UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

REDES DE DATOS INALÁMBRICAS - WLAN

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

MILTON ADRIÁN ÁLVAREZ DÍAZ

PROMOCIÓN 1998 - II

LIMA – PERÚ

2003

Dedicatoria:

A mi hermano Ossián por toda la ayuda y el apoyo.

A mis padres, hermanos, y familiares por su apoyo de siempre.

A mi buena amiga Shella por su apoyo en la realización del informe.

REDES DE DATOS INALÁMBRICAS - WLAN

ÍNDICE

INTRODUCCIÓN

Las Redes de Datos se han convertido sin lugar a duda, en la herramienta fundamental de acceso a los Sistemas de Información, Bases de Datos Programas de Aplicaciones, Internet, etc., quienes son muy indispensables actualmente para la operación y gestión de las empresas. Estas redes se han desarrollado normalmente en un entorno cableado, donde la utilización de cables de cobre de tipo coaxial, UTP (Unshielded Twisted Pair), STP (Shielded Twisted Pair), ó cables de Fibra Óptica, han sido los preferios por los Administradores de Redes, utilizando normalmente tecnologías LAN como Ethernet, Token Ring y en algunos casos FDDI.

Las Redes de datos inalámbricas surgen como parte del desarrollo de las comunicaciones de datos, con el fin de ofrecer a los usuarios el oportuno y rápido acceso los sistemas de información, además de proveer mecanismos sencillos de implementación. Actualmente las Redes de Datos Inalámbricas – WLAN, ya cuentan con soluciones de acceso a usuarios con velocidades de hasta 11Mbps para el estándar 802.11b, además de mecanismos para garantizar Roaming, Seguridad y Gestión de la Red.

Sin embargo a lo ya desarrollado por WLAN, esta tecnología sigue en constante desarrollo esperándose contar pronto con productos que sustentados en el estándar 802.11a puedan brindar velocidades de acceso de hasta 54Mbps, con esta meta de hecho no será sorpresa que en los próximos años el acceso a redes de datos mas usado sea el inalámbrico.

CAPÍTULO I

PANORAMA DE REDES DE DATOS ACTUALES

Actualmente en Comunicaciones de Datos se manejan varios conceptos y tecnologías los cuales se fueron introduciendo como parte del rápido desarrollo tecnológico: Redes LAN (Local Area Network), Redes WAN (Wide Area Network), Seguridad de las redes, Gestión de Redes, Redes Multiservicio, Redes de banda ancha, Fibra óptica, WDM y DWDM, ATM, redes de datos inalámbricas y otros más. De hecho cada plataforma y tecnología se está desarrollando constantemente, dando lugar a nuevos productos con el fin de tener cada vez redes más rápidas, de fácil crecimiento, de fácil gestión, fácil implementación, que tengan gran nivel de seguridad y sobretodo que la relación costo beneficio sea la mas adecuada.

1.1. Redes de Area Local – LAN (Local Area Network)

Las Redes de Area Local más desarrolladas y conocidas actualmente son: FDDI, Token Ring y Ethernet, siendo esta última tecnología la mas usada permitiendo ahora velocidades no-solo de 10Mbps, sino, de 100Mbps (Fast Ethernet), 1Gbps (Gigabit Ethernet), y ya se tiene en estudio acceso hasta de 10Gbps.

Actualmente en la implementación y diseño de redes LAN se están considerando además de HUBs o concentradores, equipos Switchs, los cuales permiten

aumentar el desempeño de la RED debido a la posibilidad de segmentar la misma y tener control de acceso de usuarios al nivel 2 de OSI (MAC – Media Access Control). Técnicas como Fragment Free, Store and Forward aplicadas a los switchs, han permitido que el envío y recepción de paquetes sean más eficientes, dependiendo fundamentalmente del tipo de implementación requerido por los usuarios.

1.2. Redes De Area Extensa - WAN (Wide Area Network)

Las redes de área extensa cubren grandes regiones geográficas como una ciudad, un país, un continente o inclusive el mundo. Actualmente con el ingreso de la fibra óptica además de contar con los enlaces satélites se tienen enlaces de fibra óptica submarina y se utilizan para enlazar puntos que distan grandes distancias entre sí.

Con el uso de una WAN se puede conectar por ejemplo desde Perú con USA, y se puede tener acceso además de aplicaciones de datos, servicios de voz y videoconferencia, sin embargo la implementación de una red de área extensa no es muy sencilla, se utilizan además de plataformas de equipos como multiplexores, switches, equipos SDH ó PDH, plataformas de interconexión como de acceso satelital y de fibra óptica. El mejor ejemplo de una red de área extensa es Internet.

Las Tecnologías de transporte de redes WAN más desarrolladas y conocidas son Frame Relay, ATM (Asynchronous Transmision Mode) y SDH. Actualmente las

empresas proveedoras de servicio utilizan SDH o ATM como transporte en la Red Core , y hay una tendencia a usar estás tecnologías en la distribución y en el acceso, pudiendo ofrecer en ATM una gran variedad de velocidades que van desde 2Mbs, 25Mbs, 34Mbs y hasta 155Mbs.

1.3. Gestión de RED

Para la gestión de la RED el objetivo de las empresas es tener plataformas más robustas con el fin de que los operadores puedan tener información en tiempo real sobre el estado de la Red, los equipos, y los usuarios finales. En el ámbito de protocolos se están haciendo mejoras constantes, el protocolo SNMP (Simple Network Managemente Protocol) tiene a la fecha desarrollada la versión 3, presentando mejoras respeto a la predecesora versión 2.

En el ámbito de gestión muchos proveedores tratan de incluir dentro de sus plataformas de gestión herramientas que permiten: medir el consumo de tráfico, tener reportes de facturación, configurar los equipos, detectar y manejar fallas, manejar el inventario de la red y algunos además tienen la opción de medir índices de desempeño de la RED.

1.4. Seguridad de Redes.

La integración de Redes y Servicios ha dado grandes facilidades en el sentido de poder contar con la mayor cantidad de información de la manera más rápida, sin

embargo este acontecimiento ha hecho a las redes más vulnerables. Con el objetivo de poder obtener información y negociar con la misma, o con el fin de sabotear redes y sistemas de información los *hackers,* o conocidos como piratas de red, intentan constantemente acceder a los sistemas de fuentes de información más importantes, como en Bancos, Compañías de Seguro, Entidades del estado, etc.

Tecnologías como las de Encriptación de datos, VPN (Virtual Private Network) para la creación de redes privadas sobre redes públicas, RADIUS (Remote Authentication Dial-In User Service) para autentificar a usuarios móviles, IDS (Sistemas de Detección de Intrusos), Firewalls para la seguridad de redes y otros; permiten además de cuidar la vulnerabilidad de la red tanto de usuarios externos como internos, detectar las operaciones de los mismos, permitiéndonos de esa manera redoblar esfuerzos en pro de la seguridad de nuestros sistemas de información.

1.5. Velocidad de Acceso y Ancho de Banda

La opción de transmitir información de voz, datos y videoconferencia ha hecho que las grandes compañías desarrollen equipos y tecnologías que procesen gran cantidad de información y transmitan a grandes velocidades; tecnologías como ISDN, ATM, SDH, DWDM, WDM y otros han dado auge a las telecomunicaciones, pudiendo actualmente mediante DWDM transmitir información a una velocidad de hasta de 40-Gbit/sec (OC-768).

Las telecomunicaciones en general se mueven alrededor de miles y millones de dólares con una gran cantidad de proveedores de equipos, proveedores de servicios y soluciones de comunicación. En el campo de la investigación las empresas e instituciones invierten grandes cantidades de dinero un tanto para mejorar los productos que ofrecen al mercado, en otra parte con el fin de posicionar un nuevo producto, y por otro lado para desarrollar nuevas tecnologías, dentro de este conjunto aparecen las redes de datos inalámbricas, impulsadas desde 1990 por la IEEE, y con el objetivo de establecer un estándar, el ahora conocido 802.11.

CAPÍTULO II

INTRODUCCIÓN A LAS REDES DE DATOS INALÁMBRICAS - WLAN

Uno de los temas más importantes en la implementación de redes de datos es la facilidad con la que se implementa y se da soporte a las mismas, y este es un tema por el cual las Redes de Datos Inalámbricas WLAN (Wireless Local Area Network), está ganado popularidad frente a las redes de datos cableadas convencionales, y es que tal solo con una tarjeta y un equipo concentrador de acceso, sin necesidad de cableado podemos tener acceso a los aplicativos y servicios de la RED.

El Estándar actual para las redes de datos inalámbricas es el establecido en el documento IEEE 802.11 y fue diseñado como un sistema de transmisión que usando ondas de radio-frecuencia (RF), provee soluciones móviles de acceso, logrando reducir el costo de implementación (costo x usuario) en comparación de llegar al usuario en forma cableada.

El Estándar 802.11 trabaja en los dos niveles mas bajas de OSI es decir en la capa Física y en la capa de Enlace de RED (DataLink). Por lo tanto cualquier protocolo a aplicación de una capa superior por ejemplo TCP/IP no se verá afectada por la plataforma inalámbrica.

El estándar no solo define las especificaciones, sino también una gran variedad de servicios y/o características tales como:

- Soporte de transporte de servicios asíncronos y de tiempo crítico.
- Conectividad permanente con la red cableada vía el Sistema de Distribución.
- Selección de velocidades de transmisión.
- Soporte de la mayoría de aplicaciones del mercado.
- Servicios multicast. (Incluyendo Broadcast)
- Servicios de gestión de red.
- Servicios de registro y autentificación.

Además de se tiene ambientes de aplicación de acuerdo al objetivo de implementación:

- Para aplicaciones interiores tales como oficinas, centros de convención, aeropuertos, hospitales, plantas y residencias, y
- Para aplicaciones exteriores como estacionamientos, campos, conjuntos habitacionales, plantas y residencias.

Ya en el año 1997, la IEEE saco la primer versión del 802.11 y se constituyó como el primer documento aprobado para lo que viene a ser las Redes LAN Inalámbricas, estableciendo velocidades de 1 y 2Mbps. En Septiembre de 1999, se añadió el estándar 802.11b para entonces de alta velocidad y añadía otras dos velocidades desarrolladas (5,5 y 11Mbps), sin embargo a los cambios 802.11b se definió basado

en su predecesor 802.11, con cambios únicamente en la capa física, resultando lógicamente en velocidades más altas de transmisión y conectividad más robusta.

2.1. Áreas Críticas para las Redes de Datos Inalámbricas WLAN.

Para hacer frente a las necesidades de conexión, existen cuatro áreas críticas que los sistemas de conectividad inalámbricas deben cumplir:

- ***Altos rendimientos.*** En el mundo LAN cableado los usuarios normalmente trabajan a velocidades de 10/100 Mbps (Fast Ethernet). Al mismo tiempo, la potencia de la informática móvil y la riqueza de los contenidos en red no paran de crecer rápidamente. Por ello, todos los esfuerzos de la industria y los cuerpos de estandarización deben ir hacia la ampliación de la capacidad de las WLAN y evitar que se conviertan en un cuello de botella.

- ***Movilidad.*** Aunque siempre han existido los usuarios móviles, sólo ahora pueden estar conectados mientras se desplazan. Puesto que la mayoría de los actuales sistemas de hardware y software se diseñaron para usuarios fijos, dotar de la suficiente inteligencia a los sistemas de networking inalámbricos es una cuestión crítica a la hora de dar soporte a estos usuarios móviles, a fin de que estén conectados sin interrupciones del servicio.

- ***Seguridad.*** Dado que la transmisión de señales inalámbricas no puede ser limitada enteramente al espacio privado de una empresa, las WLAN han de contar con sistemas de seguridad fiables y sencillos.

- ***Gestión.*** Para garantizar el rendimiento, la movilidad y la seguridad, es fundamental proporcionar las herramientas apropiadas para configurar estas opciones, monitorizar las redes inalámbricas, localizar y solucionar problemas.

2.2. *Estándares y las Redes de Datos Inalámbricos*

Como en todos los segmentos del networking, lo ideal sería que existiera una sola norma para todos los productos inalámbricos, pero lo cierto es que el mercado WLAN hay al menos siete estándares. En sí esto no es algo negativo, pero el mercado es todavía demasiado estrecho como para soportar tantos protocolos.

Por ello, los principales fabricantes optan por apoyar a varios estándares al mismo tiempo. Si bien lo cierto es que, al día de hoy, la gran mayoría soporta 802.11b, la norma con mayor presencia en el mercado, van creciendo los compromisos con la nueva 802.11a e, incluso, con la europea HiperLAN2. Otros añaden a estas alternativas Bluetooth, ya sea para atacar el mercado empresarial o el doméstico.

Ratificado en Junio de 1997, IEEE 802.11 opera en la banda de 2,4 GHz y define el funcionamiento e interoperatividad de las redes inalámbricas a una velocidad de 2 Mbps, con una modulación de señal de espectro expandido por secuencia directa (DS). Este primer estándar es la base de dos nuevas especificaciones 802.11b y 802.11a, que se adaptan a las necesidades actuales de ancho de banda.

En la revista Computer World Perú [2] se menciona "802.11b domina hoy el mercado, con una cuota del 83,6 por ciento de las ventas durante el primer semestre de 2001, según NPD Intelligence. Gartner, por su parte, estima que, a finales de 2002, la tasa de penetración de las WLAN basadas en esta norma ascenderá al 50 por ciento de las corporativas. Además, para el 2005 la consultora prevé que el 95 por ciento de la PC notebooks estarán preparadas para trabajar en estos entornos, lo que potenciará su presencia también en Pymes y pequeñas oficinas."

802.11b funciona en la banda de 2,4 GHz, y se apoya en la técnica de modulación CKK (Complementary Code Keying). Está diseñado para proporcionar una velocidad de transmisión de entre 1 y 11 Mbps .

En agosto de 1999 los principales promotores de la tecnología DS formaron WECA (Wireless Ethernet Compatibility Alliance), encargada de certificar la interoperatividad de productos IEEE 802.11b; sólo un mes después adoptó WI-FI (Wireless Fidelity) como sello distintivo WiFi es un certificado de interoperatividad que aparece como logo en los productos testados.

802.11a alcanza una velocidad máxima de 54 Mbps y opera a 5 GHz. Emplea la técnica de modulación OFMD (Orthogonal Frequency Division Multiplex), cuya principal ventaja es la resistencia a los ecos multicamino típicos de los entornos móviles e interiores.

Otro estándar con una presencia muy limitada es OpenAir, arquitectura de espectro expandido FH (Frequency Hopping) a 2,4 GHz, que puede alcanzar velocidades de hasta 1,6 Mbps. En 1996 se creo WLI Forum (Wireless LAN Interoperability) para apoyar a está norma.

Bajo la denominación High Performance Radio Local Area Networks (HiperLAN) reúne la familia de estándares desarrollados por ETSI (European Telecommunications Standards Institute). HiperLAN1, ratificado en 1996, emplea la tecnología de modulación GMSK (Gaussian Minimum Shift Keying), solo porta velocidades de hasta 24 Mbps, opera a 5 GHz e incorpora parámetros específicos de calidad de servicio (QoS) que priorizan el tráfico de la red. Recientemente, ETSI ha aprobado las especificaciones técnicas para HiperLAN2, cuya tecnología de modulación es OFDM y soporta velocidades de hasta 54 Mbps. A fin de garantizar la interoperatividad entre este estándar y 802.11a, el comité BRAN (Broadband Radio Access Networks) de ETSI ha estado colaborando con IEEE. Esta norma europea es apoyada por HiperLAN2 Global Forum (H2GF).

Otro de los estándares de tecnología inalámbricas, pero orientado casi exclusivamente al mercado doméstico, es SWAP, inspirado en la norma de telefonía inalámbrica DECT (Digital European Cordless Telephone) y los algoritmos de networking de 802.11. La especificación SWAP (Shared Wireless Access Protocol), base de HomeRF, ofrece una velocidad de datos y voz digital de 1 Mbps.

Concebida inicialmente como una tecnología de conectividad inalámbrica de corto alcance para sincronizar datos entre PC, dispositivos de mano y teléfonos móviles, muchos de los 1.200 miembros del Bluetooth SIG (Special Interest Group) están intentando posicionar esta tecnología como networking inalámbrico. A pesar de que técnicamente no es un estándar WLAN, sino PAN (Personal Area Network), muchos fabricantes planean integrarla en sus soluciones de LAN inalámbricas, ya que emplea modulación FH y opera en la banda de 2,4 GHz. Sin embargo, actualmente no soporta verdadera topología de red y su configuración maestro / esclavo punto a punto de corto alcance es muy limitada. En cualquier caso, parece una tecnología destinada más a complementar que a competir con las actuales WLAN. Incluso su velocidad de 1 Mbps podría disuadir de adaptar Bluetooth en las redes domésticas hasta que la especificación 2.0 traiga 4 Mbps y la posibilidad de operar a mayores distancias.

2.3. Aplicaciones de las Redes de Datos Inalámbricas

Se aplican fundamentalmente en el campo empresarial, en el hogar y en las Redes Públicas, veamos.

- ***En las empresas*** donde reducir costos y dar un mejor servicio a los usuarios quienes demandan interacciones en cualquier lugar y en cualquier momento se hace necesaria la utilización de sistemas inalámbricos. La ausencia de cables se convierte en una ventaja competitiva, especialmente en oficinas temporales, cuando el cableado no es práctico o posible y para soportar usuarios móviles dentro de la corporación. También resultan de gran utilidad para ampliar el campo de acción de una red cableada.

  Además en general la movilidad que proporcionan es ideal para determinadas actividades y entornos como hospitales, almacenes, aeropuertos, fuerzas de venta, administración de redes, fabricación, consultoría, y construcción.

- ***En el hogar*** el mercado del WLAN se ve principalmente entusiasmado en el aspecto de interconectar los computadores personales, dado que hay hogares que ya no-solo cuentan con un solo computador personal. El formar estas pequeñas redes brindará además de las posibilidades de compartir elementos periféricos como impresoras, faxes, escáner, y otros, la facilidad de acceso a Internet compartido.

- ***En las redes públicas*** está empezando la utilización de WLAN para dar servicios públicos inalámbricos por parte de los operadores de

telecomunicaciones. Las empresas podrán contratar servicios de diseño, instalación y mantenimiento de LAN inalámbricas de los operadores, que están creando redes de 11 Mbps y en el futuro 54 Mbps para proporcionar un amplio catálogo de ofertas. Por ejemplo, instalando redes 802.11b en edificios de oficinas permitirá a las empresas integrar sus redes privadas y sus enlaces a Internet en el acceso WLAN.

CAPÍTULO III

ARQUITECTURA Y TOPOLOGÍA DE REDES LAN DE DATOS INALÁMBRICAS

La arquitectura y topología de WLAN define la interacción de enlace entre el usuario final y la estructura cableada de la red que alberga a los servidores de aplicativos, otros segmentos y otras partes de la red en general.

El estándar IEEE 802.11 soporta tres esquemas topológicos básicos (Ver Fig. 01):

- IBSS (Independent Basic Service Set)
- BSS (Basic Service Set)
- ESS (Extended Service Set)

Todas a su vez son soportadas en implementaciones de la capa MAC (Media Acces Control)

3.1 IBSS (Independent Basic Service Set)

En este esquema se incluye un conjunto de nodos o estaciones inalámbricas que se comunican directamente una a una en modo ad-hoc, ó peer-to-peer, formando una topología de malla completa o de malla parcial.

3.2 BSS (Basic Service Set)

En este caso la red consiste de al menos un punto de acceso conectada a la RED cableada y un conjunto de estaciones inalámbricas, estas a su vez confían su operación en el Punto de Acceso, quien permite a las estaciones tener todas las facilidades de la RED cableada: servidores, impresoras, Internet, etc. El Punto de acceso actúa como el servidor lógico de acceso para una celda de red LAN Inalámbrica (Ver Fig. 01).

3.3 ESS (Extended Service Set)

Es un conjunto de dos o más redes con esquema topológico BSS formando una sola sub-red. El estándar IEEE 802.11 soporta configuraciones topológicas ESS en la que múltiples celdas usan el mismo canal, y usan diferentes canales para aumentar el rendimiento de la RED (Throughput). Las celdas BSS pueden ser conectadas por recursos cableados o inalámbricos (Ver Fig. 01).

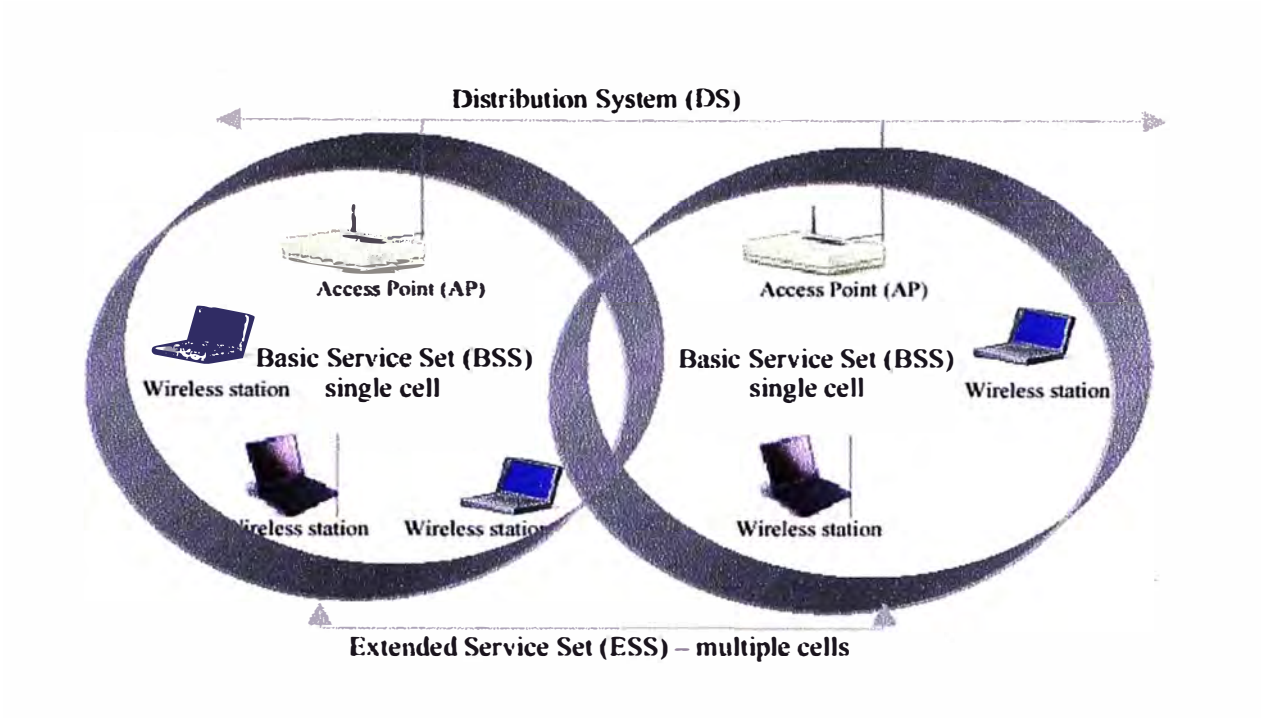

Fig 01.Topologías IEEE 802.11 BSS and ESS.

3.4 Componentes de una red WLAN (Wireless Local Area Network)

a. La estación Inalámbrica

Normalmente es una PC equipada con una tarjeta de interfaz de red inalámbrica. Las tarjetas de red inalámbricas a su vez se tienen el formatos ISA, PCI o para PC simple.

b. El Punto de Acceso

Consiste de una radio que contiene a su vez un punto de acceso a la red cableada de tipo IEEE 802.3, y un software con características de Bridging según estándar 802.11d.

El Punto de acceso actúa como la estación base para la red inalámbrica, permitiendo acceso para múltiples estaciones inalámbricas dentro de le red.

Una Red de Datos inalámbrica está basada en arquitecturas celulares. Cada celda BSS está conectada a la estación base o punto de acceso. Todos los puntos de acceso están conectados al Sistema de Distribución que es similar a un Backbone, usualmente Ethernet o también puede ser Inalámbrico. Todos los componentes mencionados son parte de los sistemas 802 para las capas superiores de OSI y son conocidas como ESS (Extended Service Set).

c. El Portal

El Estándar 802.11 no se sujeta para su desempeño de la composición del Sistema de Distribución, por ello podría no ser necesariamente compatible con el estándar 802. Si los frames de datos requieren transmisión hacia y desde una estación no compatible con el estándar LAN 802.11, luego estos frames entran y salen a través de un punto lógico llamado "Portal". El Portal provee integración lógica entre las existentes LAN cableadas y la LAN con estándar 802.11. Cuando un sistema de distribución está construido con componentes del tipo 802, como 802.3 (Ethernet) o 802.5 (Token Ring), entonces el Portal y el Punto de Acceso son el mismo dispositivo trabajando como un Bridge.

d. Sistema de Distribución

El Estándar 802.11 define el sistema de distribución como un elemento que interconecta elementos BSS dentro del ESS mediante puntos de acceso. El Sistema de Distribución soporta tipos de movilidad mediante la provisión lógica de múltiple BSSs. Un punto de acceso es una estación direccionable que provee

una interfase al sistema de distribución para estaciones localizadas dentro de varios BSSs. Las redes BSS y ESS son transparentes para la capa LLC.

CAPÍTULO IV

ANÁLISIS DEL ESTANDAR 802.11

4.1. La Capa Física 802.11, 802.11b y 802.11a.

En la Capa Física el estándar 802.11 define tres técnicas principalmente.

- Infrarojo Difuso (Diffused Infrared IR).
- Espectro Expandido por Salto de Frecuencia (FH o FHSS).
- Espectro Expandido por Secuencia Directa (DS DSSS).

Mientras la técnica infrarroja opera en banda base, las otras dos técnicas basadas en estaciones de radio pueden operar a 2,4 Ghz. Ellos pueden ser usados para redes inalámbricas sin hacer requerimiento de licencias para los usuarios finales.

4.1.1. Infrarojo Difuso (Diffused Infrared - IR).

La Técnica IR (Diffused Infrared), considera dos técnicas la Transmisión Fotónica y la transmisión IR propiamente dicha, veamos ambas.

Transmisión Fotónica Inalámbrica - Infrarrojo Difuso (IR).

Las implementaciones del tipo de transmisión fotónica en redes inalámbricas usan la banda de 850 a 950 Nm de la luz infrarroja con un pico de potencia de hasta 2Watts, y soporta de 1 a 2Mbps, y aunque soporta velocidades de transmisión mayores a los sistemas basados en RF, también tienen limitaciones.

- Está restringido a operar en línea de vista. Sin embargo el uso de propagación difusa puede reducir esta restricción permitiendo a las emisiones luminosas rebotar superficies de reflexión pasivas.
- La potencia está establecida a ser 2Watts y es bajo considerando el daño que podría causar al ojo humano, por ello las transmisiones están limitadas a valores alrededor de 25m.
- Los sensores receptores de señal deben de ser expuestos adecuadamente, de modo que la señal pueda ser recibida adecuadamente.

Una característica importante de las transmisiones fotónicas es que son inherentemente seguras y son inmunes (como lo son las redes de fibra óptica) a las radiaciones electromagnéticas que pueden interferir en sistemas cableados y de RF.

Infrarojo Difuso (IR)

Las comunicaciones Infrarrojas Difusas propiamente dichas son descritas como indirectas y de no línea de vista. La señal infrarroja difusa, que es emitida desde el transmisor, llena un área encerrada como luz y esto hace que

no necesariamente se requiera transmisión de línea de vista . Cambiando la posición del receptor no hará que se pierda la señal. Muchos productos de difusión infrarroja ofrecen también "Roaming", que permite conectar varios puntos de acceso a la Red de modo que cualquier computador personal pueda conectarse a través de estos puntos de acceso o moverse entre ellos sin perder conexión a la red. Usualmente IR provee acceso mas o menos de cobertura radial de 9 a 12 m y a velocidades de 1 hasta 2 Mbps.

4.1.2. Espectro Expandido por Salto de Frecuencia (FH o FHSS).

Los Sistemas RF de Espectro Expandido se puede decir son redes LAN inalámbricas que usan frecuencias de radio como medio físico para transmitir información. Existen dos principales subsistemas: Espectro Expandido por Salto de Frecuencia (FHSS) y Espectro Expandido por Secuencia Directa (DSSS).

Las transmisiones de espectro expandido toman una señal digital y la expanden o propaga de modo que la hace parecer mas como ruido aleatorio a una señal estándar de transmisión de datos. La codificación se realiza usando modulación FSK o PSK. Ambos métodos incrementan la magnitud de la señal de datos así como el ancho de banda, y aunque la señal aparece mas fuerte (Más ancho de banda) y fácil de detectar, la señal es inteligible y parece ser una señal de fondo ruidosa al menos que el dispositivo receptor se sintonice a los parámetros correctos de la señal de envío.

La técnica *Espectro Expandido por Salto de Frecuencia (FH ó FHSS)* propiamente *dicha* es similar a las transmisiones de radio FM, la señal de datos es superpuesta o llevada por una portadora de banda estrecha que puede cambiar de frecuencia. El estándar IEEE 802.11 provee 22 patrones de salto o desplazamientos de frecuencia para escoger de entre los 2,4Ghz de la banda ISM (Industrial, Científica, y Medica). Cada canal es de 1Mhz y la señal se debe desplazar en una razón de cambio constante (El estándar de los Estados Unidos es de 2,5 saltos/segundo). Esta tecnología modula una señal de radio desplazándola desde una frecuencia a otra, a intervalos aleatorios cercanos permitiendo proteger la señal de interferencias que se concentran alrededor de una sola frecuencia. Para decodificar la señal, el receptor debe de conocer la razón y secuencia de desplazamientos de frecuencia, proveyendo de esa manera seguridad y encriptación adicional.

Los dispositivos FHSS pueden enviar señales a velocidades desde 1,2 hasta 2 Mbps y pueden llegar a tener un alcance de hasta 1000km, además el ancho de banda puede incrementarse (hasta 24Mbps) instalando puntos de acceso múltiples en la RED.

Para el desplazamiento de frecuencia la banda de 2,4Ghz es dividida en 75 subcanales de 1Mhz. En orden de minimizar la probabilidad que dos transmisores vayan a enviar información en el mismo canal simultáneamente, saltos de frecuencia son usados para proveer un diferente patrón de salto por cada intercambio de información. El transmisor y receptor aceptan un patrón

de salto y la información es enviada en una secuencia de subcanales de acuerdo a lo establecido.

Las regulaciones FCC requieren de que cada subcanal sea de 1Mhz de modo que se fuerce a la técnica FHSS a expandir los patrones a través de la banda completa de 2,4Ghz, resultando de esa manera en mas posibilidades de saltos y en una mayor confiabilidad de la información.

4.1.3. Direct Sequence Spread Spectrum (DSSS)

La tecnología DSSS opera fundamentalmente tomando una cadena de ceros y unos y modulándolo con un segundo patrón denominado *Chipping Séquense* ó Código de Barker que es una secuencia de 11 bits (10110111000) usados para generar un patrón de bit redundante, la señal resultante aparecerá como un ruido de banda ancha para un receptor intruso.

Una de las ventajas de usar códigos expandidos es que aún se pierda uno o más bits durante la transmisión, técnicas propias del equipo de radio pueden recuperar la data original sin la necesidad de requerir retransmisiones.

La técnica de señalización para DS (Direct Séquense) divide la banda de 2,4Ghz en 14 canales de 22 Mhz, de los cuales 11 canales adyacentes se traslapan parcialmente, pero las restantes tres no. La información es enviada a través de uno de estos canales de 22Mhz sin intentar saltar otro, permitiendo

de ese modo el ingreso de ruido a la señal. Para reducir el número de retransmisiones y ruido, el Código de Barker es usado, para convertir cada bit de datos en una combinación de patrones de bit redundantes denominados *"chips"*. La inherente redundancia de estos patrones de bit, combinado con la expansión a través de canales de 22Mhz, provee de mecanismos adecuados para la detección y corrección de errores.

4.1.4. Capa Física y el Estándar 802.11b.

Las técnicas mencionadas para el estándar 802.11 proveen velocidades de 1 hasta 2Mbps, lógicamente esta velocidad es menor al especificado por el estándar 802.3 igual a 10Mbps. La única técnica que provee altas velocidades es DSSS que es usado como un estándar para las transmisiones a nivel físico soportando velocidades de 1 a 2Mbps y hasta velocidades de 5.5 y 11 Mbps.

El estándar original para 802.11 especifica los 11 bits del Código *de Barker*, para codificar la información, previa a la transmisión. Cada paquete de 11 bits representaban a un simple bit de datos (1 ó 0), el mismo que es convertido en un símbolo que se enviaba a través del aire. Estos símbolos son transmitidos a una velocidad de 1MSps es decir 1 millón de símbolos por segundo, usando una técnica sofisticada llamada BPSK (Binary Phase Shift Keying). Para las velocidades de 2Mbps se usa en cambio la técnica QPSK (Quadrature Phase Shift Keying), doblegando de ese modo la velocidad de transmisión usando BPSK.

Para incrementar la velocidad en el estándar 802.11b, en 1998, la empresa Lucent Technologies and Harris Semiconductor propusieron a la IEEE un estándar llamado CCK (Complementary Code Keying), CCK usa un conjunto de 64 palabras de código único, de 8 bits, de esta manera se requieren hasta 6 bits para representar una palabra (en lugar de un solo bit representado por un símbolo de Barker). Como un conjunto, estas palabras de código tienen propiedades matemáticas únicas que les permiten distinguirse uno de otro por un equipo receptor, aun en la presencia de ruido sustancial e interferencias multipath. (Un ejemplo es la interferencia causada de recibir múltiples reflexiones de radio dentro de un edificio)

Item	Velocidad de Transmisión de Datos	Longitud del Código	Modulación	Velocidad de Transmisión de Simbolos	Bits de Datos / Símbolo
1	1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2	2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
3	5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
4	11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Tabla 01. Especificaciones de Velocidad de Transmisión del Estándar 802.11b

La velocidad de transmisión de 5.5 Mbps usa CCK para codificar 4 bits por portadora mientras que para lograr velocidades de hasta 11Mbps codifica 8 bits por portadora. Ambas velocidades usan QPSK como una técnica de modulación y señalizan a 1,375MSps. QPSK usa 4 rotaciones (0,90,180 y 270 grados) para codificar 2 bit de información, mientras que BPSK codifica 1 en el mismo espacio.

El dilema está siempre en que se debe decidir entre incrementar la potencia o disminuir el campo de acción para mantener la calidad de la señal. Debido a que la FCC regula el nivel de potencia de los radios portátiles a 1Watt EIRP (Potencia Radiada Isotrópicamente Equivalente), el campo de acciones es el único factor que puede cambiar. Por ello para los dispositivos 802.11 mientras te alejas de la radio, esta se adapta y usa un mecanismo de codificación menos complejo para enviar información, resultando siempre en altas velocidades de transmisión de 1 a 11Mbps. (Ver Tabla 01)

4.1.5. Subcapas en la capa física

La capa física se subdivide en 2 subcapas, llamadas: PLCP (Physical Layer Convergence Protocol) y PMD (Physical Médium Dependent). (Ver Fig 2.)

Fig. 2. Formato del Frame Físico del Estándar 802.11b.

La Subcapa PMD es responsable de la codificación, la subcapa PLCP presenta una interfase común para escribir en manejadores de capas superiores y provee detección de portadoras y CCA (Clear Channel Algorythm) ó Evaluación de Canal Transparente, que es la señal que la capa MAC (Media Access Control) necesita para determinar sí el medio físico esta en uso. Veamos mas en detalle la subcapa PLCP.

a. Preámbulo PLCP.

La subcapa PLCP (Ver figura 2) contiene un preámbulo de 144 bits que es usado para sincronización de modo de determinar la ganancia de radio y establecer CCA (Para saber si el medio está en uso o no). Este es dependiente de la capa física e incluye:

- ✓ SYNC: Incluye una secuencia de 128 bits de ceros y unos alternados que son usados por la circuitería física para seleccionar la antena apropiada (Si la técnica de diversidad es usada), y para lograr correcciones y sincronizaciones de offset de frecuencia en estado estacionario con la señal de reloj del paquete recibido.

- ✓ SFD (Start Frame Delimiter): El delimitador de comienzo de frame consta de un patrón binario de 16 bits 1111001110100000, que es usado para definir el clock del frame y marca el comienzo de cada frame.

b. Cabecera PLCP.

La cabecera consiste de 48 bits, siempre es transmitido a 1 Mbps y contiene información lógica usada por la capa física para decodificar el frame (Ver figura 2). Consiste de:

- ✓ Signal: Compuesta de 8bits que contienen información de la velocidad, codificada en incrementos de 0.5 Mbps desde 1 Mbps a 4.5 Mbps;
- ✓ Service: Compuesta de 8 bits de uso reservado
- ✓ Length: Compuesto de 16 bits que representa el número de bytes contenidos en un paquete (usado por la capa física para la correcta detección del final del paquete).
- ✓ Header Error Field Check: Que consiste de 16 bit CRC de los 48 bits de cabecera.

La subcapa PLCP introduce 24 bytes de overhead dentro de cada medio ethernet. 802.11b reduce la eficiencia de la capa física en un 15% porque los 192 bits de cabecera son transmitidos a un Mbps.

4.1.6. Capa Física y 802.11a

Diferente a la operación del estándar 802.11b, 802.11a fue diseñada para operar en la mas reciente distribución de frecuencias especificada por la UNII (Unlicensed National Information Infrastructure) en la banda de 5 GHz. Diferente a la banda ISM que ofrece alrededor de 83 MHz en el espectro de 2.4 GHz, el estándar 802.11a utiliza casi 4 veces mas lo ofrecido por la banda ISM, porque la banda UNII ofrece 300 MHz de espectro relativamente libre de interferencias.

También 802.11a a diferencia de su predecesor utiliza la técnica FDM (Frequency Division Multiplexing), que es considerada más eficiente en medios de transmisión de edificio a edificio (Inter-building).

La FCC a asignado 300 MHz de espectro para UNII en el bloque de 5 GHz, 200 MGz de los cuales están dentro de 5,105 MGz a 5,350 MGz, con los otros 100 MGz dentro de 5,725 MGz a 5,825 MGz.

La primera ventaja de 802.11a sobre 802.11b es que este estándar opera en el espectro de 5.4 GHz, que le da las ventajas de desempeño propio de las altas frecuencia. Diferente a la frecuencia, la potencia irradiada y la distancia juntas están en relación inversamente proporcional, por ello trasladarse desde puntos de operación de 2.4 GHz al espectro de 5 GHz conduce a distancias más cercanas y/o requerimientos de mas potencia. Es por ello que el 802.11a incrementa la EIRP a un máximo de 50mWatt. El espectro de 5.4 MGz es dividido en tres dominios de trabajo y cada cual tiene restricciones para el máximo de potencia a trasmitir.

La segunda ventaja reside en la técnica de codificación, 802.11a usa un esquema de codificación llamado COFDM ó OFDM (Coded Orthogonal Frequency División Multiplexing). Cada subcanal en la implementación COFDM tiene un ancho de alrededor 300 KHz. COFDM trabaja dividiendo una portadora de alta velocidad de datos en varias subportadoras de baja velocidad, que son luego trasmitidas en paralelo. En nuestro caso cada

portadora de alta velocidad tiene un ancho de 20 MGz y es subdivididos en 52 subcanales cada uno aproximadamente de 300 KHZ de ancho. COFDM usa 48 de estos subcanales para datos, mientras que los restantes 4 son usados para corrección de errores.

Cada subcanal en la implementación COFDM tiene un ancho de hasta 300Khz y para codificar 125Kbps usando BPSK se logra transmitir a 6 Mbps. Usando QPSK es posible codificar hasta 250Kbps por canal que combinado permite hasta 12 Mbps. Y usando hasta 16 niveles de modulación por amplitud y cuadratura codificando 4 bits por hertz, el estándar especifica se pueden lograr velocidades básicas de 6, 12 y 24 Mbps, las cuales teóricamente deberían ser soportadas por todos los equipos que cumplen con el nuevo 802.11a. Velocidades de transmisión de 54Mbps son logradas usando la técnica de modulación 64QAM, lo que permite 8bits/10bits por ciclo, y un total de hasta 1,125 Mbps por cada canal de 300Khz, desarrollando con los 48 canales una velocidad de 54 Mbps. La velocidad máxima teórica de la técnica COFDM es 108Mbps.

4.2. Capa MAC IEEE 802.11, 802.11b and 802.11a

La capa MAC es muy similar al implementado en el estándar 802.3, donde se soporta un conjunto de usuarios en un mismo medio, y se espera que un usuario detecte el medio antes de enviar información. De la misma manera al igual que Ethernet posee de un mecanismo de detección de colisiones

CSMA/CD, 802.11 tiene un mecanismo para controlar el acceso de múltiples usuarios. Vemos mas en detalles además de los servicios brindados por la capa MAC el mecanismo para controlar colisiones

4.2.1. Servicios Brindados por la capa 802.11 MAC

La capa MAC, provee de variados servicios para gestionar autentificación, de-autentificación, seguridad en la comunicación y transferencia de información. Los servicios y características son como se verá muy similares a los del estándar 802.x.

a. Autentificación

El Servicio de autentificación es el proceso de proveer al cliente inalámbrico de una identidad que será requerida en la conexión a un AP. Por defecto los dispositivos IEEE 802.11 operan en sistemas abiertos, donde un cliente inalámbrico puede conectarse a un AP sin verificar credenciales. Una real autentificación es posible con el uso de la opción del estándar 802.11 denominado *Wired Equivalent Privacy* - WEP, donde una clave única es configurada tanto en la estación cliente inalámbrica como en el AP. Solamente los dispositivos con la clave valida tendrán las facilidades de asociarse al AP.

b. De-autentificación

La de-autentificación se desarrolla en la estación requerida para comunicación o en el PA, y es un proceso que consiste en denegar las credenciales del cliente, basado principalmente en el incorrecto establecimiento de parámetros de autentificación o en la aplicación de filtros de IP ó direcciones MAC.

c. Asociación

El Servicio de Asociación habilita el establecimiento de enlaces inalámbricos entre clientes inalámbricos y puntos de acceso.

d. Re-asociación

La re-asociación ocurre adicionalmente al servicio de asociación cuando el cliente inalámbrico se mueve desde un BSS a otro. Dos BSS adyacentes forman un ESS, y si los mismos están definidos por un mismo ESSID, proveen a un cliente inalámbrico con la capacidad de roaming al trasladarse de una área a otra. En el estándar 802.11 la asociación es un servicio implementado, sin embargo los mecanismos que permiten coordinación de AP a AP para manejar roaming aun no están especificados.

e. Privacidad

Por defecto la información es trasferida transparentemente permitiendo a cualquier dispositivo 802.11 escuchar tráfico de la misma capa fisica

802.11 y dentro del campo de acción cubierto. La opción WEP encripta información antes de que sea enviada inalámbricamente usando un algoritmo de encriptación de 40bits conocido como RC4. La misma clave usada para la autenticación es usa para encriptar o des-encriptar la información permitiendo a clientes inalámbricos con la misma clave compartida descifrar la información correctamente.

f. Transferencia de Información

El servicio primario de la capa MAC es proveer intercambio de frames entre capas MAC. Los clientes inalámbricos usan el algoritmo "Acceso Múltiple de Detección de Colisión con Evasión de Colisión" (CSMA/CA) como esquema de acceso al medio.

g. Distribución

La función de distribución es desarrollada por el método de secuencia directa DS y es usada en casos especiales de transmisiones de frames entre puntos de acceso.

h. Integración

Esta es una función desarrollada por *el portal*, que es diseñada para proveer información lógica entre las existentes LANs cableadas y las LANs 802.11.

i. Gestión de potencia

El estándar 802.11 define dos modos de potencia: Un modo activo, donde un cliente inalámbrico es alimentado para transmitir y recibir; y el modo de almacenaje de potencia, donde un cliente no es capas de transmitir o recibir, consumiendo menos potencia. El consumo actual de potencia no es un aspecto definido y depende del tipo implementación.

4.2.2. Acceso Múltiple por Detección de Portadora con Detección de Colisión (CSMA/CD)

El clásico método CSMA/CD es un mecanismo muy eficiente en un medio cableado, permitiendo operar en velocidades hasta de 1 Gbps Ethernet. Sin embargo este mecanismo permite conflictos (colisiones) y soporta mecanismos exponenciales de concesión del medio, reduciendo el desempeño en un muy competitivo medio bajo la presencia de número considerable de usuarios activos. Niveles de colisión de 30% y 40% , algunas veces menores, podrían causar significante degradación de desempeño global de los usuarios activos. Por otro lado el algoritmo de concesión podría postergar la transmisión de información hasta en 367 ms en la red de 10 Mbps.

Crear un mecanismo para prevenir conflictos potenciales en un medio compartido ha sido siempre un desafío para los diseñadores de red. Un conjunto de diferentes propuestas y anteproyectos están disponibles, inicialmente para redes cableadas y últimamente para medios inalámbricos, basados en las llamadas técnicas de evasión de colisión. La idea principal es

negociar el intercambio de información antes de que la colisión suceda, o forzar a los usuarios no activos a postergar su traspaso de información por un periodo de tiempo. La primera aproximación provee mecanismos adicionales para reducir retardos basados en colisiones, permitiendo colisiones en la fase de negociación y proveyendo por ello transferencia de información libre de colisiones. La segunda aproximación esta basada en procedimientos de "handshaking ", (timeslots), o técnicas de "polling". Ambas aproximaciones negocian con colisiones tempranas y tardías, al igual que las estaciones activas adyacentes y lejanas. Sin embargo, diferente al caso de redes cableadas, CSMA/CD, no puede ser implementada para redes inalámbricas por dos principales y obvias razones. Primero en CSMA/CD, uno de las sugerencias básicas es que todas las estaciones se escuchen a sí mismas, diferente a las redes WLAN, donde esto no puede ser garantizado. Hay un efecto denominado "Hidden Station" donde la estación escucha al punto de acceso pero no escucha a todos los miembros de la celda. En segundo lugar, no es posible para ambos transmitir y recibir en el mismo canal usando transductores de radio, al menos que usemos sistemas de radio operando en full dúplex lo que incrementarían los precios significantemente.

4.2.3. Acceso Múltiple por Detección de Portadora con Evasión de Colisión (CSMA/CA)

En este tipo de acceso CSMA/CA, trata de evadir colisiones usando la evidente confirmación de un paquete (ACK).

En la capa MAC, el estándar 802.11 para CSMA/CA define dos métodos diferentes de coordinación de acceso: La función de coordinación distribuida (DCF) y la función de coordinación de punto opcional (PCF), siendo está última la usada en 802.11b.

a. Función de coordinación de punto opcional (PCF)

La función de coordinación de punto opcional es usada para implementar servicios de tiempos críticos como voz y video. La PCF es opcional y es provista en 802.11 para asegurar servicios libres de enfrentamiento. En PCF, un único punto de acceso controla el acceso al medio y un coordinador de punto reside en el AP. Si un BSS es configurado con la característica PCF habilitada, el tiempo para el acceso es intercalado entre el sistema configurado en PCF y el configurado en modo DCF, que es una técnica clásica para compartir los tiempos, y que incluye un coordinador central.

Durante los periodos en los que el sistema esta en modo PCF, el punto de acceso sondeará cada estación indagando su requerimiento de transmisión de información, y después de un lapso de tiempo dado se trasladará a la siguiente estación, proveyendo una latencia máxima garantizada. Debido a esta aproximación, PCF provee retardos más bajos de transferencia, esencialmente excluyendo el posible control de colisión. Ninguna estación

está permitida de trasmitir al menos que haya sido consultada o sondeada; y las estaciones reciben información desde el punto de acceso solamente cuando son consultados o sondeados. Usando este modo de acceso de prioridad mas elevada, el punto de acceso publica los requerimientos de sondeos a las estaciones para la trasmisión de información.

Una limitación de PCF es que no es particularmente escalable debido a que un único punto de acceso tiene control de acceso al medio y debe consultar a todas las estaciones, lo cual puede ser inefectivo en redes grandes. PCF es esencialmente utilizado para transmisión asíncrona de datos, voz y aplicaciones mixtas e incluye mecanismos de enfrentamiento y libre de enfrentamiento, alternando los modos de operación libre enfrentamiento – libre enfrentamiento y enfrentamiento enfrentamiento sobre el control PCF. El vector NAV (Network Allocation Vector) es usado para prevenir saturación o enfrentamiento de tráfico hasta que la última transferencia en modo PCF reinicie la función usando "Reset Nav" en el último frame (CF_End) desde el AP.

b. Función de Coordinación Distribuida

Esta fundamentalmente usado en CSMA/CA. DCF opera cuando estación requiere transmitir información, esta censa el medio previamente, si esta ocupado, posterga la transmisión a un tiempo posterior pero si el medio esta libre para un tiempo especificado (Denominado Espacio entre Frame

Distribuido - DIFS), la estación transmite. La estación receptora luego revisa el CRC del paquete recibido y envía un paquete de confirmación (ACK), esta recepción indicará a la estación transmisora que no hubo detección de colisión. Si el transmisor no recibe el paquete ACK luego se considera que ha ocurrido una colisión, después del cual la información es reenviada en un tiempo aleatorio posterior.

Para aclarar si un canal esta ocupado o no, el algoritmo CCA (Clear Channel Algorythm) es usado. Este mide la energía de una señal en una antena y define la potencia de la señal recibida, si la potencia es menor al de un valor de umbral establecido, el canal es considerado libre, y la capa MAC adquiere el estado CTS; y si la potencia es mayor que el valor de umbral la transmisión de información es postergada de acuerdo a los protocolos de la regla de acceso específica. El Estándar 802.11 define un método adicionales para detectar si el medio está o no ocupado, y que puede ser usado independiente de la información de la potencia, este método es más electivo considerando que es usado para verificar el mismo tipo de la frecuencia de portadora como en la especificación de 802.11. Cual método es el mejor depende el tipo de implementación que se requiera y del nivel de ruido en el área de trabajo.

4.2.4. El efecto "Hidden Station" ó Estación Escondida.

El efecto "Hidden Station" ó "estación escondida" es una situación típica en WLAN donde las estaciones no se escuchan entre ellas pero si al AP.

El efecto de la estación escondida podría causar una colisión en cualquier fase en el proceso de transmisión – recepción. Para reducir la probabilidad de colisión de dos estaciones el estándar define un mecanismo denominado Virtual Carrier Sense (Ver Fig 3).

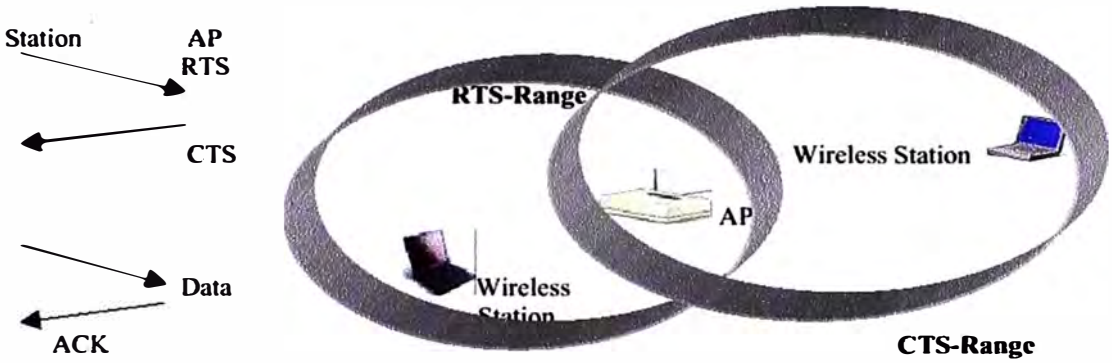

Fig. 03. El Efecto de la Estación Escondida.

Virtual Carrier Sense. Una estación antes de transferir información enviará primero un paquete pequeño de control denominado Request To Send (RTS) que incluye la fuente, destino y la duración de la siguiente transacción. Si el medio esta libre la estación de destino responde con un paquete Clear To Send (CTS) que incluye la misma información de duración. Las estaciones reciben o su RTS y/o CTS, y fijan su indicador de detección de portadora virtual (NAV, Network Vector Allocation), por el periodo de duración especificado. Este mecanismo reduce la probabilidad de colisión en un área de recepción con una estación que está "escondida" de la estación transmisora para el pequeño tiempo de duración de la transmisión RTS dado que las estaciones al escuchar el CTS consideran reservado el medio hasta el final de la transmisión.

La información del tiempo de duración del RTS también protege el área de transmisión de colisiones durante el ACK básicamente por estaciones que están fuera del rango de la estación transmisora del ACK.

Debido a los pequeños frames RTS y CTS, este método también reduce el overhead de colisiones. Si el paquete es significativamente más grande que el RTS, el paquete puede ser transmitido sin la transacción RTS/CTS. La estación controla el proceso fijando el lumbral de RTS.

El nodo de transmisión **A** (Ver Fig. 04), envía un requerimiento RTS al punto de acceso solicitando reservar una cantidad tiempo fijo necesario para transmitir un frame de un tamaño de longitud específico. Cuando el medio esta disponible, el punto de acceso Broadcasts un mensaje CTS que todas estaciones pueden escucharlas, de ese modo **B** tiene la cantidad solicitada de tiempo.

La característica de umbral RTS incrementa la disponibilidad de ancho de banda eliminando tráfico RTS/CTS desde el aire, de esta manera reduciendo costo de transmisión. Fijando el umbral de la longitud de RTS a un máximo valor, el transmisor efectivamente nunca usará RTS y la opción es virtualmente apagada. Si la estación escondida no es un problema, el umbral puede ser apagado o desactivado. Un ejemplo se puede apreciar en la figura 04. Si un usuario decide activarlo fijando algunos umbrales hay un compromiso entre introducir mas overhead y reducir la retransmisión de

mensajes debido al problema del nodo escondido. La situación en la que RTS/CTS es útil es en los medio externos punto – multipunto en la que el problema de nodo escondido puede llegar hacer uno mas grande.

El siguiente diagrama (Ver Fig. 04) muestra como el mecanismo RTS/CTS trabaja para **A** como un transmisor (o estación T), **B** como un receptor (o estación R) y los valores fijados de NAV para sus vecinos.

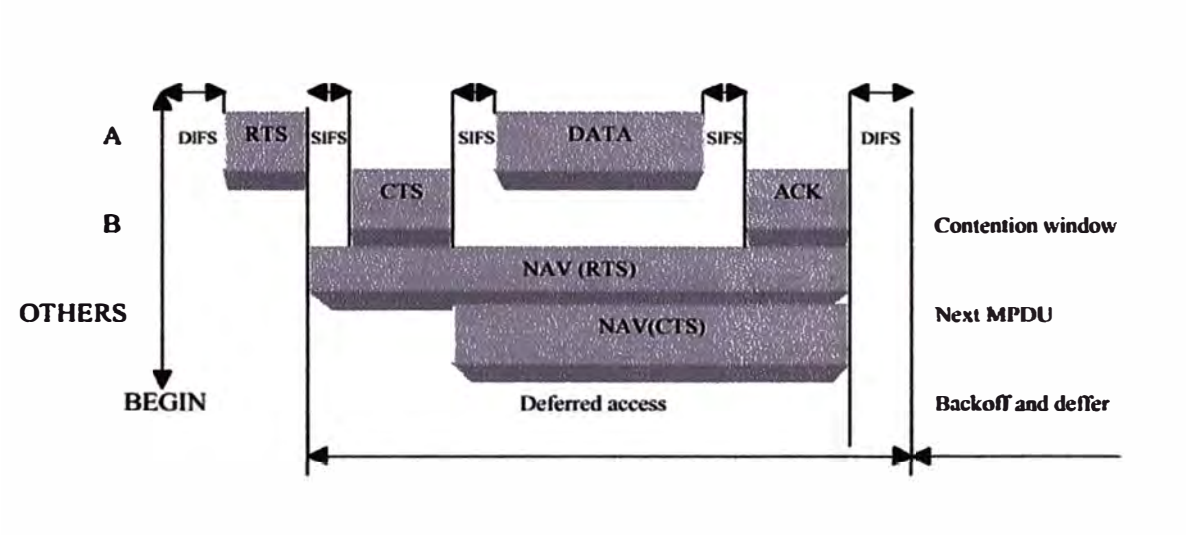

Fig. 04. El Estado de vector NAV asociado con la detección de la portadora física para indicar la disponibilidad del medio.

4.2.5. Acknowledgements de capa MAC

Los paquetes típicos ethernet son de varios cientos de bytes, siendo el paquete más grande hasta de 1,518 bytes, sin embargo sep podría decir que en medios LAN inalámbricos es mejor usar paquetes más pequeños debido a las siguientes razones:

- Debido a la elevada razón de bit de error y al comportamiento propio de los enlaces de radio. la probabilidad que un paquete se vuelva corrupto incrementa mientras más grande es el paquete.
- Para el caso en que los paquetes tornen corruptos, mientras más pequeño es el paquete, hay menos overhead para retransmitir.
- En el uso de las técnicas FHSS el medio es interrumpido periódicamente (por 20ms) para saltar, de modo que mientras más pequeño es el paquete menor es la probabilidad de que las transmisiones sean pospuestas.

A pesar de ello, no tiene mucho sentido introducir un protocolo acorde solamente con paquetes pequeños, de modo que un mecanismo de fragmentación / re-ensamblaje es añadido a la capa MAC. El mecanismo es un algoritmo simple de *Envio-y-Espera*, donde la estación transmisora no esta permitida enviar un nuevo fragmento hasta que sucede una de los siguientes eventos: la estación recibe un ACK por el fragmento enviado, o decide que el fragmento a sido retransmitido muchas veces y da de baja todo el paquete. El estándar permite a la estación transmitir a una dirección diferente entre retransmisiones para un segmento dado, esto es muy bien usado cuando el punto de acceso tiene varios paquetes en espera para diferentes destinos y uno de ellos no responde.

El estándar define cuatro tipos de espacios interframe para proveer diferentes prioridades.

a) SIFS (Short Inter Frame Space) Es usado para separar transmisiones pertenecientes a un único diálogo (Fragmentar - ACK) y este es el espacio mínimo interframe. En este caso hay a lo más una estación que requiere transmitir en cualquier tiempo, dándole por ello completa prioridad sobre todo las otras estaciones. Este valor para la capa física 802.11 se fija a 28 ms, tiempo suficiente para que la estación transmisora sea capaz de cambiar al modo de recepción y pueda decodificar el paquete entrante.
b) PIFS (Point Cordination IFS). Es usado por el AP para ganar acceso sobre el medio antes que cualquier otra estación. El valor es SIFS + Slot Time, por ejemplo 78 ms.
c) DIFS (Distributed IFS). Es el espacio Interframe usado por una estación que desea comenzar una nueva transmisión, que es calculada como PIFS + One Slot Time, por ejemplo 128ms.
d) EIFS (Extended IFS). Es el IFS de mayor longitud usado por una estación que a recibido un paquete que no puede entender. Este es usado para prevenir a la estación de colisiones con un futuro paquete del mismo dialogo en curso.

4.2.6. Algoritmo "Extended Backoff Algorithm"

802.11 define un algoritmo exponencial de concesión que debe ser ejecutado en los siguientes casos: cuando la estación percibe el medio antes de la

primera transmisión del paquete, y el medio esta ocupado; después de cada transmisión; y después de una transmisión satisfactoria. El único caso cuando este mecanismo no es usado es cuando la estación decide transmitir un paquete nuevo y el medio a estado libre por mas de un espacio DIFS.

Concesión es un método muy conocido usado para resolver enfrentamiento entre diferentes estaciones esperando acceder al medio. Este método requiere que cada estación escoja un número aleatorio (n) entre cero y un número dado (16 para 802.3), cargar este número X tiempos de slot. El tiempo de slot es definido como el mecanismo en la que una estación siempre es capaz de determinar si otra estación accedió al medio al comienzo del slot previo. Cada estación escucha a la red, y la primera estación que termina sus números asignados de tiempo de slot comienza su transmisión.

Si alguna otra estación escucha a la primera estación hablando o enviando información, esta para de descontar su tiempo de concesión. Cuando la red está disponible nuevamente, esta reanuda la cuenta de su tiempo de slot disponible.

Adicionalmente al algoritmo básico de concesión, 802.11 añade un contador de concesión que asegura ecuanimidad. Cada nodo comienza un contador aleatorio de concesión mientras espera transmitir. Este cronometro va marcando hasta llegar a cero mientras espera transmitir. Cada nodo obtiene

un nuevo contador aleatorio cuando este quiere transmitir. Este contador no es reseteado hasta que el nodo a transmitido.

4.2.7. Tipos de Frame

Hay tres tipos principales de frame usados en la capa MAC: Data, Control y Gestión. Los Frames del tipo Data son usados para transmisión de datos. Los Frame de Control son usados para controlar acceso al medio (ejemplo RTS, CTS y ACK). Los frames de Gestión son transmitidos de la misma manera que los frame de Datos para intercambiar información de Gestión, pero no son enviados hacia capas superiores (ejemplo frame de aviso). Cada tipo de frame es subdividido en diferentes subtipos de acuerdo a su función especifica. (Ver Fig. 5 como referencia de una subcapa de frame)

Octets 2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Body Frame	CRC
			MAC header					

B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol Versión	Type	Subtype	To BS	From DS	More Frag	Retry	Pwr Mgm	More Data	WEP	Order
Bits 2	2	4	1	1	1	1	1	1	1	1

Fig. 05. Formato de Subcapa de Frame del MAC.

4.2.8. Capa MAC para 802.11 a

El estándar 802.11a usa las mismas funciones MAC que 802.11b, por ello heredar el formato MAC de 802.11 al 802.11a no tendrá impacto significativo en las operaciones de red. Sin embargo, existe un muy bien conocido

inconveniente del formato MAC 802.11, es que, mientras la capa física va logrando mayor potencia y un nuevo esquema de codificación, el formato MAC va reduciendo el efecto debido a un significante overhead, causado por el objetivo y las tendencias de diseño de proveer un medio libre de colisiones y eficiente. Considerando ciertas deficiencia de la capa MAC del estándar 802.11b, las velocidades esperadas para el 802.11a están en el rango de 38 Mbps, hasta 54 Mbps. Diferente al conocido 802.11b, 802.11a no requiere que las cabeceras (headers) sean transmitidos a un Mbps, que teóricamente podrían incrementar la eficiencia esperada de rendimiento en 15%.

4.3. Roaming, Asociación y Movilidad.

La capa MAC 802.11 es responsable por la forma como un cliente se asocia con un punto de acceso. El estándar incluye mecanismos que permiten a un cliente trasladarse entre múltiples puntos de acceso que pueden estar operando en el mismo canal o en otros. Cada punto de acceso transmite una señal de aviso que incluye una marca de tiempo para sincronización del cliente, un mapa de indicación de tráfico, una indicación de velocidades de información soportadas, y otros parámetros. Los clientes desplazándose usan la señal recibida para medir la fuerza de enganche de sus conexiones existente con el punto de acceso. Si la conexión es considerada débil la estación trasladándose puede intentar asociarse así misma con un nuevo punto de acceso. La estación trasladándose primero ejecutará una función de rastreo para localizar un nuevo punto de acceso en el

mismo canal o en otro diferente ó usa información de exploraciones ó rastreos previos.

Lo que ocurre realmente cuando un usuario se desplaza desde un punto de acceso a otro es:

a. La estación envía un requerimiento de re-asociación a un nuevo punto de acceso.
b. Si la respuesta de re-asociación es satisfactoria la estación cambia hacia este nuevo punto de acceso, de otra manera la estación busca otro punto de acceso.
c. Si un punto de acceso acepta un requerimiento de asociación, el punto de acceso indica su nuevo estado de re-asociación al sistema de distribución, actualizando su información, de ese modo el anterior punto de acceso es notificado del cambio a través del sistema de distribución DS.

La re-asociación usualmente ocurre cuando la estación inalámbrica ha sido desplazada considerablemente del punto de acceso original, causando la debilitación de la señal. En otros casos, la re-asociación ocurre debido a un cambio en las características de radio en el edificio, o debido simplemente a tráfico muy alto en la red en el punto de acceso original. Tráficos fuertes de red causan re-asociación que también se manifiestan como una función de balance de carga "load balancing". Este proceso de asociación dinámica y re-asociación con los puntos de acceso permite a un cliente establecer WLANs con muy alta

cobertura creando un conjunto de celdas 802.11b traslapadas a lo largo de un edificio o campus.

Técnicas de Roaming

En general las técnicas de Roaming, 802.11b se basan en la definición como una estación se asocia con su punto de acceso, no define como un punto de acceso rastrea usuarios así como ello se desplazan.

La primera característica es manejada por los protocolos Inter-AP especificadas normalmente por proveedor del equipo (IAPP). Si el protocolo no es eficiente lo más probable es que se tengan paquetes perdidos cuando un usuario se desplace desde un punto de acceso a otro.

Como alternativa una alternativa muy usada para los problemas de desplazamiento de capa 3, es implementar el protocolo Dinámico de Configuración de Hosts a través de la Red. DHCP permite a algunos usuarios que apagan o suspenden sus computadores portátiles al cruzar a una nueva red o subnet automáticamente obtener una nueva dirección IP cuando se reinicie o se encienda el computador. DHCP habilita a los Hosts en una red cargar y enviar un requerimiento DHCP (BOOTP) a una dirección broadcast con el objetivo de obtener una dirección IP para su uso.

Como ejemplo, el sistemas operativos IOS (Internetwork Operating System) de Cisco provee una innovadora característica llamada LAM (Local Area Mobility).

LAM es un mecanismo desarrollado por la necesidades de movilidad dentro de un medio empresarial donde DHCP no es disponible, o los hosts no tienen el software apropiado instalado. LAM considera direccionamiento estático Hosts/PCs, en este caso moverse desde una subnet local a otra ubicación dentro de la red de la empresa permite mantener la conectividad transparente sin cambios en el software o en los hosts, transformando el concepto de "Transparent Bridging" a "Transparent Routing".

La segunda característica esta relacionada a los mecanismos de Roaming en capa 3. El mas popular de estos mecanismos es Mobile IP, que es conocido actualmente como RFC 2002 por la IETF. El concepto de Mobile IP de Cisco que se sustenta en los RFCs 2002, 2003 Y 2006, ofrecen la mas completa solución en medios inalámbricos. Esto incluye ambientes con tecnología celular así como situaciones de redes LAN inalámbricas que podrían requerir Roaming. Mobile IP trabaja teniendo un punto de acceso asignado como el "Home Agent" para cada usuario.

Una vez que una estación inalámbrica abandona su "Home Area" y entra a una nueva, el nuevo punto de acceso pregunta a la estación por su "Home Agent". Una vez que este ha sido localizado el envío de paquetes se establece automáticamente entre los dos puntos de acceso para asegurar que la dirección IP del usuario se conserve y el usuario pueda transparentemente intercambiar información

4.4. WLAN y Consumo de Potencia de los Dispositivos.

En el entorno empresarial los equipos de computo de fácil transporte y móviles pueden normalmente utilizar tarjetas de red NICs en formato PCMCIA, por ello conectarse a la red corporativa vía una conexión inalámbrica no debería causar mucha incomodidad. Aunque el problema en la mayoría de los casos, es que estos dispositivos deben confiar su funcionamiento en baterías para aprovisionar de energía a los dispositivos electrónicos.

Adicionalmente al control de acceso al medio, la capa MAC 802.11b soporta características de conservación de energía para de esa manera extender la vida de la batería de los dispositivos portátiles. Esta técnica habilita a las interfaces de red inalámbricas cambiar a modos *standby* de bajo consumo de energía periódicamente cuando no hay transmisión de información, reduciendo el consumo de la batería.

El estándar soporta dos modos de utilización de potencia, llamados: *Modo de Alerta Continua y Modo de Elección de Guardado de Potencia.* La capa MAC implementa funciones para manejo de potencia poniendo la radio en estado durmiente cuando no ocurre actividad de transmisión por algún específico periodo de tiempo, este tiempo también puede ser definido por el usuario. Aunque un problema resultante del estado durmiente puede ser que se omita transmisión de información crítica, 802.11 resuelve este problema incorporando buffer para poner en cola los mensajes. El estándar en este caso sugiere para las

estaciones durmientes despertar periódicamente y recuperar cualquier mensaje pertinente, como las señales de aviso desde el punto de acceso. El aviso incluye información tomando en cuenta que estaciones tienen tráfico esperando por ellas, y el cliente puede de esa manera despertar bajo notificación de aviso y recibir su información, volviendo a dormir después de ello mas adelante.

4.5. Seguridad en el uso de WLAN

El tema de seguridad está asociado a los afecciones sobre la salud humana que pueda causar el uso de dispositivos inalámbricos.

Sobre el uso de estos dispositivos los proveedores establecen como punto de partida que las redes WLAN deben soportar estrictamente los estándares establecidos por las instituciones, gobierno e industria de cada país. A pesar de ello hay preocupaciones encontradas entre cierto número de industrias de tecnología inalámbricas, respecto a los riesgos sobre la salud. A la fecha estudios científicos no han sido capaces de atribuir efectos adversos para la salud a las transmisiones WLAN. Sin embargo la potencia de salida de las redes WLAN ya han sido limitada por las regulaciones FCC a niveles bajo 100 mw (en las serie de producto Cisco Aironet 340/350 se tiene 2-30 mw), mucho menos que lo estable para telefonía móvil.

Actualmente se tiene la hipótesis que se podría tener efectos negativos para la salud en tanto se opere muy próximo a dispositivos como puntos de acceso o

antenas. Como regla se recomienda mantenerse alejado 10cm de las partes transmisoras y receptoras.

CAPÍTULO V

ANÁLISIS DE LA SEGURIDAD DE REDES DE DATOS INALÁMBRICAS

Las redes LAN inalámbricas normalmente transmiten señales sobre áreas más grandes que aquellas de redes cableadas, por ello WLANs tienen también un área mayor que proteger. En el tema de seguridad ha habido un progreso significante en términos regulatorios y estándares, dirigido principalmente por el comité de estándares 802.11 y el IEEE 802.10, quienes son responsables de desarrollar todos los mecanismos de seguridad para las series LAN 802. Como resultado de su trabajo coordinado, IEEE 802.11 provee ya mecanismos para autentificación y encriptación.

En esquemas básicos de operación una estación inalámbrica IEEE 802.11 no procesará información sobre la red inalámbrica al menos que su identificador de red (Network ID), también llamado Basic Service Set Identification (SSID), sea el mismo que el de las otras estaciones de red. Enviado en cada paquete de datos 802.11, el identificador de red es una palabra código de 6 bytes que distingue una WLAN de la otra. Los puntos de acceso revisan el identificador de red cuando cada estación inicia una conexión a la red y si el identificador no es igual al almacenado en el AP la estación no podrá establecer una conexión a la WLAN. De esta manera, un intruso deberá obtener un identificador de red necesario para conectarse a la red.

Con el correcto identificador de red, cualquiera podría configurar un computador portátil con una tarjeta de radio apropiado y acceder a la WLAN, al menos que los servidores de aplicaciones requieran un *username* y un *password*.

5.1 WEP (Wireless Equivalent Protocol)

Un nivel de seguridad lo provee el protocolo Wireles Equivalent Privacy (WEP). El protocolo WEP provee al estándar 802.11b de un mecanismo para mantener la seguridad encriptando el tráfico y autentificando el acceso a los nodos.

Una característica de WEP llamada *Shared Key Authentication*, asegura que solo las estaciones autorizadas puedan acceder a la WLAN. Esta característica trabaja de la siguiente manera (Ver Fig. 06).

a) Una estación solicitadora de un servicio 802.11 envía un frame de autentificación a otra estación.
b) Cuando la estación recibe el frame inicial de autentificación, responde con un frame de autentificación conteniendo de 40 a 128 octetos de texto recusación.
c) La estación solicitadora copia el texto de recusación dentro del frame de autentificación, lo encripta con una clave compartida usando el servicio de WEP, y envía el frame a la estación que dio respuesta.

d) La estación receptora de-encripta el texto de recusación usando la misma clave compartida y lo compara con el texto de recusación enviado previamente. Si ambos son iguales, la estación receptora responde con una confirmación de autentificación, sino, la estación envía un aviso de autentificación negativa.

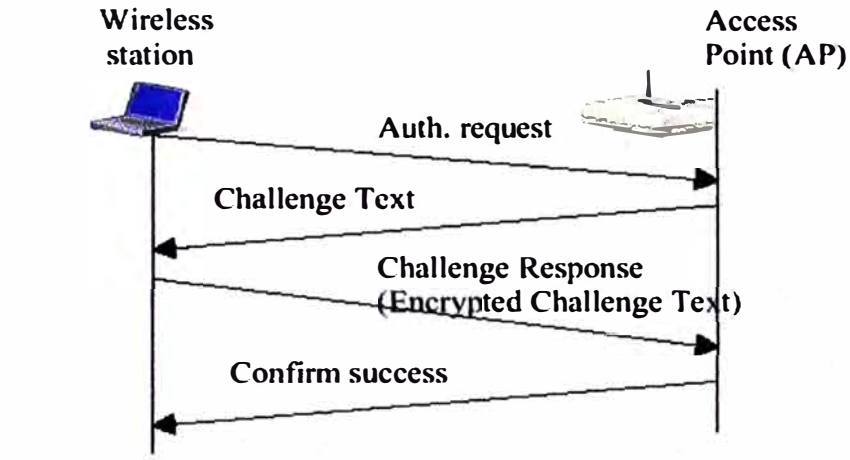

Fig. 06. Autentificación mediante clave compartida.

Para evadir problemas de escucha en WLAN, similares a los que puede hacer un sniffer en una red cableada, se usa WEP para encriptar las transmisiones entre estaciones y para evadir el descubrimiento de curiosos o intrusos. WEP usa la herramienta de encriptación RC4 y por defecto una clave de 40-bits. Las estaciones también podrían utilizar WEP sin servicios de autentificación pero las recomendaciones de seguridad es usar ambos WEP y autentificación para minimizar vulnerabilidad de la red a paquetes extraños.

Siempre que la encriptación y autentificación son incrementados en algunos sistemas tres cosas deberían ser consideradas: la necesidad de privacidad del usuario, facilidad de uso y regulaciones gubernamentales. El protocolo WEP RC4, usado en 802.11b es una tentativa para balancear todas las consideraciones mencionadas. El algoritmo de encriptación RC4 es un código de cadena simétrico que soporta una clave de longitud variable.

Para la mayoría de aplicaciones una Encriptación WEP de 40 bits realizada dentro de 802.11b debería ser suficiente, sin embargo, la parte débil de es mecanismo es el carácter estático de clave usado por WEP.

Para mostrar un ejemplo, la solución de seguridad de Cisco WLAN permite tipos de autentificación abiertos, de clave compartida y de redes EAP, y la clave puede tener 40 o 128 bits de tamaño. Cisco también recomienda para la seguridad de la WLAN, estar integrada dentro de una estrategia total de seguridad de red. En particular un usuario podría implementar encriptación de capa de red como IPSec a través de la parte cableada e inalámbrica de la red, eliminando en cambio la necesidad de tener mecanismos de seguridad 802.11. Otra alternativa para los usuarios es tener aplicaciones que encripten su propia información, por lo tanto asegurando que toda la información de la red como IP y las direcciones MAC sea encriptada junto con la carga útil de información.

Otras técnicas de control de acceso están disponibles adicionalmente a la técnica de autentificación 802.11 WEP. Algunos vendedores por ejemplo proveen una

tabla de direcciones MAC en una Lista de Control de Acceso para ser incluidas en el punto de acceso, restringiendo el acceso a clientes cuyas direcciones MAC se encuentran en la lista. Los clientes pueden luego ser explícitamente incluidos (o excluidos) bajo requerimiento. Debido a diferentes factores incluyendo regulaciones gubernamentales, WEP esta diseñado para seguridad moderada, y no como un protocolo avanzado de seguridad. La posición oficial del Grupo de Seguridad 802.11 es : "WEP no esta orientado a ser una solución completa de seguridad, pero, así como en el caso de seguridad en una LAN cableada, deberían ser suplementada con mecanismo de seguridad adicionales como los de control de acceso, encriptación end-to-end, protecciones mediante password, autentificación, redes privadas virtuales, y firewalls; siempre y cuando el valor de la información que es protegida justifique tal preocupación. El grupo de trabajo 802.11 esta actualmente desarrollando una extensión a WEP que será incorporada en la futura versión del estándar. Cualquier instalación IEEE 802.11 donde la privacidad de la información es una preocupación debería usar WEP".

5.2 La Norma 802.1x

Adicional al protocolo WEP, la IEEE se ha preocupado además de tener un mecanismo que pueda brindar encriptación, de una herramienta que pueda además brindar medios de autenticación centralizada que pueda ser más segura, desarrollando la Norma 802.1x.

La nueva norma 802.1x ayuda en la tarea proporcionando un mecanismo estándar para autentificar centralmente estaciones y usuarios. 802.1x será además lo suficientemente flexible para soportar distintos algoritmos de autentificación, y, como estándar abierto, facilitará a los fabricantes el desarrollo de innovaciones y mejoras complementarias.

Básicamente, 802.1X se apoya en el protocolo de autentificación EAP(Extensible Authentication Protocol), vinculados al medio físico de la red. Para ello, los mensajes EAP son encapsulados en mensajes 802.1X, creando lo que se conoce como EAP sobre LAN.

Esquema Funcional de 802.1x

La autentificación 802.1X para WLAN se basa en tres componentes principales: el solicitante (generalmente el software cliente), el autenticador (el punto de acceso) y el servidor de autenticación (por lo general, pero no necesariamente, un servidor RADIUS – Remote Authentication Dial-In Usser Service).

Cuando un supuesto cliente intenta conectar con el punto de acceso, éste le detecta y activa su puerto para proceder a la autentificación, al tiempo que le desautoriza a que transmita ningún tipo de tráfico salvo el relacionado con 802.x. El cliente entonces, utilizando EAP, envía un mensaje de inicio al punto de acceso, que, al recibirlo, devuelve un mensaje de petición de identidad.

El cliente le remite acto seguido un mensaje de respuesta con su identidad, que será pasado al servidor de autentificación. El resultado es un paquete de aceptación o rechazo que el servidor envía al punto de acceso, que, nada más recibirlo, vuelve a autorizar al puerto del cliente a que comience la transmisión.

Con este simple esquema centralizado de funcionamiento, 802.1x tiene el potencial de simplificar la gestión de la seguridad de grandes despliegues inalámbricos. Pero hay que recordar que la autentificación no es la única pieza del puzzle de la seguridad de los entornos 802.11su utilización requiere obviamente la presencia de un algoritmo de autentificación y de un sistema de encriptación de datos. Juntos, los tres componentes ofrecen a los administradores de redes un modo efectivo de proporcionar servicios de red móviles, flexibles, gestionables y escalables.

Operación de 802.1X

a. Cuando el cliente precisa realizar una transacción, envía antes un mensaje de "inicio" a un punto de acceso, el cual solicita su identidad e incapacita al puerto para cursar tráfico, salvo el relacionado con 802.x.

b. El cliente contesta con un paquete de respuesta que contiene la identidad, y el punto de acceso lo envía a un servidor de autentificación.
c. El servidor de autentificación envía un paquete de "aceptación" al punto de acceso.

d. El punto de acceso devuelve de nuevo el puerto del cliente a un estado autorizado y comienza la transmisión.

La nueva norma 802.1X proporciona un mecanismo estándar para autentificar centralmente estaciones y usuarios, simplificando así el soporte de cientos o miles de puestos. 802.1X será además lo suficientemente flexible para soportar distintos algoritmos de autentificación, y, como estándar abierto, facilitará a los fabricantes el desarrollo de innovaciones y mejoras complementarias.

CAPÍTULO VI

EQUIPOS DE REDES DE DATOS WLAN Y COSTOS.

Actualmente se tiene muchos proveedores que ofrecen equipos y soluciones de redes WLAN, en el Perú las mas conocidas con las provistas por Cisco Systems INC y 3COM. Para efectos del informe vamos a presentar los equipos recientemente desarrollados por Cisco System INC. con su Serie Cisco Aironet 350.

Dentro de la gama de productos de Cisco para sus soluciones de Redes WLAN Cisco presenta además de plataformas de Hardware una plataforma de Gestión de Seguridad. La gamma de productos comprende fundamentalmente:

- Adaptadores de RED para clientes de la serie Cisco Aironet 350.
- Puntos de acceso de la serie Cisco Aironet 350
- Bridge para trabajo en grupo de la serie Cisco Aironet 350
- Antenas y Accesorios Cisco Aironet
- Cisco Secure Access Control Server V.2.6 para Windows 2000 y NT

6.1. Adaptadores de RED para clientes de la serie Cisco Aironet 350.

Los adaptadores para clientes inalámbricos (Ver Fig. 07) conectan varios dispositivos a una red inalámbrica en modo directo cliente a cliente o en modo de infraestructura con puntos de acceso. Disponibles en los formatos PC Card (PCMCIA) y PCI, los

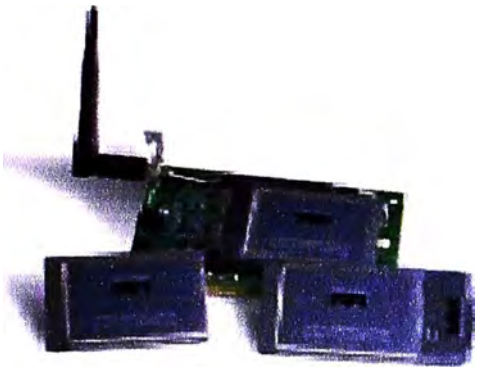

Fig. 07. Adaptadores de Red
Cisco de la Serie Aironet 350

adaptadores para clientes de la serie Cisco Aironet 350 conectan rápidamente los dispositivos informáticos de sobremesa y los dispositivos móviles de forma inalámbrica a todos los recursos de la red. Con este producto, es posible añadir al instante empleados nuevos a la red, admitir grupos de trabajo temporales o activar el acceso a Internet en las salas de reuniones o en otros espacios de encuentro (Ver Fig. 08).

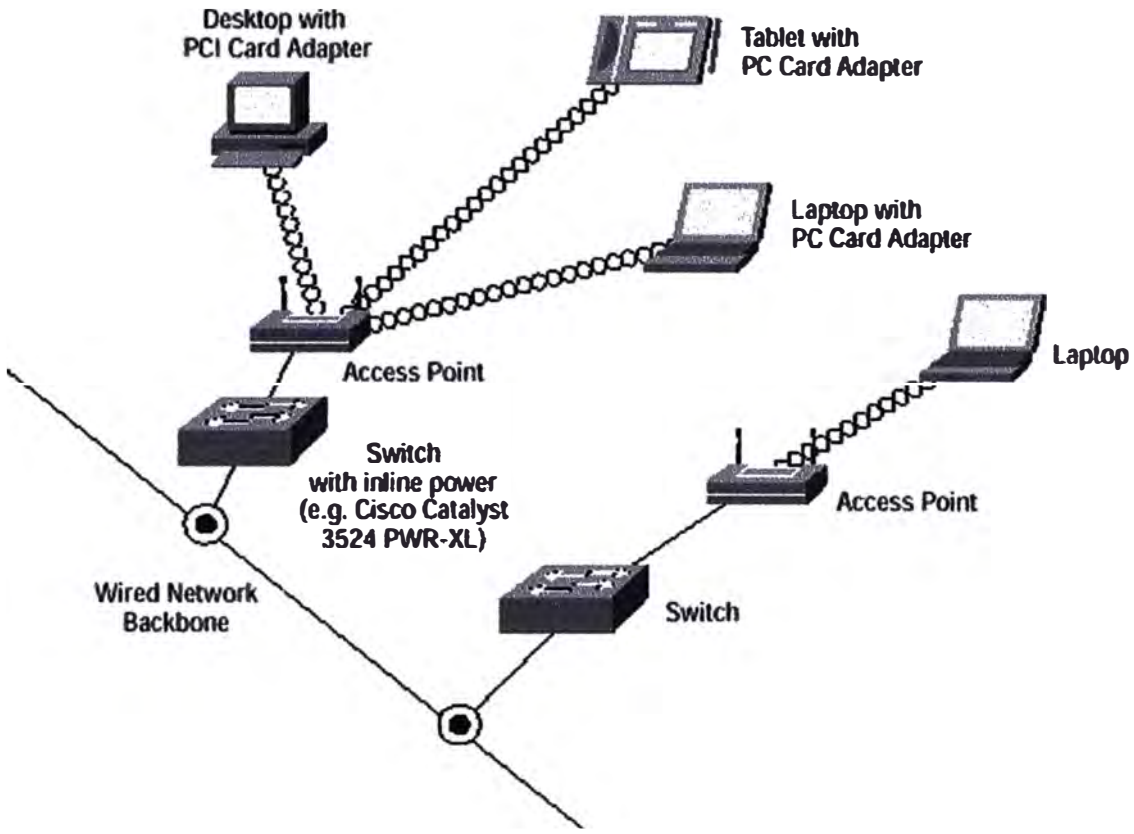

Fig. 08. Los dispositivos cliente equipados con adaptadores para clientes inalámbricos pueden desplazarse libremente a través de una instalación mediante las comunicaciones con varios puntos de acceso.

Sus características incluyen:

- Mayor alcance y transferencia.
- Comunicaciones seguras en la red.
- Modo global para la itinerancia internacional.
- Utilidades con gran número de prestaciones para facilitar la configuración y la administración.
- Compatibilidad con el estándar de alta velocidad IEEE 802.11b.
- Compatibilidad con los sistemas operativos más utilizados.

6.2. Puntos de acceso de la serie Cisco Aironet 350

Fig 09. Puntos de Acceso de la Serie Aironet 350.

El AP de la serie Cisco Aironet 350 (Ver Fig. 09) admite velocidades de datos de hasta 11 Mbps, es compatible con IEEE 802.11b y proporciona las siguientes características clave para satisfacer todos los requisitos de las empresas:

- Compatibilidad con la alimentación en línea a través de Ethernet que simplifica y reduce el costo total de instalación y propiedad.
- Diseño de radio de 100 Milliwatt (mW) de alto rendimiento, con capacidades de administración de alimentación que ofrecen la transferencia, el alcance y la fiabilidad líderes del sector.
- Arquitectura que resiste el paso del tiempo y que puede admitir actualizaciones de hardware de alto rendimiento y características de software adicionales que protejan la inversión.

Al igual que todos los productos de Cisco Aironet, la serie Aironet 350 admite las siguientes características de software:

- Los servicios del protocolo Extensible Authentication Protocol (EAP) basados en 802.1x que proporcionan una autenticación centralizada y basada en el usuario para la administración de seguridad sin problemas y la privacidad basada en el usuario.

- Selección automática de canales, protocolo Cisco Discovery Protocol (CDP), protocolo Dynamic Host Configuration Protocol (DHCP) y servicios BOOTP para simplificar la instalación y administración de las infraestructuras de WLAN.

- Servicios con alta disponibilidad, como el equilibrado de carga y la redundancia de espera en actividad para aumentar la fiabilidad y el rendimiento.

- Excelentes opciones de filtrado tanto en el lado Ethernet como en el de radio para ajustar el rendimiento y las aplicaciones, a fin de satisfacer los requisitos específicos de las empresas.

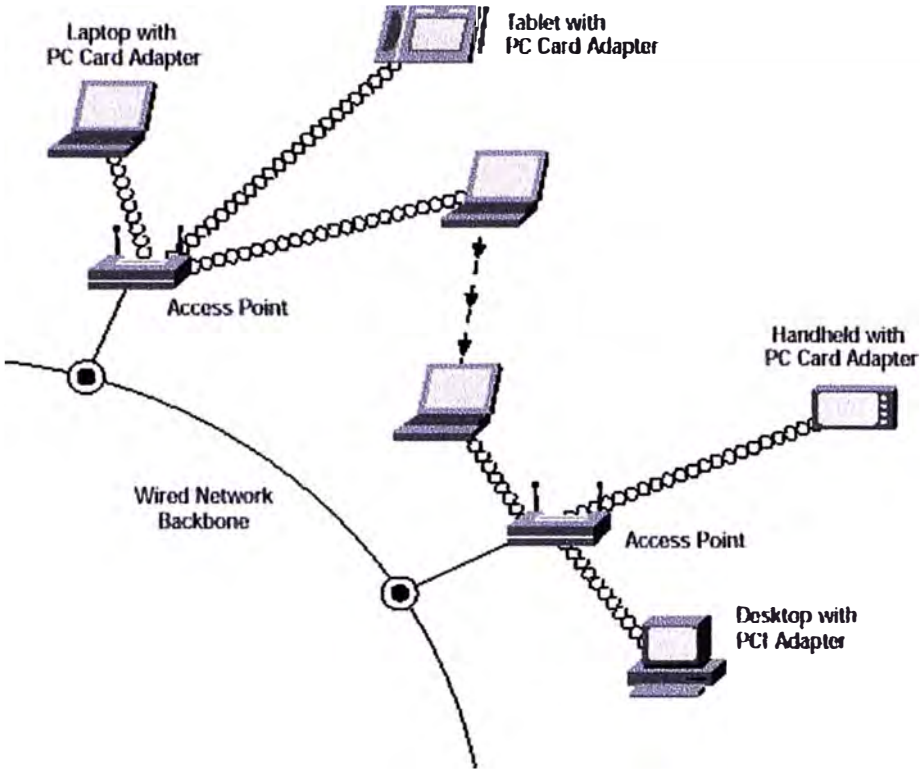

Fig. 10. Un AP es el punto central de todas las redes inalámbricas o un punto de conexión entre una red con cables y una sin cables. Pueden colocarse varios puntos de acceso en una instalación para proporcionar a los usuarios que tengan adaptadores de WLAN la posibilidad de moverse libremente a través de un área ampliada, al tiempo que se mantiene acceso ininterrumpido a todos los recursos de la red.

Instalación simplificada y menor costo total de instalación y propiedad

El punto de acceso de la serie Cisco Aironet 350 incluye un enlace ascendente Ethernet 10/100 para poder integrarse racionalmente con las LAN alámbricas existentes (Ver Fig. 10). Para reducir al mínimo los costos de instalación, el punto de acceso de la serie Cisco Aironet 350 obtiene la alimentación desde un puerto Ethernet (Ver Fig. 11). Esta configuración de alimentación en línea es compatible con el borrador del estándar de alimentación en línea 802.3af y funciona con todos los dispositivos de alimentación en línea de Cisco, como los switches Catalyst y los paneles auxiliares de alimentación en línea (Ver Fig. 12).

Para alimentar al punto de acceso de la serie Cisco Aironet 350 también se puede utilizar un inyector de alimentación en línea opcional (Ver Fig. 13).

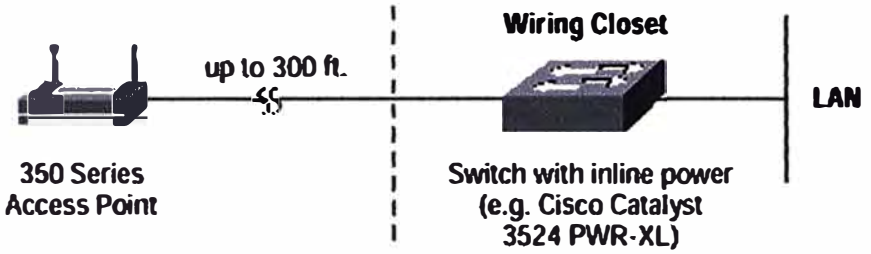

Fig. 11. El punto de acceso puede utilizar un switch Cisco Catalyst 3524-PWR-XL para su alimentación.

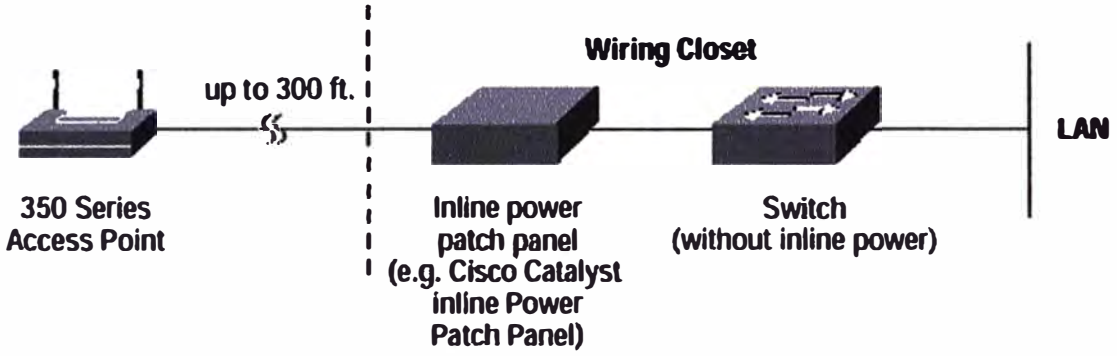

Fig. 12. Puede utilizarse un panel auxiliar de alimentación en línea Cisco Catalyst para alimentar al punto de acceso.

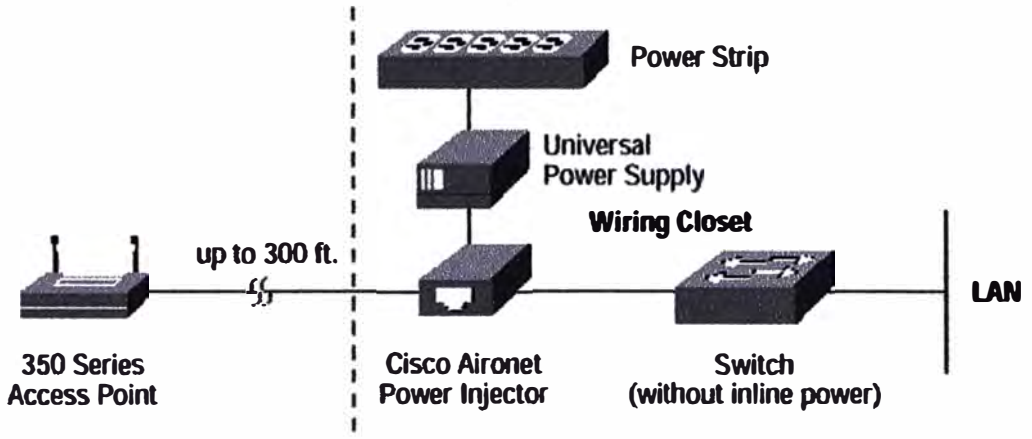

Fig. 13. Cisco también ofrece un inyector de alimentación para alimentar al punto de acceso de la serie Cisco Aironet I

Rendimiento de WLAN, alcance y fiabilidad líderes en el sector

La alimentación de transmisión y sensibilidad de recepción de 100-mW del punto de acceso de la serie Cisco Aironet 350 proporciona el mejor alcance y fiabilidad del sector. La diversidad de antenas y la duración del retardo (multiruta) de la serie Cisco Aironet 350 ofrecen un mejor rendimiento, incluso en condiciones extremas, como en almacenes, fábricas y edificios metálicos.

Los administradores también pueden configurar la potencia de transmisión de radio (1, 5, 20, 30, 50, 100 mW) de la serie Cisco Aironet 350 para satisfacer los requisitos específicos de cobertura y reducir al mínimo las interferencias. Una amplia cartera de antenas extraíbles para ampliar aún más el alcance y la disponibilidad.

Protección de la inversión

Para proteger la inversión de los usuarios, todos los puntos de acceso y los puentes de la serie Cisco Aironet 350 cuentan con suficiente memoria Flash para gestionar las actualizaciones del firmware de los próximos años.

Servicios de software para LAN inalámbrica necesarios para las aplicaciones de clase empresarial. Arquitectura de seguridad centralizada con administración dinámica de claves de sesiones

La seguridad es una preocupación principal en todas las instalaciones de WLAN. Los esquemas de seguridad inalámbrica de primera generación basados en SSID (Service Set Identifier) y la administración manual de claves WEP imponían importantes cargas administrativas que imposibilitaban las instalaciones a gran escala. La solución de Cisco lidera el sector al ofrecer una administración ampliable, basada en los estándares y centralizada de la seguridad que ofrece claves de cifrado dinámicas para un solo usuario y una sesión, integradas con el acceso a la red. La arquitectura de seguridad de Cisco se basa en el estándar propuesto por IEEE 802.1x para las redes inalámbricas. El estándar 802.1x es un esquema de seguridad ampliable que alberga varios métodos de autenticación y administración de claves. Los puntos de acceso de Cisco Aironet interoperan con servidores RADIUS con EAP activado, como Cisco Access Control Server 2000 versión 2.6 y adaptadores para clientes con EAP activado, como los clientes de la serie Cisco Aironet que proporcionan autenticación a nivel de usuarios a través de un enlace cifrado. Tras una autenticación mutua correcta con el servidor

RADIUS, el usuario deriva una clave de cifrado WEP dinámica que cifra de forma exclusiva el tráfico de dicho usuario a través del aire, lo que garantiza la seguridad tanto con relación a las fuentes exteriores como a los usuarios internos de la red. El servidor RADIUS ACS usa el protocolo LDAP (Lightweight Directory Access Protocol) o los servicios de ODBC para utilizar de modo óptimo la base de datos de identidades de la empresa y permite a los administradores de TI activar al instante la seguridad inalámbrica a todos los usuarios.

Administración integrada para la configuración, supervisión y solución de problemas

Para posibilitar una instalación, configuración y administración rápidas, en cualquier momento y en cualquier lugar, la serie Cisco Aironet ofrece servicios para simplificar la instalación y configuración. La serie admite la administración basada en Web y las características basadas en SNMP (Simple Network Management Protocol) que facilitan el control, la solución de problemas, la descarga de software y el registro de eventos. La opción de agilidad de frecuencia de la serie Cisco Aironet elimina las conjeturas de la configuración de los canales. En este modo, el punto de acceso rastrea de forma automática el área y selecciona el canal menos congestionado. El instalador no necesita conocer los parámetros de los restantes equipos inalámbricos del área de cobertura. Para la administración empresarial, la serie Cisco Aironet admite el protocolo CDP (Cisco Discovery Protocol) para habilitar el descubrimiento automático de los puntos de acceso y puentes de Cisco Aironet usando aplicaciones de

administración de empresas, como CiscoWorks 2000. Además, los puntos de acceso de Cisco Aironet admiten MIB (Management Information Base) II de SNMP estándar, MIB de la serie Cisco Aironet privada y MIB de 802.11b. Los puntos de acceso de la serie Cisco Aironet también pueden administrarse a través de la consola o de la interfaz Telnet.

6.3. Bridge para trabajo en grupo de la serie Cisco Aironet 350

Fig. 14. Bridge de la Serie Aironet 350

Diseñado para satisfacer las necesidades de los grupos de trabajo remotos, las oficinas satélites y los usuarios móviles, el puente o bridge (Ver Fig. 14) para trabajo en grupo de la serie Cisco Aironet ® 350 proporciona la libertad y flexibilidad de la conectividad inalámbrica a los dispositivos con activación Ethernet. El puente para trabajo en grupo conecta rápidamente un máximo de ocho portátiles con activación Ethernet a cualquier otra computadora portátil a una LAN inalámbrica (WLAN), y proporciona el enlace desde estos dispositivos a cualquier punto de acceso (AP) o puente multifunción de Cisco Aironet. El puente para trabajo en grupo de la serie Cisco Aironet 350 ofrece:

- Instalación sin controladores de un máximo de ocho dispositivos con activación Ethernet.
- Rendimiento y alcance óptimos.
- Seguridad centralizada basada en los estándares.
- Dos versiones para englobar a una amplia gama de requisitos de las aplicaciones.
- Utilidades con gran número de prestaciones y una sólida administración.

Compatibilidad con una gran variedad de aplicaciones

Cualquier dispositivo Ethernet, incluyendo impresoras, copiadoras, PC, dispositivos de punto de venta, o equipos de supervisión, puede ser ubicado directamente en su puesto de trabajo utilizando un puente para trabajo en grupo, sin necesidad de gastar dinero o perder tiempo en el cableado. En las aulas u

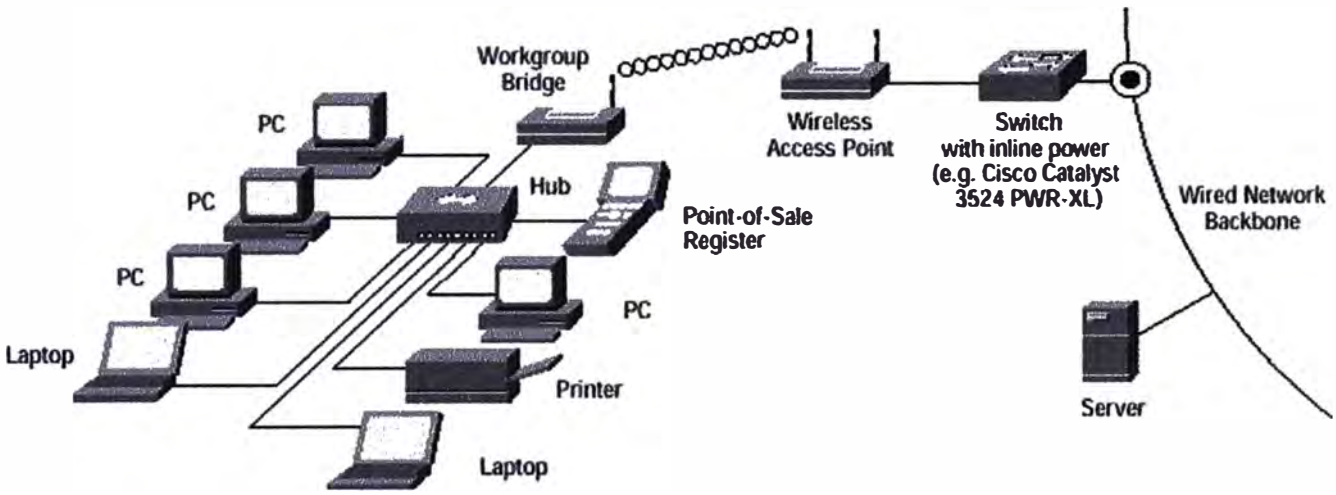

Fig. 15. Un Grupo de Trabajo Remoto

oficinas temporales, el puente para trabajo en grupo proporciona un acceso de red

fácil y flexible para un máximo de ocho dispositivos a través del uso de un hub Ethernet estándar de ocho puertos (Véase Fig. 15). Los equipos se pueden mover con facilidad según cambie la configuración de los grupos de trabajo en número de componentes o localización, disminuyendo los costos de las instalaciones.

6.4. Antenas y Accesorios Cisco Aironet

Cada instalación de una red de área local (LAN) inalámbrica es diferente. Cuando se diseña una solución para un edificio, los diferentes tamaños de las instalaciones, los materiales de construcción y las divisiones interiores hacen que surja un gran número de consideraciones relativas a la transmisión y a la multiruta. Cuando se implementa una solución edificio a edificio, hay que tener en cuenta la distancia, los obstáculos físicos entre las instalaciones y el número de puntos de transmisión implicados. Cisco no solamente se compromete a proporcionar los mejores puntos de acceso, adaptadores de clientes y puentes del mercado, también a ofrecer una solución completa para cualquier instalación LAN inalámbrica. Ese es el motivo por el que Cisco cuenta con la gama más amplia de antenas, cables y accesorios de todos los fabricantes (Ver Fig. 16). Con las antenas direccionales (i) y omnidireccionales (ii) de Cisco aprobadas por FCC, el cable con pocas pérdidas, el hardware de montaje y otros accesorios, los instaladores pueden personalizar una solución inalámbrica que cumpla los requisitos incluso de las aplicaciones más exigentes.

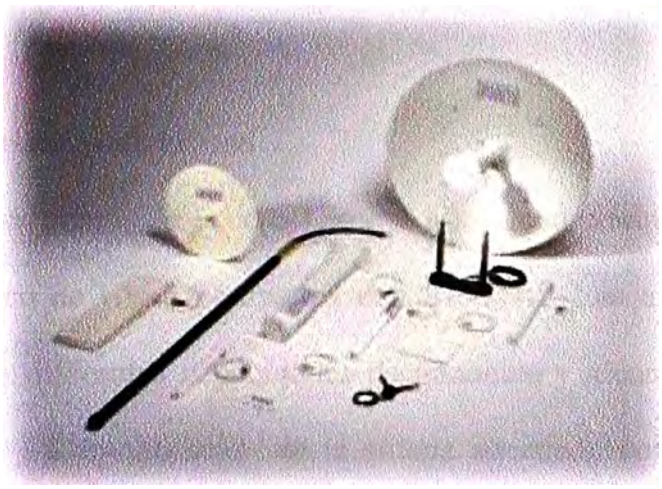

Fig. 16. Cisco ofrece una completa gama de antenas para adaptadores de clientes, puntos de acceso y equipamiento puente que posibilita una solución inalámbrica personalizada para prácticamente cualquier instalación.

(i) Una antena que concentra la potencia de transmisión en una dirección y aumenta así la distancia de cobertura a expensas del ángulo de cobertura. Entre los tipos de antenas direccionales se incluyen las yagi, las de ajuste y las parabólicas. Una yagi es un tipo de antena direccional cilíndrica. Una antena de ajuste es un tipo de antena plana diseñada para montarse en una pared y que irradia una zona de cobertura semiesférica. Una antena parabólica es un objeto cóncavo o en forma de plato. Suelen denominarse parabólicas. Las antenas parabólicas tienden a proporcionar la mayor ganancia y la menor anchura de haz, lo que hace que sean ideales para transmisiones punto a punto de larga distancia.
(ii) Una antena que ofrece un modelo de transmisión de 360 grados. Este tipo de antenas se utiliza cuando se necesita cobertura en todas las direcciones.

Antenas para adaptadores de clientes (Ver Fig. 17)

Los adaptadores de clientes inalámbricos Aironet de Cisco vienen con antenas estándar que proporcionan suficiente alcance (iii) para la mayoría de las aplicaciones a 11 Mbps. Para ampliar el alcance de transmisión a aplicaciones más especializadas, existe una gran variedad de antenas (iv) opcionales de mayor ganancia que son compatibles con adaptadores de clientes seleccionados.

(iii) Una medida lineal de la distancia a la que puede enviar una señal un transmisor.
(iv) Un método para aumentar la distancia de transmisión de una radio por la concentración de su señal en una sola dirección, normalmente a través del uso de una antena direccional. La ganancia no aumenta la

potencia de la señal de una radio, simplemente la desvía. Por lo tanto, a medida que aumenta la ganancia, la disminución en el ángulo de cobertura es inversamente proporcional.

Antenas para puntos de acceso

Las antenas para puntos de acceso Cisco Aironet son compatibles con todos los puntos de acceso de Cisco equipados con RP-TNC. Las antenas se encuentran disponibles con diferentes capacidades de ganancia y alcance, anchuras del haz (v) y formatos. La combinación de la antena adecuada con el punto de acceso adecuado permite una eficaz cobertura en cualquier instalación, así como mayor fiabilidad a velocidades de datos altas

(v) El ángulo de la cobertura de la señal que ofrece una radio; puede ser reducido por una antena direccional para aumentar la ganancia.

Antenas de Bridge o Puente

Las antenas de puente Cisco Aironet permiten distancias de transmisión extraordinarias entre dos o más edificios. Disponibles en configuraciones direccionales para la transmisión punto a punto y en configuración omnidireccional para implementaciones punto a multipunto. (Ver Fig. 18)

Cable de antena de bajas pérdidas

El cable de bajas pérdidas amplía la longitud entre cualquier puente Aironet de Cisco y la antena. Con una pérdida de 6,7 dB cada 100 pies (30 m), el cable de bajas pérdidas proporciona flexibilidad de la instalación sin un pérdida significativa del alcance.

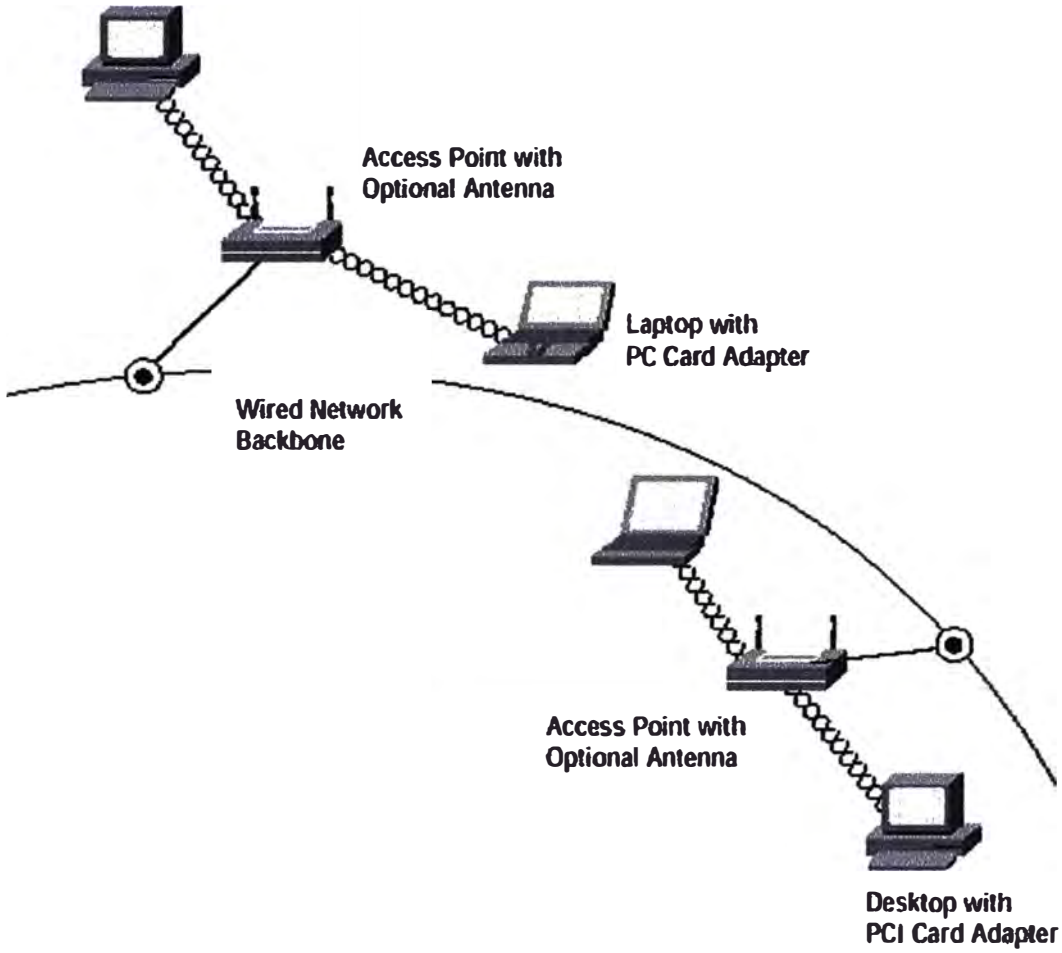

Fig. 17. Se pueden utilizar antenas opcionales de mayor ganancia para ampliar el alcance de los puntos de acceso

Fig. 18. Con las antenas de puente Cisco Aironet, el hardware de montaje adecuado y una instalación por personal cualificado, son posibles los enlaces inalámbricos a través de grandes distancias y obstáculos.

6.5. Servidor de Acceso de Control Cisco Secure V.2.6 para Windows 2000 y NT

Cisco Secure ACS es un servidor de control de acceso de alto rendimiento y gran capacidad de ampliación que funciona como un sistema servidor centralizado RADIUS o TACACS+ y que controla la autenticación, autorización y contabilidad (AAA) de los usuarios que acceden a los recursos corporativos a través de la red. Cisco Secure ACS admite la centralización del control de acceso y la contabilidad para los servidores de acceso telefónico, VPN y firewalls, soluciones de voz a través de IP (VoIP) y, en la versión 2.6, incluye nuevas mejoras referentes a la autenticación de los usuarios IEEE 802.1X basada en los estándares de los usuarios de la solución de acceso inalámbrico Aironet 350 de Cisco. En esta versión, se puede utilizar el mismo esquema de control de acceso (AAA) de la empresa para administrar el acceso de los usuarios desde clientes inalámbricos que utilizan el nuevo módulo ACS Extensible Authentication Protocol (EAP). Con ACS V.2.6, los administradores de redes pueden administrar fácilmente las cuentas de los usuarios inalámbricos y administrar y distribuir globalmente las claves de cifrado inalámbrico utilizando RADIUS. Esto mejora la capacidad global para la ampliación y el despliegue de servicios inalámbricos seguros y ahorra tiempo mediante la centralización del control, la gestión del acceso, la contabilidad y la distribución de claves inalámbricas en la estructura ACS. Con ACS, los administradores de red pueden controlar:

- Quiénes se pueden conectar a la red desde conexiones alámbricas o inalámbricas.
- Qué privilegios va a tener cada usuario en la red.
- Qué información de contabilidad queda registrada para las auditorías de seguridad o la facturación de cuentas.
- Qué controles de acceso y de comandos están habilitados para los administradores que configuran los routers Cisco IOS ® , los switches Catalyst ® y cualquier dispositivo de red compatible con TACACS+.

Características y ventajas principales

Cisco Secure ACS es un potente servidor de control de acceso con muchas características de rendimiento y capacidad de ampliación para cualquier empresa cuya WAN se encuentre en pleno crecimiento:

- *Facilidad de us*o: la interfaz de usuario basada en Web simplifica y distribuye la configuración de los perfiles de usuario, perfiles de grupo y la configuración de ACS.
- *Capacidad de ampliació*n: Cisco Secure ACS se ha creado para admitir entornos de grandes redes, con compatibilidad para servidores redundantes, bases de datos remotas y servicios de usuario de copias de seguridad.
- *Capacidad de extensió*n: la autenticación Lightweight Directory Access Protocol (LDAP) lo habilita para admitir la autenticación de perfiles de usuario almacenados en directorios de fabricantes líderes como Netscape, Novell y Microsoft.

- *Administración*: la compatibilidad con las bases de datos de Active Directory de Windows 2000 y NT consolida la administración de nombres de usuario y contraseñas de Windows y utiliza el Monitor de rendimiento de Windows para ver las estadísticas en tiempo real.
- *Administración*: los diferentes niveles de acceso para cada administrador Cisco Secure y la capacidad para agrupar dispositivos de red permiten un control más sencillo y una máxima flexibilidad para la aplicación de los cambios en la administración de las normativas de seguridad a través de todos los dispositivos de la red.
- *Flexibilidad del producto*: dado que el software Cisco IOS tiene compatibilidad integrada con AAA, el ACS puede utilizarse prácticamente en cualquier servidor de acceso (NAS) comercializado por Cisco (la versión de Cisco IOS debe admitir RADIUS or TACACS+).
- *Flexibilidad de protocolo*: Cisco Secure ACS incluye compatibilidad simultánea con TACACS+ y RADIUS para constituir una flexible solución, admitiendo VPN o acceso telefónico en el origen y la terminación del protocolo de seguridad Internet, IPsec y en los túneles del PPTP.
- *Integración*: la estrecha integración con los routers Cisco IOS y las soluciones VPN proporciona características como el protocolo Multichassis Multilink Point-to-Point Protocol y la autorización de comandos Cisco IOS.
- *Compatibilidad con otros fabricantes*: admite servidor de testigo para RSA SecurID, Axent Technologies, Secure Computing y CryptoCard \
- *Control*: cuotas dinámicas para horas del día, uso de la red, número de sesiones con acceso y restricciones de acceso por día de la semana

Requisitos de hardware y software - Equipamiento necesario para la implementación:

- Su servidor Windows 2000 o Windows NT debe cumplir los siguientes requisitos mínimos: Procesador Pentium 350 MHz o superior.
- Servidor Windows 2000 o NT 4.0 o superior; versión en inglés; Service Pack 6 o superior; consulte las notas de versión para cualquier información o para otras versiones de Service Pack compatibles.
- 128 MB de RAM
- Al menos 150 MB de espacio libre en disco; más si se está ejecutando la base de datos en la misma máquina.
- Resolución mínima de 256 colores a 800 X 600 líneas

Requisitos de software

- El servidor Windows 2000 o NT debe cumplir los siguientes requisitos mínimos de software: el NAS debe ejecutar el software Cisco IOS versión 11.2 o superior; o debe usarse un dispositivo de otro fabricante que pueda configurarse con TACACS+ o RADIUS

6.6. Costo de Equipos de Redes de Datos Inalámbricos

Los costos que se muestran son los precios unitarios de los equipos actualmente propuestos en las soluciones acceso de datos WLAN, en el cuadro se presentan los costos de: Adaptadores de RED, Puntos de Acceso y el de Un Bridge para trabajo de grupo de la Serie Cisco 350.

ITEM	PRODUCTO	DESCRIPCIÓN	CANT.	PRECIO
I.	*ADAPTADORES DE RED*			
1.1	AIR-PCI352	802.11b PCI Adapter w/RP-TNC Connector, Dipole Antenna	1	$190,61
1.2	AIR-PCM352	802.11b PC Card w/Integrated Antenna	1	$107,74
II.	*PUNTOS DE ACCESO*			
2.1	AIR-AP352E2R-A-K9	802.11b 100 mW AP w/Line Pwr, Dual RP-TNC, FCC Config	1	$541,24
2.2	AIR-AP352E2C	802.11b 100 mW AP w/Line Pwr, Capt. Ants	1	$477,49
III.	*BRIDGE*			
3.1	AIR-WGB352R	802.11b WorkGroup Bridge w/Dual RP-TNC Connectors	1	$400,99
3.2	AIR-WGB352C	802.11b WorkGroup Bridge w/Captured Dipole Antenna	1	$381,86
3.3	AIR-SSB350-A-K9	802.11b Bldg to Bldg Site Survey Kit, FCC Cnfg	1	$2.868,11
IV.	ACCESORIOS			
4.1	AIR-ACC2662	Antenna Mount for use with ANT1949	1	$43,99
4.2	AIR-ACC1725	Magnetic Antenna Mount Base w/RP-TNC Connector	1	$63,11
4.3	AIR-ACC1623	RP-TNC Female Connector for 9913 Cable	1	$12,11
4.4	AIR-ACC1655	RP-TNC Male Connector for RG-58 Cable	1	$12,11
V	ANTENAS			
5.1	AIR-ANT1729	2.4 GHz,6 dBi Patch Ant w/RP-TNC Connector	1	$139,61
5.2	AIR-ANT1949	2.4 GHz, 13.5 dBi Yagi Mast Mount Ant. w/ RP-TNC Connector	1	$235,24
5.3	AIR-ANT3213	2.4 GHz, 5.2 dBi Divers. Pillar Omni Ant. w/RP-TNC Con.	1	$133,24
5.4	AIR-ANT3338	2.4 Ghz, 21 dBi Solid Dish Antenna w/RP-TNC Connector	1	$681,49
5.5	AIR-ANT4941	2.4 GHz, 2.2 dBi Dipole Antenna w/ RP-TNC Connector	1	$31,24
VI.	*SOFTWARE DE GESTION DE ACCESO*			
6.1	CSACS-3.0	Cisco Secure ACS 3.0 for Windows	1	$3.821,81

Tabla 02. Costos Referencial de Equipos y Accesorios WLAN de Cisco

Los Adaptadores de red presentados en la Tabla 02 son uno del formato PCI para computadores personales estándar (Item 1.1) y otro para computadores portátiles (Item 1.2) de hecho se puede apreciar que este último es más económico. Normalmente las tarjetas PCI pueden venir con una conector adaptador tipo TNC donde se puede adaptar una antena para obtener mayor ganancia, allí es donde radica la diferencia de costo.

Los puntos de acceso especificados de igual manera se diferencian en que uno de ellos es simple incluye antenas dentro de su estructura, y el otro tiene conectores externos TNC para adaptar antenas de acuerdo a los requerimientos de cobertura.

De los equipo Bridge el item 3.3 incluye un kit completo para instalación Building to Building, este item incluye en pares, antenas, bridges, cables y accesorios para la instalación. El hecho de considerar un conjunto de items en bloque hace efectivo una disminución del costo respecto a considerar una compra item por item.

Los accesorios y antenas referidas se usan normalmente cuando se requiere contar con mayor cobertura ó se requiere de habilitar una solución Building to Building, de hecho la adquisición se debe basar en los requerimientos de servicio y en el diseño, sin embargo estos componentes también pueden ser adquiridas de manera independiente a otro proveedor, de acuerdo a los requerimientos de servicio.

El Software Cisco Secure Access Control del la Tabla 02 es soportado en las plataformas: Windows 2000 y NT, que son los Sistemas Operativos mas usados por el entorno gráfico en el que se presentan. Este software opera de manera similar a un Servidor RADIUS, y está licenciado para su uso en una sola PC.

Con el uso de los componentes mencionados se podría diseñar una red de acceso inalámbrica para usuarios, y los temas de costos se ajustarían a las cantidades requeridas, sin embargo hay que tener en cuenta que con los criterios de diseño adecuados de acuerdo al ambiente y medio de implementación y los requerimientos de servicio específicos, se pueden dimensionar los equipos para esta red. Con el adecuado diseño se va a poder analizar la relación costo

beneficio, de modo que los usuarios sean los mas beneficiados y el acceso a los aplicativos y servicios de red sea él mas transparente posible.

CONCLUSIONES

1. Para las aplicaciones locales de comunicaciones de datos (LAN) hasta ahora se dependía de tecnologías como Ethernet, en un medio por lo general cableado, sin embargo con el desarrollo de las tecnologías como el de la IEEE 802.11 ya se tiene en el mercado adicionalmente productos que permiten a los usuarios tener acceso inalámbrico.
2. Desde los años 90 se han hecho muchos esfuerzos con la finalidad de establecer una norma para las redes de datos inalámbricas, teniendo actualmente en posiciones de Vanguardia la norma IEEE 802.11 y la HiperLAN (Propuesta por ETSI), sin embargo a las diferencias actuales entre ambas, se están haciendo todos los esfuerzos para que en las versiones en desarrollo 802.11a y la Hiperlan2 sean compatibles. Para dar referencias ambas se están desarrollando sobre la base de la codificación COFDM or OFDM (coded orthogonal frequency division multiplexing), y trabajarán a 54Mbps.
3. El uso de las redes de datos inalámbricos se debe definir sobre la base del costo total de implementación y a los requerimientos de servicio de los usuarios, sin embargo al intentar hacer una comparación de costos frente a las redes cableadas, se debe de tener en cuenta las ventajas de WLAN, es decir movilidad e independencia y fácil implementación.
4. Debido a que el punto débil de WEP en cuanto a seguridad para WLAN está referido al carácter estático de clave usado en las transmisiones, se recomiendan usar plataformas de seguridad para trabajar en paralelo, por

ejemplo un equipo que brinde opciones de autentificación como un Servidor RADIUS.

5. En cuanto a respecta a las implementaciones de redes WLAN, debido a que está opera solamente en las dos capas mas bajas de OSI, cualquier aplicativo y protocolo que se soporte en la capa de red o superior trabajará perfectamente.
6. El informe se ha orientado fundamentalmente a analizar y entender la las redes de datos inalámbricas basados en el estándar 802.11, mostrando las ventajas de uso frente a las redes cableadas. Por lo tanto cualquier implementación debería de ser complementada con temas de diseño, además de una evaluación de costos, lo que se podría adelantar de lo visto en el presente informe es que hay tres canales en de la tecnología DSSS que no se traslapan y que pueden ser usados en un mismo lugar.

ANEXOS

ANEXO A. GLOSARIO

AP-access point

BPSK - Binary Phase Shift Keying

BSS - Basic Service Set

CCK-Complementary Code Keying

COFDM or OFDM (coded orthogonal frequency division multiplexing)

CRC - cyclic redundancy check

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

CTS - Clear to Send

DCF - Distribution Coordination Function

DHCP - Dynamic Host Configuration Protocol

DS - distribution system

DSSS - direct sequence spread spectrum

ESS - Extended Service Set

FCC - Federal Communications Commission (USA)

FHSS - Frequency Hopping Spread Spectrum

IBSS - Independent Basic Service Set

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IP - Internet Protocol

IPSec - Internet Protocol security

ISM - Industry, Scientific, and Medical

ISO - International Organization for Standardization

LLC - Logical Link Control

MAC - Media Access Control

MIB - management information base

NIC - network interface card

NOS - network operating system

PCF - Point Coordination Function

PCI - Peripheral Component Interconnect

QPSK - Quadrature Phase Shift Keying

RC4 - Ron's Code or Rivest's Cipher

RTS - Request to Send

SNMP - Simple Network Management Protocol

TCP/IP - Transmission Control Protocol/Internet Protocol

WECA - Wireless Ethernet Compatibility Alliance

WEP - Wired Equivalent Privacy

WLAN - wireless local area network

WLANA - Wireless LAN Alliance

ANEXOS B. ESPECIFICACIONES TÉCNICAS DE LOS ADAPTADORES DE LA SERIE CISCO AIRONET 350

Velocidades de datos admitidas	1, 2, 5,5 y 11 Mbps
Estándar de la red	IEEE 802.11b
Interfaz del sistema	AIR-PCM35x: PC Card (PCMCIA) tipo II AIR-PCI 351x: bus PCI
Banda de la frecuencia	De 2,4 a 2,4897 GHz
Tipos de arquitectura de red	*Infraestructura* y *directa*
Medio inalámbrico	DSSS (Direct Sequence Spread Spectrum)
Protocolo de acceso a los medios	Acceso múltiple de detección de portadora/detección de colisión (CSMA/CA)
Modulación	DBPSK a 1 Mbps DQPSK a 2 Mbps CCK a 5,5 y 11 Mbps
Canales de funcionamiento	América del Norte: 11 ETSI: 13 Japón: 15
Canales que no se superponen	Tres
Sensibilidad de la recepción	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5,5 Mbps: -89 dBm 11 Mbps: -85 dBm
Duración del retardo (típica)	1 Mbps: 500 ns 2 Mbps: 400 ns 5,5 Mbps: 300 ns 11 Mbps: 140 ns
Parámetros de potencia de transmisión disponibles	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm)
Alcance (típico)	Interiores: • 130 pies (40 m) a 11 Mbps • 350 pies (107m) a 1 Mbps Exterior: • 800 pies (244 m) a 11 Mbps • 2000 pies (610 m) a 1 Mbps
Conformidad	Funciona sin licencia bajo FCC parte 15 y está homologado como dispositivo clase B; cumple las normativas DOC; cumple los estándares ETS 300.328, FTZ 2100 y MPT 1349
Sistemas operativos compatibles	Windows 95, 98, NT 4.0, 2000, ME, CE 2.0, CE 2.1, CE 3.0, Mac OS 9.x y Linux
Antena	AIR-PCM35x: Dipolar con diversidad integrada AIR-LMC35x: dos conectores MMCX (antenas opcionales, la unidad no incluye ninguna) AIR-PCI35x: Antena dipolar externa y extraíble de 2,2 dBi con conector RP-TNC
Longitud de la clave de cifrado	AIR-PCM351, AIR-LMC351 y AIR-PCI 351: 40 bits AIR-PCM352, AIR-LMC352 y AIR-PCI 352: 128 bits
Tipo de autenticación	LEAP
Indicadores de estado	Estado del enlace y actividad del enlace
Dimensiones	AIR-PCM35x: 2,13 pulgadas (5,4 cm) de ancho x 4,46 pulgadas (11,3 cm) de fondo x 0,22 pulgadas (0,6 cm) de alto AIR-LMC35x: 2,13 pulgadas (5,4 cm) de ancho x 8,56 cm pulgadas (8,6 cm) de fondo x 0,22 pulgadas (0,6 cm) de alto AIR-PCI35x: 6,6 pulgadas (16,8 cm) de ancho por 3,9 pulgadas (9,8 cm) x 0,5 pulgadas (1,3 cm) de alto
Peso	AIR-PCM35x: 1,6 onzas (45 g) AIR-LMC35x: 1,4 onzas (40 g) AIR-PCI35x: 4,4 onzas (125 g)
Condiciones ambientales	Temperatura: de -22 a 158 F (de -30 a 70 C) De 10 a 95% (sin condensación)
Requisitos de potencia de entrada	.+5 VCC =/– 5%

ANEXOS C. ESPECIFICACIONES TÉCNICAS DE LOS PUNTOS DE ACCESO DE LA SERIE CISCO AIRONET 350

Velocidades de datos admitidas	1, 2, 5,5 y 11 Mbps
Estándar de la red	IEEE 802.11b
Interfaz del sistema	AIR-PCM35x: PC Card (PCMCIA) tipo II AIR-PCI 351x: bus PCI
Banda de la frecuencia	De 2,4 a 2,4897 GHz
Tipos de arquitectura de red	Infraestructura
Medio inalámbrico	DSSS (Direct Sequence Spread Spectrum)
Protocolo de acceso a los medios	Acceso múltiple de detección de portadora/detección de colisión(CSMA/CA)
Modulación	DBPSK a 1 Mbps DQPSK a 2 Mbps CCK a 5,5 y 11 Mbps
Canales de funcionamiento	América del Norte: 11 ETSI: 13 Japón: 15
Canales que no se superponen	Tres
Sensibilidad de la recepción	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5,5 Mbps: -89 dBm 11 Mbps: -85 dBm
Duración del retardo (típica)	1 Mbps: 500 ns 2 Mbps: 400 ns 5,5 Mbps: 300 ns 11 Mbps: 140 ns
Parámetros de potencia de transmisión disponibles	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm)
Alcance (típico a la configuración de la potencia de transmisión de una antena dipolar de diversidad de 2,2 dBi)	Interiores: • 130 pies (40 m) a 11 Mbps • 350 pies (107m) a 1 Mbps Exterior: • 800 pies (244 m) a 11 Mbps • 2000 pies (610 m) a 1 Mbps
Conformidad	Funciona sin licenciabajo FCC parte 15 y está homologado como dispositivo clase B; cumple las normativas DOC; cumple los estándares ETS 300.328, FTZ 2100 y MPT 1349
Homologación SNMP	MIB I y MIB II
Antena	AIR-AP35xE2C: dos dipolares de diversidad extraíbles de 2,2 dBi AIR-AP35xE2R: dos conectores RP-TNC (antenas opcionales, la unidad no incluye ninguna)
Longitud de la clave de cifrado	AIR-AP351Bx: 40 bits AIR-AP352E2x: 128 bits
Tipo de autenticación	LEAP
Seguridad Indicadores de estado	IEEE 802.1x (la propuesta incluye EAP y RADIUS) Tres indicadores del panel superior proporcionan información relativa al estado de las asociaciones, el funcionamiento, los errores/avisos, la actualización del firmware y la configuración, la red/módem y estado de las señales de radio.
Compatibilidad con la configuración automática	BOOTP y DHCP
Compatibilidad con la configuración remota	Telnet, HTTP, FTP, TFTP y SNMP
Configuración local	Puerto de consola directo (con cable serial incluido)
Dimensiones	6,30 pulgadas (16 cm) de ancho x 4,72 pulgadas (12 cm) de fondo x 1,45 pulgadas (3,7 cm) de alto
Peso	12,3 onzas (350 g)
Empalme de velocidad completa	Ninguno; para los puntos de acceso con empalme metálico para ofrecer velocidad completa, consulte los datos de los puentes multifunción de la serie Cisco Aironet 350
Condiciones ambientales	Temperatura: de 32 a 122 F (0 a 50 C) De 10 a 90% (sin condensación)
Requisitos de potencia de entrada	De 24 +/-10% a 60 VCC (línea de alimentación Ethernet)

ANEXOS D. ESPECIFICACIONES TÉCNICAS DE LOS EQUIPOS BRIDGE DE LA SERIE CISCO AIRONET 350

Velocidades de datos admitidas	1, 2, 5, 5 y 11 Mbps
Estándar de la red	Ethernet 10BaseT
Clientes compatibles	Directa: uno A través de hub: ocho
Tipos de arquitectura de red	Infraestructura (a través de un puente o punto de acceso Cisco Aironet)
Banda de la frecuencia	De 2,4 a 2,4897 GHz
Medio inalámbrico	DSSS (Direct Sequence Spread Spectrum)
Protocolo de acceso a los medios	Acceso múltiple de detección de portadora/detección de colisión (CSMA/CA)
Modulación	DBPSK a 1 Mbps DQPSK a 2 Mbps CCK a 5, 5 y 11Mbps
Canales de funcionamiento	América del Norte: 11 ETSI: 13 Japón: 15
Canales que no se superponen	Tres
Sensibilidad de la recepción	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5, 5 Mbps: -89 dBm 11 Mbps: -85 dBm
Duración del retardo	1 Mbps: 500 ns 2 Mbps: 400 ns 5, 5Mbps: 300 ns 11 Mbps: 140 ns
Parámetros de potencia de transmisión disponibles	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm)
Alcance (típico)	Interiores: • 130 pies (40 m) a 11 Mbps • 350 pies (107m) a 1 Mbps Exterior: • 800 pies (244 m) a 11 Mbps • 2000 pies (610 m) a 1 Mbps
Conformidad	Funciona sin licencia bajo FCC parte 15 y está homologado como dispositivo de clase B; cumple las normativas DOC; cumple los estándares de EN 300.328
Homologación SNMP	MIB I y MIB II
Antena	AIR-WGB35xC: dipolar extraíble de 2, 2-dBi AIR-WGB35xR: dos conectores RP-TNC (antenas opcionales, la unidad no incluye ninguna)
Longitud de la clave de cifrado	AIR-AP351E2x: 40 bits AIR-AP352E2x: 128 bits
Indicadores de estado	Tres indicadores del panel superior proporcionan información relativa al estado de las asociaciones, el funcionamiento, los errores/avisos, la actualización del firmware y la configuración, la red/módem y estado de las señales de radio.
Compatibilidad con la configuración remota	Telnet, HTTP, FTP, TFTP y SNMP
Dimensiones	6,30 pulgadas (16 cm) de ancho x 4,72 pulgadas (12 cm) de fondo x 1,45 pulgadas (3,7 cm) de alto
Peso	12,3 onzas (350 g)
Condiciones ambientales	Temperatura: de 32 a 122 F (0 a 50 C) De 10 a 90% (sin condensación)
Requisitos de potencia de entrada	América del Norte: 120 VCA a 60 Hz Universal: de 90 a 264 VCA a de 47 a 63 Hz

BIBLIOGRAFÍA

1. "LAN MAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer(PHY) specification. IEEE Std 802.11b/D8.0, Sept 2001,"
2. Seminario Internacional "Tendencia de las Telecomunicaciones Inalámbricas"
   Edición: Junio, Julio 2001
   OSIPTEL, Gerencia de Comunicaciones Corporativas
   Depósito Legal: 150108-2001-2320
3. CISCO SYSTEM INC.
   CISCO PRODUCT CATALOG, FEBRUARY 2002.
   Copyright © 1992--2002 Cisco Systems, Inc.
4. COMPUTERWORLD PERU
   Sección: Redes de Datos Inalámbricas
   PUBLICACION Nro. 228, Edición Quincenal (9 –22 Enero 2002)
5. WIRELESS LOCAL AREA NETWORKS AND THE 802.11 STANDARD
   Plamen Nedeltchev, PhD
   Edited by Felicia Brych
   March 31, 2001
6. Advanced Cisco Router Configuration
   Laura Chappell, Editor
   Macmillan Technical Publishing
   ISBN: 1-57870-074-4

7. Cisco LAN Switching

   Kennedy Clark, CCIE; Kevin Hamilton, CCIE

   ISBN: 1-57870-094-9

8. Wireless LAN Security

   http://wwwin.cisco.com/cmc/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

9. Hayes Vic, Tutorial on 802.11 to 802,

   http://grouper.ieee.org/groups/802/11/Tutorial/MAC.pdf

10. Cisco Aironet 350 Series Wireless Lan

    http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Hardware:Cisco_Aironet_350&s=Hardware_Info

11. Cisco Aironet 350 Series Products Overview

    http://www.cisco.com/univercd/cc/td/doc/pcat/ao350.htm