UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

“SEGURIDAD DE RED INALÁMBRICA DE BANDA ANCHA WiMAX IEEE 802.16”

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

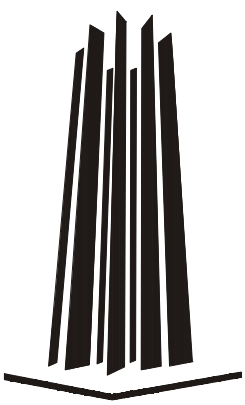
INGENIERO MECÁNICO ELECTRICISTA

(ÁREA ELÉCTRICA Y ELECTRÓNICA)

P R E S E N T A:

DANIEL VILLASEÑOR GARCÍA

ASESOR: ING. JOSÉ LUIS PÉREZ BÁEZ



MÉXICO **2010**

Agradecimientos

A la **Universidad Nacional Autónoma de México**, por la oportunidad de permanecer a una gran comunidad Universitaria como lo es la máxima casa de estudios. Y haberme ofrecido una educación de excelencia.

A la **Facultad de Estudios Superiores "Aragón"**, por forjar mi educación dentro de sus aulas y laboratorios. A las autoridades, a todo su personal administrativo y académico, a los maestros y maestras que con su labor diaria hicieron más enriquecedor mi aprendizaje.

A mi Director de Tesis **Ing. José Luis Pérez Báez**, por su orientación y apoyo al presente proyecto y por compartir sus conocimientos en materia de telecomunicaciones.

A cada uno de los miembros del H. Jurado y sinodales, por sus atenciones y consejos, **Ing. Jesús Núñez Valadez, Ing. Alejandro Rodríguez Lorenzana, Ing. María Guadalupe Zúñiga González, Ing. Francisco Javier Romero González.**

Dedicatorias

A mi papá **José**, por haber creído en mí y enseñarme que el trabajo es una bendición que Dios nos da.

A mi mamá **Lupita**, por darme la vida, los mejores consejos y sobre todo por hacer de mí un hombre de bien.

A mi hermano **José Jesús,** por brindarme tu apoyo incondicional, por ser un gran ejemplo de lucha y perseverancia.

A mi hermana **Gloria**, por inculcarme tu espíritu de superación.

En especial a mi esposa **Alma**, por estar juntos y compartir los momentos más importantes de mi vida, por enseñarme a vencer mis miedos y hacerme ver que no hay imposibles en esta vida. Y por el gran amor que me has dado, te AMO mi chaparrita.

Al **Ing. Román González**, por su paciencia, consejos y apoyo recibido durante todos estos años de amistad.

A mis amigos y familiares por todo el apoyo brindado en esta etapa de mi vida. A los que están en esta vida terrenal y con admiración y respeto a los que están en una vida celestial.

Índice de Contenido

Índice de figuras

Índice de tablas

Introducción

Con la evolución tecnológica de las redes inalámbricas y el abaratamiento de los equipos móviles ha crecido una gama de nuevos servicios que intentan explotar las ventajas que ofrecen las redes inalámbricas. No obstante, la aparición de estos nuevos servicios implica nuevas necesidades y requerimientos, entre los cuales uno de los más críticos es la seguridad.

El impacto del problema de seguridad depende en gran medida del tipo de red inalámbrica que se esté utilizando. Una red inalámbrica de tipo público no requiere una seguridad de acceso para sus usuarios, por otro lado, la red interna de una empresa privada necesita un adecuado sistema de seguridad debido a la información confidencial que maneja.

Podemos dividir la seguridad en las redes inalámbricas en dos categorías: la seguridad al momento de autenticar los usuarios e identificar sus correspondientes permisos, y la seguridad al momento de transmitir los datos entre dispositivos inalámbricos usando ondas de radio.

En este trabajo se pretende conocer que tan vulnerables son, a los diferentes tipos de ataques, y que tipo de soluciones tecnológicas hay para este tipo de redes inalámbricas hoy en la actualidad. Poniendo especial atención al estándar IEEE 802.16 WiMAX.

Capítulo I Antecedentes teóricos

1.1 Internet TCP/IP

1.1.1 Introducción

Internet es una red de redes, con alcance global, en la cual se basan la gran mayoría de los sistemas de información y comunicación actuales.

El éxito de Internet se debe, sin duda, a que es una red abierta, independiente y que funciona sobre la base del protocolo IP *(Internet Protocol, Protocolo de Internet)*, un estándar diseñado para su uso en sistemas interconectados de redes de comunicación de computadoras por intercambio de paquetes.

1.1.2 Antecedentes de Internet

El concepto de conectar sistemas y su empleo en una red compartida que permitiese la conexión entre dos computadoras comenzó a principios de la década de los 60. Pero hasta 1969 se tomo la decisión de poner en marcha una red experimental que hiciera posible el intercambio de información entre computadoras remotas. Esta red fue financiada por Estados Unidos por la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa (DARPA).

Algunos años después, cuando la Fundación Nacional de Ciencias quiso construir una red para interconectar a los institutos de investigación, adopto el protocolo del sistema de ARPAnet, que es considerado el embrión de lo que con los años ha llegado a ser Internet.

Internet surgió de la necesidad de poder interconectar sistemas de información claves, con la finalidad de que la transmisión – recepción se cumpliera de una forma correcta desde cualquier punto previamente establecido.

1.1.3 Protocolo TCP/IP

Un protocolo de red es un conjunto de reglas que deben seguir los datos de comunicaciones en una red para realizar distintas transacciones de red.

El conjunto de todos los protocolos utilizados en Internet se denominan de forma genérica familia de protocolos TCP/IP. Los protocolos más importantes dentro de esta pila son:

- **IP** *(Internet Protocol).*

  Define cómo se forman los paquetes y tiene como tarea el encaminamiento y la entrega de paquetes al punto de destino.

- **TCP** *(Transmission Control Protocol, Protocolo de Control de Transmisión)*.

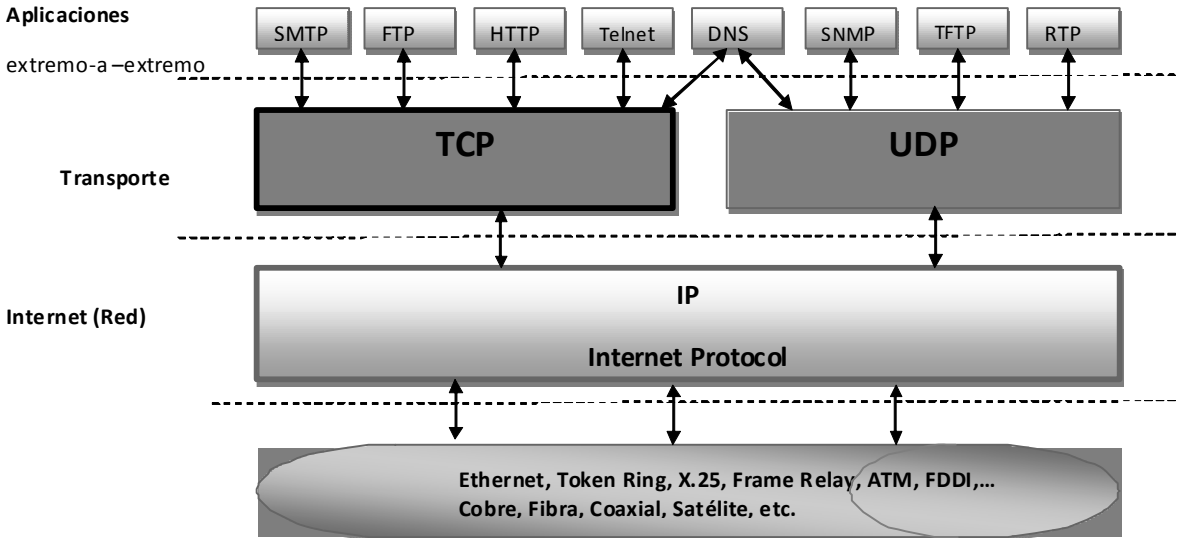
  Es un protocolo orientado a la conexión y que permite que un flujo de bytes que se originan en una computadora se entreguen sin error a otra computadora de la red.

- **Protocolos de Aplicación**.

  Incluye todos los protocolos específicos de las aplicaciones básicas de Internet, como transferencia de ficheros (FTP), acceso a terminal virtual o remota (TELNET), correo electrónico (SMTP), acceso y navegación por páginas en el World Wide Web (HTTP), Chats (IRC) etc.

TCP/IP es un paquete de protocolos (más de 100) que proporciona a los equipos el inmenso conjunto de funciones para la conexión en red disponible actualmente. Todas las funciones que se llevan a cabo en Internet son posibles gracias al protocolo TCP/IP.

Figura 1.1 Algunos de los protocolos utilizados en Internet.



Las aplicaciones del protocolo TCP/IP han ido creciendo a medida que se ha ido desarrollando Internet e integrándose en nuestras vidas.

1.2 Tipos de Internet

Los primeros trabajos de DARPA sólo incluían una versión de protocolo TCP, y de hecho estas siglas no significaban lo que significan hoy, sino *"Transmission Control Program" (Programa de Control de Transmisión).*

Versión 1

La primera versión de TCP apareció en 1973. Luego fue revisada y documentada en el RFC 675, *"Specification of Internet Transmission Control Program" (Especificación de la transmisión por Internet del Programa de Control)*, en diciembre de 1974.

Versión 2

Posteriormente el protocolo evolucionó hasta su versión 2 en marzo de 1977. Sin embargo, el verdadero surgimiento de TCP/IP no se produjo hasta agosto de ese año, en el que Jon Postel,

uno de los más importantes pioneros de Internet y TCP/IP, postuló que el hasta entonces TCP hacía demasiado.

Versión 3

Básicamente, el primer TCP englobaba funciones de las capas 3 y 4 del modelo OSI, y estas observaciones de Postel culminaron con la separación en los protocolos TCP e IP. El primer paso para separar TCP e IP se dio en 1978 con la versión 3.

Versión 4

No fue hasta 1980 cuando se publicó la versión que seguimos usando hoy día, la versión 4 de IP. Esta es la razón por la que la conocemos como IPv4. Este TCP/IP pronto se convirtió en el estándar para ARPAnet. Durante 1980 más y más máquinas se conectaron a la naciente ARPAnet y nació Internet.

IPv4 es la versión 4 del Protocolo IP. Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.

Versión 5

IPv5 es la versión 5 del Protocolo IP definida como tal en el año 1979 y que no transcendió más allá del ámbito experimental. Nunca se llegó a utilizar como una versión del Protocolo de Internet.

La versión número "5" en la cabecera de IP fue asignada para identificar paquetes que llevaban un protocolo experimental, que no era IP, sino ST. ST nunca fue extensamente usado y como la versión número 5 ya estaba asignada, la nueva versión del protocolo IP tuvo que quedarse con el identificador siguiente, el 6 (IPv6). ST está descrito en el RFC 1819.

Versión 6

IPv6 es la nueva versión del Protocolo Internet, diseñado como el sucesor para el IP versión 4 (IPv4) [RFC-791]. Los cambios del IPv4 al IPv6 recaen principalmente en las siguientes categorías:

Capacidades de Direccionamiento Extendida, el IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multienvío se mejora agregando un campo "ámbito" a las direcciones multienvío. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos.

Simplificación del Formato de Cabecera Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcional, para reducir el costo del caso común de proceso de tratamiento de paquete y para limitar el costo del ancho de banda, de la cabecera IPv6.

Soporte Mejorado para las Extensiones y Opciones Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

Capacidad de Etiquetado de Flujo Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cual el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

1.3 Manejo de los RFCs

Un documento RFC *(Request for Comment, Solicitud de Comentario)* es un documento oficial del IETF *(Internet Engineering Task Force, Grupo Especial de Ingeniería de Internet)* que especifica los detalles de las nuevas especificaciones o protocolos de Internet.

La mayoría de la documentación oficial sobre TCP/IP está disponible a través de una serie de Solicitudes de comentarios (RFCs). La biblioteca de RFC incluye estándares de Internet y reportes de grupos de trabajo.

Los RFC brindan un antecedente técnico esencial para la compresión a fondo del TCP/IP. La lista incluye varios papeles técnicos sobre protocolos, utilidades y servicios.

Algunos RFC representativos aparecen en la Tabla 1.1

Tabla 1.1 Ejemplo Representativo de los más de 3000 RFCs de Internet

Número	Título
791	Internet Protocol (Protocolo de Internet)
792	Transmission Control Protocol (Protocolo de control de Transmisión)
793	Simple Mail Transfer Protocol (Protocolo Simple de Transferencia de Correo)
959	File Transfer Protocol (Protocolo de Transferencia de Archivos)
1180	TCP/IP Tutorial (Tutorial de TCP/IP)
1188	Proposed Standard for transmission of datagrams over FDDI networks (Estándar propuesto para transmisión de datagramas sobre redes FDDI)
1597	Address Allocation for Private Internets (Localización de direcciones para Internets privadas)
2000	Internet Official Protocol Standards (Estándares de Protocolos Oficiales de Internet)
2401	Security Architecture for the Internet Protocol (Arquitectura de Seguridad para el Protocolo Internet)

Se pueden encontrar estos documentos RFCs en Internet utilizando un motor de búsqueda Web e introduciendo el número RFC.

1.4 Principios de Internet TCP/IP (Teoría de Redes)

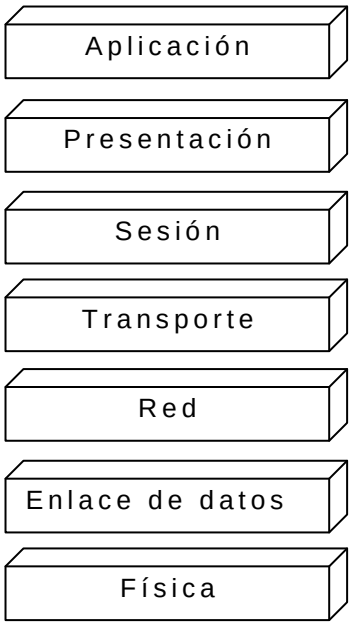
1.4.1 Modelo OSI

El modelo Sistemas Abiertos de Interconexión *(OSI, Open System Interconnection)* define los métodos y protocolos necesarios para conectar una computadora con cualquier otra a través de una red. El modelo OSI es conceptual, se utiliza principalmente para el diseño de redes y en la ingeniería de soluciones de red.

El modelo OSI fue desarrollado por la por la Organización Internacional de Estándares (ISO) en 1983 y está registrado como el estándar 7498.

El modelo OSI de red separa los métodos y protocolos necesarios para una conexión de red en siete capas distintas. Cada capa superior depende de los servicios proporcionados por una capa de nivel inferior.

Figura 1.2 Las siete capas del Modelo OSI de red



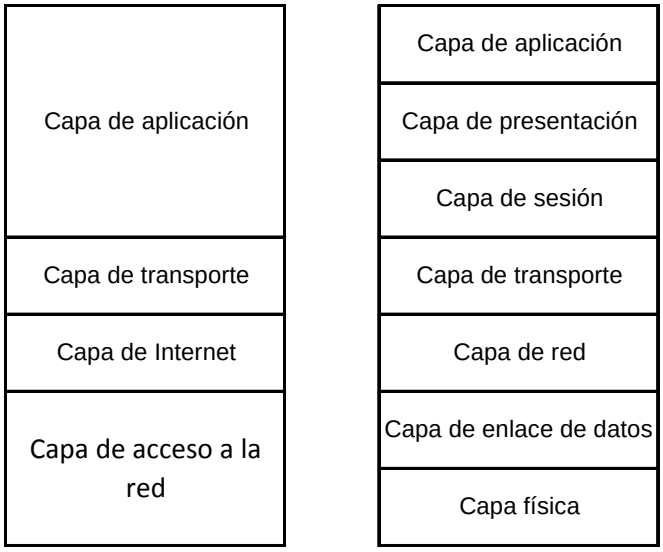
1.4.2 TCP/IP y el modelo OSI

El paquete de protocolos TCP/IP es un componente fundamental de las redes modernas. Desde su aparición, el protocolo TCP/IP ha demostrado ser lo suficientemente flexible y robusto para prácticamente cualquier uso de una red, lo que le ha convertido en el protocolo de redes más popular del mundo. IP se utiliza para direccionar la inmensa mayoría de las redes

privadas y es el único método de direccionamiento utilizado en internet. El modelo de referencia OSI está íntimamente relacionado con el protocolo TCP/IP y sus funciones de red asociadas.

El modelo OSI ha tenido bastante influencia en el crecimiento y desarrollo de las implementaciones de protocolos, por lo que es común ver la terminología del modelo OSI aplicada a TCP/IP. La figura 1.3 muestra la relación entre las cuatro capas del estándar TCP/IP y las siete capas del modelo OSI. En donde se podrá notar que el modelo OSI divide las tareas de la capa de aplicación en tres capas: Aplicación, Presentación y Sesión. El modelo OSI divide las actividades de la capa de acceso a la red en la capa de enlace de datos y la capa física.

Tabla 1.2 Relación de capas TCP/IP y OSI



1.4.2.1. Descripción de las capas de TCP/IP

- **Capa de acceso a la red**

Brinda una interfaz con la red física, da formato a los datos para adecuarlos al medio de transmisión y los direcciona para la subred basándose en direcciones físicas del hardware. Provee una verificación de errores para los datos enviados por la red física.

- **Capa de Internet**

Provee un direccionamiento lógico, independiente del hardware, para que los datos puedan pasar a través de las subredes con diferentes arquitecturas físicas. Realiza un ruteo para reducir el tráfico y soportar envíos a través de la red. Relaciona las direcciones físicas (usadas en la capa de acceso a la red) con las direcciones lógicas.

- **Capa de transporte**

Provee un control de flujo, verificación de errores y servicios de confirmación para la red. Sirve como interfaz para las aplicaciones de red.

- **Capa de aplicación**

Proporciona aplicaciones para la solución de problemas de la red, así como transferencia de archivos, control remoto y actividades de Internet. También soporta interfaces para Programación de Aplicaciones (APIs) de red, que permiten a los programas escritos para un ambiente operativo específico, tener acceso a la red.

1.4.3 Protocolo Internet (IP)

El protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de transferencia que el IP utiliza, algunas veces identificada en forma más específica como datagrama Internet o datagrama IP

Las características de este protocolo son:

- No orientado a conexión
- Transmisión en unidades denominadas datagramas.
- Sin corrección de errores, ni control de congestión.
- No garantiza la entrega en secuencia.

La entrega del datagrama en IP no está garantizada porque ésta se puede retrasar, enrutar de manera incorrecta o mutilar al dividir y reensamblar los fragmentos del mensaje. Por otra parte, el IP no contiene suma de verificación para el contenido de datos del datagrama, solamente para la información del encabezado.

En cuanto al ruteo (encaminamiento) este puede ser:

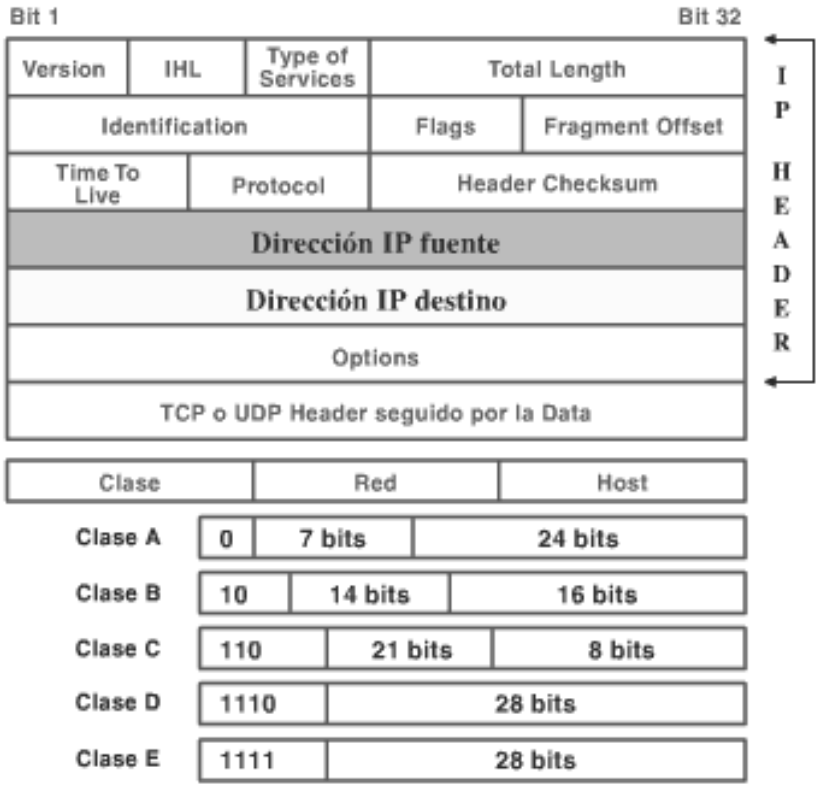
- Paso a paso a todos los nodos
- Mediante tablas de rutas estáticas o dinámicas

1.4.3.1 Direccionamiento IP

El TCP/IP utiliza una dirección de 32 bits para identificar una máquina y la red a la cual está conectada. Únicamente el NIC asigna las direcciones IP (o Internet), aunque si una red no está conectada a Internet, dicha red puede determinar su propio sistema de numeración.

Hay cinco formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase A hasta Clase E aparecen en la figura:

Figura 1.3 Clases de direcciones IP



Conceptualmente, cada dirección está compuesta por un par (RED (netid), y Dir. Local (hostid) en donde se identifica la red y el host dentro de la red.

La clase se identifica mediante las primeras secuencias de bits, a partir de los 3 primeros bits (de orden más alto).

Las direcciones de Clase A corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son 0.1.0.0 hasta la 126.0.0.0 (lo que permite hasta 1.6 millones de hosts).

Las direcciones de Clase B sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el 128.0.0.0 hasta el 191.255.0.0. Esto permite tener 16320 redes con 65024 host en cada una.

Las direcciones de Clase C tienen sólo 8 bits para la dirección local o de anfitrión (host) y 21 bits para red. Las direcciones de esta clase están comprendidas entre 192.0.1.0 y 223.255.255.0, lo que permite cerca de 2 millones de redes con 254 hosts cada una.

Por último, las direcciones de Clase D se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

Cabe decir que, las direcciones de clase E (aunque su utilización será futura) comprenden el rango desde 240.0.0.0 hasta el 247.255.255.255.

Por tanto, las direcciones IP son cuatro conjuntos de 8 bits, con un total de 32 bits. Por comodidad estos bits se representan como si estuviesen separados por un punto, por lo que el formato de dirección IP puede ser [red.local.local.local] para Clase A hasta [red.red.red.local] para clase C.

A partir de una dirección IP, una red puede determinar si los datos se enviarán a través de una compuerta *(Gateway, Router)*. Obviamente, si la dirección de la red es la misma que la dirección actual (enrutamiento a un dispositivo de red local, llamado *host directo*), se evitará la compuerta; pero todas las demás direcciones de red se enrutarán a una compuerta para que salgan de la red local. La compuerta que reciba los datos que se transmitirán a otra red, tendrá entonces que determinar el enrutamiento can base en la dirección IP de los datos y una tabla interna que contiene la información de enrutamiento.

Otra de las ventajas que ofrece el direccionamiento IP es el uso de direcciones de difusión (*broadcast addresses*), que hacen referencia a todos los host de la misma red. Según el estándar, cualquier dirección local (hostid) compuesta toda por 1s está reservada para difusión (broadcast). Por ejemplo, una dirección que contenga 32 1s se considera un mensaje difundido a todas las redes y a todos los dispositivos. Es posible difundir en todas las máquinas de una red alterando a 1s toda la dirección local o de anfitrión (hostid), de manera que la dirección 147.10.255.255 para una red de Clase B se recibiría en todos los dispositivos de dicha red; pero los datos no saldrían de dicha red.

1.4.3.2 Descripción de la capas del modelo OSI

- **Capa física**

  La primera capa define las propiedades del medio físico que se debe usar para crear una conexión de red. Los componentes de red presentes en el nivel físico sólo tienen una función: generar señales a lo largo del cableado físico y las interfaces de la red. Aunque existen varios métodos para generar señales en la red, tanto analógicas como digitales, el objetivo es el mismo. Cada método trata de transmitir datos binarios. Los dispositivos reales que se encuentran en el nivel físico consisten en cables (o conexiones inalámbricas que emplean ondas de radio o infrarrojos), conectores asociados al cableado y dispositivos jack receptores junto con los equipos de señalización conectados a los adaptadores de red (o los dispositivos transmisor/receptor para las comunicaciones inalámbricas)

- **Capa de enlace de datos**

  La capa de enlace de datos, Capa 2, define los estándares que establecen un significado a los bits que se transportan a través de la red de la capa física. Establece un protocolo confiable para la capa física de modo que la capa de red (Capa 3) pueda transmitir la información. Normalmente, la capa de red incluye la capacidad de detección de errores para asegurar un flujo de datos confiables. Los elementos de información que son transportados por la capa de enlace de datos se denominan tramas. Ejemplos de tipo de trama incluyen X.25 y 802.x.

La capa de enlace de datos de divide comúnmente en dos subcapas, conocidas como control de enlace lógico (LLC, Logical Link Control) y control de acceso a medios (MAC, Media Access Control). Cuando se usa, la subcapa LLC realiza tareas como las llamadas de establecimiento y terminación de conexión (el modelo OSI se puede aplicar tanto a redes de telecomunicaciones como a LAN) además de la transferencia de datos. La subcapa MAC controla el ensamble y la fragmentación de tramas, detección y corrección de errores, y direccionamiento. Los protocolos MAC más comunes son 802.3 Ethernet y 802.5 Token ring. También están los protocolos MAC 802.12 100BaseVBG, el 802.11 inalámbrico y 802.7 de banda ancha.

En la gran parte de los sistemas, los controladores de las tarjeta de de interfaz de red NIC (Network Interface Card) realizan el trabajo de la capa de enlace de datos.

- **Capa de red**

La capa de red, Capa 3, es donde se efectúa gran parte de la acción dentro de la mayor parte de las redes. La capa de red define la forma en que los paquetes llegan de un punto a otro dentro de una red y lo que lleva cada paquete. La capa de red define distintos protocolos de transmisión de paquetes, como el protocolo de Internet IP y el Protocolo de Intercambio de Paquetes *(IPX, Internetwork Packet Exchange)*. Estos protocolos de transmisión de paquetes incluyen la información de las direcciones fuente y destino. La información de direccionamiento dentro de cada paquete informa a la red el lugar al que debe enviar el paquete, con el fin de que alcance su destino, y a la computadora que recibe, le dice dónde se origino el paquete.

La capa de red es especialmente importante cuando la conexión de red pasa a través de uno o más direccionadores, los cuales son dispositivos de hardware que examinan cada uno de los paquetes y, según sus direcciones de origen y destino, los envían al destino adecuado. En una red compleja, como Internet, es posible que un paquete pase a través de 10 o más direccionadores antes de alcanzar su destino final. Dentro de una LAN, es posible que un paquete no tenga que pasar por ningún direccionador para llegar a su destino, sin embargo es posible que pase a través de uno o más.

Existen muchos protocolos en la Capa 3. Los más importantes son IP, ARP *(Address Resolution Protocol, Protocolo de Resolución de Direcciones)*, RARP *(Reverse Address Resolution Protocol, Protocolo Inverso de Resolución de Direcciones)* e ICMP *(Internet Control Message Protocol, Protocolo Internet de Mensaje de Control)*. Cada uno de estos protocolos proporciona servicios de resolución de direcciones a los dispositivos de red que utilizan servicios de niveles de red. Las redes TCP/IP no serían posibles sin los servicios que proporcionan estos protocolos.

- **Capa de transporte**

La capa de transporte, Capa 4, controla el flujo de la información de un nodo de la red a otro. Se asegura de que los paquetes sean decodificados en la secuencia adecuada y de que todos ellos sean recibidos.

El control de flujo asegura el mantenimiento de la integridad de los datos transmitidos, regulando el flujo de datos conocido como segmentación) procedentes de los procesos y aplicaciones que operan en las capas 5 a 7.

La capa de transporte sirve principalmente para separar y volver a unir los datos (proceso de manera que los nodos que participan en la transmisión de datos puedan recibir los datos a la misma velocidad que son enviados, y asegurando que no se envíen datos a mayor velocidad que la velocidad máxima de recepción). Los protocolos de la capa de transporte también suelen ser los responsables de controlar la fiabilidad de las conexiones, garantizados que los datos se reciban en el destino en el mismo orden en que fueron transmitidos, y que aquellos datos que no alcanzaron su destino sean transmitidos de nuevo. Los protocolos que ofrecen este tipo de fiabilidad (como TCP) se denominan protocolos orientados a conexión, mientras que los protocolos que no ofrecen este tipo de fiabilidad, como, por ejemplo, el protocolo UDP *(User Datagram Protocol, Protocolo de Datagramas de Usuario)* son protocolos no orientados a conexión.

- **Capa de sesión**

La capa de sesión, Capa 5, define la conexión de un usuario en un servidor de red, desde un punto de una red hasta otro punto.

La función principal de los servicios que operan en la capa de sesión es asegurar el correcto establecimiento y mantenimiento de las comunicaciones entre dos equipos. En general, las comunicaciones de redes se lleva a cabo un proceso de tres pasos para establecer comunicaciones entre nodos. El primer paso consiste en el establecimiento inicial de las reglas de la conexión lógica. En esta etapa del proceso se definen cuestiones como quién es el transmisor y cómo se lleva a cabo la transmisión. La comunicación entre dos equipos cualesquiera de una red pueden realizarse en uno de estos tres modos: símplex, semidúplex o dúplex.

- La comunicación en modo símplex es una comunicación unidireccional desde un emisor a un receptor. Este modo es casi totalmente pasivo: el receptor no realiza ninguna acción durante el proceso de comunicación. En la mayoría de las redes esta forma de comunicación no se suele utilizar.

- Cuando se negocia un proceso de comunicación semidúplex, los miembros que intervienen en la comunicación acuerdan que sólo uno de ellos transmitirá cada vez. A diferencia de la comunicación símplex, el modo semidúplex es bidireccional, y ambos nodos participan activamente en el proceso de comunicación.

- La comunicación dúplex es totalmente bidireccional y síncrona, lo que significa que cada nodos participante puede enviar y recibir datos al mismo tiempo (síncrona), y ambos nodos participan activamente en la comunicación (bidireccional). El modo dúplex es la forma más robusta de comunicación. Permite que ambos nodos transmitan y reciban al mismo tiempo. La comunicación dúplex es totalmente compatible con el hardware y las aplicaciones de red actuales.

Una vez establecidas las reglas de comunicación, el segundo paso consiste en trasladar los datos de un nodo a otro.

Una vez realizada la comunicación se lleva a cabo el tercer paso del proceso, conocido como liberación. La liberación es un acuerdo entre los nodos participantes para detener la comunicación finalizará formalmente cuando ambos nodos acuerden que han hecho lo que necesitaban hacer.

En la siguiente lista se describen dos de los protocolos y procesos de nivel de sesión más utilizados:

- RCP *(Remote Procedure Call, LLamada a Procediemiento Remoto)* RCP está muy extendido en los entornos cliente/servidor. Se suele utilizar para permitir el procesamiento de solicitudes de archivos cuando el equipo solicitante y el nodo utilizan diferentes sistemas operativos. RCP también se emplea en un amplio rango de funciones de interoperabilidad.

- NFS *(Network File System, Sistema de Archivos de Red)* NFS fue desarrollado por SUN Microsystems para los equipos Unix que utilizan el paquete de protocolos TCP/IP. Este sistema de archivos permite tratar cualquier recurso remoto (como, ejemplo, una unidad asignada) como si fuera un recurso local.

- **Capa de presentación**

La capa de presentación, Capa 6, recibe los datos proporcionados por las capas de nivel más bajo y los transforma de manera que puedan ser presentados al sistema.

El propósito de los procesos que operan en la capa de presentación es, fundamentalmente, el de actuar como traductor para los servicios que operan en el nivel de aplicación.

La conversión de tipos de datos sólo es el principio de las funciones especificadas en la capa de presentación. En esta capa también se definen otras funciones comunes como la compresión/descompresión y el cifrado/descifrado de los datos. Cuando se escribe un archivo de usuario en un disco duro, un proceso de capa de presentación podría cifrar dicho archivo para protegerlo. La aplicación con la que se está escribiendo el archivo puede ser ajena a este proceso de descifrado o cifrado.

Los protocolos de compartición de archivos que transfieran archivos a y desde los recursos compartidos a través de toda la red operan en la capa de presentación.

- **Capa de aplicación**

La capa de aplicación, Capa 7, controla la forma en que el sistema operativo y sus aplicaciones interactúan con la red.

La capa de aplicación sólo tiene la función de determinar el estado de la comunicación entre dos aplicaciones. El objetivo es determinar si los recursos están disponibles para iniciar la comunicación entre dos o más nodos además de averiguar si los equipos

involucrados son capaces de llevar a cabo la comunicación correctamente. Existen un gran número de protocolos y aplicaciones individuales que operan en la capa 7.

1.4.4 ¿Qué es una red?

Una red es un conjunto de estaciones de trabajo (por ejemplo, PC compatibles con IBM) y otros equipos (por ejemplo, impresoras), conectados entre sí con la finalidad de intercambiar información o compartir recursos. Las redes pueden tener diferentes tamaños: algunas caben en una sala, mientras que otras se extienden por más de un continente.

Las redes de computadoras nacen como evolución de los sistemas de acceso y transmisión de información. Además cumplen fundamentalmente el objetivo de facilitar el acceso a información remota, comunicación entre personas y entretenimiento interactivo.
Al crear una red, se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rigen la transmisión de datos. Al primer factor le llamamos nivel físico y al segundo protocolos.

En el nivel físico generalmente encontramos señales de voltaje que tienen un significado preconcebido. Estas señales se agrupan para formar entidades llamadas paquetes de datos. La forma como se accesan esos paquetes determinan la tecnología de transmisión: *broadcast*, *multicasting* o *point-to-point.*

Las redes de tipo *broadcast* se caracterizan porque todos los miembros (nodos) pueden accesar a todos los paquetes que circulan por el medio de transmisión.

Las redes *point-to-point* sólo permiten que un nodo se conecte a otro en un momento dado.

1.4.4.1 Clasificación de redes por su área de cobertura.

A veces son posibles múltiples rutas de diferente longitud. En general las redes geográficamente pequeñas suelen usar *broadcast* pues mientras estén más cerca se puede hacer la conexión de todos los elementos con todos y las redes más grandes son de *punto a punto* tal como se tienen que hacer la conexión para comunicar Europa y América a través de cableado submarino.

1.4.4.1.1 Red de área personal (PAN)

Es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal, así como fuera de ella.

1.4.4.1.2 Red de área local (LAN)

Una red de área local (LAN) consta de dos o más ordenadores enlazados entre sí en una ubicación interior como un edificio de oficinas. Al enlazar los ordenadores entre sí y crear la LAN, los usuarios pueden compartir archivos y el acceso a impresoras.

Para crear físicamente una LAN cada ordenador debe enlazarse entre sí mediante algún tipo de cableado. Generalmente, se utiliza el cableado Ethernet.

1.4.4.1.3 Red de área metropolitana (MAN)

Es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado.

1.4.4.1.4 Red de área amplia (WAN)

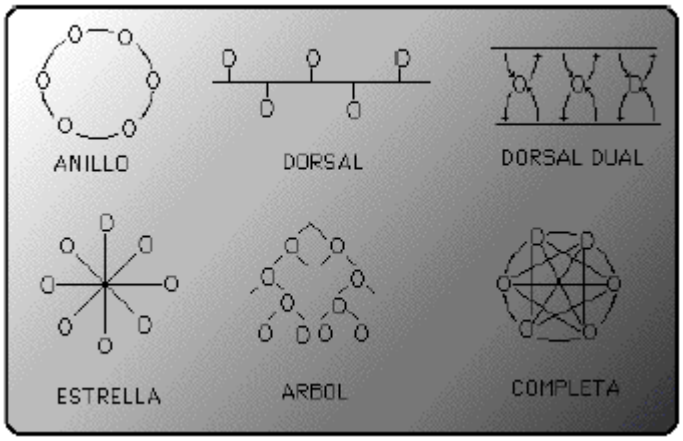
Una red de área extensa es el resultado de la conexión de dos o más LAN, generalmente utilizando servicios de acceso telefónico a través de un módem y a menudo a lo largo de distancias geográficas lejanas.

1.4.5 Topologías de las redes

La topología de una red se refiere a la forma que ésta toma al hacer un diagrama del medio físico de transmisión y los dispositivos necesarios para regenerar la señal o manipular el tráfico. Las topologías generales son mostradas en la figura 2.1 y son: anillo (ring), dorsal (bus), dorsal dual (dual bus), estrella (star), árbol (tree) y completas.

Las topologías de anillo, dorsal y árbol se adecuan mejor para redes de tipo *broadcast* y el resto para redes de tipo *point-to-point*.

Figura 1.4 Topologías de las redes



1.4.6 Nivel físico de las redes.

La capa física determina el soporte físico o medio de comunicación por el cual viajan los datos. Estos medios de transmisión pueden ser guiados y no guiados. Los primeros son aquellos que utilizan un medio sólido para la transmisión. Los medios no guiados utilizan el aire para transportar los datos: son los medios inalámbricos.

A continuación se enumeran diferentes medios de transmisión.

1.4.6.1 Medios guiados

Par trenzado UTP (*Unshielded Twisted Pair*).

El par trenzado es similar al cable telefónico, sin embargo consta de 8 hilos y utiliza unos conectores un poco más anchos. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia. Las diferentes categorías de cable son:

Categoría 3, hasta 16 Mbps,

Categoría 4, hasta 20 Mbps,

Categoría 5 y Categoría 5e, hasta 1 Gbps,

Categoría 6, hasta 10 Gbps.

Los cables par trenzado pueden ser a su vez de dos tipos:

• UTP *(Unshielded Twisted Pair, Par Trenzado no Blindado)*

• STP *(Shielded Twisted Pair, Par Trenzado Blindado)*

Los cables UTP son los más utilizados debido a su bajo costo y facilidad de instalación. Los cables STP están embutidos en una malla metálica que reduce las interferencias y mejora las características de la transmisión Sin embargo, tienen un costo elevado y al ser más gruesos son más complicados de instalar. Se utilizan únicamente para instalaciones muy puntuales que requieran una calidad de transmisión muy alta. Por otro lado, los cables UTP de categoría 5 soporta la transmisión de audio, video y datos de alta calidad, con una distancia típica de un segmento punto a punto de 100 mts. (Estándar reconocido para realizar cableado estructurado), con un número máximo de estaciones por segmento de: 1024, además de que los conectores del cable son bastante comerciales y se consiguen bajo el nombre de conector RJ45.

Cable coaxial.

El cable coaxial es similar al cable utilizado en las antenas de televisión: un hilo de cobre en la parte central rodeado por una malla y separados ambos elementos conductores por un cilindro de plástico. Las redes que utilizan este cable requieren que los adaptadores tengan un conector apropiado: los ordenadores forman una fila y se coloca un segmento de cable entre cada ordenador y el siguiente. En los extremos hay que colocar un terminador, que no es más que una resistencia de 50 Ohms. La velocidad máxima que se puede alcanzar es de 10Mbps.

La nomenclatura de los cables Ethernet tiene 3 partes: La primera indica la velocidad en Mbits/seg. La segunda indica si la transmisión es en Banda Base (BASE) o en Banda Ancha (BROAD). La tercera los metros de segmento multiplicados por 100. A continuación se describen las características de las nomenclaturas para cables coaxiales:

10-BASE-5.- Cable coaxial grueso (Ethernet grueso). Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo de 500 metros.

10-BASE-2.- Cable coaxial fino (Ethernet fino). Velocidad de transmisión: 10 Mb/seg. Segmentos: máximo de 200 metros.

10-BROAD-36.- Cable coaxial Segmentos: máximo de 3600 metros. Velocidad de transmisión: 10 Mb/seg.

100-BASE-X.- Fast Ethernet. Velocidad de transmisión: 100 Mb/seg

Este tipo de cable está dejándose de usar para la transmisión de datos, debido a las conexiones cuasi mecánicas que necesitan lo hacen poco práctico para lo cambiante que pueden llegar a ser las redes de datos. El cable coaxial más usado para la transmisión de datos cuenta con las siguientes características:

• Impedancia de 50 Ohm.

• Longitud máxima de un segmento de cable coaxial delgado 200 mts.

• Longitud máxima cable coaxial grueso 500 mts.

• Para conectar un nodo al cable coaxial grueso se requiere de un módulo receptor transmisor (*transceiver*) instalado entre el cable coaxial y el nodo.

• El cable coaxial delgado permite conectar estaciones en cadena usando conectores "T".

• Todo segmento debe estar debidamente terminado

• Número máximo de estaciones por segmento es coaxial delgado: 30.

• Número máximo de estaciones por segmento es coaxial grueso: 50.

• Distancia mínima entre estaciones con cable coaxial delgado: 0.5 mts.

• Distancia mínima entre estaciones con cable coaxial grueso: 2.5 mts (ya marcado).

El cable coaxial se clasifica como *"baseband"* si se utiliza para transmitir señales digitales y como *"bradband"* si se usa para señales analógicas. Para señales analógicas, se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada kilómetro.

Cable de fibra óptica.

La fibra óptica es una guía de onda donde la información se transmite en forma de pulsos de luz. En un extremo de la fibra se coloca un diodo luminoso (LED) o bien un laser, que puede emitir luz. En el receptor se sitúa un detector de luz (fotodiodo), cuya característica es que emite un pulso eléctrico cuando es impactado por la luz. Los fotodiodos responden hasta fracción de nanosegundo, lo cual permite velocidades en la fibra de varios Gigabits por segundo.

La fibra óptica está compuesta de un hilo ultra delgada de vidrio o silicio fundido. También existen fibras fabricadas con polímeros plásticos de calidad inferior a las de vidrio. El sistema de trasmitir luz por la fibra óptica se basa en el principio físico de la reflexión. Cuando un rayo de luz pasa de un medio a otro, el rayo se refracta en la frontera entre ambos medios. En general, la cantidad de refracción depende de las propiedades de los medios en contacto, en particular de sus índices de refracción. Si el ángulo de incidencia se encuentra por encima de un determinado valor crítico, la luz se refleja y no sale del medio.

La fibra óptica está compuesta por dos medios transparentes de distinto índice de refracción, un núcleo y un revestimiento que lo envuelve. Finalmente se envuelve el conjunto con una cubierta opaca. Así, los rayos que incidan por encima del ángulo crítico serán atrapados dentro del núcleo de la fibra.

Dado que cualquier rayo de luz incidente, por encima del ángulo crítico, se reflejará internamente, existirá una gran cantidad de rayos diferentes rebotando a distintos ángulos. A este medio de transmisión se le denomina *fibra multimodo*. Si el índice de refracción es uniforme en todo el núcleo, la fibra se conoce como de *índice escalonado*, donde los haces rebotarán en el punto de contacto del núcleo con el revestimiento, que tiene un índice de refracción diferente. Si el índice de valor del núcleo varía gradualmente, aumentando poco a poco hacia el centro del mismo, se le conoce como de *índice gradual* y los haces de luz son conducidos de forma más suave hacia el interior de la fibra, sin que reboten bruscamente, reduciendo así las perdidas en la propagación del haz de luz. Si el diámetro se reduce hasta que sea semejante al valor de la longitud de onda de la luz, la fibra actúa como una guía de ondas, y la luz se propaga en línea recta sin rebotar, produciendo así una *fibra monomodo.*

Las ventajas de utilizar fibra óptica son:

• Mayor velocidad de propagación de la señal (Velocidad de la luz)

• Mayor capacidad de transmisión (del orden de Gbps)

• Inmunidad ante interferencias electromagnéticas

• Menor atenuación (disminución de la señal) de 5 a 20 dB/Km a 400 Mhz

• Mayor ancho de banda

• Menores tasas de error : 1 error por cada 10^9 bits frente a 1 por cada 10^6 de los cables eléctricos

• No hay riesgos de corto circuito y daño de origen eléctrico

• Menor diámetro y peso

• Se pueden emplear varios canales empleando diferentes longitudes de onda simultáneamente sobre la misma fibra

• Su vida media es mucho más larga que la de un cable eléctrico

En la tabla siguiente se muestra una comparación de los distintos tipos de cables descritos:

Tabla 1.3 Cuadro comparativo de medios guiados.

	Par Trenzado	Par Trenzado Blindado	Coaxial	Fibra Óptica
Tecnología ampliamente probada	Si	Si	Si	Si
Ancho de banda	Medio	Medio	Alto	Muy Alto
Tasa de transmisión	4 Mbps	4 Mbps	500 Mbps	10 Gbps
Trasmisión de 27 Canales video	No	No	Si	Si
Distancias medias de Repetidores	100m 65 Mhz	100m 67 Mhz	500m (Ethernet)	2km(Multimodo) 100km(Monomodo)
Inmunidad Electromagnética	Limitada	Media	Media	Alta
Seguridad	Baja	Baja	Media	Alta
Costo	Bajo	Medio	Medio	Alto

1.4.6.2 Medios no guiados

Son la opción final como medio de transmisión. Esta puede tomar varias formas: ondas electromagnéticas (ondas de radio), microondas (terrestres o por satélite), transmisión infrarroja y transmisión laser.

En los medios no guiados no se requiere de cableado y algunos permiten la movilidad sin perder comunicación. Su funcionamiento es básicamente: radiar energía electromagnética por medio de una antena o transmisor y luego se recibe esta energía con otra antena ó receptor. Hay dos configuraciones para la emisión y recepción de esta energía: direccional y omnidireccional. En la direccional: toda la energía se concentra en un haz que es emitido en una cierta dirección, por lo que tanto el emisor como el receptor deben estar alineados. En el método omnidireccional: la energía es dispersada en múltiples direcciones, por lo que varias antenas pueden captarla. Cuanto mayor es la frecuencia de la señal a transmitir, más factible es la transmisión unidireccional. Por tanto, para enlaces punto a punto se suelen utilizar

microondas o laser (altas frecuencias) y para enlaces con varios receptores posibles se utilizan las ondas de radio (bajas frecuencias). Los infrarrojos se utilizan para transmisiones a muy corta distancia (en una misma habitación).

Hay ventajas y desventajas en cada uno de ellos, pero la principal desventaja es que esta forma de transmisión es susceptible al medio ambiente.
Cada día se va cableando cada vez más lugares con fibra óptica haciendo nuevas conexiones o cambiando las ya existentes, esto por las ventajas que ofrece sobre los demás medios, a pesar del costo y los algunos medios no guiados se van usando también más en redes LAN pues otorgan libertad de movilidad. Esta es la tendencia que se está siguiendo y en algún futuro posiblemente queden estos dos tipos de medios.

La transmisión inalámbrica se aplica en los usuarios móviles y cuando se necesita unir puntos separados por montañas u otros obstáculos del terreno. Algunos especialistas consideran que en el futuro los medios de transmisión serán fibra o inalámbrica.

1.4.7 Dispositivos de Interconexión de LAN's:

Los dispositivos que interconectan computadoras en una red son llamados adaptadores de comunicaciones; los dispositivos que interconectan redes son llamados elementos o dispositivos de interconexión (o conectividad).

Generalmente se clasifican de acuerdo al nivel del modelo OSI en el que operan, que puede ser:

- Físico
- De enlace de datos
- De red
- Superiores a nivel de red.

Los dispositivos de interconexión abarcan:

Segmentos: Un segmento es una interconexión física de equipos de cómputo que no contiene elementos de conectividad.

Sub-Redes: Una sub-red es una interconexión física de segmentos. Cada sub-red cuenta con sus propias direcciones de red y protocolos de comunicación.

Redes: Es una interconexión física de subredes.

Los dispositivos de interconexión también se pueden clasificar como:

- **Dispositivos de transmisión.**
  Trabajan en la capa física: Transceptores y repetidores.

- **Dispositivos de direccionamiento y segmentación.**

Operan en la capa de enlace de datos y de red: Puentes y ruteadores.

- **Dispositivos de traducción de protocolos.**
  Operan en las capas superiores del modelo OSI: Gateways o puerta de enlace.

1.4.8 Dispositivos de transmisión

Transceptores

Es un dispositivo activo sin inteligencia propia que opera en la capa física. Es utilizado para retransmitir una señal de red del nodo hacia el medio de comunicación y viceversa.
Existe una clasificación simple de acuerdo a su aplicación, los externos e internos no se consideran elementos de interconectividad:

- T. EXTERNOS: Son dispositivos externos al nodo de red, que además de sus funciones, proporcionan una interface física para la conexión del nodo de red al medio de comunicación.

- T. INTERNOS: Son dispositivos incorporados al adaptador de comunicaciones del nodo.

- MINI-TRANSCEPTORES: Son dispositivos que se incorporan opcionalmente a otro dispositivo para reconfigurar su interfaz física, o convertir una señal eléctrica en óptica y viceversa.

Ejemplo: AUI-BNC, AUI-RJ-45, AUI-ST.

Repetidor

Cuando se transmiten señales eléctricas por un cable se produce una degeneración proporcional a la longitud del cable. Es lo que se denomina *Atenuación*. Por lo tanto existen límites en cuanto a distancia antes de que la señal sea atenuada seriamente o afectada por el ruido y/o algún tipo de interferencia electromagnética.
Si la señal únicamente se amplifica en diferentes etapas, el ruido es amplificado también, por lo tanto se requiere un dispositivo que regenere y amplifique las señales, este dispositivo se conoce como repetidor. Debido a que solamente maneja la reproducción de señales y transmisión de datos a nivel de bit, se dice que se trata de un dispositivo de nivel físico. Los repetidores operan en la capa física del Modelo OSI de red.

Los repetidores actuales cumplen las siguientes funciones:

- Regenera las señales de red para que puedan viajar más lejos.

- Incrementa la longitud del cableado de un segmento.

- Incrementa el número de conexiones en red de un segmento.

- No se utiliza en protocolos superiores a la capa física del modelo OSI.

- Dos segmentos conectados por un repetidor deben usar el mismo método de acceso a la comunicación

- Los segmentos conectados mediante un repetidor forman parte de la misma red y tienen la misma dirección de red.

- Los repetidores transmiten los paquetes a la velocidad de la red.

- En Ethernet un repetidor reconstruye el campo Preámbulo de la trama.

1.4.9 Dispositivos de direccionamiento y segmentación.

Puentes (Bridges)

Es utilizado para interconectar dos segmentos de LAN a nivel de Enlace de Datos.

Las razones para su utilización pueden ser:

- Aumentar la extensión de un segmento, de la red o el número de nodos que la constituyen.

- Reducir los cuellos de botella de tráfico que se producen porque hay un gran número de equipos conectados.

- Se requiere conectar dos LAN's diferentes (Ejemplo: Token Ring y Ethernet)

- Se desea segmentar la red para evitar caídas totales de la misma.

Los puentes tienen acceso a información sobre direcciones físicas de nodos, por lo que pueden determinar el direccionamiento físico y destino de la transferencia. En base a estas direcciones pueden ser selectivos.

La operación de un puente puede resumirse en 4 pasos:

1. "Escucha" todo el tráfico.

2. Comprueba las direcciones de origen y de destino de cada paquete

3. Construye una tabla de enrutamiento cuando la información está disponible

4. Enruta los paquetes de la siguiente manera:

- Si el destino no se encuentra en la tabla de enrutamiento, el puente enruta los paquetes a todos los segmentos.

- Si el destino se encuentra en la tabla de enrutamiento, el puente envía los paquetes a ese segmento.

Los puentes realizan funciones de filtrado mediante el envío de la dirección en la trama Ethernet o en la de anillo de testigo, y de esa manera determinan a que segmento de LAN pertenece el paquete de datos. Pero no realizan funciones de encaminamiento. Las funciones de puenteado en una red se pueden implementar de dos maneras:

1. Creando el puente en los servidores mediante la instalación de varias tarjetas de red, lo cual requiere que el sistema operativo utilizado soporte puenteado.

2. Mediante dispositivos autónomos, conocido como puenteado externo, empleando puentes de fabricantes como 3COM, CISCO, entre otros…

Conmutadores (Switches)

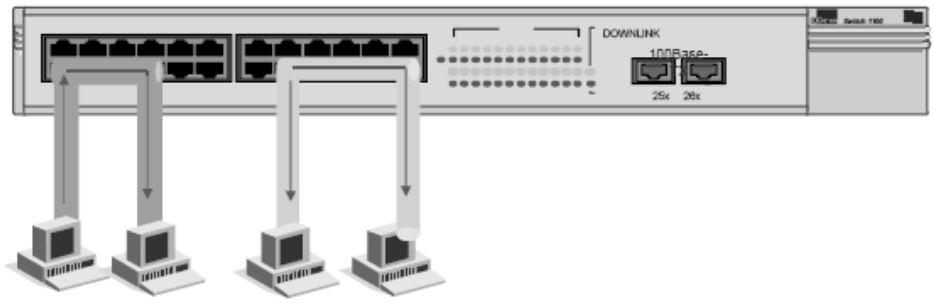
Recibe tráfico por sus puertos y lo reenvía sólo por el puerto necesario para alcanzar su destino, como se muestra en la Figura 1.4
Pueden usar dos estrategias diferentes.

- *Store and Forward:*
  Almacena el paquete en el buffer hasta que lo reciba completamente. Puede añadir latencia pero es seguro.

- *Cut Through*
  Redirecciona el paquete en cuanto puede leer la dirección destino.

- *Fragment Free*
  Transmite el paquete una vez que recibió los primeros 64 bytes. Determina si está bien el paquete y lo manda. Esta entre los dos métodos anteriores en cuento a rendimiento y confiabilidad.

Figura 1.5 Puerto Switchado o conmutado



Ruteadores o encaminadores (Routers)

Operan en el nivel de red del Modelo OSI. Se encargan de enviar información a través de una red, utilizando las direcciones lógicas de los dispositivos. Utilizan algoritmos específicos de ruteo para determinar la mejor trayectoria entre dos o más dispositivos.

Procesamiento de paquetes realizado por los enrutadores:

- Se comprueba si el paquete tiene algún error, con el uso del valor CRC contenido en el paquete.
- Se descarta la parte de información del paquete añadida por el nivel físico y de enlace de datos.
- Se evalúa la información añadida por los protocolos de red.

En base a la información obtenida es posible que:

- El paquete este dirigido al propio enrutador, por lo que continua examinando el resto de la información
- Si la dirección del paquete no se encuentra dentro de sus tablas de rutas lo descarta.
- Si no puede localizar la ruta, puede descartar el paquete y generar un mensaje de error.

1.4.10 Dispositivos de traducción de protocolos.

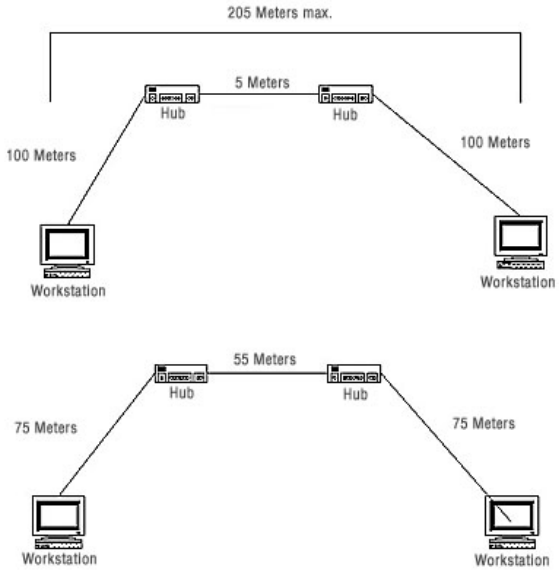
Gateway o pasarela

Consiste en una computadora u otro dispositivo que actúa como traductor entre dos sistemas que no utilizan los mismos protocolos de comunicaciones, formatos de estructuras de datos, lenguajes y/o arquitecturas.
Modifica el empaquetamiento de la información o su sintaxis para acomodarse al sistema destino. Operan en el nivel de aplicación del modelo OSI.

Concentradores (Hubs)

Un concentrador o Hub es un elemento que provee una conexión central para todos los cables de la red. Los Hubs son dispositivos con un número determinado de conectores, habitualmente RJ45 y conectores adicionales de tipo diferente para enlazar con otro tipo de red. Están provistos de salidas especiales para conectar otro Hub a uno de los conectores permitiendo así ampliaciones de la red, como se muestra en la Figura 1.8.

Figura 1.6 Ampliación de red usando Hubs



Evolución de los concentradores.

De 1era. Generación: Actuaban únicamente en el nivel físico como repetidores

De 2da. Generación: También se conocen como concentradores inteligentes, ya que incorporan características de gestión tales como detectar fallas y estadísticas en la red.

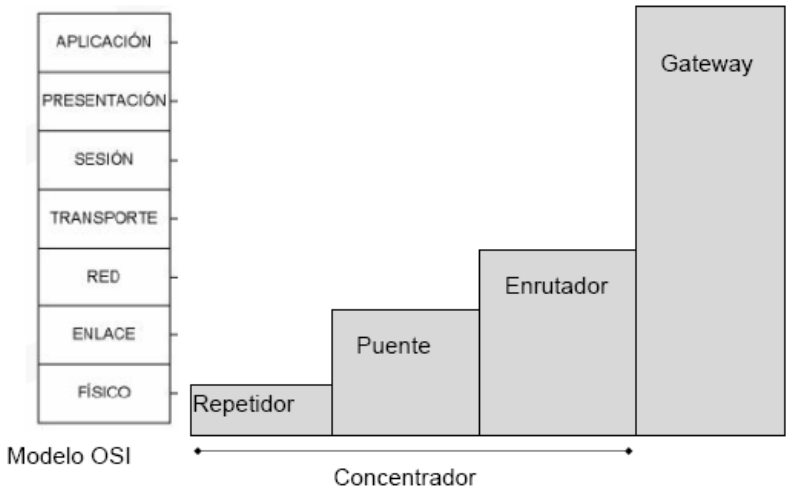
Sus principales utilidades son:

- Incluyen puertos para soportar diferentes medios como Ethernet, Token Ring y FDDI.
- Permiten crear segmentos lógicos dentro de una red.
- Administración integrada, con la que es posible administrar el concentrador en forma centralizada a través de la red, usando el protocolo SNMP u otros protocolos y software de administración de redes.
- Capacidad de descubrir en forma automática las distintas velocidades de conexión.
- Enlaces ascendentes *(uplinks)* de alta velocidad que conectan al concentrador con la red troncal. Estos enlaces trabajan normalmente 10 veces más rápido que la velocidad básica del concentrador.
- Funciones integradas de puenteo y direccionamiento, con lo que no es necesario el uso de dispositivos separados para efectuar las tareas de conexión en puente y direccionamiento.

- Capacidad de interrupción integrada, donde los nodos del concentrador pueden conmutarse o compartirse.

- Poseen señalización fuera de banda que conecta estaciones de gestión remota al concentrador por medio de líneas separadas, que permanecen activas incluso si falla la comunicación con la LAN.

Figura 1.7 Redes de área local y el modelo OSI



.

1.5 Gigabit Ethernet e IPv6

1.5.1 Ethernet

Ethernet es un estándar de conexión de redes que se ha utilizado desde mediados de los años setenta, cuando Xerox presentó el primer producto Ethernet. Ethernet es un estándar de conexión de redes definido por la especificación IEEE 802.3 *(Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos)*. Ethernet es un conjunto de especificaciones que define como se comunica y opera el hardware utilizado para crear y configurar una red.

Ha sido y sigue siendo tremendamente popular. De hecho, la gran mayoría de las redes domésticas y de oficinas pequeñas son redes Ethernet y la inmensa mayoría de las redes de gran tamaño también utilizan Ethernet, incluso las redes inalámbricas utilizan una forma de Ethernet.

Desarrollo de Ethernet

- Inicio del desarrollo e 1972 en el PARC (Palo Alto Research Center) de la compañía Xerox. Presentado por primera vez en Junio de 1976 por el Sr. Robert M. Metcalfe, su inventor.

- La primera versión (Ethernet 1.0) se presenta en 1980.
- El termino *Ether* hace referencia a un medio en el que antiguamente se creía se propagaba la luz.
- La versión 1.0 se presentó al IEEE, el cual inicia el proyecto 802 (Febrero de 1980). Con algunas modificaciones, los estándares se hacen oficiales en 1985. (10Base5). También se contemplan 1Base5 (Starlan) y 10 Broad 36 que ya no se usan actualmente.
- Para equipararse con los trabajos del IEEE, el grupo DIX (Digital, Intel y Xerox) publica en Noviembre de 1982 la versión 2.0 de Ethernet, operando a 10 Mbits/s.
- La versión 10Base2 se publica en 1988 (IEEE).
- La versión 10BaseT se publica en 1990 (IEEE).
- Hoy día ambas versiones (IEEE y DIX) tienen vigencia pero la dominante es la versión del IEEE 802.3 (ISO 8802-3: 1993).

1.5.1.1 Envío de datos con Ethernet

La especificación 802.3 define como deben enviarse los datos a través de una red Ethernet. Ethernet divide la información en pequeños fragmentos denominados tramas. Cada trama contiene entre 46 y 1500 bytes de datos. Al enviar datos a través de una red Ethernet, estos se dividen en tramas, se envían a través del cable y el equipo receptor los recompone.

Cada trama contiene información de cabecera que señala el comienzo de la misma, su procedencia y su destino. Adicionalmente, cada trama incluye un componente denominado CRC *(Cyclical Redundancy Check, Código de Redundancia Cíclica)*. El código CRC permite al equipo receptor comprobar la trama para asegurarse de que los datos contenidos en ella están intactos. Si no es así, el equipo receptor puede utilizar la información de cabecera para solicitar el reenvío de los datos al equipo transmisor.

1.5.1.2 Método de acceso

Las redes Ethernet utilizan el método de acceso CSMA/CD *(Carrier Sense Multiple Access with Collision Detection, Acceso Múltiple por Detección de Portadora con Detección de Colisiones)* para enviar datos a través de la red y controlar los problemas de transmisión. CSMA/CD no precisa ser configurado, ya que sólo indica que el dispositivo es totalmente compatible con el mecanismo de envío de datos de Ethernet.

Con CSMA/CD, todas las computadoras monitorean el medio de transmisión y esperan hasta que la línea esté desocupada antes de transmitir. Si dos computadoras tratan de transmitir al mismo tiempo, ocurre una colisión. Entonces las computadoras se detienen, esperan un intervalo de tiempo aleatorio e intenta transmitir de nuevo.

1.5.1.3 Velocidad de Ethernet

Los dispositivos Ethernet incluyen soporte para tres estándares de velocidad.

- **10Base-T** es un estándar Ethernet para redes LAN en banda base de 10 Mbps (megabits por segundo), que usa cable de par trenzado. Banda base significa que sólo se transporta un mensaje a la vez. Las redes Ethernet, normalmente, emplean cables UTP *(Unshielded Twiested-pair, Par Trenzado no Apantallado)* con conectores RJ-45.

- **100Base-T (Fast Ethernet)** las redes 100Base-T utilizan el mismo estándar Ethernet, pero tienen una capacidad de hasta 100 Mbps. La mayoría de los concentradores y adaptadores de red que se venden en la actualidad se consideran 10/100 Ethernet. Esto significa que pueden ajustarse automáticamente para comunicaciones de 10 Mbps o de 100 Mbps en función de la capacidad del resto de la red. Fast Ethernet requiere un cableado UTP con una calidad mínima de Categoría 5.

- **1000Base-T (Gigabit Ethernet)** es un nuevo estándar que proporciona una velocidad de 1000 Mbps, o 1 gigabit por segundo (Gbps). Este estándar es muy adecuado para la transferencia de vídeo de alta velocidad y otras aplicaciones multimedia relacionadas.

1.6 Seguridad, conceptos y antecedentes.

1.6.1 Antecedentes

El término seguridad proviene de la palabra *securitas* del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien.

Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

La manera en que manejamos la seguridad de la información y otros activos ha evolucionado con el tiempo, a medida que nuestra sociedad y tecnología evoluciona.

1.6.2 Seguridad física

Al inicio de la historia, todos los activos eran físicos. La información importante también era física, como lo eran las tallas en la piedra y posteriormente la escritura en papel. Para proteger estos activos, se empleaba la seguridad física, con protecciones como paredes, fosos y guardias.

1.6.3 Seguridad informática

La seguridad informática consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Hace no mucho tiempo, las redes de las empresas eran autónomas y su seguridad constituía una tarea relativamente sencilla. El perímetro de la red era fácil de definir y se podía brindar

una protección adecuada con dispositivos de seguridad simples para las brechas en la seguridad.

Sin embargo, con el avance de Internet y la generalización del uso de las redes inalámbricas, las redes de las empresas han cambiado de un modo que presenta nuevos y grandes desafíos a la seguridad. A medida que las empresas abren sus infraestructuras para admitir conectividad a Internet, trabajo remoto, movilidad inalámbrica y aplicaciones entre empresas, desaparece el perímetro de red tradicional. Las empresas han crecido tanto que desbordan los dispositivos de seguridad diseñados para las redes heredadas y ahora son mucho más vulnerables a los ataques de hackers y otros agentes perniciosos. Un dispositivo o paquete de software de seguridad individual ya no resulta adecuado como protección de redes abiertas se necesita una solución de seguridad profunda.

1.6.4 Seguridad de redes

El término “seguridad de redes” es muy amplio. En el mayor de los sentidos, significa proteger la información o los datos que están almacenados o que navegan por la red contra una modificación o divulgación intencional o accidental no autorizada.

La seguridad de redes tiene tres objetivos:

- **Confidencialidad:** Asegurar que los datos se mantengan y sean de carácter privado.
- **Integridad:** Asegurar de que los datos sean los adecuados.
- **Disponibilidad:** Asegurar que los datos sean accesibles en todo momento. Esto implica proteger la red de cualquier cosa que pueda provocar su indisponibilidad.

A medida que las empresas van volcando sus operaciones centrales a la red, la seguridad se va tornando una preocupación cada vez más importante. Antes, los ataques a la seguridad eran sólo una molestia que provocaba pérdidas de tiempo, pero ahora los riesgos son más graves. Hoy en día, una violación a la seguridad de una red cableada o inalámbrica puede desatar el caos en las operaciones más importantes de una empresa, afectando la productividad, poniendo en peligro la integridad de los datos, reduciendo la confianza de los clientes, interrumpiendo el flujo de ingresos y deteniendo las comunicaciones.

Se complica aún más la situación porque muchos sistemas de seguridad no tienen capacidad para proteger redes ni están diseñados para trabajar en cooperación con servicios de red. Esto torna a las empresas aún más vulnerables a los ataques cada vez más sofisticados que se llevan a cabo hoy.

Esto significa que las soluciones de seguridad se deben abordar como un proceso aplicado con regularidad, ya que constantemente aparecen nuevas amenazas a la seguridad. El uso de un único producto no será efectivo por mucho tiempo. Las organizaciones deben desarrollar su solución de seguridad en forma regular y dinámica a medida que surgen nuevas amenazas y que su estructura de red cambia.

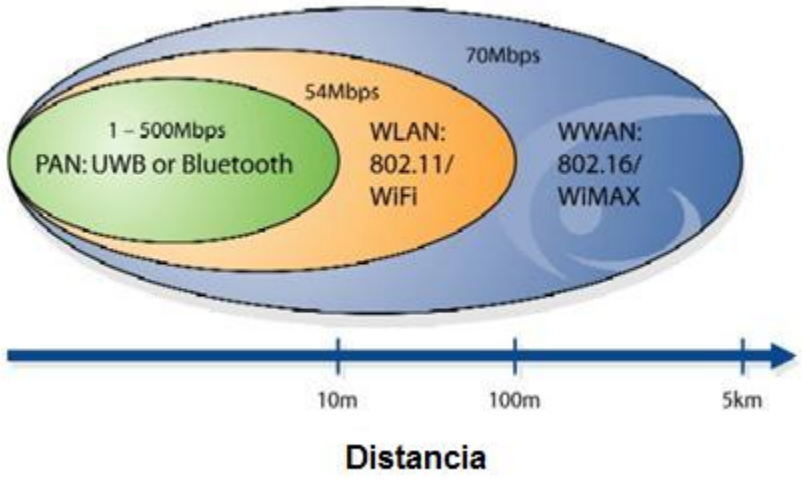
1.7 Conexiones inalámbricas de Internet.

Una de las áreas de mayor potencial en la evolución futura de las telecomunicaciones es la transmisión inalámbrica digital de banda ancha. Idealmente, un sistema inalámbrico de banda ancha permitiría la transmisión de cualquier tipo de información digitalizada (audio, vídeo, datos) desde cualquier lugar y en cualquier momento, con la posibilidad de transmitir en tiempo real de ser necesario.

Una red de área local inalámbrica o WLAN *(Wireless Local Area Network)* es un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Emplea tecnología de radio frecuencia que permite mayor movilidad a los usuarios, al minimizarse las conexiones cableadas. Las WLAN han adquirido importancia en muchos campos, incluido el empresarial, residencial, industrial y educativo, entre otros.

Existen diversas modalidades y tecnologías de redes inalámbricas, entre las que destacan Wi-Fi y WiMAX para corto/medio alcance, y Bluetooth para muy corto alcance.

Figura 1.8 Distancia de tipos de redes inalámbricas.



1.7.1 Bluetooth

El estándar Bluetooth es una especificación para redes WPAN. En realidad, no se plantea como una alternativa real a las redes WLAN propiamente dichas, sino más bien como un sustituto del cable en las conexiones de corta distancia. A pesar de que los productos basados en el estándar Bluetooth podrían ser capaces de funcionar con mayores alcances, su área de trabajo se limita normalmente a unos 10 m. El estándar se basa en tecnología FHSS, empleando una señal de 1 MHz que cambia de frecuencia central a una tasa de 1600 Hz en la banda de 2,4 GHz. El ancho de banda total ocupado es de 79 MHz. El principal potencial de Bluetooth es que ofrece bajo coste, pequeño tamaño (un solo chip) y bajo consumo de

potencia. Adicionalmente, tiene la capacidad de funcionar en entornos radioeléctricos ruidosos con buenas tasas de transmisión. Estas características, junto con el hecho de soportar tráfico de voz y de datos en tiempo real, convierten a Bluetooth en una tecnología inalámbrica muy atractiva para PDAs, periféricos, teléfonos móviles y otros dispositivos de electrónica de consumo. En la actualidad hay miles de compañías desarrollando o trabajando en productos basados en esta especificación.

La primera versión de Bluetooth, la que implementan los circuitos disponibles actualmente, puede transferir datos de forma asimétrica a 721 kbit/s y simétricamente a 432 kbit/s. Para transmitir vídeo es necesario comprimirlo en formato MPEG-4 y usar 340 kbit/s para conseguir refrescar 15 veces por segundo una pantalla VGA de 320x240 puntos. Dependiendo de las distancias que se desean cubrir, las potencias de emisión se sitúan en 1 mW para 10 m y en 100mW para 100m.

1.7.2 Wi-Fi

Wi-Fi *(Wireless Fidelity, Fidelidad Inalámbrica)* es el nombre coloquial de la familia de estándares de IEEE 802.11 para redes locales inalámbricas (WLAN) que soportan el estándar IEEE 802.11x.

Estas especificaciones definen una interfaz que va por el aire entre un cliente inalámbrico y una estación base (o punto de acceso), o entre dos o más clientes inalámbricos.

La topología de una red Wi-Fi más común es aquella en la que los equipos móviles se comunican entre sí a través de un dispositivo intermedio denominado punto de acceso (*Access Point)*. El usuario, una vez conectado a un punto de acceso, podrá ir moviéndose libremente por las zonas en las que haya cobertura y, en su movimiento irá cambiando de punto de acceso (roaming) según las necesidades, de manera que se mantenga una conexión a red en condiciones

Las WLAN disponen de un alcance más amplio que las WPAN, normalmente se ubican en edificios de oficinas, restaurantes, tiendas, casas, etc.

La norma IEEE.802.11 fue diseñada para sustituir a las capas físicas y MAC de la norma 802.3 (Ethernet). Esto quiere decir que en lo único que se diferencia una red Wi-Fi de una red Ethernet, es en la forma como los ordenadores y terminales en general acceden a la red; el resto es idéntico. Por tanto una red local inalámbrica 802.11 es completamente compatible con todos los servicios de las redes locales de cable 802.3 (Ethernet).

Todos los equipos que implementan esta tecnología (tarjetas de red, puntos de acceso, etc.) se basan en una estructura de capas de acuerdo con el modelo de referencia OSI. La primera capa es el medio de transmisión o nivel físico. Por otro lado, la siguiente capa (nivel de enlace) define el control de acceso al medio (MAC) y el control de enlace lógico (LLC). Este último está definido por el estándar IEEE 802.2, por lo que para las capas superiores una red 802.11 es equivalente a una red Ethernet, facilitándose de este modo la interconexión entre redes heterogéneas basadas en distintos estándares del IEEE. Las tasas de transmisión que permite el estándar IEEE 802.11 son de 1 y 2 Mbit/s. El esquema de modulación propuesto para

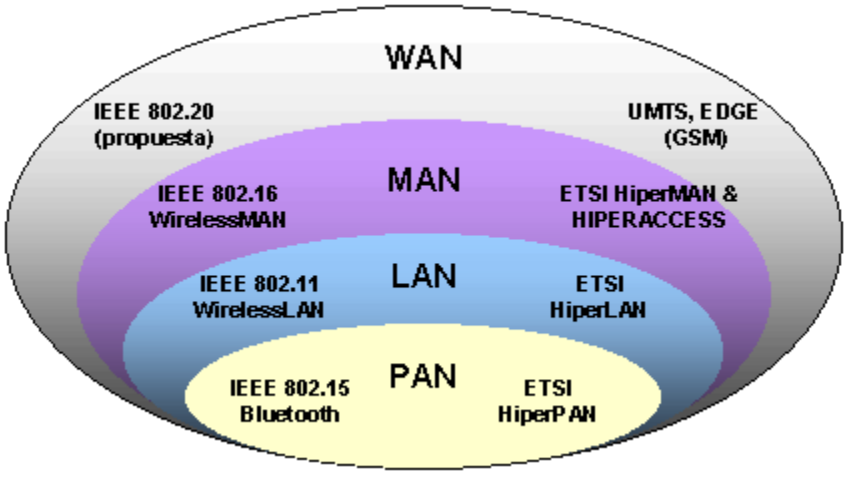
velocidades de 1 Mbps es BPSK *(Binary Phase-Shift Keying),* mientras que para 2 Mbps es QPSK *(Quadrature Phase-Shift Keying).*

1.7.3 WiMAX

La tendencia actual en telecomunicaciones es la convergencia de servicios, tecnologías, estándares; los cuales deben estar soportados por accesos de banda ancha, en la actualidad este tipo de acceso está limitado a las grandes ciudades y a los sectores con recursos económicos para utilizar estos servicios. WiMAX *(Worldwide Interoperability for Microwave Access)*, una tecnología reciente basada en el estándar IEEE 802.16 promete ser la tecnología que proveerá servicios de banda ancha en todo tipo de ambientes urbanos y rurales; zonas donde los operadores pueden suministrar diferentes servicios con inversiones bajas y despliegue rápido de tecnología, además, el servicio puede ser prestado en bandas no licenciadas, lo que aún más bajará los costos de operación.

La tecnología WiMAX es una tecnología inalámbrica basada en el estándar 802.16. En una primera versión del estándar, la 802.16-2001 se hacía referencia únicamente a sistemas que funcionaban en bandas entre 10 y 66 GHz, extendiéndose posteriormente en la versión 802.16-2004 a sistemas en bandas de frecuencias inferiores, entre 2 y 11 GHz. WiMAX hace uso de estas bandas, consiguiendo tener un funcionamiento óptimo tanto en condiciones de visión directa como en presencia de obstáculos, y siendo capaz de conseguir alcances de hasta 50 km y velocidades de hasta 70 Mbps, gracias a la utilización de capas físicas basadas en OFDM, tamaños de canal flexibles dependientes de la banda de funcionamiento, modulación adaptativa con esquemas BPSK, QPSK, 16QAM y 64QAM y duplexión tanto en tiempo como en frecuencia.

Figura 1.9 Posicionamiento de estándares inalámbricos.



Capítulo II Seguridad y aplicaciones en la actualidad

2.1 Tipos de ataque

2.1.1 Introducción

En la actualidad, los sistemas de telecomunicaciones inalámbricos han tenido un gran éxito en el mercado y se siguen extendiendo a lo largo del mundo, tal como se puede apreciar con los teléfonos inalámbricos, la telefonía celular, las redes inalámbricas de área personal "WPAN" (Bluetooth, 802.15) y de área local "Wi-Fi", (802.11a/b/g/n), entre otros, que funcionan principalmente a las frecuencias de 2.4 Ghz y 5.8 Ghz. La tecnología inalámbrica ha experimentado un gran desarrollo, y continuamente se busca la manera de superar o por lo menos brindar el mismo rendimiento que las comunicaciones mediante líneas de transmisión o alambres. La industria de acceso inalámbrico de banda ancha, provee la conexión a redes a gran velocidad y ha madurado al punto en el que ahora existe un estándar para redes inalámbricas de área metropolitana (WMAN). El estándar IEEE 802.16, conocido como WiMAX *(Worldwide Interoperability for Microwave Access)*, regula el desempeño de estas redes a nivel mundial. Este estándar es una nueva tecnología que brinda una alternativa más económica para los servicios de la última milla tales como Internet, televisión digital, videoconferencias en tiempo real y voz sobre el protocolo de Internet *(VoIP)*.

La seguridad siempre ha sido uno de los factores más delicados al momento de diseñar un sistema de comunicaciones y más aún cuando se transmite información confidencial a través de él. Las redes inalámbricas son un caso muy particular porque los datos viajan a través de un medio totalmente inseguro, lo que da origen a la necesidad de crear un sistema de seguridad específico para este tipo de tecnología.

2.2 Tipos de ataques en redes

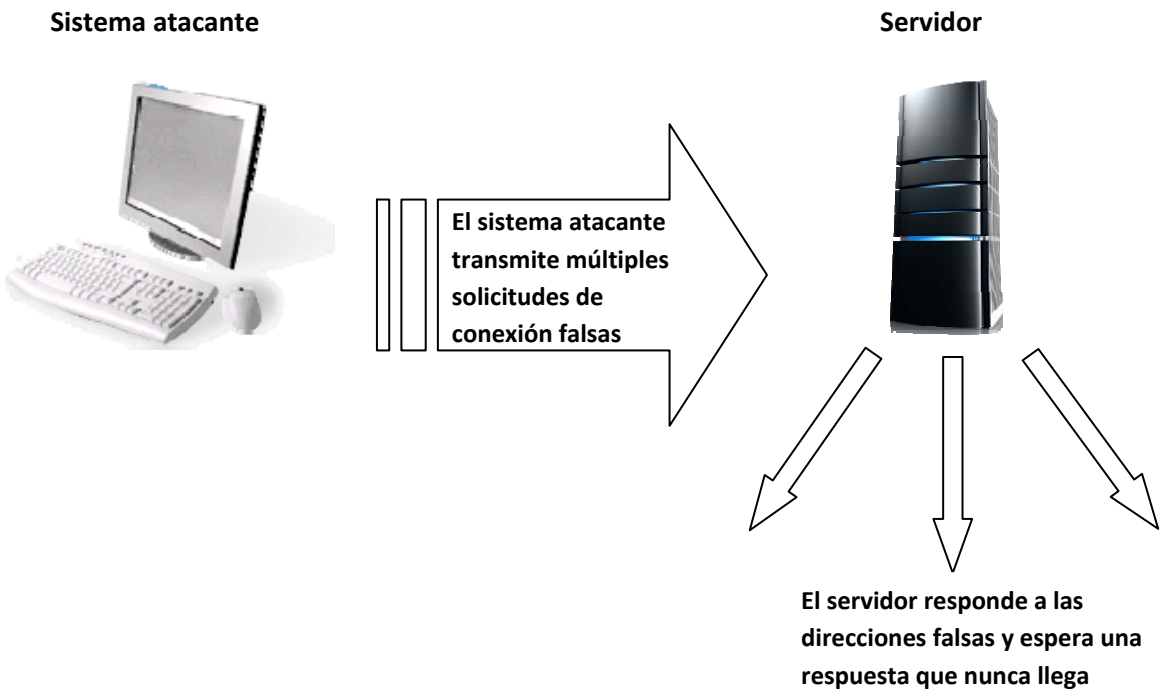
2.2.1 Denegación de servicio DoS

Los ataques de denegación de servicio *(DoS, Denial of Service)* son ataques que niegan el uso de los recursos a los usuarios legítimos del sistema. Este tipo de ataque consiste en que distintas actuaciones que persiguen colapsar determinados equipos o redes, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios.

Los ataques DoS intentan evitar que los usuarios tengan acceso a los recursos del sistema. Generalmente, este ataque se realiza saturando un servidor con solicitudes de un recurso, como ancho de banda, conexiones, espacio en disco, memoria, etc. Otra forma de este mismo ataque limita el acceso a los servicios cambiando la información de configuración.

Como se puede observar en la siguiente figura los ataques DoS saturan los servidores con tráfico y solicitudes de conexión falsos, que eventualmente agotan los recursos de un servidor.

Figura 2.1 Los ataques DoS



2.2.1.1 Métodos de ataque

Un ataque de “Denegación de servicio" impide el uso legítimo de los usuarios al usar un servicio de red. El ataque se puede dar de muchas formas. Pero todas tienen algo en común: utilizan el protocolo TCP/IP para conseguir su propósito.

Un ataque DoS puede ser perpetrado en un número de formas. Aunque básicamente consisten en:

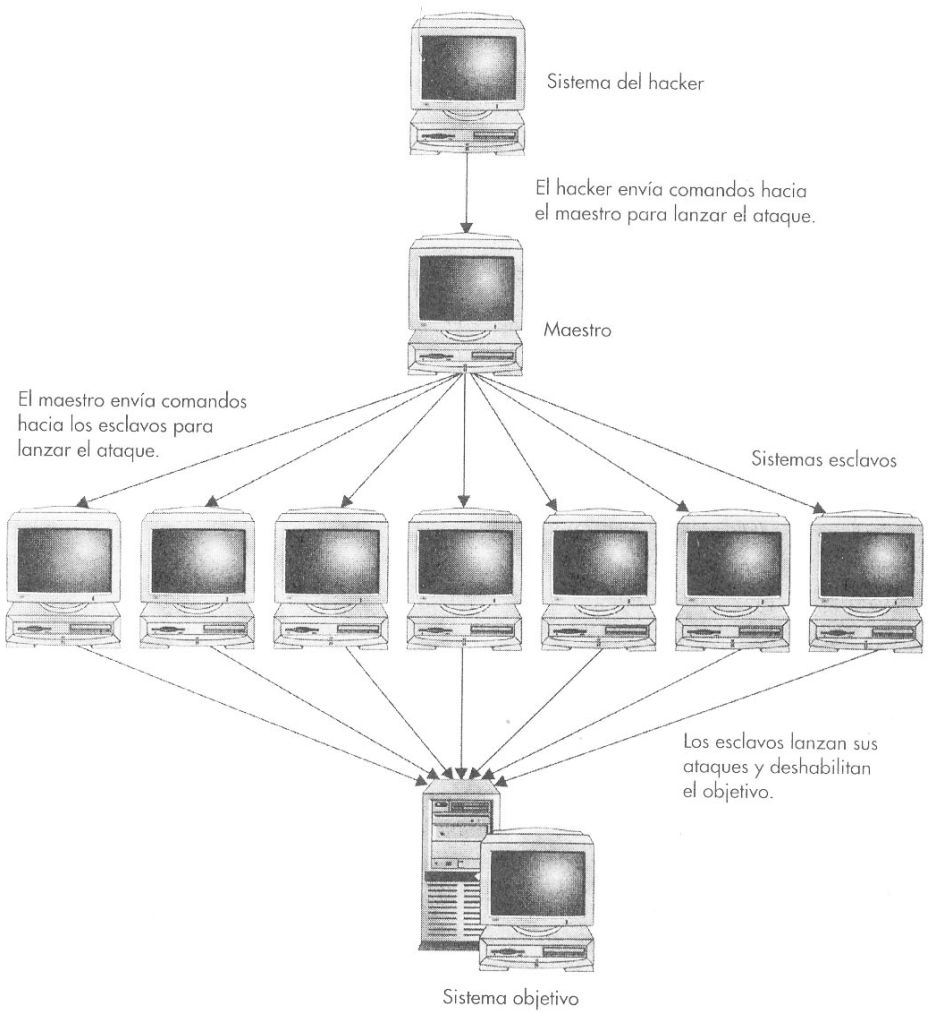
- Consumo de recursos computacionales, tales como ancho de banda, espacio de disco, o tiempo de procesador.
- Alteración de información de configuración, tales como información de rutas de encaminamiento.
- Alteración de información de estado, tales como interrupción de sesiones TCP (TCP reset).
- Interrupción de componentes físicos de red.
- Obstrucción de medios de comunicación entre usuarios de un servicio y la víctima, de manera que ya no puedan comunicarse adecuadamente.

2.2.1.2 Ataque distribuido de denegación de servicio (DDoS)

Una versión más sofisticada del ataque DoS es el ataque DDoS. Este tipo de ataque puede darse en dos fases: primero, quien origina el ataque introduce una copia del programa DoS en un sistema vulnerable. Los programas DoS están diseñados para realizar un ataque coordinado en un momento específico o después de un evento particular. Los ataques DDoS

son más difíciles de detener que los ataques DoS tradicionales debido a las múltiples fuentes del ataque. También, resulta difícil detectar quién originó el ataque.

Figura 2.2 La arquitectura de las herramientas de ataque DDoS.



2.2.2 Desbordamiento de búfer

Un ataque del tipo desbordamiento de búfer se aprovecha de un error de programación en una aplicación o en un programa del sistema.

2.2.3 Malware

El termino malware incluye todo tipo de software malintencionado o malicioso, como por ejemplo los virus, los gusanos y los troyanos o caballos de de Troya.

2.2.3.1 Virus

Desde hace mucho tiempo los virus representan un problema para la seguridad informática. Con la llegada de la PC, los antiguos virus se propagaron infectando los disquetes utilizados en diversas PC. En la actualidad, el correo electrónico, las conversaciones por Internet y otros protocolos constituyen el modo de transmisión más común. Los nuevos canales de transmisión son uno de los motivos de propagación de virus. Otro motivo es la naturaleza evolutiva de los virus en sí. Los virus son cada vez más difíciles y complejos de detectar. Tres grandes categorías de virus, en grado de complejidad ascendente, son:

- Virus no cifrados, estáticos
- Virus cifrados
- Virus polimórficos

Estas categorías representan las técnicas utilizadas por los creadores de virus para evadir la detección. Estas técnicas pueden utilizarse con diversos tipos de virus, tales como los virus de arranque, de archivos y los macro virus, los cuales varían según el método de ataque.
Independientemente de la forma en que un virus disfraza su identidad o ataca a un sistema, todos tienen tres componentes:

- La carga útil
- El método de propagación
- La fecha o condición de activación

La carga útil es el código que se ejecuta una vez que el virus se activa y puede consistir en algo tan simple como mostrar un mensaje o tan malicioso como eliminar archivos. Los métodos de propagación varían según el tipo de virus. Por ejemplo, algunos virus macro de Microsoft Word se propagan infectando la plantilla normal.dot. Algunos virus de correo electrónico recientes se propagan enviando copias de sí mismos a direcciones encontradas en el directorio infectado de un usuario. Muchos virus se activan cuando un usuario abre un archivo adjunto infectado, otros se activan en una fecha predeterminada.

2.2.3.2 Gusanos

Un gusano, como su nombre lo implica, es un programa que se arrastra de sistema en sistema sin ninguna ayuda de sus víctimas. El gusano se extiende por sus propios medios y también se reproduce por sí mismo. Todo lo que se requiere es que el creador del gusano lo active.

2.2.3.3 Caballos de Troya

Del mismo modo que los griegos utilizaron un regalo para ocultar la evidencia de sus ataque, un programa caballo de Troya oculta su naturaleza maliciosa detrás de la fachada de algo útil o interesante. Un caballo de Troya es un programa completo y autocontenido que está diseñado para realizar algún tipo de acción malintencionada. Se presenta a sí mismo como algo en que el usuario puede tener algún interés, como una nueva capacidad o correo electrónico que el usuario quiera leer.

La mayor parte de los programas de caballo de Troya también contienen mecanismos para extenderse a sí mismos a nuevas víctimas.

2.2.3.4 Phishing

Robar la identidad de una marca es un proceso denominado "*phishing"*. La técnica phishing, que comenzó como una táctica de los telemercantes para recabar información de verificación de beneficios de personas mayores, se ha convertido en una amenaza prominente para los servicios comerciales en línea.
Phishing es un engaño en el que el autor se hace pasar por una empresa legítima para hacer que las víctimas revelen información personal mediante una variedad de técnicas. Muchos engaños de phishing utilizan el correo electrónico como medio para solicitar información. El proceso comienza con una masa de correos electrónicos para solicitar al receptor que actualice su información de cuenta o que provea información personal. Supuestamente, el correo electrónico proviene de un banco, de un servicio en línea o de otro proveedor con una gran base de clientes en línea, de modo que es muy probable que los receptores sean clientes de la empresa. El mensaje contiene un enlace con un sitio de phishing que parece legítimo en el cual las víctimas deben proveer información.
Los servicios financieros y en línea son blancos conocidos de los engaños de phishing.
El Phishing constituye un ataque factible gracias a diversas razones:

Es relativamente simple falsificar una dirección de envío en SMTP (*Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo)*.

- Los autores pueden copiar fácilmente el código HTML *(HiperText Markup Language, Lenguaje de Marcado de hipertexto)*, y los archivos de imagen de sitios legítimos para crear un sitio de phishing.
- Los URL *(Uniform Resource Locator, Localizador de Recursos Uniforme)*, o los sitios de phishing a menudo parecen direcciones legítimas y logran engañar a muchas víctimas.
- Los clientes, que generalmente desconocen el potencial del phishing, confían en las empresas que supuestamente enviaron el correo electrónico.

2.2.3.5 Otras formas de malware

Los virus son probablemente la forma más conocida de software malicioso y los gusanos también son muy comunes, pero también ha surgido un host de otros tipos de malware:

Software espía *(spyware)*, también conocido como programas potencialmente no deseados (PUP): este tipo de malware puede rastrear patrones de uso y enviar información a un repositorio centralizado controlado por un atacante.

- *Keylogger*: programas que capturan las pulsaciones a medida que se tipean aprovechando las funciones de bajo nivel del sistema operativo, conocidas como hooks (conexiones), que se utilizan con fines legítimos como un código de depuración. Los keylogger (registradores de pulsaciones) son particularmente útiles para capturar nombres de usuario y contraseñas, especialmente cuando otro texto de la serie capturada indica una posible combinación de nombre de usuario y contraseña.

- Tarjetas para la captura de video, también conocidas como screen scrapper: programas que copian información del buffer de video. Resultan útiles, por ejemplo, para capturar copias de los documentos o correos electrónicos leídos por un usuario.

- *Rookit*: programas que cubren las huellas de los atacantes alterando la información de bajo nivel del sistema operativo e interceptando las llamadas al sistema de bajo nivel. Los rootkit son muy difíciles de detectar y erradicar, casi como reinstalar un sistema operativo.

- *Spam*: El spam ha crecido rápidamente y se ha convertido en un gran alterador de servicios que obstruye los sistemas de correo electrónico, atora el ancho de banda de la conexión, utiliza un espacio de almacenamiento valioso y aumenta los costos del servicio de atención al cliente. Los spammers (remitentes de correo no deseado) utilizan trucos nuevos constantemente para obstaculizar los filtros existentes y las organizaciones enfrentan el desafío de reducir la cantidad de spam garantizando que el correo electrónico comercial válido llegue a destino.

2.2.4 Ataques de suplantación de la identidad

2.2.4.1 IP *Spoofing*

Los ataques de suplantación de identidad presentan varias posibilidades siendo una de las más conocidas la denominada IP Spoofing (enmascaramiento de la dirección IP), mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así, por ejemplo, el atacante trataría de seleccionar una dirección IP correspondiente a la de un equipo legítimamente autorizado para acceder al sistema al sistema que pretende ser engañado. En el RFC 2267 se ofrece información detallada sobre el problema del “IP Spoofing”.

2.2.4.2 Protocolo ARP

También se han llevado a cabo ataques contra el protocolo *ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones)*, encargado de resolver las direcciones IP y convertirlas en direcciones físicas en una red local. Mediante esos ataques es posible secuestrar una determinada dirección física MAC *(Medium Access Control, Control de Acceso al Medio)*, de la tarjeta de red de un equipo, para hacerse pasar por este equipo ante el resto de las computadoras conectadas a esa red local.

2.2.4.3 DNS Spoofing

Los ataques de falsificación de DNS *(Domain Name System, Sistema de Nombre de Dominio)*, pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas Web falsas o bien la

intercepción de sus mensajes de correo electrónico. Estos tipos de problemas de seguridad se describen de forma más detallada a continuación:

- Redirección de los usuarios del servidor DNS atacado a *Websites* erróneos en Internet, que simulan ser los Websites reales.

- La manipulación de los servidores DNS también podría estar detrás de algunos casos de "phishing", mediante la redirección de los usuarios hacia páginas Web falsas creadas con la intención de obtener datos confidenciales, como sus claves de acceso a servicios de banca electrónica.

- Otra posible consecuencia de la manipulación de los servidores DNS serían los ataques de Denegación de Servicio (DoS), al provocar la redirección permanente hacia otros servidores en lugar de hacia el verdadero, que de este modo no podrá ser localizado y, en consecuencia , visitado por sus legítimos usuarios.

- Los mensajes de correo podrían ser redirigidos hacia servidores de correo no autorizado, donde podrían ser leídos, modificados o eliminados.

Cambios en el registro de nombres de dominio de interNIC

El registro de nombres de dominio utiliza un sistema de autenticación de usuarios registrados con bajo nivel de seguridad. Este proceso de autenticación es necesario para poder solicitar cambios ante interNIC (base de datos central con los nombres de dominio registrados en Internet) o ante alguna de las empresas registradoras de nombres de dominio. Aprovechando esta debilidad en el proceso de autentificación, un usuario malicioso podría tratar de realizar un cambio en el registro de nombres de dominio para provocar una redirección del tráfico destinado a unos determinados dominios hacia otras máquinas, o bien un ataque de Denegación de Servicio contra una determinada organización.

2.2.5 Ingeniería social

Un ataque de ingeniería social es un intento de obtener acceso a la información del sistema a partir de los empleados, mediante la utilización de juegos de rol y direcciones erróneas. Normalmente, es lo que precede a un intento para obtener acceso no autorizado a la red.

La ingeniería social es ampliamente utilizada por creadores de malware y delincuentes informáticos debido al alto nivel de eficacia logrado engañando al usuario.
Es en la preparación de un engaño en particular, donde la ingeniería social comienza a ser aplicada por parte los creadores de códigos maliciosos y otro tipo de atacantes. Cuanto más real parezca el mensaje, más confiable sea la fuente y más crédulo sea el usuario, mayores posibilidades tendrá el atacante de concretar con éxito sus propósitos y llevar a cabo la reproducción del malware.

2.2.6 Sistemas criptográficos

Los ataques contra la seguridad de los sistemas criptográficos persiguen descubrir las claves utilizadas para encriptar unos determinados mensajes o documentos almacenados en un sistema, o bien obtener determinada información sobre el algoritmo criptográfico utilizado. Podemos distinguir varios tipos de ataques contra los sistemas criptográficos:

Fuerza bruta

Una de las formas mediante las cuales se puede acceder a un sistema es ejecutando intentos de acceso por fuerza bruta. En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

La fuerza bruta se implementa con un programa que se encarga de probar múltiples claves hasta descubrir la correcta. Por lo general, las claves que se prueban son distintas combinaciones de caracteres, pero también se pueden probar palabras de un diccionario predefinido.

Por esta razón, las claves deben elegirse de gran longitud y con múltiples tipos de caracteres (números, letras y símbolos), lo que es llamado una clave fuerte.

Ataques de diccionario

Trabajan con una lista de diferentes contraseñas; palabras de un diccionario en uno o varios idiomas, nombre, nombres comunes, nombres de localidades, códigos postales, fechas de calendario, etc.

2.3 Usos y aplicaciones

En la evolución de las redes de datos, la seguridad ha ido cobrando cada vez más importancia. Ataques de diversos tipos comprometen información confidencial, bajan el desempeño de la red o incluso pueden dejarla fuera de servicio. Por esta razón, es necesario implementar técnicas que permitan proteger cualquier red de estos ataques, que cada vez son más frecuentes.

El uso de redes inalámbricas también presenta vulnerabilidades potenciales. Se sabe que los primeros protocolos de cifrado de las redes inalámbricas son débiles y fáciles de quebrar.

2.3.1 Criptografía

La criptografía es la ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar (encriptar o cifrar) la información y hacerla irreconocible a todos aquellos usuarios no autorizados de un sistema.

El termino criptografía proviene del griego *“Kriptos”* (oculto) y *“Grafos”* (escritura), por lo que significa etimológicamente el “arte de escribir de un modo secreto o enigmático”.

2.3.1.1 Sistemas criptográficos

Un sistema criptográfico está constituido por un conjunto de algoritmos y técnicas criptográficas que permiten ofrecer una serie de servicios de seguridad de la información: confidencialidad, autenticidad, e integridad.

En general, hay dos grandes tipos de sistemas criptográficos:

- Sistemas de **clave privada**: en los cuales sólo hay involucrados un emisor y un receptor, que comparten una misma clave para cifrar y para descifrar, la cual debe permanecer en secreto (por ejemplo, sucede en las comunicaciones militares o en la protección de información).
- Sistemas de **clave pública**: en los cuales hay involucrados muchos usuarios que pueden comunicarse entre sí, cada uno de los cuales tiene una clave privada (mantenida en secreto) para poder leer los mensajes que van dirigidos a él, y una clave pública (conocida por todos los usuarios) para que cualquiera pueda enviarle un mensaje cifrado (este es el caso de redes de usuarios informáticos, por ejemplo).

En la actualidad la mayor parte de los algoritmos criptográficos son públicos y se basan en una serie de operaciones elementales. La robustez del sistema criptográfico se basa en la clave utilizada.

2.3.1.2 Algoritmos de cifrado

Los algoritmos de cifrado más simples usan una única contraseña compartida para cifrar y descifrar el mensaje. Los métodos de contraseña única son, esencialmente, algoritmos de sustitución, en los que un carácter se sustituye por otro basándose en una transformación que ocurre cuando se aplica una contraseña al mensaje original.

2.3.1.3 Principales sistemas criptográficos

DES *(Data Encryption Standard)*
Se trata del algoritmo simétrico más extendido a nivel mundial, diseñado por la NSA (*National Security Agency)* en colaboración con IBM a mediados de los años setenta para las comunicaciones seguras del gobierno de los Estados Unidos.

El algoritmo DES *(Data Encryption Standard, Estándar de Encriptación de Datos)* emplea bloques de 64 bits, que se codifican mediante claves de 56 bits que gobiernan múltiples operaciones de transposición y sustitución. Estas operaciones se realizan en 16 rondas, utilizando bloques de transposición y bloques de sustitución:

- Bloques de transposición: también conocidas como “cajas P”, se encargan de la “difusión” de los bits del bloque que se está encriptando en cada ronda aplicando distintas funciones de permutación.
- Bloques de sustitución: también conocidas como “cajas S”, se encargan de añadir “confusión” al bloque de bits que se está encriptando en cada ronda del algoritmo.

Actualmente DES ya no se considera un algoritmo seguro, debido al avance experimentado por la capacidad de cálculo de las computadoras. De hecho, se puede "romper" la clave en un tiempo relativamente corto (en apenas un par de días) construyendo un equipo mediante circuitos programables *(Field Programmable Gate Array, FPGA)* de bajo costo.

DES Múltiple

Este algoritmo consiste en la aplicación del algoritmo DES en varias etapas al mensaje original, empleando distintas claves en cada etapa, para mejorar de esta forma su robustez. Se trata, por lo tanto, de una combinación de cifradores en bloque.

El más conocido es el Triple-DES, en el que se aplica el algoritmo DES tres veces: se codifica con la clave K1, se decodifica con la clave K2 y se vuelve a codificar con la clave K1, tal y como se representa en las siguientes figuras:

Figura 2.3 Encriptación con Triple-DES

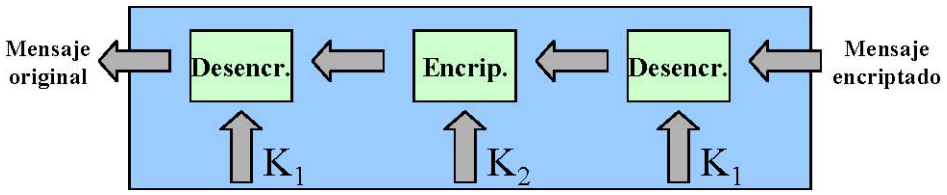
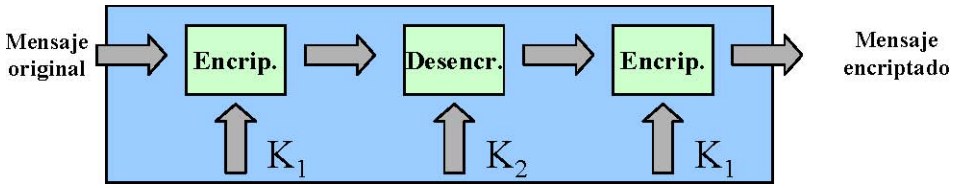


Figura 2.4 Desencriptación con Triple-DES



IDEA *(International Data Encryption Algorithm)*

Algoritmo desarrollado en Suiza (en el Instituto Federal Suizo de Tecnología, Swiss Federal Institute of Technology) a principios de los años noventa, fruto del trabajo de los investigadores Xuejia Lai y James Massey. Este algoritmo, que destaca por ser muy rápido, realiza sus operaciones en 8 rondas, emplea claves de 128 bits y trabaja con bloques de 64 bits, siendo bastante resistente a las técnicas de criptoanálisis lineal y diferencial.

Blowfish

Algoritmo desarrollado por el experto en seguridad Bruce Schneier en 1993. Se trata de un algoritmo de cifrado que trabaja con bloques de 64 bits y que realiza 16 rondas, consistente cada una de ellas en una permutación dependiente de la clave y una sustitución dependiente de la clave y de los datos, empleando claves variables de hasta 448 bits

Ha sido optimizado para poder ser ejecutado en procesadores de 32 bits y resulta bastante más rápido que el DES, por lo que ha sido elegido por bastantes empresas en los últimos años.

Skipjack
Algoritmo desarrollado por la NSA para el gobierno de Estados Unidos, dentro del proyecto del polémico chip cifrador "Clipper".

Se trata de un algoritmo clasificado como secreto, que trabaja con bloques de 64 bits, claves de 80 bits y que realiza sus operaciones en 32 rondas.

CAST
Algoritmo que realiza sus operaciones en 8 rondas sobre bloques de 64 bits y emplea claves de 40 a 64 bits. Debe su nombre a sus inventores: Carlisle, Adams, Stafford y Tavares.

RC2
Desarrollado por la empresa RSA Labs como un algoritmo de cifrado simétrico que trabaja con bloques de 64 bits y claves de tamaño variable, diseñado para operar con los mismos modos de trabajo que el DES, pero siendo el doble de rápido.

RC4
Algoritmo desarrollado por la empresa RSA Labs y presentado en diciembre de 1994, fue diseñado para el cifrado en flujo y permite trabajar con claves de tamaño variable.

RC5
Se trata de un algoritmo propuesto por RSA Labs como una mejora del RC4, para incrementar su robustez y ofrecer una mayor eficiencia computacional. Se trata, por lo tanto, de un rápido sistema de cifrado en bloque, que se basa en la realización de varias rotaciones dependientes de los datos (entre 0 y 255 rondas), trabajando sobre bloques de tamaño de 32, 64 o 128 bits, y claves de tamaño variable (entre 0 y 2.048 bits).

GOST
Este algoritmo es un estándar desarrollado por el gobierno de la antigua URSS como respuesta al algoritmo norteamericano DES. GOST realiza sus operaciones en 32 rondas y emplea claves de 256 bits.

AES (Advanced Encryption Standard)
Algoritmo conocido como "Rijndael" y diseñado por los belgas Vicent Rijmen y Joan Daemen. Resultó el ganador de un concurso convocado por el NIST (*National Institute of Standards Technology)* para la elección de un algoritmo sustituto del DES, concurso al que se presentaron 15 algoritmos candidatos. AES fue adoptado como estándar FIPS 197 *(Federal Information Processing Standard)* en noviembre de 2002.

Se trata de un algoritmo de cifrado en bloque, que utiliza bloques de 128 bits y claves variables de longitudes de entre 128 y 256 bits, con varios modos de operación.

2.3.2 Encriptación para seguridad inalámbrica

2.3.2.1 Protocolo WEP

El protocolo WEP *(Wired Equivalent Privacy, Privacidad Equivalente a Cableado)*, es el sistema de encriptación estándar aprobado en la norma IEEE 802.11b, como protocolo para redes inalámbricas, permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

2.3.2.2 Protocolo WPA

El protocolo WPA Wi-Fi Protected Access (WPA) o *(Wireless Application Protocol, Protocolo de Aplicaciones Inalámbricas)* es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas. Se trata de un sistema más robusto que WEP. Asimismo WPA emplea un protocolo de encriptación conocido como TKIP (*Temporal Key Integrity Protocol, Protocolo de Integridad de Clave Temporal)*, que permite reforzar la seguridad de las claves y proteger la red contra los ataques por falsificación o repetición.

En WPA se utilizan claves de encriptación de 128 bits que se pueden asignar de forma dinámica por usuario o por sesión, por lo que este sistema es mucho más robusto a ataques de fuerza bruta. El vector de iniciación IV del algoritmo de encriptación incrementa su tamaño de 24 a 48 bits.

Además de proporcionar autenticación y ciframiento, WPA proporciona mejor integridad de la carga útil. La verificación de redundancia cíclica *(CRC o Cyclic Redundancy Check)* utilizada en WEP es insegura porque permite alterar la carga útil y actualizar el mensaje de verificación de redundancia cíclica sin necesidad de conocer la clave WEP. En cambio WPA utiliza un Código de Integridad de Mensaje *(MIC o Message Integrity Code)* que es en realidad un algoritmo denominado «Michael», que fue el más fuerte que se pudo utilizar con dispositivos antiguos para redes inalámbricas a fin de no dejar obsoletos a éstos. El Código de Integridad de Mensaje de WPA incluye un mecanismo que contrarresta los intentos de ataque para vulnerar TKIP y bloques temporales.

2.3.2.3 Protocolo WPA2

El WPA2 (*Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2)* es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA.

WAP2 está basado en el estándar IEEE 802.11i, aprobada por la Wi-Fi Alliance (Organización creada por líderes proveedores de software y equipos inalámbricos con la misión de certificar los productos basados en el 802.11 para lograr interoperatibilidad y promover el término Wi-Fi como una marca global para cualquier producto basado en el 802.11). WPA2 provee un alto nivel de seguridad incluyendo el algoritmo AES *(Advanced Encriptyon Standard, Estándar de Cifrado Avanzado)*. WPA2 puede habilitarse en dos versiones:

- WPA2 Personal
- WPA2 Enterprise

WPA2 Personal, protege de acceso no autorizado a la red utilizando una contraseña establecida. WPA2 Enterprise, verifica a los usuarios de la red a través de un servidor.

2.3.2.4 Protocolo SSL

El protocolo SSL (*Secure Sockets Layer, Protocolo de Capa de Conexión Segura)* es un sistema diseñado y propuesto por Netscape Communications Corporation en 1994. Se encuentra en el modelo OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc. Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea reventada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

2.3.2.5 Protocolo TLS

El protocolo TLS *(Transport Layer Security, Seguridad de la Capa de Transporte)*, es una nueva propuesta que nace como una evolución de SSL, desarrollada por el IETF *(Internet Engineering Task Force)*, grupo de trabajo en ingeniería de internet), explicada en el RFC 2246.

Los protocolos SSL y TLS son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet. Tanto SSL como TLS son protocolos de nivel de transporte, por lo que podrían ser utilizados para el cifrado de protocolos de aplicación como Telnet, FTP, SMTP, IMAP o el propio HTTP. Se ubican, por tanto, entre el protocolo TCP y la capa de aplicación.

2.4 Tendencias

La seguridad de la información, va adquiriendo mayor relevancia dentro de una organización, siendo el flujo de información a través de la red el más vulnerable. A pesar del actual clima de recesión, la seguridad de la información sigue siendo una de las principales prioridades del panorama TIC (Tecnologías de la Información y Comunicación). Debido a la proliferación de amenazas y vulnerabilidades, que constituyen un riesgo permanente para la estabilidad de las redes.

2.4.1 Protección en el punto final

Se considera seguridad en el punto final *(endpoint security)* al concepto en el que básicamente cada dispositivo o punto final es responsable de garantizar su propia protección frente a amenazas y vulnerabilidades.

En este sentido, los dispositivos finales están sufriendo una importante transformación: de incluir únicamente software antivirus, han pasado a combinarlo con herramientas firewall y anti-spyware. Además, este año ampliarán sus funciones antivirus con prevención de pérdida de datos y encriptación de disco.

2.4.2 Seguridad “en la nube”

La nube es una metáfora de internet y el termino (Cloud Computing, computación en la nube) es un paradigma que permite ofrecer servicios de computación a través de Internet.

Mientras la informática Cloud Computing redefine el segmento de software a través de una aproximación basada en la web, en los próximos años serán marcados por los servicios de seguridad gestionada.

Esto se debe a que muchas empresas simplemente no cuentan con los fondos suficientes o la experiencia necesaria para enfrentarse a unas vulnerabilidades y ataques cada vez más sofisticados.

De esta forma, compañías como Trend Micro, Panda, Blue Coat o Cisco completarán su oferta de equipamiento en la casa del cliente con nuevos servicios actualizados y gestionados a través de “la nube”.

2.4.3 Ingeniería social

Cada vez más, los atacantes van directamente tras el usuario final y tratan de engañarlo para que descargue malware o divulgue información confidencial con el pretexto de que están haciendo algo perfectamente inocente. La popularidad de la ingeniería social es en parte estimulada por el hecho de que el tipo de sistema operativo y explorador Web que tiene el equipo del usuario es irrelevante en gran medida, así como lo es el hecho de que el usuario sea blanco de ataques y no necesariamente las vulnerabilidades del equipo. La ingeniería social ya es uno de los principales vectores de ataque que se utiliza actualmente y la empresa de seguridad informática Symantec, estima que la cantidad de intentos de ataque mediante técnicas de ingeniería social aumentará en los próximos años.

2.4.4 Protocolos SSL y HTTPS

Los ataques vía SSL y HTTPS se incrementarán: a medida que los sistemas de red están más preparados para bloquear los ataques externos y el malware, los delincuentes se están volviendo más hábiles a la hora de suministrar cargas útiles maliciosas en las redes. Lo que solía ser seguro, tales como los protocolos SSL y HTTPS, ahora se ha convertido en un campo fértil para llevar a cabo estos nuevos ataques.

2.4.5 Encriptación omnipresente

Las tecnologías de encriptación se han añadido de golpe a los sistemas de almacenamiento de información. Así, tanto cintas como discos duros de fabricantes como Hitachi, Fujitsu o Seagate cuentan ahora con procesadores criptográficos.

Igualmente, Intel ha anunciado el lanzamiento en 2009 de una versión de su chip vPro con soporte integrado de encriptación. Siguiendo esta tendencia, en el presente ejercicio probablemente veremos múltiples capas de tecnologías de encriptación aplicándose a todo tipo de dispositivos, generando una demanda paralela de herramientas de administración para todas ellas.

2.4.6 Virtualización

La virtualización permite que las empresas logren ahorros importantes en las operaciones de los centros de datos. Sin la seguridad basada en equipos virtuales, éstos pueden sufrir tráfico y ataques de tipo malicioso perpetrados por equipos virtuales del mismo servidor físico que se encuentran en peligro. Los sistemas operativos, las aplicaciones empresariales y las aplicaciones Web personalizadas, implementadas en equipos virtuales, son vulnerables.

A medida que la virtualización servidor y del desktop continúan avanzando, los usuarios demandarán cada vez más medidas de protección para funciones como el control de acceso basado en roles, la gestión de identidades en servidores virtuales, la seguridad de red o la Auditoría de sistemas virtuales.

VMware, Citrix y Microsoft, así como las distintas aplicaciones open source de virtualización para servidores y PCs liderarán esta tendencia, asociándose con partners del mundo de la seguridad y de las redes como IBM, McAfee, Cisco o CheckPoint.

Capítulo III Propuesta de seguridad para diversas aplicaciones

3.1 Introducción

Actualmente las redes de datos inalámbricas han revolucionado la comunicación entre computadoras, permitiendo el acceso a Internet desde cualquier lugar que pueda estar al alcance de una antena transmisora.

Para este fin se han creado distintas tecnologías que intentan que la conexión a estas redes sean lo más general posible.

Una de estas tecnologías es Wi-Fi que es un conjunto de estándares IEEE 802.11 y fue diseñada para crear redes inalámbricas locales (WLAN). Este tipo de estándares puede transmitir hasta 54 Mbps y con un alcance de hasta a 150 metros.

WiMAX es una tecnología que se basa en los estándares Wi-Fi, pero con ventajas que facilitan la creación de redes de área metropolitana (WMAN), como son: más ancho de banda, mayor distancia y mayor número de usuarios.

Las redes inalámbricas pueden aumentar potencialmente la productividad y facilitar mucho más los servicios de información a una gran cantidad de usuarios. Al mismo tiempo, las tecnologías introducen nuevas vulnerabilidades de seguridad.

3.2 Seguridad de información

Los objetivos fundamentales en Seguridad son: prevenir la revelación, la modificación y la utilización no autorizada de datos, recursos de computadora y de red. La definición del estándar ISO 7498-2 [ISO, 1989] define cinco elementos básicos que constituyen la seguridad de un sistema: la **confidencialidad** de los datos, la **autenticación** de los datos, la **integridad** de los datos, el **control de acceso** (disponibilidad) y el **no repudio**.

Confidencialidad implica que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas. **Autenticación** define mecanismos para garantizar la procedencia de la información, ya sea a nivel de usuario o de computadora. **Integridad** implica que los datos no han sido modificados o corrompidos de manera alguna desde su transmisión hasta su recepción. El **control de acceso** establece la forma en que el recurso está disponible cuando es requerido. El **no repudio** es la garantía de transmisión y recepción de información, busca proteger al emisor de que el receptor niegue haber recibido el mensaje, y proteger al receptor de que el transmisor niegue haber enviado el mensaje.

En seguridad de información, se consideran seis elementos sobre los cuales se han hecho desarrollos en busca de proporcionar ambientes protegidos:

1. **Seguridad física:** un elemento de atención básica, los recursos deben ser protegidos físicamente de accesos no autorizados, accidentes, robos, etc.

2. **Seguridad de procedimientos:** elemento enfocado a las medidas de protección en los procesos y procedimientos.

3. **Seguridad de personal:** elemento enfocado a la definición de privilegios, y accesos de personal involucrado con los recursos.

4. **Seguridad de emanación de compromisos:** elemento enfocado a la definición de responsabilidades y compromisos en el manejo de la información.

5. **Seguridad de sistemas operativos:** elemento enfocado a la protección de servicios y usuarios, accesos no autorizados al sistema operativo de una computadora.

6. **Seguridad de comunicaciones:** elemento enfocado a la transmisión segura de información a través de medios de comunicación.

3.2.1 Prevención

Prevención es la palabra clave en Seguridad, se han desarrollado una gran diversidad de técnicas y herramientas de prevención a nivel de aplicaciones, siempre dependientes del sistema operativo o la aplicación que se utilice. Los protocolos de seguridad buscan brindar servicios de seguridad en la transmisión de información, sin importar el tipo, procedencia, sistema operativo o aplicación que la genere.

3.2.2 Terminología

Dentro del área de Seguridad, se manejan diversos términos para identificar los factores que intervienen, los conceptos principales son: vulnerabilidades, ataques, y amenazas.

3.2.2.1 Vulnerabilidades

El software está desarrollado por humanos, quienes modelan e implantan programas a su criterio, concepto y conocimiento del lenguaje de programación que utilizan, es común, en consecuencia, encontrar imperfecciones en los sistemas. Son estas imperfecciones las que propician oportunidades para accesos no autorizados, las que se conocen como vulnerabilidades de los sistemas.

3.2.2.2 Ataques

Los ataques son los medios por los cuales se explotan las vulnerabilidades. Los objetivos del atacante son la intercepción y el análisis de tráfico en la red. Al estar escuchando el tráfico, el atacante puede identificar:

- El origen y destino de los paquetes de comunicación, así como la información de cabecera.
- Monitorear el tráfico y horarios de actividad.
- Identificar el uso de protocolos y observar la transferencia de datos entre protocolos que no utilicen encriptado, por ejemplo la versión no segura de Telnet o FTP que transfieren la clave de usuario en texto simple.

3.2.2.3 Amenazas

Las amenazas están dadas por condiciones de entorno, dada una oportunidad y adversarios motivados y capaces de montar ataques que explotan vulnerabilidades, podría producirse una violación a la seguridad (confidencialidad, integridad, disponibilidad y/o uso legítimo)

Cada enlace en una red y cada recurso es susceptible a diferente tipo de amenazas, de ataques, y quizá a diferentes atacantes. El análisis de riesgos y el monitoreo constante de vulnerabilidades pueden identificar las amenazas que han de ser contrarrestadas, así como especificar los mecanismos de seguridad necesarios para hacerlo.

3.3 Servicios y protocolos por capa de red.

El desarrollo de protocolos está basado en los servicios definidos en las capas de comunicación del modelo estándar OSI.

3.3.1 Seguridad en la capa física

En esta capa se tiene una dependencia significativa de la tecnología de red que se utilice. El equipo y todo lo demás cambia si hay modificación de tecnología de comunicación: Ethernet, SDH, SONET, etc. Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de trafico), no se provee servicio, pero se da soporte a las capas superiores para control de acceso, autenticación del origen de los datos e integridad orientada a no conexión. La granularidad de protección es individual o a nivel de circuitos conmutados.

3.3.2 Seguridad en la capa de enlace.

En esta capa se tiene una dependencia ligera de la tecnología (IEEE LANs) y del conjunto de protocolos que se utilice. Los servicios de seguridad son: confidencialidad, control de acceso, autenticación del origen de los datos e integridad orientada a no conexión. La granularidad de protección es en los hosts individuales y en los segmentos de la LAN.

3.3.3 Seguridad en la capa de red (inferior)

En la subcapa inferior de esta capa se tiene una alta dependencia de la tecnología de red y menor sobre el conjunto de protocolos que se utilicen. Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de tráfico limitado), control de acceso, autenticación del origen de los datos e integridad orientada a conexión y a no conexión (dependiente de la red). La granularidad de protección radica en los hosts (por conexión) y en el enrutador (LAN).

3.3.4 Seguridad en la capa de red (superior)

En la subcapa superior de esta capa no se tiene dependencia de la tecnología de red, aunque sí moderada sobre el conjunto de protocolos que se utilicen (el tunelaje de IP disminuye esto considerablemente). Los servicios de seguridad son: confidencialidad (incluyendo confidencialidad del flujo de tráfico limitado), control de acceso, autenticación del

origen de los datos e integridad orientada a no conexión y a secuencia parcial. La granularidad de protección radica en los hosts, en la red o seguridad de calidad de servicio *(QoS)*.

3.3.5 Seguridad en la capa de transporte

En esta capa no se tiene dependencia de la tecnología de red, aunque sí alta dependencia sobre el conjunto de protocolos que se utilice. Los servicios de seguridad son: confidencialidad, control de acceso, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orientada a no conexión e integridad orientada a conexión con recuperación de datos. La granularidad de protección radica en los hosts por conexión.

3.3.6 Seguridad en la capa de sesión

En esta capa no se tiene dependencia de la tecnología de red, aunque sí alta dependencia sobre el conjunto de protocolos que se utilice. Los servicios de seguridad son integridad orientada a conexión, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orientada a conexión y control de acceso. La granularidad de protección radica en las sesiones.

3.3.7 Seguridad en la capa de aplicación

En esta capa no se tiene dependencia de la tecnología de red. La dependencia es significativa sobre las aplicaciones. Los servicios de seguridad son: confidencialidad (orientado a conexión, a no conexión, o a un campo selectivo), autenticación del origen de los datos, autenticación de la entidad extremo, integridad (orientada a conexión y a no conexión, con opción a recuperación) y no repudio (en el origen y recepción). La granularidad de protección radica en los usuarios, aplicaciones y PDUs *(Protocol Data Unit)*.

3.4 Mecanismos específicos de seguridad

Se han desarrollado una gran variedad de algoritmos, mecanismos y técnicas para brindar protección a los recursos informáticos, y garantizar la integridad, confidencialidad y control de acceso de información.

La confidencialidad es necesaria para mantener un secreto, pero sin autenticación, no puede saberse que la persona con la que se está compartiendo ese secreto, es quien dice ser, y sin la confianza de la integridad del mensaje recibido, no se sabe si el mensaje es el mismo al que fue enviado. Los mecanismos descritos en esta sección están enfocados a garantizar estos aspectos.

3.4.1 Criptografía

La Criptología es un área de estudio de las Matemáticas con gran aplicación en las Ciencias de la Computación, se divide en dos ramas: la criptografía, que involucra lo relacionado al diseño de sistemas para encriptar o cifrar información, y el criptoanálisis sobre el proceso inverso, involucra los sistemas para desencriptar o descifrar códigos.

3.4.2 Mecanismos de control de acceso y autentificación

La autenticación es uno de los problemas más complicados en seguridad. Implica reconocer y garantizar que alguien (persona o computadora) es quien dice ser. La autenticación es un servicio básico de seguridad. Puede hablarse de autenticación con criptografía o sin criptografía, los grandes problemas radican en la autenticación de personas y los mecanismos de distribución de llaves y certificados.

Las firmas digitales es uno de los mecanismos más utilizados para el intercambio de mensajes en el correo electrónico. Los mecanismos de llaves digitales implican esquemas de confianza, el esquema común es que una persona cree su llave digital, y solicite que al menos otras dos firmen su llave, de esta manera hay al menos dos testigos de que esa llave le pertenece a esa persona. La generación de llaves para computadoras, son esquemas actuales, en sistemas seguros a nivel de red, no de usuario.

En lo que se está actualmente trabajando y buscando establecer, es la Infraestructura de Llaves Públicas *(Public Key Infraestructure, PKI)*. Una infraestructura que forma un sistema en el que participan entidades certificadoras que garantizan la identidad digital de personas, instituciones o aplicaciones. El sistema es a través del manejo de certificados, documentos digitales para autenticar personas, servidores o aplicaciones. Es un esquema complicado, donde intervienen entidades generadoras/revocadoras de certificados, solicitantes de certificados y solicitudes de legalidad de certificados. Es un esquema que exije la participación del gobierno o de entidades oficiales para validar la identidad de personas y organizaciones.

3.5 Estándar 802.16 (WiMAX)

WiMAX es el acrónimo de *(Worldwide Interoperability for Microwave Access, Interoperabilidad Mundial para Acceso por Microondas)*. IEEE802.16 es el grupo de trabajo del IEEE especializado en acceso punto a multipunto de banda ancha.

Es un estándar inalámbrico metropolitano creado por las empresas Intel y Alvarion en 2002 y ratificado por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) denominado IEEE-802.16.

El estándar original WiMAX, el IEEE 802.16, específica la tecnología para el rango de 10-66 GHz. Posteriormente, 802.16a añadió soporte para el rango de 2 a 11 GHz, donde algunas bandas no requieren licencia, o sólo precisan una simple autorización. Los esfuerzos se están centrando en esta variación del estándar. La ventaja principal se centra en la posibilidad de realizar comunicaciones sin disponer de línea de vista, haciendo un uso eficiente de las tecnologías existentes. Una característica importante del estándar es que define una capa MAC que soporta múltiples especificaciones físicas (PHY).

WiMAX se basa principalmente en dos subestándares del IEEE, 802.16-2004 para el acceso fijo, y 802.16e para el acceso portable o móvil.

El hecho de presentar dos estándares diferentes para WiMAX, permitirá a los operadores el escalado de las redes según diferentes requisitos, para soporte de servicios de última milla (WiMAX Fijo), o para servicios en movilidad (WiMAX Móvil).

Tabla 3.1 Características del estándar IEEE 802.16 (versiones)

	802.16	**802.16 a**	**802.16 e**
Espectro	10 – 66 GHz	<11GHz	<6GHz
Funcionamiento	Solo con visión directa	Sin visión directa	Sin visión directa
Tasa de bit	32 - 134 Mbit/s con canales de 28 MHz	Hasta 75 Mbit/s con canales de 20 MHz	Hasta 15 Mbit/s con canales de 5 MHz
Modulación	QPSK, 16QAM y 64 QAM	OFDM con 256 subportadoras QPSK, 16QAM, 64QAM	Igual que 802.16a
Movilidad	Sistema fijo	Sistema fijo	Movilidad pedrestre
Anchos de banda	20, 25 y 28 MHz	Seleccionables entre 1,25 y 20 MHz	Igual que 802.16a con los canales de subida para ahorrar potencia
Radio de celda típico	2 - 5 km aprox.	5 - 10 km aprox. (alcance máximo de unos 50 km)	2 - 5 km aprox.

WiMAX Forum

El *WiMAX Forum* es una organización sin fines de lucro, impulsada por el sector de las comunicaciones radio, que fue creada con el objeto de promover y certificar la interoperabilidad de los productos inalámbricos de banda ancha de conformidad con los estándares IEEE 802.16 y ETSI HyperMAN. El objetivo de esta institución es acelerar las implementaciones mundiales y expandir el mercado de soluciones de acceso inalámbrico de banda ancha interoperables y basadas en estándares. El foro está trabajando con las empresas asociadas a fin de desarrollar perfiles estandarizados y productos WiMAX interoperables en torno a bandas concretas del espectro de frecuencia de radio, fundamentalmente 2.3GHz, 2.5GHz, 3.5GHz y 5.8GHz. Son miembros del WiMAX Forum numerosas empresas y proveedores de servicios.

Figura 3.1 WiMAX Forum

Con precisión, WiMAX es la denominación comercial que el Foro WiMAX le da a dispositivos que cumplen con el estándar IEEE 802.16, para garantizar un alto nivel de interoperabilidad entre estos dispositivos.

Los dispositivos certificados por el Foro WiMAX pueden llevar este logotipo:

Figura 3.2 Logotipo WiMAX

3.5.1 WiMAX Fijo

También denominado IEEE 802.16-2004, determina las conexiones de línea fija a través de una antena en el techo, similar a una antena de televisión. WiMAX fijo funciona en las bandas de frecuencia 2.5 GHz y 3.5 GHz, para las que se necesita una licencia, y en la banda 5.8 GHz para la que no se necesita tenerla.

El estándar del 802.16-2004 del IEEE fue diseñado para el acceso fijo. Este estándar puede ser al que se refirió como "fijo inalámbrico" porque usa una antena en la que se coloca en el lugar estratégico del suscriptor. La antena se ubica generalmente en el techo de una habitación mástil, parecido a un plato de la televisión del satélite. También se ocupa de instalaciones interiores, en cuyo caso no necesita ser tan robusto como al aire libre.

El estándar 802.16-2004 es una solución inalámbrica para acceso a Internet de banda ancha. WiMAX acceso fijo funciona desde 2.5-GHz autorizado, 3.5-GHz y 5.8-GHz exento de licencia. Esta tecnología provee una alternativa inalámbrica al módem cable y a las xDSL.

Es particularmente interesante a la hora de proporcionar el acceso de última milla para zonas remotas, sin posibilidad de acceso a infraestructura de red cableada, u otros tipos de infraestructura inalámbrica. Principalmente se enfoca hacia usuarios de tipo residencial o de oficina, con acceso o sin acceso a servicios de banda ancha confiables, y permitirá servicios de

banda ancha para áreas remotas donde hasta el momento ha sido demasiado costoso acceder mediante infraestructura tradicional de banda ancha.

3.5.2 WiMAX Móvil

También se denomina IEEE 802.16e, permite que los equipos móviles de los clientes se conecten a Internet. Permite la conectividad en situación de movilidad completa, por ejemplo a peatones o a medios de transporte (vehículos, trenes, barcos, aviones, etc.). Una vez que el acceso a banda ancha fijo se ha convertido en común, se puede esperar que el usuario desee mantener dichos servicios, a la vez que se desea desplazar de lugar. Las redes WiMAX se implantan de manera similar a las redes 2G/3G, de manera en general sectorizada. Sin embargo, al contrario que para las redes móviles 2G/3G, los despliegues WiMAX prevén inicialmente una prestación de servicios con gran capacidad. Posteriormente se puede proporcionar escalado a la red, con lo que ésta irá migrando a una configuración típica de micro-celda, que sea capaz de proporcionar una mayor tasa de transferencia, para entornos localizados según la estación base a la que se puedan conectar, y las condiciones del entorno del acceso.

El estándar del 802.16e usa Acceso Múltiple por División Ortogonal de Frecuencia (OFDMA), similar a OFDM en que divide en las subportadoras múltiples. OFDMA, sin embargo, va un paso más allá agrupando subportadoras múltiples en subcanales. Una sola estación cliente del suscriptor podría usar todos los subcanales dentro del periodo de la transmisión.

3.5.3 Espectro radioeléctrico

COFETEL

En México el órgano regulador de las telecomunicaciones es la COFETEL (Comisión Federal de Telecomunicaciones), encargado de los procedimientos administrativos para la adquisición del buen uso y aprovechamiento del espectro radioeléctrico.

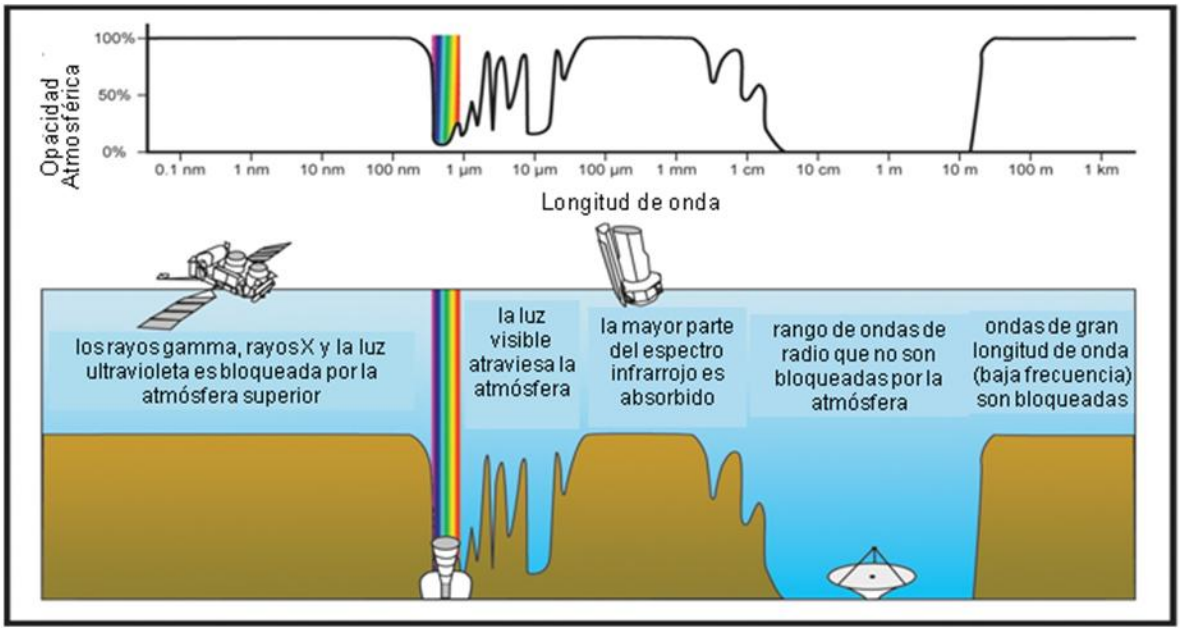
Ley Federal de Telecomunicaciones

La Ley Federal de Telecomunicaciones tiene por objeto regular el uso, aprovechamiento y explotación del Espectro Radioeléctrico, de las redes de telecomunicaciones y de la comunicación vía satélite.

3.5.3.1 Definiciones:

- **Espectro electromagnético**: representación de toda la gama de frecuencias en que puede presentarse cualquier forma de energía electromagnética.

Figura 3.3 Espectro electromagnético



- **Espectro radioeléctrico**: el espacio que permite la propagación sin guía artificial de ondas electromagnéticas cuyas bandas de frecuencias se fijan convencionalmente por debajo de los 3,000 Gigahertz (Ley Federal de Telecomunicaciones Art. 3, Fracc II.)

3.5.4 Uso del Espectro en WiMAX

Las redes WiMAX, al contrario que WLAN, deberán por lo general operar en bandas de frecuencia de uso licenciado, presentando políticas de QoS (Calidad de Servicio), y permitiendo mayor protección y calidad en las comunicaciones. El espectro accesible para WiMAX depende del área geográfica en la que se encuentre la red.

WiMAX empezó su proceso de despliegue en México al anunciar la COFETEL en su Programa de Licitaciones 2007 que se subastaran 150 Megahertz en las bandas de 3.4-3.6 y 3.6-3.7 GHz, mismas que promoverán el acceso a los servicios inalámbricos de banda ancha o WiMAX.

3.5.5.1 **Bandas 3.4-3.6 Ghz y 3.6-3.7 Ghz**

Disponibilidad

Actualmente 150 MHz de la banda 3.4-3.6 MHz se encuentran concesionados a nivel nacional. Se encuentran disponibles los 50 MHz restantes. Los 100 MHz del segmento 3.6-3.7 GHz se encuentran disponibles en su totalidad.

Propuesta

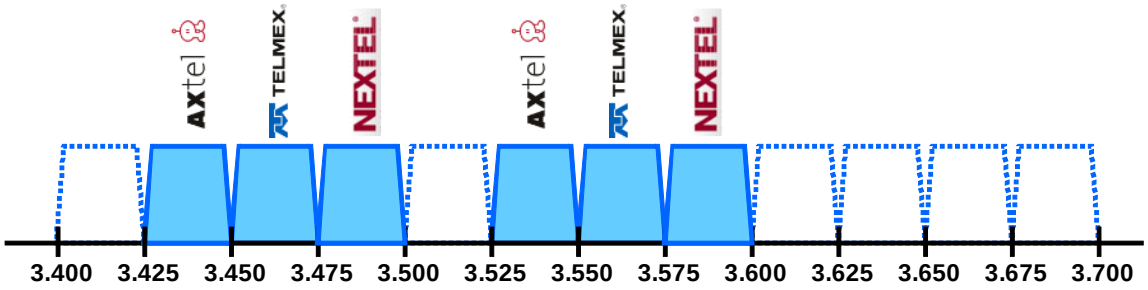
- Uso: Acceso inalámbrico fijo y móvil de banda ancha
- Cobertura: Regional y por áreas básicas de servicio
- Estas bandas se consideran listas para integrarse al programa de licitaciones.

Beneficios

- Esta es una de las bandas identificadas a nivel internacional como candidatas para los servicios de acceso inalámbrico de banda ancha comúnmente conocidos como WiMAX.

- Con las tecnologías actuales se permiten aplicaciones de acceso a Internet de alta velocidad en sus modalidades fija y móvil. En un futuro cercano se prevé su evolución a tecnologías que soporten movilidad total.

Figura 3.4 Segmentos libres en la banda de 3.4-3.7 GHz



Fuente: COFETEL

3.5.5 Bandas licenciadas

Para emplear una solución con licencia es preciso que el operador adquiera espectro, que es un proceso muy variable en función del país en el que se quiera operar, teniendo que pasar por licitaciones, elevados precios y retardos de proceso de asignación de frecuencias considerables. Por contra, esta barrera de entrada, acompañada del uso exclusivo de una banda, permite conseguir una gran calidad y una interferencia muy baja. Las frecuencias bajas asociadas a bandas licenciadas (2.5 GHz y 3.5 GHz) permiten conseguir una mejor característica NLoS (Non Line of Sight, Fuera de la Línea de Visión). Según se incremente el despliegue de los operadores aparecerán las primeras interferencias dentro de las propias redes, que se deberán reducir con un diseño apropiado de la red.

3.5.5.1 Banda de seguridad publica 4.9 Ghz

La banda de 4.9 GHz, operando en espectro licenciado dedicado para uso de agentes de policía, bomberos, ambulancias y municipalidades, proporciona tráfico prioritario para comunicaciones de datos, video y voz con el propósito de asegurar que la información vital llegue sin demora a los agentes de respuesta rápida en situaciones de emergencia.

3.5.6 Bandas no licenciadas

En la mayoría de los mercados, el espectro que no requiere licencia y que se emplea para WiMAX es de 2.4 y 5.8 GHz. Debido a que el espectro no requiere licencia, la barrera para ingresar es baja, por lo que se hace más fácil que un posible operador comience a ofrecer servicios empleando el espectro.

En ciertos países se rigen por el concepto de espectro “con licencia light”, lo que significa que el usuario tiene que presentar su intención de usar el espectro que no requiere licencia. De esta forma, los entes reguladores tienen una mejor noción de quién está empleando el espectro, y controlan la cantidad de licenciatarios y minimizan potencialmente el impacto de interferencias. Existen cuatro desventajas principales relacionadas con el uso del espectro que no requiere licencia:

- **Interferencias**

Debido a que el espectro que no requiere licencia se puede utilizar por diversos sistemas de RF (Espectro de Radiofrecuencia), lo que puede provocar altas probabilidades de que ocurran interferencias. Los sistemas de RF que no requieren licencia se pueden incluir desde las redes rivales de WiMAX o los puntos de acceso de Wi-Fi. Los teléfonos inalámbricos y aquellos que utilizan la banda de 2.4 GHz y que se basan en el estándar 802.15, denominado comercialmente como Bluetooth, también usan este espectro.
Tanto WiMAX como Wi-Fi soportan la DFS *(Dynamic Frequency Selection, Selección Dinámica de Frecuencia)* que permite que se utilice un nuevo canal si es necesario. No obstante, DFS también puede introducir una mayor latencia que, a su vez, afecta las aplicaciones en tiempo real como VoIP.

- **Mayor competencia**

Los operadores que utilizan el espectro que no requiere licencia tienen que asumir que otro operador fácilmente podría ingresar en el mercado empleando el mismo espectro. En gran medida, el número relativamente alto de puntos de acceso públicos Wi-Fi se debe a este hecho. No obstante, los gastos de capital relacionados con la instalación de un punto de acceso Wi-Fi de carácter comercial son relativamente triviales en comparación con el costo relacionado con desplegar una red WiMAX, que podría ser equivalente al costo de desplegar una red celular.

- **Potencia limitada**

Otra desventaja del espectro que no requiere licencia es que los entes reguladores del gobierno por lo general limitan la cantidad de potencia que se puede transmitir. Esta limitación es especialmente importante en 5.8 GHz, donde la mayor potencia podría compensar la pérdida de propagación relacionada con el espectro en frecuencias más altas.

- **Disponibilidad**

Mientras el espectro de 2.4 GHz está disponible universalmente, en la actualidad el espectro 5.8 GHz no se encuentra disponible en varios países. Dadas estas desventajas, los operadores deben evaluar cuidadosamente el uso potencial del espectro que no requiere licencia, en particular 2.4 GHz, antes de instalar una red. Hay excepciones, entre las que se incluyen las regiones rurales o remotas, donde hay menos probabilidades de interferencia y competencia.

3.6 Topologías de una red WiMAX

Mientras Wi-Fi ya lleva años en el mercado, WiMAX aún está haciendo el desembarco. Por ello, la tecnología Wi-Fi se ha ido adaptando en cuanto a las topologías de desempeño a las diferentes funcionalidades que se le han asignado. Así, desde acceso fijo, última milla o hotspots han desarrollado diferentes arquitecturas.

Existen tres posibles topologías para la implementación de redes WiMAX:

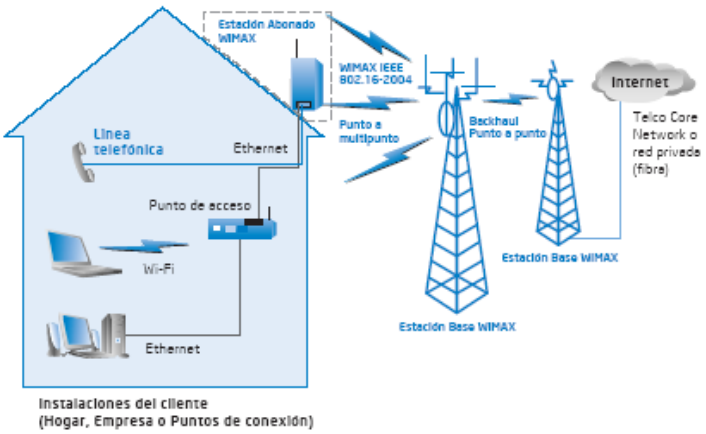
- PTP *(Point To Point, Punto a Punto)*
- PMP *(Point to Multipont, Punto-Multipunto)*
- ***Mesh*** *(Multipont to Multipont, Multipunto a Multipunto)*

La elección de cada una depende del diseño que se utilice así como de las características y necesidades específicas de la red que desee implementarse.

La topología elegida va a determinar entre otros factores,

- La disposición geográfica de los equipos de red.
- Distribución de funciones y complejidad en los equipos de red.
- El comportamiento dinámico de la red.
- La zona de cobertura.

Figura 3.5 Topología de red WiMAX



Fuente: Intel

3.6.1 Topología PTP

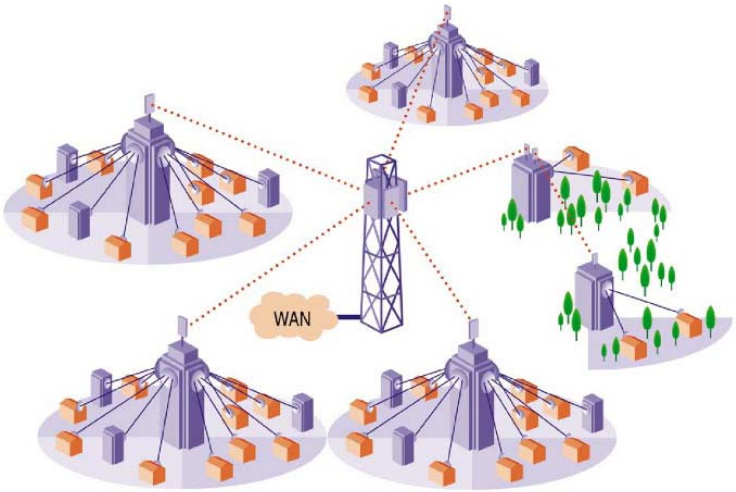
En la topología punto a punto se establece un enlace bidireccional entre dos puntos fijos. Para maximizar el rendimiento del enlace, por lo general se utilizan antenas altamente directivas y se procura línea de vista LOS entre ellas. Con estas características, y dado que todo el ancho de banda del canal se utiliza para un sólo enlace, el rendimiento de dicho enlace llega a tener valores de varias decenas de Mbps con distancias entre las estaciones que llegan hasta los 60 Km.

Este tipo de enlaces se utilizan habitualmente en conexiones dedicadas de alto rendimiento o enlaces de interconexión de alta capacidad. Este tipo de enlaces son fáciles de instalar, pero difíciles de crear con ellos una red grande. Es habitual su uso para enlaces punto a punto en clientes finales o para realizar el backhaul (enlace de interconexión de redes).

Bakchaul

Bakchaul es una conexión que se encarga de enlazar a computadoras u otros equipos de telecomunicaciones encargados de hacer circular la información. Los backhaul conectan redes de datos, redes de telefonía celular y constituyen una estructura fundamental de las redes de comunicación.

Figura 3.6 Enlace Punto a Punto



Fuente: Motorola

3.6.2 Topología PMP

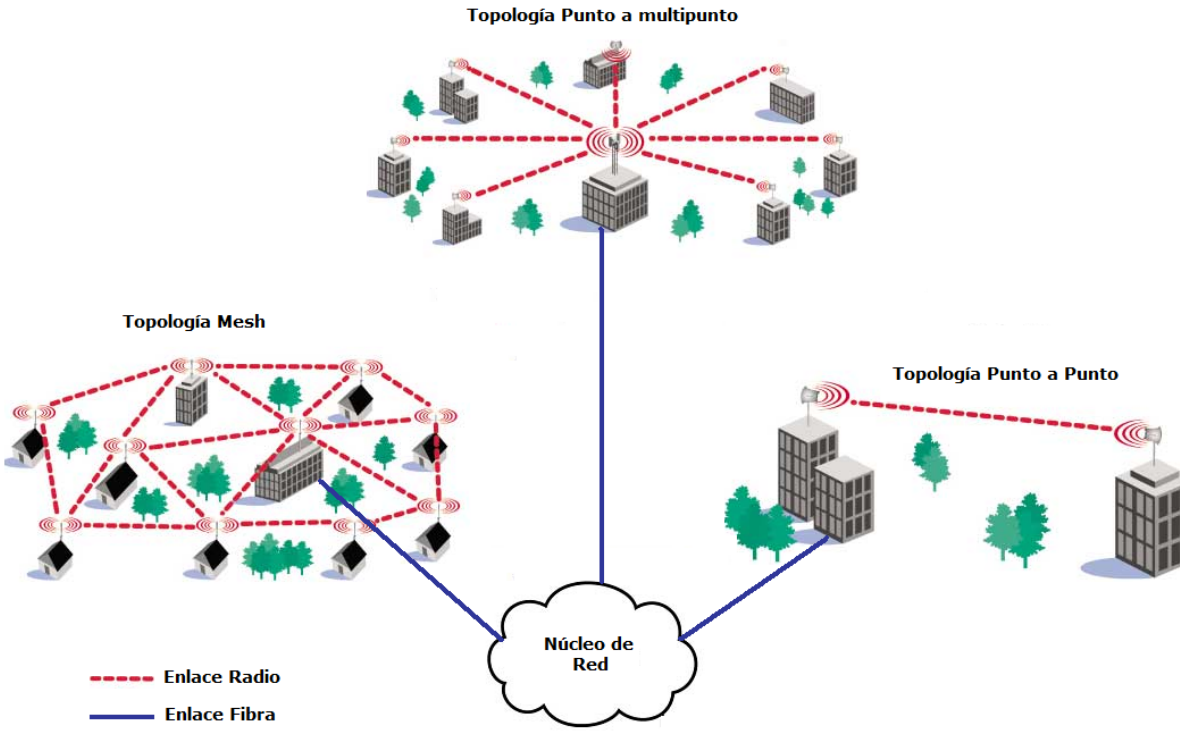
En una topología punto-multipunto se manejan varios enlaces bidireccionales que van desde una estación base fija hasta varias estaciones suscriptoras que se encuentran en su zona de cobertura. Las antenas de la estación base son de tipo sectorial, cada sector puede cubrir 60º, 90º, 120º, 180º o incluso 360º, dependiendo de las dimensiones de la red. Por lo general, los enlaces PMP no suelen rebasar los 5 km de longitud.

3.6.3 Topología Mesh

En la topología Mesh o topología de malla, se tiene un nodo que es designado como estación base y que provee servicios de autenticación, administración y control de los nodos usuarios de la red a través de su interfaz de radio.

En las redes Mesh, los nodos actúan como routers, que se instalan sobre una superficie extensa. Cada nodo transmite una señal de baja potencia, para alcanzar a los nodos vecinos, que a su vez reenvían la señal. Estas redes permiten adaptarse a los cambios de topología, ya que se pueden incorporar nodos o eliminarlos.

Figura 3.7 Topologías comunes de WiMAX



3.7 Protocolos

Las redes basadas en el estándar IEEE 802.16 cuentan con una arquitectura basada en una subdivisión de capas de acuerdo al modelo de referencia de interconexión de sistemas abiertos (modelo OSI).

El grupo de trabajo de red (NWG) del Foro WiMAX es responsable del desarrollo de las especificaciones y requerimientos de las redes, de extremo a extremo, basadas en el estándar IEE 802.16e-2005 como interfaz de radio.

3.7.1 Capas de protocolos

Generalmente, las capas que se encuentran en la parte baja del modelo OSI (física, enlace de datos y red) trabajan sobre el "hardware" mientras que las capas superiores (transporte, sesión, presentación y aplicación) se encargan de la ejecución de software para la manipulación de las capas más bajas. Dos de estas capas bajas son la física (*PHY layer*), y la capa de enlace de datos. El estándar IEEE 802.16 divide la capa de enlace de datos en dos subcapas denominadas control de enlace lógico (LLC, *Logical Link Control*) y control de acceso al medio (MAC, *Medium Access Control*) como se muestra en la figura 3.8. El propósito de la capa PHY es crear la conexión física entre las dos terminales que se comunican, la capa MAC es responsable del establecimiento y del mantenimiento de la conexión, mientras que la capa LLC especifica los mecanismos para el direccionamiento de las estaciones remotas conectadas al medio, además de controlar el intercambio de datos entre los usuarios de la red. Su operación y formato están basados en el protocolo control de enlace de datos de nivel superior (HDLC[1], *High Level Data Link Control*), donde se establecen tres tipos de servicios:

- Sin conexión y sin reconocimiento
- Con conexión
- Con reconocimiento y sin conexión

Figura 3.8 Modelo OSI para el estándar IEEE 802.16

Modelo OSI		Modelo OSI para WiMAX
7	Aplicación	
6	Presentación	
5	Sesión	
4	Transporte	
3	Red	
2	Enlace de datos	Control de Enlace Lógico (LLC)
		Control de Acceso al medio (MAC)
1	Física	Física

[1] Protocolo diseñado para proporcionar un mecanismo de detección y corrección de errores de propósito general a los enlaces digitales, entendiendo como enlace un único cable que conecta dos máquinas (enlace punto a punto), o varias máquinas (enlace multipunto).

3.7.2 Capa física (PHY)

La capa PHY establece la conexión física entre los extremos de la conexión, a menudo en dos direcciones (subida y bajada), debido a que el estándar IEEE 802.16 es evidentemente una tecnología digital, la capa física es responsable de la transmisión de las secuencias de bits. Esta capa define el tipo de señal que va a utilizarse, el tipo de modulación y demodulación, el acceso múltiple, la codificación de canal, la tecnología de las antenas, la potencia de transmisión y otras características físicas, como un despliegue flexible.

3.7.2.1 Especificaciones de las interfaces de radio en el estándar IEEE 802.16

La capa PHY de WiMAX está compuesta de cuatro secciones:

1) Red de Área Metropolitana Inalámbrica con una Sola Portadora (WMANSC, *Wireless Metropolitan Area Network – Simple Carrier*)

2) Red de Área Metropolitana Inalámbrica con Acceso a una Sola Portadora (WMAN-SCa, *Wireless Metropolitan Area Network - Single Carrier access*)

3) Red de Área Metropolitana Inalámbrica con Multiplexaje por División de Frecuencias Ortogonales (WMAN-OFDM *Orthogonal Frequency Division Multiplexing*)

4) Red de Área Metropolitana Inalámbrica con Múltiple Acceso por División de Frecuencia Ortogonal (WMAN-OFDMA, Orthogonal *Frequency Division Multiple Access*)

Cada una de estas secciones cuenta con una serie de especificaciones que resultan ser una variante del estándar en función a la técnica de modulación utilizada y las bandas de frecuencia para las que fueron diseñadas. A continuación se muestran las características de cada una de estas especificaciones con mayor detalle.

WMAN-SC

Esta especificación de la PHY está destinada para operar en la banda de frecuencia de 10-66 GHz; su diseño es altamente flexibilidad para permitir a los proveedores de servicio la optimización de los sistemas con respecto a la planeación celular, costo, capacidades de radio, servicios y capacidad de tal manera que pueda permitir el uso flexible del espectro.

Esta especificación soporta Duplexaje por División de Tiempo (TDD, *Time Division Duplex*) y Duplexaje por División de Frecuencia (FDD, *Frequency Division Duplex*). En ambos casos se usa el formato de transmisión por ráfagas cuyos mecanismos de trama permiten perfiles de ráfaga adaptables en el cual los parámetros de transmisión, incluyendo los esquemas de modulación y codificación, pueden ajustarse para cada terminal de usuario trama por trama. El FDD soporta estaciones de usuario full-duplex y también terminales de usuario half-duplex, las cuales no transmiten y reciben simultáneamente.

WMAN-SCA

Wireless MAN-SCA se basa en una tecnología de portadora simple y está diseñado para operar sin línea de vista (NLOS, *No Line-of-Sight*) en bandas de frecuencias por debajo de 11 GHz para operaciones punto a multipunto. Para bandas con licencia, los anchos de banda de canal permitidos deben ser limitados por el ancho de banda regulado, dividido por cualquier potencia de dos no menor que 1.25 MHz. Cuenta con una interfaz de radio con portadora simple modulada.

Los elementos dentro de la PHY incluyen:

- TDD y FDD
- Acceso Múltiple por División de Tiempo (TDMA, *Time Division Multiple Access*) en el enlace de subida.
- Multiplexaje por División de Tiempo (TDM, *Time Division Multiplexing*) o TDMA en el enlace de bajada
- Modulación y codificación para el control de errores adaptable tanto para el enlace de subida como bajada.
- Estructuras de tramas que permiten mejor ecualización.
- Códigos para la transmisión espacio – tiempo.

WMAN-OFDM

Está basada en multiplexaje por división de frecuencias ortogonales OFDM, y diseñada para operación NLOS en frecuencias por debajo de 11 GHz. WMAN-OFDM está orientada principalmente al acceso fijo en hogares y empresas. Los símbolos OFDM se conforman por cierto número de subportadoras (256 en este caso), que dependen del número de puntos de la transformada rápida de Fourier. WMAN-OFDM utiliza diferentes tipos de modulación como: BPSK, QPSK, 16-QAM y 64-QAM.

Los tipos de subportadoras que se ocupan son:

- Subportadora de datos: para transmisión de datos.
- Subportadora piloto: para varios propósitos de estimación.
- Subportadora nula: sin transmisión, para bandas de guarda.

WMAN-OFDMA

Tiene un esquema de 2048 portadoras OFDM para operaciones punto a multipunto en condiciones NLOS en frecuencias de 2 GHz a 11 GHz. El acceso múltiple se logra mediante la asignación de un subconjunto de portadoras a un receptor individual. Esta versión denomina comúnmente OFD de acceso múltiple (OFDMA). Utiliza modulaciones como: QPSK, 16-QAM y 64-QAM. En la tabla 3.2 se muestra un resumen de las distintas interfaces de radio en IEEE 802.16.

Tabla 3.2 Interfaces de radio IEEE 802.16

INTERFAZ	BANDA DE FRECUENCIA	DUPLEXAJE
WMAN-SC	10 - 66 GHz (LOS)	TDD y FDD
WMAN-Sca	Debajo de 11 GHz (NLOS) en bandas con licencia	TDD y FDD
WMAN-OFDM	Debajo de 11 GHz (NLOS) en bandas con licencia	TDD y FDD
WMAN-OFDMA	Debajo de 11 GHz (NLOS) en bandas con licencia	TDD y FDD

3.7.3 Capa de Control de Acceso al Medio (MAC, *Medium Acces Control*)

Esta capa que se encuentra por encima de la capa PHY y es responsable del control y multiplexaje del tráfico por el medio físico. Algunas de las funciones más importantes de la capa MAC son:

- Segmentar o concatenar las Unidades de Servicio Datos (SDU, *Service Data Units*) que recibe de las capas superiores en unidades de datos de protocolo MAC (PDU, *Protocol Data Units*).

- Seleccionar el perfil de ráfaga así como el nivel de potencia que se utiliza para la transmisión de MAC PDUs.

- Retransmitir las MAC PDUs que fueron recibidos erróneamente por el receptor utilizando Solicitud de Repetición Automática (ARQ, *Automatic Retransmissions Requests*).

- Proporcionar el control de calidad de servicio (QoS, *Quality of Service*) así como el manejo de prioridad de datos de MAC PDUs.

- Calendarizar los MAC PDUs sobre los recursos de la capa PHY.

- Proporcionar apoyo a las capas superiores para la administración de movilidad.

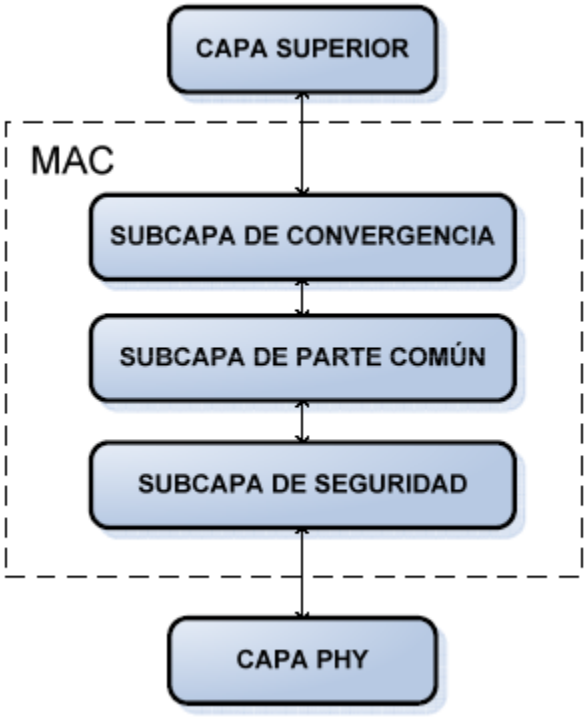
- Proporcionar seguridad y la administración de claves.

- Proporcionar el modo de ahorro de energía y el modo de funcionamiento de inactividad.

La capa MAC se divide en tres componentes distintos: subcapa de convergencia de servicio específico (CS), subcapa de parte común, y subcapa de seguridad como se ilustra en la figura 3.9. La CS, es la interfaz entre la capa MAC y la capa 3 de red, con el objetivo de recibir paquetes de datos de la capa superior.

Estos paquetes de la capa superior se conocen como Unidades del Servicio de Datos MAC (SDU, *Service Data Units*). La CS es responsable de realizar todas las operaciones de las que depende el protocolo de la capa superior, como la compresión de la cabecera y mapeo de las direcciones.

Figura 3.9 Subcapas de la capa MAC



La CS se puede ver como una capa de adaptación para el enmascaramiento del protocolo de la capa superior y de las necesidades del resto de la capa MAC y PHY en la red basada en el estándar IEEE 802.16.

La subcapa de parte común de la capa MAC realiza todas las operaciones de paquetes que son independientes de las capas más altas, como la fragmentación y la concatenación de SDUs en MAC PDUs, la transmisión de MAC PDUs, el control de QoS y la ARQ. La subcapa de seguridad es la responsable de la encriptación, autorización y el intercambio adecuado de las claves de cifrado entre la BS y el SS. La capa MAC facilita el uso eficiente de la capa PHY, apoyando una topología punto a multipunto (PMP, *point to multipoint*) y malla (*Mesh*) para compartir el medio inalámbrico. Las especificaciones de la capa MAC promueven el uso del protocolo IP como elemento fundamental del estándar para la operación y administración de la capa MAC.

3.7.3.1 Subcapa de convergencia de Servicio Específico (CS)

Además de la compresión del encabezado, la CS también es responsable del direccionamiento de las capas superiores, como las direcciones IP de las SDUs sobre las conexiones PHY y

MAC que se utilizarán para su transmisión. Esta función es necesaria porque no hay visibilidad de las direcciones de la capa superior en las capas MAC y PHY.
La capa MAC está orientada a conexión y determina una relación lógica entre la BS y el SS con un Identificador de Conexión Unidireccional (CID, *Unidirectional Connection Indentifier*). Los CIDs para conexiones de subida y bajada son diferentes. El CID puede considerarse como una asignación de dirección temporal dinámica de la capa 2 por la BS para identificar una relación unidireccional entre las entidades MAC/PHY, y se utiliza para el transporte de datos y el control del tráfico, con el fin de direccionar la capa superior al CID, la CS tiene que realizar un seguimiento de la correspondencia entre la dirección de destino y los respectivos CIDs. Es bastante probable que las SDUs que pertenecen a una determinada dirección de destino puedan enviarse por diferentes conexiones, en función de las necesidades de QoS; en ese caso la CS determina el CID apropiado, no sólo basándose en la dirección de destino, sino también en otros factores, como el Servicio de Identificador de Flujo (SFID, *Service Flow Identifier*) y la dirección de origen.

La CS realiza supresión del encabezado del paquete (PHS, *Packet Header Suppressio*n), donde el transmisor trata de eliminar la parte repetida de la cabecera de cada una de las SDUs. Por ejemplo, si las SDUs se entregan a la CS en paquetes IP, las direcciones de origen y destino se encuentran en la cabecera de cada paquete y no cambian de un paquete a otro por lo que pueden removerse antes de transmitirse por el medio. Lo mismo sucede en el receptor, la parte que se repite de la cabecera puede insertarse en la SDU antes de entregarse a las capas superiores. El mecanismo PHS establece y mantiene el grado necesario de sincronización entre las CSs del transmisor y del receptor.

La implementación de PHS en la red basada en el estándar IEEE 802.16 es opcional, pero la mayoría de los sistemas ponen en práctica esta función, ya que mejora la eficiencia de la red para prestar diferentes tipos de servicios.

La operación de PHS proporciona todos los parámetros relacionados con la supresión de la cabecera de las SDUs. Cuando una SDU llega, la CS determina la norma PHS que debe utilizarse, y algunos de los parámetros como direcciones de origen y destino. Una vez que se encuentra una regla que coincide, esta proporciona un SFID, un CID y la PHS relacionado con los parámetros utilizados en la SDU. La norma PHS depende del tipo de servicio, como voz sobre IP (VoIP), Protocolo de Transferencia de Hipertexto (HTTP, *HyperText Transfer Protocol*) ó Protocolo de Transferencia de Archivos (FTP, *File Transfer Protocol*), ya que el número de bytes que se pueden suprimir en la cabecera depende de la naturaleza del servicio.

El estándar IEEE 802.16 establece al CS utilizar normas PHS, sin embargo, no específica cómo y cuando se crean dichas normas; esto se lo deja a una entidad en la capa superior.

3.7.3.2 Subcapa de parte común

La subcapa de parte común es independiente de la capa superior y realiza operaciones como: ARQ, asignación de ancho de banda y modulación. Las SDUs llegan a la subcapa de parte común provenientes de la CS superior donde se creó la MAC PDU, la unidad básica manejada por las capas MAC y PHY. Basándose en el tamaño de la carga, varias SDUs se pueden llevar

en una sola MAC PDU, ó una sola SDU puede fragmentarse para llevarse por múltiples MAC PDUs. Cuando una SDU está fragmentada, la posición de cada fragmento dentro de la SDU tiene la etiqueta con un número de secuencia. El número de secuencia permite a la capa MAC del receptor ensamblar los fragmentos de la SDU en el orden correcto.
Con el fin de utilizar de forma eficiente los recursos de la PHY, múltiples MAC PDUs destinadas al mismo receptor pueden concatenarse y transmitirse en un solo bloque. En la subida y bajada de datos existen ranuras en la SS reservadas para su transmisión. Para las conexiones donde las ARQ no están permitidas, cada fragmento de la SDU se transmite en secuencia. Para conexiones con ARQ, la SDU primero se divide en bloques ARQ de longitud fija, y se asigna un Número de Secuencia de Bloque (BSN, *Block Secuense Number*) a cada bloque ARQ. La longitud de los bloques ARQ se especifica en la BS para cada CID, usando el parámetro ARQBLOCK-SIZE. Si la duración de las SDU no es un múltiplo entero de ARQBLOCK-SIZE, el último bloque ARQ se rellena. Una vez que el SDU está dividido en bloques ARQ, la división sigue vigente hasta que todos los bloques de ARQ se han transmitido y han sido recibidos y confirmados por el receptor. Después de la división de los bloques ARQ, se crean las MAC PDUs.

En las conexiones con ARQ habilitado, la división y el empaquetado del subencabezado contienen el BSN del primer bloque ARQ.

Los bloques ARQ llegan al receptor para su regeneración en forma de reconocimiento (ACK, *Acknowledgment*), los cuales indican la recepción correcta de los bloques ARQ. Esta información se envía como una MAC PDU independiente o como un paquete de una MAC PDU. En el estándar IEEE 802.16 la regeneración de ARQ puede ser de la forma ACK selectiva (ARQ con retransmisión selectiva) ó ACK acumulativa (ARQ retroceder N). Un ACK selectivo para un determinado BSN, indica que el bloque ARQ se ha recibido sin errores y un ACK acumulativo, indica que para un BSN determinado, todos los bloques con los números de secuencia menor o igual que el BSN se han recibido sin error.

3.7.3.3 Subcapa de seguridad

La subcapa de seguridad provee a las SS *(Subscriber station, Estación Suscriptora)* privacidad a través de la red inalámbrica de banda ancha. Esto lo hace cifrando las conexiones entre SS y BS *(Base Station, Estación Base)*. Además, de la seguridad, provee operadores de protección contra el robo de servicio. La BS protege contra el acceso no autorizado a estos servicios de transporte de los datos, validando el cifrado del flujo del servicio a través de la red. La privacidad emplea una llave de autentificación en el protocolo de administración de cliente/servidor en el cual la BS servidora controla la distribución de las llaves de la SS cliente. Además, los mecanismos básicos de privacidad se consolidan agregando autentificación digital de certificado basada en SS a su protocolo de administración.
Durante la negociación de las capacidades, si las SS especifican que no soportan la seguridad de IEEE 802.16, la autorización y el intercambio de la llave se omitirán. Si la BS, está capacitada para proveer autentificación, considerará a las SS, si no, las SS no serán considerados para proporcionar el servicio.

3.8 Aplicaciones

Las primeras versiones de WiMAX están pensadas para comunicaciones punto a punto o punto a multipunto, típicas de los radio enlaces por microondas. Las posibles aplicaciones para WiMAX se basan en el gran ancho de banda y la alta cobertura. Las próximas ofrecerán total movilidad, por lo que competirán con las redes celulares. Los primeros productos que están empezando a aparecer en el mercado se enfocan a proporcionar un enlace de alta velocidad para conexión a las redes fijas públicas o para establecer enlaces punto a punto.

Así, WiMAX puede resultar muy adecuado para unir Hot spots Wi-Fi a las redes de los operadores, sin necesidad de establecer un enlace fijo. El equipamiento Wi-Fi es relativamente barato pero un enlace E1 o DSL resulta caro y a veces no se puede desplegar, por lo que la alternativa radio parece muy razonable. WiMAX extiende el alcance de Wi-Fi y provee una seria alternativa o complemento a las redes 3G, según como se mire.

En los países en desarrollo resulta una buena alternativa para el despliegue rápido de servicios, compitiendo directamente con las infraestructuras basadas en redes de satélites, que son muy costosas y presentan una alta latencia.

Figura 3.10 Rango de aplicaciones WiMAX

3.8.1 Aplicaciones para operadores de servicios

En mercados emergentes, como Latinoamérica, son los operadores fijos los que están lanzando redes WiMAX para complementar su infraestructura existente y expandir su área de cobertura con servicios de telefonía y sobre todo banda ancha.

Las aplicaciones fijas ofrecidas por WiMAX replican las ofrecidas por tecnologías tipo ADSL o Cable. Además, los operadores consideran importante el hecho de que WiMAX puede ofrecer servicios de voz sobre IP (VoIP) y telefonía sobre IP (ToIP).

Los operadores que contaban con un modelo de negocio en la versión fija empiezan ahora a realizar pruebas para incrementar su cobertura a nuevas regiones, pero utilizando la versión móvil en lugar de la fija, y no por ello desviándose de su modelo de negocio actual. En mercados emergentes, este fenómeno se produce debido al modelo de negocio de los operadores, los cuales buscan ofrecer acceso fijo o nomádico a través de la versión móvil. Este cambio de tecnología para ampliar capacidad se debe a que en la versión móvil se esperan mayores economías de escala, lo que afectará tanto a infraestructura pero sobre todo a los CPEs *(Costumer Premises Equipment, Equipo Local del Cliente).*

En mercados emergentes, muchos operadores móviles están evaluando la posibilidad de lanzar redes WiMAX móvil una vez tengan espectro para hacerlo. Estos operadores también tienen activos en redes 3G que ofrecen velocidades de transmisión a veces muy cercanas a lo disponible en los accesos fijos.

La instalación de estaciones base WiMAX es sencilla y económica, utilizando un hardware que llegará a ser estándar, por lo que por los operadores móviles puede ser visto como una amenaza, pero también, es una manera fácil de extender sus redes y entrar en un nuevo negocio en el que ahora no están, lo que se presenta como una oportunidad.

3.8.2 Aplicaciones para las empresas

Cada vez más, las grandes empresas y Pymes se apoyan en el sector de las telecomunicaciones para incrementar su productividad. Muchas de estas empresas cuentan con redes propias dentro de su ambiente y el siguiente paso es poder llevar estas aplicaciones internas para ser utilizadas en cualquier lugar y hora. Debido a la importancia de este sector y a la concentración de los operadores móviles en satisfacer primero a los usuarios masivos, WiMAX puede ofrecer una alternativa para que estos negocios utilicen esta tecnología.

Para las empresas, es una alternativa a contemplar, ya que el costo puede ser hasta 10 veces menor que en el caso de emplear un enlace E1 o T1. De momento no se habla de WiMAX para el acceso residencial, pero en un futuro podría ser una realidad, sustituyendo con enorme ventaja a las conexiones ADSL, o de cable, y haciendo que la verdadera revolución de la banda ancha llegue a todos los hogares.

Por ello, los operadores WiMAX deben buscar un proveedor que además de infraestructura les ofrezca soluciones empresariales o, por lo menos, el poder migrar las aplicaciones internas al mundo externo.

Otra de sus aplicaciones encaja en ofrecer servicios a zonas rurales de difícil acceso, a las que no llegan las redes cableadas. Es una tecnología muy adecuada para establecer radio enlaces, dado su gran alcance y alta capacidad, a un costo muy competitivo frente a otras alternativas.

3.8.3 Monitorización

Las explotaciones energéticas se encuentran en ocasiones en zonas remotas y no permanentes vigiladas pero, por contra, disponen de infraestructuras sensibles por lo que WiMAX es una solución que permite la monitorización centralizada en una sala de control de diferentes ubicaciones.

Monitorización meteorológica

Las instalaciones solares o eólicas generan gran cantidad de información desde estaciones meteorológicas que puede ser transmitida a través de redes WiMAX.

3.8.4 Soluciones de oficinas remotas

Un despliegue de una red WiMAX multipunto puede permitir en todos los puntos de una explotación (centrales térmicas, parques solares, etc.) el acceso a voz IP, e-mail, datos de SCADA, entre otros, sin tener que desplazarse a la oficina principal.

3.8.5 Comunicaciones marítimas

Las tecnologías inalámbricas son el único medio válido para habilitar comunicaciones en entornos costeros, por lo que es la solución adecuada para los nuevos parques eólicos marinos o para sistemas mareomotrices

3.8.6 Localización

La combinación de soluciones de georeferenciación como GPS con receptores WiMAX puede permitir la localización de vehículos o personas en entornos donde otras técnicas (como GPRS) no son viables.

3.8.7 Control remoto

Existe un número creciente de sensores y actuadores en los parques solares, eólicos o en las centrales, que se pueden interconectar utilizando una única red WiMAX.

3.8.8 Videovigilancia

El mercado de la videovigilancia ha experimentado un crecimiento exponencial en los últimos años gracias al abaratamiento de los sistemas de captura y almacenamiento de imágenes basados en IP (frente a las tradicionales tecnologías analógicas).

El otro punto clave en esta expansión ha sido la disponibilidad de equipamiento radio para establecer redes inalámbricas capaces de transportar tráfico de vídeo a un costo muy competitivo y por lo tanto aumentando la facilidad de la colocación de nuevos puntos de captura de imágenes en ubicaciones donde previamente sería muy costoso o directamente imposible. La integración de las comunicaciones en una única red IP facilita la creación de nuevas aplicaciones que hacen un uso intensivo de la imagen y el vídeo.

La tecnología WiMAX ha sido concebida para su utilización por operadores de telecomunicaciones en bandas de frecuencia con licencia, para permitir a dichos operadores extender su cobertura en la “última milla” con esta tecnología ofreciendo servicios triple-play a sus abonados.

La arquitectura de los sistemas de videovigilancia WiMAX se compone de cámaras IP, servidores de vídeo y la propia infraestructura radio. Con la combinación inteligente de estos elementos, y aprovechando la existencia de equipamiento con las mismas características que WiMAX pero en banda libre, se despliegan aplicaciones para vigilancia de infraestructuras públicas (carreteras, aeropuertos, hospitales, vías de trenes, obras públicas, etc.) y para el control de tráfico (seguimiento de vehículos, reconocimiento de matrículas, gestión de aparcamientos, control de accesos, etc.). En el sector privado, las aplicaciones se centran fundamentalmente en la seguridad (control de accesos a recintos, vigilancia en lugares públicos, etc.) así como en el control de la producción y la grabación de eventos

Capítulo IV Análisis Económico

4.1 Introducción

El estándar IEEE 802.16x es conocido a nivel mundial como WIMAX, y su propósito es alcanzar velocidades de comunicación hasta los 75 Mbit/s, operando en un rango de frecuencias más bajo (2 a 11 GHz). Estas velocidades tan elevadas se consiguen gracias a utilizar la modulación OFDM *(Orthogonal Frequency División Multiplexing)* con 256 subportadoras, las cuales puede ser implementadas de diferentes formas, según cada operador, siendo la variante de OFDM empleada, un factor diferenciador del servicio ofrecido.

La seguridad en las redes inalámbricas representa una necesidad urgente, dadas las características del medio por donde se transmite la información. La gran cantidad de redes inalámbricas actualmente instaladas no tienen configurada seguridad alguna, o poseen un nivel de seguridad muy débil, poniendo en peligro la confidencialidad e integridad de dicha información, lo cual pude ser grave para cualquier empresa o institución que utilice esta tecnología.

En este sentido, un atacante con un equipo correctamente configurado y con posición adecuada puede interceptar una señal, es decir, obstaculizar los mensajes que se están enviando por un canal inalámbrico y reutilizar la trama por lo tanto, hacen falta mecanismos de confidencialidad. Debido a esta vulnerabilidad, también se podría capturar tramas de lugares autorizados y formar nuevas tramas, modificarlas y retransmitirlas. En este caso el algoritmo de seguridad debe proporcionar un mecanismo de autenticidad de los datos.

Hoy en día se hace cada vez más imprescindible y necesario un adecuado sistema de protección en los sistemas informáticos que garanticen desde la privacidad de los datos hasta la seguridad en las transacciones de información. El control de acceso, los protocolos de comunicación, las transferencias de datos, etc., son procesos que deben ser estudiados y planificados por las corporaciones/usuarios para la definición de sus políticas de seguridad y la planificación, principal objetivo de este capítulo.

4.2 Vulnerabilidad

Una vulnerabilidad es una vía de ataque potencial. Las vulnerabilidades pueden existir en redes y sistemas de cómputo permitiendo que el sistema quede abierto a un ataque técnico) o en procedimientos administrativos (al permitir que el entorno esté abierto a un ataque no técnico o de ingeniería social).

Una vulnerabilidad está caracterizada por la dificultad y el nivel da capacidad técnica que se requiera para explotarla

4.2.1 Escaneo de vulnerabilidades

Ya sea que se esté en busca de un sistema específico o sólo a la expectativa de un objetivo débil, un atacante utiliza un arsenal de herramientas para automáticamente localizar nuevos

sistemas, mapear redes externas y probar vulnerabilidades específicas que puedan ser explotables. Este primer paso del ataque es llamado de reconocimiento y puede ser lanzado por el atacante mucho tiempo antes de que saque ventaja de las vulnerabilidades y tenga acceso al sistema y/o redes. De hecho, la evidencia recogida de la actividad de reconocimiento puede ser una pista de que un nuevo ataque puede ser dirigido a ese sistema o red.

4.3 Amenaza

Una amenaza es una acción o evento que puede violar la seguridad de un entorno de sistemas de información. Existen tres componentes de amenaza:

1. Objetivos.- El aspecto de la seguridad que puede ser atacado.

2. Agentes.- Las personas u organizaciones que originan la amenaza

3. Eventos.- El tipo de acción que representa la amenaza

4.3.1 Vectores de ataque

La primera meta es entender cómo se manifiesta y cómo se puede controlar una amenaza, esto será indispensable en el escaneo de vulnerabilidades y sus remedios. Si no existen vulnerabilidades, la amenaza no podrá ser manifestada. Sin embargo, muchas clases de vulnerabilidades son imposibles de detectar con un escaneo de vulnerabilidades estándar.

En términos de los controles que podemos utilizar, necesitamos que tanto los controles defectivos, correctivos y preventivos trabajen en conjunto para aumentar el nivel de protección.

La detección es la acción de poder identificar la amenaza, lo controles correctivos actuarán en contra de la amenaza una vez que haya sido detectada. La prevención es otra medida de contención, que permite evitar que lleguen a estar en contacto las vulnerabilidades con las amenazas.

Las formas o lugares en las que se pueden presentar las amenazas son también llamadas vectores. Los podemos clasificar en 5 diferentes grupos:

- Ataques que provienen de afuera desde una red.
- Ataques que provienen de afuera desde un teléfono.
- Ataques que provienen del interior de la red.
- Ataques que provienen del interior desde un sistema local.
- Ataques por algún tipo de código malicioso.

Algunas de las amenazas que más preocupan a las organizaciones y en consecuencia las más comunes son:

- Códigos maliciosos que pueden ser ejecutados con el fin de borrar la información de los medios de almacenamiento.

- Correos maliciosos que pueden exponer información sensible en la Internet.
- Servidores de WEB comprometidos que pueden hacer quedar una mala reputación e imagen a la empresa.
- Servidores WEB que pueden exponer datos privados de clientes.
- Trabajadores enojados con la organización ejecutando bombas lógicas.
- Trabajadores traidores que venden información secreta de la compañía.
- Secretarias engañadas mediante ingeniería social proporcionando información clasificada a adversarios.
- Hacker[1] que penetra el sistema y tiene acceso a la información.

Una buena manera de saber cuáles son las vulnerabilidades que se deben atender primero, son las que pueden causar mayor impacto a la organización.

4.4 Riesgo

Riesgo es el concepto subyacente que forma los fundamentos de lo que llamamos "seguridad". El riesgo es el potencial de lo que puede ser perdido y requiere protección. Si no hay un riesgo, no hay necesidad de protección. La seguridad se consigue administrando riesgos. El riesgo puede definirse cualitativamente en estos tres niveles:

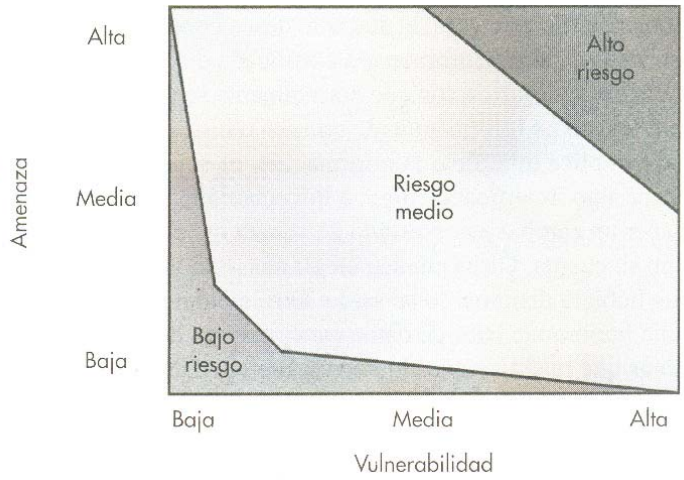
- Bajo.- La vulnerabilidad representa un nivel de riesgo para la organización, aunque es improbable que ocurra. Deberían tomarse acciones para eliminar la vulnerabilidad si fuera posible, pero el costo de esta acción debería ponderarse en relación con la pequeña reducción en el riesgo que se obtendrá a cambio.

- Medio.- La vulnerabilidad representa un nivel significativo de riesgo hacia la confidencialidad, integridad, disponibilidad y/o responsabilidad de la información, los sistemas o los sitios físicos de la organización. Existe una posibilidad real de que esto pueda ocurrir. Es aconsejable emprender acciones para eliminar la vulnerabilidad.

- Alto.- La vulnerabilidad plantea un peligro real hacia la confidencialidad, integridad, disponibilidad y/o responsabilidad de la información, los sistemas o los sitios físicos de la organización. Deberían tomarse medidas de inmediato para eliminar esta vulnerabilidad.

[1] Del inglés hack, hachar. Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no se maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo.

Figura 4.1 La relación entre la vulnerabilidad y amenaza



4.5 Escaneo de redes

Tanto negocios pequeños como empresas multinacionales; desde pequeñas redes caseras hasta redes de cafés Internet, el número de computadoras y dispositivos se ha ido incrementando de igual forma que las redes lo han hecho y no sólo por el trabajo que desarrollan en lo individual sino por lo que hacen en conjunto.

Cualquiera que sea el uso de una red, tendrá hosts conectados a ella. Después de todo este es el punto que define a las redes: Comunicar a dispositivos que necesitan servicios el uno del otro. Desde el punto de vista del usuario la pregunta clave es: ¿Qué puede hacer esta red por mí?, si la persona que está enfrente es un administrador de red o de un sistema, su respuesta sería: proveer un servidor de DNS, servidores de correo, conexiones remotas y muchos otros servicios. Pero la visión de un administrador de seguridad es muy diferente, su cuestionamiento sería: ¿Qué puede hacer esta red por mí, que aún no sepa? o peor todavía ¿Qué puede hacer esta red por los atacantes?

En general, las redes son criaturas un tanto amorfas, difíciles de entender. Cualquier persona puede ver los cables, ruteadores y switches, pero no todos pueden interactuar directamente con los bits. Hasta los administradores más experimentados, no pueden ver de manera clara en todo momento qué es lo que está pasando. Cualesquiera que sean los propósitos, diseñar o auditar políticas de seguridad, hacer una prueba de penetración o adicionar más hardware a la red, tener una lista actualizada de la topología y dispositivos conectados a la red debe ser obligatorio.

4.6 Escaneo de puertos

El mapeo de una red es el proceso por el que se enumeran todos los hosts que responden satisfactoriamente en una red. El escaneo de puertos es el segundo paso y proporcionará la información de qué puertos están escuchando y listos para iniciar comunicación. Por supuesto, si un puerto está abierto es porque algún servicio está siendo proveído por él hacia otras máquinas en la red.

4.7 Escaneo de redes inalámbricas

Las tecnologías inalámbricas se han convertido en fáciles y baratas de implementar y brindan una nueva dimensión de seguridad para cualquier red. Antes de las redes inalámbricas, se podía salvaguardar una red, protegiendo únicamente el cableado y cuartos de servidores, todo se resumía a protección física. Las redes LAN inalámbricas y sus Access Points (*Puntos de Acceso)* pueden extender su cobertura muy a lo lejos de lo que las claves lo podrían hacer, inclusive a las afueras de las instalaciones de donde se encuentren, provocando con esto un gran problema de seguridad.

Los atacantes ya no necesitan romper los perímetros de seguridad o comprometer equipos de manera remota. Un atacante puede manejar su automóvil dentro del estacionamiento de una organización, con una laptop, tarjeta de red inalámbrica y una pequeña antena, logrando tener acceso al tráfico interno de la red. Hoy en día no se puede dar el lujo de pensar que se estará a salvo con tan solo estar detrás de un firewall[2], actualmente el perímetro de red está limitado a cualquier punto por el que un atacante pueda tener acceso. Una vez que el atacante haya comprometido la seguridad de la LAN inalámbrica, tendrá los mismos privilegios que un usuario autorizado, además poder estar en cualquier locación física que esté en el rango de la red inalámbrica.

La información que proporciona una herramienta para escanear redes inalámbricas es:

- Modo de operación.
- Canal.
- Dirección MAC del Access Point.
- Nombre de la red (SSID).
- Nivel de la señal y ruido (esto puede ser usado para ubicar la locación física del Access Point).
- Marca del equipo.
- Número de frames (capa 2 del modelo OSI) por segundo.
- Detectan el algoritmo de cifrado que se está usando.

Existen diferentes escaneadores de redes inalámbricas en el mercado entre los más destacados se tienen: NetStumbler por la parte de Windows y Kismet para los usuarios de Linux. Los dos cuentan con características muy parecidas, además de permitir hacer escaneos de forma pasiva, esto quiere decir que lo harán sin dejar rastro alguno.

Debido a la naturaleza de las redes inalámbricas, existe una oportunidad muy baja de evitar mapeos de red. Si una red inalámbrica se encuentra en un área muy poblada, se puede

[2] Un muro de fuego (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

esperar que esa red sea mapeada con frecuencia, algunas veces por *wardriving*[3] o por curiosos en busca de conectarse a Internet y algunas otras por personas que quieren explotar las debilidades de la red. Se puede reducir el rango de cobertura de la red, reduciendo la señal de alcance de equipo, usar diferentes técnicas para evitar el esparcimiento de señales de radiofrecuencia como utilizar barreras metálicas en las paredes o ventanas especiales, aunque esto no siempre es viable ya que resulta muy costoso.

Otra opción menos costosa es utilizar sistemas de cifrado y autenticación fuertes. Usualmente se cree que el monitoreo de redes inalámbricas se reduce únicamente al monitoreo de radiofrecuencias y no es así, también se puede monitorear la información de los *logs*[4], de los *Access Points* y los servidores de autenticación (RADIUS, LDAP) y así poder ubicar algún uso erróneo. Si se ve que un mismo usuario se conecta a la red en repetidas ocasiones con diferentes direcciones IP origen, esto puede ser indicio de que algo anda mal.

Finalmente, se debe tomar el tiempo para escanear la red de la organización y así darse cuenta de qué es lo que el atacante puede aprender de ella. Con esto se podrá conocer cuáles son las vulnerabilidades y remediarlas antes de que una amenaza por parte de un atacante se haga presente.

4.8 Sistemas de Detección de Intrusiones (IDS)

La detección de intrusos es el proceso de monitorear la actividad en un host o red, identificando pistas que puedan dar indicio de atentados o brechas de seguridad. Un Sistema de Detección de Intrusos IDS monitoreará la actividad que se sospecha o se sabe maliciosa, mandando alertas a las personas para que estas sean atendidas.

La persona que es responsable de dar atención a las alertas (manejador de incidentes) podrá usar la información generada por el IDS para tratar de identificar la actividad sospechosa y tomar alguna acción basada en su análisis. En este sentido, un IDS es un sistema de alarma para identificar actividad no deseada en la red o en los hosts. Igual que un sistema de alarma, éste no podrá detener las amenazas por sí solo, un IDS no provee ningún tipo de protección en contra de los atacantes. De hecho un IDS sólo podrá alertar sobre la existencia de actividad que lograría ser una amenaza para la red, permitiendo al manejador de incidentes responder a este tipo de actividad dependiendo de la severidad de las alertas.

No obstante, los sistemas IDS también presentan una serie de problemas y limitaciones, como podría ser la generación de falsas alarmas, ya sean éstas falsos negativos, que se producen cuando el IDS no es capaz de detectar algunas actividades relacionadas con incidentes de

[3] Se llama *wardriving* a la búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento. Implica usar un coche o camioneta y un ordenador equipado con Wi-Fi, como un portátil o una PDA, para detectar las redes. Esta actividad es parecida al uso de un escáner para radio.

[4] Un log es un registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática un log es usado para registrar datos o información sobre quién, que, cuando, donde y porque un evento ocurre para un dispositivo en particular o aplicación.

seguridad que están teniendo lugar en la red o en los equipos informáticos, o bien falsos positivos, que se producen cuando el IDS registra y genera alertas sobre determinadas actividades que no resultan problemáticas, ya que forman parte del funcionamiento normal del sistema informático o red.

Cualquier tipo de organización no deberá implementar un IDS como primer método o medida de seguridad para proteger sus recursos. Los IDS se usan en conjunto con los firewalls, anti-virus, analizadores de vulnerabilidades y herramientas de parcheo de sistemas para implementar una postura de defensa en profundidad.

La tecnología de los IDS no es algo nuevo, de hecho, tiene muchos años participando activamente en el mercado. Muchas organizaciones hacen buen uso de esta tecnología para identificar ataques y algunas otras cosas positivas aunque muchas otras siguen sin tener la capacidad de implementación por diversas razones.

4.8.1 IDS basado en red

Los NIDS *(Network Intrusion Detection Systems, Sistema de Detección de Intrusos en una Red)* son aquellos IDS interesados en los eventos que ocurren en una red. Esta variedad de IDS recolecta paquetes desde la red de manera pasiva. Cada paquete que es recolectado es procesado para encontrar eventos de interés y ser reportados al analista.

Para recolectar la información del tráfico necesaria, el NIDS es implementado en puntos donde pase mucho tráfico por la red, además de que muchas veces es apoyado por otros equipos que mandan una copia del tráfico que capturan hacia el IDS. Gracias a esto, un IDS puede captar todo el tráfico que pasa por todos los dispositivos, esto dependerá de la capacidad y características de procesamiento con las que cuente.

Un dispositivo NIDS puede estar dentro de un servidor o ser un *appliance (dispositivo integrado de seguridad)* con un sistema operativo lo suficientemente blindado para que pueda resistir cualquier tipo de ataque. Tener la posibilidad de monitorear todo el tráfico de la red, hace que un NIDS sea muy atractivo para los atacantes que busquen capturar información de la red. Los vendedores que producen IDS han tratado de reducir la posibilidad de que reciban ataques, reduciendo el número de servicios disponibles en el dispositivo, usando sistemas de cifrado robustos para cualquier comunicación entre el IDS y las estaciones que está monitoreando.

Los NIDS utilizan diferentes métodos para identificar eventos de interés en una red, incluyendo análisis de firmas, análisis de anomalías, protocolos y aplicaciones.

4.8.2 IDS basado en host

Los IDS basados en host HIDS *(Host Intrusion Detection System)* son un sistema de sensores que se encuentran cargados en varios servidores de una organización y controlados por un administrador central. Los sensores pueden analizar varios tipos de eventos y tomar acciones en el servidor en particular o enviar una notificación.

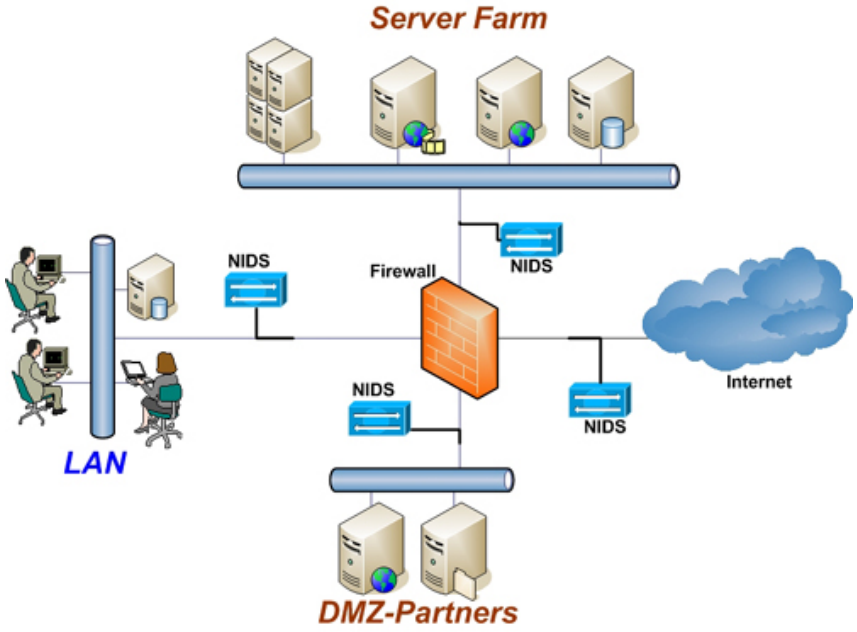
Los sensores de HIDS observan los eventos asociados con el servidor en el cual están cargados. El sensor de HIDS también puede determinar si un ataque tuvo éxito o no, puesto que el ataque estaba en la misma plataforma que el sensor.

4.8.3 IDS para redes inalámbricas

El mejor método que permite asegurar que la red inalámbrica este protegida contra intrusos, es el de implementar y monitorizar cuidadosamente un sistema de detección de intrusos (IDS), para detectar a los usuarios no autorizados cuando intentan acceder a la red. Si un hacker accede a la red, el IDS enviará una alerta de emergencia, el administrador de la red, con la esperanza de que pueda atajar el ataque en progreso, que identifique la vulnerabilidad abierta, y que impida al hacker el acceso a la red en el futuro.

Cuando se trata con una red inalámbrica, el sistema de detección de intrusos que se escoja puede ser un sistema de detección de intrusos, basado en un servidor (HIDS) o un sistema de detección de intrusos basado en red (NIDS).

Figura 4.2 Arquitectura IDS



4.9 Sistemas de Prevención de Intrusiones (IPS)

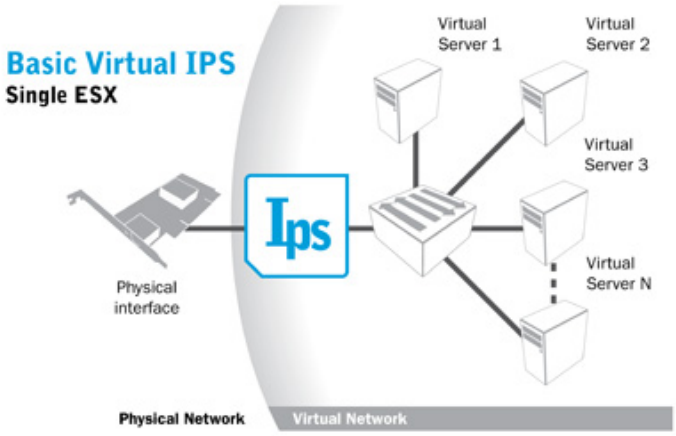
Un IPS es una tecnología que agrega otra capa de defensa para la protección de los recursos. A diferencia de los IDS que sólo reportan ataques en contra de los sistemas que monitorean, los IPS tratarán de detectar el ataque antes de que éste haya sido exitoso. Dependerá de cada vendedor el cómo se lleve a cabo la defensa de los recursos, aunque todos tendrán el mismo nombre, IPS.

Los IPS se clasifican generalmente en dos categorías, los basados en red llamados NIPS *(Network Intrusion Prevention System, Sistemas de Prevención de Intrusos Basados en Red)*,

o bien, los basados en host llamados HIPS (*Host Intrusion Prevention System, Sistemas de Prevención de Intrusos Basados en Host)*. Como su nombre lo indica, a nivel de red analizan el tráfico de forma similar a los NIDS. HIPS son instalados en host y detienen los ataques al sistema operativo o a nivel de aplicación.

Como la tecnología de IPS es reciente, se están haciendo esfuerzos significativos para reducir falsos positivos, reducir el impacto que tienen sobre el host/red y detener los ataques no conocidos hacia el objetivo. Muchas organizaciones que han implementado este tipo de herramienta son capaces de mitigar los efectos de diferentes tipos de ataque en contra de sistemas vulnerables, como ataques de hackers, gusanos y virus. El campo de los IPS crece de manera muy rápida y ha ganado importancia en empresas grandes.

Figura 4.3 IPS Virtual



Podemos clasificar los IPS que se encuentran en el mercado, en cuatro diferentes categorías:

- IPS e IDS.
- IPS y Firewall.
- IPS y Anti-Virus.
- Hardware Dedicado.

4.9.1 IPS e IDS

Esta categoría se refiere a aquellos vendedores que tradicionalmente han tenido IDS confiables a los que les han añadido la funcionalidad de detener la actividad que generó la alerta, antes de que ésta haya sido deliberada en la red o ejecutada por un host.

Esta funcionalidad de evaluar y desechar actividad maliciosa puede ejecutarse a nivel de red o a nivel de host.

Se sabe que los falsos positivos pueden ser un gran problema para la tecnología de IDS, pero lo son aún más en los IPS. Un falso positivo de un IDS genera una alerta que pudiese ser falsa, pero la actividad del IDS es benigna. Un falso positivo en un IPS detendrá servicios o tráfico legítimo, los que podrían ser una función de una aplicación de producción, un servidor de bases de datos o bien, un visitante entrando a una página web.

Falsos positivos en un IPS realmente tienen un costo significativo para la organización, ya que pueden causar ataques de denegación de servicio en recursos de producción.

4.9.2 IPS y Firewall

Los firewalls de filtrado de circuito se han convertido en una fuerte tecnología para muchas organizaciones. El paso siguiente para cada vendedor de firewalls es agregar las capacidades de un IPS a sus firewalls. Por la posición en la topología de red que tiene el firewall, es excelente para identificar eventos maliciosos en la red, implementando análisis desde la capa de transporte hasta la capa de aplicación para la identificación de ataques.

Como un firewall recolecta y analiza cada paquete que pasa a través de él, una evolución lógica sería que identificara el tráfico malicioso y generar una alerta o bien, que generara una alerta y lo eliminara, esto prevendría que el ataque fuera exitoso.

Vendedores como CISCO, NetScreen y Chek Point han integrado tecnologías de IPS a su línea de productos, además de desarrollar sus propias herramientas. El resultado son firewalls elegantes en lugar del clásico IPS, aunque este término puede confundirse a veces, ya que podrían no quedar claros los beneficios y sobre todo las limitaciones que la tecnología de IPS ofrece.

4.9.3 IPS y Anti-Virus

Un anti-virus es por mucho la herramienta de seguridad con más penetración en el mercado. La mayoría de las organizaciones han implementado manejos de control de distribución, implementación y actualización de sus antivirus. Pocas organizaciones son las que se atreven a poner un equipo en su red sin algún tipo de antivirus instalado.
Los vendedores de antivirus, se encuentran un paso atrás en el mercado de adicionar a sus productos. Tradicionalmente, los antivirus detectan actividad de virus y gusanos, pero están limitados a ese tipo de código malicioso. Recientemente, estos vendedores han empezado a expandir sus productos para identificar otros tipos de código malicioso incluyendo, spyware, puertas traseras, troyanos, etc. Este es un gran paso para la comunidad de antivirus, ya que muchos vendedores se han visto forzados a implementar en sus productos tecnologías similares a las de los antivirus para poder competir contra éstos. Compañías como Symantec han extendido su gama de productos para poder identificar todo tipo de código malicioso, en comparación de lo que tienen otros vendedores.

Las herramientas de antivirus generalmente utilizan dos métodos para proteger tanto las computadoras como los servidores de los virus. El primer método, analiza secuencialmente todos los archivos del sistema, pudiendo iniciarse dado un calendario o porque alguien lo

solicite. Cuando un archivo que está infectado es ubicado, el antivirus los limpiará. Este proceso puede llevar demasiado tiempo y consumir muchos recursos, que un equipo de producción no puede darse el lujo de desperdiciar. Al segundo método, se le conoce como analizador de memoria ya que únicamente analizará los archivos cuando éstos son abiertos y cerrados. Este método de análisis no detectará virus que estén en un estado inactivo en el sistema, pero requiere de mucho menos recursos de procesamiento. Este tipo de método no abre para su análisis archivos que no vayan hacer usados inmediatamente.

Un IPS basado en antivirus trabajará de forma muy similar a un antivirus configurado en realizar análisis de memoria, pero este incluirá también llamadas al sistema en el servidor donde esté siendo utilizado. El escáner de IPS podrá redireccionar las llamadas al sistema (incluyendo exploits y códigos maliciosos) para ser examinadas antes de que el sistema las ejecute. Una vez que el IPS las identifica como benignas, podrán ser pasadas al sistema operativo para que completen su acción. Si estás resultan ser un daño potencial para el sistema, como la alteración de un archivo, correr un proceso o escuchar un puerto, en específico para establecer una puerta trasera, el IPS rechazará la llamada y matará la aplicación.

4.9.4 Hardware Dedicado

Este tipo de IPS toma lo mejor de los firewalls, herramientas de IDS y ruteadores/switches poniendo todo esto en un dispositivo de alto rendimiento.

Este dispositivo puede describirse como un NIDS, ya que es instalado en línea en la red. Utiliza una combinación de aplicaciones de análisis, anomalías y reglas basadas en firma para identificar eventos que son malignos para la red. El tráfico de y para la red pasará a través de este dispositivo y todos los paquetes serán analizados antes de ser enviados a su siguiente destino. El tráfico que no genere ningún tipo de alerta será deliberado y el que sea marcado como tráfico malicioso será eliminado y almacenado en un log para su futura revisión. Esta tecnología parece muy buena, pero su implementación es muy compleja.

Como este dispositivo será puesto en línea en la red, deberá ser capaz de soportar la tasa de tráfico, pudiendo tener velocidades de Gigabits, además de que el manejo de paquetes debe hacerse de manera rápida y efectiva, implicando un gran consumo de recursos.

4.10 HIPS

Uno de los beneficios más grandes de la tecnología de un HIPS es la habilidad de identificar y detener tanto ataques conocidos como los que no lo son. Esta opción les permite a las organizaciones tener mucho más tiempo para desplegar parches y actualizaciones a sus equipos, ya que un HIPS los tendrá prevenidos ante las técnicas más comunes de ataques.

Para ser efectivo deteniendo los ataques, el HIPS usa una técnica llamada intercepción de llamadas al sistema, que es muy similar a lo que muchos antivirus han utilizado por años. El HIPS inserta sus propios procesos entre las aplicaciones que acceden a los recursos del host y

los recursos del sistema operativo. De esta manera el HIPS tiene la habilidad de permitir o denegar aquellas peticiones basándose en sí este las considera malignas o benignas.

Los HIPS utilizan una combinación de análisis de firma y análisis de anomalías para identificar los ataques, esto es realizado con base en el tráfico de monitoreo de las interfaces de red, monitoreando la integridad de archivos y el monitoreo del comportamiento de las aplicaciones.

Una ventaja significante de un HIPS es la habilidad de definir usuarios autorizados en tiempo real para el monitoreo de integridad de archivos. Esto se puede utilizar en un servidor WEB para prevenir que personas no autorizadas hagan cambios en las páginas de Internet, pero permitiendo a los desarrolladores web de la página hacer cambios cuando sea necesario.

4.10.1 Monitoreo de redes

Tal como lo hace un NIDS un HIPS monitoreará la red en busca de actividad maliciosa. Un HIPS utiliza análisis de firma y anomalías para identificar los ataques en contra de sistemas individuales. La diferencia es que en lugar de monitorear en forma pasiva, el software de HIPS interceptará los paquetes que se envían y reciben en la red. Al establecerse como intermediario, tendrá la posibilidad de primero analizar y después enviar el paquete a su destino o bien eliminarlo y generar una alerta. Este proceso es abstracto al tipo de red, interfaz o driver con el que se cuente. Un HIPS es capaz de monitorear tráfico del host con cualquier medio a través de una red inalámbrica, cableada, VPN[5] o un módem.

4.10.2 Ventajas de un HIPS

El uso de un HIPS incluye todas las ventajas de un HIDS, ya que identifica el cambio no autorizado de archivos, monitorea la actividad de la red y puede analizar tráfico cifrado. El beneficio que agrega un HIPS es, por supuesto, la habilidad de detener un ataque antes de que éste sea exitoso. Esto representa una gran ventaja para muchas organizaciones que luchan por tener tiempo para realizar actualizaciones y parches de sus equipos. Representa una gran ventaja para aquellas organizaciones que en los últimos años han tenido que emplear su perímetro de red. No hace muchos años las organizaciones sólo se preocupaban por los ataques provenientes de Internet, pero actualmente los ataques pueden provenir desde redes inalámbricas, módems, VPN, código malicioso introducido por usuarios que viajan hacia la red. Un HIPS provee un mejor método de defender el perímetro de la organización, cuando éste no está claramente definido.

4.11 NIPS

Desde la perspectiva de una red, un dispositivo NIPS opera como un switch conectando los segmentos internos y externos de la red. A diferencia de un switch, un NIPS usa una variedad de técnicas para detener ataques desde que entran hasta que salen de la red. Utilizando

[5] Una red privada virtual o VPN (siglas en inglés de virtual private network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

muchas de las técnicas empleadas por los NIDS, los dispositivos de NIPS pueden identificar eventos en la red que se consideren hostiles. Debido a su posición, en línea con el tráfico de red, un NIPS puede eliminar la actividad hostil antes de ser deliberada al objetivo.

Antes de que un NIPS se considerado como dispositivo efectivo, deberá superar varios retos:

Capacidades de detección

Los dispositivos NIPS utilizan las mismas técnicas de los tradicionales NIDS para reducir el riesgo de falsos negativos, pero no pueden tolerar falsos positivos en la red. Este es un reto muy importante para los NIPS y la mayoría de los vendedores están utilizando evaluación pasiva tanto de sistemas operativos como de vulnerabilidades.

Estabilidad

Debido a que un NIPS es un dispositivo que se pone en línea con el tráfico, representa un único punto de fallo para una red. Los dispositivos NIPS deben ser igual de estables que un firewall o switch para ganar la aceptación en el mercado. Deben ser también resistentes al tráfico malformado y no dejar de funcionar ante los protocolos de red existentes. Este es un riesgo muy similar que el de los falsos positivos, ya que si un NIPS no puede interpretar el tráfico correctamente o falla en el intento, puede causar una falla en la red y denegar así peticiones legítimas. Este tipo de fallas podrían ser accidentales o intencionales por parte del atacante buscando hacer una denegación de servicio.

Rendimiento de procesamiento

Los NIPS deben ser capaces de poder dar salida a todo el tráfico de red. Para ser prácticos y para monitorear redes, el IPS debe manejar velocidades de Gigabit Ethernet.

Latencia

Además de los requerimientos para usar técnicas extensivas de análisis de tráfico de red para identificar ataques, un NIPS debe ser capaz de tener una latencia muy baja, en el rango de los milisegundos.

Seguridad

Un NIPS debe ser seguro en para evitar ser comprometido, ya que un NIPS comprometido puede darle al atacante la habilidad de establecer un ataque de hombre en el medio en contra del tráfico que entra y sale en una red. Esto es logrado comúnmente configurando el NIPS sin ninguna dirección IP o MAC en las interfaces de dato o bien no contar con políticas claras de qué persona puede administrar el NIPS.

Todos los atacantes no perderán oportunidad para atacar un NIPS, hacer un ataque de denegación de servicio a la red o eludir la protección que provee, por lo tanto, los NIPS deben ser capaces de resistir cualquier ataque directo.

Con el fin de resistir las demandas de procesamiento y poder identificar tráfico malicioso a alta velocidad y sin latencia, los NIPS deben utilizar hardware de tipo ASICS[6] *(Application-Specific Integrated Circuit)* para realizar procesamientos paralelos. Usando ASICS especializados, los NIPS pueden satisfacer las demandas de rendimiento y escalabilidad, pero sacrificando flexibilidad. Mientras que los NIDS tradicionales operan bajo sistemas como Unix, Linux y Windows, los NIPS requieren más capacidad de procesamiento para cumplir las demandas de procesamiento y baja latencia.

Muchos vendedores están buscando la manera de clasificar e identificar actividad maliciosas con menor demanda de procesamiento del sistema y capacidad de memoria.

Una técnica es usar un esquema de clasificación para rápidamente explorar el tráfico para identificar eventos maliciosos. Muchos vendedores utilizan el término de filtrado de multiresolución, en esta técnica, análisis simples son aplicados en primera instancia. El análisis simple contiene sólo una parte de todas las capacidades del NIPS y aquel paquete que falle en una prueba, deberá ser sometido a un análisis profundo.

4.12 TCO

El TCO *(Total Cost of Ownership, Costo Total de Propiedad)* es un modelo presentado en el año 1987 por Hill Kirwin de Gartner Group Inc. En un principio, se trató de un modelo para evaluar las inversiones en compra de equipos de escritorio (PC), que luego fue extendido a redes LAN, sistemas cliente/servidor, computación distribuida, telecomunicaciones, centros de procesamiento de datos, y recientemente para sistemas portátiles (handheld).

El TCO es un modelo que pretende ayudar a los ejecutivos de empresas a evaluar tanto los costos directos e indirectos que están relacionados con la compra de cualquier activo informático. Por ejemplo, en el caso de la compra de una computadora, el modelo propone considerar no sólo el precio de la misma, sino también considerar como costo total, entre otras cosas, los costos de traslado, de espacio, consumo de energía, costos de implementación, costos por reparación o costos de recursos humanos. Todos estos costos ponderados permitirán tomar una mejor decisión a la hora de invertir.

Estimar el TCO involucra entender el costo inicial de adquisición: comúnmente se parte de los requerimientos técnicos y operativos que definen un conjunto de equipos, software, materiales y mano de obra de instalación. También se asocian costos con la operación, el más evidente es el mantenimiento. Las exposiciones al riesgo o responsabilidad legal, tales como multas por no conformidad con requerimientos regulatorios en ciertas industrias deben ser reducidas por diseño. Los ahorros de tiempo y ganancias en eficiencia también deben ser considerados en la ecuación.

[6] ASICS (Application-Specific Integrated Circuit), en español Circuito Integrado para Aplicaciones Específicas, es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general.

En general, los dos componentes principales del TCO son el Gasto de Capital *(*CapEX *o Capital Expenditures)* que corresponde a los gastos de adquisición, y los Gastos de Operación *(*OpEx *u Operating Expenditures)* que corresponde a todos los gastos que se generarán después de adquirido el sistema a lo largo de su vida útil.

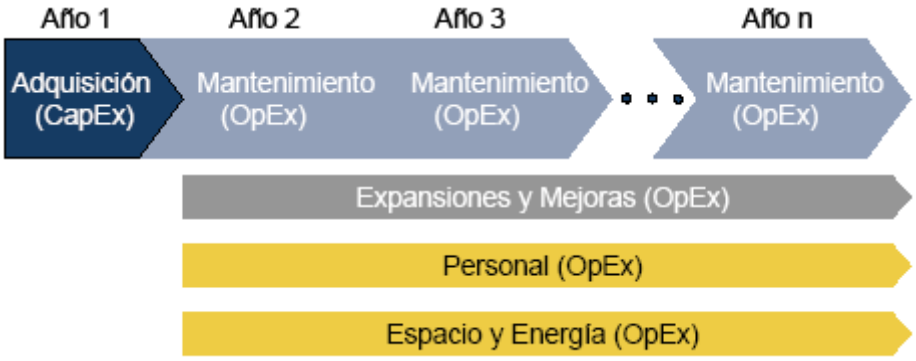
Costo de adquisición (CapEx)

- Análisis de riesgos
- Proyecto – Incluye ingeniería de detalle
- Administración del proyecto
- Construcción y/o acondicionamiento de edificios
- Equipos y software
- Equipos de red
- Equipos de comunicaciones
- Racks, energía, enfriamiento, etc.
- Canalizaciones y cableado
- Instalación, configuración y carga de información (servidores y clientes).
- Servicios profesionales de integración y personalización
- Documentación “Como fue construido”
- Comisionamiento y Arranque del Sistema

Costo de Operación (OpEx)
Normalmente se considera lo siguiente:

- Mantenimiento preventivo
- Mantenimiento correctivo
- Actualizaciones (Hardware y Software)
- Expansiones
- Mejoras

Figura 4.4 Componentes del TCO



Fuente: Bosh

4.12.1 TCO en Seguridad

Al poder implementar un modelo de inversión en seguridad, se podrán obtener beneficios para la organización, considerando el TCO y ROI para su evaluación.

Como se cita en el siguiente ejemplo, algunos de los costos que pueden evaluarse además del precio, para calcular el TCO de una solución antivirus serían:

- Consumo de recursos en el sistema
- Necesidad de inversión en hardware
- Necesidad de inversión en software y/o actualizaciones del sistema operativo
- Costo de horas necesarias de administración
- Costo de horas necesarias para desinfección de equipos con malware
- Costo de horas de implementación
- Costo de capacitación

Es decir, todos estos factores van a impactar en el dinero que la empresa necesitará para contar definitivamente con una solución antivirus. Por ejemplo, un antivirus cuyas tecnologías de detección sean más efectivas, tendrán un impacto en menor cantidad de infecciones, y por lo tanto disminuirá el costo por soporte. Una solución con bajo consumo de recursos, no tendrá costo adicional para invertir en hardware en los sistemas que noten una necesidad de mejorar su performance. Sin embargo, es frecuente que sólo se considere el precio de la solución como único factor respecto a la economía de la empresa y la implementación de la tecnología.

Figura 4.5 Relación Nivel de seguridad - TCO

Fuente: Check Point

4.13 ROI

ROI *(Return on Investment, Retorno de la Inversión)* se puede interpretar como el cálculo del beneficio económico o recompensa recibida que se obtendrá al proporcionar una cantidad de dinero o un capital de inversión para un producto, servicio o negocio.

Este término es usado comúnmente en el campo de tecnologías de la información y seguridad de la información y es calculado con la siguiente fórmula:

ROI= (ganancia – gastos)/(gastos) X 100%

Su medida es un número relacionado con la razón Costo/Beneficio. El costo es más sencillo de medir: casi siempre sabemos cuánto nos estamos gastando. Lo complicado es calcular el beneficio.

Los usos más comunes de ROI se aplican en el desarrollo de algún negocio, para evaluar si es viable la compra de un producto, servicio o la predicción de ingresos.

El ROI es difícil de medir por la entrada en juego de factores como

- El cambio tecnológico
- El desorden al controlar y medir las operaciones económicas durante un proyecto
- Factores intangibles como satisfacción de usuarios, mejoras o comunicación.

Recordemos que cualquier gasto en seguridad no deberá ser mayor que el costo del que se pretende proteger. La seguridad normalmente es considerada un gasto inútil por algunas empresas ya que sus beneficios no son tangibles hasta que algún tipo de amenaza se consolida.

4.14 Solución de un sistema IPS en seguridad

Las amenazas de hoy en día –tanto conocidas como desconocidas- son cada vez más destructivas y ocurren con más frecuencia que en el pasado. Las amenazas internas y externas, como los gusanos, ataques de denegación de servicio (DoS), caballos de Troya entre otros, tienen la capacidad de afectar de forma significativa la seguridad de las organizaciones.

Se requieren tecnologías de seguridad junto con una agudeza avanzada en la conexión de redes para poder defenderse con eficacia de esos ataques. Para una mayor eficacia estas tecnologías deben implementarse en toda la red, en lugar de limitarse a productos o tecnologías puntuales, puesto que el origen de un ataque puede estar en cualquier parte y propagarse de forma instantánea a todos los recursos de la red.

4.14.1 Check Point

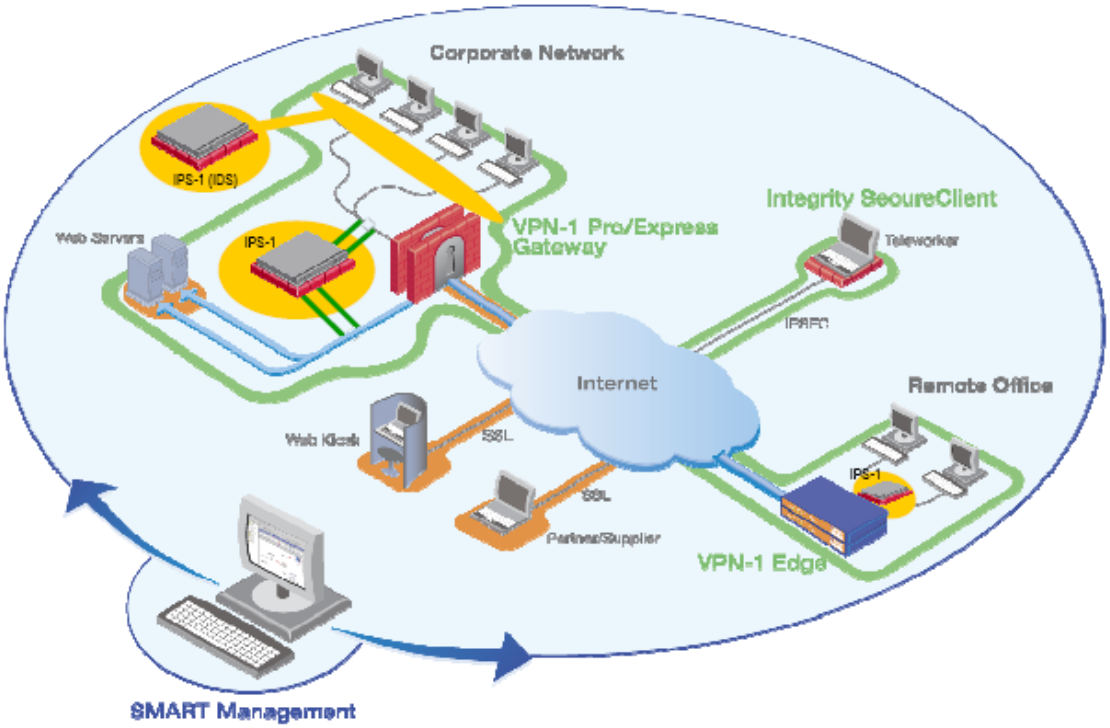
Check Point Software Technologies Ltd., es una compañía de software de seguridad. La compañía fue fundada en 1993 en Ramat-Gan, Israel, por Gil Shwed, Shlomo Kramer y Marius Nacht, y actualmente cuenta con oficinas centrales en EE.UU.

4.14.1.1 Check Point IPS-1

El IPS-1 de Check Point ofrece protección contra intrusiones en tiempo real para el perímetro de la red, las redes externas y la cada vez más vulnerable red interna. El sistema utiliza

sensores, los cuales son equipos de red de alta velocidad, que analizan paquetes de red individuales y detectan cualquier actividad sospechosa. Si el flujo de datos presenta una actividad no autorizada o un ataque a la red, los sensores pueden detectar la actividad indebida en tiempo real, enviar alarmas a un administrador y expulsar al atacante de la red.

Figura 4.6 Opciones de implementación de un IPS-1 dedicado



Fuente: Check Point

4.14.1.2 Descripción del IPS-1

IPS-1 está diseñado para la prevención de intrusos a escala empresarial a través de una arquitectura de múltiples niveles que ofrece escalabilidad y fiabilidad. La arquitectura del producto se muestra en la Figura 4.8

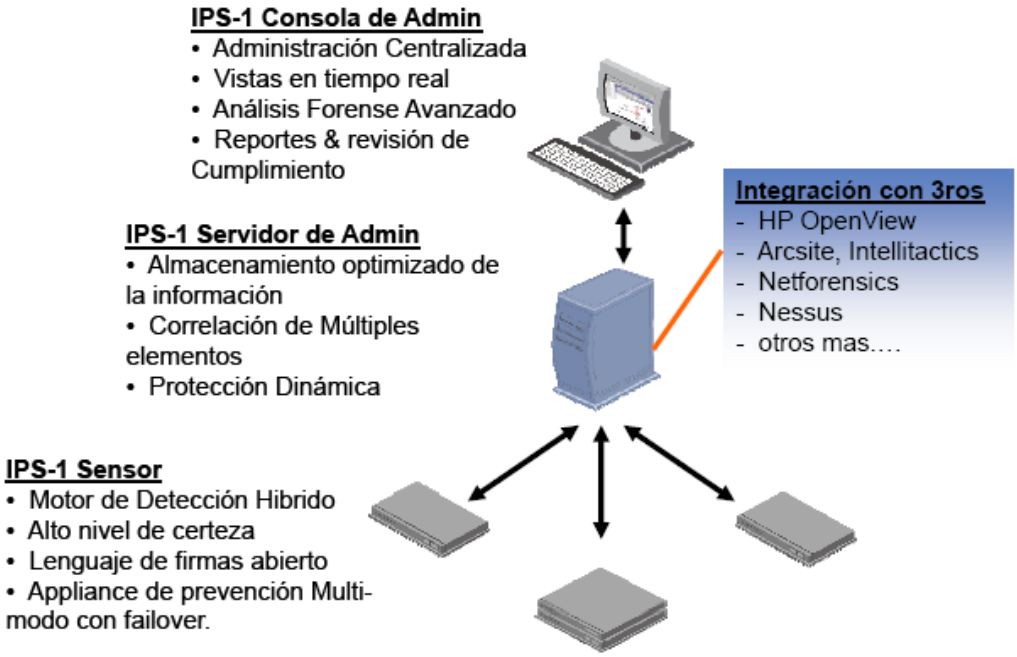
Figura 4.7 Check Point IPS-1

Check Point IPS-1 es un sistema de detección de intrusos y sistema de prevención (IDS / IPS) que ayuda a las organizaciones a proteger su red empresarial, y proteger los servidores y datos críticos contra ataques de gusanos conocidos y desconocidos, malware automatizado y amenazas combinadas.

Algunas características de IPS-1 son:

- Prevención de intrusos robusta y precisa
- Prevención de ataques precisa y granular
- Seguridad activa, accionable y adaptable
- Reportes y análisis forenses y avanzados
- Administración centralizada escalable e intuitiva

Figura 4.8 Arquitectura IPS-1



Fuente: Check Point

La arquitectura del IPS-1 se integra de tres componentes:

- IPS-1 Sensor
- IPS-1 Servidor de administración
- IPS-1 Consola de administración

4.14.1.3 Características y ventajas del IPS-1

Protección de Alto Desempeño

Desempeños desde 50Mbps hasta 4Gbps. IPS-1 Power Sensors ofrecen soporte a múltiples puertos, alta disponibilidad, incremento del desempeño a través de plug-ins, garantizado sin necesidad de afectar el desempeño.

Soporte a IPv6
IPv6 es un requerimiento crítico para los gobiernos de USA y Europa. IPS-1 soporta completamente IPv6.

Lenguaje Abierto de Firmas
Las firmas y el lenguaje de firmas de IPS-1 (llamado **N-Code**) es abierto, por lo que los usuarios pueden modificar las firmas existentes o crear sus propias firmas acoplándolas a sus necesidades.

Centro de Investigación de SmartDefense
Equipo de expertos en seguridad dedicado a la investigación y monitoreo continuo de nuevas vulnerabilidades o amenazas en Internet; y que provee soluciones rápidas a dichas amenazas.

Una de las características del IPS-1 es la habilidad única para combinar múltiples entradas para identificar ataques por lo que la seguridad es preparada y se adapta a protecciones automáticas.

Figura 4.9 Características y Ventajas IPS-1

4.14.1.4 Modelos de IPS-1

Check Point cuenta con una gama de productos de la familia IPS-1, a continuación se detallan algunas de sus características técnicas en la tabla 4.1.

Tabla 4.1 Modelos de IPS-1

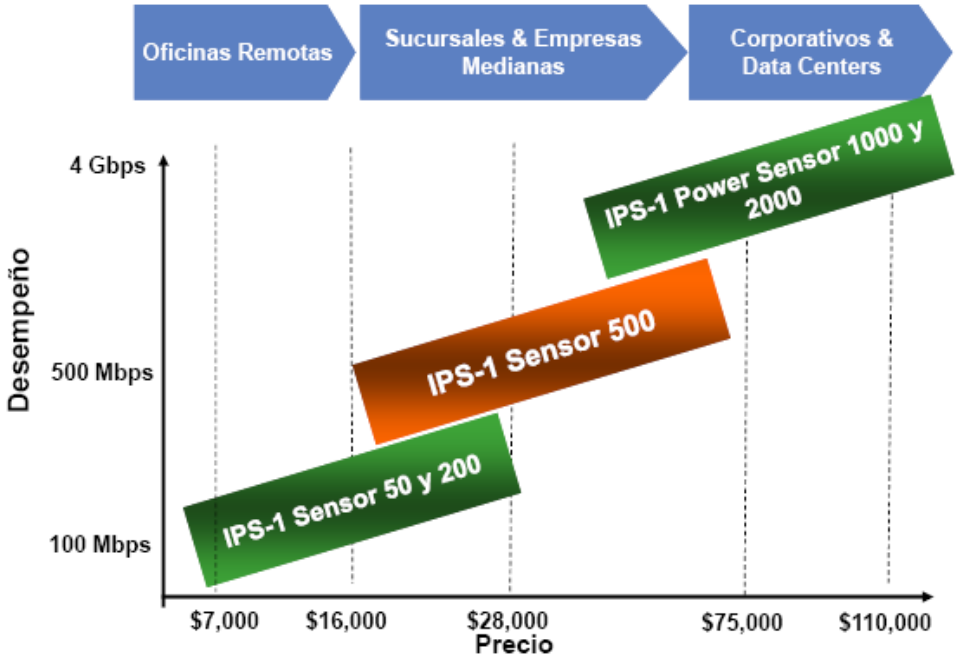
	IPS-1 Sensor 50	IPS-1 Sensor 200	IPS-1 Sensor 500	IPS-1 Power Sensor 1000	IPS-1 Power Sensor 2000
Localización en la Red	Oficinas remotas / Red Perimetral	Oficinas remotas / Red Perimetral	Red Perimetral (multi-segmentos)	Red core (multi-segmentos)	Red core (multi-segmentos)
Desempeño (IPS/IDS)	50/75 Mbps	200/250 Mbps	500Mbps/ 1Gbps	1/2Gbps	2/4Gbps
Sesiones Concurrentes	100,000	200,000	500,000	1.2 millones	2.8 millones
Interfases de Monitoreo	2 x 10/100/1000 Mbps en cobre	2 x 10/100/1000 Mbps cobre o 2 x 1000 Mbps fibra	4 x 10/100/1000 Mbps cobre o 4 x 1000 Mbps fibra	8 x 10/100/1000 Mbps cobre o 8 x 1000 Mbps fibra	8 x 10/100/1000 Mbps cobre o 8 x 1000 Mbps fibra

Fuente: Check Point

4.14.1.5 Costos de IPS-1

Los costos de los dispositivos IPS-1 van de acuerdo a las necesidades específicas de cada organización, es importante hacer notar que los diferentes productos IPS-1, pueden ser instalados desde una pequeña empresa hasta grandes corporativos, viéndose reflejado en el costo de adquisición (CapEx).

Figura 4.10 Línea de productos



Fuente: Check Point (Precios en USD)

4.14.1.6 Precios en el mercado de IPS-1

La tecnología de seguridad en especial el de los appliances, su costo de implementación y operación es elevado comprado con otro tipo de soluciones, ya que al integrar Hardware y Software robustece más el ámbito de la seguridad en la organización. Así mismo se debe de considerar el CapEx y el OpEx para conocer a fondo la viabilidad de implementación de la solución.

Tabla 4.2 Detalle de precios en USD

IPS-1 Administración			
SmartCenter UTM (5)	$10,000	SmartCenter Power (5)	$15,000
SmartCenter UTM (Unlimited)	$14,000	SmartCenter Power (Unlimited)	$22,000

IPS-1 Sensors		
IPS-1 Sensor 50	$7,000	50/75Mbps IPS/IDS, 1/3 networks IPS/IDS
IPS-1 Sensor 200	$16,000	200/250Mbps IPS/IDS, 1/3 networks IPS/IDS
IPS-1 Sensor 500	$28,000	500Mbps/1Gbps IPS/IDS, 2/4 networks IPS/IDS

IPS-1 Power Sensors		
IPS-1 Power Sensor 1000	$75,000	1/2Gbps IPS/IDS, 4/8 networks IPS/IDS
IPS-1 Power Sensor 2000	$110,000	2/4Gbps IPS/IDS, 4/8 networks IPS/IDS

Capítulo V Conclusiones

5.1 Introducción

Teniendo como objeto de estudio el análisis del protocolo de seguridad existente, y consecuentemente la identificación de las posibles vulnerabilidades de que puede ser objeto. Se pretende que al establecer una red inalámbrica de banda ancha, tal como WiMAX; se aporte la seguridad suficiente y eficiente, con la intención de que los usuarios puedan acceder a una red sin mayores problemáticas, tales como, la pérdida de datos de emisión críticas en las ondas, o el perímetro de cobertura, entre otros que hemos venido señalando. Bajo estos lineamientos hemos llegado a las siguientes consideraciones finales.

5.2 Conclusiones finales

Si bien es cierto, que la seguridad informática, es de suma importancia porque las redes inalámbricas pueden aumentar potencialmente la productividad y facilitar mucho más los servicios de información a una gran cantidad de usuarios. Al mismo tiempo, cabe considerar que las tecnologías introducen nuevas vulnerabilidades de seguridad, luego entonces, debe existir una planeación estratégica, para evitar posibles ataques a la red.

Las señales inalámbricas pueden retransmitir incluso atravesar paredes, permitiendo, que la red se escape fuera del dominio de la oficina, y que cualquier otro usuario, pueda insertar un dispositivo de acceso al flujo de red y poder realizar ataques dañinos.

Bajo estas consideraciones la seguridad de redes debe ser sistemática, al abarcar aspectos globales de un ambiente distribuido, como el hardware, software y las comunicaciones. Así mismo, la gran diversidad de ataques en las redes, y no contar con un eficiente sistema centralizado, acarrearía consecuencias, tales como, la denegación de servicios, o de ingeniería social, evitando que los usuarios legítimos puedan acceder a los recursos de la red. El ataque puede inundar una red con paquetes que ocupen todo el ancho de la banda, de ahí que los protocolos de seguridad buscan brindar servicios de seguridad en la transmisión de la información, sin importar el tipo, procedencia, sistema operativo o aplicación que la genere.

La protección no es exclusiva para le red en general, sino bien, abarca tanto a la organización como a los dispositivos y las aplicaciones, a saber, atiende primordialmente a los usuarios. Por lo que se debe establecer un blindaje bajo un esquema de seguridad, abarcando elementos de voz, datos, y video.

De la seguridad informática, se desprenden factores de autentificación, autorización y responsabilidad de los usuarios en los sistemas informáticos, así mismo, se han

desarrollado una gran variedad de algoritmos, mecanismos y técnicas para brindar protección a los recursos informáticos, y garantizar la integridad, confidencialidad y control de acceso de información. Puede hablarse de autenticación con criptografía o sin criptografía, los grandes problemas radican en la autenticación de personas y los mecanismos de distribución de llaves y certificados.

En un sistema de prevención de intrusos (IPC) se puede monitorear el tráfico de códigos maliciosos, consecuentemente, en base a herramientas tecnológicas, se podrá bloquear las vulnerabilidades a que están sujetos. Tal y como lo reiterábamos en el presente trabajo, las redes inalámbricas son un caso muy particular porque los datos viajan a través de un medio totalmente inseguro, lo que da origen a la necesidad de crear un sistema de seguridad específico para este tipo de tecnología de uso cotidiano.

Es sabido que, las redes inalámbricas de banda ancha se regulan mediante la familia de estándares 802.16x, en tanto, la importancia de WiMAX estriba en una tecnología que se basa en los estándares Wi-Fi, pero con ventajas que facilitan la creación de redes de área metropolitana (WMAN), como son: más ancho de banda, mayor distancia y mayor número de usuarios.

Es imposible que una red sea totalmente segura, y donde una organización que desee minimizar sus riesgos, tanto como sea, tecnológica como económicamente posible, se deberá empezar por implementar nuevas tecnologías de seguridad. Las primeras versiones de WiMAX están pensadas para comunicaciones punto a punto o punto a multipunto, típicas de los radio enlaces por microondas. Las posibles aplicaciones para WiMAX se basan en el gran ancho de banda y la alta cobertura. Las próximas ofrecerán total movilidad, por lo que competirán con las redes móviles, como los celulares. Empezando a aparecer en el mercado aquellas tecnologías que se enfoquen a proporcionar un enlace de alta velocidad para conexión a las redes fijas públicas o para establecer enlaces punto a punto.

Cada vez más, encontramos que el sector empresarial, se apoya indubitablemente del sector de las telecomunicaciones, con la finalidad de incrementar su productividad. Muchas de estas empresas cuentan con redes propias dentro de su ambiente y el siguiente paso es poder llevar estas aplicaciones internas para ser utilizadas en cualquier momento. Debido a la importancia de este sector y a la concentración de los usuarios masivos, WiMAX puede ofrecer una alternativa para brindar una red de expansión.

Glosario

AES: Un método de cifrado de clave simétrica que soporta contraseñas de hasta 256 bits.

Backhaul: Enlaces troncales para transmisión de datos ubicados entre la red central y los puntos de distribución de la red.

Broadband: Se refiere generalmente a conexiones a Internet con mucho más ancho de banda que con un modem de "dial-up" convencional.

Broadcast: Técnica para transmitir un mensaje a todos los usuarios dentro de una red. También se conoce como difusión.

Buffer: Entidad lógica para el almacenamiento temporal de datos.

Carrier: Proveedor de servicios de telecomunicaciones.

CapEX: Capital EXpenditures (CAPEX o CapEX o gastos de capital) son erogaciones o inversiones de capital que crean beneficios.

Default: Valor por omisión, o predeterminado de un parámetro o sistema.

Downlink: Canal físico o lógico para el envío desde la BS hacia los usuarios.

DoS: Un ataque que impide a los usuarios legítimos acceder a un cierto recurso. Puede desbordar la red consumiendo su ancho de banda o puede actuar sobrecargando los procesos de un servidor hasta conseguir que se colapse.

Ethernet: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10 Mbps, por lo tanto tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

Frame: También conocida como trama, es la unidad de transmisión de información digital a nivel de capa 2 en el modelo OSI.

Firewalls: Dispositivos físicos o lógicos utilizados para bloquear el acceso no autorizado a una red permitiendo la salida de tráfico de la misma.

Gateway: Un gateway es un punto de red que actúa como entrada a otra red.

Host: Nodo terminal en una red. Generalmente asociado a los usuarios finales.

Ingeniería Social: Engañar a alguien para que muestre su información confidencial convenciéndole de que debe hacerlo por algún motivo.

Intrusion Detection System (IDS): Software que monitoriza el tráfico de una red y alerta a los administradores del sistema cuando se detecta un intento de acceso no autorizado.

Intrusion Prevention System (IPS): Software que monitoriza el tráfico de una red e intenta identificar los ataques antes de que lleguen a penetrar las defensas del router.

LoS: Término utilizado en radiofrecuencia para un enlace de radio con visibilidad directa entre antenas.

Multicast: Técnica para transmitir un mensaje a un determinado grupo de usuarios dentro de una red.

Net ID: Es la identificación de la RED, es una dirección IP (IPv4), son los octetos situados al principio de la dirección del Host que identifica una máquina en una red.

nLoS: Sin línea de vista.

OpEx: Es una herramienta para el cálculo de gastos operativos (OPEX) para la gerencia de Servicios Técnicos

PDUs: (en inglés, *Protocol Data Units*), Unidades de Datos de Protocolo. Se utiliza para el intercambio entre unidades parejas, dentro de una capa del modelo OSI.

QoS: Acrónimo de Calidad de servicio. Una característica de algunos protocolos de red que trabajan con tipos distintos de tráfico de red en forma distinta para asegurar los niveles requeridos de confiabilidad y latencia de acuerdo con el tipo de tráfico.

QPSK: Acrónimo de la Modulación de fase por desplazamiento en cuadratura. Un método de modulación de señales digitales en señales de portadora de frecuencia de radio mediante el uso de cuatro estados de fase para codificar dos bits digitales.

RC4: Un algoritmo de seguridad que usa WEP. Considerado abiertamente como un algoritmo inseguro, RC4 fue desarrollado en 1987 por Ron Rivest, para la compañía RSA Data Security y fue un algoritmo propietario hasta 1994, cuando el código fue publicado en Internet y por tanto, para el resto del mundo.

RF: Acrónimo de Frecuencia de radio. En general, se refiere a las comunicaciones inalámbricas con frecuencias por debajo de 300 GHz. El término RU se usa comúnmente también para cubrir todos los tipos de sistemas inalámbricos.

RFC: Acrónimo de Solicitud de comentarios. Conjunto de documentos que se usa como el medio principal para comunicar información acerca de Internet. Probablemente las versiones más conocidas son las del IEEE. Algunas RFC son designadas como estándares de Internet.

Roaming: Tecnología que permite extender la conectividad de un usuario cuando se encuentra fuera de la red donde se registró su equipo y/o servicios.

ROI: Son las siglas en inglés de Return On Investment y es un porcentaje que se calcula en función de la inversión y los beneficios obtenidos, para obtener el ratio de retorno de inversión.

Router: Un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino.

Secure Sockets Layer (SSL): Un protocolo usado, inicialmente, para la transmisión segura de datos de una página Web a un servidor Web, pero también implementado para su uso en VPN.

Spoofing: Acciones encaminadas a hacer que una transmisión electrónica ha sido originada por un puesto en concreto cuando no es verdad.

Switch: Dispositivo que realiza la conmutación de las tramas en una red con base en hardware. Se utiliza para establecer distintos dominios de colisión dentro de una red.

TCO: El Costo total de propiedad (*Total Cost of Ownership, TCO*) es el costo total de un producto (por ejemplo, un sistema de información) a lo largo de su ciclo de vida completo.

TripleDES: Una versión de DES que usa contraseñas de 192 bits que en realidad son tres claves de 64 bits del DES tradicional.

TKIP: Un Protocolo de cifrado que incluye un método para cambiar la clave de cifrado con cada paquete que se envía durante una sesión.

UDP: Protocolo de Datagramas de Usuario

Uplink: Canal físico o lógico para el envío de datos de un usuario hacia la BS.

VoIP: La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos

Web: Gráfico Sistema utilizado para la visualización de páginas dentro de Internet.

WEP: Protocolo de seguridad perteneciente al estándar 802.11b.

Wi-Fi: Acrónimo de Wireless Fidelity. Es un conjunto de estándares para redes inalámbricas basado en las especificaciones IEEE 802.11.

WiMAX: Worldwide Interoperability for Microwave Access (Intercomunicación Mundial para Acceso por Microondas). Es un estándar de transmisión inalámbrica de datos (802.16d) diseñado para ser utilizado el área metropolitana o MAN, proporcionando accesos concurrentes en áreas de hasta 48 kilómetros de radio y a velocidades de hasta 70 Mbps, utilizando tecnología portátil LMDS.

WPA: Un protocolo de seguridad para redes inalámbricas que emergió como alternativa más segura a WEP.

xDSL: (Líneas de Subscripción Digital). Tecnología de tranmisión de datos que permite que los cables de cobre telefónicos (pots) transfieran hasta 16 Mbps.

Referencias Bibliográficas

Sweeney Daniel, *WiMax Operator´s Manual: Building 802.16 Wireless Network,* EUA: Paperback, 2004

Goldsmith Andrea, *Wireless communications,* EUA: Cambridge University Press, 2005.

Pareek Deepoak, *WiMax Taking Wireless to the MAX,* EUA: Taylor & Francis Group, 2006.

Miller S. Stewart, *Seguridad en Wifi,* (Traducción: Rafael Rodríguez de Cora & Gregorio Pérez Van Kappel), España: McGraw-Hill/ Interamericana de España, 2003.

Andrews G. Jeffrey, Ghosh Arunabha & Muhamed Rias, *Fundamentals of WiMAX: understanding broadband wireless networking*, EUA: 2007

Huidobro José Manuel, Millán Ramón J & Roldán David, *Tecnologías de Telecomunicaciones*, 1ª ed., México: Alfaomega Grupo Editor, 2006.

Hallberg Bruce A., *Fundamentos de Redes*, (Traducción: Jorge Omar Fuentes Zárate), 1ª ed., México: McGraw-Hill Interamericana, 2003.

Casad Joe & Willsey Bod, *Aprendiendo TCP/IP en 24 Horas*, (Traducción: Agustín Cacique Valadez), 1ª ed., México: Prentice-Hall Hispanoamericana, 1999.

Maiwald Eric, *Fundamentos de Seguridad de Redes*, (Traducción: Efrén Alatorre Miguel), 2ª ed., México: McGraw-Hill Interamericana, 2003.

Gómez, Álvaro, *Enciclopedia de la Seguridad Informática*, 1ª ed., México: Alfaomega Grupo Editor, 2007.

Harrington Jan L., *Manual Práctico de Seguridad de Redes*, 1ª ed., España: Ediciones Anaya Multimedia, 2006.

Referencias Electrónicas

The IEEE 802.16 Working Group on Broadband Wireless Access Standards

http://ieee802.org/16/

WiMAX Forum

http://www.wimaxforum.org/

RFC Editor Webpage

http://www.rfc-editor.org/

Broadband Wireless Metropolitan Area Network

http://standards.ieee.org/getieee802/802.16.html

Enterate en línea (Internet Computo y Telecomunicaciones)

http://www.enterate.unam.mx

Alvarion: A wireless broadband pioneer, a founder of the WiMAX industry

http://www.alvarion.com

LatinWiMAX 2.1 (Beta)

http://www.latinwimax.com

Comisión Federal de Telecomunicaciones

http://www.cofetel.gob.mx

Telesemana

http://www.tele-semana.com/noticias/

Unión Internacional de Telecomunicaciones

http://www.itu.int

Intel

http://www.intel.com

Cisco

http://www.cisco.com

Laboratorio de Seguridad - UNAM

http://www.seguridad.unam.mx/labsec/

IPv6 México, Capítulo Mexicano del Foro IPv6

http://www.ipv6.unam.mx

Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información

http://www.canieti.org

Motorola

http://www.motorola.com

Security Appliances, Security Gateways, Security Management, Endpoint Security

http://www.checkpoint.com