UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA ELÉCTRICA Y ELECTRÓNICA

REDES INALÁMBRICAS – 802.11N E IMPLEMENTACIÓN TECNOLOGÍA MIMO

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JUAN FREDY ORTEGA ROJAS

PROMOCIÓN
2001-I

LIMA - PERU

2006

REDES INALÁMBRICAS – 802.11N E IMPLEMENTACIÓN TECNOLOGÍA MIMO

A mi madre, Alicia Rojas, por su abnegado sacrificio, por dejarme la mejor herencia de inmenso valor, mi educación.

"Dos cosas en el mundo no me abandonaran jamás, el ojo de Dios que me ve por todas partes y el corazón de mi madre que siempre me acompañara".

SUMARIO

En la actualidad se tiene para la transmisión de datos la tecnología inalámbrica con una opción adicional a las tecnologías ya existentes. La fabricación de equipos se desarrolla bajo los estándares de la IEEE 802.11b/a/g alcanzando velocidades de hasta 54Mbps.

Las topologías de red a implementarse combinan con los equipos en algunos casos con una red alambrica, encontrándose dos tipos de topología: "infraestructura" y "ad hoc".

A través del informe se desea mostrar la evolución de la tecnología inalámbrica bajo el estándar 802.11n que llevara a mejorar los servicios voz, video y datos. Además, mostrar un caso de éxito con implementación de equipos PRE-N.

La tecnología emergente se llama MIMO y tiene mejor rendimiento que las anteriores.
En el mercado se cuenta con equipos PRE-N que están bajo el estándar inicial del 802.11n pero las empresas han preferido desarrollar como una solución completa desde el nodo principal hasta el cliente.

La versión final del estándar 802.11n será aprobado en el año 2,006-2,007.

INDICE

PROLOGO

Hoy en día existe una necesidad de transmitir los datos a un tiempo mucho menor a través del medio inalámbrico y tenga mejorado la calidad de servicio, en ese contexto nace el estándar 802.11n.

Para el desarrollo de este informe se contó con algunos inconvenientes de información por ser un tema de innovación tecnológica reciente.

Los temas contenidos en el presente informe son:

Capitulo I, Introducción a las redes inalámbricas

En este capitulo se realiza una introducción al concepto de las Redes inalámbricas, determinando su modelo de capas, topología y su funcionamiento respectivo.

Capitulo II, Tecnología MIMO

Se brinda la información del rendimiento, funcionamiento, eficiencia y compatibilidad con los estándares inferiores de esta tecnología.

Capitulo III, Soluciones MIMO

Se presenta las soluciones comerciales existentes, ventajas y desventajas que actualmente ofrecen estos productos.

Capitulo IV, Sistema de Seguridad Actual

Como al inicio esta tecnología 802.11 adolecía de seguridad ahora se ha mejorado con el establecimiento WPA y con el cifrado respectivo 802.11i.

Capitulo V, Implementación con tecnología MIMO

Se establece un plan de trabajo de una implementación con tecnología MIMO.

CAPITULO I
INTRODUCCION A LAS REDES INALAMBRICAS

1.1 Introducción

Vamos a conocer un poco mas el funcionamiento de los sistemas y tecnologías de redes inalámbricas que usamos en el entorno domestico. Veremos como funciona esta tecnología, cual es su futuro, cuales son los sistemas de seguridad de que disponemos y también veremos como asegurar prácticamente nuestra red mediante el uso de los nuevos sistemas de encriptación. Esta información nos permitirá conocer como funciona una red inalámbrica, cuales son sus posibilidades y hacia donde se dirigen los próximos productos y tecnologías.

IEEE 802.11.

El protocolo 802.11, más conocido familiarmente como Wi-Fi[1], está comenzando a cautivar a todo el mundo. Miles de millones de dispositivos Wi-Fi se vendieron el 2,005 como se muestra en la figura 1.1. Eso incluye la mayoría de los ordenadores portátiles. La mayoría de los portátiles de hoy día cuentan con prestaciones 802.11.

El 802.11 es un grupo de trabajo del IEEE (Institute of Electrical and Electronics Engineers) dedicado a la estandarización de las tecnologías Wireless orientadas a "traducir" los estándares de redes locales al entorno inalámbrico ya sea mediante puntos de acceso o mediante la conexión entre dispositivos. Hasta ahora hemos disfrutado en el entorno domestico de tres revisiones de este estándar y se espera que para este año se hagan publicas las especificaciones del próximo estándar.

Hasta ahora hemos utilizado las revisiones A, B y G de esta tecnología y se supone

---

[1] Wi-Fi (802.11b) - Es el estándar para redes inalámbricas del Instituto de Ingenieros Eléctricos y Electrónicos de los EEUU (IEEE por sus siglas en inglés).

que la próxima revisión será la N. Con estas revisiones se han aumentado notablemente la velocidad de transmisión y también la seguridad pero donde no se ha hecho demasiado hincapié es en el alcance de estas redes en el entorno domestico.

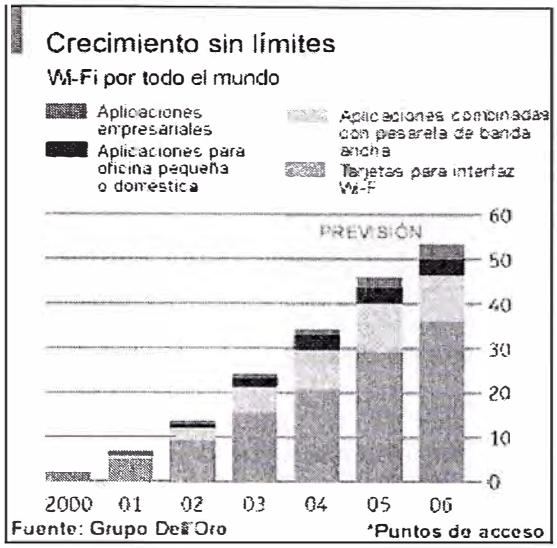

Figura 1.1: Crecimiento de Wi-Fi

Las velocidades han aumentado progresivamente desde las 2Mb del 802.11a, hasta las 54Mbps y modos extendidos, del 802.11g pasando por las 11Mbps del 802.11b. En un futuro, si la revisión sale adelante, las velocidades de transferencia y los alcances se duplicaran gracias a la tecnología y sobre todo a la metodología MIMO.

La IEEE ya se ha decidido por un estándar 802.11n. El 18 de marzo del 2,005, IEEE anunció que sólo se iba a trabajar con un único grupo de investigación, el defendido por TGn Sync. Este grupo de investigación recibió el apoyo del 75% de los votos del IEEE. Al ser elegido por mayoría, la propuesta debería acabar siendo el estándar del 802.11n que se aprobará entre el 2006 y 2007.

802.11n está diseñado para reemplazar las actuales 802.11a, 802.11b y 802.11g, con las que sería compatible, y que el TGn Sync asegura que puede llegar a alcanzar 315Mbits/s o incluso 630Mbits/s en algunos sistemas.

La pregunta es, que ocurrirá con los llamados productos pre-802.11n? que algunas empresas se apresuraron a sacar al mercado, como Airgo Networks, que el año pasado empezó a comprar algunos chips con esta tecnología para incluirlos en el F5D8xxx de Belkin, como por ejemplo un portátil, una tarjeta Wireless o un Router, y que estaban en el grupo WWiSE, que al final ha sido el ´perdedor´.

1.2 Modelo de capas de 802.11

1.2.1 La capa física de 802.11

La capa física la componen dos subcapas: PLCP (Physical Layer Convergence Protocol): Se encarga de codificación y modulación.

- Preámbulo (144 bits = 128 sincronismo + 16 inicio trama).
- HEC (Header Error Control): CRC 32
- Modulación (propagación) DSSS o FHSS o IR.
- PMD (Physical Medium Dependence): Es la que crea la interfaz y controla la comunicación hacia la capa MAC (a través del SAP: Service Access Point).

Este nivel lo conforman dos elementos principales:

- Radio: Recibe y genera la señal.
- Antena: Existe una gran variedad y no será tratado en este texto.

- FHSS (Frequency Hopping Spread Spectrum) para la banda de 2,4 GHz (ISM: Industrial, Scientific and Medical Band).
- DSSS (Direct Sequence Spread Spectrum para 2,4 GHz.
- IR (InfraRed).

Cuando se habla de transmisión, se deben diferenciar tres palabras:

- ***Modulación*:** Es el método de emplear una señal portadora y una moduladora (que da forma a la anterior). Cada una de ellas puede ser analógica o digital, con lo cual se obtienen cuatro posibles combinaciones de portadora y moduladora (AA – AD – DA y DD), con las cuales se conforman todas las técnicas de modulación. WiFi en la mayoría de los casos emplea la técnica QAM (Modulación de amplitud en cuadratura con más de un nivel de amplitud).
- ***Propagación*:** Es la forma en la cual "van saliendo" las señales al aire. Aquí es donde verdaderamente se aplican las técnicas de DSSS y FHSS. SS (Spread Spectrum) es la técnica de emplear muchas subportadoras de muy baja potencia con lo cual se "expande" el espectro útil. En cuanto a DS y FH, el ejemplo típico que se emplea para estas técnicas es la analogía con una terminal de trenes, en la cual existen varios andenes. Para DS, los trenes estarían saliendo, primero el andén 1, luego el 2, a continuación el 3, 4, 5... y así sucesivamente, respetando siempre este orden. Para FH, la salida de los trenes no respeta el orden y puede ser aleatoria o acorde a un patrón determinado (WiFi hace un muy buen uso de esto, pues en las subportadoras que recibe mucha interferencia no las usa o emplea menos cantidad de bits en las mismas).

- *Codificación*: Es la asociación de bit a cada "muestra" que se obtiene. WiFi en la mayoría de los casos emplea el código Barker.

1.2.2 La capa de enlace de 802.11

En el nivel de enlace, los dos subniveles que lo conforman (MAC: Medium Access Control y LLC: Logical Link Control). Desde el punto de vista de 802.11, solo interesa hacer referencia al subnivel MAC.

Capa MAC: Controla el flujo de paquetes entre 2 o más puntos de una red. Emplea CSMA/CA (Carrier Sense Multiple Access / Collision avoidance).

Sus funciones principales son:

- Exploración: Envío de Beacons que incluyen los SSID: Service Set identifiers ó también llamados ESSID (Extended SSID), máximo 32 caracteres.

- Autenticación: Proceso previo a la asociación.

Existen dos tipos:

- Autenticación de sistema abierto: Obligatoria en 802.11, se realiza cuando el cliente envía una solicitud de autenticación con su SSID a un AP, el cual autorizará o no. Este método aunque es totalmente inseguro, no puede ser dejado de lado, pues uno de los puntos más fuertes de WiFi es la posibilidad de conectarse desde sitios públicos anónimamente (Terminales, hoteles, aeropuertos, etc.).
- Autenticación de clave compartida: Es el fundamento del protocolo WEP (hoy totalmente desacreditado), se trata de un envío de interrogatorio (desafío) por parte del AP al cliente.

Asociación: Este proceso, es el que le dará acceso a la red y solo puede ser llevado a cabo una vez autenticado.

Seguridad: Mediante WEP, con este protocolo se cifran los datos pero no los encabezados.

RTS/CTS: Funciona igual que en el puerto serie (RS-232), el aspecto más importante es cuando existen "nodos ocultos", pues a diferencia de Ethernet, en esta topología si pueden existir nodos que no se escuchen entre sí y que solo lleguen hasta el AP, (Ejemplo: su potencia está limitada, posee un obstáculo entre ellos, etc), en estos casos

se puede configurar el empleo de RTS/CTS. Otro empleo importante es para designar el tamaño máximo de trama (en 802.11 Es: mínimo=256 y máximo=2312 Bytes).
- Modo ahorro de energía: Cuando esta activado este modo, el cliente envió previamente al AP una trama indicando "que se irá a dormir", El AP, coloca en su buffer estos datos. Se debe tener en cuenta que por defecto este modo suele estar inactivo (lo que se denomina Constant Awake Mode: CAM).
- Fragmentación: Es la capacidad que tiene un AP de dividir la información en tramas más pequeñas.

1.3 Velocidad vs. Modulación

Cuando transmitimos información entre dos dispositivos inalámbricos, la información viaja entre ellos en forma de tramas. Estas tramas son básicamente secuencias de bits. Las secuencias de bits están divididas en dos zonas diferenciadas, la primera es la cabecera y la segunda los datos que verdaderamente se quieren transmitir.

La cabecera es necesaria por razones de gestión de los datos que se envían. Dependiendo de la forma en la que se module la cabecera (o preámbulo), podemos encontrarnos con diferentes tipos de tramas, como son:

- **Barker**. (RTS / CTS)

- **CCK**. Complementary Code Keying

- **PBCC**. Packet Binary Convolutional Coding

- **OFDM**. Orthogonal Frequency-Division Multiplexing

Una representación gráfica de las tramas más importantes:

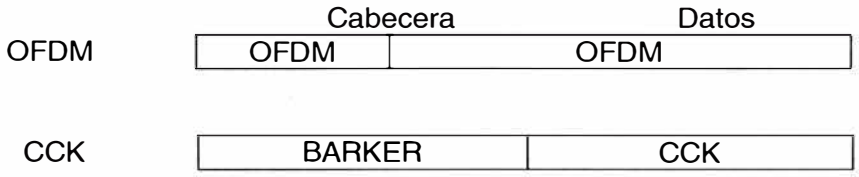

Figura 1.2 Tipos de tramas

Como podemos ver la cabecera en el caso de la codificación **OFDM** es más pequeña. A menor tamaño de cabecera menor "overhead" en la transmisión, es decir, menor tráfico de bits de gestión luego mayor "sitio" para mandar bits de datos. Lo que repercutirá positivamente en el rendimiento de la red.

Ya a primera vista podemos ver que el estándar **802.11g** es una unión de los estándares **802.11** "**a**" y "**b**". Contiene todos y cada uno de los tipos de modulación que éstos usan, con la salvedad de que "a" opera en la banda de los 5 Ghz, mientras que los otros dos operan en la de los 2.4 Ghz.

		802.11a		802.11b		802.11g	
Velocidad Nominal	Portadora	Obligatorio	Opcional	Obligatorio	Opcional	Obligatorio	Opcional
1	única			BARKER		BARKER	
2	única			BARKER		BARKER	
5.5	única			CCK	PBCC	CCK	PBCC
6	múltiple	OFDM				OFDM	CCK,OFDM
9	múltiple		OFDM				OFDM
11	única			CCK	PBCC	CCK	
12	múltiple	OFDM				OFDM	
18	múltiple		OFDM				
22	única						
24	múltiple	OFDM				OFDM	
36	múltiple		OFDM				
48	múltiple		OFDM				
54	múltiple		OFDM				CCK,OFDM

Figura 1.3 Velocidad de algunos estándares 802.11x

Cuando tenemos una red inalámbrica en la que todos los dispositivos son tipo "a" o todos de tipo "b" no hay problemas en las comunicaciones. Cada AP tipo "a" tendrá sólo TRs tipo "a" y los APs tipo "b" tendrán sólo TRs tipo "b". Se seleccionará la mejor modulación y se transmitirá. Si la comunicación óptima no es posible debido a una excesiva distancia entre los dispositivos o por diferentes tipos de interferencias se va disminuyendo la velocidad hasta que se encuentre la primera en la que la comunicación es posible.

En el caso de dispositivos AP 802.11g normalmente estaremos usando la modulación OFDM, modulación que es la óptima para este estándar.

Si por un casual un dispositivo 802.11b quisiera hablar con otro dispositivo 802.11g, este último debería aplicar una modulación compatible con el estándar "b", cosa que es capaz de hacer. Sin embargo el dispositivo "b" no puede escuchar las transmisiones de los otros dispositivos "g" que hablan con su "partner" pues éstos usan una modulación que él no es capaz de entender. Si un dispositivo "b" comenzase a hablar a la vez que un dispositivo "g" se producirían colisiones que impedirían la transmisión, no por que

interfieran, ya que usan diferente modulación, sino porque el AP normalmente sólo será capaz de hablar con un dispositivo a la vez.

Para evitar las colisiones, los equipos "b" usan la modulación **Barker** con **TRS/CTS** (Request To Send / Clear To Send), que básicamente significa que deben pedir permiso al AP para transmitir.

1.4 Topologías de redes LAN Inalámbricas

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 documento se utilizarán los términos "infraestructura" y "ad hoc". Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

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.

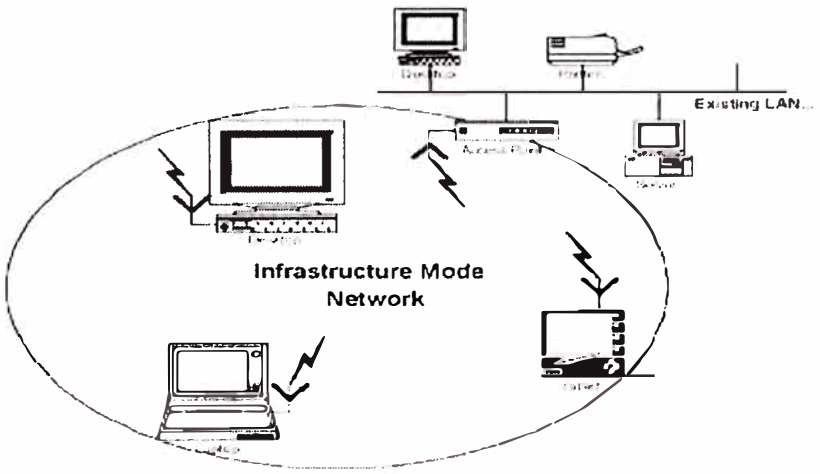

Figura 1.4. Red de la modalidad de infraestructura

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.

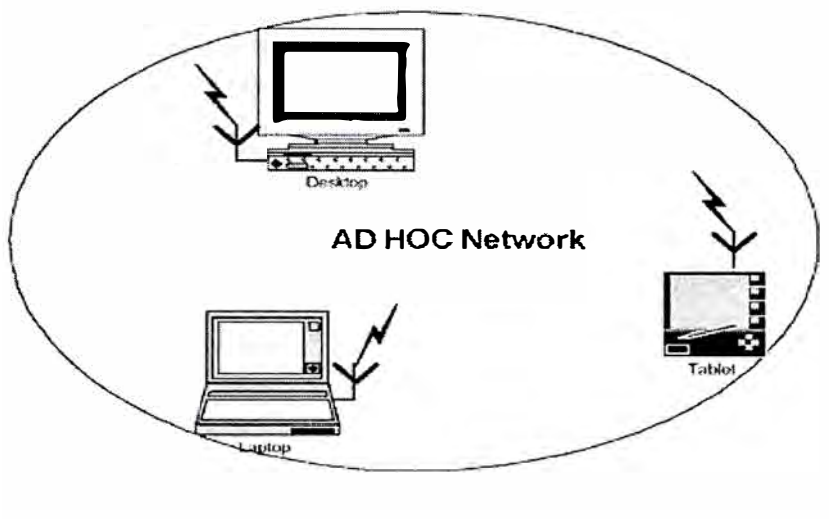

Figura 1.5. Red Ad Hoc

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 de componentes de las mismas:

- BSS (Basic Service Set): Es el bloque básico de construcción de una LAN 802.11. En el caso de tratarse de únicamente 2 estaciones ser denomina IBSS (Independent BSS), es lo que a menudo se denomina “Ad Hoc Network”.
- DS (Distribution System): Es la arquitectura que se propone para interconectar distintos BSS. El AP es el encargado de proveer acceso al DS, todos los datos que se mueven entre BSS y DS se hacen a través de estos AP, como los mismos son también STA, son por lo tanto entidades direccionales.
- ESS (Extended Service Set): Tanto BSS como DS permiten crear wireless network de tamaño arbitrario, este tipo de redes se denominan redes ESS.

1.5 Descripción general del funcionamiento

1.5.1 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 da una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. Observe que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar, antes de transmitir un paquete mediante un intercambio de tramas

"petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

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

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

1.5.2 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.

Cuando un medio de red nuevo se introduce en un nuevo entorno siempre surgen nuevos retos. Esto es cierto también en el caso de las redes LAN inalámbricas. Algunos retos surgen de las diferencias entre las redes LAN con cable y las redes LAN inalámbricas. Por ejemplo, existe una medida de seguridad inherente en las redes con cable, ya que la red de cables contiene los datos. Las redes inalámbricas presentan nuevos desafíos, debido a que los datos viajan por el aire, por ondas de radio.

Otros retos se deben a las posibilidades únicas de las redes inalámbricas. Con la libertad de movimiento que se obtiene al eliminar las ataduras (cables), los usuarios pueden desplazarse de sala en sala, de edificio en edificio, de ciudad en ciudad, etc., con las expectativas de una conectividad ininterrumpida en todo momento.

Las redes siempre han tenido retos, pero éstos aumentan cuando se agrega complejidad, tal como sucede con las redes inalámbricas. Por ejemplo, a medida que la configuración de red continúa simplificándose, las redes inalámbricas incorporan características (en ocasiones para resolver otros retos) y métrica que se agrega a los parámetros de configuración.

1.6 Resumen

La excitante tecnología para redes LAN inalámbricas está naciendo como solución para implementaciones empresariales, públicas y domésticas. Para admitir estas implementaciones, se deben satisfacer varios desafíos.

Las redes inalámbricas se adaptan en redes alambricas, es el modo "infraestructura" además en el modo "Ad Hoc" permite una transmisión sin Access Point para distancias muy cortas.

En la actualidad se cuenta con estándares de la 802.11b/g y el 802.11a donde su operación de trabajo es en 2.4GHz y 5GHz respectivamente. La demanda de uso en Perú es el 802.11b/g por la compatibilidad existente entre ambos estándares.

La IEEE ha designado a la TGn Sync para concluir la investigación y aprobar el estándar 802.11.

CAPITULO II

TECNOLOGIA MIMO (MULTIPLE INPUT, MULTIPLE OUTPUT)

2.1 Introducción

Este sistema, que ya se puede disfrutar en productos ya comercializados, usa un sistema inteligente de antenas para aumentar notablemente el alcance del sistema inalámbrico y para mantener unas tasas de velocidad, aunque no muy superiores, si mucho más estabilizadas. Para máximizar el alcance se establece un nuevo sistema de antenas, normalmente caracterizado por tres antenas. Lo que ocurre actualmente en un entorno cerrado como un domicilio de una o más plantas es que la señal se ve repetida por muebles metálicos, electrodomésticos, los propios compuestos de la fabricación, etc. Esto se traduce en que la señal se ve interferida por sus propios rebotes en estos elementos y por otras fuentes de interferencias que usan rangos de frecuencia similares como teléfonos inalámbricos, microondas, monitores para bebes y como no, las redes inalámbricas de nuestros vecinos. Todo esto reduce notablemente la capacidad y el alcance de la red inalámbrica.

El sistema de múltiples antenas del MIMO permite que cada antena ajuste de forma dinámica la recepción y la emisión de datos maximizando el alcance del mismo sobretodo en entornos muy cargados. Además de aumentar el alcance de la red y evitar interferencias el MIMO también permite menos perdida de velocidad a largas distancias. Existen ya múltiples productos MIMO en el mercado, antes de que salga la estandarización, por lo que son sistemas "propietarios" que normalmente necesitan de aparatos compatibles tanto en los puntos de acceso como en las tarjetas de cada aparato. Cuando este sistema se estandarice, cualquier producto 802.11n podrá aprovechar cualquier punto de acceso compatible, no habrá diferenciación entre marcas, no por lo menos, hasta que cada fabricante lance soluciones personalizadas como es ahora el MIMO.

Figura 2.1: Aumento de la capacidad de proceso con sistemas de antena múltiple

Un enfoque de Intel consiste en investigar para incrementar la velocidad de transferencia física de los sistemas inalámbricos 802.11 que utilizan múltiples sistemas de antena tanto para el transmisor como para el receptor. Esta tecnología se conoce como MIMO (entrada múltiple salida múltiple) o sistemas de antena inteligentes. MIMO explota el uso de señales múltiples transmitidas hacia las señales múltiples y medias inalámbricas recibidas desde el medio inalámbrico para mejorar el rendimiento inalámbrico. Al usar varias antenas, MIMO utiliza el espectro de forma más eficaz sin sacrificar la fiabilidad.

Intel espera que la tecnología MIMO desarrolle un papel importante al lograr los objetivos del grupo de trabajo de 802.11n. MIMO utiliza múltiples y diversas antenas afinadas con el mismo canal de distribución, cada una transmitiendo con diferentes características espaciales. Cada receptor escucha las señales de cada transmisor, habilitando varias rutas en las que las reflexiones de ruta múltiple (normalmente interrupciones con la recuperación de la señal) pueden volver a combinarse para mejorar las señales deseadas.

802.11	La WLAN estándar original. Soporta desde 1 Mbps hasta 2 Mbps.
802.11ª	Estándar WLAN de alta velocidad para la banda de 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2,4 GHz. Soporta hasta 11 Mbps.
802.11d	Itinerancia internacional: configura dispositivos

	automáticamente para que cumplan con las regulaciones RT locales
***802.11e**	Dirige la calidad de los requisitos de servicios para todas las interfaces de radio de WLAN IEEE.
802.11f	Define comunicaciones del punto de acceso interno para facilitar redes WLAN múltiples distribuidas por proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de 2,4 GHz. Soporta velocidades de hasta 54 Mbps.
802.11h	Define la gestión del espectro de la banda de 5 GHz.
***802.11i**	Dirige las flaquezas de la seguridad actual tanto para los protocolos de codificación como de autenticación. El estándar abarca los protocolos 802.1X, TKIP y AES.
802.11n	Proporciona mejoras de mayor capacidad de proceso. Se pretende que proporcione velocidades de hasta 500 Mbps.

Figura 2.2: **Gráfico de estándares de la WLAN**

***802.11e, 802.11i ver anexo.**

2.2 MIMO

MIMO explota multitrayectos, tradicionalmente obstáculos en comunicaciones inalámbricas para realzar la señal en lugar de degradarla. Los sistemas de MIMO consisten en transmisores y receptores múltiples. Para que los sistemas de MIMO sean los más eficientes, se necesita crear un ambiente multidireccional rico en dispersión es necesario para crear canales de propagación independiente. Es la dispersión más abundante en el canal de propagación, que ofrece a múltiples subcanales paralelos en la misma frecuencia, por lo tanto dando mayor capacidad por la misma banda ancha.

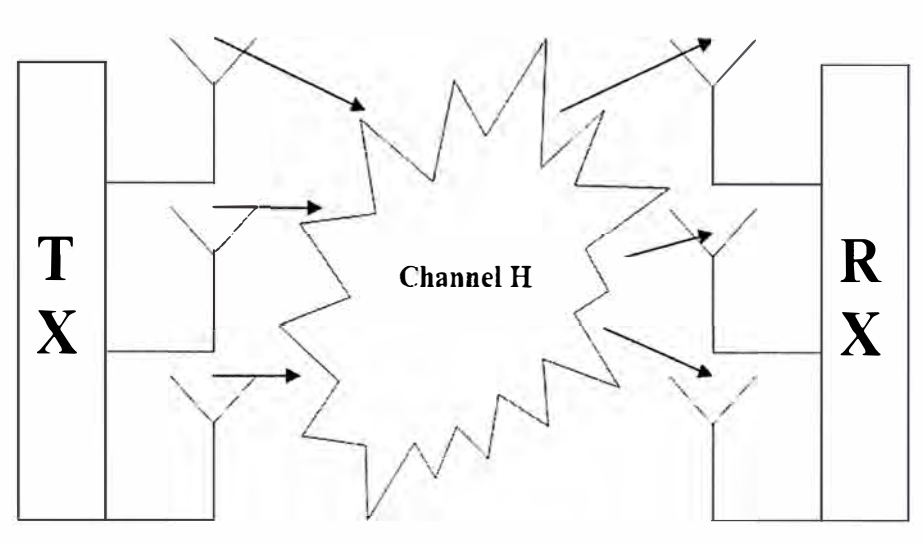

Figura 2.3: Sistema MIMO de tres elementos

En la Figura 2.3 muestra un de sistema transmisión MIMO que consiste en tres antenas de transmisión y tres antenas de recepción. El canal H se presume como un ambiente abundante en dispersión. MIMO utiliza una multi antena de diversidad espacial en ambas puntas finales del acoplamiento, tratando la multiplicidad de las diversas trayectorias de la dispersión como subcanales paralelos separados.

2.2.1 MIMO Transmisión

La Figura 2.4 demuestra cómo los datos se transmiten en un sistema MIMO. Considere la secuencia de datos del bite 6 que se muestra arriba, esta secuencia de datos se analiza (desmultiplexada) en secuencias de datos iguales de proporción N, donde N es el número de antenas que transmiten, que es tres en este caso.

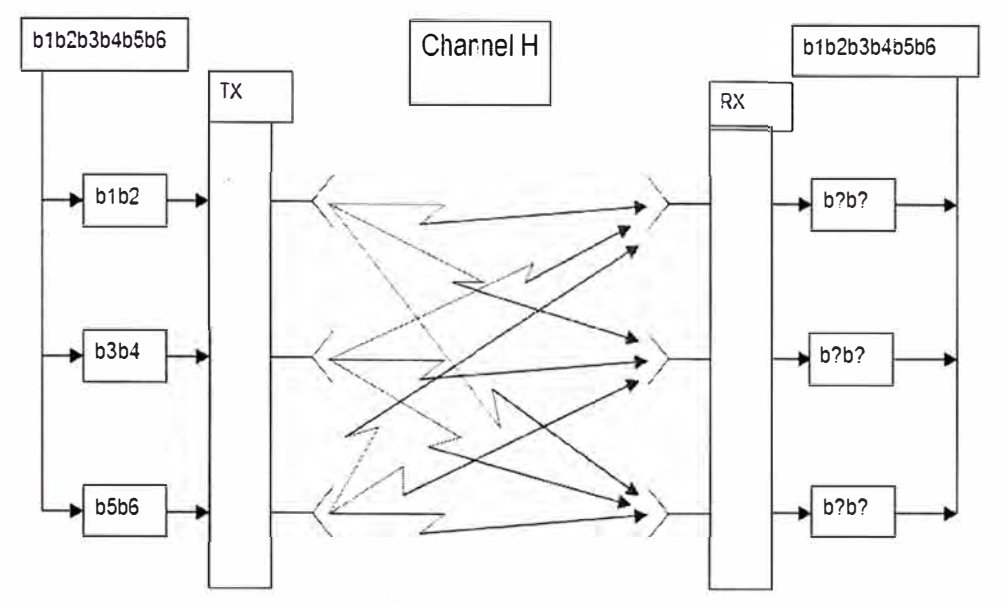

Figure 2.4: Transmisión de información en sistemas MIMO

Cada una de los índices más bajos de las subsecuencias se transmite a partir de una de las antenas. Todos se transmiten en el mismo tiempo y en la misma frecuencia, por lo tanto se mezclan juntos en el canal. Puesto que todas las corrientes secundarias se están transmitiendo en la misma frecuencia, es muy espectralmente eficiente.

Cada una de las antenas de la recepción toma todas las señales transmitidas sobrepuestas sobre una otra. Si el canal H es un ambiente suficientemente rico en dispersión, cada una de las señales sobrepuestas habrá propagado trayectorias levemente diversas del excedente y por lo tanto tendrá firmas espaciales diferenciales. Las firmas espaciales existen debido a la diversidad espacial en ambos extremos del acoplamiento, y por lo tanto crean los canales independientes de la propagación. Cada par de antenas de transmisión - recepción se puede tratar como sub-canales paralelos (es decir un canal Single-Output Single-Input (SISO)), éste llegará a estar más claro cuando abordemos el análisis del canal H. Puesto que los datos se están transmitiendo en canales paralelos, un canal para cada par de la antena, la capacidad de canal aumenta en proporción con el número de pares de transmisión - recepción.

2.2.2 Canal H del MIMO

Desde que cada antena de recepción detecta todas las señales transmitidas, hay trayectos de propagación independiente NxN, donde hay N antenas de transmisión y recepción. Esto permite que el canal se represente como una matriz NxN.

Nuevamente usando un sistema como ejemplo, se obtiene la matriz siguiente:

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_{11} & \mathbf{h}_{12} & \mathbf{h}_{13} \\ \mathbf{h}_{21} & \mathbf{h}_{22} & \mathbf{h}_{23} \\ \mathbf{h}_{31} & \mathbf{h}_{32} & \mathbf{h}_{33} \end{bmatrix}$$

Cada uno de los elementos en la matriz del canal es una trayectoria de propagación independiente. Refiriéndose de nuevo al cuadro 2.4 las trayectorias que se pueden ver, representan la trayectoria de la antena de transmisión ii, a la a la antena de recepción. La señal transmitida se puede representar como vector, al igual que la señal recibida. Por lo tanto, el sistema se puede representar como la ecuación siguiente.

$$r = Hs + n$$

Donde r = Vector de señal recibida, H= Matriz del canal, s= Vector de señal transmitida, n= Ruido.

Las señales transmitidas en el *"Vector r"* son señales complejas, al igual que los valores de la matriz del canal y las señales recibidas en el *"Vector s"*. La forma compleja en cada uno de los elementos en los vectores representa la energía de la señal y su fase de retardo. La forma compleja de los elementos de la matriz del canal 'H' representa la atenuación y la fase retardada asociada con esa trayectoria de propagación. El paso siguiente es ver cómo se puede descifrar la señal recibida.

2.3 Rendimiento más alto de las redes inalámbricas

En respuesta a la demanda del mercado creciente para redes de áreas locales inalámbricas (WLAN) de alto rendimiento, el Instituto de electrónica e ingenieros electrónicos - Asociación de estándares (IEEE-SA) ha aprobado la creación del Grupo de enfoque N (802.11 TGn) del IEEE 802.11 durante el segundo semestre del 2,003. El alcance del objetivo del TGn consiste en definir modificaciones para la Capa física y la Capa de control del acceso medio (PHY/MAC) que generan resultados de un mínimo de 100Mbps en el MAC SAP (encima del MAC, consulte la Tabla 2.1 a continuación).

Los resultados mínimos requeridos representan un incremento 4 veces superior, aproximadamente, en el rendimiento de WLAN en comparación con las redes 802.11a/g actuales. El propósito de TGn para este próximo paso en el rendimiento de WLAN consiste en mejorar la experiencia del usuario con las aplicaciones WLAN existentes a tiempo de habilitar aplicaciones nuevas y segmentos del mercado recientes. Al mismo tiempo, TGN espera una transición lúcida para su adopción al requerir compatibilidad retroactiva con las soluciones IEEE WLAN legadas existentes (802.11a/b/g).

Wireless LAN Throughput by IEEE Standard

Tabla 3.1: Comparación de diferentes 802.11 tasas de transferencia

IEEE WLAN Standard	**Over-the-Air (OTA) Estimates**	**Media Access Control Layer, Service Access Point (MAC SAP) Estimates**
802.11b	11Mbps	5Mbps
802.11g	54Mbps	25 Mbps (when .11b is not present)
802.11a	54Mbps	25Mbps
802.11n	**200+Mbps**	**100Mbps**

La Wi-Fi* Alliance (Alianza de Wi-Fi) también ha demostrado interés en el trabajo del TGn a favor del 802.11n. Los representantes de la industria se han congregado bajo la Alianza de Wi-Fi: Grupo de enfoque en comercialización de alto desempeño, a fin de definir y publicar un Documento de requisitos para la comercialización (MRD). El Wi-Fi Alliance MRD especifica las expectativas de rendimiento que mejorarán la experiencia del usuario final con respecto a resultados anteriores, rango aumentado, control de interferencias más robustas y una experiencia del usuario más fiable en todo el Conjunto de servicios básicos (BSS).

Intel está contribuyendo al éxito del 802.11n de distintas maneras. Primero, Intel participó en el comité de TGn responsable de desarrollar los documentos principales que se utilizarán para guiar el TGn en el desarrollo del estándar para 802.11n y ha presentado

contribuciones a estos documentos fundamentales, incluidos los modelos para canales, los modelos de uso, los requisitos de funcionalidad y el criterio de comparación.

Intel también ha tomado la iniciativa de enviar propuestas técnicas para TGn en las tecnologías MAC y PHY, metodologías de medida del rendimiento y metodologías de simulación. Intel ha ayudado a coproducir el MRD de la Alianza Wi-Fl para redes WLAN de alto rendimiento y continúa liderando a la industria al llevar a cabo conversaciones regulares con los líderes en la industria de WLAN. A consecuencia de todos estos esfuerzos, Intel y otros líderes de la industria desarrollarán conjuntamente y enviarán una propuesta completa sobre IEEE TGn para la estandarización de IEEE 802.11n. Intel considera que con solamente demostrar 100Mbps bajo ciertas condiciones no será suficiente para asegurar una experiencia de usuario robusta con las aplicaciones que están emergiendo. La visión de Intel para el estándar de IEEE 802.11n logrará y aún sobrepasará la meta deseada para IEEE TGn de 100Mbps en la MAC SAP. Intel espera que la tecnología WLAN para 802.11n admitirá computación personal y plataformas de comunicaciones de bolsillo para todos los entornos principales corporativos, domésticos y los lugares públicos con conexión de red.

El alcance amplio de esta visión promueve implementaciones prácticas y rentables que escalarán robustamente desde los dispositivos de bajos requisitos hasta las aplicaciones de alto rendimiento usando métodos técnicos que pueden ser desarrollados e implementados dentro de las fechas límites especificadas en el IEEE TGn.

Intel cree que el 802.11n debería emplear una filosofía evolucionaría al volver a utilizar las tecnologías existentes, cuando sea práctico, a tiempo de introducir nuevas tecnología donde proporcionan mejoras en el rendimiento efectivo a fin de satisfacer las necesidades de las aplicaciones en evolución. La reutilización de tecnologías legadas tales como Multiplexado por división de frecuencia ortogonal (OFDM), cifrado de la Corrección de errores de reenvío (FEC), asignación de intercalado y Modulación de amplitud de 'Quadratura' (QAM), deben mantenerse para mantener los costos bajos y facilitar la compatibilidad retroactiva.

Los paquetes de la Unidad de datos del protocolo PHY (PPDU) deben ser decodifícales sin previo conocimiento del método de transmisión. Los dispositivos legados deben tener la capacidad de decodificar parcialmente y evitar transmisiones por los nuevos paquetes de alto rendimiento. Aún si dichos paquetes no son descifrados completamente por los dispositivos legados. Al mismo tiempo, la interoperabilidad (dispositivos legados que

funcionan en una red 802.11n de alto rendimiento) de legado sin problemas (802.11a/g) debe ser admitida sin penalidades de rendimiento poco razonables para el funcionamiento de alto rendimiento.

Existen tres áreas clave que necesitan ser consideradas cuando se resuelven los incrementos en el rendimiento de una LAN inalámbrica. Primero, mejoras en la tecnología de radio serán necesarias para incrementar la velocidad de transferencia física. Segundo, deben desarrollarse mecanismos nuevos que implementen la administración efectiva de los modos de rendimiento PHY mejorados. Tercero, se necesitan mejoras en la eficiencia de la transferencia de datos a fin de reducir el impacto en el rendimiento de los encabezados de PHY y las demoras de ciclado en la serial de radio que, caso contrario, reducen las mejoras logradas con incrementos en la velocidad de transferencia física.

Al mismo tiempo, para desarrollar métodos nuevos para lograr mejoras en el rendimiento, se necesita la coexistencia con los dispositivos legados de 802.11a/b/g existentes. Todas estas áreas deben tenerse en cuenta al considerar las implementaciones prácticas y efectivas para los segmentos del mercado sensibles a costos.

2.4 Incremento en la Tasa de Transferencia física

Un método para incrementar la velocidad de transferencia física de los sistemas inalámbricos utiliza varios sistemas de antenas tanto para el transmisor como el receptor. Esta tecnología se conoce como Multiple-Input Multiple-Output (MIMO) (entrada múltiple, salida múltiple), o sistemas de antenas inteligentes. MIMO aprovecha al máximo el uso de varias señales transmitidas en el medio inalámbrico y varias señales recibidas del medio inalámbrico a fin de mejorar el rendimiento inalámbrico.

MIMO puede proporcionar muchos beneficios, todos ellos derivados de la habilidad de procesar diferentes señales espaciales simultáneamente. Dos beneficios importantes considerados aquí son la diversidad de antenas y multiplexado espacial. Usando varias antenas, la tecnología MIMO ofrece la habilidad de resolver información coherentemente desde varias rutas de señales mediante antenas receptoras separadas espacialmente. Las señales de multiruta son las señales reflejadas que llegan al receptor en cualquier momento después de la señal original o de la línea de vista (LOS) que ha sido recibida. Generalmente, la multiruta es considerada como una interferencia que reduce la habilidad del receptor para recuperar la información inteligente. MIMO posibilita la oportunidad de

resolver espacialmente las señales multirutas, al proporcionar ganancias de diversidad que contribuyen a la habilidad de un receptor para recuperar la información inteligente.

Otra oportunidad valiosa que puede proporcionar la tecnología MIMO es el Multiplexado de división espacial (SDM). El SDM crea una división espacial multiplexada en varios flujos de datos independiente, transferidos simultáneamente dentro de un canal espectral del ancho de banda. El MIMO SDM puede incrementar notablemente el rendimiento de datos así como la cantidad de flujos de datos espaciales resueltos. Cada flujo espacial requiere su propio par de antenas TX/RX en cada extremo de la transmisión (Figura 2.1). Es importante comprender que la tecnología MIMO precisa una cadena de frecuencia de radio (RF) individual y un convertidor de 'análogo a digital' (ADC) para cada antena MIMO. Esta complejidad adicional se traduce en gastos superiores de implementación así como en la necesidad de contar con sistemas de alto rendimiento.

Intel espera que la tecnología MIMO juegue un papel importante en el logro de las metas de IEEE TGn. La tecnología MIMO debe ser utilizada en IEEE 802.11n para evolucionar a la interfaz física OFDM existente que se ha implementado en la actualidad con el 802.11a/g. No obstante, las soluciones prácticas seguramente necesitarán métodos tecnológicos adicionales. Las implementaciones que precisan más de dos cadenas de antenas RF necesitarán ser organizadas cuidadosamente en su arquitectura a fin de mantener los costos bajos a tiempo de satisfacer las expectativas de rendimiento.

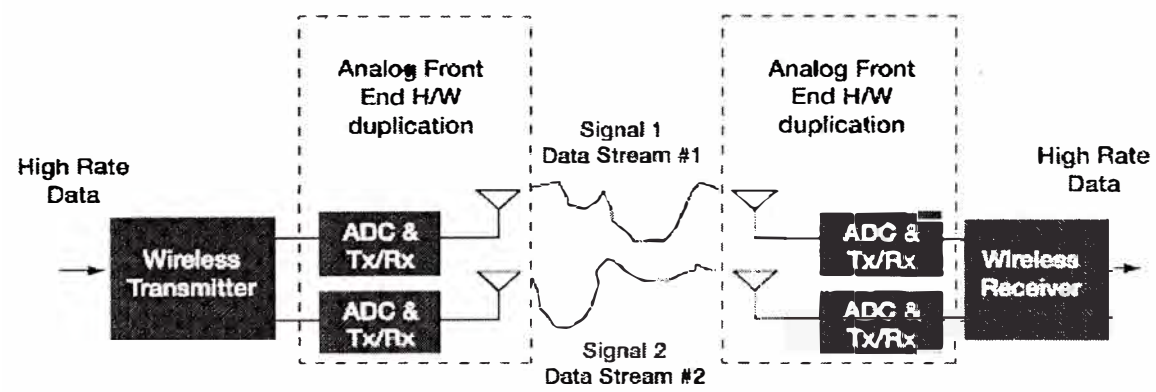

Figura 2.5: Sistema básico de la dos-antena MIMO con ejemplo de la dos-corriente SDM

Otra herramienta importante que puede incrementar la velocidad de transferencia PHY constituyen los canales con un ancho de banda espectral más amplio. El incremento del ancho de banda de los canales no es un concepto nuevo. Puede verse claramente en la ecuación de capacidad de Shannon [C = B log2 (1+SNR)], los límites de capacidad

teorética "C" disminuyen directamente cuando se consideran incrementos en el ancho de banda ocupado "B" (consulte la Figura 2.6).

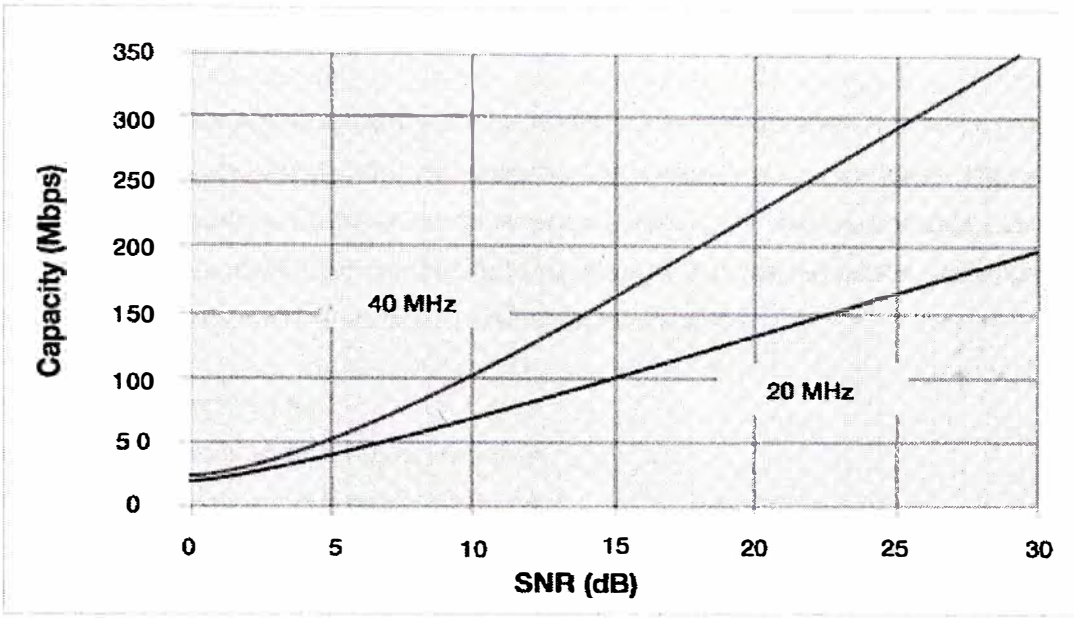

Figura 2.6: Límites de aumento de la capacidad.

El uso de un ancho de banda para canales más amplio con OFDM ofrece ventajas significativas durante la maximización del rendimiento. Los canales de ancho de banda más amplio son rentables y se pueden lograr con facilidad gracias a incrementos moderados en el procesamiento de señales digitales (DSP). Si se implementaron correctamente, los canales a 40MHz pueden proporcionar más del doble del ancho de banda utilizable de dos canales 802.11 legados. Al combinar la arquitectura MIMO con los canales de ancho de banda más amplio se ofrece la oportunidad de crear métodos muy poderosos y, al mismo tiempo, rentables para incrementar la velocidad de transferencia física.

Los métodos MIMO que utilizan solamente canales de 20MHz requerirán costos de implementación superior para satisfacer el requisito para TGn de 100Mbps en la MAC SAP. El satisfacer el requisito del IEEE TGn con solamente canales de 20MHz requeriría al menos tres antenas con extremos frontales tanto en el transmisor como en el receptor. Al mismo tiempo, una solución con 20MHz tendría dificultades al proporcionar una experiencia robusta con aplicaciones que exigen un rendimiento superior en entornos reales de usuarios.

La figura 3.3 ilustra los resultados de un simulacro (usando el modelo D de canales TGn) y refleja el resultado over-the-air (OTA) en diferentes valores SNR donde el SNR sucede posterior a la detección después de que los impedimentos de los canales han sido tomados en cuenta. Se asume una eficiencia MAC del 70% para ilustrar el requisito Top-of-MAC de 100Mbps en TGn (140Mbps de OTA).

Estos resultados comparan el rendimiento de las implementaciones a 20MHz y a 40MHz. Ilustraremos cada configuración de sistema al utilizar la convención siguiente. Un transmisor de dos antenas que se comunica con un receptor de dos antenas por un canal a 40MHz es representado por un 2x2-40MHz, donde 2 flujos de datos son transferidos. También se encuentran representados en estos resultados:

- 4x4-20MHz transfiriendo 4 flujos de datos
- 2x3-20MHz transfiriendo 3 flujos de datos
- 2x2-20MHz transfiriendo 2 flujos de datos

La ventaja principal que ofrece una implementación 2x3-20MHz sobre la implementación 2x2-20MHz es la relación de señal a ruido (SNR) mejorada. Esto se nota con el rango mejorado para una capacidad de rendimiento dado. Estos datos muestran que una implementación de dos flujos MIMO no logra satisfacer los requisitos de Top-of-MAC de 100Mbps. Para lograr la meta de 100Mbps usando solamente canales de 20MHz requerirá que las implementaciones MIMO admitan al menos tres flujos de datos. Es fácil apreciar la ventaja de una implementación 2x2-40MHz en estos resultados. Fíjese que aún duplicando la cantidad de cadenas RF usando una implementación 20MHz para transmitir cuatro flujos de datos no se logra el rendimiento posible con solamente dos cadenas RF usando un canal de 40MHz transmitiendo dos flujos de datos. El uso de dos canales de 40MHz permite una complejidad reducida, lo cual mantiene los costos bajos a tiempo de ofrecer resultados para una experiencia robusta del usuario.

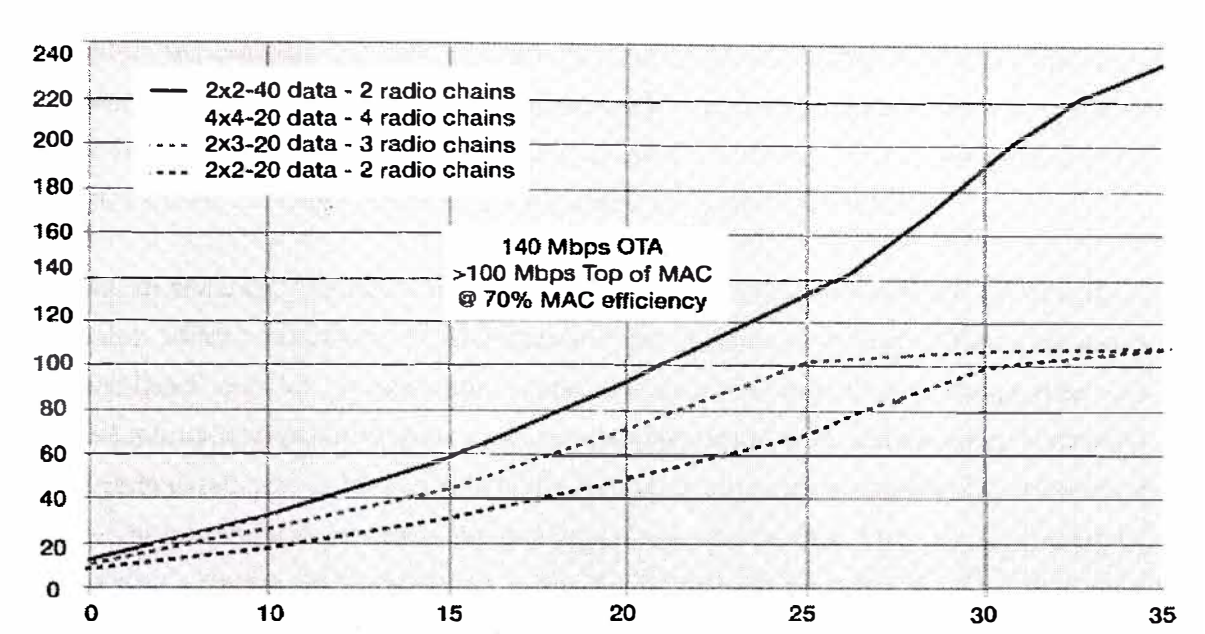

Figura 2.7: Sobre el Aire (OTA) Throughput con diferentes canales de ancho de banda.

Intel cree que tanto la tecnología MIMO así como los canales de ancho de banda más amplio serán requeridos para satisfacer fiablemente las demandas de resultados superiores que se esperan del 802.11n. Al seleccionar incrementos conservadores en el ancho de banda de los canales, combinados con métodos conservadores en la tecnología MIMO, se habilitarán soluciones rentables para satisfacer dichos requisitos. Un método combinado, empleando tanto canales MIMO como 40MHz, habilitarán la tecnología IEEE 802.11n para alcanzar un rendimiento aún superior como la Ley de Moore y las mejoras en la tecnología del proceso CMOS avanza las capacidades del DSP.

La visión de Intel para el estándar IEEE 802.11n ofrecerá una capacidad, a fin de asegurar que las redes de alto rendimiento funcionen eficientemente. El estándar debe admitir a los canales de 20MHz así como a los de 40MHz, donde los canales de 40MHz son los más amplios, que consistirán de dos canales espectrales de 20MHz legados colindantes y los canales de 20MHz para ser utilizados donde la disponibilidad de espectro sea limitada.

Todos los dispositivos de 802.11n deben ser compatibles con 40MHz, donde lo permitan las normas gubernamentales o regulatorias. Se necesita compatibilidad con los canales de 40MHz en todos los dispositivos de 802.11n a fin de prevenir ineficiencias, asociadas con el multiplexado del ancho de canales entre los dispositivos de alto rendimiento de 20 MHz y de 40MHz. Esto permitirá el rendimiento más alto posible dentro de una red de 802.11n. Los entornos que limitan el ancho del canal a 20MHz serán sobrecargados con

los costos adicionales de las implementaciones MIMO complejos a fin de lograr el rendimiento requerido. Intel espera que las restricciones regulatorias en dichos entornos que en la actualidad no permitan que los canales a 40MHz, se alineen para admitir a 40 MHz tales como los dispositivos 802.11n, y que se vuelvan obsoletos.

Además, el estándar de 802.11n debe requerir compatibilidad con, al menos, dos flujos espaciales MIMO mediante el Multiplexado de división espacial (SDM). Si especifica compatibilidad con al menos dos flujos de datos espaciales, esto provee diseños arquitectónicos que pueden ínter funcionar eficientemente en redes de alto rendimiento. La compatibilidad con al menos dos flujos de datos espaciales requiere un mínimo de dos antenas de transmisión en todas las implementaciones de 802.11n. La compatibilidad con más de dos antenas de transmisión o dos flujos espaciales debe ser espacial, siendo la cantidad máxima limitada a cuatro, por razones prácticas.

Las características avanzadas que pueden maximizar el rendimiento para aquellas aplicaciones que requieren el rendimiento más alto, se pueden implementar de forma opcional. Intel espera que las características avanzadas de este tipo se especifiquen en el estándar 802.11n a fin de garantizar la ínter funcionalidad pero que sean opcionales para la implementación solamente donde tenga sentido hacerlo. Esto podría incluir características tales como: más de dos antenas de transmisión, formación de canal adaptivo para canales y los métodos de cifrado FEC avanzados

2.5 Administración de los modos de rendimiento PHY

Cuando se máximiza el rendimiento de los datos, los mecanismos inteligentes serán requeridos para administrar la selección de los modos de rendimiento de la Capa PHY. Aunque la Capa MAC no contribuye directamente al incremento de la velocidad de transferencia física, desempeñará un papel clave en la selección de optimización efectiva de los modos de rendimiento de la Capa PHY.

Se cree que la adaptación rápida de canales debe ser administrada en la Capa PHY sin interacción de MAC. Una vez que se establece la adaptación inicial, usando la señalización “over-the-air” en el momento apropiado, la capa MAC necesitará establecer y mantener la adaptación a las condiciones inalámbricas de los canales. Esto incluirá la administración de la selección de esquemas de cifrado de modulación, velocidad de códigos, configuraciones de antena, anchos de banda de los canales y la selección de canales donde la optimización de las relaciones TX/RX pueden maximizar el rendimiento.

2.6 Mejorar Eficientemente la Transferencia

Un contribuidor cuantioso al rendimiento general del MAC SAP serán las nuevas características MAC que maximizan la eficiencia del rendimiento. Es importante tener en cuenta que el encabezado de PHY y las demoras de respuesta por radio pueden limitar notablemente el rendimiento alcanzable. Estos retrasos fijos no son reducidos a la misma relación a la que la velocidad de carga PHY está incrementando. De hecho, los encabezados de PHY necesitan ser más largos a fin de admitir los nuevos modos de la Capa PHY avanzados que se describieron anteriormente. Siendo que los encabezados necesitarán crecer en tamaño, debe minimizarse el desgaste fijo total de la conexión.

Las nuevas secuencias de intercambio agregadas ofrecen una manera importante de mejorar la eficiencia de transferencia. Un intercambio agregado sucede cuando varias Unidades de protocolo MAC (MPDU) son congregadas en una sola Unidad de datos de protocolo PHY (PPDU). Las secuencias de intercambio agregadas son posibles con un protocolo que reconoce varias unidades MPDU con un solo reconocimiento en bloque (Bloque ACK), en respuesta a una solicitud de reconocimiento en bloque (BAR). Este protocolo elimina efectivamente la necesidad de iniciar una transferencia nueva para cada unidad MPDU. Si intenta utilizar los protocolos MAC existentes sin la agregación, una velocidad del PHY de 500Mbps será necesaria para lograr la meta de rendimiento del TGn a 100Mbps en el MAC SAP.

Existen oportunidades adicionales con los nuevos mecanismos MAC para transferir datos en ambas direcciones, también sin iniciar una transferencia nueva. Este método permite que un contestador agregue unidades MPDU agregadas, en una dirección inversa, en respuesta a una transferencia de estaciones de iniciación. Los mecanismos que también posibilitan la minimización de las instancias de ciclos entre el iniciador y el contestador, a tiempo de garantizar la protección contra conflictos dentro del BSS.

A fin de transferir datos más efectivamente y reducir el tiempo fijo de conexión, Intel cree que se necesitan unidades PPDU agregadas que contengan varias MPDU, a partir de una sola fuente hacia un solo destino. Para maximizar la eficiencia para esta clase de capacidad se requerirán varias PPDU más largas que las que permite el estándar actual (4095bytes).

Intel espera que las PPDU agregadas también puedan transferir datos a varios destinos mediante los nuevos formatos de las MPDU. Esto será muy valioso para aplicaciones

tales como Voz sobre Internet Protocoló (VoIP). Este método proveerá una alta capacidad de BSS para muchas estaciones que necesitan acceso, donde cada una de ellas contará con un rendimiento relativamente bajo de los requisitos por estación.

2.7 802.11 La coexistencia de la herencia

El IEEE TGn requiere compatibilidad retroactiva con los dispositivos 802.11a/b/g. Se espera que los dispositivos 802.11b legados coexistirán, y que los dispositivos 802.11a/g legados interfuncionarán con los dispositivos 802.11n cuando funcionen en la misma banda y canal. Esto significa que 802.11n necesitará la compatibilidad con los canales de 20MHz para dicha compatibilidad retroactiva.

La MAC será responsable por la administración de la compatibilidad retroactiva con los dispositivos 802.11 a/b/g legados existentes. Esto incluirá la coexistencia con todos los dispositivos legados (802.11a/b/g) que se conecten con un 802.11n BSS. La MAC también proveerá interfuncionalidad con los esquemas de modulación admitidos (tales como OFDM) en entornos espectrales coincidentes (por ejemplo: 2,4GHz ISM o 5,0GHz U-NII tal como se implementó). Los mecanismos de coexistencia necesitarán administrar los mensajes del ancho de banda del canal en los entornos BSS combinados y asegurar que el funcionamiento en modos mixtos es compatible con gastos fijos bajos entre 802.11n y 802.11a o 802.11g legados.

2.8 Resumen

La visión de Intel para el estándar IEEE 802.11n se logrará y sobrepasará las expectativas de 100Mbps del IEEE TGn en el MAC SAP (Top-of-MAC). La tecnología de 802.11n admitirá todas las plataformas principales, incluidas las de electrónicos del consumidor, computación personal y plataformas de comunicaciones de bolsillo para todos los entornos principales corporativos, domésticos y los lugares públicos con conexión de red. El alcance amplio de esta visión promueve implementaciones prácticas que funcionarán robustamente usando métodos técnicos que pueden ser desarrollados e implementados de forma rentable dentro de las fechas límite definidas por el IEEE TGn.

CAPITULO III
SOLUCIONES MIMO

3.1 Productos PRE-N

Llamase PRE-N porque todavía no trabajan con la versión final del estándar de la IEEE 802.11n.

No todos los fabricantes disponen actualmente de soluciones MIMO. Deseamos seleccionar un par de ellas que destacan por sus prestaciones y diseño.

Linksys, es sin duda un fabricante de referencia y por ello hemos seleccionado uno de sus últimos Routers como punto de referencia. Este modelo es el más moderno de su gama con MIMO, ya tienen unos cuantos, y es conocido como WRT54GX4. Es la cuarta generación de Routers MIMO, dispone tres antenas y presume de ampliar la cobertura hasta en tres veces frente a un producto sin este sistema MIMO. Linksys denomina a esta cuarta generación de productos MIMO como SRX400 y presume de que es capaz de aumentar la velocidad de transmisión hasta 10 veces frente a productos 802.11g convencionales. En realidad esta ganancia de velocidad esta todavía por demostrar, el WRT54GX4 un producto que acaba de ser lanzado al mercado y Linksys no proporciona datos concretos.

Figura 3.1 Router MIMO LINKSYS

Belkin también dispone de soluciones MIMO que acertadamente han llamado gama Pre-N. Estos productos incorporan MIMO y tienen un precio mas "adecuado" que las soluciones de otros fabricantes. Como en el caso del Linksys se trata de un producto con triple antena inteligente.

D-LINK, líder en conectividad de consumo, anuncia una nueva línea de productos inalámbricos basados en el estándar 802.11g WiFi con la revolucionaria tecnología de redes inalámbricas Smart Antenna que proporciona prestaciones de vanguardia de hasta ocho veces la potencia efectiva sobre redes inalámbricas tradicionales 802.11g/b. D-Link Super G™ con MIMO dota de mayor velocidad y mejor gama a una red inalámbrica mediante la tecnología Smart Antenna que incluye el "beamforming", una característica técnica para direccionar la señal inalámbrica en ángulo hacia el cliente elegido. Mejorando de esta manera la transmisión inalámbrica omni-direccional que generalmente propaga la misma gama en todas las direcciones, el beamforming permitirá que la señal se dirija al dispositivo de destino y propague más gamas en esta dirección. En el dispositivo receptor, la tecnología de recepción óptima utiliza un proceso de señales avanzado para asegurar que las señales entrantes en el D-Link Super G™ con implementación MIMO se juntan con la mayor fuerza combinada para conseguir una capacidad de tratamiento máxima. Incluso con productos inalámbricos no preparados para MIMO, la solución D-Link Super G™ aportará más prestaciones a las actuales familias de productos D-Link Xtreme G™ y AirPlus™ G que se beneficiarán de nuestro Super G™ con tecnología MIMO Smart Antenna.

"Las soluciones de red inalámbrica de alta velocidad como nuestro nuevo D-Link Super G™ con MIMO no sólo tienen beneficios en un entorno de oficina sino también para el consumidor en un hogar digital, permitiendo que las velocidades y gamas de nueva generación manejen las aplicaciones emergentes que requieren mucho ancho de banda, incluyendo las señales HD y los juegos en línea," dijo Luigi Salmoiraghi, Country Manager para España y Portugal.

"El avanzado D-Link Super G™ con tecnología Smart Antenna MIMO tiene una terminación única lo que significa que permite la máxima capacidad de tratamiento entre dos dispositivos MIMO y que también se comunica con todos los dispositivos inalámbricos heredados Wi-Fi 802.11g y 802.11b en un intercambio transparente de tráfico, mientras optimiza la red al amplificar las señales sin comprometer la interoperabilidad," añadió Luigi Salmoiraghi. "D-Link Super G™ con MIMO proporciona

velocidades de tratamiento muy rápidas, gamas sin precedentes y una completa interoperabilidad entre tecnologías 802.11 y entornos multi-fabricantes."

El D-Link Super G™ con implementación MIMO no sólo es más compatible sino que ofrece el diseño más económico, lo que da como resultado un nivel de precio global más bajo para los consumidores aportando mejores prestaciones. Utilizando el beamforming, D-Link Super G™ con MIMO operará a las velocidades más altas posibles proporcionando a la vez una fuerte señal 11g a los dispositivos heredados 11g y 11b alcanzando unas prestaciones y una capacidad de tratamiento sin igual.

La solución D-Link Super G™ con MIMO dispone de una robusta seguridad para proteger la red inalámbrica de los intrusos, cumpliendo con los últimos protocolos de seguridad de red inalámbrica, incluyendo la encriptación WEP y WPA (Wi-Fi Protected Access), un componente integral del último estándar de seguridad IEEE 802.11i. La solución de red inalámbrica D-Link Super G™ además incluye el router inalámbrico Super G™ con MIMO DI 624M de 4 puertos y el adaptador inalámbrico CardBus Super G™ con MIMO DWL-G650M.

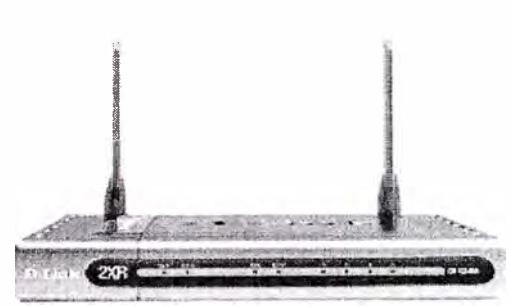

Figura 3.2 Router MIMO D-LINK

3.2 Problema de Compatibilidades

Los clientes empresariales con experiencia WLAN han mostrado ciertas reticencias respecto del estándar pese a la promesa de una gran mejora en la tasa de transferencia. Al contrario, se muestran preocupados por otras cuestiones críticas como la utilidad y efectividad de 802.11n en un entorno incontrolado, compartido y con diversos puntos de acceso, o la compatibilidad con las redes 802.11b/g. Para resolver esta última cuestión, el 11n Task Group ha creado un subcomité que tendrá que determinar si recomienda uno o diversos mecanismos para evitar el problema y si hace que sean opcionales u obligatorios, ya que 802.11n puede ejecutarse en los canales de 20MHz y 40MHz, que

proporcionan una mayor transferencia, pero su uso en la frecuencia de 2,4GHz puede crear problemas en los dispositivos 802.11b/g que transmiten en 20MHz.

Pese al escepticismo empresarial, los analistas predicen un mercado preparado para productos pre - 802.11n. Estos se harán con cerca del 15% de todos los productos WLAN para el mercado de consumo lanzados en este año, según Dell´Oro Group. La firma augura que para 2009 las redes 11n coparán el 90% de las WLAN domésticas. Sin embargo, habrá una adopción más lenta en la empresa, si bien los despliegues a gran escala se acelerarán hacia 2008 y 2009.

3.3 Resumen

El enrutador MIMO tiene un excelente desempeño y un amplio rango de cobertura (que requiere, por supuesto, para aprovecharla al máximo, de una tarjeta de la misma tecnología fabricada por su fabricante hasta que se publique el estándar 802.11n), un buen manejo de las molestas interferencias de teléfonos inalámbricos o de las redes inalámbricas de los vecinos.

Así que si esta buscando una solución para llegar más lejos con una red inalámbrica, o si se presenta problemas de interferencia, puede valer la pena pagar más por este dispositivo que te permitirá compartir la conexión a Internet, archivos e impresoras con las demás máquinas de tu red, y sin cables.

CAPITULO IV
SISTEMAS DE SEGURIDAD ACTUALES

4.1 Introducción

Es evidente que una red inalámbrica esta predispuesta a una mayor intrusión que una red con cable. En el caso de una red domestica la intrusión suele ser un mero aprovechamiento de terceros de nuestra línea de datos y de nuestra salida a Internet pero también debemos saber que si nuestra red esta accesible y sin asegurar cualquier puede acceder a nuestros archivos, datos personales, etc. Es importante asegurar nuestro sistema debidamente y para ello las tecnologías wireless disponen de diversas tecnologías, que aunque no perfectas, si que nos librarán del intruso ocasional o de proximidad.

Para ello se usan sistemas de encriptación de la señal que usan algoritmos para proteger los datos enviados de los ojos curiosos. Estas encriptaciones también nos permiten establecer códigos, con los que se genera la encriptación, que inhabilita a cualquiera que no sepa la contraseña para entrar en nuestra red. También podemos establecer otros mecanismos para conservar la privacidad como el control por MAC (La MAC es un indicador único, como una matrícula, que tiene cualquier tarjeta de red) pero este tipo de control es fácilmente violable mediante la suplantación de la MAC.

Con las revisiones A y B del 802.11 el único sistema de encriptación disponible era el conocido WEP (Wired Equivalent Privacy - Privacidad Equivalente al Cable). Este sistema usa un sistema de control de acceso y encriptación simétrica con una clave única en el punto de acceso y las estaciones. En el caso empresarial este sistema tiene inconvenientes de seguridad y de mantenimiento ya que la clave esta situada en cada estación, comprometiendo la seguridad, y tampoco hay ningún sistema dinámico de autenticación por lo que el administrador tiene que estar configurando cada puesto de forma individual. En cuanto a la seguridad tiene agujeros importantes basados sobretodo en su vector de inicialización. No entrare en detalles pero básicamente, incluidas las actualizaciones a 128-bit que sufrió el WEP en un segundo estadio, permiten a los atacantes averiguar o falsificar el CRC-32 que controla la encriptación. A parte de esto las

claves que debemos usar son hexadecimales por lo que para un usuario convencional se convierte en un incordio recordar una clave hexadecimal de hasta 26 caracteres.

El WPA entra en acción para salvar al WEP de sus carencias. Este estándar denominado WiFi Protected Access se incorpora con el 802.11G y se encuentra ya en su segunda actualización con códigos de encriptación de 256-Bit. Básicamente "arregla" los dos problemas principales del WEP, por un lado la administración más costosa con la integración de diversos sistemas de autenticación, y por otro lado mejorando las carencias tanto de los códigos a usar como su vulnerabilidad en la clave compartida y el vector de inicialización con la incorporación de un doble vector de 48-bit frente al único vector de 24-Bit del WEP. Lo mejor es que el WPA permite a los entornos empresariales el uso de servidores Radius para la autenticación de los clientes y que en el caso de los usuarios domésticos podamos usar cualquier clave alfanumérica que creamos conveniente.

El WPA surgió después de que el WEP mostrara sus vulnerabilidades allá por el 2001 cuando ya llevaba en funcionamiento desde 1999. Es una actualización de software y por tanto compatible con cualquier generación 802.11x de productos pero la verdad es que solo la veremos soportada en productos comerciales domésticos marcados por el 802.11g. el WPA2, que es el sistema que se comienza a usar, cambia el sistema algoritmos, mucho mas potentes, y requerirá no de un hardware especifico pero si más potente para gestionar estos algoritmos más potentes.

4.2 Estableciendo seguridad WPA

Crackear una red inalámbricas protegida por WEP es relativamente fácil. Existen distribuciones de Linux pensadas para monitorizar la seguridad de los sistemas que en apenas unos minutos nos permiten crackear una red WEP con encriptación de 128-Bit. Para ello solo basta con bombardear el punto de acceso victima del ataque hasta que nos reenvíe suficientes vectores de iniciación como para configurar un patrón. En apenas unos minutos de captura de datos podremos establecer la contraseña usada para encriptar la red inalámbrica.

Los tres aspectos fundamentales que se deben tener en cuenta en una red WiFi de una cableada, son:

- Autenticación

- Control de acceso
- Confidencialidad

Autenticación y control de acceso:

Los métodos que se emplean son los siguientes:

a. SSID (Service Set Identifier): Contraseña (WEP)

El Standard 802.1x permite un empleo de autenticación que se denomino "Dynamic WEP", que permite emplear este algoritmo como parte de 802.1x, de forma un poco más segura que el "WEP estático", pero la alianza Wi-Fi recomienda no emplear ninguno de ellos en entornos seguros.

b. Seguridad por restricción de direccionamiento MAC: Permite restringir a un listado de direcciones, las que se pueden conectar y las que no.

c. Contraseñas no estáticas:
- Periódicas
- OTP (One Time Password): Contraseñas de un solo uso, también conocidas como token flexibles.

d. 802.1x: Este estándar no fue presentado para WiFi, sino para el acceso seguro PPP (En tecnologías de cable).

Una de las grandes características de WiFi es la de "no reinventar la rueda" y emplear todas las herramientas que ya existen y pueden prestar utilidad al mismo. 802.1x es uno de los mejores ejemplos de esto.

La arquitectura 802.1x está compuesta por tres partes:

- Solicitante: Generalmente se trata del cliente WiFi.
- Autenticador: Suele ser el AP, que actúa como mero traspaso de datos y como bloqueo hasta que se autoriza su acceso (importante esto último).
-Servidor de autenticación: Suele ser un Servidor RADIUS (Remote Authentication Dial In User Service) o Kerberos, que intercambiará el nombre y credencial de cada usuario.

El almacenamiento de las mismas puede ser local o remoto en otro servidor de LDAP, de base de datos o directorio activo.

Otra de las grandes ventajas de emplear 802.1x es que el servidor de autenticación, permite también generar claves de cifrado OTP muy robustas, tema en particular que ya lo posiciona como imprescindible en una red WiFi que se precie de segura.

e. 802.11i: El Task Group de IEEE 802.11i, se conformó en el año 2001, con la intensión de analizar una arquitectura de seguridad más robusta y escalable, debido a la inminente demanda del mercado en este tema y en julio de 2004 aprobó este estándar. Por su parte la WiFi Alliance lo lanzó al mercado en septiembre de ese año.
En forma resumida, este nuevo estándar, propone a 802.1x como protocolo de autenticación, pudiendo trabajar con su referencia EAP (Extensible Authentication Protocol: RFC 2284), este último proporciona una gran flexibilidad (sobre todo a los fabricantes) en la metodología de autenticación.

Previo al estándar, Cisco Systems ofreció el primer tipo de autenticación que se denominó LEAP (Lightweight EAP), protocolo que inicialmente fue propietario de Cisco, pero en la actualidad lo emplean varios fabricantes. Cisco se está volcando hacia PEAP (se describe a continuación).

Por su parte Microsoft, inicialmente junto con Windows XP (hoy con todos sus SSOO), lanzó al mercado su protocolo denominado EAP/TLS (Extensible Authentication Protocol with Transport Layer Security - RFC: 2716), y fue aceptado por IEEE, se basa en certificados en lugar de contraseñas como credenciales de autenticación. Otros fabricantes han presentado EAP/TTLS (EAP with Tunneling Transport Layer Security), el cual realiza un túnel de nivel 2 entre el cliente y el AP, una vez establecido el túnel, EAP/TTLS opera sobre él, lo cual facilita el empleo de varios tipos de credenciales de autenticación que incluyen contraseñas y certificados, en realidad no deja de ser una variante de EAP/TLS.

La última variante es PEAP (Protected Extensible Authentication Protocol), inicialmente fue la versión “0” y ya está vigente la versión “1”, el cual aplica una metodología muy similar a EAP/TTLS en cuanto al empleo de túnel y sobre el una amplia variedad de credenciales de autenticación, este último ya está soportado por los más importantes

fabricantes. En general, se considera que PEAP es el método más seguro del momento. Este protocolo fue desarrollado por Microsoft, Cisco y RSA.

4.3 Cifrado

a. WEP: Emplea el algoritmo de cifrado de flujo RC4 (Rivest Cipher 4), este algoritmo es una de las bases de RSA y cabe aclarar que es también empleado en el estándar SSL (Secure Socket Layer), se trata de un algoritmo robusto y veloz. Los problemas de WEP, no son por este algoritmo, sino por la debilidad de sus claves, tanto en 64, 128 (y hoy también 156) bits, de los cuales se deben excluir los 24 del VI (Vector de inicialización), hoy en día cualquier usuario con "Airsnort" lo descifra, sin tener ningún conocimiento especializado, incluso la metodología de "Airsnort" es pasiva, es decir, únicamente escucha tráfico, hoy existen herramientas mucho más potentes que operan de forma activa, que emplean varias técnicas para generar tráfico y basado en las respuestas de la red permiten acelerar exponencialmente el proceso. Estas últimas metodologías se denominan INDUCTIVAS y existen dos grandes familias: ataques de repetición y ataques de modificación de bits.

Existen también ataques de fuerza bruta, basados principalmente en técnicas de diccionario, las cuales en el caso de WEP, son de especial interés, pues el nombre de usuario viaja en texto plano, lo cual ofrece una gran ventaja para generar posibles claves.

b. Las deficiencias presentadas por RC4 y WEP, se están tratando de solucionar en la actividad de cifrado, a través del protocolo TKIP (Temporal Key Integrity Protocol).

Esta propuesta aparece a finales de 2002, también se basa en RC4, pero propone tres mejoras importantes:

- Combinación de clave por paquete: La clave de cifrado, se combina con la dirección MAC y el número secuencial del paquete. Se basa en el concepto de PSK (Pre-shared Key). Esta metodología, genera dinámicamente una clave entre 280 trillones por cada paquete.
- VI (Vector de inicialización) de 48 bits: Esta duplicación de tamaño implica un crecimiento exponencial del nivel de complejidad, pues si 24 bits son 16 millones de combinaciones, 48 bits son 280 billones. Si se realiza una gran simplificación (pues el caso es más complejo) y se divide 280 billones sobre 16 millones, el resultado es:

17.500.000, por lo tanto si un VI de 24 bits se repite en el orden de 5 horas en una red

Wireless de una mediana empresa, entonces:

Un VI de 48 bits = 5 x 17.500.00 horas = 87.500.000 horas = 3.645.833 días = 9.988 años.

- MIC (Message Integrity Check): Se plantea para evitar los ataques inductivos o de hombre del medio. Las direcciones de envío y recepción además de otros datos, se integran a la carga cifrada, si un paquete sufre cualquier cambio, deberá ser rechazado y genera una alerta, que indica una posible falsificación del mismo.

Desafortunadamente TKIP, no está contemplado aún en la totalidad de los productos.

c. Microsoft ofrece otra alternativa que inicialmente denominó SSN (Simple Security Network), el cual es un subconjunto de 802.11i y al mismo tiempo una implementación de TKIP al estilo Microsoft. SSN lo adoptó 802.11i renombrándolo como WPA (WiFi Protected Access), en el año 2004 aparece WPA2 que es la segunda generación del WPA; Este ya proporciona encriptación con AES (que se menciona a continuación), un alto nivel de seguridad en la autentificación de usuarios y está basado en la norma IEEE 802. 11i y forma parte de ella.

Aunque la WPA impulsa la seguridad WLAN, muchos la consideran una solución temporal pues la solución de 802.11 se orienta más hacia el Modo Conteo con el Protocolo del Código de Autenticación de Mensajes en cadena para el bloqueo de cifrado (Counter-Mode/CBC-Mac Protocol, que se abrevia: CCMP), que también forma parte de la norma 802.11i. Se trata de un nuevo modo de operación para cifrado de bloques, que habilita a una sola clave para ser empleada tanto en autenticación como para criptografía (confidencialidad). Se trata de un verdadero "Mix" de funciones, y su nombre completo proviene el "Counter mode" (CTR) que habilita la encriptación de datos y el Cipher Block Chaining Message Authentication Code (CBC-MAC) para proveer integridad, y de ahí su extraña sigla CCMP.

El protocolo CCMP usa la Norma de Encriptación Avanzada (AES) para proporcionar encriptación más fuerte. Sin embargo, AES no está diseñada para ser compatible con versiones anteriores de software.

A pesar de todos los esfuerzos realizados, muchas entidades siguen considerando a TKIP y WPA como métodos insuficientes de seguridad, el mayor exponente de esta posición es FIPS (Federal Information Process Standard), que excluye a RC4 en las comunicaciones confidenciales. Su publicación FIPS-197 de finales del 2001, define al estándar AES (Advanced Encription Standard) que se mencionó en el punto anterior, con clave mínima de 128 bits, como el aplicable a niveles altos de seguridad. Este estándar,

propuesto por Rijndael, surgió como ganador de un concurso mundial que se celebró en el año 2000, para definir la última generación de estos algoritmos. La mayoría de los fabricantes están migrando hacia este algoritmo y se aprecia que será el estándar que se impondrá en el muy corto plazo.

El tema de AES tampoco es tan sencillo como parece, pues las implementaciones por software imponen una dura carga de trabajo al sistema, ocasionando demoras de rendimiento que pueden llegar al 50 % de la tasa efectiva de transmisión de información, por lo tanto, se debe optimizar este aspecto para que sea asumido por el mercado.

La WiFi Alliance propone dos tipos de certificación para los productos, cuyas características se presentan a continuación:

- Modelo Empresas:

WPA:

- Autentication: IEEE 802.1x/EAP.
- Encryptation: TKIP/MIC.

WPA2:

- Autentication: IEEE 802.1x/EAP
- Encryptation: AES-CCMP.

- Modelo personal (SOHO/personal):

WPA:

- Autentication: PSK.
- Encryptation: TKIP/MIC

WPA2:

- Autentication: PSK.
- Encryptation: AES-CCMP.

CAPITULO V
IMPLEMENTACION CON TECNOLOGIA MIMO

5.1 Descripción de implementación

El objetivo es interconectar los tres locales en Lima (Sede Central, Ribeyros y la ENEI) usando equipos inalámbricos y también establecer en las oficinas departamentales una red inalámbrica de topología infraestructura porque muchos de los locales son alquilados y no es conveniente instalar una red alambrica por problemas de disponibilidad presupuestal pero manteniendo la calidad de transmisión como es el caso de la tecnología FASTETHERNET (100Mbps).

Para implementar la red de la figura 5.1 se realizo previamente un estudio de transferencia de datos, tipo de aplicaciones existentes y los servicios de red. Además, la cantidad de usuarios promedios por cada oficina departamental.

La Institución cuenta con sucursales en el interior del país, llamadas Oficinas Departamentales (ODEI's). Para la implementación se utilizo 26 Access Point con tecnología MIMO distribuidas según topología de la red a nivel nacional de las cuales 23 ODEI's se conectan al Internet a través del servicio Speedy. Las antenas son del tipo omnidireccional.

Previamente se realizo un piloto para medir el rendimiento de los Access Point de la 802.11g y los de la tecnología MIMO, se observo un gran desempeño del MIMO a medianas y largas distancias llegando hasta los 108Mbps. Para conseguir este rendimiento las PC's e impresoras deben ser del mismo fabricante.

Se requiere pasar los servicios de voz, video y datos a través de esta tecnología donde tiene un mejor rendimiento que versiones anteriores.

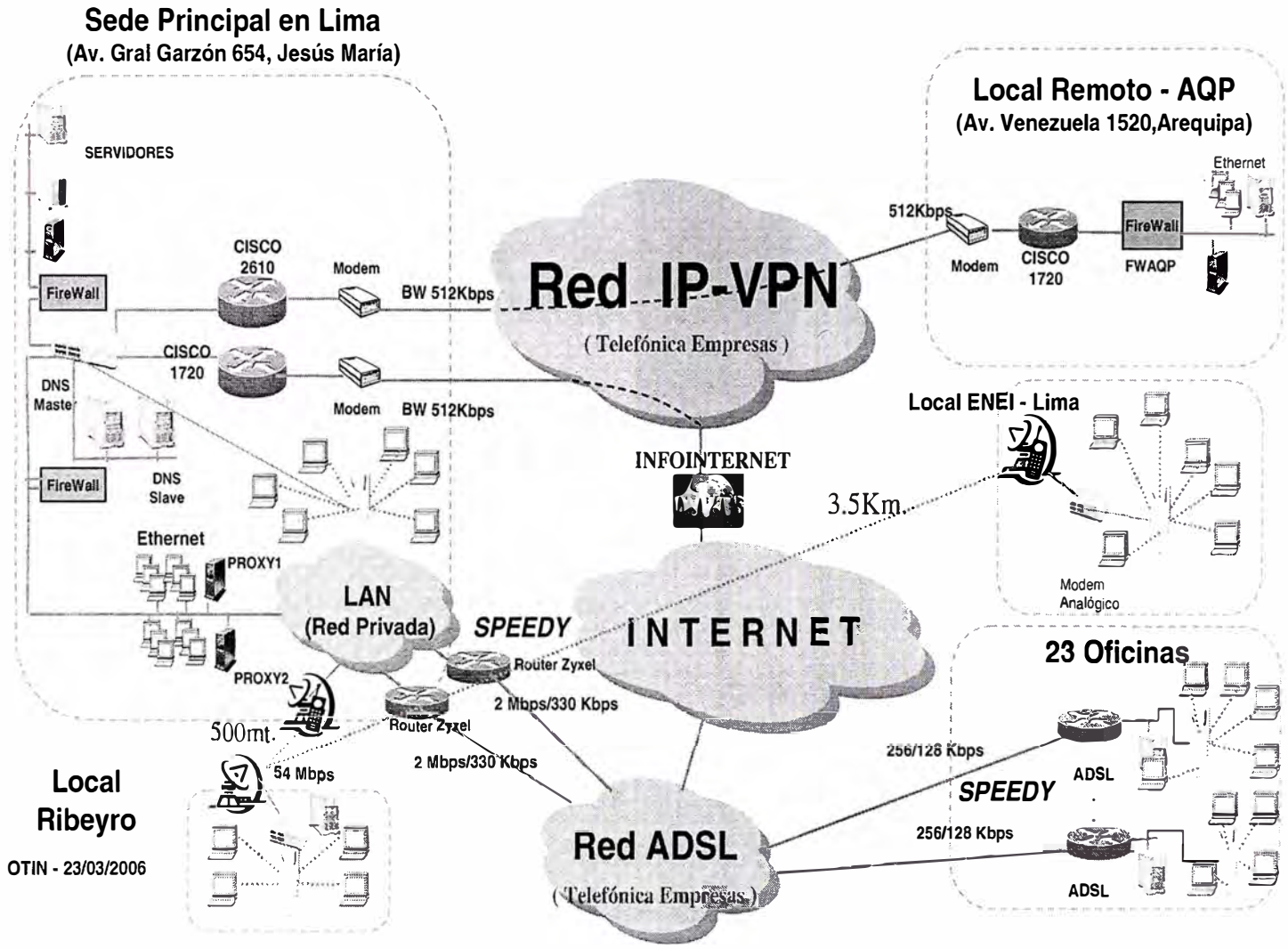

Figura 5.1 Red de comunicaciones a nivel nacional del INEI

Los equipos utilizados son de la marca D-LINK serie DI-624M y los adaptadores son del tipo DWL-G520M.

Además, se cuenta con dos bridges Wireless LAN Outdoor Building-to-Building de 54Mbps para la integración de locales. La implementación tuvo un tiempo de duración de 20 días útiles. En el caso de los bridges para su instalación es considerar la línea de vista luego los demás parámetros son parte de configuración como asegurar la transmisión de la información a través de su consola de administración. (Figura 5.2)

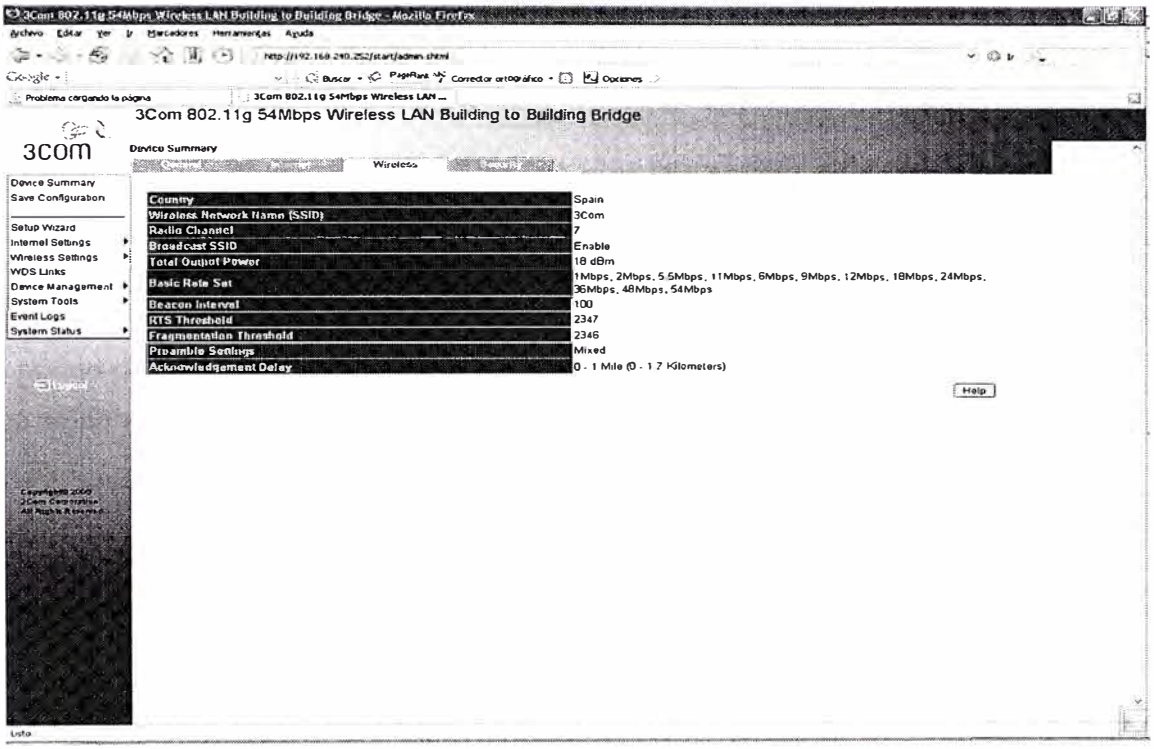

Figura 5.2: Consola de Administración WEB

En cada oficina se instalo un equipo PRE-N atendiendo a un total de 10 usuarios y estos salen al Internet a través del servicio Speedy.

El personal que participo en este proyecto fueron 3, una Ingeniero como analista de proyecto, tecnico y un operador.

Actualmente estos equipos son monitoreados vía SNMP, desde la Sede Central. Para realizar auditoria tenemos las herramientas como software Kismet, Ethereal, Sniffer Wireless, etc. Los primeros son de plataforma Linux en su código nativo pero existen entre otros también para Windows.

Estados del Sistema (Bridge) → Estadísticas

Transmitted Fragments	153485877
Transmitted Multicasts	0
Transmitted Frame Count	153453854
Failed Packets	35922
Retry Count	4263960
Multiple Retry Count	505351
Duplicate Frames	651241
RTS Success Count	0
RTS Failure Count	0
ACK Failure Count	6624317
Received Fragment Count	144421053
Received Multicasts	0
FCS Errors	18408214
WEP Undecryptable	0

Figura 5.3: Estados del Sistema

Se puede observar que no hay transmisiones multicasts, existe paquetes fallados pero esto se debería a las tasas de error de bit que son superados por las retransmisiones.

La configuración de Wireless → Radio

Radio Setup	
Country	Peru
Regulatory Domain	ETSI
Wireless Network Name (SSID)	3Com
Band	2.4GHz G-only (Allow 11g Only)
Radio Channel	7
Broadcast SSID	On Off
Domain Max Output Power	20 dBm
Antenna Gain	Built-in Antenna 18dBi
Antenna Cable	-
Wireless Output Power	0 dBm
Total Output Power (EIRP)	18 dBm

Figura 5.4: Configuración del Inalámbrico

Esta es la configuración que se requiere para que opere el bridge inalámbrico.

Configuración Avanzada

Advanced Setup			
Basic Rate Set	☑ 1Mbps	☑ 2Mbps	☑ 5.5Mbps
	☑ 11Mbps	☑ 6Mbps	☑ 9Mbps
	☑ 12Mbps	☑ 18Mbps	☑ 24Mbps
	☑ 36Mbps	☑ 48Mbps	☑ 54Mbps
	☑ ALL	☑ 108Mbps	
Beacon Interval (TUs)	100		
RTS Threshold (bytes)	2347		
Fragmentation Threshold (bytes)	2346		
Preamble Settings	Mixed		

Figura 5.5: Configuración Avanzada del Inalámbrico

CONCLUSIONES

1. Las redes WLAN 802.11a/b/g proporcionan el rendimiento adecuado para las aplicaciones de conexiones de redes actuales, donde la conveniencia de una conexión inalámbrica puede proporcionar gran valor al usuario. A medida que la próxima generación de aplicaciones inalámbricas emerge, se requerirá un rendimiento superior para los datos de WLAN. En respuesta a esta necesidad, tanto IEEE TGn como la Wi-Fi Alliance han definido expectativas para el rendimiento de la próxima generación de redes WLAN.

2. Las consideraciones clave en la definición de la arquitectura de la proxıma generación de redes WLAN son los costos y el rendimiento robusto. El grupo encargado para la investigación IEEE TGn cree que tanto la tecnología MIMO así como los canales de ancho de banda más amplio serán requeridos para satisfacer fiablemente las demandas de resultados superiores. Al mismo tiempo, el rendimiento general de la MAC SAP será habilitado con las características nuevas de la MAC, lo cual maximizará la eficiencia del rendimiento.

3. MIMO usara canales de 40MHz para alcanzar un rendimiento superior que consistirá en dos canales espectrales de 20MHz.

4. Esta tecnología MIMO bajo el estándar 802.11n es compatible con la 802.11b/g.

5. Tanto la especificación WPA como IEEE 802.11i solucionan todos los fallos de seguridad conocidos de WEP y, en estos momentos, se consideran soluciones fiables.

6. La ventaja de WPA es que no requiere de actualizaciones de hardware en los equipos. Mientras no se descubran problemas de seguridad en WPA, esta implementación puede ser suficiente en los dispositivos para los próximos meses.

ANEXO A

GLOSARIO

LAN, Local Area Network: Red de área local. En general, red basada en cables dentro de una oficina o edificio.

PAN, Personal Area Network: Red de área personal. Red local de corto alcance.

WAN, Wide Area Network: Red de comunicaciones extendida. Redes con alcance mundial.

WEP, Wired Equivalent Privacy: Equivalencia de privacidad con cables. Normas y sistemas de cifrado en comunicaciones inalámbricas.

WIRELESS, sin cables: Tecnologías de transmisión de datos sin enlace física, el cable, entre los equipos. Generalmente basadas en radiofrecuencia., el cable, entre los equipos. Generalmente basadas en radiofrecuencia.

802.11: Estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54Mbps, apoyándose en la banda de los 5GHz. A su vez, elimina el problema de las interferencias múltiples que existen en la banda de los 2,4GHz (hornos microondas, teléfonos digitales DECT, BlueTooth).

802.11b: Extensión de 802.11 para proporcionar 11Mbps usando DSSS. También conocido comúnmente como Wi-Fi (Wireless Fidelity): Término registrado promulgado por la WECA para certificar productos IEEE 802.11b capaces de ínter operar con los de otros fabricantes. Es el estándar más utilizado en las comunidades inalámbricas.

802.11e: Estándar encargado de diferenciar entre video-voz-datos. Su único inconvenientes el encarecimiento de los equipos.

802.11g: Utiliza la banda de 2,4GHz, pero permite transmitir sobre ella a velocidades teóricas de 54Mbps. Se consigue cambiando el modo de modulación de la señal, pasando de 'Complementary Code Keying' a 'Orthogonal Frequency División

Multiplexing'. Así, en vez de tener que adquirir tarjetas inalámbricas nuevas, bastaría con cambiar su firware interno.

Afiliadas: Compañías que trabajan con proveedores más grandes para construir una red nacional. Las afiliadas pueden utilizar el nombre de marca, operaciones de red, servicio al cliente u otros recursos del proveedor más grande.

Análogo: El método tradicional para adaptar señales de radio para que puedan transportar información. AM (Amplitud Modulada) y FM (Frecuencia Modulada) son dos de los sistemas análogos más comunes. El método análogo ha sido repuesto ampliamente por la tecnología digital, la cual es más segura, más eficiente y
Proporciona mejor calidad.

Antena: Un dispositivo para transmitir y recibir señales. Frecuentemente disfrazadas en edificios existentes, árboles, torres de agua u otras estructuras altas, el tamaño y la forma de las antenas son determinadas generalmente por la frecuencia de la señal que manejan.

Estación Base: La central radio transmisora / receptora que se comunica con los teléfonos móvil dentro de un rango dado (típicamente, un sitio célula).

Banda Ancha: Un término general que describe sistemas de telecomunicación que pueden mover datos tales como voz y servicios de video, a velocidades más altas.

BTA (Área Básica de Mercado): Un área de servicio definida por la FCC para promover el rápido lanzamiento de Servicios Personales de Comunicaciones (PCS) y una variedad de otros servicios. Las BTA generalmente son compuestas de varios condados vecinos. Existen 493 BTA en los Estados Unidos.

Proveedor: También conocido como portador de servicio u operador, un proveedor de servicios es una compañía de comunicaciones que proporciona servicio a los clientes (incluyendo Tiempo Aire) para sus teléfonos inalámbricos.

CDMA (Acceso Múltiple por División de Códigos): Una tecnología utilizada para transmitir llamadas inalámbricas asignándoles códigos. Las llamadas son esparcidas en el más amplio rango de canales disponibles. Entonces, los códigos permiten que

muchas llamadas viajen en la misma frecuencia y también guían a esas llamadas al teléfono receptor correcto.

División de Célula: Una forma de incrementar la capacidad de un sistema inalámbrico al subdividir una célula en dos o más células más pequeñas.

Canal: Una ruta por la cuál se transmite una señal de comunicación.

Digital: Tecnología que convierte señales (incluyendo voz) en los dígitos binarios '0' y '1'. Estos datos son comprimidos y transformados en pulsos electrónicos para una red alambrada, ondas de luz óptica para redes de fibra óptica u ondas de radio para redes inalámbricas. La tecnología digital inalámbrica está reemplazando rápidamente a la análoga, porque la tecnología digital ofrece mejor calidad de sonido, señales más seguras, más usuarios por sitio célula y servicios de datos más rápidos.

Banda Dual: Un aparato telefónico que funciona en frecuencias de 800 MHz y frecuencias de 1900 MHz PCS.

Modo Dual: Un aparato telefónico que funciona tanto con redes análogas como digitales.

FCC: Comisión Federal de Comunicaciones. La agencia del gobierno responsable de regular las telecomunicaciones en los Estados Unidos.

FWA (Acceso Fijo Inalámbrico): También conocido como el centro local inalámbrico. Fijo Inalámbrico se refiere a los dispositivos o sistemas inalámbricos colocados en ubicaciones fijas, tales como en una oficina o una casa, a diferencia de dispositivos móviles, tales como teléfonos inalámbricos y PDA. Los dispositivos inalámbricos fijos generalmente obtienen su energía de servicios públicos fijos, a diferencia de los dispositivos portátiles inalámbrico que obtienen su energía de baterías.

Entrega (Handoff): El proceso en el que una red inalámbrica transmite automáticamente una llamada móvil a un sitio célula adyacente con una señal más fuerte.

Hertz: Una medida de energía electromagnética, equivalente a una "onda" o ciclo por segundo.

Interconexión: Conectar una red inalámbrica a otra, tal como enlazar la red de un proveedor de servicios inalámbricos con una red de intercambio local.

Interoperabilidad: La habilidad de una red para coordinar y comunicarse con otras redes, tales como dos sistemas basados en diferentes protocolos o tecnologías.

LAN: La Red de Área Local (LAN) es una pequeña red de datos que cubre un área limitada, tal como un edificio o grupo de edificios. La mayoría de las LAN conectan estaciones de trabajo o computadoras personales. Esto permite a muchos usuarios compartir dispositivos, tales como impresoras de rayo láser así como datos. La LAN también permite comunicación fácil, facilitando el correo electrónico (e-mail) o respaldando sesiones de conversación (chat).

Megahertz: Megahertz (MHz) es una unidad de frecuencia equivalente a un millón de hertz o ciclos por segundo. Las comunicaciones inalámbricas móviles en los Estados Unidos ocurren en las bandas de 800 MHz, 900MHz y 1900MHz.

Paquete de Datos: Información que es reducida en piezas o paquetes digitales de bytes, para que puedan viajar más eficientemente a través de las ondas aéreas de radio y las redes inalámbricas.

Repetidora: Dispositivos que reciben una señal de radio, la amplifican y retransmiten en una nueva dirección. Utilizados en las redes inalámbricas para extender el rango de las señales de la estación base y expandir la cobertura. Las repetidoras son típicamente utilizadas en edificios, túneles o terreno difícil.

Antena Inteligente: Una antena inalámbrica con tecnología que enfoca su señal en una dirección específica. Las redes inalámbricas utilizan antenas inteligentes para reducir el número de llamadas caídas, y para mejorar la calidad de las llamadas y la capacidad de canal.

Distribución del Espectro: Proceso por medio del cual el gobierno federal designa las frecuencias para usos específicos, tales como servicios de comunicaciones personales y seguridad pública. La asignación es generalmente lograda a través de largos procedimientos FCC, los cuáles intentan acomodar cambios en la demanda y el uso del espectro.

Espectro Disperso: Un método para transmitir una señal de radio dispersándola sobre un amplio rango de frecuencias. Esto reduce la interferencia y puede incrementar el número de usuarios en una banda de radio frecuencia.

Tecnología Inalámbrica: Término general para el uso del espectro de radio frecuencia para transmitir y recibir comunicación de voz, de datos y video.

Internet Inalámbrica: Término general para utilizar servicios inalámbricos para obtener acceso al Internet, correo electrónico y/o el World Wide Web.

IT Inalámbrica (Tecnología de Información Inalámbrica): El monitoreo, manejo y solución de equipo de computación a través de una red inalámbrica.

Red Inalámbrica de Área Local (WLAN): Utilizando tecnología de radio frecuencia (RF), las WLAN transmiten y reciben datos de forma inalámbrica en una cierta área. Esto permite a los usuarios en una zona pequeña transmitir datos y compartir recursos, tales como impresoras, sin conectar físicamente cada computadora con cables o alambres.

WLL (Centro Local Inalámbrico): WLL es un sistema que conecta usuarios inalámbricos con la red de teléfono de conmutador público (PSTN) utilizando tecnología inalámbrica y otro sistema de circuitos para tratar de completar la "última milla" entre el usuario inalámbrico y el equipo de intercambio. Los sistemas inalámbricos frecuentemente pueden ser instalados más rápidamente y más baratos que los sistemas cableados tradicionales.

Wi-Fi: Fidelidad inalámbrica. Nombre y logo dado por la Alianza Inalámbrica de Compatibilidad Ethernet (WECA) a proveedores de sistemas inalámbricos cuyos Puntos de Acceso conforman con el estándar 802.1b.

WLAN: Red de Área Local Inalámbrica.

ANEXO B

RESUMEN DE ESTANDARES

A. 802.11e: La nueva especificación inalámbrica

Hasta ahora las conexiones inalámbricas no habían sido capaces de dar prioridad a ciertas transmisiones, lo que provocaba saltos al reproducir música o vídeo.
La nueva especificación inalámbrica 802.11e, mejorará las conexiones de vídeo y voz, además ha recibido la aprobación del Institute of Electrical and Electronics Engineers.
La especificación es un conjunto de tecnologías que darán prioridad a cierto tráfico y podrán prevenir colisiones y retrasos, por lo cual mejorará la experiencia VoIP para usuarios con redes en el hogar.
La especificación 802.11e permite que varios bloques de información sean transmitidos por red con prioridad para cuatro clases de tráfico: voz, vídeo, entornos, y best-effort. Las cuatro clases de tráfico pueden ser cambiadas, los bloques darán especial importancia a las transmisiones de voz. Esta nueva especificación parece ser un buen comienzo para estandarizar las prioridades en las redes inalámbricas LAN, el único problema parece ser es que marca el correo electrónico como "alta prioridad".

B. 802.11h:

El objetivo es cumplir los reglamentos europeos para redes WLAN a 5 GHz. Los reglamentos europeos para la banda de 5 GHz requieren que los productos tendrán control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

C. 802.11i: Nuevo estándar permitirá el avance de las redes inalámbricas

La aprobación del estándar 802.11i, por parte del Institute of Electrical and Electronic Engineers (IEEE), cierra el ciclo de una serie de mejoras que eran necesarias en las

comunicaciones inalámbricas, como parte integral de las redes empresariales. Aunque, según los analistas de la consultora Gartner, aún persisten importantes desafíos, como por ejemplo, la interoperabilidad a través de diversos proveedores y tipos de redes.

"La aprobación del estándar 802.11i es un paso importante hacia la legitimación de las redes inalámbricas de área local (WLANs), ya que usa algoritmos criptográficos más fuertes y reduce el número de paquetes involucrados en la administración de claves. Pero aún quedan desafíos significativos", señalaron los especialistas.

802.11i está basado en el componente de autenticación 802.1X, que invoca uno de dos métodos de encriptación: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP, Protocolo de Código de Autenticación de Mensaje Encadenado de Bloqueo de Cifrado), parte del algoritmo de Advanced Encryption Standard (AES, Estándar de Encriptación Avanzado); o bien el Temporal Key Integrity Protocol (TKIP, Protocolo de Integridad de Clave Temporal).

Desde Gartner sostienen que "las empresas no han desplegado extensamente el encuadre 802.1X en sus redes; además, las alternativas dentro del 802.1X permite a los fabricantes escoger opciones de implementación que no son necesariamente interoperables. Por esta razón, la mayoría de las implementaciones serán únicas para sus vendors hacia fines de 2004, y la promesa de interoperabilidad con otros vendors se basará oportunamente en una prueba estructurada de un subset de 802.11i y 802.1X llamado Wi-Fi Protected Access 2 (WPA2)".

Sin embargo, señala Gartner, WPA2 fue sólo parcialmente definido. Su predecesor, WPA, que soporta sólo TKIP con la adición de CCMP es la base para las primeras versiones del WPA2. El dispositivo de prueba inicial incluirá EAP-TLS (Extensible Authentication Protocol-Transport Layer Security, ó Protocolo de Autenticación Extensible - Seguridad por Capa de Transporte) a través de los servidores y clientes de autenticación de Microsoft y Funk Software. La actualización futura de WPA2 -que podría, confusamente, también ser denominada WPA2- soportará tipos de EAP, y otros vendors como Cisco Systems y Meetinghouse Data Communications".

Para Gartner, la versión final de WPA2 ostenta la actual promesa de interoperabilidad, pero su futuro aún es una incógnita, pues la Wi-Fi Alliance, que certifica los productos WLAN, no publicó aún la matriz de testeo. "Mientras tanto, sin embargo, 802.11i como

estándar implementado propietariamente dentro de cada vendedor podrá al menos proveer un marco de trabajo para una cantidad de niveles de seguridad para una red inalámbrica segura", agregan.

Gartner recomienda a los compradores de equipos WLAN que soliciten en los equipos la conformidad con 802.11i. Si bien se necesita de la certificación del estándar 802.11i de parte de la Wi-Fi Alliance en la forma de WPA2, esto no significa que por ahora soporte interoperabilidad. Si se desean interoperabilidad, es importante monitorear las releases de de parte de la Wi-Fi Alliance para que se logren prácticas de certificación más rígidas.

Para la mayoría de las instalaciones, la encriptación basada en TKIP será suficiente y trabajará mejor con equipamiento propietario. Que las empresas soporten 802.11i implica soporte de autenticación 802.1X, lo que derivará en estrategias para su uso tanto en autenticaciones de redes cableadas como inalámbricas. Las empresas que persigan esta integración enfrentarán problemas de divergencia cuando traten de reconciliar la interoperabilidad de vendors con 802.11i y deban planificar de acuerdo a eso.

BIBLIOGRAFIA

1. Mischa Schwarts , “Redes de Telecomunicaciones”
   Ed. McGraw-Hill - Julio 2003

2. Wireless Networks International Inc.
   http://www.wininc.com

3. IEEE
   http://www.domodesk.com/content.aspx?co=87&t=132&c=44

4. Nicolás Baran, “Redes Inalámbricas”,
   Revista PC/Tips Byte - Abril 1992

5. Adam Engst; Glenn Fleishman, “Introducción a las redes inalámbricas”
   Ed. Anaya Multimedia - Julio 2003

6. Gast, Matthew S. , “Redes Wireless 802.11”,
   Ed. Anaya Multimedia - Noviembre 2005