información referida al proceso de autentificación sea realizado sobre un medio seguro como la red Lan y no a través de a red wireless.

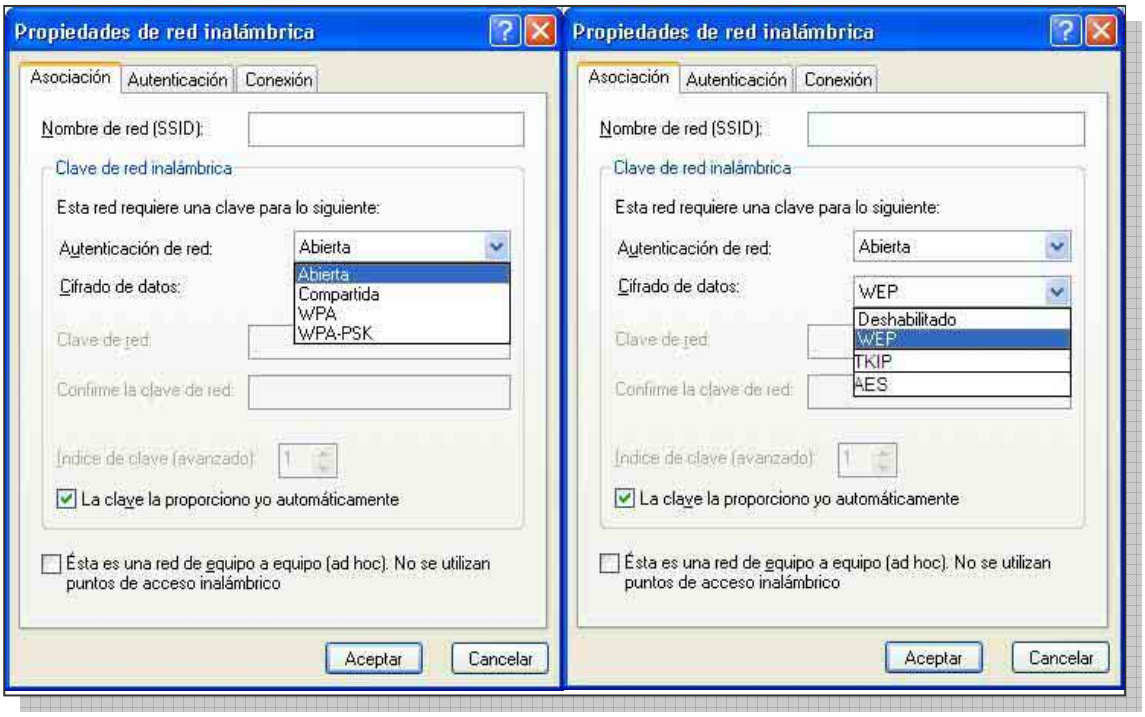
Los servicios de AAA son también se los conoce como RADIUS (Remote Authentication Dial-In User Service).

Esto no es la única novedad, también se mejoró la seguridad a nivel encriptación con la incorporación de de TKIP (Temporal Key Integrity Protocol – Protocolo de Clave de Integridad Temporal) esta sirve para asegurarse que todos frames sean encriptados distintos, ya que esto no era obligatorio en WEP. Respecto al cifrado de la información la novedad se llama EAS Advanced Encryption Standard – Clave de encriptación Avanzada, que utiliza 128 bits para el encriptado.

También se incorporó un nuevo sistema para detectar la integridad de los datos llamado MIC (Message Integrity Check – Verificador de Integridad de Mensaje) que reemplaza al utilizado anteriormente.

Finalmente el vector de inicialización también fue reformado llevando su extensión de 24 a 48 bits, dificultando así la posibilidad de desencriptar los datos transmitidos.

Todo esto visto desde una ventana de configuración de Windows es muy sencillo, ya que se reduce a seleccionar en primera instancia que tipo de autentificación se utilizará, tal como podemos observar en la próxima figura.



Algunas de las opciones disponibles ya son conocidas y las nuevas son WPA y WPA-PSK.

De la primera ya hablamos pero requiere de un servidor AAA, lo cual resultaría muy oneroso para implementar por usuarios SOHO o uno hogareño.

En este punto aparece la opción WPA-PSK (WPA - Pre Shared Key - WPA con Clave Pre Compartida), este es un mecanismo donde no se requiere de un AAA y se utiliza una única clave, la cual se utiliza por una sola vez y en cada progreso de asociación, garantizando así la confidencialidad de estas.

A la derecha de la figura se pueden ver las opciones de seguridad disponibles tales como TKIP, AES y WEP (utilizado por el IEEE802.11b) el cual todavía se encuentra disponible por cuestiones de compatibilidad, pero que a futuro desaparecerá.

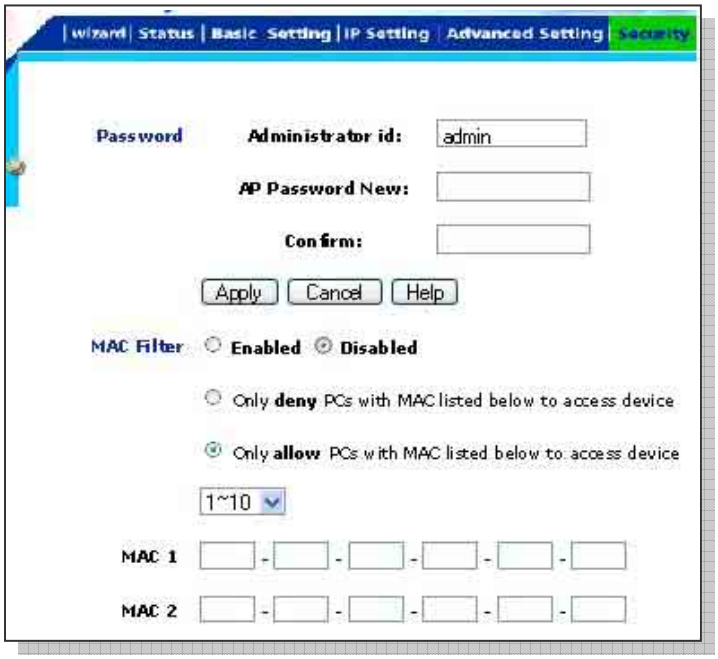
3.3.2 WPA2

WPA2 es versión final de la norma IEEE 802.11i, es igual a WPA1 pero incorpora a la seguridad AES antes descripta y toas las novedades de seguridad se implementarán en ambas configuraciones de red BSS y IBSS.

3.4 SEGURIDAD AVANZADA EN ACCESS POINT

Recordemos que esta opciones de autentificación y cifrado de datos también se encuentran disponibles en los Access Point, además de estas realizar estas tareas estos incorporan otros mecanismos de seguridad para reforzar los antes descriptos, estos se encuentran disponible solo a nivel local y dependen de cada fabricante su disponibilidad.

Entre los sistemas mas difundidos se encuentra el filtrado de acceso por direcciones MAC, esto significa que solo las estaciones de trabajo cuyas direcciones MAC se encuentren en la base de datos del Access Point podrán ingresar al mismo y se serán rechazados los intentos de conexiones cuya MAC no figuren en la lista.



Un ejemplo de esta propiedad la podemos ver en la próxima figura, en el caso particular de este fabricante se presenta un sencilla interfaz la cual nos ofrece la posibilidad de habilitar o deshabilitar esta función y el permitir o denegar el acceso a las direcciones MAC de la lista inferior.

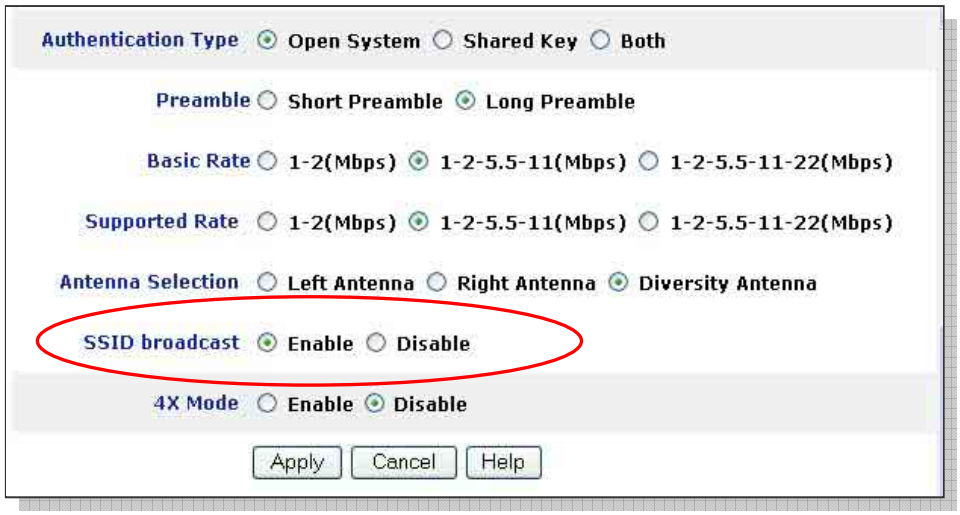
Para poder realizar esta tarea obviamente que será necesario el conocimiento de la direcciones MAC de los puestos , para ello se podrá recurrir a las propiedades de la placas de red wireless o en algunos casos dentro del mismo Access Point observando la lista de los dispositivos conectados en ese momento.

Otro método el cual también se encuentra dirigido a limitar el acceso, es algo menos difundido y consiste en dejar a nuestro Access Point no visible para las estaciones de trabajo en busca de nuevas redes disponibles.

Para esclarecer esto primero debemos decir que una estación de trabajo puede ver a un Access point gracias a que este emite un frame especial cada cierto tiempo para que pueda ser visto por todo aquel que se encuentre dentro su área de cobertura, para evitar que cualquiera en la vecindad pueda visualizarlo e intente accederlo es que se bloquea este frame espacial.

A esta funcionalidad la podes ver en la próxima figura y se la describe en ocasiones como permitir o denegara el ***SSID Broadcast***, al SSID ya lo conocemos es el nombre de la red o zona y Broadcast es la difusión de la misma.

Por lo tanto si escogemos no dejar visible a nuestro Access Point los usuarios deberán conocer los datos de la red (SSID), la clave compartida, la configuración de seguridad utilizada y que su dirección MAC este permitida para poder ingresara a la red.


Authentication Type Open System Shared Key Both
Preamble Short Preamble Long Preamble
Basic Rate 1-2(Mbps) 1-2-5.5-11(Mbps) 1-2-5.5-11-22(Mbps)
Supported Rate 1-2(Mbps) 1-2-5.5-11(Mbps) 1-2-5.5-11-22(Mbps)
Antenna Selection Left Antenna Right Antenna Diversity Antenna
SSID broadcast Enable Disable
4X Mode Enable Disable
Apply
Cancel
Help

NOTAS

CUESTIONARIO CAPITULO 15

1.- ¿Cual es el dispositivo que coordina las comunicaciones en una red BSS?

2.- ¿Cual es el mecanismo de autentificación utilizado por la norma IEE802.11?

3.- ¿Que método de seguridad recomendaría utilizar en grandes empresas?

4.- ¿Que tareas realizaría para limitar el ingreso de extraños a una red BSS?

5.- ¿Es posible mejorar el ancho de banda en redes Wireless? ¿Como?