Recomendaciones de seguridad para el despliegue de redes inalámbricas.

Índice de contenido

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Avda. Cardenal Benlloch, 69 Entlo – 46021 VALÈNCIA

Tel. 963985300 – Fax. 961961781

Introducción

En la sociedad actual es cada vez más importante el acceso a la información, independientemente de la ubicación desde la que se encuentre el usuario. Es por ello que en esta "sociedad de la información" han ganado mucha fuerza las redes inalámbricas sobre las redes cableadas tradicionales, ya que ofrecen unas características de desempeño similares a las redes cableadas, aumentando la facilidad y reduciendo los costes de despliegue, y facilitando la movilidad del usuario, entre otros.

No obstante, estas características diferenciadoras, como por ejemplo el hecho de que se transmitan por el aire, medio donde cualquiera puede emplazar un receptor para una red que esté transmitiendo, hacen que se deban tener en cuenta otros problemas, además de los comunes a las redes cableadas.

En este documento se tratan los problemas más comunes de las redes inalámbricas y se marcan una serie de mínimos exigibles en materia de seguridad de las comunicaciones.

Objetivo

Esta guía trata de acercar a los responsables de GVA las características de las redes inalámbricas, al tiempo que se dan directrices y recomendaciones para el proceso de implantación o actualización de la infraestructura existente.

Sin entrar a fondo en discusiones acerca de las diferentes tecnologías o la legislación vigente (aunque si que se dan las pinceladas necesarias de ambas para ayudar a clarificar las posibles dudas que se puedan tener al respecto), esta guía pretende dar a conocer, de manera sencilla, los aspectos fundamentales que los responsables de informática de las entidades involucradas deben tener en cuenta a la hora de plantearse un despliegue de red inalámbrica para proporcionar servicios de comunicaciones, tanto a redes internas como a Internet, en sus instalaciones.

En la introducción se ha definido de forma breve qué son las redes inalámbricas y su importancia estratégica actual, así que el primer paso a partir de aquí será mostrar las debilidades que estas redes pueden tener. El segundo punto cubrirá los parámetros que se deben tener en cuenta al realizar el estudio de implantación de las mismas y salvar los problemas descritos en el primer paso, pasando a dar unas recomendaciones, dependiendo del uso que se quiera dar a las redes inalámbricas a desplegar.

Para finalizar, se ofrecen una serie de enlaces relacionados, así como un glosario de términos utilizados a lo largo de la presente guía.

Principales riesgos de seguridad de las redes Wifi

Los riesgos en las redes inalámbricas son muy variados, ya que incluyen los que afectan a una red cableada tradicional, más aquellos introducidos por esta nueva tecnología. Para controlar estos riesgos, aquellas entidades que quieran implantar este tipo de redes deben adoptar medidas que permitan reducir al mínimo estos riesgos, y el posible impacto sobre estas infraestructuras y otras ya implantadas. Además, es imprescindible un continuo seguimiento de los nuevos desarrollos y vulnerabilidades que puedan aparecer en el futuro afectando a éstas, ya que este campo se encuentra en constante desarrollo.

En la siguiente lista, se muestran los principales riesgos y amenazas que afectan a redes inalámbricas, además de todas las vulnerabilidades que afectan a una red de cable convencional:

- Puede obtenerse acceso a través de conexiones inalámbricas a otros servicios, que aún no siendo inalámbricos, estén conectados a éstos.
- La información que se transmite sin cables puede ser fácilmente interceptada, incluso a una distancia elevada, sin posibilidad de detectar esta captura, debido al medio *no confinado* por el que se transmite la información.
- Se pueden producir fácilmente ataques de denegación de servicio (DoS) contra este tipo de infraestructuras mediante perturbadores de señal, paquetes maliciosos, etc.
- Se puede inyectar tráfico en las redes inalámbricas a gran distancia.
- Se pueden desplegar equipos falsos para obtener información y realizar ataques de tipo "Man in the Middle". Estos ataques modifican la ruta que siguen los paquetes hasta que llegan a la red cableada, permitiendo su alteración por usuarios malintencionados.
- Se puede obtener detalles críticos de la conexión con sólo tener acceso a un equipo legítimo (Ej. claves guardadas en registro de sistemas operativos, ficheros de configuración, etc.).
- Se puede obtener acceso a redes inalámbricas utilizando redes de terceros que no mantengan una política de seguridad adecuada.
- Se pueden realizar ataques internos desplegando redes inalámbricas no autorizadas.
- Se puede revelar información de la entidad propietaria y/o el creador del equipamiento utilizado en datos transmitidos en abierto y fácilmente capturables (SSID, MAC).

En la presente guía se discutirán soluciones para todos estos problemas, ayudando así a la creación de redes inalámbricas con un nivel de seguridad adecuado.

Parámetros de configuración

Tecnología de la red

Se refiere al protocolo de comunicaciones que utilizará la red inalámbrica que se quiere desplegar en su nivel físico, que corresponde a las ondas radioeléctricas que emitirá. En estos protocolos se definen, entre otros, las bandas sobre las que se emitirá, el ancho de banda utilizado, los canales existentes, la tasa de transferencia máxima, el formato de las ondas emitidas, los servicios que se pueden ofrecer, etcétera. En la actualidad existen muchos y muy diversos protocolos, cada uno de ellos con características distintas, que pueden ser útiles en distintos escenarios. En esta guía se van a tratar las tecnologías de red más extendidas actualmente, que son las 802.11a, 802.11b, 802.11g y 802.11n. A continuación se muestra una tabla con sus características principales:

	802.11a	802.11b	802.11g	802.11n
Banda	5GHz	2,4GHz	2,4GHz	2,4GHz 5GHz
Canales (en España)	19	13	13	13/19
Tasa transferencia máxima	54Mbps	11 Mbps	54Mbps	600 Mbps
Alcance máximo (int/ext)	35m / 120m	38m / 140m	38m / 140m	70m / 250m

En lo que respecta a la banda, el uso de la de 5GHz reduce el número de interferencias, ya que ese espectro está menos congestionado que el de 2,4GHz (cabe recordar que en esta banda funcionan las redes Bluetooth, telefonía inalámbrica y hornos microondas, entre otros), aunque también se pierde alcance ya que las ondas de mayor frecuencia se degradan más rápido.

La legislación referente a los canales utilizables en las redes inalámbricas es diferente en cada país. Para las redes de 2,4GHz, por ejemplo, se pueden utilizar 13 canales en toda Europa, mientras que en los EEUU se pueden utilizar sólo 11, y en Japón 14. En el caso de los canales de la banda de los 5GHz, la situación es similar.

La tasa de transferencia indicada en la tabla es la máxima que puede soportar el estándar, que no será nunca la tasa real obtenida en un uso normal de la red. Para las redes 802.11a y 802.11g se obtiene una media de 20Mbps en un uso normal, mientras que en las redes 802.11n se pueden obtener entre 320 y 400 Mbps.

Seguridad

Este parámetro define el nivel de seguridad que se aplicará a las comunicaciones establecidas. Por defecto, las tecnologías de red explicadas anteriormente transmiten la información sin cifrar, pero se pueden incluir protocolos que cifran las comunicaciones, haciéndolas más seguras.

Actualmente los protocolos de seguridad más extendidos son: WEP, WPA-Personal, WPA-Enterprise, WPA2-Personal y WPA2-Enterprise.

El protocolo WEP (*Wired Equivalent Privacy* o "Privacidad Equivalente a Cableado") fue el primero en ser desarrollado, y como su nombre indica, trata de ofrecer una privacidad similar a la obtenida en las redes cableadas. Para ello cifra las comunicaciones a nivel 2 (Ethernet) con una clave compartida (conocida tanto por el punto de acceso como por todos los equipos que se conectan a él) de 64 o 128 bits. Este protocolo tiene vulnerabilidades conocidas y se considera obsoleto, por lo que no se recomienda en ningún caso su uso.

El protocolo WPA (*Wi-Fi Protected Access* o “Acceso protegido a redes Wifi”) surge como

evolución del WEP, e implementa la gran parte del estándar 802.11i, sobre codificación de las comunicaciones inalámbricas. Fue creado como puente entre el descubrimiento de las debilidades del protocolo WEP y la finalización del estándar 802.11i, implantado en WPA2.

Ambos protocolos (WPA y WPA2), ofrecen una mayor seguridad, al incorporar claves temporales que se actualizan con el uso de la red, habilitan el soporte a servidores centralizados de autenticación, aumentan el tamaño de los vectores de inicialización de las comunicaciones, habilitan distintos algoritmos de autenticación y comprobación de contraseñas, etcétera.

Al ser un estándar puente, WPA conserva partes del protocolo WEP que lo hacen algo más susceptibles a ataques de fuerza bruta si se usan contraseñas débiles. Si se utilizan contraseñas fuertes (más de 10 caracteres, mezclando mayúsculas, minúsculas, números y símbolos, y evitando palabras incluidas en diccionarios) el protocolo sigue siendo seguro, ya que el tiempo necesario para romper la seguridad de este sistema crece exponencialmente.

En estos nuevos protocolos se habilita una opción muy interesante, que consiste en la utilización de un servidor centralizado para el control de la autenticación mediante el protocolo 802.1X, implementado, por ejemplo, por los servidores RADIUS. Estos servidores deben estar ubicados fuera de la red inalámbrica a la que dan servicio, pero accesibles desde los puntos de acceso inalámbricos, para poder ofrecer su servicio. El hecho de tener un servidor centralizado y no accesible físicamente permite aumentar también la seguridad y llevar un control más fiable de los usuarios y sus acciones. Este método de autenticación se implementa en las versiones Enterprise de los protocolos WPA y WPA2, siendo las versiones Personal aquellas que utilizan una clave previamente compartida.

Direccionamiento

Este parámetro controla el modo en que los equipos conectados a la red obtienen su dirección IP y otros parámetros de conexión (máscara de subred, puerta de enlace, servidores DNS, ...), y por tanto, conectividad para poder realizar sus tareas. La dirección IP es un requisito indispensable para poder realizar cualquier acción en la red a la que conectan. El direccionamiento puede ser:

- **Estático:** cada equipo debe tener preconfigurada su dirección IP. En caso contrario no obtendrá conectividad.
- **Dinámico:** existe un servidor, al que los nuevos equipos en la red preguntan, que asigna dinámicamente las direcciones IP de que dispone (pueden cambiar con el tiempo) a los equipos conectados según sea necesario.
- **Dinámico con enlaces estáticos:** Existe un servidor, como en el caso anterior, pero esta vez asigna siempre las mismas IP a los mismos equipos (basándose en su dirección de nivel más bajo, la dirección MAC, para hacer la correspondencia), respetando en este caso otros parámetros que se hayan configurado para los equipos afectados (reglas en el cortafuegos, accesos privilegiados, etc.). Es posible que existan solo unas pocas direcciones reservadas, o que todas lo estén, siendo entonces el funcionamiento obtenido como en el modo estático.

En este caso, el modo de funcionamiento más seguro es el estático, pero esto conlleva la incomodidad de tener que preconfigurar en cada equipo estos parámetros les resta movilidad, ya que si se quieren conectar a otra red tendrán que modificar todos estos parámetros cada vez.

Además, el modo de funcionamiento estático no evita en si mismo las conexiones de equipos no autorizados, puesto que alguien que conozca los parámetros de conexión puede configurarlos en su equipo y obtener conectividad. Para eso se introduce también la restricción de acceso, como vamos a ver en el siguiente punto.

Restricciones de acceso

Aquí se definen las restricciones que se aplicarán a los nuevos equipos detectados en las redes inalámbricas. Basándose en la dirección MAC, que es el identificador único de nivel más bajo de que disponen los dispositivos inalámbricos, se pueden aplicar distintas restricciones de acceso a los nuevos equipos conectados. En este campo las opciones son:

- **Sin restricciones:** No se realiza ningún tipo de control sobre los nuevos dispositivos conectados, por lo que se permite el acceso (y por tanto la obtención de una dirección IP y el resto de parámetros de conexión) a cualquier equipo que se acabe de conectar.
- **Lista de exclusión:** Se mantiene una lista de dispositivos que tienen explícitamente denegado el acceso a la red inalámbrica. Si el dispositivo que se quiere conectar no se encuentra en la lista se le permite el acceso.
- **Lista de inclusión:** Se mantiene una lista con los dispositivos que pueden acceder a la red, siendo denegado el acceso a cualquier dispositivo que no se encuentre en la lista de permitidos. Se suele implementar junto con el direccionamiento dinámico con enlaces estáticos, de forma que solo se permite acceder a aquellos equipos para los que se han definido los parámetros de conexión de forma explícita.

La opción más segura aquí es la de la lista de inclusión, ya que como se acaba de comentar se da acceso únicamente a los equipos incluidos en esa lista, que además pueden tener configurados sus parámetros de conexión según el direccionamiento elegido.

Para redes no críticas, como pueden ser las redes de invitados, se acepta el uso de la política sin restricciones, ya que se van a conectar usuarios distintos a lo largo del tiempo, cambiando a la política de lista de exclusión en caso que se detecte el acceso de algún usuario malintencionado que pueda acceder debido a la propagación de las ondas hasta su ámbito (algún vecino, transeúnte o cualquier otro usuario que use la red de modo no autorizado).

Aislamiento

Trata la situación y comunicación de la red inalámbrica con el resto de redes disponibles en la organización. Se puede decidir aislar la red, incluirla como subred dentro de otra, o hacer que tenga visibilidad parcial de las redes internas. También se define aquí si tendrá conectividad a recursos externos, como las redes DMZ e internet o no. Aunque las configuraciones pueden ser muy diversas, se pueden englobar en los siguientes tipos:

- **Conectividad total:** Se permite el acceso tanto a Internet como a las redes internas y DMZ de la organización. No tiene ninguna restricción. Se puede corresponder con un segmento de usuarios de una red cableada.
- **Conectividad hacia el exterior:** Se permite el acceso únicamente hacia Internet. La red está aislada completamente de la de la organización, y no se permite ningún tipo de acceso a la misma.
- **Conectividad hacia segmentos externos:** Se permite el acceso tanto a internet como a los servicios externos (redes DMZ) de la organización. La red está aislada de la red interna de la organización, aunque puede acceder a sus recursos externos como si de un usuario interno se tratara (utilizando el direccionamiento interno).
- **Conectividad a servicios internos:** Se permite únicamente el acceso a redes internas de la organización, sin posibilidad de acceder a internet.

En lo que respecta a la situación de la red, se pueden dar los siguientes casos:

- **Segmento de red existente:** La red inalámbrica comparte direccionamiento con otra red ya

existente, y equipos cableados pueden ver equipos inalámbricos y viceversa dentro de esa red.

- **Red aislada:** Se define un segmento de red distinto para los equipos inalámbricos, de forma que estos no comparten direcciones con ningún equipo fuera de la subred inalámbrica.

Carga

Se especifican umbrales de carga del equipamiento, para que pueda ofrecer un buen servicio acorde a lo planeado. En concreto se define aquí el número de usuarios que se podrán conectar a un mismo punto de acceso (AP) sin perder funcionalidad.

Escalado

En este parámetro se define como se conectan los puntos de acceso entre si, en caso de ser necesaria la utilización de más de uno de ellos para realizar un despliegue. En este caso se pueden utilizar tanto tecnologías cableadas como inalámbricas para transmitir la información entre varios puntos de acceso.

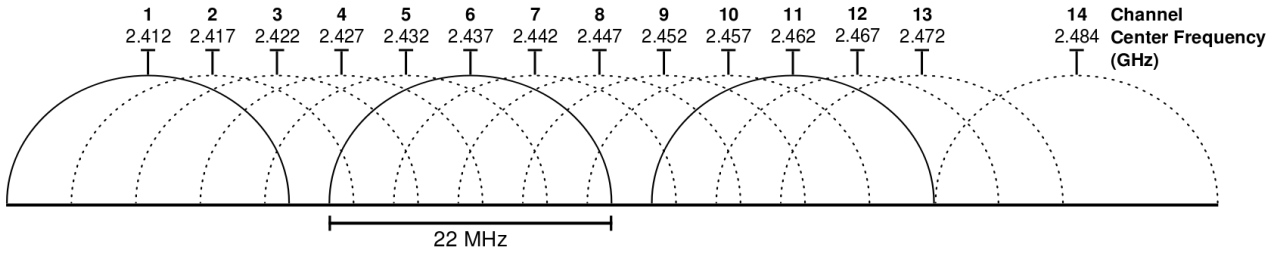
Otras consideraciones a tener en cuenta

Canal de radio

Este parámetro se debe elegir de forma cuidadosa. El canal de radio es la frecuencia exacta por la que se transmite la información. Cada país tiene su legislación al respecto, existiendo en España 13 canales para las redes del tipo 802.11b/g.

Estos canales están solapados causando interferencias hasta cuatro canales de diferencia, por lo que si, por ejemplo, utilizamos el canal 5, estaremos emitiendo información en un rango que va desde el canal 1 al 9, y causaremos interferencias, menores cuanto más alejado se encuentre el canal, con ellos.

Se debe elegir por tanto el canal de radio que tenga menos interferencias con canales contiguos para maximizar así la calidad de las transmisiones y el alcance real.



SSID

El SSID es el nombre que tiene la red cuando se accede a ella, y nos sirve para identificarla. Debe ser un nombre descriptivo y acorde a la organización en que nos encontramos. En ningún caso se debe dejar el nombre de red por defecto de los dispositivos.

También se puede elegir ocultar el nombre de la red inalámbrica. De este modo es necesario que cada usuario introduzca el nombre de la red al mismo tiempo que introduce sus credenciales de acceso.

Análisis del lugar de despliegue

Uno de los factores principales que determinan el éxito de un despliegue de una red inalámbrica es dónde se sitúan los puntos de acceso (AP). Para conseguir una adecuada instalación, ofreciendo una óptima cobertura inalámbrica, se debe estudiar con detalle el lugar a cubrir y los obstáculos a evitar.

Estudio de la cobertura deseada

En primer lugar se debe conocer qué cobertura se desea ofrecer. Puede que no importe la existencia de zonas sin cobertura (como pasillos, entrada, etc) y sin embargo se prefiera ofrecer una mejor cobertura en otras zonas más utilizadas (salas de reuniones, despachos, etc.).

El alcance de la señal de una red inalámbrica depende de varios factores, entre los que destaca los obstáculos que la señal tenga que atravesar. La velocidad de la conexión depende directamente de la distancia existente entre el AP y el cliente conectado y es inversamente proporcional al número de obstáculos existentes entre ambos.

Un ejemplo es una oficina en forma de L donde se sitúa el AP en un extremo de la L, y se desea cobertura en el otro extremo. Aunque la distancia directa sea suficiente, hay que tener en cuenta no

solo las paredes interiores sino también las dos paredes exteriores o muros (la curva de la L) que puede llegar a hacer imposible la comunicación entre esos dos puntos. La solución en este caso es mover el AP a una posición central de la oficina. De este modo se puede conseguir una mejor distribución de la señal por todo el inmueble, ya que tendrá que atravesar menos obstáculos para llegar a los dos extremos que se querían conectar inicialmente.

Tipos de antenas

Los AP están generalmente equipados con antenas omnidireccionales, pero también existen otro tipo de antenas que pueden ser útiles para según que usos.

Las antenas omnidireccionales ofrecen un círculo de cobertura alrededor de la antena, pero es importante tener en cuenta que justo debajo del mismo AP la cobertura obtenida es pequeña ya que las señales de radio se propagan hacia fuera de la antena de una manera circular. En este caso se aconseja situar la antena perpendicular al equipo (en posición vertical) para obtener una cobertura circular alrededor de él.

Si se quiere reducir el radio de acción de la red inalámbrica, bien porque sale fuera de nuestros dominios (a la vía pública o a otros vecinos, por ejemplo) o bien porque queremos evitar interferencias con otros aparatos, se pueden montar otros tipos de antenas. Si la reducción en el radio de acción es parcial, se pueden usar antenas planares. Para reducciones más acusadas, acercándose a comunicaciones punto a punto, se pueden usar antenas direccionales.

Localización de los puntos de acceso

A continuación se exponen algunas ideas a tener en cuenta a la hora de decidir dónde situar los AP para ofrecer una buena cobertura:

• Cuanto más lejos (linealmente) se quiera llegar, más alto se deberá colocar el AP. Es aconsejable situarlo a la máxima altura posible con objeto de evitar los obstáculos que fundamentalmente se encuentran a poca altura. Esto nos servirá además para evitar que sea fácilmente accesible a cualquier persona que pase por su posición, para prevenir posibles robos, desconexiones, reseteos o reconfiguraciones de usuarios malintencionados.

• Si se desea obtener una cobertura global, se debe situar en una posición central del inmueble, ya que la cobertura ofrecida es circular (con antenas omnidireccionales).

• Si se desea obtener cobertura en lugares estratégicos (sala de reuniones o en un lugar determinado) es necesario realizar un estudio de dónde situar el AP. Como la señal inalámbrica se refleja de forma similar al sonido, se puede pensar desde qué punto se reparte mejor la voz llegando a recibirse adecuadamente en la sala de reuniones o la zona a cubrir. Una ventana, un patio de luces, un hueco de escaleras, pueden ayudar a distribuir la señal. También puede ayudar el cambio de antena a uno de tipo planar o direccional, que proyectan la señal hacia una sola dirección.

• También es importante observar los obstáculos o barreras que se pueden producir en la cobertura, estudiando los objetos que pueden absorber o reflejar la señal llegando a degradar e incluso bloquear la misma. Algunos posibles obstáculos pueden ser: paredes, armarios, azulejos, cristales revestidos, techos, etcétera.

• Asimismo, otros dispositivos electrónicos también pueden provocar interferencias en la señal, por lo que se deben alejar los AP de equipos de gran consumo (neveras, monitores, televisiones, …) e intentar alejarlos de otros equipos que emiten radiación como teléfonos inalámbricos u hornos microondas.

• No es aconsejable encerrar el equipo inalámbrico dentro de un mueble (sobre todo si es metálico), ni situarlo entre libros u objetos que lo cerquen.

Canales de configuración del equipamiento de red

Los elementos de red tales como routers, switches, puntos de acceso (AP) y demás, suelen tener interfaces de configuración disponibles, que tienen unas credenciales de acceso por defecto, de dominio público.

Es necesario modificar las credenciales de acceso de todos estos equipos para evitar accesos no deseados a los paneles de configuración, con las consecuencias que podrían tener estos accesos en forma de, por ejemplo, modificación de configuraciones, escalada de privilegios y denegaciones de servicio.

Además, también se deberán deshabilitar todas aquellas interfaces que no sean seguras y no dispongan de métodos de autenticación y cifrado seguros.

Parametrización de redes

En este punto se especifican las configuraciones mínimas y recomendadas, según los parámetros definidos en el punto anterior, para distintos tipos de redes, dependiendo del uso al que vayan a ser destinadas.

Redes de uso interno

Se entienden como redes de uso interno aquellas que serán utilizadas únicamente por el personal de la organización, y se utilizarán exclusivamente para fines profesionales. Generalmente se requerirá acceder a aplicaciones corporativas y a servidores de datos, siempre de forma restringida. Las configuraciones recomendadas son las siguientes:

Característica	**Mínimo**	**Recomendado**
Tecnología	Cualquiera	802.11g
Seguridad	WPA-Enterprise No se puede usar LEAP.	WPA2-Enterprise No se puede usar LEAP.
Direccionamiento	Dinámico	Dinámico con rutas estáticas
Restricciones de acceso	Solo usuarios previamente autorizados	Solo usuarios previamente autorizados
Aislamiento	Subred dentro de la red de usuarios cableados. Acceso a redes DMZ e internet y a recursos internos.	Red aislada de la red de usuarios cableados. Acceso a redes DMZ e internet. Sin acceso a otras redes internas.
Carga	Unos 15 usuarios por AP como máximo.	Unos 7 usuarios por AP como máximo.
Escalado	Puntos de acceso cableados.	Puntos de acceso cableados.

Redes de invitados

Se entienden por redes de invitados aquellas cuyo uso está destinado a la conexión ocasional de personas externas a la organización que requieran algún tipo de conectividad. Generalmente no tienen ninguna necesidad especial de velocidad o conectividad. Las configuraciones recomendadas son las siguientes:

Característica	**Mínimo**	**Recomendado**
Tecnología	Cualquiera	Cualquiera
Seguridad	WPA-Personal Se debe cambiar la contraseña cada 6 meses.	WPA2-Personal Se debe cambiar la contraseña cada 2 meses.
Direccionamiento	Dinámico	Dinámico
Restricciones de acceso	Cualquier usuario puede acceder.	Solo usuarios previamente autorizados
Aislamiento	Red completamente aislada. Acceso limitado a redes DMZ e	Red completamente aislada. Acceso limitado a redes DMZ e

	internet. Sin acceso a otras redes internas.	internet. Sin acceso a otras redes internas.
Carga	Unos 25 usuarios por AP como máximo.	Unos 15 usuarios por AP como máximo.
Escalado	Puntos de acceso conectados con WDS.	Puntos de acceso cableados.

Enlaces de interés.

Wi-Fi Alliance: Organización precursora y mantenedora de los estándares relacionados con las redes inalámbricas (http://www.wi-fi.org).

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos): Organización internacional dedicada, entre otras tareas, a la creación y mantenimiento de estándares. Publica los estándares 802.11. (http://www.ieee.org).

Estudio sobre la (in) seguridad del protocolo WEP (http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html).

Listado de protocolos IEEE 802.11 (http://es.wikipedia.org/wiki/IEEE_802.11).

Tipos de antenas para transmisiones inalámbricas (http://www.ensenadamexico.net/hector/it/reporte_antenas.php).

Glosario.

AP (Access Point): Punto de acceso inalámbrico. El dispositivo que proporciona el acceso inalámbrico a la red a los usuarios finales.

DMZ (Demilitarized Zone): También conocida como red perimetral. Una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. En ella se permiten conexiones desde ambas redes, pero la red DMZ solo puede establecer comunicaciones con la red externa, siendo la interna inaccesible para los equipos dentro de la red DMZ.

LEAP (Lightweight Extensible Authentication Protocol): Versión ligera del protocolo de autenticación extensible. Es el más sencillo de los protocolos de autenticación extensible utilizados en las redes inalámbricas. Más información sobre estos protocolos en: http://es.wikipedia.org/wiki/Extensible_Authentication_Protocol