

Boletín Advisory*

Junio 2006

Seguridad en redes inalámbricas (wireless networks)

1 de 2

Introducción

¿Qué son las
redes inalámbricas?

Clasificación

Entornos de uso

Dispositivos y
topología

Estándares de comunicación
y seguridad

Créditos



ESPIÑEIRA, SHELDON Y ASOCIADOS

Firma miembro de

PRICEWATERHOUSECOOPERS 



Introducción	¿Qué son las redes inalámbricas?	Clasificación	Entornos de uso	Dispositivos y topología	Estándares de comunicación y seguridad	Créditos
--------------	----------------------------------	---------------	-----------------	--------------------------	--	----------

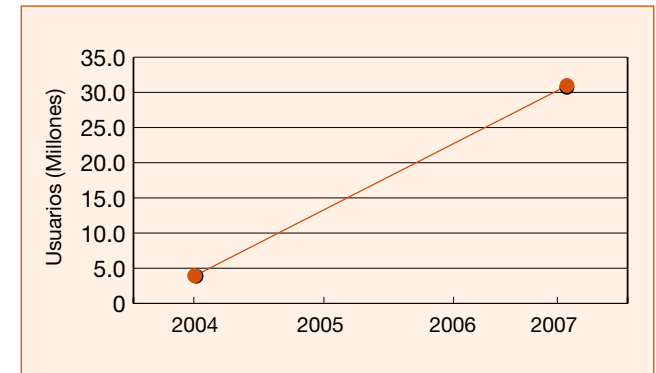
Introducción

La popularidad de la tecnología inalámbrica ha crecido exponencialmente. Desde hace ya varios años muchas organizaciones han implementado redes inalámbricas (o están actualmente en dicho proceso), mayormente a causa del bajo precio de los dispositivos, la reducción en el costo de cableado y la facilidad para el despliegue de nuevas redes o la extensión de las ya existentes.

La demanda actual que existe en las organizaciones de tener acceso inalámbrico a la red LAN viene dado por la creciente y común utilización de dispositivos móviles, tales como laptops, PDA's, así como la necesidad de los usuarios de mantenerse conectado a la red, sin tener que hacerlo físicamente. Las redes inalámbricas llevan años ofreciendo la posibilidad de unir puntos de difícil acceso, y además le permiten moverse dentro de un entorno manteniendo su conectividad.

Estos servicios estaban restringidos a las grandes empresas, pero actualmente, gracias a los últimos desarrollos que mejoran en velocidad, la consolidación y madurez de los estándares que definen estas redes y la ampliación de terminales

económicos, hace que se abra cada vez más el marco de usuarios finales a pequeños negocios e incluso a usuarios residenciales que ven en las tecnologías inalámbricas nuevas maneras de comunicarse. De acuerdo con Gartner Group, para el año 2007 existirán más de 31 millones de usuarios en redes inalámbricas, sólo en los Estados Unidos (ver la Figura N°1).



[Retorno](#)

Figura N°1: Crecimiento del mercado inalámbrico en USA
Fuente: Gartner Group



Para ampliar cualquier gráfico del boletín, haga click sobre el mismo. Para retornar al tamaño de lectura, haga click en la palabra 'Retorno'.





Introducción	¿Qué son las redes inalámbricas?	Clasificación 1/3	Entornos de uso	Dispositivos y topología	Estándares de comunicación y seguridad	Créditos
--------------	----------------------------------	----------------------	-----------------	--------------------------	--	----------

¿Qué son las redes inalámbricas?

Una red inalámbrica es un sistema de comunicación de información que proporciona conexión inalámbrica entre equipos situados dentro de la misma área (interior o exterior) de cobertura. En lugar de utilizar el par trenzado, el cable coaxial o la fibra óptica, utilizado en las redes LAN convencionales, las redes inalámbricas transmiten y reciben información a través de ondas electromagnéticas. Conceptualmente, no existe ninguna diferencia entre una red con cables y una inalámbrica, salvo su flexibilidad debido a la eliminación del uso de cables. Ambas ofrecen las mismas expectativas de comunicaciones como puede ser compartir dispositivos periféricos, acceso a bases de datos, directorios compartidos, acceso a un servidor de correo o navegar a través de Internet.

Las redes inalámbricas constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones de banda ancha. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado y le permite competir con otro tipo de tecnologías de acceso inalámbrico de última generación, tales como: UMTS (Sistema de Telecomunicaciones Móviles Universal) y LMDS (Sistema de Distribución Local Multipunto), pues éstas requieren de un

importante desembolso económico previo por parte de los operadores del servicio. Ahora bien, ello también obliga al desarrollo de un marco regulatorio adecuado que permita un uso eficiente y compartido del espectro radioeléctrico de dominio público disponible.

¿Cómo se clasifican las redes inalámbricas?

Lo mismo que las redes coaxiales, las redes inalámbricas se pueden clasificar en diferentes tipos en función de las distancias mediante las cuales se transmite la información. En la Figura N° 2 se muestran las clasificaciones principales de las redes inalámbricas.

[Retorno](#)

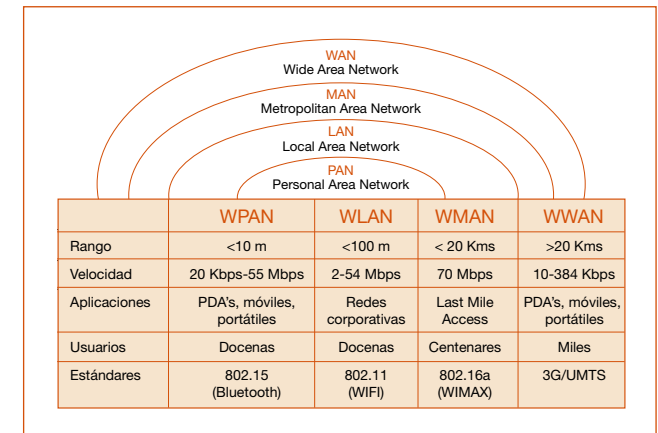



Figura N° 2: Clasificación de las redes inalámbricas


 Para ampliar cualquier gráfico del boletín, haga click sobre el mismo. Para retornar al tamaño de lectura, haga click en la palabra 'Retorno'.

- Wireless Personal Area Network (WPAN) o Red inalámbrica de ámbito personal:

Las tecnologías WPAN permiten a los usuarios establecer comunicaciones inalámbricas de par a par para dispositivos, tales como: PDA, teléfonos celulares y equipos portátiles) que se utilizan



Introducción	¿Qué son las redes inalámbricas?	Clasificación 2/3	Entornos de uso	Dispositivos y topología	Estándares de comunicación y seguridad	Créditos
--------------	----------------------------------	----------------------	-----------------	--------------------------	--	----------

¿Cómo se clasifican las redes inalámbricas?

continuación

dentro de un espacio operativo personal (“Personal Operating Space – POS”). Un POS es el espacio que rodea a una persona, hasta una distancia de 10 metros. Actualmente, las dos tecnologías WPAN principales son: Bluetooth y la luz infrarroja. Bluetooth es una tecnología de sustitución de cables que utiliza ondas de radio para transmitir datos a una distancia de hasta 30 pies. Los datos de Bluetooth se pueden transferir a través de paredes, bolsillos y maletines. El desarrollo de la tecnología de Bluetooth lo dirige el “Grupo de Interés General” (SIG) de Bluetooth, que publicó la especificación de la versión 1.0 de Bluetooth en 1999. Otra posibilidad que tienen los usuarios para conectar dispositivos en un radio de acción muy cercano (1 metro o menos) es crear vínculos de conexión mediante luz infrarroja.

Para normalizar el desarrollo de tecnologías WPAN, el IEEE ha establecido el grupo de trabajo 802.15 para las WPAN. Este grupo de trabajo está desarrollando una norma WPAN, basada en la especificación de la versión 1.0 de Bluetooth. Los objetivos principales en esta norma preliminar son baja complejidad, bajo consumo de energía, interoperabilidad y coexistencia con redes de 802.11.

- Wireless Local Area Network (WLAN) o Red inalámbrica de ámbito local:

Las tecnologías WLAN permiten a los usuarios establecer conexiones inalámbricas dentro de un área local (por ejemplo, un edificio corporativo o campus empresarial, o en un espacio público como un aeropuerto). Las WLAN se pueden utilizar en oficinas temporales u otros espacios donde el costo de la instalación de extenso cableado sería prohibitivo, o para complementar una LAN existente de modo que los usuarios pueden trabajar en diferentes lugares dentro de un edificio a diferentes horas.

- Wireless Metropolitan Network – (WMAN) o Red inalámbrica de ámbito metropolitano:

Las tecnologías WMAN permiten a los usuarios establecer conexiones inalámbricas entre varias ubicaciones dentro de un área metropolitana (por ejemplo, entre varios edificios de oficinas de una ciudad o en un campus universitario), sin el alto coste que supone la instalación de cables de fibra o cobre y el alquiler de las líneas. Además, WMAN puede servir como copia de seguridad para las redes con cable, en caso de que las líneas alquiladas principales para las redes con cable no estén disponibles. WMAN utiliza ondas de radio o luz infrarroja para transmitir los datos. Las redes

de acceso inalámbrico de banda ancha, que proporcionan a los usuarios acceso de alta velocidad a Internet, tienen cada vez mayor demanda. Aunque se están utilizando diferentes tecnologías, como el servicio de distribución multipunto de canal múltiple (MMDS) y los servicios de distribución multipunto locales (LMDS), el grupo de trabajo de IEEE 802.16 para los estándares de acceso inalámbrico de banda ancha sigue desarrollando especificaciones para normalizar el desarrollo de estas tecnologías.

- Wireless Wide Area Network (WWAN) o Red inalámbrica de área extensa:

Las tecnologías WWAN permiten a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como ciudades o países, mediante el uso de antenas en varias ubicaciones o sistemas satélite que mantienen los proveedores de servicios inalámbricos. Las tecnologías WWAN actuales se conocen como sistemas de segunda generación (2G). Entre los sistemas 2G principales se incluyen: “Global System for Mobile Communications” (GSM), “Cellular Digital Packet Data” (CDPD) y “Code Division Multiple Access” (CDMA). Los esfuerzos van encaminados a la transición desde redes 2G, algunas de las cuales



Introducción	¿Qué son las redes inalámbricas?	Clasificación 3/3	Entornos de uso 1/2	Dispositivos y topología	Estándares de comunicación y seguridad	Créditos
--------------	----------------------------------	----------------------	------------------------	--------------------------	--	----------

¿Cómo se clasifican las redes inalámbricas?

continuación

tienen capacidades limitadas de movilidad y son incompatibles entre sí, a tecnologías de tercera generación (3G) que seguirían un estándar global y proporcionarían capacidades de movilidad internacional. La Unión Internacional de Telecomunicaciones (UIT) está promoviendo activamente el desarrollo de una norma global para 3G.

Entornos donde utilizar una red inalámbrica

La fácil instalación y la flexibilidad que ofrecen estas redes las hacen imprescindibles en ciertos entornos como:

- Entornos difíciles de cablear

Son muchas las situaciones en las que el tendido de cables no es posible o resulta complicado. Edificios históricos o antiguos, áreas abiertas o calles muy concurridas impiden o elevan notablemente el coste de instalación de una red

- Equipos de trabajo provisionales

Zonas como parques, pistas de atletismo, exposiciones, zonas catastróficas u otras localidades que exigen la instalación de oficinas provisionales en donde es conveniente el establecimiento de redes locales temporales que se retiran una vez finalizado su cometido.

- Posibilidad de acceso a la información en tiempo real

Médicos y personal sanitario, empleados de establecimientos o responsables de almacén podrán acceder a la información en tiempo real mientras tratan a sus pacientes, clientes o procesan información.

- Entornos que varían con frecuencia

Salas de exposición, salas de reunión, establecimientos de venta al público o fábricas en las que el espacio de trabajo se modifica con frecuencia.

- Redes para pequeñas oficinas

Los trabajadores que desarrollan sus actividades en pequeñas oficinas o en su propia casa requieren una red asequible, de pequeñas dimensiones, que se instale y utilice fácilmente.

- Redes para usuarios residenciales

Cada vez es más frecuente que los hogares cuenten con más de un computador, siendo ideal disponer de una red sin cables, que permita compartir recursos entre los miembros de la familia.

- Ampliaciones de redes Ethernet

Los administradores de redes de entornos dinámicos pueden reducir, gracias al empleo de una red local inalámbrica, los gastos generales originados por los traslados, ampliaciones de redes u otras modificaciones en sus sistemas. ►



Introducción	¿Qué son las redes inalámbricas?	Clasificación	Entornos de uso 2/2	Dispositivos y topología 1/4	Estándares de comunicación y seguridad	Créditos
--------------	----------------------------------	---------------	------------------------	---------------------------------	--	----------

Entornos donde utilizar una red inalámbrica

continuación

- **Backup para redes de cable**
Los administradores de redes utilizan redes locales inalámbricas como sistema de contingencia en aplicaciones críticas ejecutadas en redes de cable.
- **Instalaciones de adiestramiento/educación**
Las salas de formación de las empresas y los alumnos de escuelas y universidades pueden recurrir a la conectividad inalámbrica para acceder e intercambiar información y aprender, sin la complejidad de cablear múltiples puestos para los alumnos.
- **Movilidad en la comunicación**
Las redes inalámbricas permiten a sus usuarios moverse libremente por el área de cobertura de su unidad base inalámbrica o punto de acceso.

Dispositivos y topología de las redes inalámbricas

Al igual que para una red convencional se debe equipar a los terminales que la forman con interfaces de red (tarjetas de red). Existen básicamente dos tipos de dispositivos básicos inalámbricos:

- Un Punto de Acceso (Access Point - AP)
- Un cliente habilitado en una LAN inalámbrica o clientes inalámbricos
- **Punto de Acceso (Access Point - AP):**

Wireless access point (WAP) o Access Point (AP), dispositivos que permiten conectar equipos de comunicación inalámbrica, para conformar así una red inalámbrica. Proporcionan un área de cobertura para los clientes inalámbricos. El espacio cubierto dependerá de la capacidad del equipo y sobre todo del entorno físico que se quiera cubrir: espacios exteriores o interiores con más o menos obstáculos. Pueden ofrecer funciones de "firewall" que permite aumentar la seguridad de la red. También pueden ofrecer mecanismos de autenticación para los clientes inalámbricos.

El punto de acceso recibe la información, la almacena y la transmite. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al

menos treinta metros y hasta varios cientos. El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena. Si es necesario ofrecer conexión inalámbrica a áreas más extensas, se pueden utilizar varias unidades bases conectadas entre sí, cada una cubriendo una parte del área total.

- **Clientes inalámbricos:**
Un cliente habilitado en una LAN inalámbrica puede ser: un computador portátil, una impresora, un PDA o cualquier otro dispositivo capaz de comunicarse a través de una red LAN inalámbrica. Muchos de estos dispositivos, especialmente algunos, tienen por configuración de hardware de fábrica las capacidades de conectividad inalámbricas incluidas en ellos mismos.

Son adaptadores inalámbricos que convierten las señales de datos Ethernet a señales de radio (IEEE 802.11b para el caso de redes Wi-Fi) y permiten a un equipo (ordenador





Introducción	¿Qué son las redes inalámbricas?	Clasificación	Entornos de uso	Dispositivos y topología 2/4	Estándares de comunicación y seguridad	Créditos
--------------	----------------------------------	---------------	-----------------	---------------------------------	--	----------

Dispositivos y topología de las redes inalámbricas

continuación

sobremesa o portátil, impresora, PDA, etc.) acceder a la red inalámbrica. Los sistemas operativos los tratan como adaptadores de red, análogos a las tarjetas Ethernet, por lo que desde el punto de vista del usuario final no existe diferencia entre disponer de uno u otro adaptador, ni de estar conectado a una u otra red.

Un terminal equipado con un cliente inalámbrico y situado dentro del área de cobertura de una unidad base, puede comunicarse con los demás dispositivos de la misma red local sin necesidad de cables.

Tipos de clientes inalámbricos:

- **Adaptador USB inalámbrico:** Se conecta al puerto USB del ordenador o dispositivo.
- **Tarjeta de red inalámbrica:** Es un dispositivo electrónico que permite acceder a una red inalámbrica y compartir recursos entre dos o más equipos.
 - Capa 1 y 2 del modelo OSI.
 - Diversas tecnologías: PCMCIA, USB, PCI, SD, MMC.
 - Precio relativamente económico.

La versatilidad y flexibilidad de las redes inalámbricas es el motivo por el cual la complejidad de una LAN implementada con esta tecnología sea tremendamente variable. La topología se refiere a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos.

Existen diversas topologías para crear una red inalámbrica, dependiendo de las necesidades de la red (con o sin acceso a Internet), el espacio a cubrir, el número de clientes estimado, etc. En este apartado se presentan diferentes despliegues de una red inalámbrica. A continuación se presentan cuatro (4) topologías utilizadas:

1. Ad-Hoc:

En este tipo de red inalámbrica cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red punto a punto o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID¹ igual para todos los nodos, que estén dentro del rango de cobertura de la señal y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre sí.

Se trata de la alternativa más sencilla permitiendo la visibilidad entre equipos inalámbricos. Consiste simplemente en proveer a los equipos con una tarjeta de red inalámbrica de modo que “todos hablen con todos” como puede observarse en la Figura N° 3. En este caso, no es necesario incorporar un punto de acceso. Presenta la ventaja de su sencillez pero, a cambio, tiene el inconveniente de crear una red aislada de otras redes y no ofrecer facilidades de seguridad ni gestión como cuando se dispone de un punto de acceso.



Figura N° 3: Topología de red inalámbrica “ad hoc”

¹ SSID: Service Set Identificación, Conjunto alfanumérico de hasta 32 caracteres que identifica a una red inalámbrica.



Introducción	¿Qué son las redes inalámbricas?	Clasificación	Entornos de uso	Dispositivos y topología 3/4	Estándares de comunicación y seguridad	Créditos
--------------	----------------------------------	---------------	-----------------	---------------------------------	--	----------

Dispositivos y topología de las redes inalámbricas

continuación

2. Infraestructura:

Esta solución ofrece la conexión entre redes con hilos e inalámbricas. Está especialmente indicada para incorporar a una red con cables equipos con conexión inalámbrica, permitiendo la ampliación de la red.

Como se observa en la Figura N° 4, es necesario utilizar un punto de acceso (Access Point) o pasarela inalámbrica que, por un lado, se conecte sin cables con los equipos nuevos y que, por otro, disponga de una tarjeta de red convencional para conectarse al equipamiento antiguo. Es importante resaltar que, a diferencia del modo ad-hoc, los equipos inalámbricos no hablan directamente entre sí, sino que lo hacen a través del punto de acceso, lo que ofrece más seguridad y conectividad con los terminales situados en la red con cables.

Este nodo central o punto de acceso que sirve de enlace para todos los demás (tarjetas de red). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del punto de acceso. Un único punto de acceso puede soportar un pequeño grupo de usuarios y

puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros.

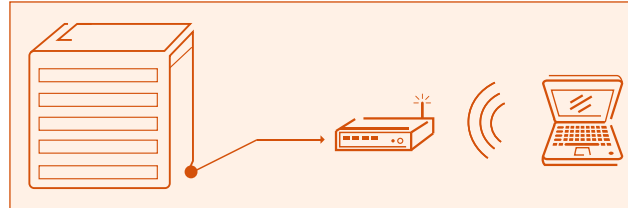


Figura N° 4: Topología de red "Infraestructura" [Retorno](#)

3. Red inalámbrica + ADSL:

Esta alternativa es la opción más recomendable porque permite construir una red inalámbrica local y dotar a todos los equipos que formen parte de ella de conexión a Internet a través de ADSL.

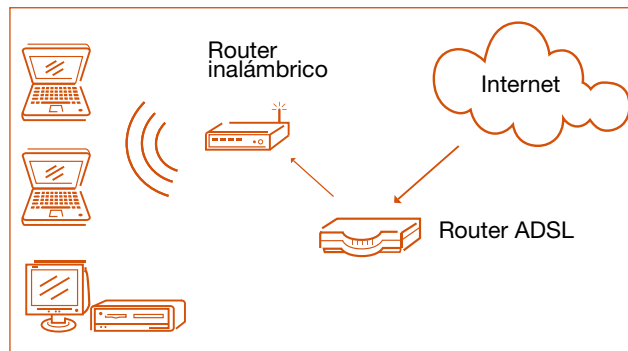


Figura N° 5: Red inalámbrica local con opción ADSL [Retorno](#)

En este diseño es necesario utilizar un punto de acceso o unidad base inalámbrica que, conectada directamente al router ADSL, dote al conjunto inalámbrico de un acceso a Internet de banda ancha. Como ocurría en el modo infraestructura, los equipos se conectan inalámbricamente a través del punto de acceso o unidad base.

Como se observa en la Figura N°5, se trata de una alternativa sencilla, sin necesidad de inversiones en cableado, para dotar a un domicilio u oficina de una red WLAN de conexión a Internet de banda ancha

4. Red inalámbrica con más de un punto de acceso ("roaming"):

Si el área que hay que cubrir es muy extensa, es necesario realizar un despliegue de una red inalámbrica local utilizando varios puntos de acceso de manera que los clientes inalámbricos pueden desplazarse entre las diferentes áreas de cobertura manteniendo la conexión. Esta facilidad se conoce como "itinerancia" o "roaming". Tal como se muestra en la Figura N°6 un cliente inalámbrico puede cambiar de área de cobertura sin perder la conectividad con la red y, por tanto, el acceso a los recursos de la empresa.



Introducción	¿Qué son las redes inalámbricas?	Clasificación	Entornos de uso	Dispositivos y topología 4/4	Estándares de comunicación y seguridad 1/5	Créditos
--------------	----------------------------------	---------------	-----------------	---------------------------------	---	----------

Dispositivos y topología de las redes inalámbricas

continuación

[Retorno](#)

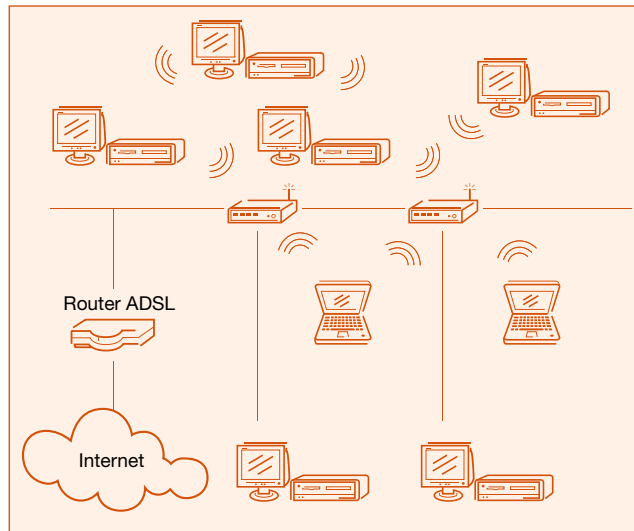


Figura N°6: Red inalámbrica con varios puntos de acceso (roaming)

Estándares de comunicación y seguridad en redes inalámbricas

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. En este sentido, en cuanto a los estándares de comunicación y seguridad en redes inalámbricas tenemos lo siguiente:

- Estándares de comunicaciones:
 - 802.11a
 - 802.11b (más ampliamente utilizado)
 - 802.11g
- Estándares de seguridad:
 - WEP
 - 802.11i (WPA2)
 - 802.1x

Estándares de comunicaciones en redes inalámbricas

Ante la existencia de dispositivos de redes inalámbricas de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades. En la Figura N°7 se muestran algunos de los estándares de comunicaciones y

seguridad en redes inalámbricas. Los estándares WLAN (redes de área local inalámbricas) comenzaron con el estándar 802.11, desarrollado en 1997, por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Estos estándares permiten transmisiones de datos de hasta 2 Mbps, transferencias que han sido mejoradas con el paso del tiempo.

[Retorno](#)

Tipo	Descripción
a	54 Mb/s en bandas de 5 GHz
b	11 Mb/s secuencia directa en 2.4 GHz banda
c	Operaciones de Bridging
d	Dominios internacionales
e	Calidad de Servicio (QoS)
f	Interoperatividad de Access point
g	54 Mb/s a 2.4 GHz (802.11b compatible)
h	Coordinación con estándares HiperLAN2 Europeos
i	Estándar de seguridad
j	Bandas adicionales de 4.9 y 5 Ghz en Japón
k	Mejoras en recursos de medición de radio
m	Mantenimiento de estándares anteriores
n	High throughput (>100 Mb/s)
p	Hand-off vehicular
r	Roaming rápido
s	Red en malla

Figura N° 7: Estándares de seguridad y comunicaciones en redes inalámbricas



Introducción	¿Qué son las redes inalámbricas?	Clasificación	Entornos de uso	Dispositivos y topología	Estándares de comunicación y seguridad 2/5	Créditos
--------------	----------------------------------	---------------	-----------------	--------------------------	---	----------

Estándares de comunicación y seguridad en redes inalámbricas *continuación*

Las extensiones a estas reglas se reconocen con la adición de una letra al estándar original, incluyendo 802.11a, 802.11b y 802.11g.

– 802.11a

Fue la primera aproximación a las redes inalámbricas y llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero que no están (a día de hoy) estandarizadas por el IEEE. Esta variante opera dentro del rango de los 5 Ghz.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares 802.11b y g, la no incorporación a la misma de QoS (posibilidades de aseguramiento de Calidad de Servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos multimedia online), la no disponibilidad de esta frecuencia en Europa dado que esta frecuencia está reservada a la HyperLAN2² y la parcial disponibilidad de la misma en Japón. Los

equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que en la banda de 5Ghz las ondas son más fácilmente absorbidas.

– 802.11b

Es la segunda aproximación de las redes inalámbricas. Alcanza una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes pero sin la estandarización (a día de hoy) del IEEE. Opera dentro de la frecuencia de los 2.4 Ghz.

Adolece de varios de los inconvenientes que tiene el 802.11a como son la falta de QoS, además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues en los 2.4 Ghz funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos Bluetooth, lo cual puede provocar interferencias.

En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita

alrededor de todo el mundo. Está estandarizado por el IEEE.

– 802.11g

Es la tercera aproximación a las redes inalámbricas, y se basa en la compatibilidad con los dispositivos 802.11b y en el ofrecer unas velocidades de hasta 54 Mbps. Opera dentro de la frecuencia de los 2.4 Ghz. Una nueva mejora de esta tecnología es la “Súper G” la cual permite velocidades de hasta 108Mbps.

Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Las ventajas de las que dispone son las mismas que las del 802.11b además de su mayor velocidad.

²HiperLAN2: es un estándar desarrollado por el ETSI (European Telecommunications Standard Institute) para redes WLAN.





Introducción	¿Qué son las redes inalámbricas?	Clasificación	Entornos de uso	Dispositivos y topología	Estándares de comunicación y seguridad 3/5	Créditos
--------------	----------------------------------	---------------	-----------------	--------------------------	---	----------

Estándares de comunicación y seguridad en redes inalámbricas *continuación*

Estándares de seguridad en redes inalámbricas

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle.

El estándar inalámbrico 802.11 original incorpora encriptación y autenticación WEP (Privacidad Equivalente a Cable). Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado.

Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica.

- WEP (Wired Equivalent Privacy)

Es el mecanismo de seguridad definido originalmente para el estándar 802.11

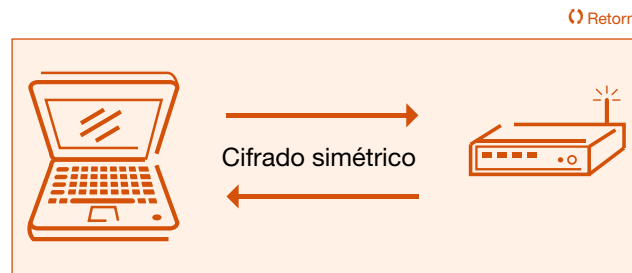


Figura N° 8: Cifrado simétrico - WEP

WEP proporciona dos tipos de autenticación:

- Sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN
- Autenticación mediante clave compartida, que controla el acceso a la WLAN

La seguridad del estándar WEP se basa en la utilización de un sistema de claves compartido, o en su defecto, el uso de claves estáticas en los dispositivos, tal como se muestra en la Figura N°8. En este modo, se envía una cadena de bytes al dispositivo que intenta conectarse a la red inalámbrica, y éste debe responder con la misma cadena cifrada con la clave que ambos conocen, resultando en un esquema clásico de “challenge – response”. Si el cliente falla en mandar la cadena correctamente cifrada, no se le permite el acceso a la red.

Adicionalmente, WEP provee un mecanismo para el cifrado de los datos transmitidos en el aire, utilizando un algoritmo llamado RC4 el cual puede operar con claves de 40 o 128 bits (ver Figura N°9). Toda la información en tránsito entre los puntos de acceso y las tarjetas de red inalámbrica de los clientes se encuentra cifrada y es en este mecanismo en el que se confía para proveer de seguridad a toda la red.

Sin embargo, el protocolo incluye algunos errores de diseño que evitan que la seguridad provista sea efectiva. En particular, el denominado “key schedule” (esencialmente la forma en la que las claves se eligen y van cambiando) y el tamaño del vector de inicialización que se utiliza para cifrar cada byte, unidos a la previsibilidad de muchos de los datos en tránsito (cabeceras de los paquetes IP, cabeceras de protocolos de transferencia de datos, etc.) permite que se puedan ejecutar ataques sobre el sistema criptográfico.

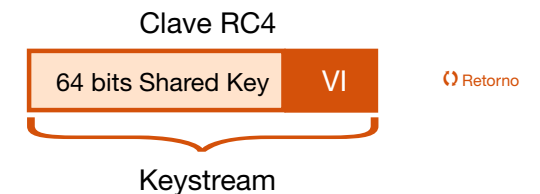


Figura N° 9: Algoritmo RC4

[Introducción](#)[¿Qué son las redes inalámbricas?](#)[Clasificación](#)[Entornos de uso](#)[Dispositivos y topología](#)[Estándares de comunicación y seguridad
4/5](#)[Créditos](#)

Estándares de comunicación y seguridad en redes inalámbricas *continuación*

Dichos ataques son fácilmente ejecutables con herramientas disponibles libremente en Internet. A modo de ejemplo, y para una de las herramientas más usuales, basta con obtener entre unos 5 y 10 millones de paquetes cifrados para deducir la clave, lo cual en una red de mediano porte se puede conseguir en unos 15 minutos de escucha pasiva. Cabe indicar que esto no es una debilidad específica del algoritmo RC4, sino de la forma en la cual el mismo es utilizado (incorrectamente) dentro de WEP.

La otra opción disponible -claves estáticas en los dispositivos- genera un esfuerzo administrativo considerable, requiriendo de mucho más tiempo para su correcta implementación. Además, si un equipo que tiene la clave incorporada es robado, ésta puede ser fácilmente recuperada de la configuración, lo que pone en peligro a toda la red desde el momento del robo hasta el cambio del total de las claves estáticas, y esto recién ocurre cuando el dispositivo es declarado como robado.

Ventajas:

- Fácil configuración
- Compatible con la mayoría de los dispositivos de hardware y software

Desventajas:

- Las claves son estáticas, por lo que requiere la intervención directa del administrador en cada equipo para habilitar la seguridad. La clave debe ser ingresada a cada dispositivo de la WLAN
- Se pueden encontrar las claves con la captura de paquetes de datos. Existen herramientas gratuitas en el mercado que permiten deducir la clave en función del tráfico regular
- No ofrece servicio de autenticación
- La custodia de la WEP key es bajo criterio del fabricante del software

En una reciente reunión de la ISSA (Information Systems Security Association) en Los Angeles (marzo, 2005), un equipo de agentes del FBI demostraron técnicas sencillas de WEP-cracking donde hallaron una clave de 128 bit en 3 minutos aproximadamente.

- WPA (Wi-Fi Protected Access)

El protocolo WPA esta basado en algunas especificaciones de 802.11i orientado a solventar las debilidades presentadas por WEP, usando:

- Autenticación y Cifrado usando TKIP (Temporal Key Integrity Protocol)
- Integridad con MIC (Message Integrity Check)
- Incorpora un servidor de autenticación (Radius) para el manejo de las claves
- La clave de cifrado es cambiada cada 10,000 paquetes (aprox.)
- En el encabezado se envía el hash del IV (Vector de inicialización) y no en texto claro





Introducción	¿Qué son las redes inalámbricas?	Clasificación	Entornos de uso	Dispositivos y topología	Estándares de comunicación y seguridad 5/5	Créditos
--------------	----------------------------------	---------------	-----------------	--------------------------	---	----------

Estándares de comunicación y seguridad en redes inalámbricas *continuación*

- WPA2 (802.11i)

Es una mejora al estándar 802.11 que especifica mejoras de seguridad (Ver Figura N°10). Entre las ventajas y desventajas presentadas por WPA2 están:

[Retorno](#)

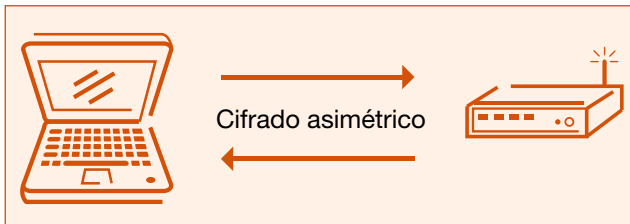


Figura N° 10: Cifrado asimétrico –WPA2

Ventajas:

- Advanced Encryption Standard (AES) como algoritmo de cifrado
- Verifica la integridad de los paquetes

Desventajas:

- No es compatible con el hardware anterior

- 802.1x (port based)

Fue diseñado para brindar seguridad en la autenticación, control de acceso y manejo de claves, facilitando el escalamiento de las WLAN's ya que provee una autenticación centralizada de los usuarios y las estaciones. (Ver Figura N° 11)

[Retorno](#)

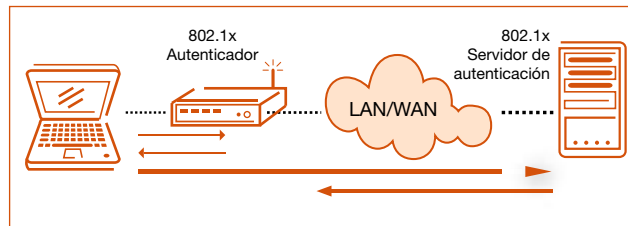


Figura N° 11: Autenticación centralizada

Ventajas:

- Autenticación y administración de claves de acceso centralizada
- La autenticación se realiza al medio
- Está basado en Extensible Authentication Protocol (EAP)
- Permite transportar WEP y WPA2

Desventajas:

- Costos

Las tecnologías de interconexión inalámbrica proporcionan comodidad y movilidad, pero también suponen riesgos relativos a la seguridad de la red. En la Figura N°12 se muestra un cuadro comparativo de los estándares mencionados.

[Retorno](#)

	WEP	WPA	802.11i
Algoritmo de Cifrado	RC4	RC4	AES
Manejo de claves	None	EAP-Based	EAP-Based
Longitud de la clave	40 bits	128 bits	128 bits
Integridad de la información	CRC-32	Michael	CCM
Integridad del encabezado	None	Michael	CCM

Figura N° 12: Cuadro comparativo de los distintos estándares de seguridad de redes inalámbricas



[Introducción](#)[¿Qué son las redes inalámbricas?](#)[Clasificación](#)[Entornos de uso](#)[Dispositivos y topología](#)[Estándares de comunicación y seguridad](#)[Créditos](#)

Boletín Advisory

El Boletín Advisory es publicado mensualmente por la Línea de Servicios Advisory de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. *connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados
Depósito Legal pp 1999-03CS141
Teléfono master: (58-212) 700 6666

Si está interesado en recibir en su correo electrónico este Boletín, por favor envíenos su dirección de e-mail a:
advisory.venezuela@ve.pwc.com



© 2006. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3