UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SEGURIDAD E IMPLEMENTACION DE WIRELESS LAN
INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JHONNY PEDRO ROSAS TORRES

PROMOCIÓN
2002 - II

LIMA – PERÚ
2008

SEGURIDAD E IMPLEMENTACION DE WIRELESS LAN

Dedicado a:

Mi madre, Maribel y hermanas Elizabeth y Gloria.

Quienes me brindaron todo su apoyo para culminar mis estudios universitarios

SUMARIO

El presente informe detalla los fundamentos de seguridad y las características del lugar a considerar en la implementación de una red inalámbrica Wireless LAN así como la forma es que ésta se va a complementar con la red LAN cableada tradicional. Se describe también las recomendaciones y aplicaciones de protocolos de seguridad basados en estándares internacionales.

El desarrollo de este informe consta de 4 capítulos, estructurados de la siguiente manera:

En el Capítulo I: Breve descripción de la tecnología inalámbrica
Se describen los tipos y características de transmisión inalámbrica así como las razones a considerar para la decisión de implementar una solución WLAN

En el Capítulo II: Estándares y entidades reguladoras de WLAN
Mención a los principales estándares internacionales que tienen que cumplir las redes inalámbricas así como los protocolos de seguridad.

En el Capítulo III: Fundamentos de Wireless LAN
Se detalla los fundamentos de seguridad de una red Wireless LAN así como las vulnerabilidades y ataques a los que están expuestas estas redes; a su vez se menciona la evolución de la tecnología de seguridad en WLAN y las consideraciones en políticas de seguridad a nivel empresarial. Se detalla también una infraestructura de red con equipos cisco, empresa que está a la vanguardia en equipo de comunicaciones

En el Capítulo IV: Implementación de red Lan y Wireless Lan realizada por la empresa Orange Business, líder en tecnología de información a la Empresa Inkia Perú, en los que se destaca los características a considerar para la implementación de una red Interna.

ÍNDICE

PRÓLOGO

La seguridad de la red es el proceso por el cual se protegen los recursos de información digital, los objetivos de la seguridad son mantener la integridad, proteger la confidencialidad y asegurar la disponibilidad. El crecimiento exponencial de las redes y la computación ha generado enormes avances en la forma en que las personas viven y trabajan. Por lo tanto, todas las redes deben estar protegidas para alcanzar su máximo potencial. Las redes WILAN no son la excepción, su crecimiento sostenido a nivel mundial ha obligado a la necesidad de implementar normas de seguridad más confiables dando lugar a los avances en temas de seguridad.

El objetivo es las consideraciones a tener en cuenta en una implementacion de una red local debido a que en nuestro país hay un gran número de pequeñas empresas que poseen una red interna en las cuales no les dan la importancia debida a la seguridad; a esto se suma el crecimiento de la tecnología inalámbrica la cual por sus características es necesario implementarla aumentando considerablemente los riesgos de seguridad.

Se detalla también las consideraciones a tener en cuenta en la implementación de una red interna y la forma como se van relacionando los diversos protocolos de seguridad en una red LAN tradicional con una Wireless LAN basándonos en una implementación realizada a la empresa Inkia Peru, en la cual se realizó el estudio completo de su infraestructura, en cuya implementación se utilizaron equipos cisco debido a su confiabilidad y escalabilidad que brinda.

Hablaremos sobre los fundamentos de la seguridad de las WLAN, la forma como han ido evolucionando, las vulnerabilidades de la primera generación de WLAN hasta el estándar 802.11i, el cual mejora a sus predecesores tanto en lo que autenticación de usuarios como la robustez de los métodos de encriptación se refiere. Y lo consigue en el primer caso gracias a su capacidad para trabajar en colaboración con 802.1X, y en el segundo lugar, mediante la incorporación de encriptación Advanced Encryption Standard (AES).

CAPÍTULO I

DESCRIPCIÓN DE LA RED WLAN

1.1 Introducción a las WLAN

Las WLANs redefinen la forma en que la industria contempla las LANs. La conectividad ya no implica conexión física. El networking inalámbrico proporciona todas las funciones y beneficios de las tecnologías de LAN tradicionales sin alambres ni cables. La libertad de movilizarse sin perder la conectividad ha ayudado a conducir al networking inalámbrico hasta nuevos niveles.

Existen cuatro factores importantes a considerar antes de implementar una red inalámbrica:
Alta disponibilidad
Escalabilidad
Gestionabilidad
Arquitectura abierta

En términos sencillos, una red de área local inalámbrica (WLAN) proporciona todas las funciones y beneficios de las tecnologías LAN tradicionales, como Ethernet y Token Ring, pero sin las limitaciones impuestas por los alambres o cables. De esta forma, las WLANs redefinen la forma en la cual la industria contempla las LANs. Conectividad ya no significa conexión física. Las áreas locales ya no se miden en pies cuadrados ni en metros cuadrados, sino en millas o kilómetros cuadrados. Una infraestructura no necesita estar enterrada u oculta detrás de los muros, sino que puede desplazarse y cambiar según las necesidades de una organización.

1.2 Medios De Transmisión

Las señales inalámbricas son ondas electromagnéticas, que pueden viajar a través del espacio. La capacidad de las ondas de radio de atravesar las paredes y abarcar grandes distancias convierte a la tecnología inalámbrica en una forma versátil de construir una red.

Una WLAN, requiere un medio físico a través del cual pasan las señales de transmisión, utilizan luz infrarroja (IR) o frecuencias de radio (RFs). El uso de la RF es más común debido a su mayor alcance, ancho de banda y más amplia cobertura.
Las WLANs utilizan las bandas de frecuencia de 2,4 gigahertz (GHz) y de 5 GHz. Estas porciones del espectro de RF están reservadas en la mayor parte del mundo para dispositivos sin licencia. El networking inalámbrico proporciona la libertad y la flexibilidad para operar dentro de edificios y entre edificios.

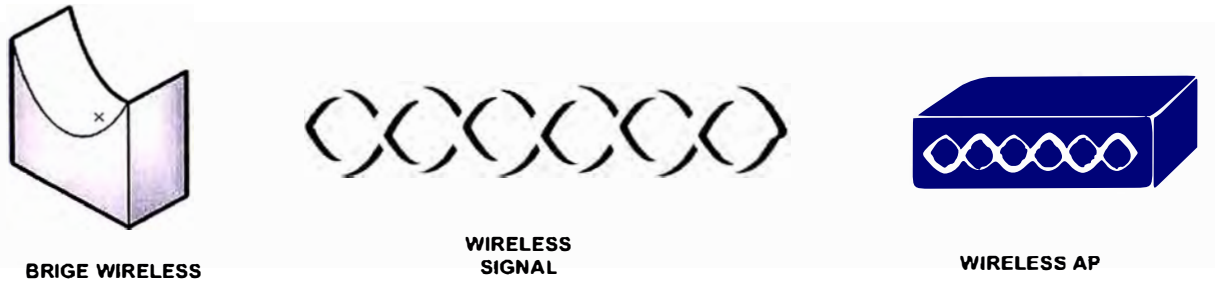

Fig. 1.1 Símbolos representan los típicos dispositivos inalámbricos y sus funciones

Los dispositivos inalámbricos son sólo una parte de la LAN cableada tradicional. Estos sistemas inalámbricos, diseñados y construidos utilizando microprocesadores y circuitos digitales estándar, se conectan a sistemas LAN cableados. Además, los dispositivos inalámbricos deben recibir alimentación que les proporcionen energía para codificar, decodificar, comprimir, descomprimir, transmitir y recibir señales inalámbricas.
Los dispositivos WLAN de primera generación, con sus bajas velocidades y falta de estándares, no fueron populares. Los sistemas estandarizados modernos pueden ahora transferir datos a velocidades aceptables.
El comité IEEE 802.11 y la Alianza Wi-Fi han trabajado diligentemente para hacer al equipo inalámbrico estandarizado e interoperable.

La tecnología inalámbrica soportará ahora las tasas de datos y la interoperabilidad necesarias para la operación de la LAN. Las WLANs son una opción costeable para la conectividad LAN. En la mayoría de los países estos dispositivos no requieren licencia gubernamental.

1.3 Tipos De Transmisión

El estándar de WLAN 802.11 permite la transmisión a través de medios diferentes. Los medios especificados incluyen los siguientes:

Luz infrarroja

Tres tipos de transmisión de radio dentro de las bandas de frecuencia de 2,4 GHz no licenciadas:

Espectro expandido de saltos de frecuencia (FHSS)

Espectro expandido de secuencia directa (DSSS)

Multiplexado por división de frecuencia ortogonal (OFDM) 802.11g

Un tipo de transmisión de radio dentro de las bandas de frecuencia de 5 GHz no licenciadas:

Multiplexado por división de frecuencia ortogonal (OFDM) 802.11a

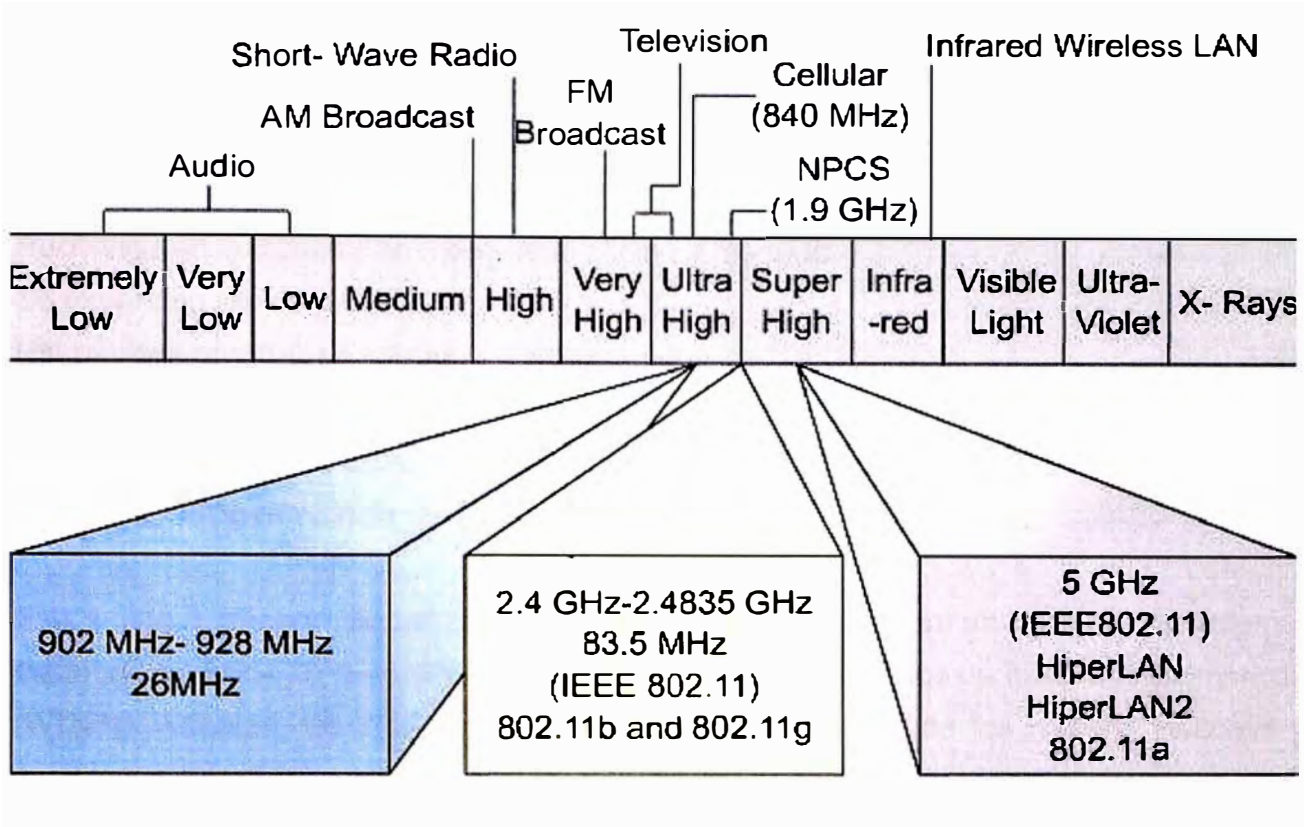

Fig. 1.2 Banda de frecuencias no licenciadas

1.4 Razones Para Utilizar Tecnología Inalámbrica

Las LANs Ethernet cableadas actuales operan a velocidades de alrededor de 100 Mbps en la capa de acceso, 1 Gbps en la capa de distribución, y hasta 10 Gbps a nivel de la capa principal. La mayoría de las WLANs operan a una velocidad de 11 Mbps a 54 Mbps en la capa de acceso y no tienen como objetivo operar en la capa de distribución o en la capa principal.

El costo de implementar WLANs compite con el de las LANs cableadas. A nivel de la capa de acceso el ancho de banda es comparable teniendo en cuenta que el Ancho de banda brindado por las WLAN es suficiente para soportar las necesidades de las aplicaciones y del usuario

Con muchas oficinas conectadas ahora a la Internet por medio de servicios de banda ancha como DSL o cable, las WLANs pueden manejar las demandas de ancho de banda. Las WLANs permiten a los usuarios movilizarse dentro de un área definida con libertad y aún así permanecer conectados. Durante las reconfiguraciones de oficina, las WLANs no requieren un recableado ni sus costos asociados.

Los entornos que es beneficiarían con una solución WLAN tienen las siguientes características:
Requieren las velocidades de una LAN Ethernet estándar
Se benefician de los usuarios móviles
Reconfiguran la disposición física de la oficina a menudo
Se expanden rápidamente
Utilizan una conexión a Internet de banda ancha
Enfrentan dificultades significativas al instalar LANs cableadas
Necesitan conexiones entre dos o más LANs en un área metropolitana
Requieren oficinas y LANs temporales

Existe una tendencia actual para que los ISPs proporcionen un servicio de Internet inalámbrico. Estos ISPs se denominan Proveedores de Servicios de Internet Inalámbricos (WISPs). Además, las WLANs no reemplazan la necesidad de los routers, switches y servidores cableados tradicionales de una LAN típica.
Incluso aunque las WLANs han sido diseñadas principalmente como dispositivos LAN, pueden utilizarse para proporcionar una conectividad de sitio a sitio a distancias de hasta 40 Km. (25 millas). El uso de dispositivos de WLAN es mucho más eficaz en costos que el uso del ancho de banda WAN o la instalación o arrendamiento de largas trayectorias de fibra. Por ejemplo, para instalar una WLAN entre dos edificios se incurrirá en un costo único de varios miles de dólares estadounidenses. Un enlace dedicado, que sólo proporciona una fracción del ancho de banda de una WLAN, costará mucho más. Instalar fibra a grandes distancias, es más costoso que una solución inalámbrica.

CAPÍTULO II

ESTANDARES Y ENTIDADES REGULADORAS DE WLAN

En los sistemas de redes existen entidades encargadas de registrar y regular los estandares y para el caso de wireless LAN tenemos el Institute of Electrical and Electronics Engineers (IEEE) the Internet Engineering Task Force (IETF) entre las más importantes. Por ejemplo, el estandar 802.11 esta definida por IEEE y el Protocolo de Seguidad Extensible (EAP) utilizado para autenticación de clentes WLAN está definida por la IETF los cuales son los más importantes para el soporte de seguridad de WLAN

2.1 Institute Of Electrical And Electronics Engineers – IEEE

Define el grupo de estandares 802.11 los cuales son aplicados para la redes WLAN. Se tiene por ejemplo, los standares 802.11b, 802.11a, 802.11g para la trasferencia de bit en medios inalámbricos, el 802.11e para calidad de servicio QoS, también define el 802.1X para seguridad que utiliza el estándar 802.11i para la autenticacion de clientes WLAN.

2.2 Internet Engineering Task Force - IETF

Provee el principal protocolo asociado con el protocolo 802.11, el protocolo de autenticacion extendida EAP, el cual es transportado a través de las WLAN en tramas 802.1X para la autenticación y autorización de clientes WLAN

2.3 WI-FI Alliance

Provee el estándar para la interoperatividad de entre dispositivos de varios marcas, permitiendo la integración de diversas plataformas

La Wi-Fi Alliance es quien certifica la interoperatividad entre dispositivos WLAN, el protocolo Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), y Wi-Fi Multimedia (WMM) certification programs.

El estándar WPA fue desarrollado para direccionar el proceso de encriptación WEP el cual existía antes de la estndar 802.11i y una de sus objetivos fue precisamente asegurar la compatibilidad con el hardware basado en WEP

2.4 Federal Communications Commission – FCC

La FCC es la entidad que regula y controla es spectro de Radio Frecuencia utilizado por las WLAN en los EE. UU, así como también las potencias de radio y ganancia de una antena. El espectro de radio correspondiente al 802.11 no es licenciado y está disponible pero está regulado en caso que el abuso del spectro de radio interfiera con otras señales

CAPÍTULO III

FUNDAMENTOS DE WIRELESS LAN

3.1 Fundamentos de Seguridad

La seguridad de la red es el proceso por el cual se protegen los recursos de información digital. Los objetivos de la seguridad son mantener la integridad, proteger la confidencialidad y asegurar la disponibilidad. El crecimiento de la computación ha generado enormes avances en la forma en que las personas viven y trabajan. Por lo tanto, todas las redes deben estar protegidas para alcanzar su máximo potencial. Debido al crecimiento exponencial del networking, incluyendo las tecnologías inalámbricas, ha conducido a aumentar los riesgos de seguridad.

Un propósito principal de la seguridad es mantener afuera a los intrusos. En el caso de las LAN cableadas es restringir el acceso de personas a las instalaciones donde se ubican los puntos de red implementados, pero debido al crecimiento de las redes inalámbricas que es el caso de WLAN estas formas de seguridad sean inadecuadas.
Las soluciones de seguridad deben estar integradas sin fisuras y ser muy transparentes, flexibles y administrables. Cuando se habla de seguridad, se hace referencia a asegurar que los usuarios puedan realizar sólo las tareas que tienen autorizado hacer y que puedan obtener sólo la información que tienen autorizado tener. La seguridad también significa asegurar que los usuarios no puedan causar daño a los datos, a las aplicaciones o al entorno operativo de un sistema. La palabra seguridad comprende la protección contra ataques maliciosos. La seguridad también comprende el control de los efectos de los errores y de las fallas del equipo. Todo lo que pueda proteger contra un ataque inalámbrico evitará también otros tipos de problemas.

Tabla 3.1 Balance entre permitir el acceso autorizado y evitar el acceso no autorizado

ACCESO TRANSPARENTE	SEGURIDAD
Conectividad	Autenticación
Performance	Autorización
Facilidad de utilización	Asociacion
Facilidad de administración	Confiabilidad
Disponibilidad	Integridad de los Datos

3.2 Vulnerabilidades de las WLANs

Las WLANs son vulnerables a ataques especializados. Muchos de estos ataques explotan las debilidades de la tecnología, ya que la seguridad de WLAN 802.11 es relativamente nueva. También existen muchas debilidades de configuración, ya que algunas compañías no están usando las características de seguridad de las WLANs en todos sus equipos. Muchos dispositivos son entregados con passwords de administrador predeterminadas. Finalmente, hay debilidades de políticas. Cuando una compañía no tiene una política inalámbrica clara sobre el uso de la tecnología inalámbrica, los empleados pueden configurar sus propios APs. que raramente es seguro.

Se detalla los principales vulnerabilidades del protocolo 802.11:

• Autenticación débil únicamente de dispositivo

Se autentican los dispositivos clientes. Los usuarios no se autentican.

• Encriptación de datos débil

Se ha probado que la Privacidad Equivalente a la Cableada (WEP) es ineficiente como medio para encriptar datos.

• No hay integridad de mensajes

Se ha probado que el Valor de Control de Integridad (ICV) no es efectivo como medio para asegurar la integridad de los mensajes.

Para que las vulnerabilidades de seguridad del 802.11 no afecte el desarrollo de las WLAN empresariales, Cisco ha desarrollado la Suite de Seguridad Inalámbrica el cual presenta mejoras solidas a la encriptación WEP y autenticación centralizada basada en usuarios.

3.3 Amenazas a la WLAN

Existen cuatro clases principales de amenazas a la seguridad inalámbrica:

- Amenazas no estructuradas
- Amenazas estructuradas
- Amenazas externas
- Amenazas internas

Las amenazas no estructuradas consisten principalmente en individuos inexpertos que están usando Herramientas de hacking como scripts de shell y crackers de passwords.

Las amenazas estructuradas vienen de hackers que son técnicamente mejor capacitados, estas personas conocen las vulnerabilidades de los sistemas inalámbricos y pueden comprender y desarrollar explotación de códigos, scripts y programas.

Las amenazas externas son individuos u organizaciones que trabajan desde el exterior de la compañía. Ellos no tienen acceso autorizado a la red inalámbrica. Ingresan a la red principalmente desde el exterior del edificio. Estos son los tipos de amenazas por los que las empresas gastan la mayor parte del tiempo y dinero en protegerse.

Las amenazas internas ocurren cuando alguien tiene acceso autorizado a la red con una cuenta en un servidor o con acceso físico al cableado.

El acceso inalámbrico puede ser una gran amenaza a la seguridad de la red. La mayoría de las WLANs, Tienen pocas o ninguna restricción. Una vez asociado a un access point, un atacante puede recorrer libremente la red interna.

3.4 Métodos de ataques Inalámbricos

Los métodos de ataques inalámbricos pueden ser divididos en tres categorías:

- Reconocimiento
- Ataque de acceso
- Negación del Servicio (DoS)

3.4.1 Reconocimiento

El reconocimiento es el descubrimiento y mapeo no autorizado de sistemas, servicios o vulnerabilidades, también es conocido como reunión de información y normalmente precede a un acceso real o ataque DoS.
La realización del reconocimiento comprende el uso de comandos o utilitarios comunes para conocer tanto como sea posible el sitio a accesar

El snooping (simulación) inalámbrico y el sniffing (rastreo) de paquetes son términos comunes para las escuchas. El usar encriptación y evitar protocolos que son fácilmente escuchados puede combatir las escuchas. Los analizadores de protocolos inalámbricos comerciales como AiroPeek, AirMagnet, o Sniffer Wireless se pueden usar para escuchar las WLANs. Las escuchas inalámbricas se pueden usar para ver el tráfico de la red y descubrir los SSIDs en uso, las direcciones MAC válidas o para determinar si la encriptación está siendo usada. El reconocimiento inalámbrico a menudo es llamado wardriving. Los utilitarios usados para explorar las redes inalámbricas pueden ser activos o pasivos. Las herramientas pasivas, como Kismet, no transmiten información mientras están detectando redes inalámbricas.

Los utilitarios activos, como el NetStumbler, transmiten pedidos de información adicional sobre una red inalámbrica, una vez que es descubierta.
El sistema operativo Windows XP es sensible a la tecnología inalámbrica. Windows XP realiza una búsqueda activa. Intentará conectarse automáticamente a una WLAN descubierta. Algunas personas que usan herramientas WLAN están interesadas en recolectar información acerca del uso de la seguridad inalámbrica. Otros están interesados en encontrar WLANs que ofrezcan acceso libre a Internet o una puerta trasera fácil hacia una puerta corporativa.

3.4.2 Acceso

El acceso al sistema, en este contexto, es la capacidad para que un intruso no autorizado logre acceder a un dispositivo para el cual no tiene una cuenta o password. Para ingresar se debe ejecutar un hack script o una herramienta que explote una vulnerabilidad conocida del sistema o aplicación a ser atacada. Acceso es un término que hace referencia a la manipulación de datos, acceso a sistemas o escaladas privilegiadas no autorizados.

Algunos ejemplos de acceso son los siguientes:

- Explotación de passwords débiles o no existentes
- Explotación de servicios como HTTP, FTP, SNMP, CDP y Telnet.

3.4.3 Ataque de un AP furtivo

La mayoría de los clientes se asociarán al access point con la señal más fuerte. Si un AP no autorizado, que por lo general es un AP furtivo, tiene una señal fuerte, los clientes se asociarán al él. El AP furtivo tendrá acceso al tráfico de red de todos los clientes asociados. Por lo tanto, el AP furtivo puede ser usado para realizar ataques por desconocidos contra tráfico encriptado como SSL o SSH. El AP furtivo también puede usar spoofing de ARP e IP para engañar a los clientes para que envíen passwords e información confidencial. El AP furtivo puede también pedir sesiones no protegidas con La Privacidad Equivalente a la Cableada (WEP) con clientes durante la asociación.

3.4.4 Negación del servicio

La DoS ocurre cuando un atacante desactiva o corrompe las redes, sistemas o servicios inalámbricos, con la intención de negar el servicio a usuarios autorizados. Los ataques DoS toman muchas formas. En la mayoría de los casos, la realización del ataque comprende simplemente ejecutar un hack, una script o una herramienta. El atacante no necesita acceder previamente al objetivo, porque todo lo que se necesita normalmente es una forma de acceder a él. Por estas razones y a causa del gran daño potencial, los ataques DoS son los más temidos, ya que son los más difíciles de evitar.

Muchos ataques DoS contra las redes inalámbricas 802.11 han sido teorizados. Un utilitario, llamado Wlan Jack, envía paquetes de disociación falsos que desconectan a los clientes 802.11 del access point. Siempre que se ejecute el utilitario de ataque, los clientes no pueden usar la WLAN. De hecho, cualquier dispositivo que opere a 2.4 GHz o a 5 GHz puede ser usado como una herramienta DoS

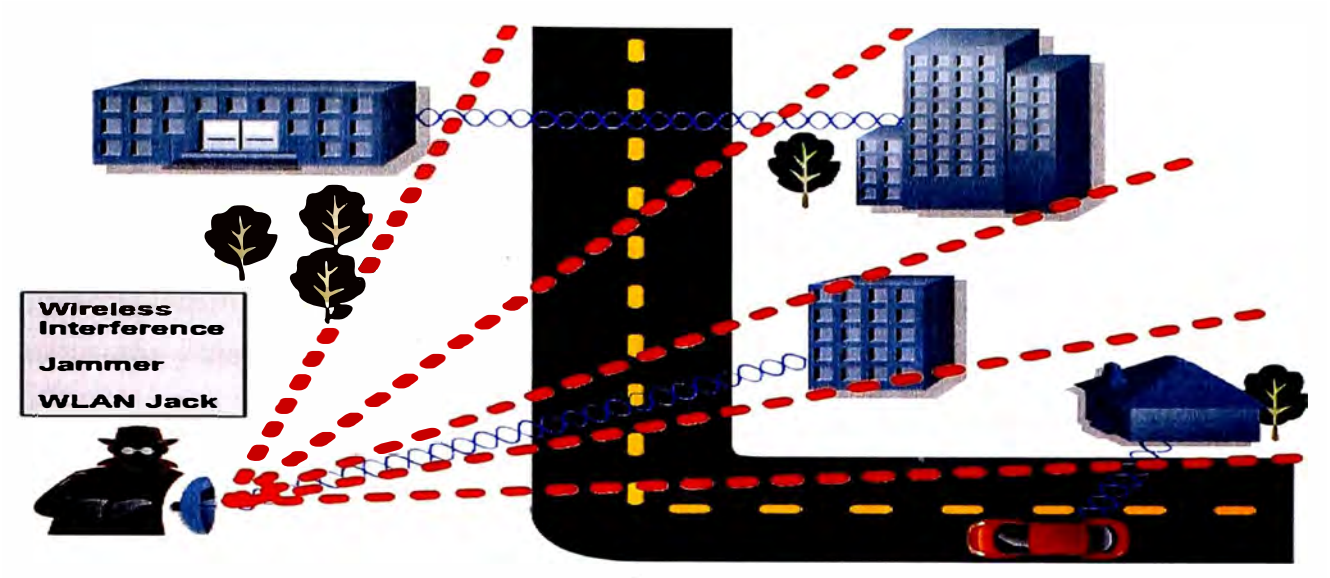

Fig. 3.1 Interferencia de Wireless

3.5 Tecnologías de Seguridad WLAN Básica

3.5.1 La rueda de la seguridad WLAN

La mayoría de los incidentes de seguridad inalámbrica ocurren porque los administradores de sistemas no implementan contramedidas. Entonces no es sólo confirmar que existe una vulnerabilidad técnica y encontrar una contramedida que funcione. También es crítico verificar que la contramedida está en su lugar y que funciona correctamente. Aquí es donde la Rueda de la Seguridad WLAN, que es un proceso de seguridad continuo, es efectiva. Porque no sólo promueve la aplicación de medidas de seguridad a la red, sino que lo más importante es que promueve el control y la aplicación de medidas de seguridad actualizadas en forma continua.

La rueda de la seguridad está conformada por las siguientes fases:

a - Aplicación e implementacion de las siguientes soluciones de seguridad:

Implementar una plataforma de Autenticación, autorización y asociación.

Instalación de Firewall

Cofiguración de redes privadas virtuales (VPNs)

Implementar la detección de intrusos

b - Monitoreo del sistema

Detectar la violación de políticas de seguridad

Detección de intrusos en tiempo real

Prueba del sistema

c - Prueba del sistema

Validar la implementacion de las políticas de seguridad a través de testeo de sistema y scaneo de vulnerabilides

d - Utililizar la información de Monitoreo y prueba del sistema para proveer la implementacion de políticas de seguridad. Así como ajustar las políticas de seguridad a los riesgos y las vulnerabilidades detectadas.

Para comenzar el proceso de la Rueda de la Seguridad, primero desarrolle una política de seguridad de WLAN que permita la aplicación de medidas de seguridad.
Una política de seguridad debe realizar las siguientes tareas:
- Identificar los objetivos de seguridad inalámbrica de la organización
- Documentar los recursos a ser protegidos
- Identificar la infraestructura de la red con los mapas e inventarios actuales

Las políticas de seguridad proporcionan muchos beneficios. Ellas valen el tiempo y el esfuerzo necesarios para desarrollarlas. El desarrollo de una buena política de seguridad logra lo siguiente:
- Proporciona un proceso para auditar la seguridad inalámbrica existente.
- Proporciona un marco de trabajo general para implementar la seguridad
- Define los comportamientos que están o no permitidos
- Ayuda a determinar cuáles herramientas y procedimientos son necesarios para la organización
- Ayuda a comunicar un consenso entre un grupo de directivos clave y define las responsabilidades de los usuarios y de los administradores
- Define un proceso para manipular violaciones inalámbricas

Una política de seguridad inalámbrica efectiva trabaja para asegurar que los recursos de la red de la organización estén protegidos contra el sabotaje y el acceso inapropiado, que incluye tanto el acceso intencional como el accidental. Todas las características de la seguridad inalámbrica deberían ser configuradas en conformidad con la política de seguridad de la organización. Si no está presente una política de seguridad, o si está desactualizada, se debería crear o actualizar antes de decidir cómo configurar o hacer uso de los dispositivos inalámbricos.

3.6 Seguridad inalámbrica de primera generación

La seguridad no era una gran preocupación para las primeras WLANs. El equipo era propietario, costoso y difícil de conseguir. Las WLANs usaban el Identificador del Conjunto de Servicio (SSID) como una forma básica de seguridad. Algunas WLANs controlaban en acceso ingresando la dirección de control de acceso al medio (MAC) de cada cliente en los access points inalámbricos. Ninguna opción era segura, ya que el sniffing inalámbrico podía revelar las direcciones MAC válidas y el SSID.

El SSID es una cadena de 1 a 32 caracteres del Código Estándar Norteamericano para el Intercambio de Información (ASCII) que puede ser ingresada en los clientes y en los access points. La mayoría de los access points tienen opciones como: SSID broadcast y permitir cualquier SSID. Estas características están normalmente activas por defecto y facilitan la configuración de una red inalámbrica, la cual permite que un cliente con un SSID en blanco acceda a un access point. El SSID broadcast envía paquetes baliza que publican el SSID. El desactivar estas dos opciones no asegura a la red, ya que un sniffer inalámbrico puede fácilmente capturar un SSID válido del tráfico normal de la WLAN. Por tanto Los SSIDs no deberían ser considerados una característica segura.

La autenticación basada en MAC no está incluida en las especificaciones del 802.11. Sin embargo, muchos fabricantes han implementado una autenticación basada en MAC. La mayoría de los fabricantes simplemente requieren que cada access point tenga una lista de direcciones MAC válidas. Algunos fabricantes también permiten que el access point consulte una lista de direcciones MAC en un servidor centralizado.

Controlar el acceso a una red inalámbrica usando direcciones MAC es tedioso. Se debe mantener un inventario preciso y los usuarios deben reportar rápidamente la pérdida o el robo de equipo. Las direcciones MAC no son un verdadero mecanismo de seguridad, ya que todas las direcciones MAC no están encriptadas cuando se transmiten. Un atacante sólo necesitaría capturar una dirección MAC válida para poder acceder a la red. En ciertos casos, la autenticación de direcciones MAC puede suplementar las características de seguridad, pero no debería ser nunca el método principal de seguridad inalámbrica.

3.7 Privacidad equivalente a la cableada (WEP)

El estándar IEEE 802.11 incluye a WEP, especificaba una clave de 40 bits, por lo que WEP podía ser exportado y usado en todo el mundo, posteriormente se extendio el WEP a 128 bits o más. Cuando se usa el WEP, tanto el cliente inalámbrico como el access point deben tener una clave WEP idéntica. WEP está basado en un tipo de encriptación existente y familiar, la Rivest Cipher 4 (RC4).
El estándar IEEE 802.11 proporciona dos esquemas para definir las claves WEP a ser usadas en una WLAN.

En el primer esquema, un conjunto de hasta cuatro claves predeterminadas son compartidas por todas las estaciones, incluyendo clientes y access points, en un subsistema inalámbrico. Cuando un cliente obtiene las claves predeterminadas, ese cliente puede comunicarse en forma segura con todas las otras estaciones en el subsistema. El problema con las claves predeterminadas es que cuando llegan a estar distribuidas extensamente, es más probable que estén en peligro. Los equipos WLAN de Cisco utiliza este primer esquema.

En el segundo esquema, cada cliente establece una relación de mapeo de clave con otra estación. Esta es una forma más segura de operación, porque menos estaciones tienen las claves. Sin embargo, la distribución de tales claves unicast se vuelve más difícil a medida que la cantidad de estaciones aumenta. La forma en que 802.11 utiliza la encriptación WEP es débil en varias formas. Han sido mejoradas con el estándar 802.11i.

3.8 Autenticación y Asociación

La Autenticación Abierta y la Autenticación de Clave Compartida son los dos métodos que define el estándar 802.11 para que los clientes se conecten a un access point. El proceso de asociación puede ser dividido en tres elementos, que son investigación, autenticación y asociación.

3.8.1 Autenticación abierta

El método de Autenticación Abierta realiza el proceso de autenticación completo en texto abierto. La Autenticación Abierta es básicamente una autenticación nula, lo que significa que no hay una verificación del usuario o de la máquina. La Autenticación Abierta está normalmente ligada a una clave WEP. Un cliente puede asociarse al access point con una clave WEP incorrecta o incluso sin una clave WEP. Un cliente con la clave WEP

incorrecta no podrá enviar o recibir datos, ya que la carga de paquetes estará encriptada. Tenga presente que el encabezado no está encriptado por el WEP. Sólo la carga o los datos están encriptados.

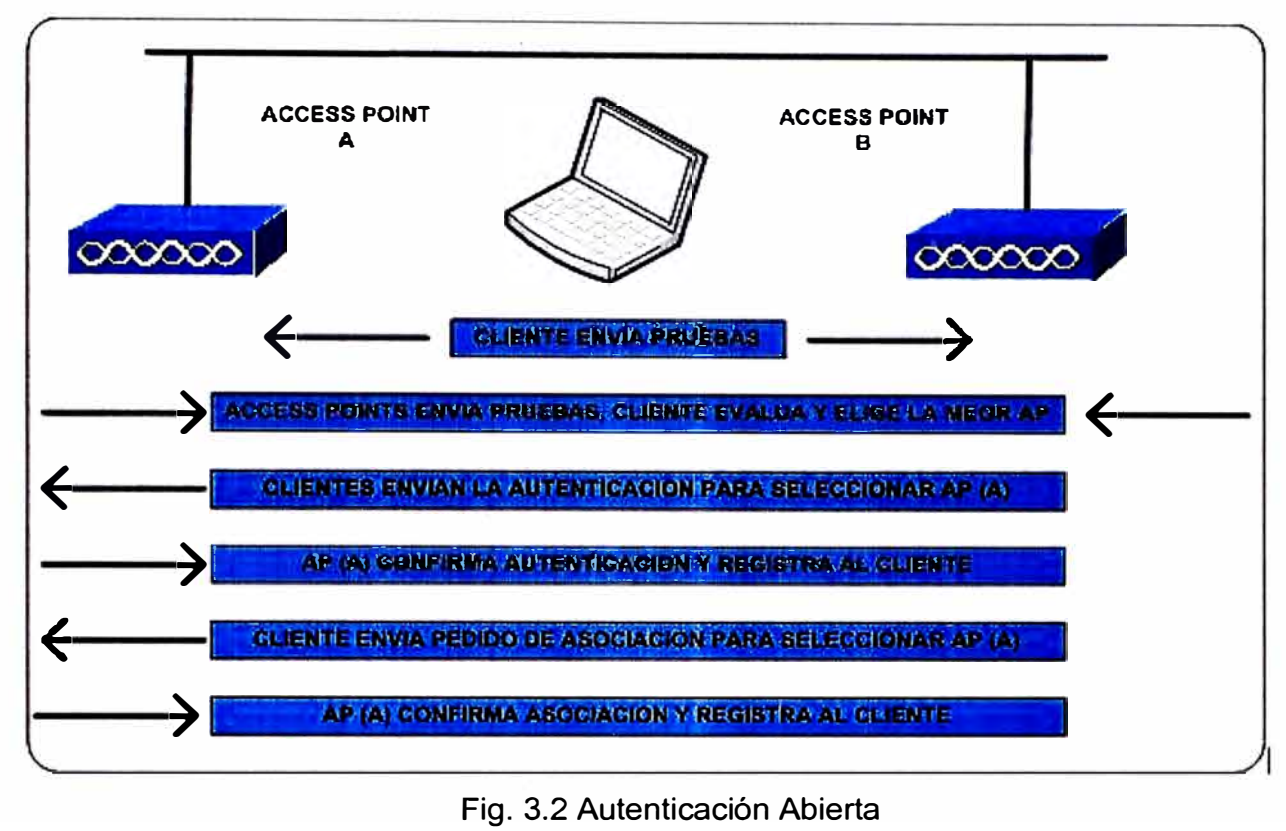

Fig. 3.2 Autenticación Abierta

3.8.2 Autenticación de Clave Compartida

La Autenticación de Clave Compartida funciona en forma similar a la Autenticación Abierta, excepto que utiliza la encriptación WEP para un paso. La clave compartida requiere que el cliente y el access point tengan la misma clave WEP. Un access point que usa la Autenticación de Clave Compartida envía un paquete de texto de desafío al cliente. Si el cliente tiene la clave equivocada o no tiene clave, fallará en esta parte del proceso de autenticación. El cliente no tendrá permitido asociarse al AP. La clave compartida es vulnerable a un ataque por desconocidos, por lo que no es recomendada.

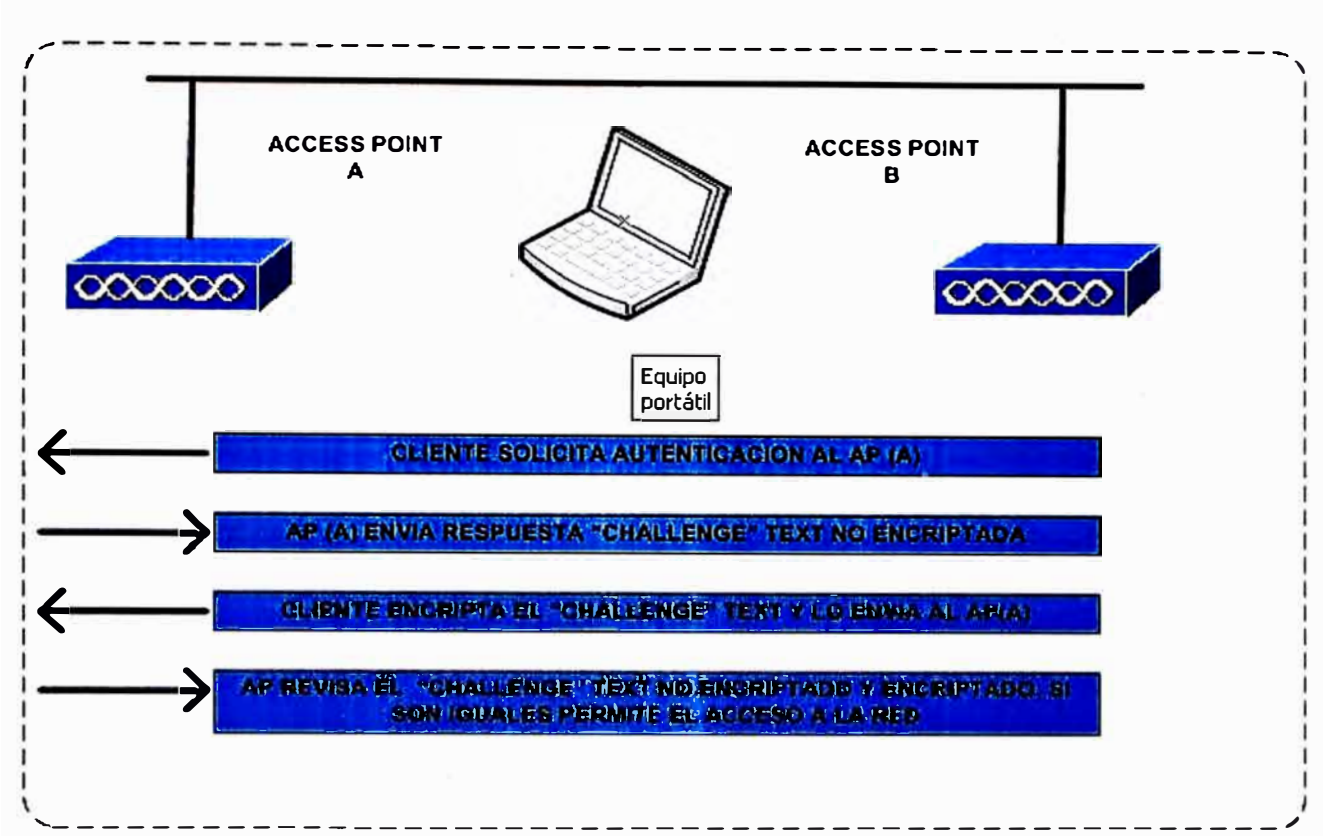

Fig. 3.3 Autenticacion share WEP

Interoperabilidad

En la mayoría de los access points, incluyendo los de Cisco, es posible usar la Autenticación Abierta con o sin una clave WEP. Para una interoperabilidad básica que requiera WEP. La Encriptación de Datos es fijada, y TKIP, MIC, y BKR están todos desactivados.

3.9 Configuración de Seguridad WLAN Básica

3.9.1 Seguridad WLAN Básica

El equipo de red ofrece muchos protocolos adicionales, lo que simplifica la administración de la red y el acceso de los usuarios. Dependiendo de la configuración de la red, sólo algunos de estos protocolos pueden ser necesarios. Si un protocolo es necesario, es importante comprender sus debilidades y cómo puede ser asegurado.

- Acceso Físico

La mayoría de los access points son fácilmente accesibles. Normalmente están ubicados cerca de los usuarios y fuera de habitaciones cerradas. Esto pone a los access points en

peligro de ser robados y al alcance de usuarios malintencionados. Se puede usar la supervisión de la red para determinar cuándo un access point se desactiva. Casi todos los fabricantes de tecnología inalámbrica publican los métodos para reconfigurar un access point usando botones de reset o el puerto consola.

- Firmware

El firmware deberá estar actualizado, ser probado y usado. Se deberán aplicar parches de seguridad o actualizaciones cuando se justifique.

- Acceso por Consola

Las cuentas y los privilegios del administrador deberán estar configurados correctamente El puerto consola debería estar protegido por una password.

- Telnet/SSH

Telnet es un protocolo no encriptado e inseguro. Implemente un Shell seguro (SSH) para todas las funciones de la Interfaz de Línea de Comando (CLI). y desactive el Telnet

- TFTP/FTP

El Protocolo de Transferencia Trivial de Archivos (TFTP) y el Protocolo de Transferencia de Archivos (FTP) son usados para enviar y recibir archivos a través de una red. TFTP no permite que se utilicen passwords, y está limitado a archivos menores a 16 Mb. FTP permite nombres de usuario y passwords, pero aun es un protocolo no encriptado.

- SSID

El SSID no debería ser considerado como una característica de seguridad. Los SSIDs pueden ser usados en conjunto con las VLANs para permitir el acceso limitado a invitados.

3.9.2 Activación de filtros de protocolo y de MAC en APs

El filtrado puede proporcionar una capa adicional de seguridad inalámbrica,los filtros de protocolos evitan o permiten el uso de protocolos específicos a través del access point. Por ejemplo, un filtro SNMP en el puerto de radio del access point evita que los dispositivos clientes inalámbricos usen SNMP con el access point pero no bloquea el acceso de SNMP desde la LAN cableada.

3.9.3 Seguridad en clientes y APs

La seguridad del cliente es importante, después de que estén protegidas las debilidades de los access points, el ataque a los clientes se convierte en la forma más fácil de obtener acceso a la red. La seguridad apropiada para los clientes debería ser especificada en la política de seguridad inalámbrica. Esto incluye medidas de seguridad como búsqueda de virus, firewalls personales y mantener a los programas clientes y a los sistemas operativos actualizados.

Puede ser deseable el tener seguridad adicional para clientes inalámbricos. Por ejemplo, WEP debería ser activado cuando sea posible. La WEP estática tiene debilidades. Características de seguridad adicionales, como la clave por paquete de protocolo de integridad de clave temporal (TKIP) y el Control de Integridad de Mensajes (MIC), necesitan estar activas para la seguridad adicional.

3.9.4 Supervisión del equipo WLAN

El registro de eventos a través de SNMP o Syslog es muy importante en el proceso de seguridad general. los niveles de notificación de eventos pueden ser definidos para SNMP y Syslog. Debe estar definido un servidor Syslog para que se puedan enviar mensajes Syslog a un servidor de supervisión central.

Protocolo Simple de Administración de Red (SNMP)

SNMP permite que los programas de administración de red vean y cambien configuraciones de equipos. SNMP puede ser usado para ver configuraciones utilizando el pedido Get SNMP también puede ser usado para cambiar las configuraciones usando un pedido Set. Finalmente, los dispositivos SNMP pueden enviar alertas a las estaciones de administración usando la función Trap. SNMP utiliza un secreto no encriptado llamado cadena o nombre de comunidad. Los nombres de comunidad de sólo lectura sólo permiten pedidos Get, mientras que los nombres de comunidad de lectura y escritura permiten pedidos Get y Set. Las versiones 1 y 2 de SNMP son inseguras, porque el nombre de comunidad puede ser visto en los pedidos. La versión 3 de SNMP agrega seguridad adecuada, pero aun no está ampliamente usada o soportada. No utilice public o private como nombres de comunidad porque son los predeterminados. Utilice un nombre de comunidad.

3.9.5 Desactivación de servicios no necesarios

Es importante desactivar o asegurar todos los servicios no necesarios. Por ejemplo, si el protocolo de descubrimiento de Cisco (CDP) , el servicio de nombre de dominio (DNS), el protocolo de tiempo de la red (NTP), el protocolo de transferencia de hipertexto (HTTP) , TFTP, SNMP y Telnet no son usados en la red, deberían ser desactivados

3.10 Autenticación WLAN Empresarial

3.10.1 Autenticación de segunda generación

La verdadera seguridad inalámbrica requiere más que sólo hacer dinámicas las claves WEP o mejorar el WEP. Asi tambien debe poder autenticar a los usuarios, no sólo a los dispositivos.

Las organizaciones deben decidir cuánta seguridad necesitan e incluirla en la política de seguridad inalámbrica. Algunas redes implementarán el control de acceso y los arreglos para WEP, que están incluidos en el Acceso Protegido Wi-Fi (WPA). WPA utiliza elementos de 802.11i, una solución de seguridad estandarizada de más largo plazo, para asegurar las WLANs. WPA también es llamado Networking de Seguridad Simple (SSN).

3.10.2 Autenticación de usuarios inalámbricos

Una limitación de una WLAN con sólo WEP es que los usuarios no se autentican. WPA permite la autenticación de usuarios a través del protocolo IEEE 802.1x. El cual es un estándar que permite controlar la entrada a las LANs cableadas e inalámbricas. 802.1x proporciona autenticación mutua. La autenticación mutua significa que la red y el usuario se intercambian las identidades,

El estándar 802.11i también utiliza 802.1x y las mejoras TKIP para WEP. Una ventaja del estándar 802.1x es que puede soportar una variedad de tipos de autenticación. Un access point que soporta 802.1x y a su protocolo, el Protocolo de Autenticación Extensible (EAP), actúa como la interfaz entre un cliente inalámbrico y un servidor de autenticación como el servidor de Servicio al Usuario de Acceso Telefónico Remoto (RADIUS). El access point se comunica con el servidor RADIUS a través de la red cableada.

3.10.3 Fundamentos de 802.1X

802.1x requiere soporte en el cliente, en el access point y en el servidor de autenticación, ver figura 3.4. 802.1X utiliza un proxy RADIUS para autenticar a los clientes en la red.

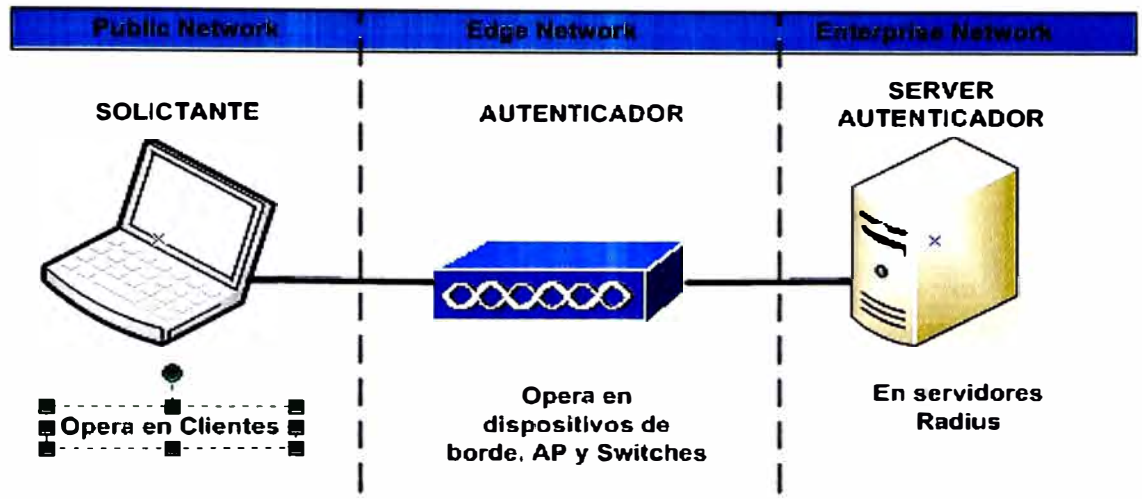

Fig. 3.4 Equipos involucrados en 802.1X

El cliente o solicitante EAP envía las credenciales de autenticación al autenticador el que a su vez envía la información al servidor de autenticación, donde el pedido de ingreso es comparado con una base de datos de usuarios para determinar si el usuario puede obtener acceso a los recursos de la red, y a qué nivel.

El access point recibe el nombre de autenticador. El servidor de autenticación es normalmente un RADIUS o un servidor de autenticación, autorización y asociacion (AAA). El servidor de autenticación necesita ejecutar un software extra para comprender el tipo de autenticación que está usando el cliente.

Cualquier cliente que no tiene incorporado el 802.1x debe usar un software llamado solicitante, los S.O. Windows 2000 , XP tiene incorporado el EAP que proporciona soporte a 802.1x. Al igual que el cliente Cisco LEAP. El cliente debe tener alguna prueba de su identidad. Las formas de identidad incluyen un nombre de usuario, password y certificación digital algunas veces.

3.10.4 Funcionamiento del 802.1X

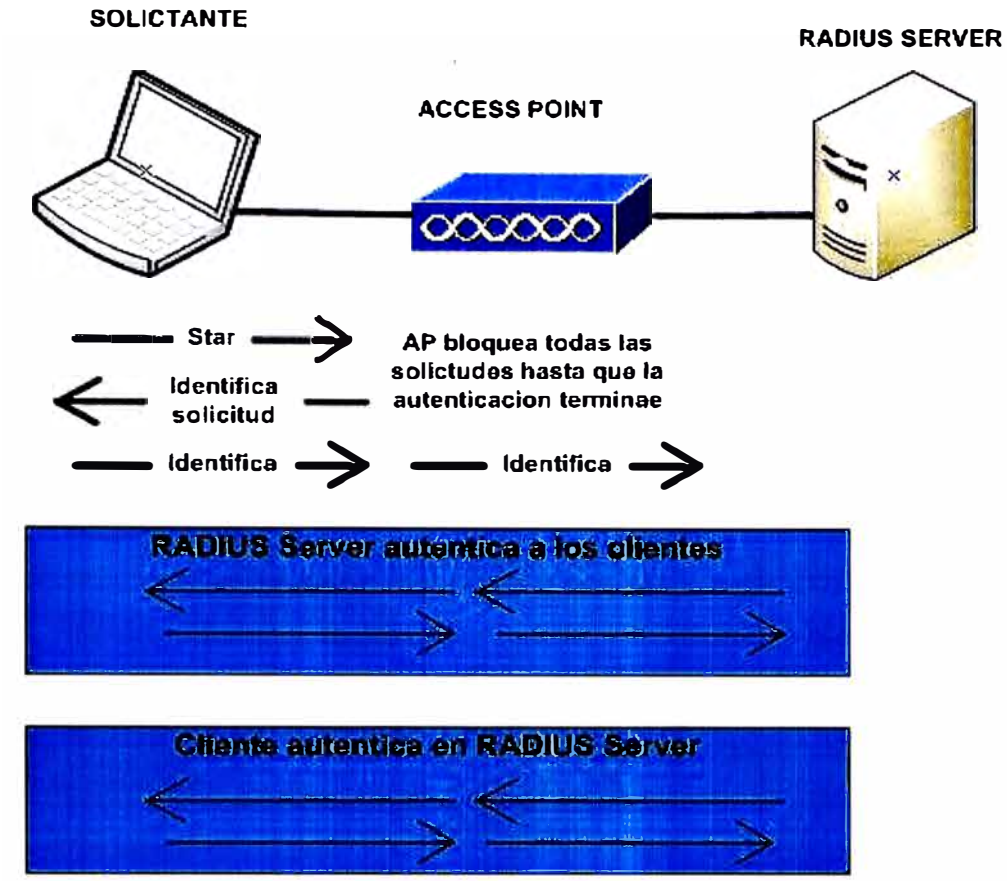

Fig. 3.5 Funcionamiento del protocolo 802.1X

La Figura proporciona una descripción general de la forma en que trabaja el 802.1x. Después de que el cliente se ha asociado al access point, el solicitante comienza el proceso para usar EAPOL (EAP sobre LAN) pidiéndole al usuario su nombre y password.
El cliente responde con su nombre de usuario y password. Usando 802.1X y EAP el solicitante luego envía el nombre de usuario y un hash de un sentido de la password al access point. El access point luego encapsula el pedido y lo envía al servidor RADIUS.
El servidor RADIUS luego compara el nombre de usuario y la password con la base de datos para determinar si el cliente debería ser autenticado en la red. Si el cliente debe ser autenticado, el servidor RADIUS emite luego un desafío de acceso, que es pasado al access point y después enviado al cliente.
El cliente envía la respuesta EAP para el desafío de acceso al servidor RADIUS a través del access point.
Si el cliente envía la respuesta correcta entonces el servidor RADIUS envía un mensaje de acceso exitoso y una clave WEP (EAP sobre Inalámbrico) al cliente a través del

access point. La misma clave WEP de sesión también es enviada al access point en un paquete exitoso.

El cliente y el access point luego comienzan a usar las claves WEP de sesión. La clave WEP usada para multicast es luego enviada desde el access point hacia el cliente. Es encriptada usando la clave WEP de sesión.

Ante la desconexión del cliente, el access point vuelve al estado inicial, permitiendo que sólo pase tráfico 802.1X.

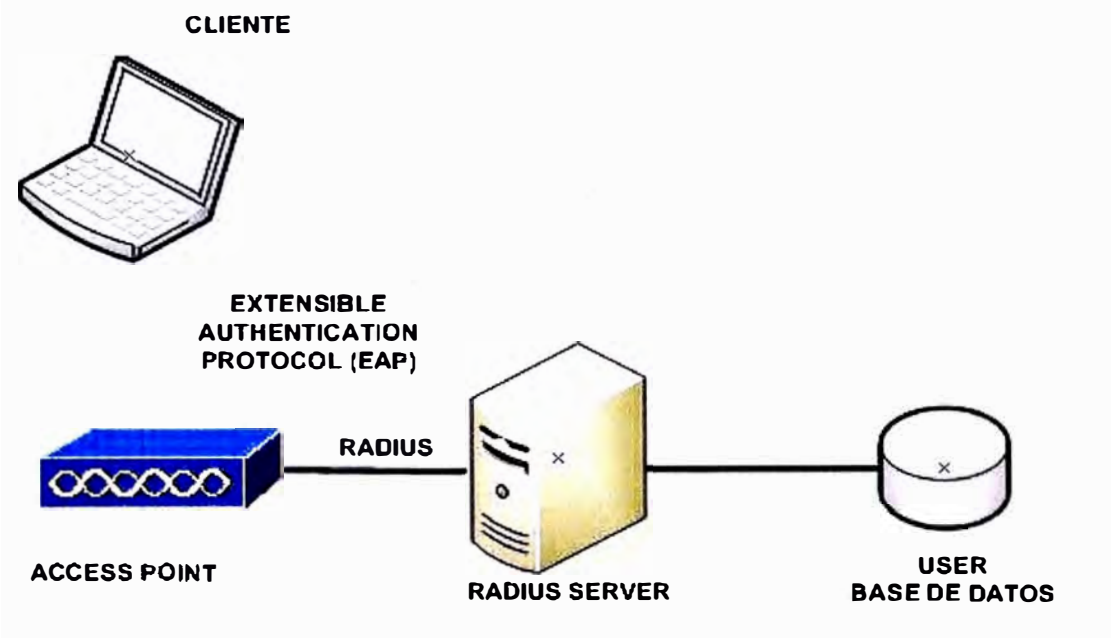

Fig. 3.6 Proceso de autenticación general 802.1X

3.10.5 Tipos de autenticación de 802.1x

Cuando se utiliza 802.1x sobre una WLAN están soportados diferentes tipos de autenticaciones.

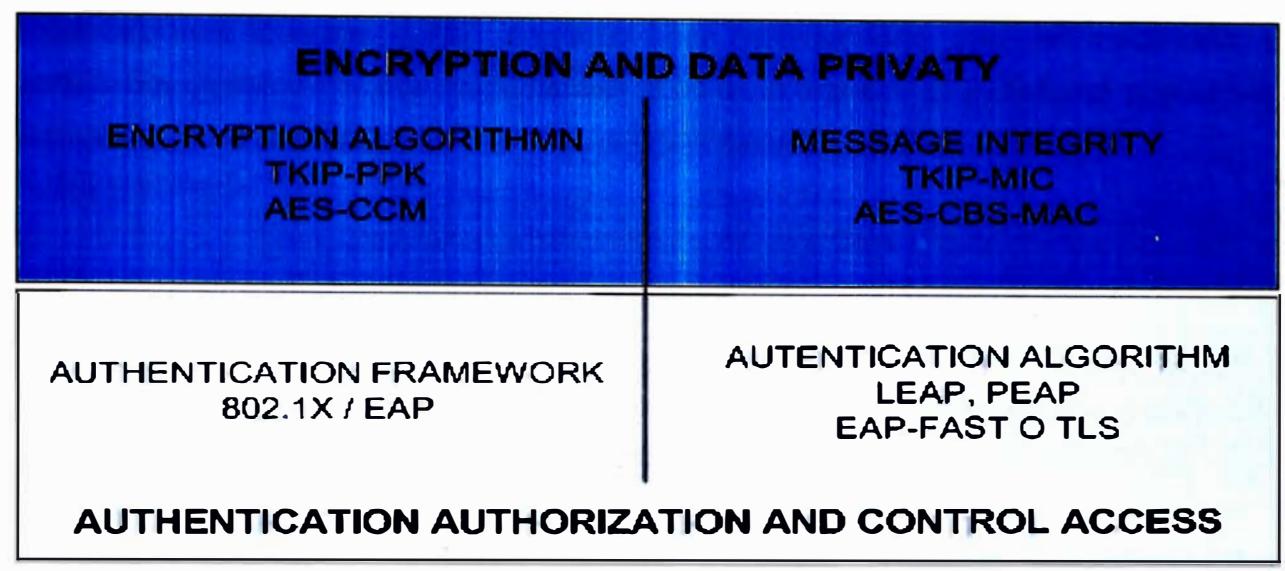

Fig. 3.7 Tipos principales de autenticación 802.1X

LEAP - Lightweight EAP (LEAP) es también llamado EAP-Cisco. LEAP es la versión de Cisco de EAP. Es para usar sobre redes que actualmente no soportan EAP. Las versiones actuales de EAP pueden no proporcionar la funcionalidad que se necesita y pueden ser demasiado exigentes. Esto podría comprometer el rendimiento del equipo WLAN. LEAP es una buena opción cuando se utiliza equipo Cisco junto con sistemas operativos como Windows 95, Windows 98, Windows Me, Windows CE, Windows NT/2000/XP y Linux.

EAP-TLS - La EAP-Seguridad de Capa de Transporte (EAP-TLS), es una opción de seguridad de trabajo intensivo. EAP-TLS requiere que haya un certificado digital configurado en todos los Clientes WLAN y en el Servidor. EAP-TLS está basado en certificados 509X. Normalmente es más fácil de usar que PEAP, que está basado en EAP-TLS.

PEAP - EAP Protegido (PEAP) es un tipo de autenticación EAP borrador que está diseñado para permitir la autenticación híbrida. PEAP emplea la autenticación PKI del lado del servidor. Para la autenticación del lado del cliente, PEAP puede usar cualquier otro tipo de autenticación EAP. Como PEAP establece un túnel seguro por medio de la autenticación del lado del servidor, se pueden usar tipos de EAP no mutuamente

autenticables para la autenticación del lado del cliente. Las opciones de autenticación del lado del cliente incluyen EAP-GTC para passwords ocasionales y EAP-MD5 para autenticación basada en password. PEAP está basado en EAP-TLS del lado del servidor y soluciona los defectos de administrabilidad y escalabilidad de EAP-TLS. Las organizaciones pueden evitar los problemas relacionados con la instalación de certificados digitales en cada máquina cliente como lo requiere EAP-TLS. Se puede elegir el metodo de autenticación del cliente más conveniente.

EAP-MD5 - El Protocolo de Autenticación Expandible MD5 (EAP-MD5) no debería ser usado, porque no proporciona autenticación mutua. EAP-MD5 es una autenticación de un sentido que esencialmente duplica la protección de password CHAP en una WLAN. EAP-MD5 se utiliza como un bloque de construcción en EAP-TTLS.

EAP-OTP - EAP-Passwords Ocasionales (EAP-OTP) también recibe el nombre de EAP-Tarjeta Token Genérica [EAP- Generic Token Card (EAP-GTC)]. No es recomendable, ya que las OTPs no son una forma de autenticación mutua.

EAP-SIM - EAP-SIM utiliza la misma tarjeta inteligente o SIM que se utiliza en los teléfonos móviles GSM para proporcionar autenticación. EAP-SIM puede fácilmente montarse sobre EAP-TLS.

EAP-TTLS - EAP-Seguridad de Capa de Transporte en Túnel (EAP-TTLS) provee una funcionalidad similar a PEAP. EAP-TTLS protege las passwords usando TLS, que es una forma avanzada de Capa de Socket Seguro (SSL). EAP-TTLS actualmente requiere un servidor RADIUS de Funk software.

Kerberos - Kerberos no es parte del estándar 802.1x, sino que está siendo promocionado por algunos fabricantes. Kerberos es un sistema de autenticación que permite la comunicación protegida sobre una red abierta, que utiliza una clave única llamada ticket. Requiere configuración del servicio. PEAP puede soportar Kerberos a través del EAP-Servicio de Seguridad Genérico (EAP-GSS).

3.10.5 Elección de un tipo de 802.1X

Es importante elegir un tipo de 802.1x que sea lo más compatible con la red existente. Los métodos disponibles son LEAP, EAP y PEAP. 802.1x no especifica el tipo de autenticación a usar.
Las consideraciones principales a tener en cuenta cuando se elige un tipo de autenticación son la integración sencilla y la seguridad adecuada.
Antes considerar antes de utilizar una seguridad basada en 802.1x:
Elija un método que se integre bien con la red existente.
Elija un método que soporte la autenticación mutua.
Revise la política de seguridad y averigüe cuáles tipos de 802.1x son compatibles.
Finalmente, vea que los clientes estén protegidos y elija la mejor forma de asegurar al equipo existente.

LEAP proporciona una solución WLAN completa. LEAP debería utilizarse cuando se necesita un inicio de sesión único al dominio de Windows o cuando se necesita un Active Directory. El Active Directory permite que las organizaciones administren y compartan información sobre los recursos y usuarios de la red en forma centralizada mientras que actúa como la autoridad central para la seguridad de la red.
LEAP también puede ser usado cuando se necesita una clave WEP dinámica y autenticación mutua.

EAP debería ser usado cuando se necesita utilizar certificados digitales para la identificación de los usuarios. EAP es la mejor solución cuando hay una Infraestructura de Clave Pública (PKI) existente en el lugar. PKI asegura que las comunicaciones electrónicas sensibles sean privadas y estén protegidas contra la manipulación. Proporciona garantías en las identidades de los participantes en esas transacciones, y evita su rechazo posterior en la participación en la transacción.

EAP-TLS también puede ser usado para vincular el ingreso con el NT/2000 y el Protocolo Liviano de Acceso a Directorios (LDAP) LDAP le permite usar servicios de directorio para integrar un cliente de Registro de Red e información de arrendamiento. Al construir el esquema de estándares existentes para objetos almacenados en directorios LDAP, puede manipular la información sobre entradas de clientes del protocolo de configuración dinámica de hosts (DHCP). Así, en lugar de mantener la información de los clientes en la base de datos del servidor DHCP, puede pedir que el servidor DHCP de Registro de Red

envíe consultas a uno o más servidores LDAP para obtener información en respuesta a las peticiones del cliente DHCP.

PEAP puede ser usado cuando la clave WEP y la autenticación mutua son necesarios. Recuerde que debería utilizarse el TKIP para asegurar el LEAP

3.11 Encriptación Inalámbrica Empresarial

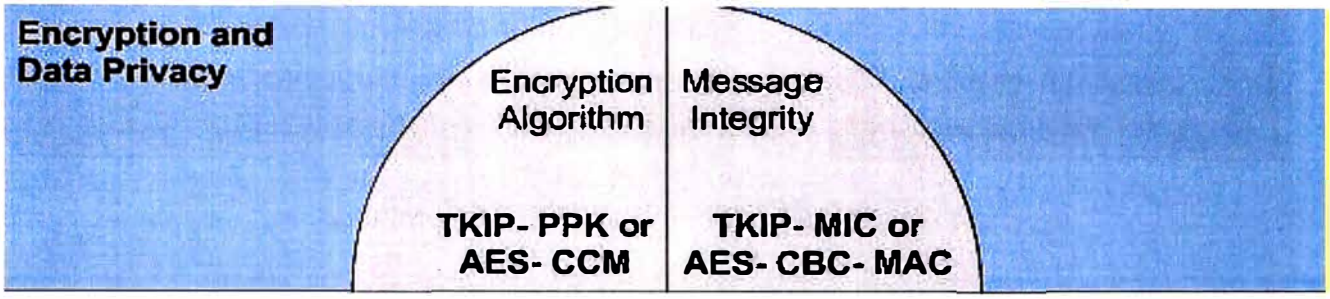

Fig. 3.8 Privacidad y encriptación de los datos

3.11.1 Fortalecimiento WEP

WPA incluye mecanismos del estándar emergente 802.11i para mejorar la encriptación de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente. Estas tecnologías son fácilmente implementadas usando la interfaz gráfica de usuario (GUI) del AP de Cisco.

TKIP es también llamado hashing de Clave WEP y recibió inicialmente el nombre WEP2. TKIP es una solución temporal que soluciona el problema de reutilización de clave de WEP, Figura 3.9

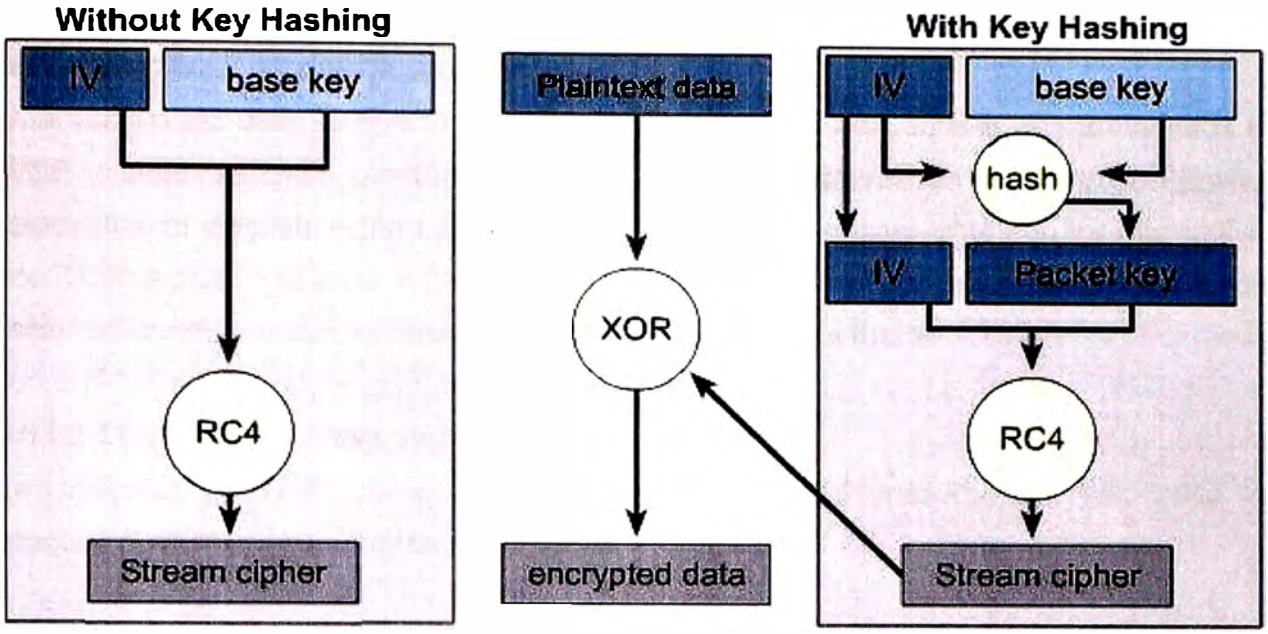

Fig. 3.9 Proceso de encriptación WEP

WEP utiliza periódicamente la misma clave para encriptar los datos. El proceso de TKIP comienza con una clave temporal de 128 bits que es compartida entre los clientes y los access points. TKIP combina la clave temporal con la dirección MAC del cliente. Luego agrega un vector de inicialización relativamente largo, de 16 octetos, para producir la clave que encriptará a los datos. Ver figura

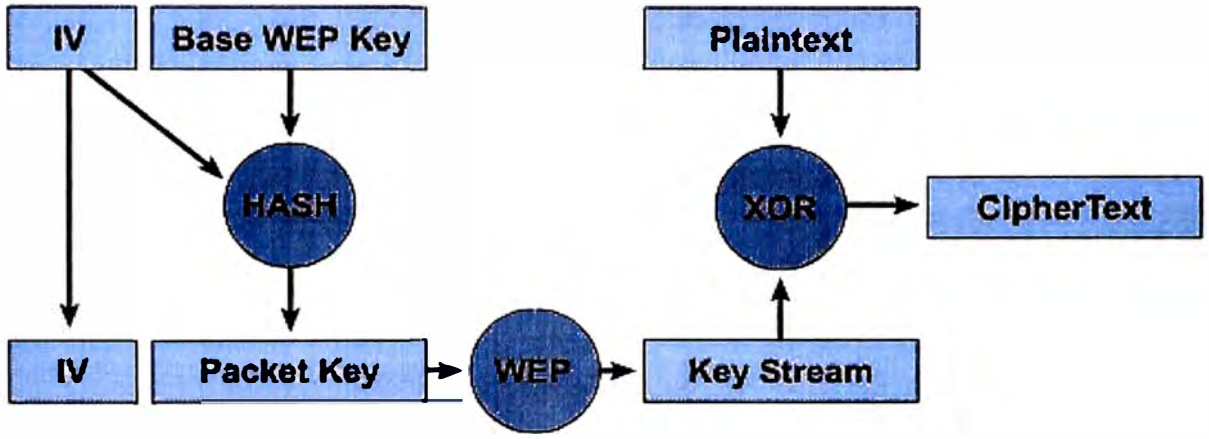

Fig. 3.10 Proceso de encriptación WEP

Este procedimiento asegura que cada estación utilice diferentes streams claves para encriptar los datos. El hashing de clave WEP protege a los Vectores de Inicialización (IVs) débiles para que no sean expuestos haciendo hashing del IV por cada paquete.

TKIP utiliza el RC4 para realizar la encriptación, que es lo mismo que el WEP. Sin embargo, una gran diferencia con el WEP es que el TKIP cambia las claves temporales

cada 10.000 paquetes. Esto proporciona un método de distribución dinámico, lo que mejora significativamente la seguridad de la red.

Una ventaja de usar TKIP es que las compañías que tienen access points basados en WEP y NICs de radio pueden actualizarse a TKIP a través de patches de firmware relativamente simples. Además, el equipo sólo WEP aún interoperará con los dispositivos con TKIP activado usando WEP. TKIP es sólo una solución temporal. La mayoría de los expertos creen que aun es necesaria una encriptación más fuerte.

3.11.2 Control de la integridad de los mensajes

Las mejoras de TKIP, como MIC, proveen claves WEP más fuertes. MIC evita los ataques de bit-flip en paquetes encriptados. Ver figura

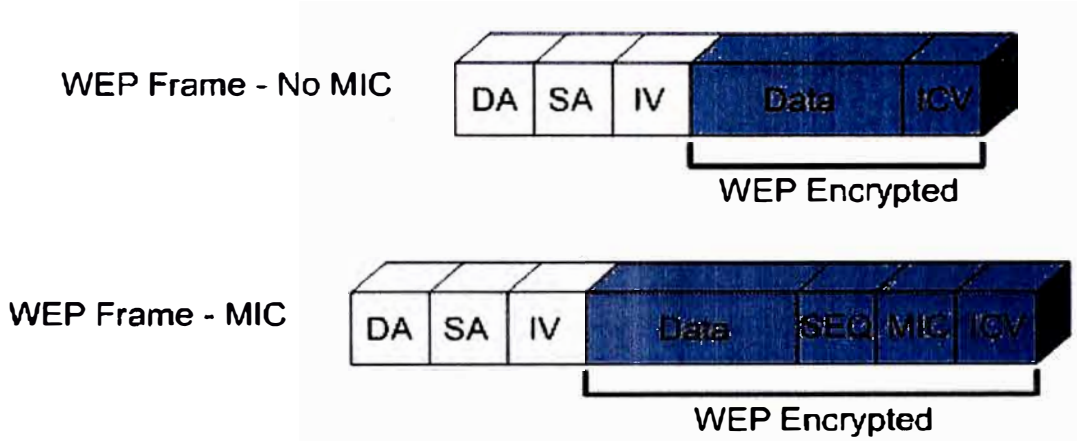

Fig. 3.11 Control de integridad de mensajes MIC

Durante un ataque bit-flip, un intruso intercepta un mensaje encriptado, lo altera levemente y lo retransmite. El receptor acepta el mensaje retransmitido como legítimo. El controlador y el firmware del adaptador cliente deben soportar la funcionalidad del MIC, y MIC debe estar activo en el access point. Las mejoras de TKIP, como MIC y hashing de Clave WEP pueden ser activados usando claves WEP estáticas. No necesitan un servidor RADIUS para funcionar.

3.11.3 Rotación de clave de broadcast - BKR

La característica Rotación de Clave de Broadcast (BKR), es también una mejora de TKIP. BKR protege al tráfico multicast del access point para que no sea explotado cambiando dinámicamente la clave de encriptación.

El access point genera claves WEP de broadcast usando un generador de números pseudo aleatorios (PRNG) sembrados. El access point rota la clave de broadcast después de que se agota un temporizador configurado de clave WEP de broadcast. Este proceso por lo general debería estar en sincronía con los tiempos vencidos configurados en los servidores RADIUS para la re-autenticación de los usuarios.
Se recomienda que la rotación de clave de broadcast esté activa cuando el access point sirve a una LAN inalámbrica exclusiva de 802.1x. No es necesario activar la rotación de clave de broadcast si el hashing de clave WEP está activado. El uso de la rotación de clave y de hashing de clave provee de protección innecesaria. Cuando la rotación de clave de broadcast está activada, sólo pueden usar el access point los dispositivos clientes inalámbricos que usan autenticación LEAP o EAP-TLS. Los dispositivos clientes que usan WEP estática con clave abierta compartida o autenticación EAP-MD5 no pueden usar el access point cuando la rotación de clave de broadcast está activada.

3.11.4 Encriptación de segunda generación

Además de la solución TKIP, el estándar 802.11i es muy probable que incluya al protocolo Estándar Avanzado de Encriptación (AES) AES ofrece una encriptación mucho más fuerte. Con el inconveniente que requiere un coprocesador o un hardware adicional para funcionar. Esto significa que las compañías necesitan reemplazar los access points y las NICs clientes existentes para implementar AES.
AES especifica tres tamaños de claves, que son 128, 192 y 256 bits. Utiliza el Algoritmo Rijndael.

3.11.5 Uso de VPNs

La Seguridad IP (IPSec) es un marco de trabajo de estándares abiertos para asegurar la comunicación privada segura sobre redes IPs. Las Redes Privadas Virtuales (VPNs) IPSec utilizan los servicios definidos dentro de IPSec para asegurar la confidencialidad, la integridad y la autenticidad de las comunicaciones de datos a través de redes como la Internet.

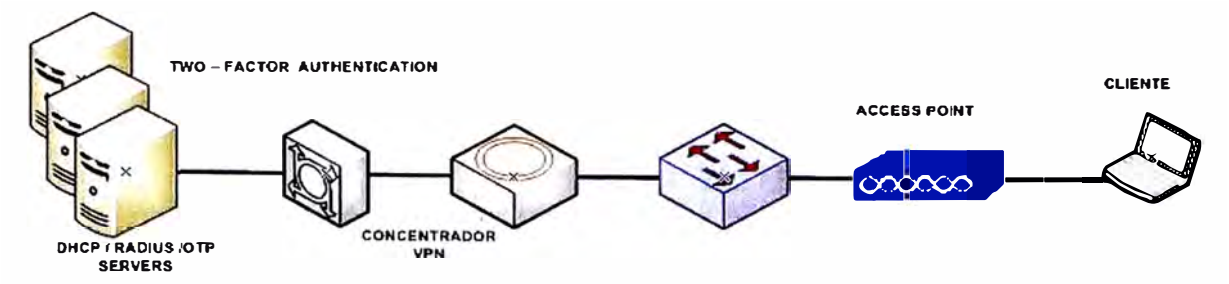

Fig. 3.12 Implementacion VPN

IPSec también tiene una aplicación práctica para asegurar las WLANs. Logra esto superponiendo IPSec por sobre el tráfico inalámbrico de 802.11.

Cuando se implementa IPSec en un entorno WLAN, se coloca un cliente IPSec en cada PC conectada a la red inalámbrica.

Se necesita que el usuario establezca un túnel IPSec y que enrute todo el tráfico hacia la red cableada, como lo muestra la Figura Se colocan filtros para evitar que el tráfico inalámbrico llegue a cualquier destino que no sea el concentrador VPN y el servidor DHCP/DNS. Los clientes VPN también pueden ser terminados sobre un router IOS Firewall o un Aparato de Seguridad PIX.

IPSec proporciona confidencialidad al tráfico IP. También tiene capacidades de autenticación y anti-respuesta usando el Resumen de Mensajes 5 (MD5) o el Algoritmo Hash Seguro [Secure Hash Algorithm (SHA)]. La confidencialidad se logra a través de la encriptación, que utiliza el Estándar de Encriptación de Datos (DES), el Triple DES (3DES) o el AES.

Fig. 3.13 Proceso de utilizar VPN sobre WLAN

El filtrado puede proporcionar una capa adicional de seguridad inalámbrica. Los filtros pueden ser creados para filtrar un Protocolo o un puerto IP. Cuando un access point está diseñado para utilizarse sólo en VPN, se pueden usar filtros para permitir sólo tráfico específico como la Carga de Seguridad Encapsulada (ESP) y el Intercambio de Clave de Internet [Internet Key Exchange (IKE)], que son necesarios para asegurar la comunicación VPN.

CAPITULO IV

IMPLEMENTACION DE RED LAN Y WIRELESS DE INKIA

Se describe la solución que fue implementada y los servicios de soporte proveídos por Orange Business Services para la solución del servicio acordado. El objetivo es proveer el proceso que debe seguirse para el soporte específico de la solución implementada por Orange Business Services para el cliente Inkia.
El presente documento incluye información relacionada a la gestión de fallas y operación proveída por Orange Business Services.

Asimismo, recoge los detalles técnicos de los equipos instalados y de la implementación y configuración de la red Wireless y LAN Switching de Inkia. Y define la línea base de operación y el tipo de seguridad implementado por orange de acuerdo al solicitado por el cliente. Orange Business Services, en base a la documentación anexada en el presente documento, cierra el proyecto de implementación instalación y configuración de los equipos adquiridos.

4. 1 Evaluación de Site Survey

Orange en base a reuniones sostenidas con el cliente, recoge información técnica relevante sobre aspectos físicos y lógicos de la red actual de Inkia. Toda la información recogida y analizada es con propósitos únicos de la implementación, no constituye un análisis de configuraciones, de topologías y de funcionamiento.

Los puntos de análisis de Orange Business están divididos según:

- Evaluación de la infraestructura física.
- Evaluación de la solución actual de LAN, WLAN Switching.
- Evaluación de protocolos LAN y WAN.
- Evaluación del direccionamiento IP.
- Evaluación de la configuración de VLANs.
- Evaluación de la seguridad de red.
- Evaluación de los clientes Wireless.
- Evaluación de la infraestructura Wireless.
- Evaluación de la seguridad Wireless.

4.1.1 Evaluación de la infraestructura física.

a.- Información de sitio
Información de contacto y administrador de red.

b.- Información de facilidades de sitio
Las áreas físicas donde trabajar son los pisos 11 y 13 de la Torre real 5 (según lo especificado en información de sitio) en cada piso, De acuerdo a la información la existencia de un cuarto de comunicaciones adecuado para el trabajo, el desplazamiento del personal y acceso a áreas involucradas son irrestrictas, dentro de los horarios programados de trabajo.

Todas las coordinaciones se efectúan con las personas indicadas en Información de contacto y administrador de red.

El cuarto de comunicaciones cuenta con fuentes de energía, estabilizadas y protegidas de corriente alterna a 220V y con la potencia proveída de manera adecuada.
Distancia de proximidad de las tomas de tensión de 2m aproximadamente con respecto a la ubicación de los equipos, No se utilizan equipos de conexión directa DC.

Las tomas de tensión poseen puntos a tierra así mismo la toma de tierra tiene los ohm adecuados para la operación de los equipos.

Disponibilidad de espacio físico dentro del rack de comunicaciones para la instalación y rackeo de los equipos en cada una de las áreas involucradas,

El cableado estructurado tanto horizontal y vertical, cumplan las normas establecidas, y su certificación de categoría 6 brindada por el cliente.

La asignación de puertos, patchcords, concernientes al cableado estructurado son brindadas por el cliente.

Información de equipos existentes
Infraestructura de LAN, WLAN:
Piso 13:

01 SWITHC 3COM	01 SWITHC DLINK	02 AP DLINK	01 SWITHC ALCATEL

Piso 11:
Sin infraestructura de red aun.

4.1.2 Evaluación de la situación actual de LAN Switching

El diseño de la red sigue un esquema plano de funcionamiento, con un nivel mínimo de jerarquía que es punto de agregación de los switches de acceso.
No existe un esquema VLANs, todo bajo un ambiente Mult.-vendor.

Los equipos de LAN que se mantendrán se encuentran operativos y se mantendrá instalados, están con los recursos de hardware y software adecuados.

Los switches existentes, trabajan con todos los requerimientos de implementación y seguridad, soportan los protocolos, 802.1Q, 802.1, QoS (802.1p), la configuración está a cargo del cliente

4.1.3 Evaluación de protocolos LAN y WAN.

Para propósitos de esta implementación e instalación solo protocolos LAN son cubiertos, el único protocolo soportado por la implementación es IP. No está soportado, protocolos tales como: Token Ring, IPX, DECNet entre otros.

4.1.4 Evaluación del direccionamiento IP

La organización tiene un direccionamiento ya definido tanto para la redes de voz y datos. En ambos casos la cantidad de direcciones IPs es brindada por el cliente y es suficiente para el crecimiento futuro.

Los equipos IP Phone que manejan doble VLAN una de voz y otra de dato. Debido a que las redes de Voz y Datos están separadas por Switches físicamente distintos.

4.1.5 Evaluación de la configuración de VLANs

Actualmente la red tiene un diseño plano, no existe VLANs. Entonces Se verifica que todos los switches soportan VLANs y trunking en el estándar 802.1Q. Las VLANs se extenderán por toda la LAN cableada e inalámbrica, es decir cada Switch deberá ser capaz de conmutar tráfico de cualquier otra VLAN existente.

Los switches existentes soportan 802.1D Spanning tree protocolo como mínino. Por ser un ambiente multi-vendor No se garantiza la operación de features como RSTP, MST, VLAN load balancing, y otros propietarios de Cisco.

4.1.6 Evaluación de la seguridad de red.

Red alámbrica
Asignación dinámica de IPs DHCP
Sin mecanismos de autenticación para acceso físico (802.1x)
Llaves WEP como método de Autenticación/encriptación.

Los equipos de LAN y Wireless están protegidos con passwords en diferentes modos de privilegios de manera local. No hay servidores de autenticación autenticación, autorización y Asociación (AAA) como mecanismo de seguridad para acceso a los equipos.

4.1.7 Evaluación de los clientes Wireless

El promedio de la cantidad de usuarios inalámbricos de la red son 30. Todos pueden conectarse simultáneamente. Esencialmente son Laptops y/o PCs. No hay PDAs, no RF Bar Codes, no IP Phones Wireless, no dispositivos RFID.

Las laptops usan las tarjetas inalámbricas internas con suplicantes (Software en el cliente, que se encarga de la conexión a la red inalámbrica) propietarios a la laptop (IBM Laptops).

Existe un ambiente homogéneo de clientes, en caso de existir estaciones/laptops con distintos solicitantes.

4.1.8 Evaluación de la infraestructura Wireless

La red inalámbrica existente consta de dos Access Point DLINK para acceso corporativo; su ubicación es criterio del cliente. No existen configuraciones de alta disponibilidad, no hay un plan de frecuencias y features particulares en la red inalámbrica.

4.1.9 Evaluación de la seguridad Wireless

Los clientes usan claves WEP (la cantidad de bits de encriptación no es especificado). Ningún otro mecanismo de seguridad es aplicado.

4.2 Detalles técnicos de los equipos y configuración Lógica.

4.2.1 detalles técnicos de los equipos

Tabla 4.1 Detalles técnicos de los equipos

EQUIPO	MODELO	CARACTERISTICAS
Cisco Catalyst 3560G	WS-C3560G-24TS-S	24 Ethernet 10/100/1000 ports
Cisco Aironet 1130AG Series	AIR-AP1131AG-A-K9	IEEE 802.11a/b/g access points
Cisco Catalyst CE520G-24TC	WS-CE520G-24TC-K9	24 Ethernet 10/100/1000 ports

4.2.2 Description lógica de la implementación.

Tabla 4.2 Description Logica

VLAN	DESCRIPCION	SUBNET	ACCESO
VLAN 10	CORPORATIVA	192.168.0.0/24	ALAMBRICO E INALAMBRICO
VLAN 20	VOZ	192.168.5.0/24	ALAMBRICO
VLAN 30	NO CORPORATIVA	192.168.8.0/24	ALAMBRICO E INALAMBRICO
VLAN 1	DEFAULT	SIN USO	ALAMBRICO

Cada VLAN tiene una dirección IP asignada, El ruteo entre VLAN se realizará por el Switch de Capa 3 Cisco Catalyst 3560G

Los access point estarán instalados sobre los switches Cisco de manera que todos los esquemas de VLAN y seguridad serán trasportados hacia la red

La conectividad de los Server / usuarios, es decisión del cliente, el grafico solo da una muestra de conectividad de los equipos.

La conectividad entre el Switch principal (Cisco 3560) y los demás Cisco CE520 se realiza con dos puertos de para redundancia y para balanceo de carga, tiene configurado 2 puertos Etherchannel para lograr una forma efectiva de utilización (esta conectividad es vía cables de cobre UTP).

4.2.3 Configuración Wireless

Los Access point funcionaran como redundancia activo/activo uno del otro en cada piso hasta donde la cobertura se permita. Entre Access point existe roaming capa 2 de manera transparente y el "aire" transportará las VLANs en cada piso. Los protocolos de seguridad estarán implementados de acuerdo al perfil del usuario.

4.3 Topología de red implementada

Realizada la instalación en base a la información recogida por el cliente que es base del documento Design Process el diagrama siguiente muestra la topología

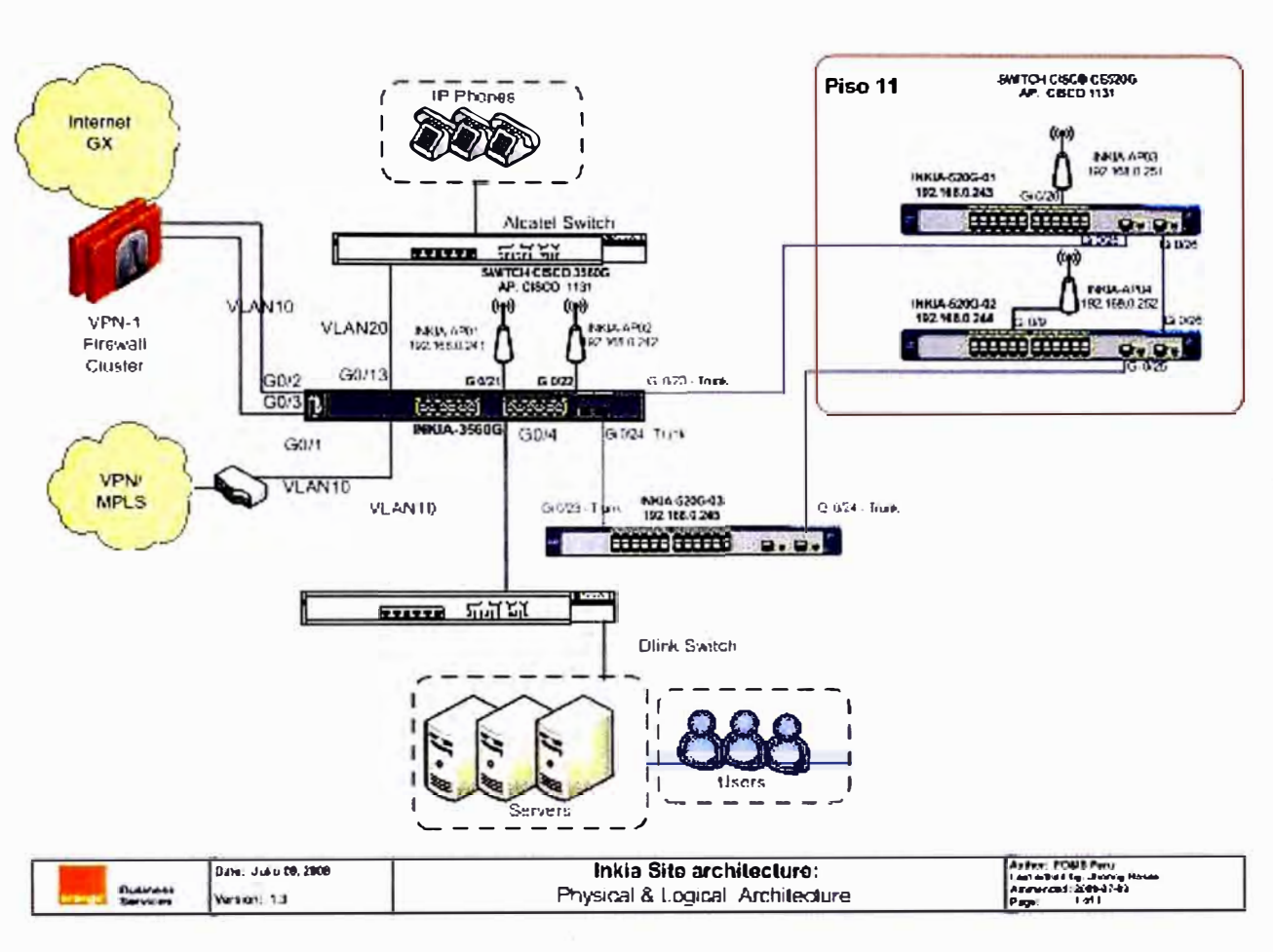

Fig. 4.1 Topología de Red LAN y WIRELESS Implementada

4.4 Configuración de equipos.

Se realizó la configuración de los equipos de acuerdo a los requerimientos de seguridad indicados por el cliente.

4.4.1 Configuración de Swich de Core

La configuración las interfaces virtuales SVI creadas en el Switch cisco Catalyst 3560G

(Las SVI son interfaces virtuales que asocian una VLAN a una interfaz ruteada)
SVI VLAN10: IP@192.168.0.253
SVI VLAN20: IP@192.168.5.1
SVI VLAN30: IP@192.168.8.1
Command Line Interface (CLI) acceso por Telnet (No restringido).
IP Management VLAN10: 192.168.0.253
User: administration
Pass: password
Enable password: password

Tabla 4.3 Distribución de puertos de switch C3560G

PUERTO	VLAN	CONECTADO
Gi0/1	10	Router
Gi0/2 to Gi0/20	10	Server / users
Gi0/21	Trunk	AP 1
Gi0/22	Trunk	AP 2
Gi0/13	20	Switch Alcatel
Gi0/23	Trunk	Switch 520G
Gi0/24	Trunk	Switch 520G

4.4.2 Configuración de Switches de Acceso

Switches Cisco CE520G
Switch INKIA-520G-01 IP Address Management VLAN10: 192.168.0.243
Switch INKIA-520G-02 IP Address Management VLAN10: 192.168.0.244
Switch INKIA-520G-03 IP Address Management VLAN10: 192.168.0.245

Distribución de puertos
Todos los puertos son asignados a la VLAN 10. A excepción de los puertos:
G0/25 Uplink Tunks.
G0/26 between CE520.

4.4.3 Instalación y configuración de Access points.

Piso 13 & Piso 11

Ambos pisos, comparten los mismos perfiles de seguridad de acceso inalámbrico (estos se detallan más adelante).

Tabla 4.4 Detalle de configuración de Access Point

Hostname	IP Management	User	Password	Locación
INKIA-AP01	192.168.0.241	Cisco	Cisco	Piso 13
INKIA-AP02	192.168.0.242	Cisco	Cisco	Piso 13
INKIA-AP03	192.168.0.251	Cisco	Cisco	Piso 11
INKIA-AP04	192.168.0.252	Cisco	Cisco	Piso 11

VLANs dentro de los Access Points: VLAN10, VLAN30.

4.5 Características técnicas de la implementación

4.5.1 Solución LAN Switching

La configuración de los equipos de LAN Switching responde a criterios de diseño:

Disponibilidad:

Esquema redundante de cuatro switches en rombo, que brinda seguridad redundante protegiéndolo ante la caída entre los enlaces de los switches del piso 11 y el Switch del piso 13. El protocolo de redundancia Spanning-Tree protocolo es habilitado y optimizado para lograr tiempos mínimos de convergencia.

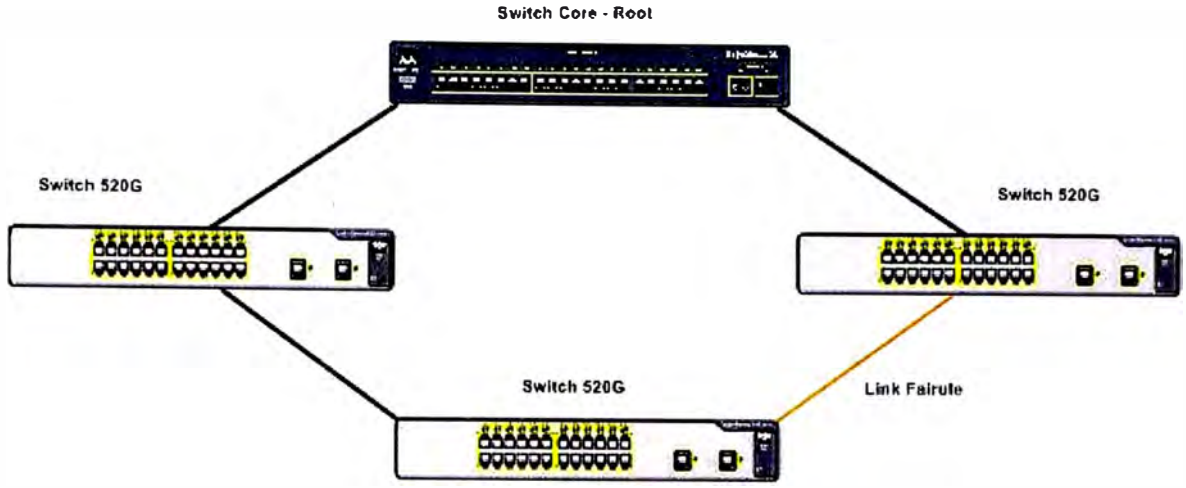

Fig. 4.2 Topología de seguridad redundante

Escalabilidad

Creación de VLANs, esto permite hacer una segmentación de red, a nivel de dominio broadcast, permitiendo que la red crezca de manera ordenada y de manera eficiente. Se sugiere que a medida se agreguen más dispositivos también se efectúe una segmentación

4.5.2 Solución Wireless

Cisco ha implementado muchas características de seguridad sobre los Access Point de acuerdo a las normas y protocolos de seguridad. La solución configurada en los equipos Wireless Lan de INKIA cumple con todos las normas de seguridad y es una configuración de VLANs que aplican en el medio inalámbrico de WLAN y cada uno de los Access Point con un perfil de seguridad propio, de acuerdo a las demandas corporativas,.El tipo de seguridad con sus características se detallan en la siguiente tabla.

Tabla 4.5 Parámetros de seguridad Wireless

PERFIL	Corporativo	Perfil no corporativo
SSID	corporacioninkia	nocorporativoinkia
SSID Broadcast	no	si
VLAN	VLAN 10.	VLAN 30.
Perfil de seguridad	WPA2	WEP
Encryption mode:	AES-CCM.	WEP 128 bits.

CONCLUSIONES

1. Es fundamental el levantamiento de información previo a la implementacion a su vez cumplir con los estandares te permite el crecimiento empresarial de una forma ordenada confiable y escalable.
2. En la actualidad gran parte de los problemas son ocacionados por la falta de conocimientos en la forma como se aplican los modernos esquemas de seguridad al campo de la información.
3. Las implementaciones de Redes internas inalambrica en el Peru, sobre todo en pequeñas empresas, La forma como se accede a la Red por ese medio es simple con poco énfasis en la seguridad, seria recomendable realizar un analizis los costos que implicarian el filtrar información confidencial y el daño que ocacionarian el acceso a personal no autorizado.
4. En la tecnología inalámbrica la información viaja a través del aire por tanto se encuentra expuesta a que cualquier persona pueda obternerla por ello es imprescindible la implementacion de algoritmos de Encriptación como una medida de seguridad.
5. En la implementacion de la Red Lan se han considerado las medidas de seguridad en la parte de acceso a la red, Autenticación de PC y usuarios y encriptación de la data. Asi como creación de VLAN para los usuarios corporativos y los no corporativos.
6. Para las soluciones inalámbricas complejas se tiene una amplia gama de productos para gestionar la red Wiresless facilitando la administración y configuración de equipos inalambricos asi como la verificación de los usuarios que se conectan a la red por ese medio.

ANEXO A

DETALLE DE CONTACTOS

DETALLE DE CONTACTOS DE ORANGE

Name	Function	Phone/Fax	Address	Hours
Omar Parihuana	Senior Engineer	511-611 4500	Av. Victor A. Belaunde 147 San Isidro	M-Fri 0900-1800 Lima time
Jhonny Rosas	Field Engineer	511-611 4500	Av. Victor A. Belaunde 147 – San Isidro	M-Fri 0900-1800 Lima time

DETALLE DE CONTACTOS DE INKIA

Name	Function	Phone/Fax	Address	Hours
Alberto Gonzales	System Manager	511-706-7800	Av. Victor A. Belaunde 147, Torre 3, San Isidro	M-Fri 0900-1800 Lima time

ANEXO B

HANDOVER DE EQUIPOS INSTALADOS

HANDOVER DE LOS EQUIPOS

El principio de inicio de handover se establece cuando todos los equipos están completamente configurados, según el alcance del servicio, y pasaron satisfactoriamente las pruebas de conectividad, es decir, están listos para entrar en operación.

Tabla anexo b.1: Relacion de equipos bajo mantenimiento de hardware

QTY	DESCRIPTION	SERIE NUMERICA
1	SWITCH CATALYST 3560G	FOC1216Z3XT
		FTX1218N15E
		FTX1218N15F
		FTX1218N15G
4	AIR-AP1131AG-A-K9	FTX1218N15H
		FOC1139U1D2
	SWITCH CATALYST EXPRESS 520G	FOC1139U19J
3	SERIES	FOC1139U185

Se realizaron las siguientes actividades:
Entrega de Equipos Cisco.
Montaje de cada uno de los equipos.
Configuración de cada uno de los equipos.
Pruebas de conectividad entre los equipos.

La fecha de handover es el día 10 de Julio del 2008.

ANEXO C

GARANTIA DE EQUIPOS Y PROCEDIMIENTO PARA SOLICITAR LA GARANTIA

Garantía de los Equipos.

Todos los equipos suministrados por Orange Business Services a Inkia Perú, cuentan con garantía por tres (03) años, a partir de la fecha de firma de este contrato. Para hacer efectiva la garantía, el cliente deberá seguir los siguientes pasos:

- Abrir un caso en nuestro GCSC.
- Obtener, si corresponde, un número de RMA válido.
- Entregar el equipo afectado en nuestras bodegas de Lima.
- Transcurrido el plazo de reparación o reemplazo, retirar el equipo de nuestras bodegas.
- Es responsabilidad del cliente la re-instalación y configuración del equipo reemplazado.

El RMA de reparación o reemplazo, sólo se generará, una vez realizado el diagnóstico de la anomalía reclamada por el cliente, por el GCSC de Orange Business Services y/o el servicio de Asistencia Técnica (TAC) del fabricante. La garantía sólo incluye los equipos suministrados y aplica sólo en casos de defectos de fabricación y falla o mal funcionamiento atribuibles al fabricante.

Se excluyen de la garantía, las fallas causadas por el cliente o por causas de inadecuadas condiciones de operación, alimentación eléctrica o medio ambiental, así como también las causadas por mal uso o desgaste. Orange Business Services se reserva el derecho de determinar si corresponde un RMA, en caso de falla de la plataforma LAN. Una vez expirado el periodo de tres (03) años, cesa toda responsabilidad de garantía provista por Orange Business Services a los equipos, según se describe anteriormente

Proceso para reporte de Fallas:

Inkia reportara el problema a Orange Business Services Global Customer Service Center (GCSC) llamando a un número local o directamente al GCSC

Proveer la siguiente información :

Company Name: **INKIA**

Callers Name & Telephone Number: **ALBERTO GONZALES/ 511-706-7810**

Site ID, Router Name or DNA (Network Address): **LIMINKIA-1**

Country & City: **PERU & LIMA**

Fault Symptoms:

Date/Time problem started

Is this a new Service?

Business Impact

El personal de soporte revisara la informacion del cliente en la base de datos Clarify (CMR) confirmando el codigo de usuario aceptará y le creará un ticket de atención. Posteriormente realizarán la revisión del problema y su solución en el menor tiempo posible.

BIBLIOGRAFÍA

1. Adamut, "Fundamentals of Wireless LANs", Jun. 2006
2. Cisco System, "Secure Wireless Design", Ver 1.0. Jul. 2007
3. Cisco System "Aironet Wireless LAN Fundamentals" Ver 3.1 2007
4. Orange Business Services " Site Survey Wireless " Ver 1.0 2007