TRABAJO ESPECIAL DE GRADO

TÉCNICAS PARA MEJORAR LA SEGURIDAD DE LA RED INALÁMBRICA DE ÁREA LOCAL DE LA EMPRESA DESCA

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Bachiller Jaimes C., Alfonso J.
Para optar al título de
Ingeniero Electricista

Caracas, 2006

TRABAJO ESPECIAL DE GRADO

TÉCNICAS PARA MEJORAR LA SEGURIDAD DE LA RED INALÁMBRICA DE ÁREA LOCAL DE LA EMPRESA DESCA

Profesor Guía: Ing. Vincenzo Mendillo
Tutor Industrial: Ing. Daniel Villavicencio

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Bachiller Jaimes C., Alfonso J.
Para optar al título de
Ingeniero Electricista

Caracas, 2006

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE INGENIERIA ELECTRICA
DEPARTAMENTO DE COMUNICACIONES

CONSTANCIA DE APROBACIÓN

Caracas, 24 de octubre de 2006

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Alfonso J. Jaimes C ., titulado:

"TÉCNICAS PARA MEJORAR LA SEGURIDAD DE LA RED INALÁMBRICA DE ÁREA LOCAL DE LA EMPRESA DESCA"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por los autores, lo declaran APROBADO.

Pilar Medrano
Prof. Pilar Medrano
Jurado

Prof. Luis Fernández
Jurado

Vincenzo Mendillo
Prof. Vincenzo Mendillo
Prof. Guía

UNIVERSIDAD CENTRAL DE VENEZUELA FACULTAD DE INGENIERIA ESCUELA DE INGENIERIA ELECTRICA DEPARTAMENTO DE COMUNICACIONES

Edificio Escuela de Ingeniería Eléctrica, piso 1, oficina 201, Ciudad Universitaria, Los Chaguaramos, Caracas 1051, D.F.
TELÉFONOS. (VOZ) +58 212 6053300 (FAX) +58 212 6053105
Mail: eie-com@elecrisc.ing.ucv.ve

AGRADECIMIENTOS

Agradezco en especial a mi madre a mi padre y a mi hermana, quienes siempre confiaron en mí y me apoyaron en los momentos difíciles. Gracias por creer en mí.

Agradezco a la ilustre Universidad Central de Venezuela, y en especial a la Escuela de Ingeniería Eléctrica, la cual se convirtió en mi segunda casa y me permitió la formación, no sólo como ingeniero, sino como un ser humano integral. Gracias a todos aquellos profesores que colaboraron en mi formación, así como todos mis compañeros con los que compartí en las aulas a lo largo de la carrera.

Agradezco a mis tutores, el Prof. Vincenzo Mendillo, y el Ing. Daniel Villavicencio, quienes me prestaron su ayuda y colaboración en el momento requerido durante el desarrollo de este trabajo.

Agradezco a la Secretaria del Departamento de Comunicaciones María Auxiliadora Rojas, quien siempre tuvo una palabra de aliento y orientación en las situaciones adversas.

Agradezco a Yuruari López, quien siempre estuvo a mi lado brindando apoyo en la elaboración de este trabajo de grado.

Jaimes C., Alfonso J.

TECNICAS PARA MEJORAR LA SEGURIDAD DE LA RED INALAMBRICA DE AREA LOCAL DE LA EMPRESA DESCA

Profesor Guía: Ing. Vincenzo Mendillo. Tutor Industrial: Ing. Daniel Villavicencio. Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Comunicaciones. Institución: DESCA. 2005 102 h. + anexos.

Palabras Claves: Redes inalámbricas de área local (WLAN), estándar IEEE 802.11, seguridad en redes inalámbricas.

Resumen. En el presente trabajo especial de grado se estudian las diferentes técnicas de aseguramiento de las redes inalámbricas de área local. En base al estudio, se plantea el desarrollo de dos propuestas técnicas de aseguramiento de la red inalámbrica de área local de la empresa venezolana Desarrollos de soluciones específicas específicas C.A., que permitan brindar un nivel de seguridad superior al que posee en la actualidad. Posteriormente, se seleccionan y desarrollan los lineamientos básicos de implementación de la propuesta de aseguramiento que mejor se adapte a las necesidades y situación actual de la red de la empresa, para que dicha propuesta sea implementada en la sede de Caracas, y a continuación replicada en las demás sucursales, y así, contar con una red corporativa segura, que ofrezca además un nivel de alta calidad de servicio.

ÍNDICE GENERAL

LISTA DE FIGURAS

LISTA DE FIGURAS Pág.

LISTA DE TABLAS

LISTA DE TABLAS Pág.

ACRÓNIMOS

AAA	Authentication, Authorization, and Accounting
ACK	Acknowledge
ACS	Cisco Secure Access Control Server
AD	Active Directory
AES	Advanced Encryption Standard
AP	Access Point
ASDP	Automatic Power Save Delivery
BA	Block Acknowledgments
CA	Certification Authority
CCK	Complementary Code Keying
CFP	Contention Free Period
CF-Poll	Contention Free-Poll
CHAP	Challenge-Handshake Authentication Protocol
CP	Contention Period
CRL	Certificate Revocation List
CSMA/CD	Carrier Sense Multiple Access / Collision Detect
CTS	Clear To Send
DCF	Distributed Coordination Function
DES	Data Encryption Standard
DESCA	Desarrollos Específicos Compañía Anónima
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DSSS	Direct-Sequence Spread-Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAP-FAST	EAP-Flexible Authentication via Secure Tunneling
EAP-SIM	EAP - Subscriber Identity Module
EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunneled TLS
EDCA	Enhanced DCF Channel Access
EEUU	Estados Unidos de América
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
EWC	Enhanced Wireless Consortium
FCC	Federal Communications Commission
FDM	Frequency-Division Multiplexing
FTP	File Transfer Protocol
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HP	Hewlett-Packard

HTTP	Hypertext Transmission Protocol
IAS	Internet Authentication Service
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute Of Electrical And Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	Industrial, Scientific And Medical
ISP	Internet Service Provider
IT	Information Technology
IV	Initialization Vector
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
Mbps	Mega bits por segundo
MD4	Message Digest 4
MGCP	Media Gateway Control Protocol
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
MITM	Man in the Middle
NIC	Network Interface Card
OFDM	Orthogonal Frequency-Division Multiplexing
OSI	Open Systems Interconnection
OTP	One-Time Password
OUI	Organizacional Unique Identifier
PAN	Personal Area Network
PC	Personal Computer
PCF	Point Coordination Function
PDC	punto de contacto
PEAP	Protected EAP
PKI	Public Key Infrastructure
PPK	Per-Packet Keying
QoS	Quality of Service
RADIUS	Remote Access Dial-in Service
RC4	Rivest Code 4
RFC	Request For Comments
RSA	Rivest, Shamir y Adelman
RSADSI	Rsa Data Secutity Inc
RTP	Real Time Protocol
RTS	Request To Send
SGCP	Simple Gateway Control Protocol
SHF	Super High Frequency
SNMP	Simple Network Management Protocol

SO	Sistema Operativo
SSH	Secure Shell Protocol
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSO	Single sing-on
SWAP	Shared Wireless Access Protocol
TC	Traffic Class
TEG	Trabajo Especial de Grado
TIP	Telefonía IP
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TXOP	Transmit Opportunity
UHF	Ultra High Frequency
U-NII	Unlicensed National Information Infrastructure
VACL	VLAN Access Control List
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WISP	Wireless ISP
WLAN	Wireless Local Area Network
WLSE	Wireless LAN Solution Engine
WME	Wireless Multimedia Extension
WMM	Ver WME
WPA	Wi-Fi Protected Access
WWiSE	World-Wide Spectrum Efficiency
xDSL	Digital Subscriber Line
XML	Extensible Markup Language

INTRODUCCIÓN

La empresa Desarrollo de soluciones específicas compañía anónima (DESCA), dedicada a la integración de soluciones orientadas al diseño, construcción, optimización y mantenimiento de plataformas de networking e infraestructura de Tecnologías de Información (IT), está en la búsqueda de una solución que le permita mejorar la seguridad de las WLAN (acrónimo del inglés universalmente utilizado por 'Red Inalámbrica de Área Local') para su implantación en la red corporativa de ésta empresa, cuyas oficinas principales están ubicadas en la ciudad de Caracas / Venezuela.

Por definición, una de las características principales de las WLAN (y a la vez su mayor atractivo a la hora de implementarlas) es la facilidad para acceder a ellas sin la necesidad del uso de cableado, si bien es preocupante la lista de vulnerabilidades en lo que seguridad se refiere. Para los efectos de este proyecto de Trabajo Especial de Grado (TEG), se plantea el estudio de las técnicas disponibles y mejores prácticas, que permitan la selección de una opción de tecnología de seguridad que se pueda convertir en una solución factible, económica y acorde con las características y necesidades actuales de la red inalámbrica de esta empresa.

A lo largo de este TEG, conformado por 5 capítulos, se desarrolla el basamento teórico de las WLAN, levantamiento de información de la red de DESCA, dos propuestas factibles de diseño de WLAN seguras y el detalle de la implementación de las propuestas de seguridad que mejor se adaptan a la empresa, todo esto en base al problema propuesto en este trabajo. A continuación una breve descripción del contenido del TEG:

CAPITULO I: Se hace el planteamiento del problema en el cual se basa este trabajo, se proponen el objetivo principal y secundario, y se realiza una breve reseña histórica de la empresa DESCA.

CAPITULO II: Se hace una revisión de las tecnologías de redes inalámbricas y su funcionamiento; se expone su evolución a lo largo del tiempo y lo que será en un futuro con la aprobación de nuevos estándares. También se hace una revisión de las vulnerabilidades de las WLAN basadas en 802.11, y de tecnologías y técnicas de aseguramiento utilizadas para mitigar dichas vulnerabilidades. Por ultimo, se explica cómo debe ser la arquitectura y los fundamentos de diseño de las WLAN seguras en la actualidad.

CAPÍTULO III: Se realiza el levantamiento de información de la topología de la red y servicios ofrecidos en la red de DESCA, y de la situación actual, en cuanto a seguridad se refiere, de la WLAN de la oficina de Caracas.

CAPÍTULO IV: Se proponen con cierto nivel de detalle dos propuestas de aseguramiento de WLAN que satisfacen los requerimientos de seguridad de empresas como DESCA, basadas en los fundamentos de diseño de WLAN seguras reseñados en el capítulo II.

CAPITULO V: En base a la información expuesta en los capítulos II y IV, se realiza la elección de una propuesta técnica de aseguramiento que aporte los niveles de seguridad requeridos por una empresa como DESCA, y que además, se adapte a la situación actual de la red tal como se describe en el capítulo III. Posteriormente, se presentan los lineamientos básicos de configuración de los equipos necesarios para la implantación de la propuesta elegida.

Por último, y en base a toda la información expuesta en este TEG, se presentan las conclusiones y recomendaciones, con el objetivo de resaltar los puntos más importantes de este trabajo.

CAPITULO I

1 PLANTEAMIENTO DEL PROBLEMA

A partir de la introducción de los estándares 802.11 del IEEE (acrónimo del inglés Institute of Electrical and Electronics Engineers), la popularidad de las WLAN se ha visto incrementada, sobre todo en las redes corporativas, por su capacidad de eliminar la gran cantidad de cableado, como su más notable ventaja. Aunque ésta es sólo una de las muchas ventajas de la tecnología WLAN, a la cual se suman la movilidad y el acceso a los recursos de los sistemas IT desde cualquier lugar en una empresa, todo lo cual brinda un ambiente de trabajo más productivo y eficiente puesto que permite al personal acceder a los recursos sin estar atados a la tradicional red cableada.

La empresa DESCA cuenta con siete sucursales, ubicadas en los Estados Unidos, México, Costa Rica, Venezuela y Colombia. Actualmente tiene instalada una infraestructura de WLAN, conformando una red corporativa a través de la cual comparten recursos e información, todo ello junto a una red de telefonía de IP (TIP), cuya infraestructura está basada principalmente en Ethernet. Esta red inalámbrica, al igual que la mayoría de las instaladas en otras corporaciones a nivel mundial, enfrenta la posibilidad de ver vulnerada su seguridad.

Cada una de las sucursales de DESCA tiene una WLAN, basada en equipos Aironet de Cisco, que de estar configurados de forma inapropiada, pueden presentar graves vulnerabilidades en cuanto a seguridad. Es esta condición la que ha estimulado al estudio y revisión de las opciones tecnológicas de seguridad WLAN disponibles para los equipos Cisco y al establecimiento de procedimientos que permitan el mejor manejo y gestión de la misma.

2 OBJETIVOS

2.1 Objetivo general

Revisar y analizar las tecnologías disponibles para el aseguramiento óptimo de las WLAN instaladas en las sedes de la empresa DESCA, que permita seleccionar el modelo más adecuado para el establecimiento de configuraciones, procedimientos y políticas de seguridad en la red de la corporación.

2.2 Objetivos específicos

- Evaluar y comparar las distintas tecnologías y estándares de WLAN
- Evaluar y comparar las tecnologías y estándares de seguridad WLAN, con sus fortalezas y debilidades.
- Analizar la infraestructura de la WLAN de la empresa DESCA.
- Proponer niveles, directivas y procedimientos de seguridad como meta factible.
- Comparar las técnicas de aseguramiento estudiadas con las disponibles en los equipos actualmente en uso en DESCA.
- Desarrollar y proponer dos posibles soluciones técnicas adaptadas a las necesidades de la empresa.
- Implementar la propuesta de solución técnica y realizar pruebas de desempeño.

3 IDENTIFICACIÓN DE LA EMPRESA

3.1 Nombre de la empresa

Desarrollos Específicos Compañía Anónima

DESCA, The Networking Company.

3.2 Misión de la empresa

Satisfacer las cambiantes necesidades presentes y futuras del empresario venezolano en él área de la tecnología de la información, contando con aliados de alto valor estratégico, tecnología de punta y personal altamente capacitado.

3.3 Visión de la empresa

Ser líder en el mercado venezolano de las tecnologías de información, ofreciendo soluciones integrales de alto valor agregado, enfocadas en reducir los costos operativos e incrementar la competitividad de sus clientes.

3.4 Reseña histórica de la empresa

DESCA fue fundada en 1996, orientada desde sus inicios a la especialización en soluciones de redes. Para ese momento existía la necesidad creciente en las empresas de contar con una compañía que ofreciera gran variedad de soluciones de conectividad y de tecnología de información. En el año 2003, DESCA abrió sus oficinas en Bogotá-Colombia, además de atender el área de servicios profesionales para Centro América y El Caribe, desde oficinas ubicadas en Miami-EEUU. En el año 2005, abrió oficinas en la Ciudad de México y en Medellín (Colombia). Hoy en día es una empresa especializada en soluciones para infraestructura en *internetworking* y tecnología de la información.

Trabaja en alianza con los principales proveedores de tecnología para la implementación de redes basadas en el protocolo IP. Cuenta con recursos calificados para analizar las tecnologías, evaluar su impacto en el negocio de los clientes e implementar soluciones orientadas a mejorar el retorno de la inversión. La mayoría de sus miembros son jóvenes profesionales motivados, con mucho talento y conocimientos. Posee soporte de consultoría, cuenta con un grupo de ingenieros certificados en las tecnologías Cisco Systems, EMC^2, Motorota y Tandberg.

CAPITULO II

4 LAS REDES INALÁMBRICAS DE ÁREA LOCAL

4.1 Necesidad de las WLAN

Las WLAN basadas en el estándar 802.11 proveen movilidad a los usuarios de la red y a su vez conectividad a los recursos de la red corporativa. A medida que las computadoras portátiles van ocupando cada vez más los lugares de trabajo, los usuarios son cada vez más propensos a utilizarlas como su principal herramienta de trabajo, permitiéndoles mayor portabilidad en las reuniones y conferencias, y durante viajes de trabajo. Las WLAN ofrecen a las empresas mayor productividad por empleado permitiéndoles conectividad constante a las redes tradicionales desde lugares desde donde antes era inimaginable.

La conectividad inalámbrica no sólo se limita al uso corporativo, ya que las WLAN también ofrecen incremento de la productividad afuera del tradicional ambiente de oficina. Son numerosos lo proveedores de servicios de Internet inalámbrico (WISP) en los aeropuertos, cafés, centros comerciales, hoteles, y en los centros de conferencias y convenciones, permitiendo a los usuarios de la empresas conectarse a sus redes corporativas desde puntos de libre acceso, conocidos como *hotspots*.

4.2 Introducción a las tecnologías WLAN

Las WLAN han existido desde hace muchos años, permitiendo la conexión a infraestructuras cableadas en lugares de trabajo donde la movilidad es un requisito específico de la actividad realizada. Estas primeras redes se basaban en el uso de técnicas de modulación sencillas, y a velocidades de transmisión de 1 y 2 Mbps, y sus implementaciones no estaban normalizadas por ningún estándar en específico. La no existencia de recomendaciones estándares para estas redes inalámbricas, obligaba a los fabricantes a implementar tecnologías propietarias, que no garantizaban la interoperabilidad entre marcas, por lo que el crecimiento de su uso se vio muy limitado. Hoy en día existen varios estándares para la implementación de WLAN, entre los cuales están IEEE 802.11, HiperLAN, HomeRF SWAP, y Bluetooth.

4.3 Funcionamiento

Desde el punto de vista funcional, las WLAN pueden ser divididas en tres tipos: redes punto a punto (*ad hoc*), redes de infraestructura de una o más celdas, y redes de larga distancia en enlaces punto a punto, o punto a multipunto. En el caso de conexiones *ad hoc*, los clientes inalámbricos deben estar equipados con tarjetas de red inalámbricas (NIC) para comunicarse entre sí sin la necesidad de un punto de acceso (AP). La cobertura está limitada a la red punto a punto, y los clientes inalámbricos no tienen acceso a recursos de la red cableada. Las WLAN de infraestructura ofrecen una mayor zona de cobertura con el uso de celdas solapadas entre si. Las características de los AP son las que determinan el área de cobertura de cada celda, y cada uno de éstos AP funciona como un puente que coordina la comunicación entre los clientes inalámbricos y el acceso a los recursos de la red cableada.

Las WLAN de larga distancia proveen conectividad entre dos o mas LAN cableadas ubicadas en edificaciones separadas, por ejemplo, la red de un campus. Existen dos tipos de estas redes inalámbricas: punto a punto, y punto a multipunto. Las redes inalámbricas punto a punto entre dos edificios están basadas en enlaces de radiofrecuencia o láser. Los de radio frecuencia utilizan antenas direccionales que maximizan la distancia de transmisión. Las basadas en láser utilizan generalmente luz infrarroja como portadora de los datos a transmitir. Los enlaces punto a multipunto, basados en radiofrecuencia, utilizan antenas con un patrón de radiación más amplio que en el caso anterior, con el objetivo de conectar varias redes ubicadas en otras edificaciones.

4.4 Tecnologías de WLAN

A pesar de que este trabajo se concentra en el estudio del estándar 802.11, es importante conocer los otros estándares de redes inalámbricas que se utilizan actualmente en el mercado mundial.

4.4.1 HiperLAN

HiperLAN es un estándar europeo ratificado en 1996 por ETSI (European Telecomunications Standards Institute). HiperLAN/1 opera en la banda de 5 GHz a una velocidad de transmisión de hasta 24 Mbps. En el año 1999, ETSI aprobó HiperLAN/2, el cual igualmente opera en la banda de 5 GHz alcanzando velocidades de hasta 54 Mbps, y

que además utiliza protocolos orientados a conexión para acceso compartido entre usuarios finales.

4.4.2 HomeRF SWAP

En 1988, el grupo llamado HomeRF SWAP Group, publicó un estándar para comunicaciones inalámbricas digitales entre computadores personales y dispositivos electrónicos del hogar llamado SWAP (Shared Wíreless Access Protocol). SWAP permite transmisiones de voz y datos por medio de una misma interfaz inalámbrica a velocidades de transmisión de 1 y 2 Mbps, mediante el uso de las técnicas de *frecuency-hopping* y *spread-spectrum* en la banda de 2,4 GHz. Este es un estándar obsoleto que ya ha entrado en desuso.

4.4.3 Bluetooth

Bluetooth es una tecnología para redes de área personal (PAN), especificada por Bluetooth Special Interest Group, que provee conectividad inalámbrica de corto alcance y a bajas potencias en la banda de los 2,4 GHz. Se basa también en las técnicas de *frecuency-hopping* y *spread-spectrum*.

4.5 Tecnología WLAN 802.11

IEEE se encarga de elaborar el grupo de estándares 802.11, así como otros de los grupos de trabajo 802, como por ejemplo el estándar Ethernet 802.3. También existe otra organización sin fines de lucro, y sin influencia de fabricantes, conocida como Wi-Fi Alliance, la cual le asigna una certificación a todos los productos que cumplen con sus especificaciones, lo que obliga a los fabricantes a garantizar la interoperabilidad entre dispositivos de distintas marcas, para que estos puedan obtener la certificación Wi-Fi. Esto quiere decir que cualquier producto certificado Wi-Fi puede funcionar con otro que cuente con esta certificación, sin importar el fabricante.

Las tecnologías inalámbricas basadas en 802.11 utilizan como medio físico de transmisión el espectro radial considerado para uso público. Este espectro radial está regulado para uso Industrial, Científico y Médico, por lo cual se le da el nombre de banda ISM (acrónimo del inglés Industrial, Scientific and Medical). El estándar se aprovecha de dos de las tres bandas de frecuencias utilizadas para este fin, la de 2,4000 GHz a 2,4835

GHz, banda UHF utilizada para las WLAN 802.11b, 802.11g y 802.11n; y la de 5,150 GHz a 5,825 GHz, banda SHF utilizada para las redes basadas en 802.11a.

Dependiendo de la regulación de cada país, la utilización de estos espectros puede no requerir licencia, lo que significa que no tiene ningún propietario mientras se cumplan las limitaciones dispuestas por la Federal Communications Commission (FCC) o el organismo regulador de correspondiente. Entre las limitaciones pueden estar la potencia máxima de transmisión de los equipos, los tipos de modulación utilizados, etc.

4.6 Componentes de una WLAN

Los componentes de una WLAN son los AP, NIC inalámbricos, puentes y las antenas.

Puntos de Acceso: Los AP operan en una gama de frecuencias específicas y utilizan las técnicas de modulación especificadas en el estándar 802.11. Se encargan de informar a los clientes de su disponibilidad, y autenticarlos y asociarlos a la WLAN. Un AP también coordina el uso de los recursos de la red cableada por parte de los clientes inalámbricos.

NIC inalámbrico: Un computador personal (PC) o una estación de trabajo utiliza un NIC inalámbrico para conectarse a la red inalámbrica. El NIC busca dentro del espectro de frecuencia la presencia de una red disponible, y se asocia a ella a través de un AP o de otro cliente. El NIC está bajo el control del sistema operativo del PC o estación de trabajo a través de los programas controladores.

Puente: Es utilizado para conectar múltiples LAN (cableadas e inalámbricas) a nivel de capa de acceso al medio o capa 2 del modelo OSI por medio de enlaces punto a punto. Los enlaces con puentes inalámbricos pueden cubrir distancias de más de 8 km, y se han reportado conexiones exitosas de hasta 120 km. Quien se disponga a instalar un enlace punto a punto de estas características, debe estar atento a las limitaciones legales respecto a la potencia efectiva irradiada por los equipos de microondas.

Antena: Las antenas irradian la señal modulada a través del aire, de forma tal que pueda ser recibida por los dispositivos de conexión inalámbrica. Las características de las antenas vienen dadas por su patrón de radiación (direccional u omnidireccional), la ganancia, potencia de transmisión, etc.

4.7 Métodos de modulación de radio frecuencia en las WLAN

La técnica de s*pread-spectrum* es la utilizada en la banda ISM de 2,4 GHz para las WLAN. Esta técnica se basa en que las transmisiones de datos son esparcidas en varias frecuencias, la razón de esto es que la banda ISM operan otros equipos que tienen derecho legal de su uso, un ejemplo de estos son los hornos de microondas, que transmiten en la misma banda de frecuencia pero a una potencia mucho mayor. Las típicas WLAN operan a 100 mW mientras que los hornos microondas operan a 600 W. Sin la tecnología *spread-spectrum* sería imposible evitar las interferencias con las señales de radiofrecuencia emitidas por otros dispositivos operando en la misma banda. 802.11 especifica dos tipos de interfaces de capa 1 para dispositivos de radio, una de ella es llamada *frequency hopping*, y la otra *direct sequencing*.

4.7.1 Frequency hopping

La banda ISM de 2,4 GHz ofrece 83,5 MHz de ancho de banda. La técnica de frequency-hopping sintoniza un rango de frecuencias, de las 79 disponibles de 1 MHz de ancho de banda, que elige mediante un patrón aleatorio y transmite a través de ella por periodos pequeños (Figura 1). (Referencia bibliográfica: Estándar IEEE 802.11 página 174)

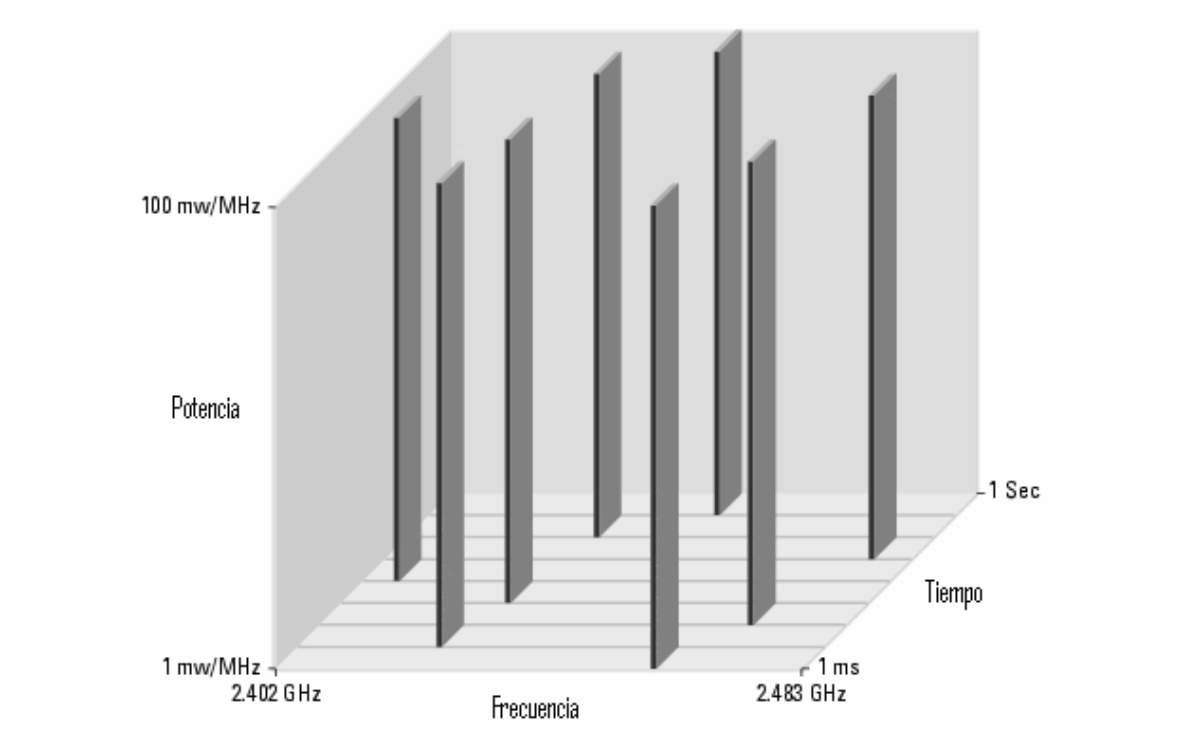

Figura 1. Frequency Hopping

Esta configuración permite una transmisión de datos tolerante a la interferencia. Si uno de los canales posee interferencia, entonces éste será utilizado por un periodo muy pequeño, dado que rápidamente la transmisión saltará hacia otro canal para la retransmisión en otra frecuencia.

El mayor inconveniente para *frequency hopping* es que la máxima tasa de transmisión es de 2 Mbps [1]. Se ha trabajado mucho en el concepto de *frequency hopping* de banda ancha, pero este aún no ha sido estandarizado por la IEEE. *Frequency hopping* promete velocidades de transmisión de hasta 10 Mbps.

4.7.2 Direct Sequencing y 802.11b

Las WLAN basadas en *direct sequencing* realizan la transmisión de los datos de forma totalmente distinta. El ancho de banda total se divide en 11 diferentes canales solapados de 22 MHz dentro de la banda ISM de 2,4 GHz. Entre los 11 canales, existen 3 canales de 22 MHz de ancho de banda que no se solapan entre si, ver Figura 2. En cada uno de estos canales no solapados se utiliza la técnica de modulación *direct-sequence spread-spectrum* (DSSS), que se basa en aumentar el ancho de banda de transmisión de los datos al combinarlos con una secuencia de bits a una tasa de transmisión más alta. De esta forma se distribuyen los datos a todo lo ancho del canal de transmisión de 22 MHz, logrando mayores tasas de transmisión y aumento de la resistencia ante interferencia de radio frecuencia.

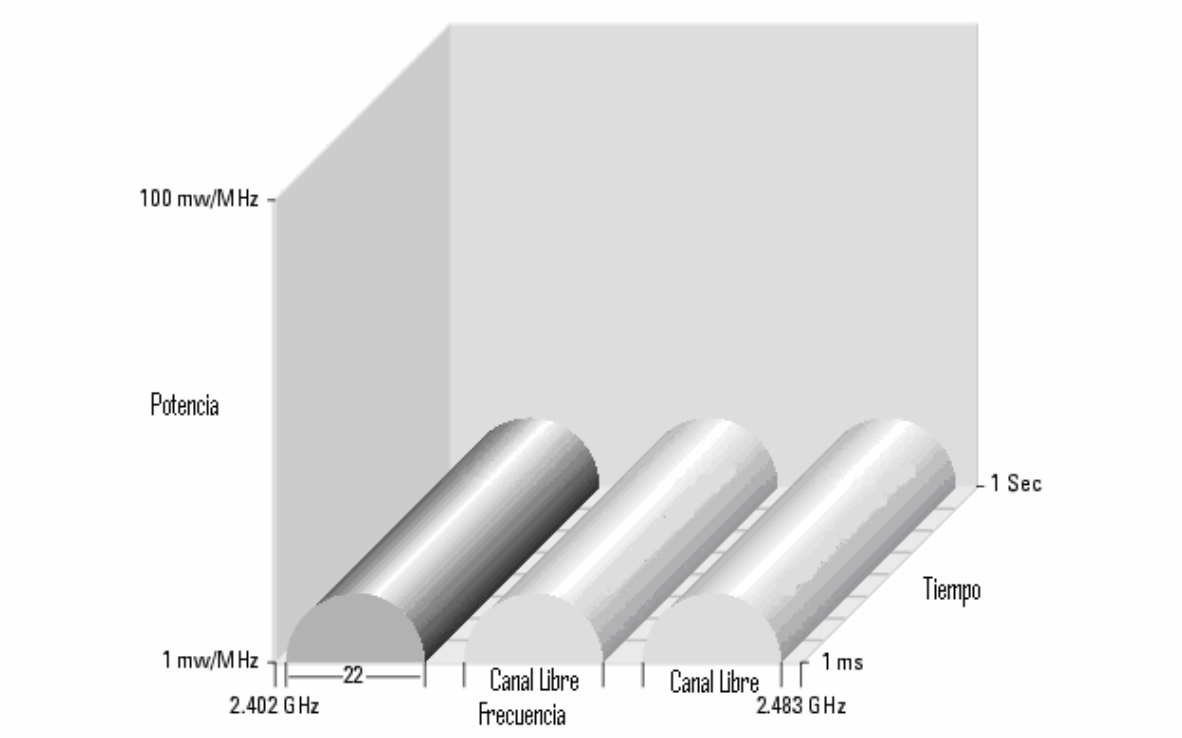

Figura 2. Direct Sequencing

La velocidad de transmisión ofrecida por *direct sequencing* es mucho mayor que la ofrecida por *frequency hopping* y esto se logra con la unión de un gran ancho de banda de transmisión combinada con modulación avanzada basada en *complementary code keying* (CCK). Adicionalmente, dado que existen tres canales no solapados, se pueden utilizar tres AP simultáneamente para ofrecer velocidades de transmisión superiores combinación de estos tres canales. IEEE ratificó el estándar 802.11b en el año 1999, ratificación que contiene nuevos tipos de modulación avanzada que permite que las WLAN basadas en direct sequencing alcancen velocidades de hasta 11 Mbps, y de 33 Mbps utilizando simultáneamente los tres canales que no se solapan.

La desventaja que tiene *direct sequencing* frente a *frequency hopping* es la menor tolerancia a la interferencia y la velocidad de transmisión en una red basada en *direct sequencing* cae enormemente cuando hay interferencia.

4.8 Redes 802.11a

En el año 1999 IEEE ratificó otro estándar de capa 1 llamado 802.11a. Este estándar utiliza la banda SHF de 5 GHz y alcanza velocidades de transmisión de 54 Mbps. A diferencia de los estándares 802.11 y 802.11b, el estándar 802.11a utiliza un tipo de

multiplexación por división de frecuencia (FDM) llamada orthogonal FDM (OFDM). En un sistema FDM, el ancho de banda es dividido en múltiples portadoras y los datos a ser transmitidos son divididos a lo largo de las múltiples portadoras. Una banda de guarda debe ser colocada alrededor de cada una de las portadoras, ya que éstas son tratadas individualmente una de las otras, y estas bandas de guarda disminuyen la eficiencia en el uso de todo el ancho de banda.

Con OFDM, al igual que con FDM, se dividen los datos a lo largo de múltiples portadoras. Sin embargo, con OFDM no es necesaria la utilización de bandas de guarda, y esto se logra haciendo que cada portadora es ortogonal a sus adyacentes, lo que hace que las portadoras sean independientes o no estén relacionadas entre sí.

La banda de 5 GHz asignada en EEUU a la Infraestructura Nacional de Información no Licenciada (Unlicensed National Information Infrastructure, U-NII) fue dividida por la FCC en tres bandas. Cada una de esas bandas consiste de cuatro canales no solapados de 20 MHz contenidos en un ancho de banda de 100 MHz. Cada uno de estos canales está dividido en 52 subcanales de 300 kHz de ancho. Cuarenta y ocho de los subcanales son utilizados para transmisión de los datos, y el resto para corrección de errores. Tres bandas de la U-NII están disponibles para el siguiente uso:

- Dispositivos U-NII 1 operan en la gama de frecuencia de 5,15 a 5,25 GHz a una potencia máxima de 50 mW, una antena de ganancia máxima de 6 dBi. Es requerido que el transmisor de radio y la antena sean una sola unidad para ser utilizados sólo en ambientes internos.
- Dispositivos U-NII 2 de la gama de frecuencias de 5,25 a 5,35 GHz, con 250 mW de potencia máxima de transmisión y antena de 6 dBi de ganancia máxima. Esto dispositivos puedes ser utilizados tanto en interiores como en exteriores, y pueden tener antenas removibles.
- Dispositivos U-NII 3 operan en la gama de frecuencias de 5,725 a 5,825 GHz. Estos dispositivos poseen máxima potencia de transmisión de 1 W y se le permiten antenas removibles, pueden operar sólo en ambientes externos. Se permiten antenas de hasta 23 dBi para conexiones punto a punto, y de 6 dBi para conexiones punto a multipunto.

En la Figura 3 se puede observar de manera gráfica las divisiones de la banda ISM de 5 Ghz.

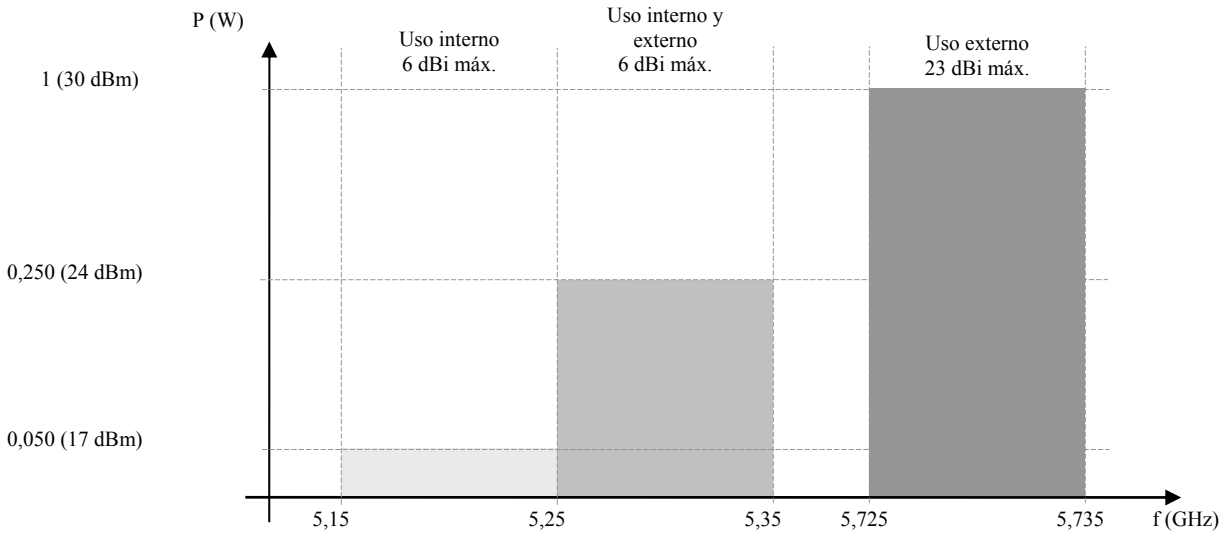

Figura 3. Distribución de bandas U-NII

4.9 Redes 802.11g

En junio de 2003 fue ratificado el estándar 802.11g, que opera en la banda de 2.4GHz a una tasa máxima de transmisión de 54Mbps. Los dispositivos 802.11g deben trabajar con los equipos compatibles con 802.11b, aunque la presencia de equipamiento 802.11b en redes 802.11g reduce significativamente el desempeño.

El tipo de modulación utilizado es OFDM para tasas de transmisión de 6, 9, 12, 18, 24, 36, 48, y 54 Mbps, y utiliza la modulación del estándar 802.11b para tasas de transmisión de hasta 11Mbps.

Para principios de 2003 ya estaban disponibles para la venta dispositivos compatibles con 802.11g, aunque el estándar fue ratificado para mediados de 2003. Para el momento de la ratificación existía enorme aceptación en el mercado de los productos compatibles, sin importar la disminución de desempeño que le producían los dispositivos 802.11b ya establecidos.

4.10 Redes 802.11n

En enero de 2004, IEEE anunció la creación de un nuevo grupo de trabajo de la familia 802.11 que desarrollaría el estándar 802.11n. Este nuevo estándar para WLAN tiene como objetivo alcanzar la tasa máxima teórica de transmisión de 540 Mbps, la cual requiere

un cambio de filosofía de transmisión a nivel de capa física, para lograr ser 100 veces más rápido que 802.11b, y unas 10 veces más rápido que 802.11g y 802.11a. Se espera también que 802.11n logre ofrecer mayor distancia de operación que las redes de la actualidad.

Existe dos propuestas en competencia para ser incluidas en el estándar 802.11n: WWiSE (World-Wide Spectrum Efficiency) respaldada por empresas como Broadcom, y TGn Sync, respaldada por Intel y Phillips. Estas empresas enviaron sus propuestas al IEEE para finales de 2005. Se espera que el proceso de estandarización sea completado en el segundo semestre del año 2006.

El estándar está basado en 802.11 y le añade la tecnología MIMO (multiple-input multiple-output) que significa múltiples entradas y múltiples salidas. MIMO utiliza múltiples transmisores y antenas que le permiten incrementar el ancho de banda de transmisión por medio de la multiplexación espacial de las señales, y aumenta el área de cobertura aprovechándose de la diversidad en espacio de las antenas.

Una institución llamada Enhanced Wireless Consortium (EWC) fue creada para acelerar el desarrollo del estándar y promover las especificaciones tecnológicas que garanticen la interoperabilidad de los productos WLAN de próxima generación.

En enero de 2006 el grupo de trabajo 802.11n aprobó la propuesta de especificaciones de la EWC, y para marzo de 2006 IEEE envió el borrador de 802.11n al grupo de mas de 500 especialistas del grupo 802.11 para que realicen su revisión, corrección, cambios y mejoras. En mayo de 2006, el grupo de trabajo 802.11 no aprobó este primer borrador del estándar, y publicó más de 12000 comentarios respecto a él. Se espera que la aprobación del estándar final ocurra para el año 2007 [2].

4.11 Roaming en las WLAN

El mecanismo roaming es el que permite a un dispositivo cliente inalámbrico cambiar su asociación de un AP a otro AP dentro de la misma WLAN, sin perder conectividad y sin que sea percibido por el usuario.

No existe ningún mecanismo especial para el roaming en la especificación 802.11, sin embargo, queda de parte de cada fabricante el definir un algoritmo para los clientes de la WLAN que les permita hacer decisiones de roaming. Actualmente el grupo de trabajo de IEEE 802.11 está trabajando en el anexo 802.11r llamado *Fast BSS Transitions*, y en cual se estandarizarán los mecanismos de *roaming*. A continuación se revisa la arquitectura de

redes Ethernet 802.3 antes de adentrarnos en cómo se podría lograr el roaming en la redes 802.11.

Las LAN basadas en Ethernet utilizan la arquitectura de acceso múltiple por detección de portadora con detección de colisiones (carrier sense multiple access / collision detect, CSMA/CD). Cuando una estación desea transmitir información a otra, primero chequea la presencia de otra transmisión en el medio y ésta es la función de detección de portadora de CSMA/CD. Todas las estaciones tienen acceso por igual al medio compartido al cual están conectadas y ésta es la característica de acceso múltiple de CSMA/CD. Si la estación detecta que el medio se encuentra libre para transmitir, entonces comenzará la transmisión. Si dos estaciones inician la transmisión al mismo tiempo, ocurrirá la colisión en las tramas que transmiten, y éstas quedarán inservibles. Las estaciones transmisoras tienen la capacidad de detectar las colisiones, función de detección de colisiones de CSMA/CD, y posteriormente ejecutar algoritmos de parada de la transmisión y retransmisión luego de un período aleatorio.

La arquitectura 802.3 fue diseñada para redes cableadas, y sus diseñadores le dejaron cierto nivel de confiabilidad en el medio cableado a través del cual se realiza la transmisión desde la estación origen hasta la destino. Por este motivo 802.3 no posee un mecanismo por medio del cual se determine si una trama ha alcanzado su estación destino, 802.3 le transfiere esta tarea y la de retransmisión de los datos perdidos a protocolos de capas superiores.

Las redes del estándar 802.11 utilizan al aire como medio de transmisión y estas transmisiones están sujetas a numerosas fuentes de interferencia. Los diseñadores del estándar tomaron en cuenta este inconveniente, e introdujeron en la capa de enlace de datos la funcionalidad de confirmación de recepción de tramas, en donde por cada trama enviada el emisor recibe una trama de confirmación de recepción (ACK) por parte del receptor.

Las estaciones clientes utilizan los mensajes ACK para determinar cuán lejos del AP se encuentra. Cuando una estación realiza la transmisión de una trama, se activa una ventana de tiempo en la cual se espera la recepción, desde el AP, de una trama ACK. Una estación logra saber cuándo se está alejando del área de cobertura del AP una vez comienza a recibir tramas ACK luego de haber expirado la ventana de tiempo.

Adicionalmente los AP envían periódicamente tramas de administración conocidas como *beacons*. Estos contienen información del AP como el identificador de la WLAN (Service Set Identifier, SSID), velocidades de transmisión soportadas, cuándo el AP soporta *direct sequencing* o *frequency hopping*, etc. Los *beacons* son tramas *broadcast* desde el AP, y se envían en intervalo regular configurable, usualmente de 100 ms.

Las tramas ACK y los *beacons* le dan al cliente la información suficiente para tomar la decisión de cuando es necesario realizar el roaming. Si una cierta cantidad de *beacons* se ha perdido, el cliente puede asumir que se ha salido de la zona de cobertura del AP al cual está asociado.

La forma de realizar el roaming varía de fabricante en fabricante. La forma básica es tomar la decisión de hacer el roaming, seguida de la localización de un nuevo AP al cual asociarse. Este escenario puede implicar el reinicio total de la búsqueda de AP de la misma forma como si el cliente fuese inicializado, u otras formas como el uso de tablas de referencias creadas en asociaciones previas.

El tiempo de roaming también varía entre fabricantes, pero en la mayoría de los casos es inferior a 1 segundo, y en los mejores casos es inferior a los 200 milisegundos. Es importante destacar que como el roaming es específico de cada fabricante, el tiempo de roaming entre AP de distintos fabricantes tiende a ser mayor.

4.12 IEEE 802.11e

Para finales de 2005 fue aprobado como un estándar el conjunto de mejoras de calidad de servicio (QoS) para las aplicaciones sobre WLAN. Este estándar es de importancia crítica cuando se utilizan, sobre una WLAN, aplicaciones sensibles al retardo como voz sobre IP (VoIP) y aplicaciones multimedia como video conferencia. Este estándar introduce mejoras en la capa de control de acceso al medio (MAC) de 802.11.

4.12.1 Capa MAC 802.11 original

Para lograr compartir el medio inalámbrico entre varios dispositivos clientes, la capa MAC de 802.11 utiliza un método de coordinación de acceso al medio llamado Distribuited Coordination Function (DCF), que se basa en CSMA/CA y el opcional 802.11RTS/CTS. Esta técnica de acceso al medio tiene las siguientes limitaciones.

- Si muchos clientes inalámbricos se intentan comunicar al mismo tiempo, entonces ocurrirán muchas colisiones que disminuirán el ancho de banda disponible
- No existe una clase de tráfico más importante que otro
- Un cliente inalámbrico puede utilizar su turno de transmisión todo el tiempo que le sea necesario. Si este cliente está transmitiendo a una velocidad baja, entonces se tardará mucho más tiempo en transmitir una trama grande, y esto afecta el ancho de banda disponible para los demás clientes
- En resumen, la QoS no está garantizada

La capa MAC original de 802.11 define un método adicional de coordinación para el uso del medio inalámbrico llamado Point Coordination Function (PCF), sólo disponible para operar bajo el modo infraestructura. Este modo de acceso al medio es opcional, y son muy pocos los fabricantes de AP y NIC inalámbricos que lo implementan. Su funcionamiento se basa en la definición de dos períodos llamados Contention Free Period (CFP) y Contention Period (CP). En el CP se utiliza DCF como mecanismo de coordinación de acceso al medio. En CFP el AP envía a cada cliente inalámbrico, uno a la vez, una trama llamada Contention Free-Poll (CF-Poll), adjudicándole el derecho de enviar una trama. El AP es quien coordina los turnos de transmisión, esto permite un mejor manejo de la QoS, desafortunadamente PCF tiene muy poco soporte y algunas limitaciones, como por ejemplo que no puede realizar la definición de clases de tráfico.

4.12.2 Operación de la capa MAC en 802.11e

El estándar 802.11e mejora DCF y PCF con la introducción de una nueva función de coordinación, la llamada Hybrid Coordination Function (HCF). Con HCF hay dos métodos de acceso al medio similares a las definidas en la capa MAC 802.11 original y estas son las funciones llamadas HCF Controlled Channel Access (HCCA) y Enhanced DCF Channel Access (EDCA). Ambas se utilizan para definir clases de tráfico, por ejemplo, al tráfico FTP se le puede asignar la clase con prioridad más baja, y al tráfico RTP de VoIP la clase con prioridad más alta.

4.12.2.1 EDCA

Con EDCA, el tráfico con mayor prioridad tiene mayor oportunidad de ser enviado que un tráfico con baja prioridad: un cliente inalámbrico con tráfico de alta prioridad espera en promedio menos tiempo para enviar sus paquetes que un cliente con tráfico de prioridad baja. Además, cada nivel de prioridad tiene asignado un valor de Oportunidad de Transmisión (TXOP). Un TXOP es un intervalo de tiempo limitado durante el cual un cliente inalámbrico puede enviar tantas tramas como le sea posible (mientras la duración de las transmisiones no se extienda más allá de la duración máxima del TXOP). Si una trama es demasiado grande para ser transmitida en un solo TXOP, esta debe ser fragmentada en tramas más pequeñas. Esto reduce el problema inducido por los clientes inalámbricos de baja velocidad de transmisión al tomar el medio de transmisión por periodos excesivamente largos.

Existe una certificación llamada WI-FI Multimedia (WMM) que obliga a los AP tener habilitado EDCA y TXOP. Todas las demás mejoras del estándar 802.11e son opcionales para esta certificación.

4.12.2.2 HCCA

HCCA trabaja de forma similar a PCF dividiendo el intervalo entre dos *beacons* en dos períodos, CFP y CP. Durante el periodo CFP, el AP controla el acceso al medio. Durante el periodo CP, todos los clientes inalámbricos utilizan EDCA. La diferencia principal con PCF es que son definidas clases de tráfico (TC). Además, el AP puede manejar el tráfico de muchas formas distintas, y no solo round-robin. Mas aún, los clientes inalámbricos envían información acerca del tamaño de sus colas para cada tipo de tráfico, y el AP puede utilizar esta información para dar mayor prioridad de acceso al medio de un cliente sobre otro.

Se considera que HCCA es el más avanzado y complejo método de coordinación de acceso al medio. La QoS puede ser configurada con gran precisión con el uso de HCCA. Los clientes con la QoS habilitada tienen la habilidad de solicitar parámetros de transmisión específicos, como velocidad de transmisión, jitter, etc., lo que permite que las aplicaciones en tiempo real como VoIP y transmisión de video tengan un desempeño mas eficiente sobre una WLAN.

4.12.3 Otras especificaciones de 802.11e

Además de HCCA, EDCA y TXOP, el estándar 802.11e especifica otros protocolos opcionales para manejo de QoS mejorado en la capa MAC de 802.11. Entre estos protocolos están:

4.12.3.1 APSD

ASDP es el acrónimo de Automatic Power Save Delivery que es un método más eficiente de la administración de la potencia de transmisión. ASDP es muy útil para un teléfono de VoIP, en donde la tasa de transmisión es prácticamente igual en ambos sentidos de la transmisión. Esto permite que el teléfono IP entre en un estado de adormecimiento cuando está recibiendo un flujo largo de paquetes de VoIP, y de esta forma se logra ahorrar energía.

4.12.3.2 BA

BA es el acrónimo de Block Acknowledgments, que permite que la totalidad de un TXOP sea respondido con una sola trama de confirmación de recepción. Este permite que se ocupe menos ancho de banda cuando se configure TXOP largos.

4.12.4 Wireless multimedia extension

El consorcio Wireless Ethernet Compatibility Alliance (WECA) ha unido un conjunto de especificaciones 802.11e como parte de su certificación Wireless Multimedia Extension (WME). La certificación de interoperabilidad WME, también conocida como WMM está basada en el borrador del estándar 802.11e. Esta proporciona características básicas de QoS a las redes 802.11. WMM divide el tráfico de acuerdo a 4 Categorías de Acceso (AC), cada categoría tiene un nivel distinto de prioridad.

5 INTRODUCCIÓN A LA SEGURIDAD EN LAS WLAN

Según el estándar IEEE 802.11, la seguridad en las redes se basa en dos componentes, cifrado y autenticación. El uso de estos dos componentes de seguridad ha sido catalogado y documentado por usuarios y fabricantes como inseguro. A continuación describiremos el funcionamiento del cifrado y la autenticación tal como la propone el IEEE.

5.1 Cifrado de tramas

Cuando el cifrado se realiza apropiadamente, éste garantiza la confidencialidad. El cifrado es un proceso mediante el cual se toma un mensaje, conocido como mensaje en texto en claro, y es pasado a través de un algoritmo matemático el cual produce lo que se llamará texto cifrado. El proceso inverso para obtener texto en claro a partir del texto cifrado es conocido como descifrado. Los algoritmos de cifrado por lo general se basan en un valor, llamado clave de cifrado, con el cual se cifran y descifran los datos. Son dos las formas de cifrado que se utilizan con mayor frecuencia en la actualidad: cifrado simétrico (conocido también como shared-key encryption) y el cifrado asimétrico (conocido también como public or private encryption). El cifrado simétrico resulta unas mil veces más rápido que el asimétrico y en consecuencia, esto hace que sea a su vez el más utilizado para el cifrado de grandes cantidades de datos. Por lo general los algoritmos de cifrado bien diseñados, en compañía de claves de gran longitud, resultan en un mayor grado de seguridad. Esto es debido a que los ataques de fuerza bruta necesitarían mayor poder de cómputo y más tiempo para lograr encontrar la clave, y así poder descifrar los datos. El IEEE ha diseñado, dentro del estándar 802.11, un mecanismo de cifrado que aseguraría un nivel de confidencialidad equivalente a las redes cableadas, llamado WEP (Wired Equivalent Privacy). WEP realiza un cifrado de las tramas 802.11 de datos utilizando el algoritmo de cifrado RC4, inventado por Ron Rivest de RSA Data Secutity Inc. (RSADSI). RC4 es un algoritmo de cifrado simétrico que permite claves de longitud variable. El algoritmo cifrador es el que realiza el cifrado y descifrado de las tramas. Este cifrador realiza cifrado de flujo (s*tream cipher*), en contraste con el tradicional cifrador de bloques, que procesa una cantidad fija de bytes para cifrado o descifrado. Con el cifrado simétrico, la clave debe ser una pieza de información conocida por ambos extremos que realizan el proceso de cifrado y descifrado. IEEE especifica que los dispositivos 802.11 deben soportar claves de una longitud de 64 bits, con la opción de utilizar mayores longitudes. Muchos fabricantes ofrecen en sus productos WLAN claves para cifrado WEP de 128 bits y más.

Dado que WEP es un cifrador de flujo, se requiere de un mecanismo que evite que el mismo texto en claro siempre produzca un mismo texto cifrado. La IEEE tiene estipulado que se utilice una vector de inicialización (IV) que combinado con la clave simétrica genere el *stream chipher*.

El IV es un valor de 24 bits de longitud que genera una gama de números de 0 hasta 16.777.215. El IEEE recomienda - pero no obliga – que el valor del IV cambie por cada trama que se envía. Dado que el emisor no tiene un esquema estándar para generar el IV, éste debe ser enviado en texto en claro en la porción de encabezado de la trama de datos 802.11. El receptor puede entonces concatenar el IV recibido con la clave compartida (Clave WEP) que tiene guardada localmente para descifrar los datos de la trama. Como se puede observar en la Figura 4, el texto en claro no es procesado por el algoritmo cifrador RC4, más bien el cifrador RC4 es utilizado para generar un *stream cipher* único que posteriormente será combinado con el texto en claro a través de la función lógica XOR, para así producir el texto cifrado.

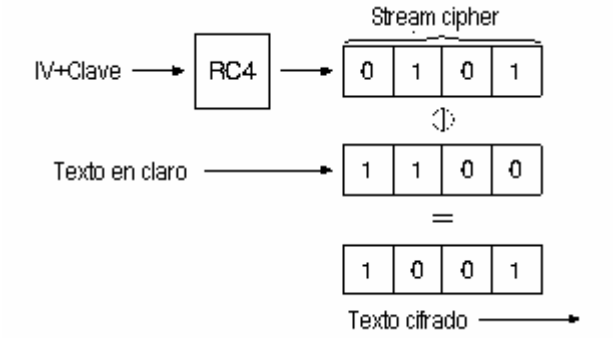

Figura 4. Algoritmo de cifrado WEP

5.2 Mecanismo de autenticación

IEEE especifica dos algoritmos de autenticación para las redes 802.11. El primero es la autenticación abierta, el cual es un algoritmo donde la autenticación es nula y cualquier cliente (que conozca el SSID de la WLAN) que realice una petición para conectarse, será aceptado y tendrá acceso garantizado. La segunda forma de autenticación es la llamada autenticación con clave compartida, la cual requiere que ambos extremos de la conexión tengan configurada la misma clave WEP. Este mecanismo de autenticación funciona de la siguiente forma: el extremo 1 realiza la petición de conexión al extremo 2 y el extremo 2 le responde enviando una trama en texto en claro, la cual es cifrada por el extremo 1 y reenviada de vuelta. El extremo 2 intenta descifrar la trama y si lo logra, quiere decir que las claves WEP coinciden y el acceso está asegurado.

Es importante destacar que la autenticación por clave compartida tiene defectos en su concepto. Dado que la trama primero es enviada en texto en claro, y luego es regresada

cifrada, un atacante puede encontrar el *stream cipher* analizando ambas tramas. Esta información puede ser utilizada para crear diccionarios de "descifrado" para determinada clave WEP. Las vulnerabilidades conocidas de WEP serán discutidas más adelante.

6 DESCRIPCIÓN DE LA ARQUITECTURA DE WLAN SEGURAS

6.1 Fundamentos de diseño

Con los siguientes fundamentos de diseño se intenta describir, lo más fielmente posible, los requerimientos funcionales de las WLAN de la actualidad. Dependiendo de las funcionalidades de red requeridas, varían las decisiones al momento de realizar las implementaciones. Sin embargo, los objetivos de diseño nombrados a continuación, en orden de prioridad, han guiado el proceso de toma de decisiones.

- Las políticas establecen las normas de seguridad y los métodos de respuesta ante ataques.
- Acceso a recursos de la red por medio de autenticación y autorización.
- Confidencialidad de los datos que se transmiten de forma inalámbrica.
- Diferenciación de los usuarios (administradores, usuarios de la red, visitantes, etc.)
- Gestión de los puntos de acceso.
- Autenticación de los usuarios que tengan acceso a los recursos de la red.
- Opciones que garanticen alta disponibilidad

La seguridad de la red inalámbrica de la empresa debe acercarse lo más posible a las políticas de seguridad implementadas, además debe brindar acceso a la red corporativa, manteniendo la mayoría de las características de seguridad que otorga la red cableada. Esto quiere decir que las WLAN deben integrarse a los lineamientos de seguridad de la red de la empresa.

6.2 Debilidades de seguridad de las WLAN

Hoy en día, las WLAN se han convertido en unos de los blancos más interesantes para los hackers. Las organizaciones y empresas están implantando rápidamente esta tecnología, y en muchos de los casos sin tomar en cuenta el aspecto de la seguridad. Esta rápida implantación se debe en parte a los bajos costos de los equipos, sencilla configuración, y altas ganancias de productividad; y dado que la mayoría de los

dispositivos de WLAN eran vendidos e instalados con todas las funcionalidades de seguridad deshabilitadas, han atraído la atención de la comunidad hacker. Es enorme la cantidad de páginas en Internet en donde se encuentran publicadas de forma gratuita las redes inalámbricas disponibles y conseguidas para realizar *wardrive*. La mayoría de los hackers utilizan estas conexiones para ganar acceso gratis e ilimitado a Internet o para ocultar su identidad, y un pequeño grupo ve esto como una oportunidad de entrar a redes a las que se le haría muy difícil atacar desde Internet. Al contrario de las redes cableadas, las WLAN envían los datos a través del aire y estos datos pueden ser accesibles incluso desde afuera de las instalaciones de la organización. Cuando los datos en una WLAN no están cifrados, los paquetes enviados de forma inalámbrica pueden ser capturados por cualquier persona que se encuentre dentro del área de cobertura de la red. Por ejemplo, una persona con una computadora portátil con el software adecuado, un adaptador de red inalámbrica, y una aplicación *sniffer*, puede recibir, ver y almacenar todos los paquetes que circulen en una WLAN.

6.2.1 Interferencia y "jamming"

También es sencillo interferir las transmisiones de una WLAN con un simple transmisor que haga imposible la comunicación. Por ejemplo, realizar constantes peticiones de acceso a un AP, sean satisfactorias o no, puede eventualmente ocupar todo el espectro de frecuencia disponible para la transmisión y disminuir gravemente el desempeño de la WLAN. Otros servicios inalámbricos que utilicen la misma gama de frecuencias que las WLAN puede reducir el área de cobertura y disminuir el ancho de banda disponible para la WLAN. La tecnología Bluetooth, utilizada para redes de área personal, es una de las tecnologías que utiliza la misma banda de frecuencias de 2,4 GHz, y puede interferir con las comunicaciones de la WLAN.

6.2.2 Autenticación por dirección MAC

Los AP pueden identificar cada una de los NIC inalámbricos que han sido fabricados mediante su dirección MAC, la cual está grabada en los circuitos de la tarjeta. Algunas WLAN requieren que sean registradas cada una de las tarjetas inalámbricas antes de otorgarles acceso, pero este escenario es complejo dado que cada AP debe conocer la lista de tarjetas que tienen acceso, y aún siendo implementado, no es posible evitar que un

hacker que cuente con una tarjeta inalámbrica equipada con el software adecuado que le permite cambiar la dirección MAC del dispositivo por alguna elegida al azar o por una deliberadamente copiada (*spoofed*) de uno de los usuarios de la WLAN. Utilizando esta dirección MAC el hacker puede inyectar tráfico a la red o puede robar la identidad de usuarios legítimos para autenticarse en la WLAN.

6.2.3 Modo Infraestructura versus modo Ad Hoc

La mayoría de las WLAN implementadas por las empresas funcionan en el llamado modo infraestructura, en el cual todos los clientes se conectan al AP para lograr todas las comunicaciones. Se puede también implementar una WLAN de modo que todas las comunicaciones se realizan en forma de redes independientes punto a punto, modo que se conoce con el nombre de Ad Hoc. En las WLAN Ad Hoc los computadores portátiles o de escritorio que cuentan con un adaptador de WLAN compatible y que se encuentren dentro de su área de cobertura pueden compartir archivos directamente, sin la intervención de un AP. El área de cobertura depende del tipo de WLAN y los equipos con dispositivos de red 802.11 pueden alcanzar distancias para redes Ad Hoc de más de 100 metros entre ellos.

El impacto de las WLAN Ad Hoc sobre la seguridad es grande. Cuando un adaptador tiene esta funcionalidad activada, un hacker podría utilizarlo como una puerta trasera para ganar acceso a la información del usuario.

6.2.4 Negación ó degradación del servicio (DoS)

Los mensajes de gestión de las redes 802.11 son los siguientes:

- beacon
- probe request o probe response
- association request o association response
- re-association request o re-association response
- disassociation
- de-auntentication

Estos mensajes de gestión son enviados y recibidos sin la necesidad de una autenticación previa y esto hace posible los ataques de negación de servicio (DoS, Denial-of-Service). Un ejemplo de estos ataques DoS puede ser demostrado con una herramienta de código abierto como WLAN-jack.

6.2.5 Puntos de acceso no autorizados

Los Puntos de Acceso no autorizados (llamados Rogue Access Point) son aquellos que son accesibles para los usuarios de la red pero no son administrados como parte de la infraestructura de red segura. Los AP no autorizados por lo general son instalados por empleados a los cuales la empresa no les da acceso a la WLAN. Un AP no autorizado es un equipo de bajo costo que el empleado compra y conecta a la red en cualquier punto de red libre, por lo general con ninguna medida de seguridad activada. Un hacker, aún estando a las afueras de las instalaciones físicas de la organización, podría ganar acceso a la red segura simplemente asociándose al AP no autorizado. Otro tipo de AP no autorizado es aquel que se disfraza para parecer un AP autorizado y engaña a los usuarios para que se asocien con él. De ésta forma el hacker puede manipular las tramas a medida que ellas fluyen a través del AP.

El uso de los AP no autorizados puede ser aplacado evitando su instalación y detectando los que hayan sido instalados.

Medidas de prevención:

- Políticas corporativas
- Seguridad física
- Implementación de una infraestructura de WLAN
- Seguridad basada en los puertos de los switches mediante 802.1X

Medidas de detección:

- Uso de analizadores o sniffers de WLAN
- Uso de aplicaciones de detección desde la red cableada
- Observación de la ubicación física y uso de los AP

6.3 Las redes 802.11 son inseguras

Como se discutió en páginas anteriores, las WLAN basadas en los estándares 802.11, 802.11b, 802.11g y 802.11a son las más ampliamente implantadas a nivel mundial hoy en día. Tradicionalmente la seguridad de una WLAN 802.11 incluye el uso de autenticación abierta o por medio de clave compartida, y privacidad basada en una clave estática WEP. Esta combinación ofrece un nivel muy básico para el control del acceso y la privacidad, dado que cada uno de los elementos puede ser comprometido. A continuación

se describen estos elementos que hacen inseguras las WLAN 802.11, y los retos que significa su implementación en ambientes empresariales.

6.3.1 Autenticación

El estándar 802.11 incluye dos métodos de autenticación: abierta y de clave compartida. La autenticación abierta consiste en proporcionar al usuario el SSID de la red. La autenticación de clave compartida consiste en que el AP le envía una trama en texto en claro a modo de reto, el cliente toma la trama, la cifra con la clave WEP y se la envía de vuelta al AP, si el AP descifra la trama devuelta mediante su clave WEP y ésta coincide con el reto, entonces se permite el acceso a la red. Si no, entonces quiere decir que el cliente no tiene la misma clave WEP y se le niega el acceso. Este tipo de autenticación no se considera segura porque si un hacker detecta la trama en texto en claro y la misma trama cifrada, entonces podría eventualmente encontrar la clave WEP.

6.3.2 Gestión de las claves

El tipo de claves más usualmente utilizada es la de claves WEP estáticas. Una clave WEP estática es una clave compuesta por 40 ó 108 bits que es definida por el administrador de la red en los AP y en todos los clientes que se comuniquen con esos AP. Cuando se utilizan claves estáticas, el administrador de la red se debe dedicar a la larga tarea de configurar la clave estática en cada uno de los dispositivos de la WLAN. Si uno de estos dispositivos es robado, podrá tener acceso no autorizado a la red, y el administrador de la red no podrá detectar el dispositivo robado, por lo tanto la clave WEP estática tendrá que ser cambiada en todos los dispositivos de la WLAN cuando sea reportado el robo. En un ambiente empresarial donde se conecten cientos o miles de dispositivos, esta situación puede llegar a ser desalentadora. Peor aún, si la clave WEP es detectada utilizando un programa como AirSnort, el administrador de la red no tendría forma de enterarse que la seguridad de la WLAN se encuentra seriamente comprometida por un hacker.

6.4 WEP

IEEE 802.11 define WEP como un mecanismo simple para proteger la transmisión, a través del aire, entre el AP y el NIC inalámbrico dentro la WLAN. WEP trabaja a nivel de capa 2, y requiere que todos los dispositivos a comunicarse compartan la misma clave

secreta. Para evitar conflictos con los controles de exportación de los Estados Unidos de América que estaban vigentes para el momento del desarrollo del estándar, se decidió el uso de claves de 64 bits, sin embargo muchos fabricantes dan soporte a claves de 128 bits opcionales en el estándar. WEP puede ser fácilmente vulnerado en ambas versiones, 64 y 128 bits, utilizando aplicaciones que se consiguen de forma gratuita en Internet. En una red con tráfico considerable se puede obtener la clave WEP en aproximadamente 15 minutos, de acuerdo con las estimaciones. Este tipo de ataques son descritos a continuación.

Como se mencionó con anterioridad, WEP utiliza el algoritmo de cifrado RC4 y éste algoritmo en un cifrador simétrico que soporta claves de longitud variable. 802.11 describe el uso del algoritmo RC4 y de la clave WEP, pero no especifica ningún método para la distribución de las claves. Sin ningún método automático de distribución de clave WEP, todo protocolo de cifrado tendrá problemas de implementación debido al potencial error humano al momento de escribir, transferir y administrar la clave. Como se discutirá más adelante en este trabajo, el estándar 802.1X fue ratificado por la IEEE como la potencial solución a ser adoptada por la comunidad WLAN para el problema de la distribución automática de las claves.

El vector de inicialización (IV) es el centro de atención al momento de hablar de la mayoría de las vulnerabilidades de seguridad que sufre WEP. Como el IV es transmitido en texto en claro y colocado en el encabezado de las tramas 802.11, cualquier persona puede ver su valor tan sólo husmeando en la WLAN. Con una longitud de 24 bits, en IV ofrece una gama de 16.777.216 posibles valores. En una publicación [3] de la Universidad de Berkeley se explica que cuando se utiliza el mismo vector de inicialización con la misma clave en un paquete cifrado (esto es conocido como colisión de vector de inicialización), un hacker puede capturar tramas de datos y derivar información acerca de los datos y de la red atacada.

En años pasados, los analistas en criptografía de la Universidad de California, Berkeley, la Universidad de Maryland y Cisco Systems Inc., reportaron [4] debilidades en los esquemas de autenticación y cifrado WEP del estándar de WLAN IEEE 802.11. Los investigadores realizaron un llamado por la creación de una solución para una administración más robusta de las claves.

Los expertos en criptografía Fluhrer, Mantin y Shamir (FMS) descubrieron defectos inherentes al algoritmo de manejo de las claves RC4. La implementación de RC4 en WEP utiliza un IV de 24 bits y no realiza rotación dinámica de las claves para cifrado. Se ha demostrado que mediante el uso de este defecto se pueden descifrar tramas 802.11 que utilicen WEP. El ataque ilustrado en esta publicación [5] se enfoca en la enorme cantidad de IV vulnerables que pueden ser generados por RC4, y resalta los métodos para descubrir las claves utilizando ciertos patrones en los vectores de inicialización. El ataque es pragmático, y es aún más desconcertante que este tipo de ataques es completamente pasivo. Esta forma de quebrantar la confidencialidad de WEP es conocido como el ataque FMS.

Las más nuevas implementaciones prácticas del ataque FMS han demostrado su capacidad de derivar un clave estática WEP mediante la captura de alrededor de un millón de tramas. Esto es demostrado en la publicación [6] de los Laboratorios AT&T y la universidad Rice.

Las implementaciones más famosas del ataque FMS, desarrolladas por implementadores independientes, son el AirSnort y el Aircrack-ng.

A pesar que la seguridad de las WLAN tradicionales se basa en autenticación abierta y en claves WEP compartidas, lo que es mucho mejor que no utilizar seguridad alguna, esta forma de aseguramiento no es lo suficientemente robusta para su uso empresarial. Sólo pequeñas empresas, o aquellas que no manejan datos confidenciales, pueden confiar en el nivel de seguridad brindado por estos métodos. Todos los demás tipos de empresas y organizaciones deben utilizar soluciones más robustas y de clase empresarial para el aseguramiento de sus WLAN.

6.5 Mejoras de seguridad adicionales al estándar 802.11

En base a los antecedentes en la seguridad de las WLAN y los fundamentos de diseño expuestos en capítulos anteriores, se realizará a continuación una introducción a los elementos de implementación de tres tecnologías que son alternativas a WEP tal como es descrito en el estándar 802.11. Las tecnologías a discutir tienen elementos de cifrado a nivel de capa de red basado en IP Security (IPSec), en autenticación mutua, métodos de distribución de claves utilizando el estándar 802.1X, y algunos elementos implementados por Cisco Systems que mejoran el desempeño de WEP.

6.5.1 IPSec

IPSec (Internet Protocol Security) es un conjunto de estándares abiertos para el aseguramiento de las comunicaciones privadas sobre las redes IP. Las redes privadas virtuales (VPN) basadas en IPSec utilizan los servicios definidos dentro del estándar IPSec para garantizar la confidencialidad, integridad y autenticidad de los datos que viajan a través de redes públicas, como Internet. IPSec tiene aplicación práctica en el aseguramiento de las WLAN, ya que se sobrepone por encima de las tramas en texto en claro del tráfico 802.11.

Cuando es implementado IPSec dentro de un ambiente WLAN, una aplicación cliente IPSec es instalada en cada PC conectada a la red inalámbrica, y es requerido que el usuario establezca un túnel IPSec a través del cual se enruta todo el tráfico hacia la red cableada. Se utilizan filtros en la red para evitar que cualquier tráfico inalámbrico alcance algún otro destino que no sea el concentrador VPN, el servidor DHCP o el servidor DNS. IPSec ofrece confidencialidad del tráfico IP, autenticación y tiene capacidades anti-replicación. La confidencialidad se alcanza utilizando una variante del Estándar de Cifrado de Datos (Data Encryption Standard, DES) llamado triple DES, o mediante el uso del Estándar de Cifrado Avanzado (Advanced Encryption Standard, AES).

En vista que IPSec es utilizado primordialmente para obtener confidencialidad de los datos y autenticación de usuario, se utilizan extensiones que permiten al estándar añadir la autenticación y autorización del usuario como parte del proceso IPSec.

6.5.2 802.1X/EAP

Una alternativa para las WLAN seguras se enfoca en la implementación de una solución que permita la autenticación centralizada y la distribución dinámica de claves. Esta solución se basa en el trabajo realizado por el grupo IEEE 802.11i. Este grupo de trabajo diseña toda una solución de extremo a extremo utilizando 802.1X y Extensible Authentication Protocol (EAP) para proporcionar funcionalidades mejoradas. Los tres principales elementos del conjunto 802.1X y EAP son los siguientes:

- Autenticación mutua entre cliente y un servidor de autenticación RADIUS (Remote Access Dial-in Service).
- Derivación dinámica de las claves para cifrado luego de la autenticación.

- Política de control centralizada, donde temporizadores de la sesión obliguen a la re-autenticación y a la generación de nuevas claves.

Cuando están implementadas estas características, los clientes inalámbricos que se asocian a un AP no tienen acceso a los recursos de la red hasta que realice el inicio de sesión a la red (network logon). Luego de la asociación, el cliente y la red (AP o servidor RADIUS) intercambian mensajes EAP para ejecutar la autenticación mutua con el cliente verificando las credenciales del servidor RADIUS y viceversa. Un mensaje de súplica EAP es usado en el cliente para obtener las credenciales del usuario, como lo son un nombre de usuario y contraseña, ID de usuario y una clave de un solo uso (one-time password, OTP), o un certificado digital. Luego de la exitosa autenticación mutua entre cliente y servidor, el servidor RADIUS y cliente en conjunto derivan una clave WEP específica del cliente, que va a ser utilizada por el cliente para inicio de sesión. Las contraseñas de usuario y las claves de sesión nunca son enviadas en texto en claro a través de la conexión inalámbrica.

La secuencia de eventos es la siguiente, y es ilustrada en la Figura 5:

- El cliente inalámbrico se asocia con al AP
- El AP bloquea cualquier intento del cliente para ganar acceso a los recursos de la red hasta que el cliente inicie sesión en la red.
- El usuario en el cliente proporciona las credenciales de inicio de sesión a la red (identificación de usuario y contraseña, identificación de usuario y OTP, o identificación de usuario y certificado digital) por medio de una súplica EAP.
- Utilizando 802.1Xy EAP, en cliente inalámbrico y el servidor RADIUS en la red cableada realizan la autenticación mutua y el servidor RADIUS verifica las credenciales del cliente. En una segunda fase, la autenticación mutua es opcionalmente completada por el cliente al verificar las credenciales del servidor RADIUS.
- Cuando la autenticación mutua es completada satisfactoriamente, el servidor RADIUS y el cliente determinan una clave WEP que es única para el cliente. El cliente carga dicha clave y se prepara para utilizarla para el inicio de sesión.

- El servidor RADIUS envía la clave WEP, llamada clave de sesión, hacia el AP a través de la red cableada.
- El AP cifra su clave de broadcast con la clave de sesión y la envía al cliente, quien utiliza la clave de sesión para descifrarla.
- El cliente y el AP activan WEP y utilizan la clave de sesión WEP y la clave de broadcast WEP para todas las comunicaciones por lo que resta de la sesión.
- Para mayor seguridad las claves WEP pueden ser cambiadas en intervalos regulares. Al final de la autenticación EAP el servidor RADIUS puede especificar al AP el tiempo de vida de la clave de sesión, y en el AP se puede configurar el tiempo de vida de la clave broadcast.

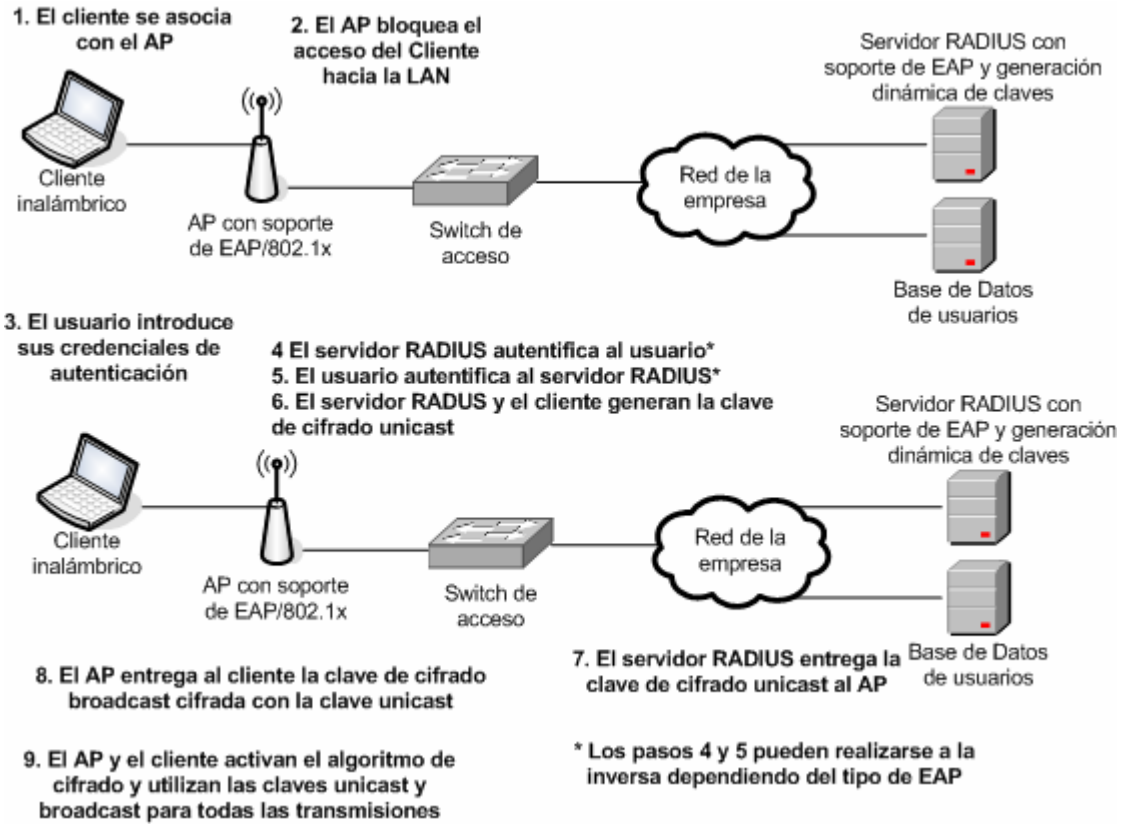

Figura 5. Proceso de autenticación EAP

EAP ofrece tres significantes beneficios a la seguridad básica de 802.11:

- El primero es el esquema de autenticación mutua, descrita previamente. Este mecanismo elimina efectivamente los ataques "Man in the Middle" (MITM), introducidos por lo AP y servidores RADIUS no autorizados.
- El segundo es la administración y distribución centralizada de las claves de cifrado. Aún suponiendo que la implementación de WEP no tuviese debilidades, es administrativamente complicada la distribución de claves estáticas a todos los AP y clientes de la red. Se elimina la situación de que cada vez que un dispositivo cliente sea extraviado, se tendrían que asignar nuevas claves a la totalidad de la red como medida preventiva al acceso no autorizado del dispositivo perdido.
- El tercero de los beneficios es la habilidad de definir políticas de control centralizadas, donde la finalización de tiempos de vida activan la generación de nuevas claves.

6.5.3 Protocolos de autenticación EAP

Hoy en día existen numerosos tipos de EAP utilizados para la autenticación de usuarios sobre redes cableadas o inalámbricas. Los más utilizados son:

- EAP-Cisco Wireless (LEAP)
- EAP-Transport Layer Security (EAP-TLS)
- Protected EAP (PEAP)
- EAP-Tunneled TLS (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)

Está documentado en la literatura de WLAN seguras que LEAP, EAP-TLS y PEAP han comprobado ser soluciones viables como protocolos EAP de autenticación mutua.

6.5.3.1 Cisco LEAP

LEAP es la implementación propietaria de Cisco de EAP para se utilizado en las WLAN. LEAP soporta los tres elementos 802.1X y EAP mencionados anteriormente. Con LEAP, la autenticación mutua se basa en una clave compartida, la contraseña de inicio de sesión del usuario, la cual es conocida por la red y por el cliente. LEAP no requiere certificados digitales en el lado del servidor ni del cliente. Como se muestra en la Figura 6, el servidor RADIUS envía un desafío de autenticación al cliente. El cliente utiliza un hash

de la contraseña proporcionada por el usuario en forma de respuesta al desafío, y envía esta respuesta al servidor RADIUS. Utilizando la información de la base de datos de usuarios, el servidor RADIUS crea su propia respuesta y la compara con la respuesta del cliente. Una vez el servidor RADIUS autentica al cliente, el proceso se repite en sentido inverso, permitiéndole al cliente autentificar al servidor RADIUS. Al completarse satisfactoriamente este proceso, un mensaje EAP de éxito es enviado al cliente, y tanto el cliente como el servidor RADIUS derivan la clave WEP dinámica.

En el año 2004 Joshua Wright publicó en Internet una aplicación llamada ASLEAP [7], la cual permite capturar tráfico de WLAN en modo pasivo para posteriormente recuperar clave LEAP ó PPTP débiles. Lo más peligroso del uso de esta aplicación es que en LEAP los nombres de usuarios y contraseñas son usualmente los mismos que se utilizan para el inicio de sesión dentro de dominios de red, y un atacante a la WLAN utilizando ASLEAP puede conseguir de esta forma acceso a la WLAN y a los recursos de la red.

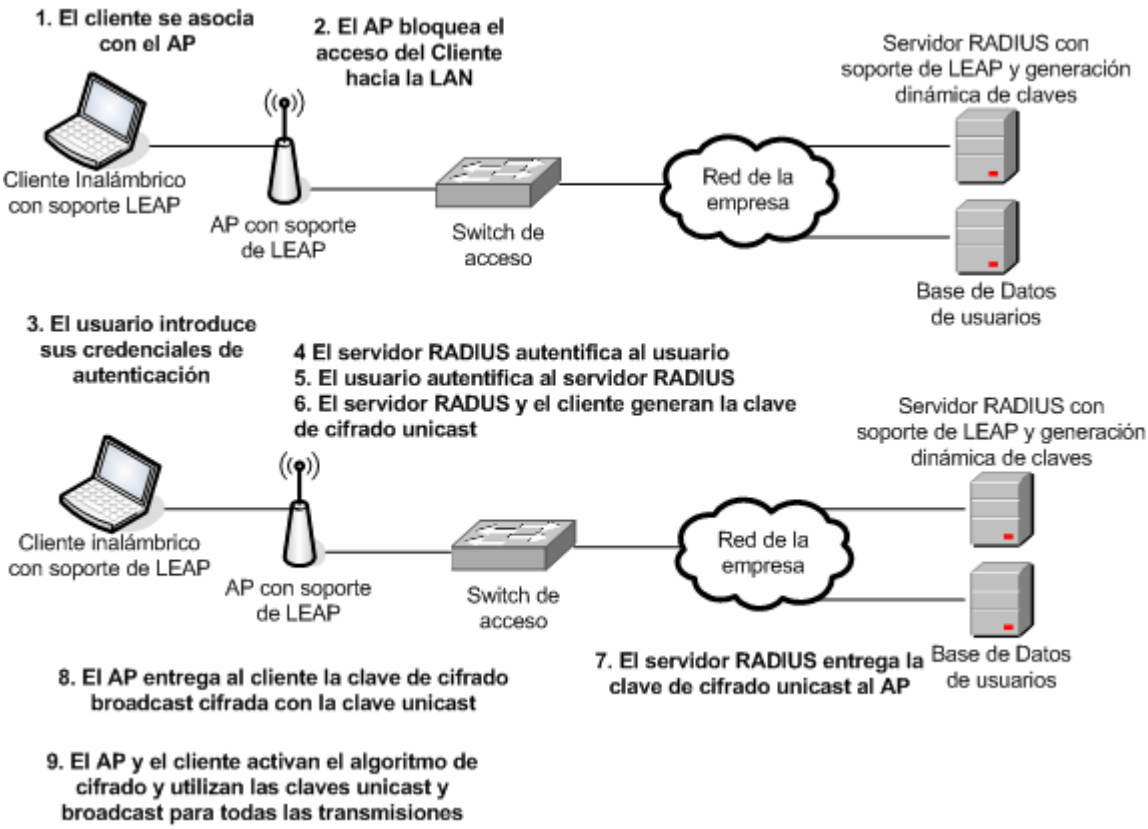

Figura 6. Proceso autenticación LEAP

En respuesta a la publicación de ASLEAP, Cisco Systems desarrolló EAP-FAST (EAP-Flexible Authentication via Secure Tunneling), protocolo de autenticación donde las credenciales del cliente son intercambiadas a través de un túnel cifrado y en donde es opcional el uso de una infraestructura de certificados digitales.

6.5.3.2 EAP-TLS

EAP-TLS es el estándar (RFC 2216) basado en el protocolo TLS (RFC 2246) diseñado por la Internet Engineering Task Force (IETF). EAP-TLS utiliza certificados digitales en el servidor de autenticación y en el cliente, y soporta los tres elementos claves de 802.1X/EAP mencionados previamente. Como se muestra en la Figura 7, el servidor RADIUS envía su certificado al cliente en la fase 1 de la secuencia de autenticación (lado servidor TLS). El cliente chequea el certificado del servidor RADIUS mediante la verificación del emisor del mismo (certificate authority server entity) y los contenidos del certificado. Al completarse la fase 1, se inicia la fase 2 de la secuencia de autenticación con el envío del certificado del cliente al servidor RADIUS (lado cliente TLS). El servidor RADIUS valida el certificando verificando su emisor y contenido. Al completarse satisfactoriamente las dos fases, un mensaje EAP de éxito es enviado el cliente, y el servidos y cliente derivan la clave WEP dinámica.

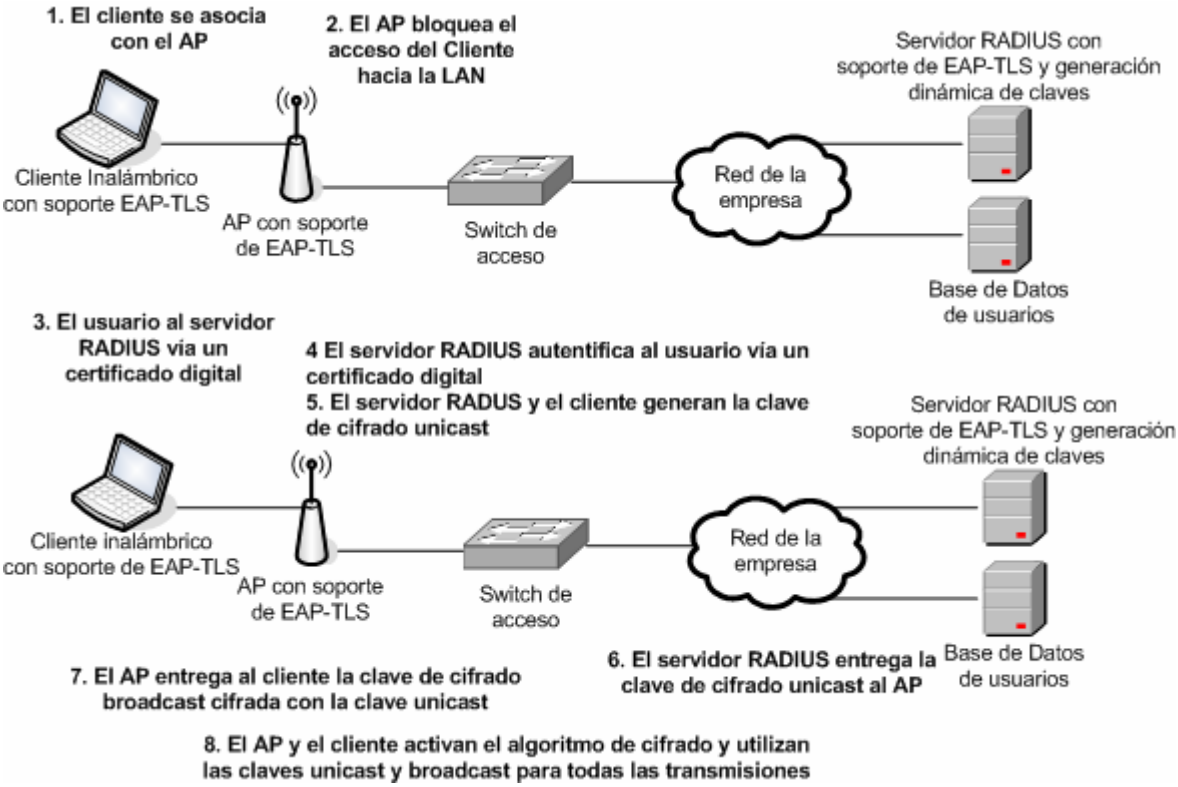

Figura 7. Proceso de autenticación EAP-TLS

6.5.3.3 PEAP

PEAP es Una propuesta para un estándar abierto desarrollado por Cisco Systems, Microsoft y RSA Security que utiliza certificados digitales para autenticación del servidor. Para la autenticación del usuario soporta varios métodos de encapsulamiento EAP a través de un túnel TLS protegido. PEAP soporta los tres elementos de la solución 802.1X/EAP descritas previamente en este trabajo. Como se puede observar en la Figura 7. Proceso de autenticación EAP-TLS, la fase 1 de la secuencia de autenticación es la misma utilizada en EAP-TLS (lado servidor TLS). Al finalizar la fase 1, se crea un túnel TLS entre el servidor RADIUS y el usuario, a través del cual se enviarán los mensajes de autenticación EAP. En la fase 2, el servidor RADIUS autentifica el cliente a través de un túnel TLS cifrado, utilizando cualquiera de los otros métodos EAP mencionados anteriormente. Por ejemplo, un usuario puede ser autentificado utilizando una OTP por medio de EAP-OTP (un subtipo de EAP definido en el borrador PEAP). En este caso el servidor RADIUS dejará las credenciales OTP (usuario u contraseña OTP) en manos de un servidor OTP que valide la

entrada del usuario. Una vez completada la fase 2, un mensaje EAP de éxito es enviado al cliente, y el servidor RADIUS y el cliente generan una clave WEP dinámica.

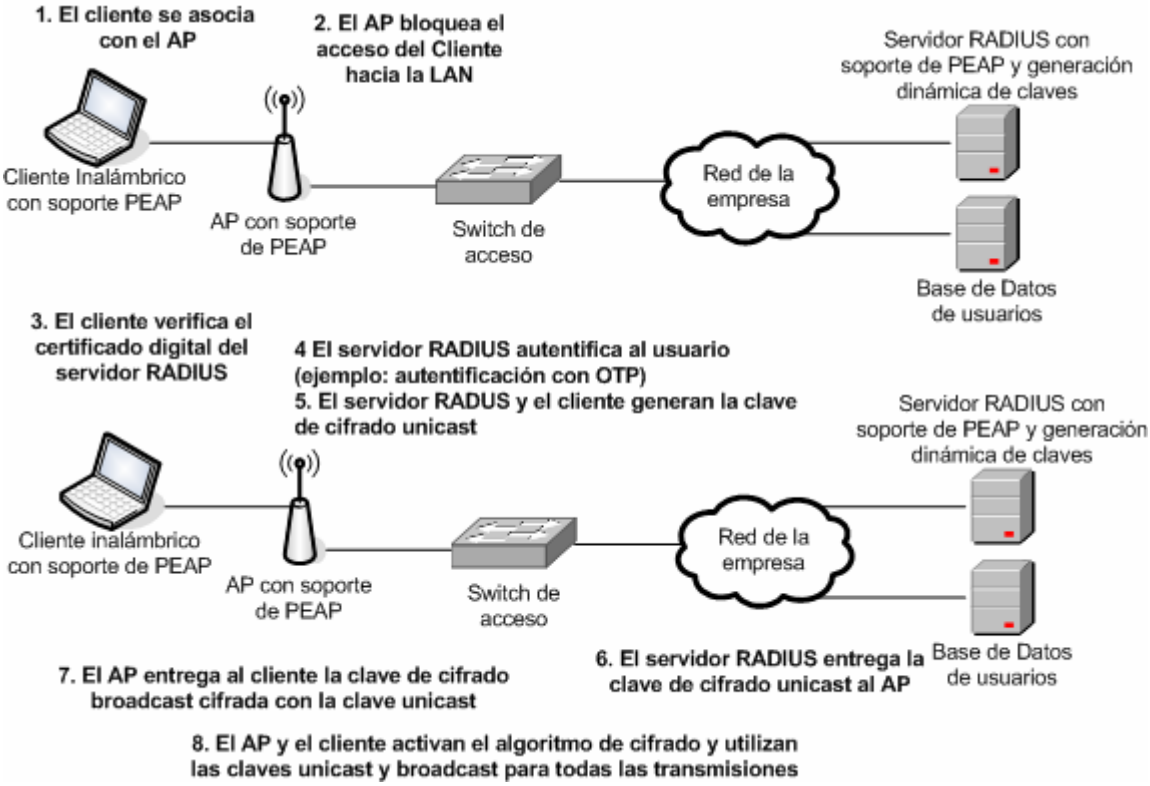

Figura 8. Proceso de autenticación PEAP

6.5.4 WPA y 802.11i

WPA (Wi-Fi Protected Access) fue creado por WECA que es una alianza de fabricantes que utilizan la marca Wi-Fi como sello de certificación a los productos WLAN que cumplen con sus especificaciones de interoperabilidad. La certificación Wi-Fi se inició en abril de 2003, y se convirtió en obligatoria en noviembre de 2003.

WPA ha sido creado para se utilizado en conjunto con un servidor de autenticación 802.1X, que cumple la función de distribuir diferentes claves a cada usuarios. Sin embargo, puede ser también utilizado en un modo menos seguro en el cual los dispositivos de red conocen una clave compartida o *pre-shared key* (de donde viene el término WPA-PSK). WECA le da el nombre de WPA-Personal a la modalidad de clave compartida, y WPA-Enterprise a la modalidad que utiliza autenticación 802.1X.

El estándar IEEE 802.11i (también conocido como WPA2) es un añadido al estándar 802.11 que especifica los mecanismos de seguridad para las WLAN. WPA

representa un subconjunto de 802.11i que fue certificado por WECA como una respuesta inmediata a las deficiencias de WEP.

WEP presenta tantas vulnerabilidades y debilidades, tal como se propone en el estándar 802.11, que se ha hecho imperativo establecer mejoras. WPA incluye dos mejoras al cifrado para aumentar la seguridad de las WLAN basadas en 802.11:

- Temporal Key Integrity Protocol (TKIP), que es un protocolo de integridad de clave temporal, conformado por un conjunto de mejoras de software a WEP basado en RC4.
- AES, que es una alternativa mucho más robusto que RC4.

En diciembre de 2001 Cisco introdujo en sus productos de WLAN soporte para TKIP pero dado que el estándar aún no había sido completado, esta implementación es un pre-estándar, y por lo general es llamada Cisco TKIP. En el año 2002, el grupo de trabajo 802.11i finalizó la especificación para TKIP, y la Wi-Fi Alliance anunció que TKIP formaría parte de WPA, el cual se convirtió en un requerimiento para la obtención de la certificación Wi-Fi para finales de 2003.

Cisco TKIP y WPA TKIP incluyen el uso de claves por paquetes (per-packet keying, PPK) y de mensajes de chequeo de integridad (message integrity check, MIC). Además WPA TKIP incluye un aumento del tamaño del vector de inicialización de 24 bits a 48 bits. A continuación se discutirán las mejoras obtenidas con TKIP cuando es implementado Cisco TKIP.

6.5.4.1 Cisco TKIP, Claves por cada paquete

El ataque más popular en contra de WEP se basa en las múltiples debilidades que presenta el vector de inicialización en un flujo de tráfico cifrado que utilice la misma clave. Por lo tanto, el uso de una clave distinta por cada paquete sería una buena forma de aminorar este tipo de ataques. Como se ilustra el la Figura 9, mediante el uso de un algoritmo hash se produce una clave única para cada paquete (clave temporal) a partir del IV y la clave WEP. La clave única es combinada con el IV, y se introduce en la función matemática XOR junto con el texto en claro.

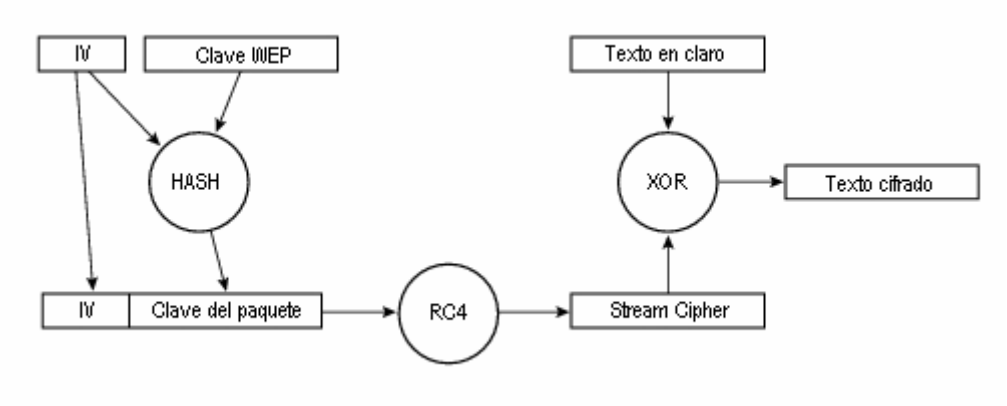

Figura 9. Uso de hash en PPK

Con este escenario se evita el uso de los IV débiles para conseguir la clave WEP, y esto es porque la clave WEP es única para cada paquete. Para prevenir los ataques basados en las colisiones del IV, la clave base debe ser cambiada antes que el IV se repita. Dado que las redes con alto tráfico pueden repetir el IV en cuestión de horas, pueden ser utilizados mecanismos de autenticación del tipo EAP en donde se solicite reautenticación periódica del cliente para la generación de nuevas claves.

Del mismo modo que las claves unicast, la clave de broadcast de una WLAN (usada por los AP y los clientes para las comunicaciones broadcast y unicast de capa 2) es susceptible a ataques cuando ocurren colisiones del vector de inicialización. Los AP Cisco soportan rotación de las claves para reducir esta vulnerabilidad. Los AP calculan dinámicamente la clave broadcast (como una función de un número aleatorio), y la clave aleatoria se entrega a los clientes por medio de mensajes EAPOL; esto obliga a que si se desea habilitar la opción de rotación automática de claves, entonces se deben habilitar protocolos EAP como LEAP, EAP-TLS y PEAP que soportan la rotación dinámica de claves.

6.5.4.2 Cisco MIC, Chequeo de integridad de mensaje

Otra de las vulnerabilidades de WEP que más preocupa es la que permiten los ataques de replicación. MIC protege a las tramas WEP de la posibilidad de ser cambiadas. El valor de MIC se basa en un valor semilla, la MAC destino, MAC origen y la carga útil, y cualquier cambio en estos valores afectará el MIC. El MIC se incluye como parte de la carga útil cifrada de la trama. El valor de MIC se obtiene a través de un algoritmo hash. Esta es una gran mejora al valor CRC-32 utilizado por el estándar basado en WEP. El

algoritmo CRC permite calcular fácilmente el cambio que un bit del mensaje haría en el valor de CRC y de esta forma un hacker podría en las condiciones adecuadas cambiar el contenido del mensaje transmitido en una WLAN, luego cambiar el CRC para hacer creer que este mensaje es el válido.

6.6 Comparación de las mejoras en seguridad

Las departamentos de IT de las empresas que desean implementar seguridad robusta en sus WLAN, deberían escoger entre la alternativa de IPSec, ó implementar 802.1X/EAP combinado con TKIP o Cisco TKIP. Las empresas que tienen una enorme preocupación en la confidencialidad de los datos que manejan, deben implementar IPSec. La alternativa 802.1X/EAP con TKIP debe ser implementada en el caso de que las empresas deseen manejar un nivel de seguridad razonable y confidencialidad en la transmisión aceptable.

Las mejoras básicas de WEP pueden ser implementadas en cualquier WLAN donde esté implementado WEP. Para la gran mayoría de las WLAN, es suficiente la seguridad ofrecida por 802.1X/EAP con TKIP. En la Tabla 1 Comparación de las tecnologías de cifrado en WLAN. se da una vista detallada a las ventajas y desventajas de los protocolos IPSec y EAP en el diseño de una WLAN.

Tabla 1 Comparación de las tecnologías de cifrado en WLAN.

	Cisco LEAP con TKIP	EAP-TLS con TKIP	EAP-PEAP con TKIP	VPN IPSec
Longitud de la clave (en bits)	128	128	128	168/128, 192, 256
Algoritmo de cifrado	RC4	RC4 ó AES	RC4 ó AES	3DES ó AES
Integridad de paquetes	CRC-32/MIC	CRC-32/MIC	CRC-32/MIC	MD5-HMAC/ SHA-HMAC
Autenticación de dispositivos	No	Certificado	Certificado	Clave compartida ó Certificados
Autenticación de usuario	Usuario/contraseña	Certificado	Usuario/contraseña ó OTP	Usuario/contraseña ó OTP
Requerimientos para certificados	Ninguno	Servidor RADIUS / cliente WLAN	Servidor RADIUS	Opcional
Diferenciación de usuarios(1)	Grupo	Grupo	Grupo	Usuario
Single sing-on (SSO)	Sí	Sí	Sí	No
Requiere listas de control de acceso	Opcional	Opcional	Opcional	Requerido
Hardware adicional	No	Servidor de Certificados	Servidor de Certificados	Concentrador IPSec
Clave única por	Sí	Sí	Sí	Sí

	Cisco LEAP con TKIP	EAP-TLS con TKIP	EAP-PEAP con TKIP	VPN IPSec
usuario				
Soporte de Protocolo	Todos	Todos	Todos	IP unicast
Soporte de Sistema Operativo de cliente	Amplio	Amplio	Amplio	Amplio
Estándar abierto	No	Sí	RFC de IETF	Sí

(1)Diferenciación de usuarios se discute en el aparte "Diferenciación de usuarios en WLAN"

6.7 Impacto de la disponibilidad de la red en la WLAN

Cuando el objetivo es diseñar e implementar una WLAN segura y de alta disponibilidad, los diseñadores de la red deben tomar en cuenta los elementos de diseño tanto de la red inalámbrica como de la cableada. Existen tres servicios relacionados con los servicios de seguridad que requieren alta disponibilidad. Estos servicios son:

- DHCP
- RADIUS
- IPSec

6.8 Diferenciación de usuarios en WLAN

En las redes tradicionales cableadas, por lo general es posible diferenciar los usuarios en grupos a través de la segmentación de capa 3, por ejemplo, para separar las redes de los departamentos de una empresa. La programación de esta segmentación se realiza habitualmente en los equipos centrales de la red, el cual es el punto principal de la red para la comunidad de usuarios; esta segmentación se mantiene a lo largo de la red realizando filtrado de las direcciones IP que tienen acceso a cada segmento. Aún así, este tipo de segmentación puede resultar compleja para los administradores, dado que las separaciones físicas y funcionales son por lo general totalmente distintas. Por ejemplo, un empleado de la compañía con acceso a sistemas de administración de la red puede estar sentado al lado de un cubículo de visitantes, el cual sólo tiene acceso a los servicios básicos de la red.

De igual modo que el mundo cableado, la diferenciación de usuarios puede ser implementada en el mundo inalámbrico aplicando el concepto de redes virtuales (VLAN). Implementaciones de múltiples estándares de seguridad (802.1X/EAP y IPSec) son soportados por múltiples VLAN inalámbricas, cada VLAN utilizando un distinto esquema

de seguridad. Una única VLAN con su SSID único puede ser enrutada a su VLAN correspondiente en la red cableada. Continuando con el ejemplo, el administrador de la red y el visitante pueden obtener acceso a la red por medio de distintos SSID. Cada SSID es enrutado a una VLAN distinta, y mejor aún, mecanismos de control de acceso a las VLAN puede ser implementado por medio del uso de un servidor RADIUS. Por ejemplo, el AP puede ubicar a un usuario administrador de la red, en la VLAN de administración, posterior a una exitosa autenticación del tipo 802.1X/EAP. Adicionalmente, con el uso de las VLAN en los AP de la empresa, se podría separar el tráfico de administración de la red del tráfico normal producido por los usuarios.

A través de la implementación de VPN basadas en IPSec se puede mejorar la diferenciación de privilegios de grupos de usuarios, sin la necesidad del uso de las VLAN. Con el uso de clientes VPN en los dispositivos de los usuarios, se puede utilizar la WLAN únicamente como medio de transporte para los datos cifrados, dejando que la VPN maneje cualquier control de seguridad. Este tipo de diseño se discutirá más adelante.

CAPÍTULO III

7 DESCRIPCIÓN DE LA RED DE DESCA

DESCA es una empresa que ha experimentado un crecimiento sostenido en los últimos años y esto ha provocado el aumento del número de empleados en todas sus oficinas, en especial la de Caracas. Todos estos nuevos de empleados se suman a la gran cantidad de usuarios que utilizan los recursos de la red corporativa, y se conectan a ella de forma cableada e inalámbrica. Los usuarios han comenzado a utilizar muchos más la conectividad inalámbrica a la red, por medio de la red WLAN corporativa de la empresa, dado que la mayoría de los equipos computacionales que se les asignan cuentan con los dispositivos de conexión 802.11.

La red de todas las oficinas de DESCA es del tipo conmutado, basada en switches centrales a los cuales se conectan todos los switches que dan conectividad a los usuarios o a los AP, A los switches principales también están conectados todos los equipos y servidores que brindan los servicios de la red corporativa de DESCA. A su vez, todas las oficinas regionales cuentan con conectividad WAN que le permite conectarse a las otras oficinas, formando de éste modo la red corporativa de la empresa.

La red de las oficinas de DESCA se puede describir como varias redes locales totalmente conmutadas (basadas en switches marca Cisco) que poseen conectividad WAN de tipo estrella por medio de un proveedor de servicios externo.

En general en las LAN de las oficinas de DESCA se cumplen con las normas de cableado estructurado, así como el dimensionamiento de los anchos de banda para las conexiones, brindando así conectividad cableada e inalámbrica a todos los usuarios.

7.1 Topología de la WAN de DESCA

La empresa DESCA está conformada por una oficina principal en Venezuela y cinco oficinas regionales en Maracaibo, Miami, México, Bogotá y Medellín. Cada una de las sedes está conectada a Internet por medio de un enlace WAN vía un ISP (Internet Service Provider) externo, a través de la cual logra interconexión con las otras. Además, las sedes de Caracas y Maracaibo están interconectadas por medio de un enlace dedicado, y ambas tienen conexiones adicionales a Internet con la tecnología xDSL.

.

En la Figura 10 se muestra el diagrama de conectividad WAN de DESCA, la cual consta de enlaces dedicados a Internet, y la comunicación entre oficinas se realiza por medio de túneles VPN para así proteger los datos transmitidos entre oficinas a través de Internet.

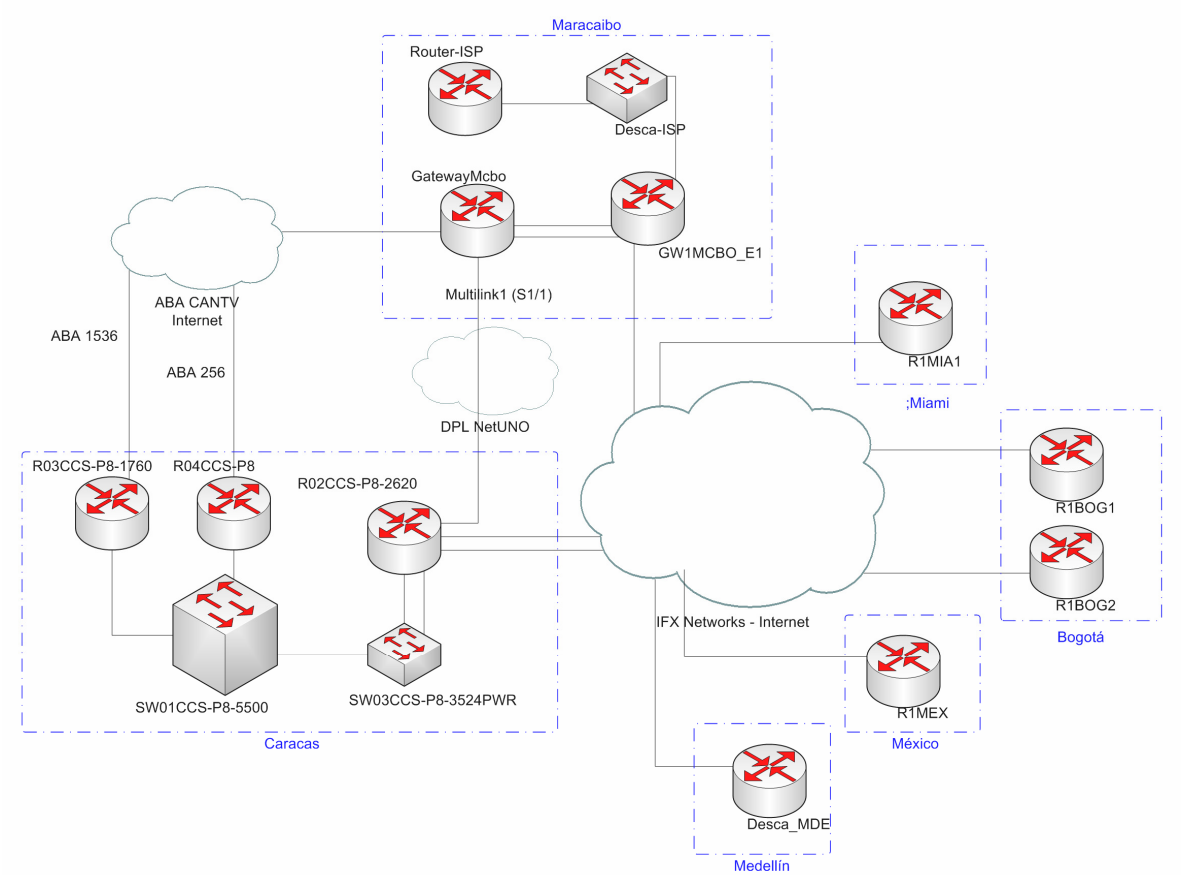

Figura 10. Red WAN de DESCA

La conectividad a Internet vía enlaces WAN se logra utilizando routers marca Cisco en cada localidad, conectados a proveedores de servicios de Internet. Esto permite que la red de cada localidad forme parte de toda única red corporativa de DESCA en donde se comparten recursos, y en la cual también se sustenta la red de telefonía IP (TIP) de la empresa.

7.2 Topología de la LAN de DESCA

Cada sede cuenta con el equipamiento necesario para ofrecer conectividad, cableada e inalámbrica, a Internet y a los recursos de la red corporativa. Entre los equipos que ofrecen conectividad en cada sede se pueden nombrar los routers, switches y puntos de

acceso. Entre los equipos que ofrecen recursos de la red corporativa están los servidores de aplicaciones, directorio activo de Microsoft, publicación de la página Web, almacenamiento, TIP, correo electrónico, conexiones remotas vía VPN, etc.

Cada localidad está conformada por una red LAN-WLAN, a la cual se accede por medio de switches y puntos de acceso de marca Cisco. El direccionamiento IP forma parte de un único plan de direccionamiento IP de la red corporativa de DESCA. Para lograr esto se han creado subredes la cuales tienen distintas longitudes de máscaras de subred con el propósito de cubrir los distintos requerimientos de direcciones para hosts, dependiendo si se trata de direcciones para interfaces de un enlace WAN, servidores, equipos de red o clientes, etc.

Cada sede cuenta con los servidores necesarios para ofrecer a los usuarios los recursos de la red, es decir, ninguna sede obtiene recursos de red de alguna otra sede remota, a menos que sea en forma de respaldo.

7.3 Topología de la LAN de DESCA en Caracas

Para este trabajo de grado se realizó el levantamiento de información de la LAN de DESCA en Caracas, que es la sede más grande de la empresa, para de esa forma realizar una propuesta de las técnicas de seguridad en las WLAN que se aplicarían de forma más idónea en esta sede. Dado que la configuración de la LAN de DESCA Caracas se repite en las demás sedes, entonces se hará sencilla la replicación de la propuesta para el aseguramiento en todas las sedes de la empresa.

Los recursos de red disponibles en la LAN de DESCA Caracas son, a grandes rasgos, los siguientes:

- Servicio Controlador de Dominio
- Servicio telefonía IP de Cisco
- Servicio de mensajería electrónica
- Servicio de mensajería unificada
- Servicio de almacenamiento
- Servicio de impresión
- Servicio de aplicaciones corporativas
- Servicio de servidor HTTP y FTP

- Servicio de gestión y monitoreo

En la Figura 11, se puede observar la distribución de los equipos en la LAN de la sede Caracas.

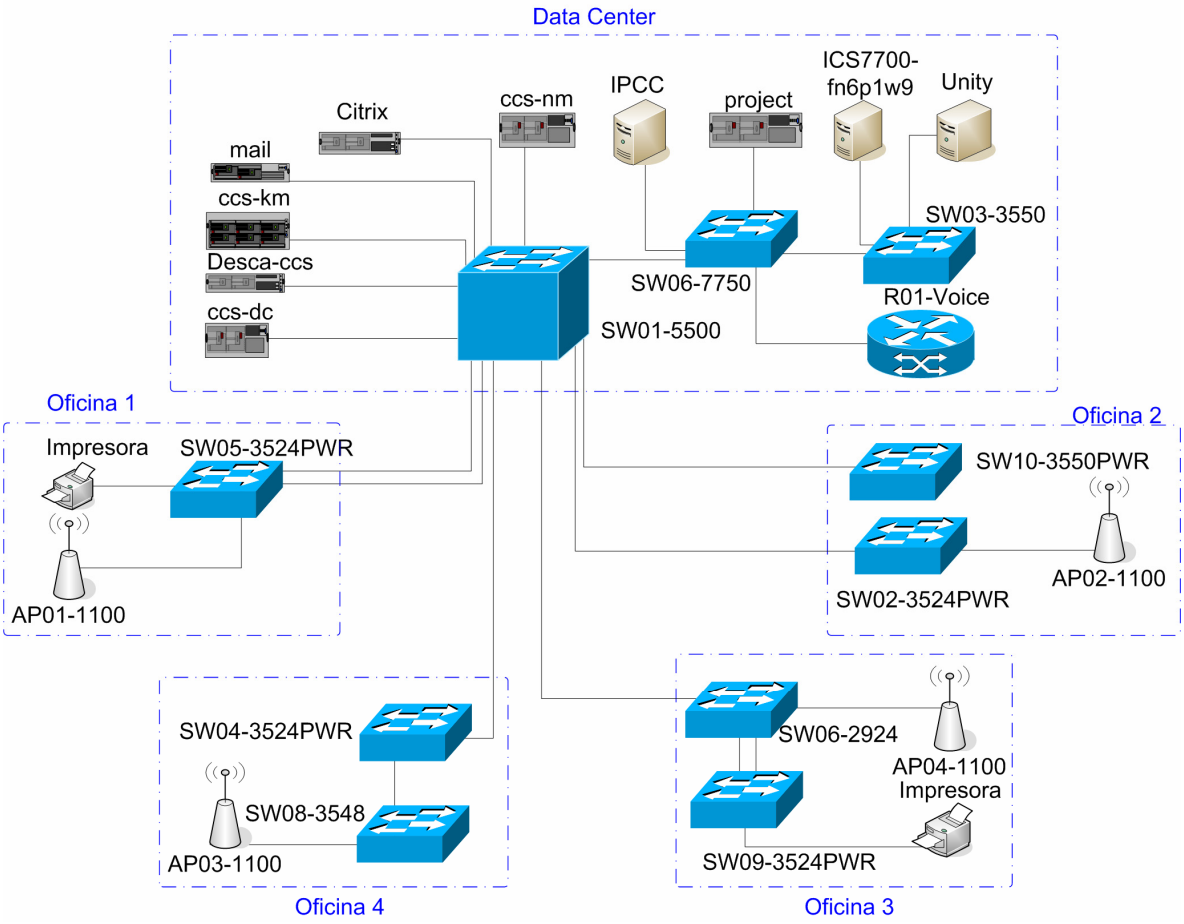

Figura 11. LAN de DESCA en Caracas

7.4 Plataforma cliente/servidor.

La plataforma de la red de datos local de la sucursal DESCA Caracas está conformada por un aproximado de 120 estaciones de trabajo con sistema operativo Microsoft Windows XP SP2, a las cuales se le brindan servicios con catorce servidores Hewlett-Packard (HP) que operan bajo los sistemas operativos Microsoft Windows 2000 Server y 2003 Server. Los servicios ofrecidos por la plataforma son accedidos por los empleados de la organización desde la LAN corporativa desde cualquier oficina y desde Internet por medio de conexiones VPN. Entre los servicios más importantes que ofrece dicha plataforma, destacan:

7.4.1 Servicio controlador de dominio

El acceso de los usuarios a los recursos y servicios de red que se describirán a continuación es manejado por un servidor HP con sistema operativo Microsoft Windows 2000 Server. Este servidor es el encargado de establecer el dominio del cual forman parte todos los servicios de la red y que son accedidos por los usuarios que están almacenados en la base de datos de usuarios. La base de datos de usuarios es manejada de forma centralizada por el administrador de la red por medio de la tecnología de Directorio Activo de Microsoft, que se encuentra alojada en el mismo servidor.

7.4.2 Servicio telefonía IP de Cisco

El servicio de telefonía IP de Cisco está instalado en servidores HP con Windows 2000 Server y la aplicación Cisco CallManager, ofrece servicio de TIP a la LAN de DESCA Caracas y el servicio de VoIP para la comunicación telefónica con todas las demás sucursales de la empresa. Presta servicio a teléfonos IP Cisco conectados a la red cableada, y a teléfonos IP Cisco inalámbricos conectados a las WLAN de la empresa.

7.4.3 Servicio de mensajería electrónica

El servicio de correo está alojado en un servidor HP con Microsoft Windows 2000 Server en conjunto con la aplicación Microsoft Exchange Server. Este servicio es accesible vía el cliente Microsoft Outlook y por medio de una interfaz Web desde Internet.

7.4.4 Servicio de mensajería unificada

El servicio de mensajería unificada es prestado por sendos servidores HP con el sistema operativo Windows 2000 Server, y con aplicaciones Cisco para la mensajería de voz, para el centro de contacto telefónico IP, y está integrado totalmente con el servicio de mensajería electrónica de la empresa.

7.4.5 Servicio de almacenamiento

Se cuenta con dos servidores HP con el sistema operativo Windows 2000 Server y Windows 2003 Server, cuya función es la de brindar almacenamiento de archivos y la facilidad de compartirlos a las distintas gerencias que conforman la empresa.

7.4.6 Servicio de impresión

Existen impresoras locales, conectadas directamente al puerto de los switches y que están compartidas a todos los usuarios conectados al dominio de la red LAN.

7.4.7 Servicio de aplicaciones corporativas

Se cuenta con 3 servidores HP, dos de ellos con sistema operativo Microsoft Windows 2000 Server y uno con Windows 2003 Server, en los cuales están instaladas aplicaciones de uso interno, como por ejemplo para el manejo de proyectos, nómina de empleados, emulador de aplicaciones, manejo de facturación e inventario, etc.

7.4.8 Servicio de servidor HTTP y FTP

El servicio FTP es ofrecido localmente por los servidores de almacenamiento de archivos, haciendo uso de un software de cliente FTP se puede establecer una sesión con estos servidores. A su vez, el servicio HTTP para la página Web interna reside uno de los servidores de almacenamiento de archivos.

7.4.9 Servicio de administración y monitoreo

Están instalados 2 servidores HP con sistema operativo Windows 2000 Server, en los cuales está instalada la aplicación Cisco Works, la cual permite el monitoreo y gestión centralizada vía HTTP de todos los dispositivos de red por medio del protocolo SNMP.

7.5 WLAN de DESCA en Caracas

La WLAN de DESCA en Caracas está integrada por 4 puntos de acceso distribuidos a lo largo de cuatro oficinas. Los AP de marca Cisco modelo Aironet 1100 están conectados a switches que poseen la facilidad de Power-in-Line, que les suministras alimentación de corriente continua a través del la conexión Ethernet. Ninguna de las áreas de cobertura de un AP se solapa con de otro.

El acceso a Internet a través de la conexión inalámbrica es abierto, y a los recursos de la red es por medio del uso de un nombre de usuario y contraseña perteneciente al directorio activo de la red.

Los dispositivos que utilizan la WLAN de la empresa son los computadores personales de los empleados y los teléfonos IP inalámbricos.

Los AP son compatibles con el estándar 802.11b, lo cual le da a la WLAN una tasa máxima de transmisión de datos de 11 Mbps, a ser repartida entre los usuarios que están conectados a la WLAN y a los teléfonos IP.

Cabe destacar que las WLAN de las otras sedes de DESCA comparten las mismas características técnicas y de configuración de la sede DESCA Caracas.

7.5.1 Características de puntos de acceso

Los AP instalados en la sede DESCA Caracas son marca Cisco, modelo Aironet 1100. Los AP Cisco® Aironet 1100 (ver Figura 12. Puntos de acceso Cisco Aironet 1100) ofrecen conexión inalámbrica según el estándar 802.11b a una velocidad de transmisión de 11 Mbps.

Figura 12. Puntos de acceso Cisco Aironet 1100

El AP cuenta con dos antenas dipolos dispuestas para diversidad en espacio para brindar una cobertura robusta en oficinas o ambientes con las mismas características de radio frecuencia. A este modelo de AP se le puede realizar una actualización de la tarjeta de radio para hacerlo compatible con el estándar 802.11g, y de esa forma alcanzar velocidades de conexión de hasta 54 Mbps, siempre garantizando la compatibilidad con los dispositivos 802.11b.

El AP es compatible con las técnicas de cifrado WEP, WPA y WPA2 y es compatible con la mayoría de los mecanismos de autenticación EAP por medio del estándar 802.1X. Además, soporta el estándar de seguridad 802.11i ya que es parte de Cisco Wireless Security Suite. En el anexo 1 se encuentran las especificaciones técnicas de este equipo.

En la Tabla 2. Especificaciones relevantes del AP Cisco Aironet 1100 se presenta un listado de las características principales que ofrece este modelo de AP.

Tabla 2. Especificaciones relevantes del AP Cisco Aironet 1100

Característica	Beneficio
Radio 2.4 GHz 802.11b, Potencia de salida configurable hasta 100 mW	Ofrece tasa de transmisión de hasta 11Mbps en la banda de 2.4 GHz.
Cifrado AES asistida por hardware	Ofrece alto nivel de seguridad sin provocar degradación del rendimiento.
Calidad de Servicio (QoS)	Le asigna prioridad al tráfico según los requerimientos de las aplicaciones. Mejora la experiencia del usuario en las aplicaciones de audio y video.
Multimedia Wi-Fi (WMM)	Es un subconjunto de normas del borrador del estándar de QoS IEEE 802.11e, que prioriza las tramas de multimedia utilizando el método EDCA. Mejora la experiencia del usuario en las aplicaciones de audio, video y voz sobre la conexión a la WLAN.
Multiples SSID (MBSSID)	Soporta la configuración de hasta 8 SSID diferentes, para mayor flexibilidad al momento de segmentar el tráfico.
Montaje flexible con orientación variable	Puede ser instalado en distintos lugares, incluyendo paredes, techo, escritorios o tabiquería.
Antenas dipolos con diversidad en espacio integradas	Ofrece cobertura omnidireccional. La diversidad en espacio ofrece cobertura mejorada en ambientes con alto efecto de multi-trayectoria.
Selección de canales automática	Determina y selecciona el canal de transmisión menos congestionado.
Soporte para Inline Power over Ethernet	Elimina la necesidad de una toma corriente alterna local. Reduce la cantidad de cableado Facilita la instalación en lugares remotos

Los AP están ubicados en cada una de las 4 oficinas, dispuestos sobre escritorios y conectados al switch correspondiente de la oficina mediante un cable UTP.

7.5.2 Características de los dispositivos clientes

En las sedes de DESCA existen dos tipos de dispositivos clientes que utilizan la WLAN de la empresa, estos son los computadores personales y los equipos telefónicos IP inalámbricos.

En la WLAN de DESCA de Caracas se conectan aproximadamente 100 computadores portátiles de distintas marcas y modelos, todos ellos utilizan el sistema operativo Microsoft Windows XP en la versión SP2, que por política de seguridad se actualiza automáticamente. En la Tabla 3 se presenta un resumen de los modelos de computadores portátiles de los usuarios de la WLAN de DESCA de Caracas, acompañado de las especificaciones de seguridad soportadas por sus dispositivos de red inalámbrica.

Tabla 3. Especificaciones de los NIC inalámbricos de DESCA Caracas

Marca	Modelo	Estándar	WEP (bits)	WPA	WPA -PSK	WPA 2	LEAP	PEAP	EAP-TLS	TKIP	AES
Compaq	EVO-N610C	802.11b	128	no	no	no	si	si	si	si	no
Compaq	nx9010	802.11b/g	128	si	no	no	si	si	si	si	no
Compaq	nx9040	802.11b/g	128	no	no	no	si	si	si	si	no
Lenovo	Thinkpad R50e	802.11b	128	no	no	no	no	si	si	si	no
Lenovo	Thinkpad T30	802.11b	128	no	no	no	no	si	si	si	no
Lenovo	Thinkpad T41	802.11b	128	si	si	no	si	si	si	si	no
Lenovo	Thinkpad T42	802.11a/b/g	128	si	si	si	si	si	si	si	si
Lenovo	Thinkpad T43	802.11a/b/g	128	si	si	si	si	si	si	si	si

Como se puede observar en la Tabla 3, las características comunes de seguridad que comparten todos los dispositivos de red inalámbrica son: cifrado WEP de 128 bits y TKIP, soporte para el estándar de autenticación 802.1X PEAP de Microsoft y EAP-TLS.

Los equipos de telefonía IP de Cisco utilizados en la red inalámbrica de DESCA Caracas son los modelos 7920 y están actualmente en uso cuatro de ellos.

El teléfono IP inalámbrico 7920 de Cisco ofrece comunicación inalámbrica bajo el estándar 802.11b con el CallManager de Cisco en conjunto con los AP de la serie Aironet de Cisco. Este ofrece movilidad, seguridad, calidad de servicio y opciones de administración a lo largo de la red corporativa de la empresa. Entre las especificaciones técnicas más relevantes de este equipo están:

- Radio compatible con el estándar 802.11b que opera en la banda de 2,4 GHz

- Soporte para los codecs de compresión de audio G.711a, G.711u, y G.729
- Soporte para configuración estática o por DHCP de parámetros IP
- Soporte para TFTP
- Soporte para CDP (Cisco Discovery Protocol)
- Soporte para el estándar 802.1q para la configuración automática de las VLAN
- Cifrado WEP de 40 bits y 128 bits, WPA, WPA-PSK, TKIP y MIC
- Soporte para autenticación 802.1X LEAP de Cisco

7.5.3 Necesidad de una WLAN en DESCA Caracas

En la red de DESCA Caracas más del 80% de los usuarios cuenta con un computador personal con la capacidad de conexión a la WLAN, y aunque la mayoría de los puestos de trabajo poseen uno o dos puntos de red cableada y que la velocidad de conexión vía la red cableada es por mucho superior a la de la WLAN, los usuarios tienen preferencia por el uso de la WLAN en vez de la red cableada. Esto se debe a la gran movilidad que ofrece la WLAN a usuarios que se muevan dentro de la oficina.

Es por ello, que en pro de ofrecer a los usuarios mayores facilidades para el desarrollo de sus actividades laborales, la WLAN forma en su totalidad parte de la red corporativa de la empresa, es decir, los recursos y servicios de red que son accesibles desde la red cableada, también lo son desde la WLAN.

7.5.4 Seguridad en la LAN de DESCA Caracas

El acceso a los recursos de la red de DESCA Caracas se logra si la conexión al domino de la red se realiza utilizando un nombre de usuario y contraseña que sean parte de la base de datos del Directorio Activo. Ahora bien, cualquier computador personal conectado a la WLAN puede obtener una dirección IP válida de la gama definida por los servidores DHCP, y podrá tener acceso a Internet y conectividad a los demás equipos de usuarios de la red, más no podrá compartir archivos con ellos ya que no pertenecen al mismo dominio. El acceso a todos los recursos de la red es manejado por el servidor de Controlador de Dominio.

7.5.5 Seguridad en la WLAN de DESCA de Caracas

El nivel de seguridad de la WLAN es el mismo de la red cableada, con la desventaja que la conectividad puede ser alcanzada en cualquier lugar dentro del área de cobertura de los AP, incluso fuera de las oficinas y en los pisos superiores e inferiores.

Para lograr asociarse a la WLAN sólo debe ser configurado en el dispositivo cliente el SSID de la WLAN el cual, aunque no es publicado en forma de broadcast por los AP, puede ser obtenido fácilmente con una herramienta de monitoreo de WLAN como Kismet.

La conectividad inalámbrica a la WLAN de DESCA no cuenta con los mecanismos apropiados para brindar un nivel de seguridad adecuado a la de una empresa, ya que no se garantiza la confidencialidad ni la integridad de los datos que cursan a través de ella.

Los teléfonos IP inalámbricos también se conectan a la WLAN configurándoles un SSID exclusivo de la VLAN de voz, VLAN en donde se encuentran conectados todos los equipos que brindan los servicios de telefonía sobre IP. La VLAN de voz de la red de DESCA tiene configuradas las políticas de QoS apropiadas para el tráfico de VoIP, pero en cuanto a seguridad, tiene las mismas deficiencias que la WLAN de los equipos de la red de datos.

7.5.6 Gestión de red de DESCA Caracas

La gestión de los dispositivos que ofrecen conectividad a la red se realiza por medio de sesiones Telnet, protocolo de acceso remoto que es muy inseguro, y su autenticación se realiza con usuarios locales y contraseñas configurados manualmente en cada equipo.

No existe ningún mecanismo de autorización de comandos ni de trazabilidad de los mismos. Esto quiere decir, que cualquier usuario conectado a la red, y que tenga el conocimiento del direccionamiento IP interno y las contraseñas de los equipos, puede realizar modificaciones en las configuraciones de los equipos de red sin que quede registrado ninguno de los cambios para una posterior auditoria.

7.5.7 Perfil de los usuarios de la red de DESCA Caracas

En la red de DESCA no existe una clasificación de los usuarios y dado que no se cuenta con un servidor AAA, no se puede realizar diferenciación de usuarios. Pero empíricamente se puede dividir en dos tipos de usuarios, usuarios comunes y usuarios con derechos administrativos.

Los usuarios comunes son lo que tienen acceso a los recursos de la red por medio de su nombre de usuario y contraseña definidos en el directorio activo. Estos acceden a la red a través de la conexión cableada o inalámbrica. En general estos usuarios no tienen conocimiento de los riesgos de seguridad que implica el uso de la WLAN, y tampoco muestran interés por aumentar los niveles de seguridad de su conexión inalámbrica.

Los usuarios administrativos son los que cuentan con la autorización y las claves para realizar labores administrativas en los equipos de la red, labores de administración que no están respaldadas por un servidor AAA en donde se podría realizar autenticación del usuario, autorización de los comandos utilizados, y llevar un registro de los cambios realizados por cada usuarios para efectos de auditoria.

CAPÍTULO IV

8 PROPUESTAS DE DISEÑO

En este capítulo se resuelven de forma general las vulnerabilidades de seguridad expuestas en capítulos anteriores. Se integran las vulnerabilidades y técnicas de defensa explicadas en los fundamentos de diseño a la red de la Empresa, con el fin de realizar una comparación y luego recomendación en cuanto a qué solución adoptar. Las soluciones a exponer están adaptadas al nivel de seguridad y al tamaño de la red en estudio, y se presentan las ventajas y desventajas específicas de cada tecnología para tener una base sobre la cual decidir cual implementar. Las dos principales opciones de las cuales elegir son:

- Implementación de WEP/WPA con claves dinámicas utilizando el modelo 802.1X/EAP con TKIP.
- Implementación de una VPN sobrepuesta a la WLAN mediante el uso de IPSec.

8.1 Principios básicos de diseño de una WLAN segura

A continuación se discutirán los elementos básicos a tomar en cuenta en el diseño de una WLAN segura. Dado que son elementos básicos, estos se incluirán con algunas variaciones en las propuestas a ser presentadas para su implementación en la red de DESCA. Se asumirá en este diseño, que la mayoría de los servicios disponibles en la red cableada estarán también disponibles en la red inalámbrica.

Se tomarán en cuenta los siguientes principios de seguridad para la WLAN:

Recomendaciones para seguridad en los Puntos de Acceso:

- Uso de autenticación de usuario centralizada (RADIUS, TACACS+).
- Implementación y cambio frecuente de nombres robustos de comunidades de Protocolo Simple de Administración de Redes (SNMP).
- Tomar en consideración el uso de comunidades de sólo lectura para SNMP.
- Deshabilitación de cualquier protocolo de gestión no esencial que sea ofrecido por el fabricante.
- Utilización de protocolos seguros de gestión, por ejemplo Secure Shell Protocol (SSH).

- Confinar el tráfico de gestión a una única VLAN de la red cableada.
- Aislar el tráfico de gestión, separándolo del tráfico de usuario, y de ser posible cifrarlo.
- Habilitar el cifrado de las tramas inalámbricas.
- Asegurar físicamente los puntos de acceso.

Recomendaciones de seguridad para los clientes:

- Deshabilitar el modo Ad Hoc

8.1.1 Elementos básicos de diseño EAP con TKIP

En este diseño se expone el método genérico de implementación de EAP con TKIP como mecanismo de seguridad para acceder a la red cableada a través de la WLAN. Ver Figura 13.

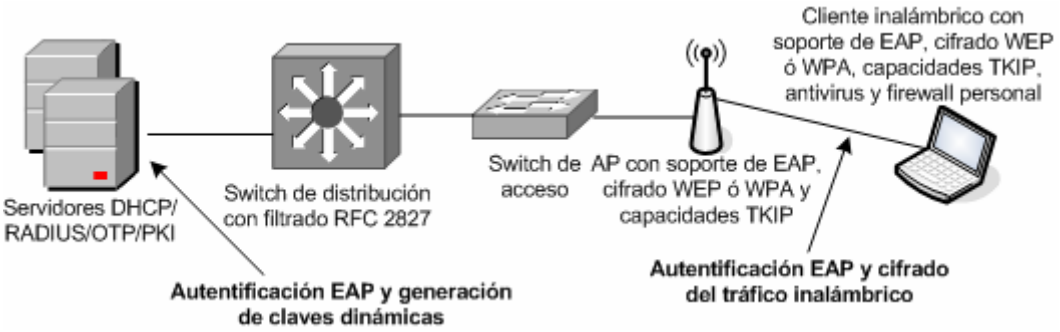

Figura 13. Diseños estándar de una WLAN con EAP

8.1.1.1 Dispositivos claves para EAP

Adaptador de cliente inalámbrico y software: que ofrezca los elementos necesarios para lograr comunicación inalámbrica con el AP, mediante la cual se establezca la autenticación mutua. Es necesario que el cliente cuente con soporte apropiado para el tipo de autenticación EAP.

Punto de acceso inalámbrico: que se autentifique mutuamente con los clientes vía EAP, y que soporte múltiples VLAN para la diferenciación de los usuarios.

Switch capa 2 ó 3: para la conectividad Ethernet y filtrado de capa 3 ó 4 entre los AP y la red de cableada. Filtrado descrito en el RFC 2827.

Servidor RADIUS: para autenticación basada en usuarios para los clientes inalámbricos y los AP. Adicionalmente, el servidor RADIUS se puede utilizar para

especificar los parámetros de control de acceso de los usuarios y grupos de usuarios a las VLAN específicas.

Servidor DHCP: Para configuración IP de los clientes inalámbricos.

Servidor OTP (opcional): para la autorización de la información OTP brindada por el servidor RADIUS, sólo aplica para clientes PEAP.

Servidor PKI (Public Key Infrastructure) (opcional): para la emisión de certificados digitales X.509v3 para la identificación de servidores y usuarios.

8.1.1.2 Amenazas mitigadas

Sniffer de paquetes inalámbricos: Se puede utilizar un sniffer de redes inalámbricas para sacar provecho de cualquiera de los conocidos ataques a WEP que intente conseguir la clave de cifrado. Esta amenaza es aminorada con las mejoras que se pueden aplicar a WEP, específicamente con TKIP para la rotación de las claves WEP, y con WPA.

Acceso no autentificado: Sólo los usuarios autentificados tienen acceso a la red inalámbrica y cableada. Adicionalmente se pueden utilizar lista de control de acceso en los switches de capa 3 para limitar el acceso a la red cableada.

Ataque MITM: La naturaleza de autenticación mutua de los distintos tipos de autenticación EAP, combinado con MIC, puede prevenir que los hackers se coloquen en el medio de la comunicación inalámbrica.

IP Spoofing: sin haberse autentificado con la WLAN, y después del opcional filtrado RFC 2827 de switch capa 3, un hacker no puede realizar IP Spoofing de la gama de direcciones de la subred local.

ARP Spoofing: los hackers no podrán realizar ARP Spoofing sin antes autentificarse con la WLAN, aunque luego de la autenticación se podría realizar un ataque ARP Spoofing para interceptar los datos de otro usuario de la misma forma que se realiza en una red cableada.

Descubrimiento de la topología de la red: mientras un hacker no se logre autentificar no podrá realizar descubrimiento de la topología de la red. El atacante se puede enterar de la existencia de una red inalámbrica mediante su SSID, pero no puede acceder la red. Posteriormente a la autenticación vía EAP, el descubrimiento de la topología de la red se puede realizar de la misma forma que es posible en un ambiente de red cableada.

8.1.1.3 Amenazas no mitigadas

Ataques de contraseñas: los mecanismos EAP toman en consideración que un atacante puede monitorear pasivamente el tráfico 802.1X/EAP entre un cliente y el AP, y se encargan de este problema con varios métodos. PEAP mitiga esta vulnerabilidad por medio de la creación de un túnel TLS entre el cliente y el servidor, y a través del túnel se intercambian las credenciales de autenticación de usuario. Además, dado que EAP-PEAP aprovecha otros tipos de autenticación EAP cliente-servidor, se puede elegir implementar métodos más robustos de autenticación como lo es OTP. EAT-TLS mitiga esto vía criptografía de claves públicas (PKI), ver Tabla 4.

Tabla 4 Mitigación de amenazas de seguridad con 802.1X/EAP con TKIP.

Ataque	Cisco LAEP con TKIP	EAP-TLS con TKIP	EAP-PEAP con TKIP
Ataque MITM (ataque activo)	Mitigado	Mitigado	Mitigado
Autenticación Forjada	Mitigado	Mitigado	Mitigado
Ataque Pasivo (ataque FMS)	Mitigado	Mitigado	Mitigado
AP no autorizados	Mitigado	Mitigado	Mitigado
Ataques de diccionario.	Vulnerable(1)	Mitigado	Mitigado
Spoofing	Mitigado	Mitigado	Mitigado

(1) Se recomienda el uso de una política robusta de contraseñas para mitigar ataque de fuerza bruta contra LEAP. EL administrador debe además configurar el límite de intentos de acceso para bloquear la cuenta.

8.1.1.4 Lineamientos de diseño de EAP con TKIP

Un diseño de red seguro se logra al prevenir el acceso de usuarios no autentificados a la red. El proceso de autentificación ocurre en el servidor RADIUS, así como la mayoría de las técnicas de mitigación de los riesgos de seguridad en las WLAN. Por esta razón se debe garantizar la alta disponibilidad del servicio RADIUS.

Los clientes inalámbricos y los AP utilizan EAP para autentificar los dispositivos clientes y los usuarios finales de la WLAN contra el servidor RADIUS. Con fines de escalabilidad y administración, los dispositivos están configurados para utilizar DHCP para su configuración IP. DHCP se activa después que el dispositivo y el usuario se ha autentificado satisfactoriamente contra el servidor RADIUS vía un protocolo EAP. Luego

de una satisfactoria configuración DHCP, los clientes inalámbricos ganan acceso a la red corporativa y el filtrado capa 3 ocurre, si está configurado. Este tipo de solución hace que el proceso a acceso seguro a la red se vea obstaculizado al fallar el servidor DHCP. Por lo tanto, para garantizar gran disponibilidad de los servicios de red para los usuarios inalámbricos, se debe dar consideración especial al lugar de la red donde se colocan los servidores RADIUS y DHCP que son usados por EAP.

Para diseño a gran escala, se debe considerar la escalabilidad del servidor RADIUS. Por ejemplo, soluciones de balanceo de carga de servidores entre múltiples servidores RADIUS.

8.1.1.5 Lineamientos específicos de diseño para el protocolo EAP

Para EAP-TLS, se recomienda el uso de PKI para la emisión de los certificados digitales. Esto permite la integración de la infraestructura PKI con las bases de datos de usuarios, por ejemplo, el directorio activo de Microsoft, para la administración de los certificados.

Para EAP-TLS y EAP-PEAP, se recomienda la configuración en los clientes inalámbricos de un certificado digital, y evitar que los usuarios comunes puedan modificar esta configuración. Sólo el administrador de IT debe tener los privilegios suficientes para modificar esta configuración en los clientes inalámbricos. Si no se configuran certificados digitales confiables, emitidos por una autoridad de certificados, se haría posibles ataques de MITM vía la usurpación de identidad (spoofing).

Para EAP-TLS y EAP-PEAP, cuando se utilizan contraseñas estáticas, se recomienda el bloqueo de cuentas luego de algunos intentos fallidos de login. Las cuentas de usuarios se bloquean para evitar ataque de fuerza bruta en una cuenta de usuario. El número de intentos fallidos se especifica en el servidor RADIUS, y además es recomendable que se les solicite a los usuarios el cambio constante de las contraseñas. Otra opción para mitigar estas amenazas es mediante el uso de OTP para la autenticación del cliente.

Para EAP-TLS, se recomienda que el servidor RADIUS se configure para el chequeo de la lista de revocación de certificados (certificate revocation list, CRL) de la autoridad emisora, en la búsqueda de clientes con certificados expirados.

Adicionalmente, se puede considerar la implementación de una VLAN exclusiva para la WLAN en conjunto con el diseño EAP. Utilizando el servidor RADIUS y configurando grupos de usuarios, puede ser implementada la asignación dinámica de VLAN para los usuarios EAP. Esto ofrece la ventaja de separar los usuarios inalámbricos en comunidades de usuarios, y permite el uso de distintas políticas de acceso para estos grupos. Mediante el uso de VLAN en los AP, el tráfico de gestión puede ser aislado del tráfico de usuarios comunes, con la implantación de una VLAN de administración en los AP.

8.1.2 Elementos básicos de diseño VPN

A continuación se describirá la técnica genérica para el uso de IPSec VPN como un mecanismo de seguridad para acceder a la red corporativa desde una WLAN. Ver Figura 14.

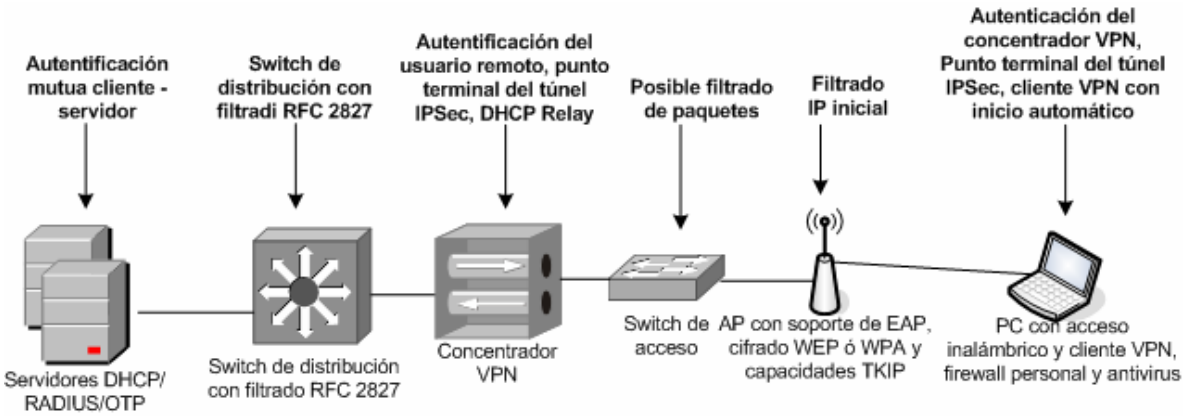

Figura 14. Mitigación de ataques es el diseño de la WLAN con VPN

8.1.2.1 Dispositivos claves para VPN

Adaptador de cliente inalámbrico y software: que ofrezca los elementos necesarios para lograr comunicación inalámbrica con el AP.

Cliente VPN de acceso remoto con software de firewall personal: una aplicación cliente que permita la conexión entre cliente PC individuales y el Concentrador VPN corporativo a través de un túnel cifrado. El software de firewall personal ofrece protección individual a cada PC.

AP inalámbrico: que ofrezca el filtrado IP inicial entre la WLAN y la red corporativa.

Switch capa 2: para conectividad Ethernet entra los AP inalámbricos y la red corporativa. Adicionalmente, se puede contar con switches que posean la capacidad de utilizar listas de control de acceso en VLAN (VLAN ACL, VACL), que permite filtrado adicional a nivel de IPSec.

Switch capa 3: que enrute y conmute los datos de la red corporativa, y además ofrece facilidades de filtrado de protocolos para el tráfico inalámbrico, lo que ayuda a reforzar las políticas de acceso.

Servidor RADIUS: autentifica usuarios inalámbricos que llegan al concentrador VPN, adicionalmente, puede negociar con un servidor OTP.

Servidor OTP: Emite información OTP solicitada por el servidor RADIUS.

Servidor DHCP: entrega la configuración IP a los clientes inalámbricos antes y después de establecida la VPN.

Concentrador VPN: autentifica individualmente a los usuarios inalámbricos remotos y es el final del túnel cifrado, además, puede ofrecer funcionalidades de DHCP para los clientes inalámbricos.

8.1.2.2 Amenazas mitigadas

Sniffer de paquetes inalámbricos: esta amenaza se mitiga mediante el cifrado del tráfico inalámbrico. Adicionalmente, mejoras en las aplicaciones VPN cliente permiten al diseñador de la red especificar que el túnel VPN sea iniciado una vez asignada al cliente la dirección IP correcta de la WLAN. Esto elimina la interacción del cliente con el software para levantar el túnel IPSec, y además protege al PC cliente de transmitir tráfico broadcast al medio inalámbrico que puede ser utilizado para ataques basados en interferencia.

Ataques MITM: se mitiga mediante el cifrado IPSec y la autenticación del tráfico inalámbrico del cliente.

Acceso no autorizado: para el tráfico entre la WLAN y la red corporativa se permiten únicamente los protocolos para la configuración IP inicial (DHCP) y el acceso VPN (DNS, Internet Key Exchange [IKE], y Encapsulating Security Payload [ESP]), a través del filtrado en el AP y switch. Adicionalmente, pueden ser configuradas en el concentrador VPN políticas de autorización para distintos grupos de usuarios.

IP Spoofing: los hacker pueden introducir tráfico en la WLAN, pero sólo los paquetes válidos y autentificados podrán llegar hasta la red corporativa.

ARP Spoofing: estos ataques pueden ser ejecutados, pero como los datos están cifrados hasta el concentrados VPN, los hackers jamás podrán leer su contenido.

Ataques de contraseñas: estas amenazas pueden ser disminuidas con la implementación de buenas políticas de contraseñas, y opcionalmente con OTP.

Descubrimiento de topología de la red: desde el segmento de la WLAN hacia la red corporativa sólo son permitidos los protocolos IKE, ESP, DNS y DHCP. Se recomienda que para propósitos de resolución de problemas se habilite ICMP desde las interfaces salientes del concentrador VPN.

8.1.2.3 Amenazas no mitigadas

MAC y IP Spoofing de usuarios no autentificados: El spoofing ARP e IP pueden ser efectivos en el segmento WLAN, pero sólo hasta que los clientes utilicen IPSec para asegurar su conexión. En la Tabla 5 se puede observar un cuadro

Tabla 5. Mitigación de amenazas de seguridad en WLAN mediante VPN IPSec.

Ataque	Diseño VPN IPSec
Ataque MITM (ataque activo)	Mitigado
Autenticación forjada	Mitigado
Ataque pasivo (ataque FMS)	No aplica porque no utiliza WEP
AP no autorizados	Mitigado
Ataques de diccionario.	Mitigado
Spoofing	Mitigado (mientras no se establezca el túnel)

8.1.2.4 Lineamientos de diseño de VPN en WLAN

Los AP de la WLAN son conectados a switch capa 2 para tener acceso a la red cableada, y pertenecen a una VLAN especialmente dedicada a transportar el tráfico IPSec desde los clientes inalámbricos. Este tráfico se mantiene separado del tráfico común a la red cableada hasta que es descifrado por un extremo de la VPN. Es importante aclarar que en este diseño no se hace uso de WEP. La red inalámbrica como tal es un medio inseguro de transmisión, que se utiliza únicamente para transito del tráfico IPSec. Con el objetivo de aislar por completo esta WLAN insegura, no se debe mezclar bajo ningún concepto la

VLAN de los usuarios WLAN y las VLAN de la red cableada. El no cumplir ésta premisa podría permitirle a los hackers atacar a los usuarios de la red cableada desde la red inalámbrica.

El procedimiento de asociación de un cliente inalámbrico al ambiente seguro de la red corporativa es el siguiente. Los clientes inalámbricos se asocian con el AP para establecer conectividad de capa 2 con la red corporativa, y estos utilizan los servicios de DHCP y DNS para establecer conectividad de capa 3 con la red. Luego de la configuración inicial de capa 3, el túnel VPN se autentifica con el concentrador VPN. El concentrador VPN puede utilizar certificados digitales ó clave compartida para la autenticación del dispositivo inalámbrico. Si el concentrador VPN utiliza clave compartida para la autenticación, entonces es recomendable el uso de OTP para la autenticación de usuario. De no utilizarse OTP, el concentrador VPN es vulnerable a ataques de intento de acceso mediante fuerza bruta por parte de los hackers que hayan obtenido la clave compartida de IPSec utilizada por el concentrador VPN. El concentrador VPN utiliza los servicios del servidor RADIUS, quien a su vez entra en contacto con el servidor OTP para la autenticación de usuario. El concentrador VPN utiliza DHCP para la configuración IP, para que de esta forma el cliente inalámbrico se comunique a través del túnel. De presentarse una falla en el concentrador VPN o en el servidor RADIUS, se bloquea el acceso a la red con el fin de mantener el nivel de seguridad adecuado. Ambos servicios son imperativamente necesarios para permitir que el cliente inalámbrico logre acceso a la red corporativa. Cabe destacar que cuando el cliente inalámbrico se está comunicando con la red corporativa, pero antes que el túnel ha sido establecido, no se considera seguro el tráfico del cliente. Esto quiere decir que mientras el cliente logra establecer una conexión segura por medio de la VPN IPSec, todas las vulnerabilidades de las WLAN expuestas en este trabajo se mantienen. Sin embargo tres técnicas de mitigación son recomendadas:

Primero, los AP deben estar configurados con filtros de protocolos y de puertos basados en la política de uso de la WLAN de la empresa. Se recomienda la aplicación de filtros restrictivos que permitan sólo los protocolos necesarios que son requeridos para el establecimientos de un túnel seguro hasta el concentrador VPN. Entre estos protocolos se incluyen DHCP para la configuración inicial del cliente, DNS para resolución de nombre de los concentradores VPN, los protocolos específicos para la VPN que son IKE (puerto 500

UDP) y ESP (puerto 50 IP), y ICMP para realizar resolución de problemas. Aún con estos filtros aplicados, los servidores DNS y DHCP están expuestos a ataques hacia estos mismos protocolos. Se debe tener cuidado adicional para asegurarse que estos sistemas sean lo más seguros posibles a nivel de los servidores. Esto incluye el mantener los sistemas operativos y aplicaciones actualizadas y con los *parches* más recientes instalados, y utilizar sistemas de detección de intrusión. Adicionalmente, los switches más recientes ofrecen la capacidad de implementar la tecnología VACL. Implementando VACL para los protocolos relacionados con la VPN y las direcciones IP específicas de los concentradores VPN, se puede lograr un nivel mayor de filtrado que garantice que sólo el tráfico destinado para los concentradores VPN sea el que atraviese los switches. El tráfico DNS es opcional, y depende si el cliente inalámbrico necesita que se le sea configurado un nombre DNS del concentrador VPN, o le es suficiente con su dirección IP. Es recomendable que los paquetes ICMP sean permitidos sólo a través de las interfaces salientes del concentrador VPN.

Segundo, utilizar las características del cliente VPN que le permiten establecer automáticamente el túnel VPN una vez recibida la dirección IP correcta de la WLAN desde el servidor DHCP. Esto elimina la necesidad de que el usuario final sea quien establezca manualmente el túnel VPN luego que el computador ya haya iniciado.

Tercero, una aplicación de firewall personal debe ser incluida en el cliente inalámbrico, para que esté protegido mientras se encuentre conectado a la WLAN insegura y sin la protección de IPSec.

En conclusión, el concentrador VPN es quien hace de frontera entre la WLAN no segura y la red corporativa alambrada y segura. El cliente inalámbrico establece una conexión VPN contra el concentrador VPN para lograr una comunicación segura con la red corporativa. En el proceso de lograr esto, el concentrador VPN realiza autenticación de cliente y usuario vía la VPN IPSec. La característica *Split Tunnel* debe estar deshabilitada en el cliente para que todo el tráfico sea enviado por el túnel. La característica *Split Túnel* es la que impide el paso de tráfico de datos desde la conexión no cifrada hacia la red cifrada de la VPN, de esta forma se evita que un hacker pueda tomar control remoto de un cliente inalámbrico y entrar a la red corporativa a través de la VPN.

8.1.2.5 Alternativas de diseño en WLAN con VPN

Como una alternativa para añadir algo más de dificultad a las ataques de los hackers, se puede considerar la configuración de claves WEP estáticas en todos los dispositivos. Pero esta alternativa se hace prácticamente inaplicable si se piensa en la dificultad de la administración en una WLAN de gran tamaño. Este enorme trabajo de administración se puede eliminar si se decide no cambiar las claves nunca, pero esta solución entraría en la categoría de mantener un nivel de seguridad dudoso.

Adicionalmente, se puede considerar el uso de 801.1X/EAP con la implementación de la VPN basada en IPSec para asegurar el ambiente WLAN. Pero esto significaría el tener que administrar dos infraestructuras separadas de seguridad para las WLAN.

Para asegurar más aún los servicios DNS y DHCP, se puede tomar en cuenta el uso de servidores DHCP y DNS dedicados únicamente a la VPN de la WLAN. Esta opción mitigaría dos potenciales riesgos que podrían afectar los recursos de la red cableada:

- Ataques de negación de servicio contra los servidores DNS y DHCP podrían afectar a los usuarios de la red cableada.
- Descubrimiento de la topología de la red a través del uso de *DNS queries* y *reverse lookups*.

8.1.3 Alternativas de diseño de seguridad en WLAN

Como una alternativa se puede evaluar la factibilidad de la instalación de protocolos de seguridad a nivel de capa de aplicación como el protocolo *Secure Socket Layer* (SSL) o un protocolo como SSH para lograr mayor seguridad en las WLAN. Para que estos protocolos sean utilizados efectivamente en un ambiente WLAN, es necesario que sean implementados utilizando mecanismos robustos de autenticación mutua, para evitar ataques MITM. Esto requiere del uso de certificados en el lado del cliente cuando se utiliza SSL para proteger la capa de aplicación. Cabe destacar que SSL está presente en la mayoría de los sistemas (SO) corporativos a través de una distribución gratis en los exploradores. Por el contrario, SSH no es soportado nativamente por los SO corporativos y esto implicaría un costo adicional con la instalación de un cliente SSH por cada dispositivo. Existen soluciones empresariales que ofrecen aseguramiento de las WLAN por medio de VPN basadas en SSL, su funcionamiento de basa en la conexión a la WLAN segura a través de

un portal, sin la necesidad de instalar una aplicación cliente VPN, y ofreciendo conectividad total a la red por medio de una VPN de capa 3 [8].

Otra alternativa para mejorar la seguridad es la aplicación de filtros por direcciones MAC, en donde en cada AP existe un listado de direcciones MAC de los dispositivos clientes que tienen permitido la asociación. La aplicación de esta alternativa significa que se debe mantener actualizado el listado de direcciones MAC en cada uno de los AP, lo cual puede convertirse en una tarea difícil, sobre todo cuando se tiene un gran número de dispositivos clientes. Por otro lado, es requerido en el estándar 802.11 que las direcciones MAC sean transmitidas sin ser cifradas, esto trae como resultado que un hacker puede capturar el tráfico de la WLAN y obtener la dirección MAC de uno de los dispositivos clientes permitidos, posteriormente realizar *spoofing* tal como fue expuesto en el aparte "Debilidades de las WLAN". Esta alternativa adicional de aseguramiento es más adecuada para WLAN de pequeño tamaño y con pocos usuarios.

CAPITULO V

9 DESARROLLO DE LA PROPUESTA

En este capitulo se exponen los niveles de seguridad deseados en la WLAN de DESCA, para así, en combinación con el levantamiento de información de la Red de DESCA y las dos propuestas estudiadas en el capítulo anterior, desarrollar un escenario posible en el cual se conjuguen estos tres factores, y se logre alcanzar los niveles de seguridad y disponibilidad acordes con una red corporativa como la de la empresa.

Es importante destacar que la seguridad de las WLAN se basa en elementos y mecanismos de seguridad propios de las redes cableadas, como los son la autenticación basada en puertos de 802.1X, autenticación mutua basada en certificados digitales, políticas de filtrado de tráfico capa 3 con el uso de listas de acceso, diferenciación de usuarios y aplicaciones por medio de VLAN, etc. Todos estos elementos y mecanismos de seguridad han sido adaptados a las características y requerimientos propios de las comunicaciones inalámbricas de las WLAN, y por lo tanto, si se quiere contar con un nivel más alto de seguridad en una WLAN, es recomendable la implementación de estos mecanismos y elementos de seguridad en la red cableada en donde reside la WLAN.

9.1 Niveles de seguridad requeridos

Los niveles de seguridad requeridos para esta propuesta deben tomar en cuenta los siguientes aspectos:

- Garantizar la autenticidad de los usuarios que utilizan la WLAN y la confidencialidad de la información que fluye por la WLAN desde sus equipos hasta la red cableada.
- Garantizar la autenticidad de los usuarios que administran la red inalámbrica, basados en una gestión segura de la red.
- Prevenir y detectar el uso de puntos de acceso no autorizados.
- Establecimiento de políticas de seguridad de la WLAN.

Para lograr estos objetivos, en primer lugar se debe realizar la elección de los mecanismos de seguridad a utilizar, para posteriormente exponer con más detalle los pasos a seguir para lograr la implantación de cada una de esas técnicas.

9.2 Equipamiento con el que se cuenta para la propuesta de seguridad

Para elegir cuál de las dos propuestas descritas en el capitulo anterior se debe tomar en cuenta las características de la red de DESCA. En primer lugar se tomará como línea base las capacidades de seguridad de los equipos WLAN clientes que están en uso. Como se observa en la Tabla 3 del capítulo III, donde se resumen las características de seguridad de todos los dispositivos WLAN clientes de la red, las opciones de seguridad que comparten todos los dispositivos son: cifrado basada en WEP de 128 bits y TKIP, soporte para el estándar de autenticación 802.1X PEAP de Microsoft y EAP-TLS.

Como segundo aspecto a tomar en cuenta, están las capacidades de los AP, pero dado que éstos sobrepasan por mucho las capacidades comunes de seguridad de los clientes inalámbricos, los AP no juegan un rol importante en la elección de la propuesta ya que soportarían sin ningún problema les requerimientos de cualquiera de las dos.

Por encima de los AP se encuentran los dispositivos de conectividad cableada de la red. Estos son los switches capa 2 de distribución y el switch capa 3 con los que se cuenta en la sede de DESCA Caracas, equipos que también son capaces de soportar los requerimientos de cualquiera de las dos propuestas.

A nivel de servidores, en la empresa se cuenta con los servicios de Directorio Activo que es donde se administran de forma centralizada la base de datos de los usuarios, pero no se cuenta con servidores 802.1X, ni servidores de certificados digitales ni de OTP, o un servidor que haga las funciones de concentrador VPN. Por lo tanto, sería necesario la adquisición de un servidor que realice las funciones 802.1X como primer paso para poder elegir cualquiera de las dos propuestas.

9.3 Elección de las técnicas de aseguramiento

Como se estudió en el capítulo anterior, tanto la propuesta de diseño de VPN como la de EAP/802.1X logran sus objetivos en cuanto a la capacidad de mitigación de las vulnerabilidades de las WLAN, haciendo la salvedad que en el diseño VPN la red es vulnerable mientras no se establezca el túnel VPN.

Pero, en cuanto a facilidad de uso por parte del usuario, como de integración con la red de la empresa, la propuesta de diseño EAP/802.1X con TKIP tiene las siguientes ventajas:

- No es necesario la instalación de un cliente VPN en los dispositivos clientes.

- No hay que establecer un rango de direcciones IP adicional para los túneles VPN.
- No es necesaria la instalación de un concentrador VPN.
- La WLAN no es vulnerable mientras se establece la conexión del usuario.
- Los mecanismos de seguridad son transparentes a la experiencia del usuario.
- Se reduce el riesgo de caídas inesperadas del servicio ocasionada por fallas en el concentrador VPN.
- Se logra un mayor ancho de banda dado que no se une todo el tráfico de la WLAN en el concentrador VPN.
- Mejoran los tiempos de respuesta, dado que se eliminan los retardos de procesamiento de cifrado y descifrado que está centralizado en el concentrador VPN.

Basados en los argumentos anteriormente expuestos, la propuesta de técnicas de aseguramiento que mejor se adapta a la WLAN es la de diseño con EAP/802.1X con TKIP.

9.3.1 Descripción de la propuesta de diseño EAP/802.1X con TKIP

La propuesta de diseño para la implementación de técnicas de seguridad en la red de DESCA Caracas se basará en:

- Cifrado: WEP de 128 bits con TKIP y WPA con TKIP, según lo soporte el dispositivo cliente
- Autenticación: PEAP-MS-CHAP v2

WEP con TKIP es el método de cifrado compatible con todos los dispositivos de red de los computadores personales en DESCA Caracas, tal como se expuso en el levantamiento de información de la red. WPA con TKIP es un mecanismo de cifrado mucho mas robusto, y que puede ser utilizado como una opción para los equipos de la WLAN que los soportan.

La técnica de autenticación a elegir es PEAP-MS-CHAPv2, en vista que todos los computadores personales con conexión WLAN tienen instalado el sistema operativo Microsoft Windows XP, en la versión SP2 que tiene integrada la posibilidad de autenticación 802.1X elegida para esta propuesta. PEAP-MS-CHAPv2 es un protocolo de autenticación mutua basado en contraseñas, desafíos y respuestas, con el uso del estándar

Message Digest 4 (MD4) y en algoritmos DES para el cifrado de las respuestas. Los elementos necesarios para el uso de esta técnica de autenticación para una WLAN son:

- Clientes inalámbricos con SO Microsoft Windows XP SP2.
- AP que soporten los requerimientos de seguridad de esta propuesta.
- Servidor Microsoft Windows 2000 ó 2003 con los servicios de controlador de dominio y el directorio activo: el directorio activo (AD) permite la administración de los usuarios en grupos para diferenciar los usuarios de la WLAN y de la LAN.
- Servidores Microsoft Windows 2003 con los servicios IAS y de Certificaction Authority (CA): IAS (Internet Authentication Service) es la implementación Microsoft de un servidor RADIUS que permite realizar funciones de autenticación, autorización, y contabilidad (AAA) para muchos tipos de accesos a las redes, incluyendo WLAN. El servicio de CA es el que emite certificados digitales confiables al servidor IAS y a los clientes inalámbricos para la fase de autenticación.

De acuerdo a la recomendación del fabricante en relación a aspectos de seguridad y rendimiento de los servidores, no es recomendable que servicios de controlador de dominio y AD, y los de IAS y CA estén alojados en un mismo servidor. Sin embargo, los servicios de IAS y CA pueden compartir un mismo servidor, por lo tanto, se hace necesaria la adquisición de un solo servidor en el cual residirán estos dos nuevos servicios.

Adicional a los elementos que tienen funciones en la propuesta 802.1X/EAP con TKIP, para ofrecer una red segura con opciones que aumenten su disponibilidad, mejoren el desempeño y administración centralizada, se debe contar con los siguientes elementos:

- Switches Capa 2 y 3
- Servidores DHCP
- Servidores de monitoreo y administración
- Sistemas de Detección de Intrusos (IDS)

El diagrama de red de la propuesta de seguridad 802.1X/EAP con TKIP quedaría como se muestra en la Figura 15.

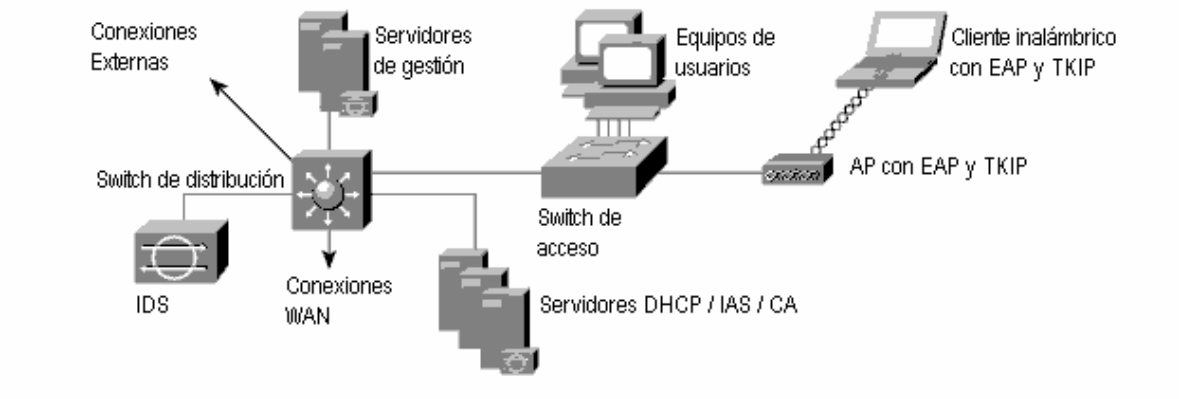

Figura 15. Diagrama de WLAN segura 802.1X/EAP con TKIP

Es importante tomar en cuenta los mecanismos y procesos de administración de los dispositivos de la red para complementar la seguridad a nivel de autenticación y confidencialidad brindada por la propuesta técnica de aseguramiento. Para ello, se debe garantizar que sólo realicen modificaciones en los equipos de red los usuarios que cuenten con la autorización adecuada. Esto se logra habilitando las funcionalidades AAA de los dispositivos de red basadas en protocolos de acceso seguros como SSH, o en el caso de administración vía HTTP, utilizar protocolos seguros como SSL.

9.4 Lineamientos de configuración 802.1X/EAP con TKIP

A continuación se presentan los elementos básicos de configuración de los equipos y dispositivos que forman parte de la solución 802.1X/EAP con TKIP. Para ello, se asume que se cuenta con los servicios de controlador de dominio y directorio activo activados y funcionando de forma adecuada, así como con los elementos básicos de configuración de los elementos de red que garantizan conectividad, como por ejemplo, el servicio de DHCP o un esquema de direccionamiento IP apropiado.

9.4.1 Configuración del directorio activo

En la base de datos del directorio activo, se deben configurar los distintos grupos de usuarios que van a utilizar la WLAN, para así definir los niveles de privilegios de cada grupo según las políticas de seguridad emitidas por la empresa.

9.4.2 Configuración de la autoridad de certificados digitales

Se requiere que se le sea instalado un certificado digital confiable al servidor con IAS. Para ello, se necesita que esté habilitado el servicio de emisión de certificados digitales. Los sistemas operativos de Microsoft Windows 2000 y 2003 tienen instalados una selección de entidades emisoras de certificados raíz confiables, o también, se le pueden instalar certificados digitales que hayan sido comprados a empresas como VeriSign. Una vez instalado el certificado digital, la CA debe hacer su emisión para que dicho certificado pueda ser solicitado por el IAS.

El sistema operativo Windows XP tiene instalado un listado de distintos entes certificadores, pero en caso que se compre un certificado digital de un ente certificador que no se encuentre en este listado, entonces se tendrá que instalar dicho certificado en cada uno de los dispositivos cliente que requieran ser autenticados.

9.4.3 Configuración del servidor IAS

El servidor con IAS es el que ofrece las facilidades AAA en la que se basa esta solución de seguridad. En él deben estar configurados:

- El certificado digital (solicitado e instalación)
- El método de autenticación PEAP
- Integración con el directorio activo
- Registro de todos los dispositivos de red

9.4.3.1 Solicitud e instalación del certificado digital

Una vez que la CA ha emitido el certificado digital, se debe proceder a su solicitud e instalación por parte del IAS, para que de esa forma cuente con un certificado digital, vigente y activo, a ser utilizado en la autenticación mutua con el cliente inalámbrico. Se recomienda la instalación de sólo una CA para DESCA y que cualquier otro requerimiento de certificados digitales esté subordinado a ésta.

Para la solicitud e instalación del certificado digital, se debe ingresar a la página Web local de solicitud de certificados digitales de la CA, luego indicar que el certificado debe ser del tipo de autenticación de servidor e ingresar todos los datos necesarios para la solicitud del certificado. Luego que la solicitud ha sido generada, el administrador de la CA debe realizar la emisión del certificado. Una vez emitido el certificado, se debe ingresar de

nuevo a la página de solicitud del certificado, en donde se encontrará que el estatus de la solicitud ha cambiado, se selecciona el certificado que ha sido emitido, y se siguen los pasos para su instalación en el servidor con IAS.

9.4.3.2 Integración con el directorio activo

El servidor con IAS debe ser registrado en el directorio activo, con el objetivo que para esta propuesta los usuarios utilicen su nombre de usuario y contraseña de red para su autenticación en la WLAN, y también para facilitar la administración de los usuarios de la red, ya que con un solo nombre de usuario y contraseña pueden acceder a todos los recursos y servicios de la red corporativa.

Para registrar el IAS en el directorio activo, simplemente se debe ir a la sección de IAS de la consola de administración del directorio activo, y elegir la opción *registrar servidor IAS en el directorio activo.*

9.4.3.3 Configuración de autenticación PEAP

En la configuración del IAS, se debe indicar la política de acceso remoto inalámbrico, que es la que indica los mecanismos a utilizar en el proceso de autenticación mutua entre el servidor RADIUS y el cliente inalámbrico.

Para la configuración de la política de acceso remoto inalámbrico, se debe crear una política nueva dentro del servicio IAS y ser configurada con los siguientes parámetros:

1. Indicar que es una política de acceso inalámbrico
2. Seleccionar el grupo de usuarios que va a tener acceso a la WLAN
3. Seleccionar PEAP como método EAP de autenticación
4. Seleccionar el certificado digital previamente instalado
5. Esta política de acceso remoto debe ser colocada como número uno en el orden de prioridad, y de ser posible que sea la única.

9.4.3.4 Registro de todos los dispositivos de red

Dado que el servidor IAS ofrece funciones AAA, entonces para garantizar que la administración de los dispositivos de red como los AP y los switches sea realizada por el personal autorizado, y que además quede un registro de las actividades de administración realizada por estos usuarios, cada uno de estos dispositivos de red administrables deben estar registrados en el IAS.

9.4.4 Configuración del dispositivo cliente

La configuración del dispositivo cliente se basa en la definición del SSID de la WLAN, de la técnica de cifrado de los datos y del mecanismo de autenticación EAP a utilizar. Como se discutió anteriormente en este trabajo, todos los computadores de DESCA Caracas con facilidad de conexión a la WLAN son compatibles con la técnica de cifrado WEP y algunos con WPA, y con el método de autenticación PEAP-MS-CHAPv2.

9.4.4.1 Configuración de la autenticación EAP

La primera fase de la autenticación PEAP se realiza entre el servidor de autenticación y el cliente inalámbrico. En ella se establece un túnel TLS cifrado a través del cual serán intercambiadas las credenciales PEAP de forma segura. Los parámetros de configuración del cliente, para que realice la autenticación, son configurados en el Administrador de Propiedades del dispositivo siguiendo los siguientes pasos:

1. En la ventana de configuración de propiedades de las conexiones de red inalámbricas (Figura 16) debe estar habilitada la opción **Use Windows to configure my wireless network settings.**

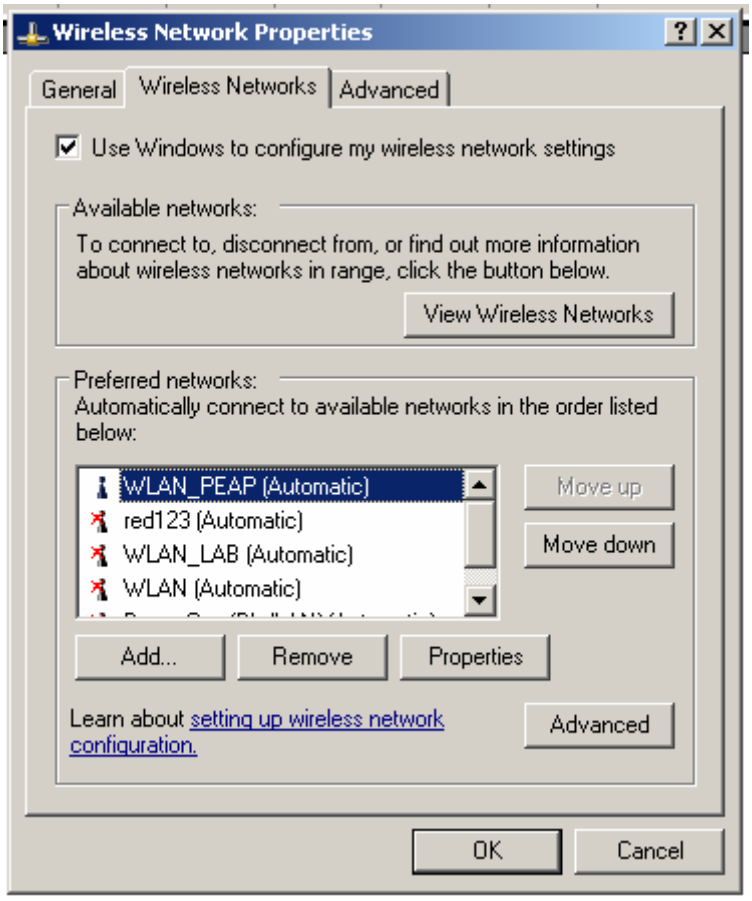

Figura 16. Configuración de propiedades de las conexiones de WLAN

2. Crear el SSID a utilizar para la autenticación PEAP
3. En la configuración del SSID creado se debe elegir el método de autenticación abierto y el tipo de cifrado WEP ó WPA según sea el caso (Figura 17). Se debe habilitar la opción **The key is provided for me automatically** para que las claves de cifrado sean entregadas por el servidor de autenticación.

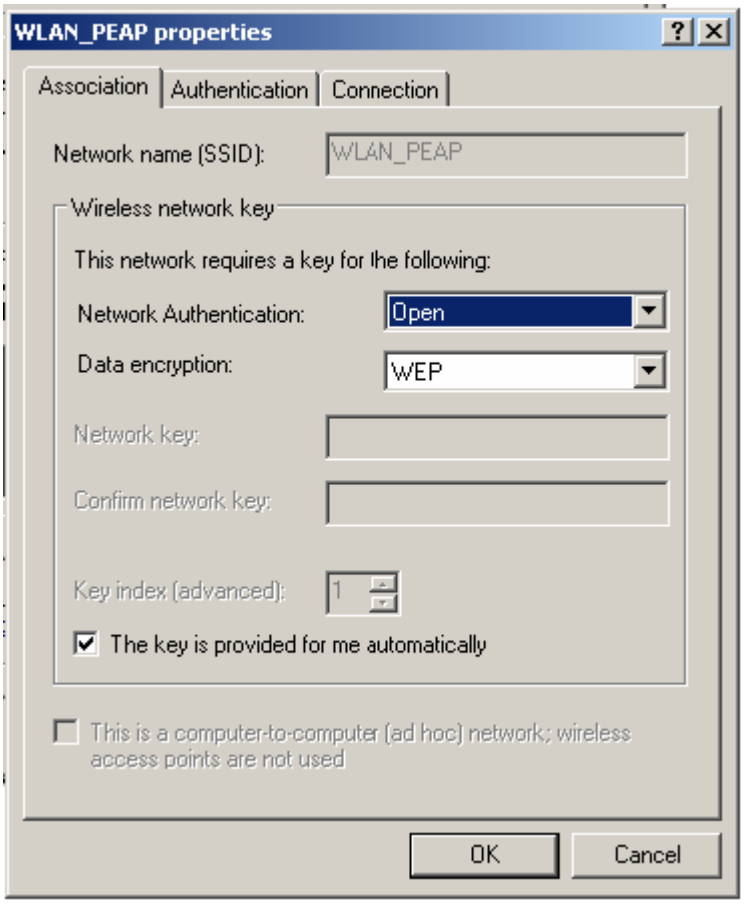

Figura 17. Configuración de los parámetros de cifrado y autenticación

4. En la ventana de autenticación debe estar habilitada la opción **Enable IEEE 802.1X authentication for this network** (Figura 18).

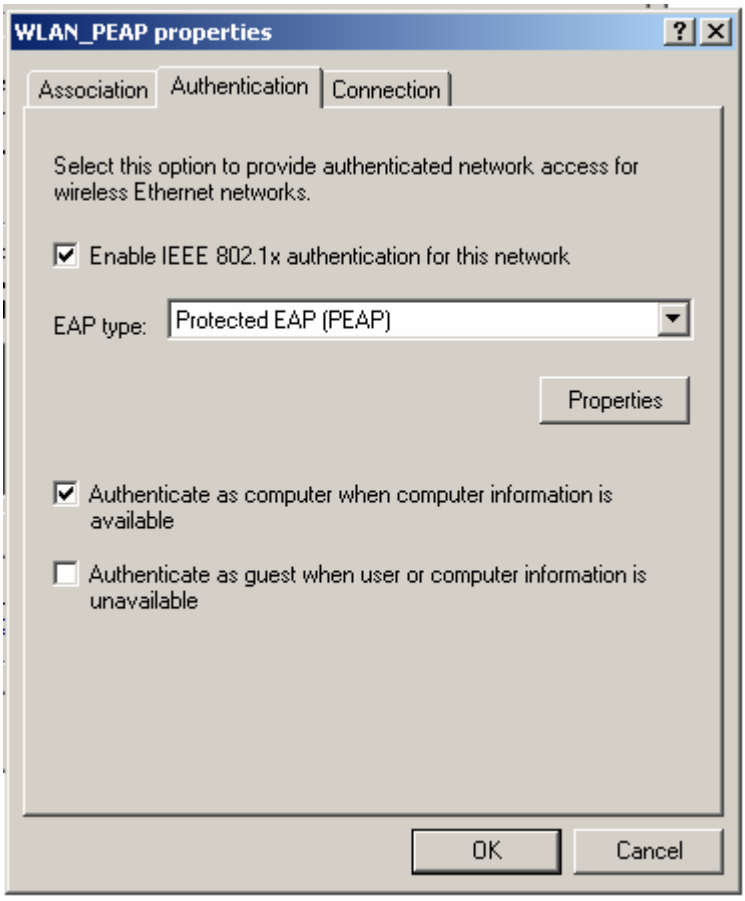

Figura 18. Ventana de configuración para autenticación PEAP-MS-CHAPv2

5. Elegir **Protected EAP (PEAP)** como mecanismo de autenticación.
6. Para que el cliente inalámbrico sea autenticado en el dominio Microsoft debe ser habilitada la opción **Authenticate as computer when computer information is available.**
7. Habilitar la opción **Validate server certificate.**
8. Seleccionar del listado de CA confiables el certificado digital adecuado. Si no aparece en la lista, este deber ser instalado.
9. En las propiedades de la autenticación PEAP elegir **Secured password (EAP-MSCHAPv2)** como método de autenticación (Figura 19).

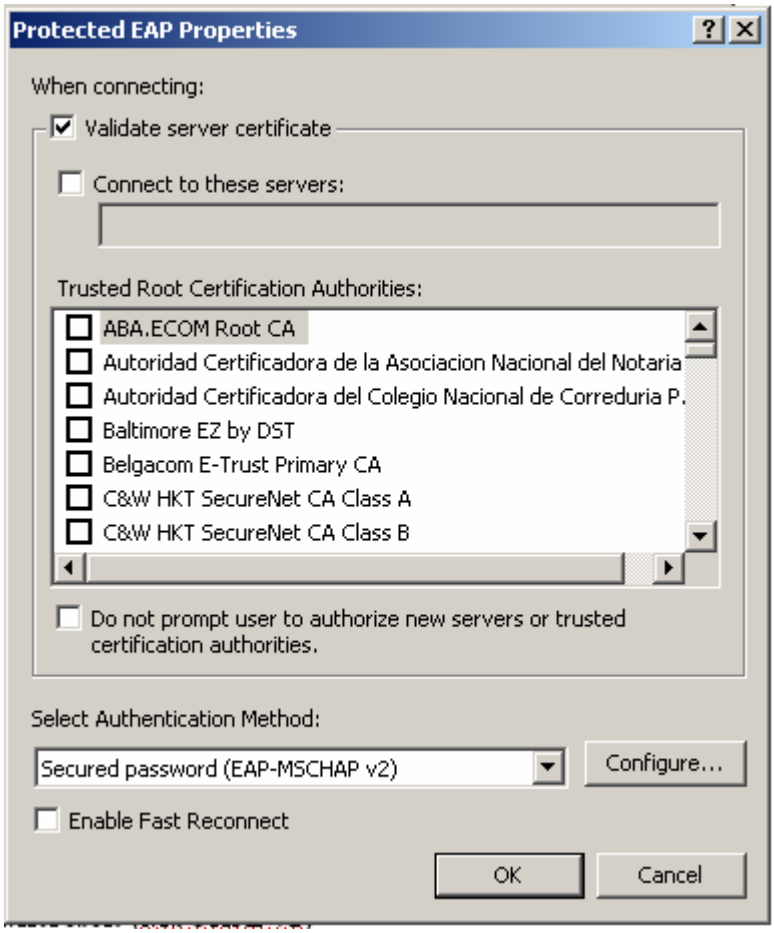

Figura 19. Ventana de configuración de Microsoft (MSCHAPv2)

10. Entrar a la ventana de la configuración de propiedades de MSCHAPv2.

11. Habilitar la opción **Automatically use my Windows logon name and password (and domain if any)** para que se utilicen en la autenticación el nombre de usuario y contraseña asignados a ese dispositivo en el directorio activo.

9.4.5 Configuración del AP

El AP debe ser configurado para que sepa en cual lugar de la red está ubicado el servidor RADIUS. Además, se le debe configurar los elementos de conectividad de los clientes como son el SSID y el algoritmo de cifrado, y por último se debe configurar el método de autenticación que se va a utilizar entre en servidor RADIUS el cliente inalámbrico.

9.4.5.1 Definición del servidor RADIUS

En el AP se debe definir el servidor de autenticación y establecer su relación con él. Para ello se define el servidor RADIUS dentro de un grupo de servidores, se indica su dirección IP y puertos de operación, y además los mecanismos de autenticación, que para este caso es PEAP. A continuación, un ejemplo de los comandos a utilizar en el AP Cisco Aironet 1100:

```
aaa group server radius rad_eap
  server 10.0.0.3 auth-port 1645 acct-port 1646
aaa new-model
  aaa authentication login eap_methods group rad_eap
  radius-server host 10.0.0.3 auth-port 1645 acct-port 1646 key labap1200ip102
```

El AP debe estar definido en el servidor RADIUS como un cliente AAA.

9.4.5.2 Definición del SSID

Para la definición de los SSID que se van a asignar a cada VLAN de la red inalámbrica de la empresa, se debe tomar en consideración lo siguiente:

Nombre de la empresa: es usual utilizar el nombre de la empresa como parte del SSID, pero esto es la mejor forma de hacer publicidad a una WLAN que se supone se quiere sea segura. Utilizar el nombre de la empresa dentro del SSID es útil en caso que uno desea ofrecer una WLAN pública. Para una WLAN privada como la de DESCA, es peligroso publicar el nombre de la empresa en el SSID, ya que esto podría ser utilizado para iniciar un ataque DoS en contra de la red.

Uso de caracteres especiales: el uso de SSID con caracteres especiales, como por ejemplo "D35c4_W1@|\|", en realidad no esconde la identidad de la empresa, mas bien da la impresión que se está ocultando algo importante, lo que atrae la atención de los hackers. Mucha gente elige este tipo de SSID con la idea que hace su WLAN más segura, pero se debe tener en mente que, con las herramientas computacionales adecuadas, cualquier persona puede obtener fácilmente un SSID oculto y además el uso de un SSID con caracteres especiales hace más difícil la gestión de la red.

Con el propósito de ocultar la identidad de la empresa, un SSID totalmente desligado al nombre de la empresa es la mejor solución. Pueden ser utilizados SSID como *WLANempresa* para los usuarios de la red, *WLANV* para la subred de voz, o *WLANinvitado* para los usuarios visitantes, etc. De esta forma alguien interesado en vulnerar la seguridad

de una empresa, no podrá identificar su WLAN según su SSID, y probablemente tendrá poco interés en realizar un ataque a una WLAN sin conocer su dueño. Para la elección de un SSID se debe considerar como afectaría la funcionalidad, seguridad y la facilidad de gestión. Es una buena práctica elegir un SSID que no se encuentre en uso en otra WLAN en las cercanías de las oficinas de la empresa, para así evitar conflictos con otras redes, una forma de saber cuales SSID están en uso, sin importar sean publicados o no, es mediante el uso de herramientas como Kismet.

A continuación se presenta un ejemplo de cómo configurar un SSID en un AP Cisco Aironet, y además como deshabilitar la función de incluir el SSID en los *beacons*:

```
interface dot11radio 0
  ssid WLAN_PEAP
  no guest-mode
```

9.4.5.3 Definición del algoritmo de cifrado

Una vez que ya el AP conoce hacia donde enviar las peticiones de autenticación del cliente, debe ser configurado para utilizar el algoritmo de cifrado WEP ó WPA. El método de cifrado WEP de 128 bits y se configura en un AP Cisco Aironet 1100 de la siguiente forma.

```
interface dot11radio 0
  ssid WLANwep
  authentication open eap eap_methods
  encryption mode WEP mandatory
```

El método de cifrado WPA se configura en un AP Cisco Aironet 1100 de la siguiente forma.

```
interface dot11radio 0
  ssid WLANwpa
  authentication open eap eap_methods
  authentication key-management wpa
```

El método de cifrado depende del SSID al cual se conecte el dispositivo cliente, y los AP Cisco Aironet 1100 tienen la capacidad de manejar de forma simultánea ambos esquemas de cifrado.

9.4.5.4 Definición del método de autenticación

Una vez definidos el SSID y el algoritmo de cifrado, debe ser configurado el método de autenticación abierta PEAP en la interfaz inalámbrica de AP. En un AP Cisco Aironet 1100, el método de autenticación se configura como se muestra a continuación.

```
interface dot11radio 0
  authentication open eap peap
```

El realizar esta configuración básica, garantiza que el AP permita la autenticación PEAP entre el cliente y el servidor RADIUS. Posteriormente se pueden realizar mejoras a esta configuración, añadiendo diferentes VLAN asociadas a distintos SSID y métodos de autenticación que permitan la diferenciación de usuarios. Además de esto, y para el caso de DESCA en Caracas, se debe agregar una VLAN a la cual se conecten únicamente los teléfonos IP. Para que el AP reciba el listado de VLAN desde el servidor de VLAN, éste deber ser configurado en modo cliente.

9.4.6 Configuración de los switches

Los switches capa 2 deben ser configurados según el estándar 802.1Q en los puertos que estén conectados los AP, para que éstos puedan trabajar en conjunto con la administración de VLAN centralizada en el switch capa 3.

En el switch capa 3 es donde están configurados los filtros capa 3 que aumentan la seguridad de la propuesta, y además donde están definidas las VLAN que permiten la diferenciación de usuarios o dispositivos.

La definición de las VLAN se puede realizar de la siguiente forma; VLAN administrativa, VLAN que trabaja bajo EAP, y una tercera VLAN para la telefonía IP. También podría ser configurara una VLAN para usuarios visitantes.

Para cada VLAN se configuran listas de acceso que permiten el paso de tráfico capa 3 necesario para cada tipo de VLAN, y se restringe todo tipo de tráfico no deseado.

Por ejemplo, para la VLAN administrativa, se tienen listas de acceso que sólo permiten tráfico de autenticación y contabilidad desde el AP hacia el servidor RADIUS y viceversa, y también se tienen otras listas de acceso que sólo permiten tráfico Web o SSH desde o hacia el AP, tráfico utilizado sólo para la gestión remota.

También se debe contar con una VLAN de sólo tráfico EAP, es decir ésta es la VLAN en donde se establece la autenticación PEAP, y posteriormente el acceso del cliente inalámbrico desde un AP registrado en el servidor RADIUS. Para ello se configuran listas de acceso que permitan las peticiones y respuestas DHCP, y que permiten tráfico desde cualquier lugar de la red segura hacia la VLAN EAP, y además niegan todo tráfico administrativo y cualquier otro tipo de tráfico que no pertenece a la red.

A continuación se presenta un ejemplo de configuración del switch capa 3, en el cual se muestra la separación del tráfico en VLAN con listas de acceso aplicadas.

```
! Definición de la VLAN de administración de los AP
interface Vlan100
ip address 10.1.10.1 255.255.255.0
ip access-group 110 in
ip access-group 111 out
ip helper-address 10.3.2.50
no ip redirects
no cdp enable
! Permite solo peticiones de  autentificación y contabilidad desde el AP hacia el servidor RADUIS
access-list 110 permit udp host 10.1.10.120 gt 1023 host 10.1.20.253 eq 1645
access-list 110 permit udp host 10.1.10.120 gt 1023 host 10.1.20.253 eq 1646
! Permite tráfico administrativo Web y SSH saliente del AP hacia la subred administrativa
access-list 110 permit tcp host 10.1.10.120 eq www 10.1.20.0 0.0.0.255 gt 1023 established
access-list 110 permit tcp host 10.1.10.120 eq 22 10.1.20.0 0.0.0.255 gt 1023 established
! Niega cualquier otro tráfico
access-list 110 deny ip any any log
! Permite tráfico Web y SSH de administración desde la red administrativa hacia el AP
access-list 111 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.10.120 eq www
access-list 111 permit tcp 10.1.20.0 0.0.0.255 gt 1023 host 10.1.10.120 eq 22
! Permite respuestas RADIUS desde el servidor AAA hacia el AP
access-list 111 permit udp host 10.1.20.253 eq 1645 host 10.1.10.120 gt 1023
access-list 111 permit udp host 10.1.20.253 eq 1646 host 10.1.10.120 gt 1023

! Definición de la VLAN PEAP
interface Vlan200
ip address 10.1.40.1 255.255.255.0
ip access-group 210 in
ip access-group 211 out
ip helper-address 10.1.50
no ip redirects
no cdp enable
! Permite solo peticiones BOOTP para que lleguen hasta el servidor DHCP
access-list 210 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
! Niega el acceso a la VLAN administrativa de los AP desde la VLAN PEAP
access-list 210 deny ip 10.1.40.0 0.0.0.255 10.1.10.0 0.0.0.255 log
! Permite todo el tráfico IP desde cualquier origen de la WLAN hacia la VLAN PEAP
access-list 210 permit ip 10.1.40.0 0.0.0.255 any
! Niega cualquier otro tipo de tráfico
access-list 210 deny ip any any log
! Permite las respuestas DHCP para la configuración IP inicial del cliente inalámbrico
access-list 211 permit udp host 10.1.30.50 eq bootps host 255.255.255.255 eq bootpc
! Permite todo el tráfico IP desde la VLAN PEAP hacia cualquier destino en la WLAN
```

```
access-list 211 permit ip any 10.1.40.0 0.0.0.255
¡ Niega cualquier otro tráfico
access-list 211 deny ip any any log
```

9.4.7 Consideraciones adicionales

En la WLAN de DESCA Caracas se encuentran en uso cuatro teléfono IP inalámbricos Marca Cisco, modelo 7920. Como se discutió en el capitulo 3, estos teléfonos se conectan a una VLAN de voz exclusiva para los servicios de telefonía de la empresa, en la cual están aplicados los parámetro de QoS adecuados.

Se pueden utilizar dos opciones para la autenticación de los teléfonos inalámbricos: por clave compartida, o por el mecanismo LEAP. En vista que son pocos los teléfonos en uso en la WLAN, y que no sería difícil para la administración de las claves estáticas en cuatro teléfonos, se recomienda el uso de autenticación WPA-PSK, soportada tanto por los teléfonos como por los AP, para la autenticación de los teléfonos; y el mecanismo de cifrado WPA para asegurar la confidencialidad de las conversaciones. WPA es un mecanismo de cifrado más poderoso que WEP, y es mucho más difícil de descifrar la clave compartida, que por política de la empresa debería ser cambiada frecuentemente.

La VLAN de voz debe tener aplicada listas de acceso que sólo permitan el tráfico de paquetes RTP (Real Time Protocol) para el tráfico de voz, y de los puertos 1720, 2000, 2002 y 11000 de señalización de las llamadas del protocolo SGCP (Simple Gateway Control Protocol), que es un subconjunto del protocolo MGCP (Media Gateway Control Protocol) implementado por Cisco en el CallManager. Para evitar ataque de DoS a través de estos puertos, se deben configuran limitadores de tráfico en el switch capa 3, estos limitadores funcionan descartando el tráfico de estos puertos cuando excede un límite máximo, límite que debe ser configurado acorde al tráfico máximo, por ejemplo, que pueden generar los cuatro teléfonos IP conversando simultáneamente.

En caso que se desee conectar a la WLAN otros dispositivos inalámbricos como PDA (Personal Digital Assistant), se deben estudiar las capacidades técnicas de dicho dispositivo, y en base a eso el departamento IT debe plantear las técnicas de aseguramiento que mejor se le adapten, y que no afecten los demás mecanismos de seguridad aquí descritos.

9.5 Prueba básica de funcionamiento

A continuación se presenta el resultado de pruebas de funcionalidad del proceso de autentificación basado en PEAP. Para esta prueba se dispuso de un cliente inalámbrico compatible con PEAP y con el cifrado WPA, AP Cisco Aironet 1100, servidores de controlador de dominio y de directorio activo en producción de la empresa, y un servidor Microsoft Windows 2003 Server configurado como emisor de certificados digitales y como servidor IAS. Los equipos y servicios fueron configurados tal como se describe en el aparte 9.4 *Lineamientos de configuración 802.1X/EAP con TKIP*.

Se procedió a asociar el cliente inalámbrico a la WLAN, y se obtuvieron los siguientes resultados una vez lograda la asociación y autentificación:

En la Figura 20 se observa el evento del servicio IAS generado por la autentificación exitosa a la red inalámbrica con 802.1X.

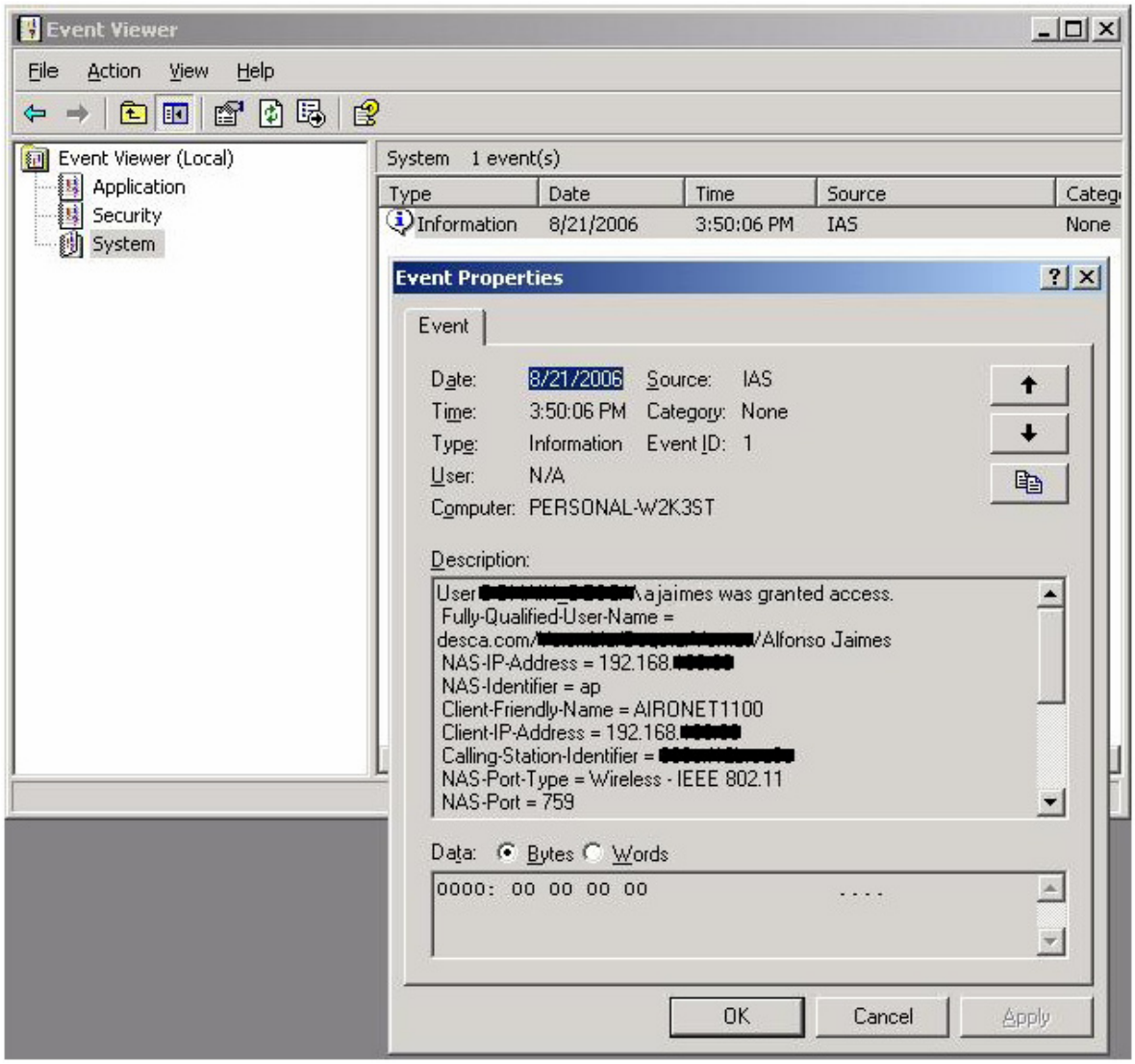

Figura 20. Evento autentificación 802.1X en el IAS

En la Figura 21 obtenida de la interfaz WEB del AP se puede observar el detalle de la conexión del dispositivo cliente con PEAP y WPA TKIP

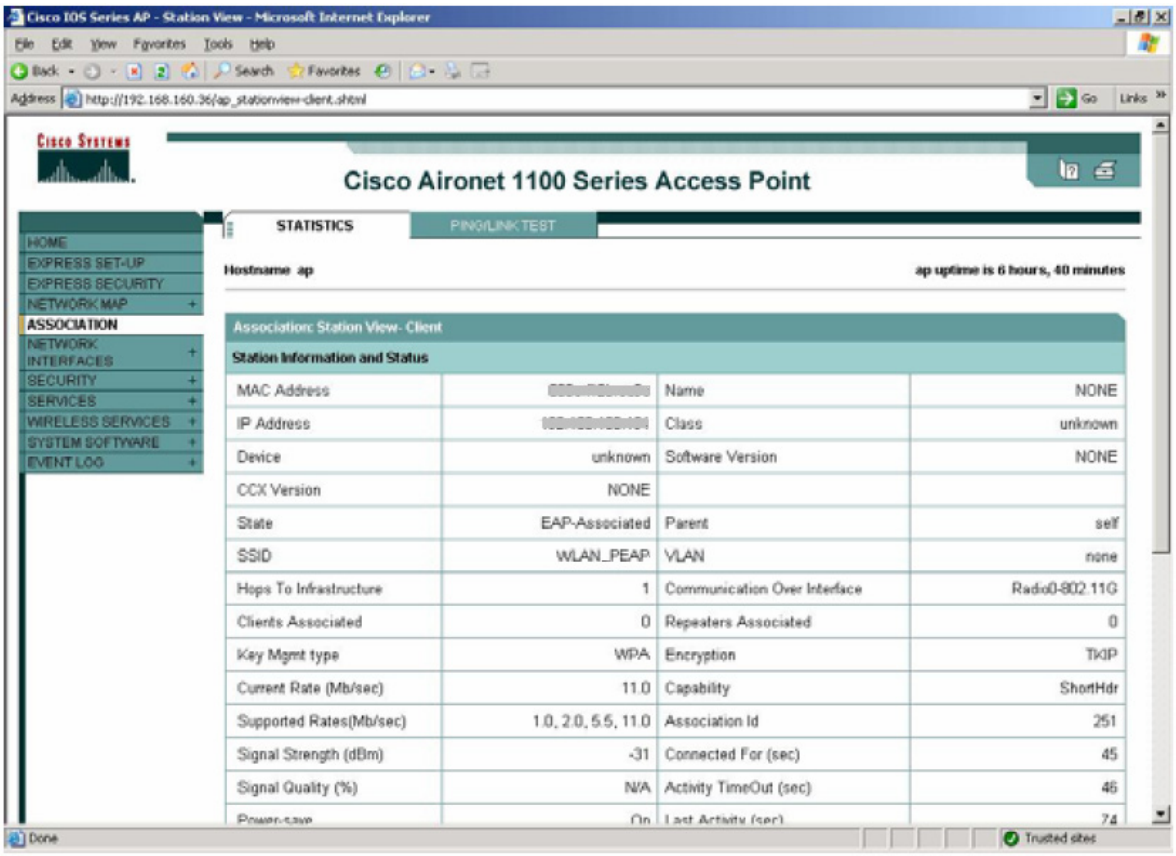

Figura 21. Detalle de autentificación PEAP y cifrado WPA TKIP

La Figura 22 es la continuación de la Figura 21. Detalle de autentificación PEAP y cifrado WPA TKIP, se continúa observando el detalle de la conexión del cliente inalámbrico con el AP, en donde se aprecia el tipo de autentificación PEAP y el cifrado WPA TKIP.

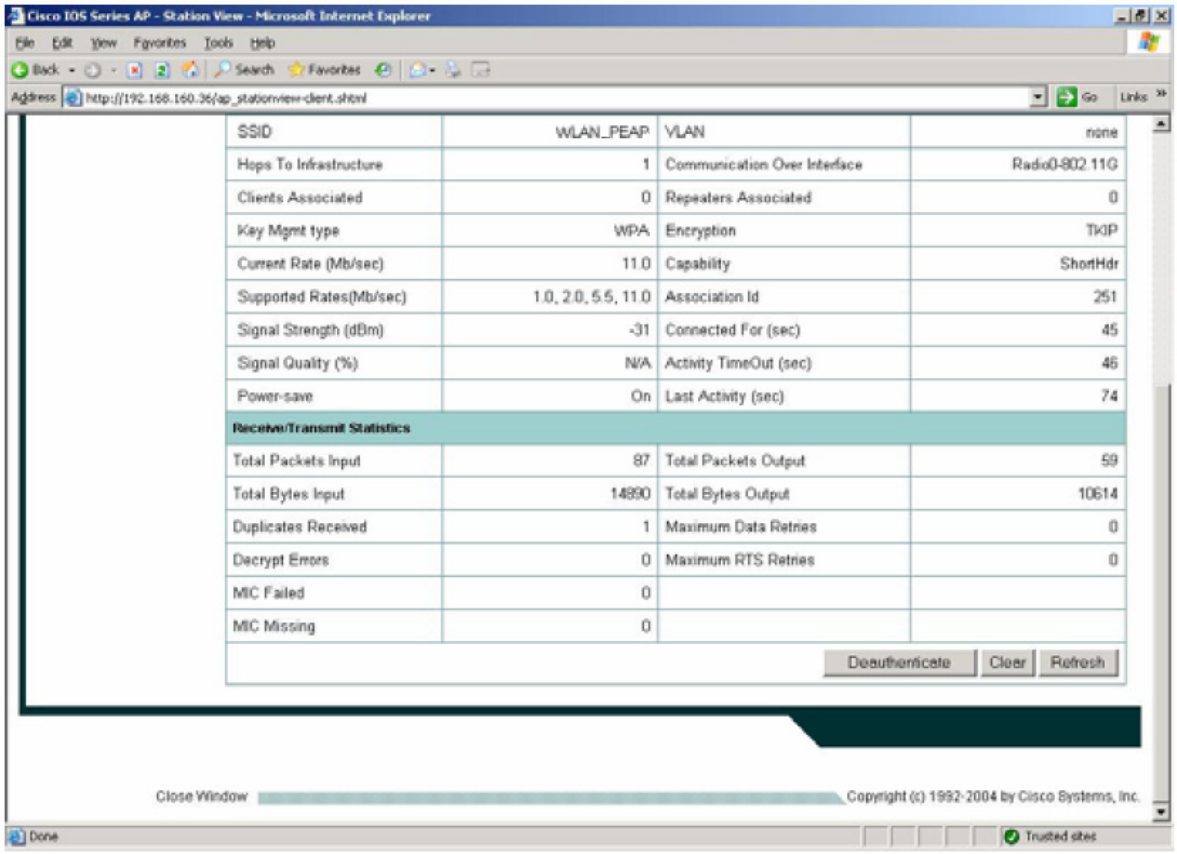

Figura 22. Detalle de autentificación PEAP y cifrado WPA TKIP(continuación)

9.6 Ejemplo de una política de seguridad para una WLAN

Políticas de seguridad para la WLAN de DESCA

Dirigido a: Todos los usuarios de la WLAN

1. Propósito

En esta política de seguridad se establecen los requerimientos para las oficinas de DESCA, las cuales garantizan que la información confidencial y tecnológica no se vea comprometida, y que los servicios en producción y demás intereses de la empresa DESCA estén protegidos

2. Alcance

Esta política de seguridad aplica a todas las oficinas conectadas a la red corporativa, a los empleados de DESCA, y a cualquier tercero que tenga acceso a las instalaciones de la empresa. Todo el equipamiento existente y futuro, que forme parte del alcance de esta política, debe ser configurado acorde con los documentos referidos en esta política. Todos los servidores y computadores dentro de la DMZ (acrónimo del inglés “Demilitarized

Zone") están exentos de esta política. Sin embargo, los computadores de la DMZ deben cumplir con las políticas de seguridad establecidas para la DMZ.

3. Políticas

3.1 Responsabilidades

1. Todos los gerentes de las oficinas son responsables de suministrar al Departamento de IT un punto de contacto (PDC) y un PDC de respaldo por cada oficina. Cada gerente de oficina es responsable de mantener al día la información de los PDC. Todos los gerentes de oficina y su respaldo deben estar disponibles en caso de presentarse una emergencia, en el caso que no lo estén, se tomarán acciones sin contar con su consentimiento.

2. Los gerentes de las oficinas son responsables de la seguridad de sus oficinas y del impacto que causen sus oficinas a la red corporativa en producción y a cualquier otra red. Los gerentes de las oficinas son responsables por mantenerse dentro de las reglas de ésta políticas y sus procesos asociados. En caso que las políticas y sus procesos asociados estén indefinidas, los gerentes de las oficinas deberán hacer su mejor empeño por salvaguardar la Corporación DESCA de vulnerabilidades de seguridad.

3. Los gerentes de las oficinas son los responsables de que sus oficinas cumplan con las políticas de seguridad de la WLAN de DESCA. Las siguientes son en particular importantes: Políticas de gestión de contraseñas de los dispositivos de red y de usuarios, Política de seguridad de la WLAN, Políticas de antivirus, y Políticas de seguridad física.

4. Los gerentes de oficinas son los responsables de controlar el acceso a sus oficinas. Sólo tendrá acceso a las oficinas aquel personal que cuente con la aprobación del gerente de la oficina, o aquel que por motivos laborales necesite acceso temporal a las oficinas. Para los accesos temporales se debe monitorear continuamente para evitar dar acceso a persona que su periodo de acceso haya expirado.

5. El departamento de IT tiene la potestad de desconectar de la red corporativa a cualquier oficina que esté generando un impacto negativo en la red

corporativa en producción o que represente un riesgo de seguridad para el desarrollo normal de las actividades propias de a empresa.

6. Todas las contraseñas de usuario deben cumplir con la política de contraseñas de DESCA. Las contraseñas de los computadores en las oficinas deben ser cambiadas cada 3 meses.

3.2 Requerimientos Generales de Configuración

1. Todo el tráfico entre la red corporativa en producción y la red de la oficina debe ir a través de un firewall administrado por el departamento IT de la empresa, ó las conexiones entre oficinas se deben hacer por medio de túneles cifrados.

2. Todas las configuraciones originales y los cambios en los equipos de red deben ser aprobados por el departamento IT de la empresa.

3. La instalación de nuevos AP a la red y su inclusión dentro de la red segura debe ser autorizada por el departamento de IT

4. Está prohibido realizar actividades de escaneo de puertos, *spamming* ó *flooding* de tráfico, o alguna otra actividad parecida que impacte negativamente el desempeño de la red corporativa y ponga en riesgo el desarrollo normal de las actividades propias de la empresa.

5. El departamento IT se reserva el derecho de auditar en cualquier momento todos los datos que tienen que ver con la oficina o los procesos administrativos, incluyendo, pero no limitado a los paquetes entrantes o salientes, firewalls, y los periféricos de red.

6. Todos los equipos que ofrecen conectividad deben cumplir con las recomendaciones de seguridad emitidas por la empresa y deben autentificarse contra los servidores de AAA de la empresa.

7. Los usuarios y contraseñas de administración de los equipos de red deben cumplir con las políticas de contraseñas de la empresa y deben autentificarse contra los equipos de autenticación corporativos. Las contraseñas de gestión de los equipos de red deben ser sólo entregadas al personal del departamento IT encargados de la administración de la red corporativa.

8. Todas las conexiones externas a la oficina deben ser revisadas y aprobadas. En caso de conexiones vía líneas analógicas, estas deben ser configuradas para sólo aceptar números confiables. Contraseñas robustas deben ser configuradas para estos casos.

4. Sanción

Cualquier empleado que se le encuentre violando esta política de seguridad podrá ser sujeto de sanciones disciplinarias, proporcionales al daño generado o al grado de incumplimiento de la política, y que pueden llegar hasta la culminación de su contrato.

9.7 Defensa ante los AP no autorizados

9.7.1 Información de los puntos de acceso no autorizados

Tal como ha sido expuesto anteriormente en este trabajo de grado, la amenaza que representa el uso de AP no autorizados puede ser atenuada. A continuación se expondrán las técnicas utilizadas para la minimización del riego que representan los AP no autorizados en una red empresarial.

Prevención

- Políticas corporativas
- Seguridad física
- Soporte robusto de infraestructura WLAN
- Uso del estándar 802.1X en los switches de acceso.

Detección

- Uso de analizadores o sniffers inalámbricos
- Uso de aplicaciones de detección desde la red cableada
- Vigilancia física del lugar de instalación y uso de los AP.

Al final de este anexo se presentará un listado de los sniffers inalámbricos más comunes.

9.7.2 Prevención de los AP no autorizados

Es prioritario para el departamento de IT de la empresa el prevenir la instalación de puntos de acceso no autorizados dentro de la red corporativa. Esto se puede lograr aplicando los siguientes correctivos

- Crear y publicar una política empresarial que prohíba la instalación de equipamiento WLAN
- Garantizar la seguridad física
- Ofrecer una buena cobertura de WLAN en toda las oficinas, para desmotivar a los usuarios a la instalación de AP no autorizados
- Uso de 802.1X
- Uso de filtros en los switch capa 2 y 3.

9.7.3 Crear una política WLAN corporativa

El primer paso es la creación de una política corporativa de seguridad que incluya la prohibición de la instalación de AP no autorizados. Esta política debe incluir quién es el personal autorizado para la instalación de AP, y qué políticas de seguridad deben cumplir estos una vez instalados. Para ello, la política debe incluir los esquemas de seguridad que el AP debe utilizar para garantizar conectividad segura a los clientes.

9.7.4 Seguridad física.

La seguridad física juega un papel importante en la prevención de los AP no autorizados. La seguridad física implica prevenir que un intruso pueda ganar acceso a los equipos o a las cercanías de la red corporativa inalámbrica. Otra forma es la detección del intruso, si éste ha logrado ganar acceso físico.

9.7.5 Ofrecer una buena infraestructura WLAN

Dado que la mayoría de los AP no autorizados son instalados por trabajadores de la misma empresa que se encuentran frustrados al no contar con acceso a la WLAN corporativa, la mejor forma de prevenir estas instalaciones no autorizadas, es la de ofrecer a todos los usuarios el acceso a una WLAN instalada, administrada y asegurada por el departamento de IT de la empresa, y de esta forma, eliminar la motivación de los empleados a instalar sus propios AP.

9.7.6 Uso de 802.1X

Los switches más recientes ofrecen soporte para seguridad basada en puertos del estándar 802.1X. Con 802.1X activado en los switches, ningún dispositivo puede ser

conectado a menos que sea capaz de ser autenticado y autorizado por un servidor RADIUS. De esta forma no sería posible la conexión de un AP no autorizado a cualquier puerto del switch con 802.1X activado.

9.7.7 Uso de filtros en los switch capa 2 y 3.

Se pueden utilizar dos tipos de filtros para los switches Catalyst de Cisco:

Filtros de direcciones MAC por puerto: se puede prevenir que el tráfico pase desde los clientes de un AP no autorizado hasta la red cableada, limitando el número de direcciones MAC que pueden ser utilizadas por cada puerto.

Filtro para descarte de tramas: existe la posibilidad de configurar el switch para que descarte las tramas que vienen de equipos de marcas distintas a Cisco. Esta opción no es factible dado que los switch no aceptan máscaras wild-cards para los filtros de direcciones MAC.

9.7.7.1 Limitaciones del uso de los filtros para la prevención de AP no autorizados

- Filtros que eviten la conexión de AP de otras marcas también evitaran la conexión de clientes de esa marca; por ejemplo, el evitar la conexión de AP de la marca A también evitara la conexión de NIC de la marca A.
- El tráfico que viene de una NIC inalámbrica posee su dirección MAC y no la del AP al cual está conectado, esto quiere decir, que si un AP de la marca A esta conectado a un puerto con un filtro para la marca A, entonces, sólo se filtrará el tráfico que venga de una NIC inalámbrica de marca A, y no será filtrado el tráfico que viene de una NIC inalámbrica marca B conectada al mismo AP marca A.
- Dado el variable mercado de los vendedores de AP, nunca habrá una lista de todos los vendedores de AP según su identificador único de organizaciones (OUI, Organizacional Unique Identifier) de la dirección MAC.
- Las direcciones MAC pueden ser cambiadas o copiadas (spoofed).

9.7.8 Detección de AP no Autorizados

Además de los mecanismos de prevención de AP no autorizados, mencionados anteriormente, el departamento de IT puede utilizar una combinación de los mecanismos de detección que a continuación se enumeran.

- Detección inalámbrica
- Detección desde la red cableada
- Detección por vigilancia física

9.7.8.1 Detección inalámbrica

La detección inalámbrica de AP no autorizados se realiza mediante el uso de equipamiento WLAN y las aplicaciones adecuadas para detectarlos.

Ventajas de la detección inalámbrica

- Con frecuencia detecta AP no autorizados que no son detectados por otros métodos
- Es efectivo para la detección de AP instalados por empleados de la empresa y que por lo general tienen configurados los valores de seguridad y SSID de fábrica.

Desventajas de la detección inalámbrica

- Este método requiere que el dispositivo inalámbrico se encuentre dentro del rango de cobertura del AP no autorizado para poder detectarlo, lo que implica que el personal de IT realice recorridos por todas las áreas de la empresa con el analizador inalámbrico
- Algunas de las aplicaciones no detectan los AP que no hacen broadcast del SSID
- No se puede realizar fácilmente el monitoreo de oficinas remotas.
- A veces puede ser difícil de detectar la señal de los AP, dado que los materiales de construcción de las edificaciones bloquean las señales 802.11.

Muchas herramientas WLAN son, en distintos grados, capaces de realizar la detección de los AP no autorizados. Más adelante, en la sección de analizadores inalámbricos de este capítulo, se listan los más comunes. Una vez es detectada una WLAN no autorizada, es recomendable el uso de antenas direccionales, por parte del analizador, para así localizar con más facilidad el AP.

9.7.8.2 Detección desde la red cableada

Los AP no autorizados pueden ser detectados desde la red cableada utilizando:

- Direcciones MAC

- Huella digital del sistema operativo
- SNMP
- Detección de intrusos

Un gran número de herramientas están disponibles para la detección de AP no autorizados desde una estación de trabajo ubicada en el segmento Ethernet de la red.

Ventajas de la detección desde la red cableada

- Es mucho más sencillo monitorear la red y se pueden obtener resultados casi en tiempo real
- Utiliza aplicaciones que trabajan automáticamente, lo que implica que requiere menos tiempo para su operación por parte del administrador
- Con este método es posible el monitoreo de oficinas remotas

Desventajas de la detección desde la red cableada

- Con este método se puede fallar en la detección de algún AP
- Este método puede crear falsas alarmas en los sistemas de detección de intrusos o de firewalls personales.

9.7.8.3 Detección utilizando direcciones MAC

Las herramientas de monitores de direcciones MAC se basan en la detección de AP no autorizados mediante la búsqueda de direcciones MAC conocidas, o también, catalogando todas las direcciones MAC conocidas de la red y buscando direcciones nuevas. La segunda opción posee la ventaja que se puede alertar cuando se conecte un dispositivo inalámbrico cuya dirección MAC es desconocida, como por ejemplo, un computador portátil no autorizado. A continuación se presenta un listado de herramientas de monitoreo de direcciones MAC.

Access Point Tools: esta herramienta puede descubrir un AP basado en su dirección MAC, y luego, chequea vía HTTP si es un AP y no un cliente inalámbrico. Esta herramienta, además puede chequear los valores configurados de seguridad y SNMP vía HTML. http://winfingerprint.sourceforge.net/aptools.php

Arpwatch: esta aplicación monitorea la actividad Ethernet y guarda en una base de datos emparejamientos de direcciones IP. Además, esta aplicación envía notificaciones de cambios vía correo electrónico.

9.7.8.4 Detección utilizando la huella digital del sistema operativo

Estas herramientas pueden ser utilizadas para descubrir las características propias (fingerprint o huella dactilar) de cada SO, como el SO de un punto de acceso. Lo hacen observando las características particulares de cada SO, como la forma que responde a paquetes TCP que contienen banderas activadas. Estas herramientas son capaces de identificar ciertos AP, pero la identificación de un AP no autorizado depende de si la herramienta posee o no almacenadas las características particulares del OS colocado por el fabricante del AP.

A continuación, algunas herramientas de fingerprinting:

NMAP: es una herramienta de código abierto para la exploración y auditoria de seguridad de una red. NMAP no es en sí una herramienta para la detección de AP no autorizados, pero puede ser útil si se usa en conjunto con otras técnicas de detección de de AP no autorizados. Esta aplicación por lo general genera muchas alertas en los equipos de detección de intrusos y en los firewall personales.

9.7.8.5 Detección utilizando SNMP

SNMP no fue pensado como una herramienta efectiva para la detección de AP no autorizados. Con toda seguridad, la mayoría de los AP no autorizados no tienen habilitada la opción de SNMP, y suponiendo que la tuviesen activada, la comunidad SNMP probablemente no sea conocida. Existen paquetes de aplicaciones para administración de redes que poseen la capacidad de realizar descubrimiento IP y SNMP en caso que se requiera la utilización de SNMP para la detección de AP no autorizados.

9.7.8.6 Detección por observación física

Los administradores del departamento IT pueden además detectar la presencia de actividad WLAN no autorizada por medio de la observación física del ambiente de trabajo. Los administradores deben estar alertas a lo siguientes:

- AP no autorizados localizados a simple vista
- Empleados que utilizan acceso inalámbrico en lugares donde no existe cobertura de la WLAN autorizada
- Si es parte de la cultura del lugar donde esta ubicada la empresa, se debe estar pendiente de simbología típica del *warchalking* que notifiquen la

presencia de redes inalámbricas. Para más información sobre la simbología: http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf.

En resumen, cada una de las técnicas de prevención o detección de AP no autorizados es por si misma limitada. Es recomendable que se elija una combinación de los métodos de prevención y herramientas de detección para la protección de la red. Cada método de prevención y herramienta de detección posee distintas ventajas y desventajas: algunas son gratuitas y de código abierto, corren en distintas plataformas como Linux, Unix o Windows, y cuentan con capacidades que se pueden complementar entre sí para ofrecerles a los administradores del departamento IT una buena combinación de herramientas para combatir los AP no autorizados.

9.7.8.7 Analizadores inalámbricos

A continuación se presenta en la Tabla 6 un listado de las aplicaciones para análisis inalámbrico.

Tabla 6. Listado de analizadores Inalámbricos

Aplicación	Características
Airmagnet	Airmagnet es un producto comercial con todas las capacidades para realizar site-survey de WLAN y que está diseñado para ser utilizado en una Compaq iPaq. www.airmagnet.com
Boingo	Boingo es una aplicación gratuita que puede ser descargado de Internet, esta busca todas las redes inalámbricas disponibles, y alerta cuando se encuentra dentro del rango de alguna de las redes, o indica donde se encuentra la más cercana. www.boingo.com
Netstumbler	Herramienta gratuita muy popular y bien conocida que puede ser descargada de Internet. Esta detecta los AP de WLAN y muestra información acerca de ellas, tales como: la potencia, la relación señal a ruido, el SSID si está disponible. Etc. www.netstumbler.org
Sniffer	Este analizador profesional puede ser utilizado para capturar tráfico inalámbrico, y mediante filtros, poder detectar los *beacons* de AP no autorizados, o definiendo filtros que permitan observar los OUI de las direcciones MAC, y de esa forma filtrar los de los AP de marcas autorizadas. www.sniffer.com
Wildpackets AiroPeek	Este es un analizador de tramas inalámbricas que mediante la aplicación de los filtros apropiados puede ser utilizado para excluir los *beacons* de los SSID autorizados, o para buscar los OUI de las direcciones MAC de los distintos vendedores de AP. www.wildpackets.com/products/airopeek
Wellenreiter	Herramienta similar a Netstumbler pero menos conocida. Wellenreiter detectas las WLAN y muestra información acerca de ellas. www.remote-esploit.org

Aplicación	Características
Kismet	Kismet es un sniffer inalámbrico de código abierto que puede ser utilizado para detectar los SSID de las redes inalámbricas pero filtrando los SSID conocidos. www.kismetwireless.net
Dachb0den	Esta es una herramienta no muy conocida que parece combinar las funciones de Netstumbler y Airsnort. www.dachb0den.com/projects/bsd-airtools.htm
Hornet	Es un dispositivo dedicado exclusivamente a buscar la dirección MAC de los AP que han sido configurados y descargados a un computador. Parece hacer no mucho más de lo que cualquier sniffer puede hacer. www.bvsystems.com/Products/WLAN/Hornet/horne.htm
IBM Distributed Wireless Security Auditor	Esta herramienta es un prototipo, y no está a la venta. Utiliza una aplicación cliente en una NIC empresarial que reporta todos los AP detectados y su configuración de seguridad, otro equipo compara todos los AP detectados con una lista de de los AP autorizados y alerta la presencia de AP no autorizados. www.research.ibm.com/gsal/dwsa
Fluke AnalyzeAir	Es una herramienta para análisis en tiempo real del espectro RF con el objetivo de detectar e identificar dispositivos inalámbricos que operan con los estándares 802.11a/b/g. Esta aplicación puede ser instalada en un computador portátil o un tablet PC. http://www.flukenetworks.com/.

9.8 Disponibilidad de la red

A continuación se describirá en detalle los elementos que deben ser considerados cuando se implementan servicios con el fin de asegurar una WLAN. Los elementos que a continuación se describen son las piezas claves que garantizan un alto nivel de disponibilidad necesaria en una red corporativa.

9.8.1 DHCP

Peticiones por segundo: el servidor DHCP, tanto el hardware como el software, deben ser capaces de soportar el número proyectado de peticiones por segundo que debe ofrecer a los clientes inalámbricos. De sobrepasarse la capacidad del servidos DHCP, los usuarios inalámbricos no serán capaces de obtener una dirección IP, negándoles a los usuarios EAP que logren la autenticación y posterior conectividad IP, o también, no permitiendo la autenticación IPSec, para luego establecer la comunicación segura VPN.

DHCP Safe Failover Protocol: el departamento IT puede instalar servidores duales que ofrezcan redundancia por medio del borrador de RFC: DHCP Safe Failover Protocol. Con la implementación de este protocolo se puede aumentar la disponibilidad de la red para los usuarios inalámbricos.

Administración de las direcciones IP de la red: el departamento IT debe considerar un plan de direccionamiento IP que sea capaz de soportar el aumento que significa la adquisición de más equipos con capacidades inalámbricas. Adicionalmente, si se elige la opción de asegurar las conexiones inalámbricas por medio de VPN IPSec, un direccionamiento IP adicional es necesario para el establecimiento de los túneles. Si en algunos de los dos casos se agotan las direcciones IP, entonces, los usuarios no podrán ganar acceso a la red corporativa.

Consideraciones de diseño de la red: es recomendable considerar dónde se localizan los servicios DHCP en función de los servicios que utilizan los usuarios. Una red redundante se requiere entre dos oficinas con el fin de lograr alta disponibilidad. Además, es recomendable que no se agrupen los servicios DHCP en una misma subred. Esto se debe a que un ataque de negación de servicio en una subred podría denegar el servicio DHCP a todos los usuarios inalámbricos.

9.8.2 RADIUS

Peticiones por segundo: en servidor RADIUS, tanto el hardware como el software, debe ser capaz de soportar la cantidad de peticiones por segundo que se hayan proyectado para los usuarios inalámbricos de la red. Si este servicio se ve sobrepasado por el número de peticiones, entonces, los AP ó concentradores VPN no serán capaces de autentificar a los usuarios inalámbricos, y de este modo, los usuarios no podrán ganar acceso a la red corporativa. Por otro lado, si los administradores del departamento IT deciden utilizar una base de datos de usuarios aparte para la autenticación de los usuarios, ésta debe ser capaz de manejar la cantidad de usuarios que sumará los usuarios inalámbricos.

Implementación se servidores redundantes: más de un servidor RADIUS debe ser instalado con el fin de brindarle a los dispositivos que requieren autenticación, concentrador VPN o AP, opciones redundantes que reciban sus peticiones de autenticación. Estas opciones redundantes deben ser configuradas en los dispositivos autentificadores de forma alternada entre la opción primaria y secundaria. Esta configuración posee dos ventajas, limita el tamaño del dominio de falla y además le permite a cada servidor RADIUS que tome el control de la red más fácilmente en caso de una falla de otro servidor RADIUS.

Administración de los usuarios: los servidores RADIUS deben ofrecer alta disponibilidad al acceso de la base de datos de usuarios que se requiere para la autenticación. Debe ser considerado el implementar servidores que mantengan sincronizadas sus bases de datos de usuarios, para que de esta forma se logre contar con un punto central de administración y se elimine la posibilidad de que un usuario esté definido un servidor RADIUS y no en otro.

9.8.3 IPSec

Conexiones por segundo: el concentrador VPN y su software debe ser capaces de soportar la cantidad de peticiones por segundo que serán requeridas por los usuarios inalámbricos.

Ancho de banda de cifrado: el concentrador VPN debe ser capaz de soportar el nivel de procesamiento y ancho de banda requerido por el cifrado de las tramas que lo atraviesan. Los concentradores VPN usan más poder de procesamiento en el cifrado de tramas pequeñas comparado con las tramas grandes y esto causa bajo ancho de banda de cifrado en los concentradores VPN. Quienes diseñan la red deben tomar en cuenta el tamaño promedio de los paquetes y su distribución en la red cableada con el objetivo de dimensionar las capacidades del concentrador VPN para la cantidad de usuarios inalámbricos.

Sesiones IPSec simultáneas: el concentrador VPN debe ser capaz de soportar la cantidad estimada de sesiones IPSec que serán establecidas con los usuarios inalámbricos. Los concentradores VPN están diseñados para manejar un número finito de sesiones simultáneas.

Una falla de diseño en un ambiente IPSec con alguna de las consideraciones expuestas anteriormente, podría causar que los usuarios inalámbricos se vean imposibilitados de ganar acceso a la red corporativa, o en caso de lograr el acceso, experimentarán un servicio degradado.

CONCLUSIONES

El estándar IEEE 802.11 en conjunto con la certificación Wi-Fi se han impuesto a nivel mundial en las WLAN, y han inundado el mercado con productos compatibles y que garantizan la interoperatividad entre marcas. Con la aprobación de nuevos extensiones a 802.11, se espera contar en un futuro cercano, con WLAN más veloces, seguras y con mejores capacidades de QoS que brinden a los usuarios un mejor servicio de conectividad inalámbrica.

Con la aprobación del estándar de seguridad IEEE 802.11i, se espera que se establezcan los lineamientos base para la implementación de técnicas de seguridad efectivas que mitiguen las vulnerabilidades relacionadas a esta tecnología, sin embargo, ya son muchos los avances de seguridad alcanzados con el conjunto de mejoras introducidos por WECA en su estándar WPA2. Con 802.11i y WPA2 se puede alcanzar altos niveles de seguridad en redes modernas y compatibles. Para WLAN ya antiguas, se cuenta con un conjunto de mejoras y mecanismos de seguridad que, aunque no ofrecen un nivel de seguridad alto, ofrecen un nivel de seguridad adecuado para uso empresarial y sin la necesidad de realizar inversiones en el reemplazo de equipamiento antiguo.

La WLAN de DESCA es una red basada en dispositivos clientes no compatibles con WPA y WPA2, sin embargo, en esta red se pueden utilizar mecanismos se aseguramiento muy parecidos a los establecidos en WPA2 y 802.11i. Con la implantación de un nuevo servidor, la instalación de los servicios de certificados digitales y RADIUS, se puede lograr implementar un esquema de seguridad en el cual se garanticen la autenticidad de los usuarios que utilizan la WLAN y la confidencialidad de los datos que transiten en la WLAN. Estas mejoras técnicas de WEP/WPA con TKIP y de los protocolos de autentificación EAP, acompañadas de un esquema de seguridad basado en políticas, le brindarían a la empresa un nivel de seguridad acorde con sus necesidades.

En la propuesta técnica de aseguramiento, expuesta en este TEG, se buscó alcanzar niveles de seguridad en la WLAN de DESCA que garanticen la integridad de la información que se maneja en la empresa. Para ello se desarrolló una propuesta basada en 802.1X/PEAP con TKIP, que utiliza los recursos tecnológicos disponibles en la empresa, y

que además brinda una experiencia de usuario transparente. Además, se sugieren políticas de administración de la red y acceso a sus recursos de forma segura.

Con la pronta implementación de la propuesta técnica de seguridad expuesta en éste TEG, y tomadas en cuenta las normas de seguridad sugeridas en el trabajo, se podrán considerar la WLAN y LAN de DESCA como seguras.

Los mecanismos, métodos y políticas de seguridad presentados en este TEG para la WLAN de la sede DESCA Caracas, son replicables en el resto de las oficinas de la empresa, y su implementación a nivel corporativo permitiría la movilidad de los usuarios inalámbricos entre todas las sedes de la empresa bajo el mismo esquema general de seguridad.

Se puede considerar que las técnicas de aseguramiento propuestas en este TEG, para aumentar el nivel de seguridad de la WLAN de la empresa DESCA, están casi completos, y el riesgo que representan las amenazas que pueden no haber sido tomadas en cuenta es mínimo comparado con las medidas que tendrían que tomarse para lograr mitigarlos.

RECOMENDACIONES

- Para la implementación de la propuesta técnica de aseguramiento de la WLAN de DESCA Caracas, es recomendable redactar un protocolo de pruebas en el cual se explique detalladamente los pasos a seguir y pruebas a realizar, que esté basado en las experiencias adquiridas en la implementación de un laboratorio funcional de pruebas, en donde se utilicen los componentes y configuraciones antes de su despliegue definitivo en la WLAN de DESCA, para así garantizar un tiempo mínimo de implementación y con el mínimo de impacto en la disponibilidad de la red.
- De ser exitosa la implementación de la propuesta en DESCA Caracas, es recomendable replicar la propuesta en las otras oficinas regionales de la empresa, y de esta forma establecer un esquema de grupos de servidores que ofrezcan servicios de red redundantes entre oficinas, con lo que se lograría aumentar la disponibilidad de la red corporativa de DESCA.
- Dado que la mayoría del equipamiento WAN, LAN y WLAN de la empresa DESCA es de marca Cisco, se recomienda estudiar la implementación de la solución Cisco de seguridad de redes inalámbrica, la cual incluye productos como Wireless LAN Solution Engine (WLSE), Cisco Secure Access Control Server (versión Cisco de un servidor 802.1X), sistemas Cisco de detección de intrusos (IDS), y que provee integración con un ambiente de red Microsoft Windows.
- Definir una política general de uso de las WLAN de la corporación DESCA, y en los casos que sea necesario, la aplicación de políticas de uso específicas a cada oficina de la empresa, y que puede variar según el país en donde se encuentre.
- Por último, para la realización de otros TEG de este tipo, se recomienda contar con el equipamiento, recursos y permisos necesarios que permitan la implementación de la propuesta técnica de seguridad expuesta en este trabajo, y así poder certificar la funcionalidad y desempeño de la propuesta en una red en producción.

REFERENCIAS BIBLIOGRAFICAS

[1]ANSI/IEEE Std 802.11, 1999 Edition (R2003). Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Reaffirmed 12 June 2003 IEEE-SA Standards Board.

[2] OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES - 09/22/06 [en línea]. <http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm> [Consulta: 2005]

[3] Security of the WEP algorithm. [en línea]. <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html> [Consulta:2005]

[4] Your 802.11 Wireless Network has No Clothes. [en línea]. <http://www.cs.umd.edu/~waa/wireless.pdf> [Consulta: 2005]

[5] Weaknesses in the Key Scheduling Algorithm of RC4 [en línea]. <http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps> [Consulta: 2005]

[6] Using the Fluhrer, Mantin, and Shamir Attack to Break WEP [en línea]. <http://warlinux.wardriving.com/doc/wep_attack.pdf> [Consulta: 2005]

[7] As in "asleap behind the wheel". [en línea]. <http://asleap.sourceforge.net/> [Consulta:2005]

[8] Securing Wireless LAN Campus Array Networks SSL VPN Solution Brief [en línea]. <http://www.arraynetworks.net/pdf/SecuringWLAN%20Campus.pdf> [Consulta: 2005]

BIBLIOGRAFÍA

- AirDefense, Inc. Best Practices for Rogue Wireless LAN Detection. [en línea] <https:// www.airdefense.net> [Consulta: 2005]
- AirDefense, Inc. Layered Approach to Wireless Network Security & Management. [en línea] <https:// www.airdefense.net> [Consulta: 2005].
- AirDefense, Inc. Wireless LAN Security: What Hackers Know That You Don't? [en línea] <https:// www.airdefense.net> [Consulta: 2005].
- AirDefense, Inc. Wireless LANs: Six Steps for Enterprise & Regulatory Policy Compliance. [en línea] <https:// www.airdefense.net> [Consulta: 2005].
- AirMagnet, The top seven security problems of 802.11 wireless. [en línea] <http://www.AirMagnet.com> [Consulta: 2005]
- AirSpace, Inc. Wireless Intrusion Detection & Prevention. [en línea] <https://www.airespace.com> [Consulta: 2005].
- AirSpace, Inc. Wireless Intrusion Detection & Prevention. [en línea] <https://www.airespace.com> [Consulta: 2005].
- Baghaei, N.; y Hunt, R., Security Performance of Loaded IEEE 802.11b Wireless Networks, Computer Communications, Elsevier, U.K., Vol 27, No 17, Noviembre 2004, pp 1746-1756
- Baghaei, Nilufar; Hunt, Ray. Security performance of loaded IEEE 802.11b wireless networks. [en línea]< http://www.elsevier.com/locate/cose> [Consulta: 2005]
- Burns, J.; y Hill, J.. Evolution of WLAN Security [en línea] <www.mtghouse.com/MDC_Evolving_Standards.pdf> [Consulta:2005]
- Burns, Jim; Hill, John. Evolution of WLAN Security. United States of America: Meetinghouse Data Communications, 2003.
- Cisco Aironet Wireless LAN Security, [en línea] <http://www.cisco.com> [Consulta:2005]
- Cisco structured wireless-aware network Q&A, [en línea] <http://www.cisco.com> [Consulta:2005]
- Cisco structured wireless-aware network, [en línea] <http://www.cisco.com> [Consulta:2005]

- Convery, Sean; Miller, Darrin; Sundaralingam, Sri. Cisco SAFE: Wireless LAN Security in Depth, [en línea] <http://www.cisco.com> [Consulta:2005]
- Flickenger, Rob. Wireless Hacks, United States of America: O'Reilly & Associates, Inc., 2003.
- Gast, Matthew. 802.11® Wireless Networks: The Definitive Guide, United States of America: O'Reilly, 2002
- Gast, Matthew. The Top Seven Security Problems of 802.11 Wireless. [en línea] <http://www.airmagnet.com> [Consulta:2005]
- Geier, Jim. Wireless LAN Security Assessments Steps, [en línea] http://www.wi-fiplanet.com/tutorials/article.php/1545731 [Consulta: 2005]
- Hassell, Jonathan. Wireless Attacks and Penetration Testing. [en línea] <http://www.securityfocus.com/infocus/1785> [Consulta:2005]
- Hurley, Chris; Puchol, Michael; Rogers, Russ; Thornton, Frank; WarDriving: Drive, Detect, Defend: A Guide to Wireless Security, United States of America: Syngress Publishing, 2004.
- IEEE 802.11™ WIRELESS LOCAL AREA NETWORKS - The Working Group for WLAN Standards. [en línea] <http://grouper.ieee.org/groups/802/11/> [Consulta: 2005]
- IEEE-SA GetIEEE 802.11 LAN/MAN Wireless LANS. [en línea] <http://standards.ieee.org/getieee802/802.11.html> [Consulta:2005]
- Khan, J.; Khwaja, A. Building Secure Wireless Networks with 802.11. United States of America: Wiley, 1era Edición, 2003.
- Manual de referencia: Cisco Aironet 1100 Series Access Point Command Reference Cisco Systems, Inc., 2004. _134 p.
- Manual de referencia: Cisco AVVID Wireless LAN Design, Solutions Reference. Network Design. Cisco Systems, Inc., 2005. _184 p.
- Manual de referencia: Cisco IOS Software Configuration Guide for Cisco Aironet Access Points. Cisco Systems, Inc., 2005. _434 p.
- Manual de referencia: Cisco 7920 Wireless IP Phone Design and Deployment Guide. Cisco Systems, Inc., 2005. _184 p.
- Manual de referencia: Give your network users freedom and mobility without giving up network security. Cisco Systems, Inc., 2005. _14 p.

- Manual de referencia: Wireless Quality-of-Service Deployment Guide. Cisco Systems, Inc., 2003. _25 p.
- Mishra, Arunesh; Arbaugh, William. An initial security analysis of the IEEE 802.1X Standard. Department of Computer Science, University of Maryland. United States of America: 2002. _12 p.
- Peikari, Cyrus; Fogie, Seth; Maximum Wireless Security, United States of America: Sams, 2002.
- Scambray, Joel; Mcclure, Stuart; Kurtz, George. Hacking exposed: Network security secrets & solutions. United States of America: Osborne/McGraw-Hill, 2001.
- Vladimirov, Andrew A.; V. Gavrilenko, Konstantin ; Mikhailovsky, Andrei A.; Wi-Foo, United States of America: Addison-Wesley, 2004.
- Von Solms, Basie; Marais, Emil. From secure wired networks to secure wireless networks - what are the extra risks? [en línea]< http://www.elsevier.com/locate/cose> [Consulta: 2005]
- Wi-FiPlanet. [en línea] <http://www.wi-fiplanet.com/> [Consulta: 2005]
- Williamson, Wade. The Best Practice For Securing Your Enterprise WLAN. [en línea] <http://www.AirMagnet.com> [Consulta: 2005].
- Wireless LAN Security Articles, Links, Whitepapers (802.11) (Wireless LAN Security & Wardriving - 802.11). [en línea] <http://www.wardrive.net/security/links> [Consulta: 2005]

ANEXO 1

Tabla 7. Características técnicas del AP Cisco Aironet 1100

Característica Técnica	Especificaciones
Software	Cisco IOS
Tasa de transferencia Suportada	802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, y 54 Mbps
Standard de Red	IEEE 802.11b ó IEEE 802.11g
Conexión Cableada	802.3 10/100BaseT Ethernet Autosensible
Banda de Frequencia	802.11g: · 2.412 to 2.462 GHz (FCC) · 2.412 to 2.472 GHz (ETSI) · 2.412 to 2.484 GHz CCK: (TELEC) · 2.412 to 2.472 GHz OFDM (TELEC)
Tipo de arquitectura de red	Infraestructura, topología en estrella
Media inalámbrico	802.11g: OFDM 802.11b and 802.11g: DSSS
Protocolo de acceso al medio	CSMA/CA
Modulación	OFDM: · BPSK @ 6 y 9 Mbps · QPSK @ 12 y 18 Mbps · 16-QAM @ 24 y 36 Mbps · 64-QAM @ 48 y 54 Mbps DSS: · DBPSK @ 1 Mbps · DQPSK @ 2 Mbps · CCK @ 5.5 y 11 Mbps
Canales de operación	802.11g ETSI: 13; América: 11; TELEC (Japón): CCK-14, OFDM-13
Canales no solapados	Tres
Sensibilidad de recepción	802.11b: · 1 Mbps: -94 dBm · 2 Mbps: -91 dBm · 5.5 Mbps: -89 dBm · 11 Mbps: -85 dBm 802.11g: · 1 Mbps: -95 dBm · 2 Mbps: -91 dBm · 5.5 Mbps: -89 dBm · 6 Mbps: -90 dBm · 9 Mbps: -84 dBm · 11 Mbps: -88 dBm · 12 Mbps: -82 dBm · 18 Mbps: -80 dBm · 24 Mbps: -77 dBm · 36 Mbps: -73 dBm

Característica Técnica	Especificaciones
	· 48 Mbps: -72 dBm · 54 Mbps: -72 dBm
Configuraciones de potencia de transmisión disponibles	802.11g: · CCK: · 100 mW (20 dBm) · 50 mW (17 dBm) · 30 mW (15 dBm) · 20 mW (13 dBm) · 10 mW (10 dBm) · 5 mW (7 dBm) · 1 mW (0 dBm) · OFDM: · 30 mW (15 dBm) · 20 mW (13 dBm) · 10 mW (10 dBm) · 5 mW (7 dBm) · 1 mW (0 dBm) La configuración de potencia máxima puede variar según las regulaciones de cada país.
Cobertura	Interiores: Distancia en un ambiente abierto de oficina · 90 ft (27 m) @ 54 Mbps · 95 ft (29 m) @ 48 Mbps · 100 ft (30 m) @ 36 Mbps · 140 ft (42 m) @ 24 Mbps · 180 ft (54 m) @ 18 Mbps · 210 ft (64 m) @ 12 Mbps · 220 ft (67 m) @ 11 Mbps · 250 ft (76 m) @ 9 Mbps · 300 ft (91 m) @ 6 Mbps · 310 ft (94 m) @ 5.5 Mbps · 350 ft (107 m) @ 2 Mbps · 410 ft (125 m) @ 1 Mbps Exteriores: · 110 ft (34 m) @ 54 Mbps · 200 ft (60 m) @ 48 Mbps · 225 ft (69 m) @ 36 Mbps · 325 ft (100 m) @ 24 Mbps · 400 ft (122 m) @ 18 Mbps · 475 ft (145 m) @ 12 Mbps · 490 ft (150 m) @ 11 Mbps · 550 ft (168 m) @ 9 Mbps · 650 ft (198 m) @ 6 Mbps · 660 ft (201 m) @ 5.5 Mbps · 690 ft (210 m) @ 2 Mbps

Característica Técnica	Especificaciones
	· 700 ft (213 m) @ 1Mbps
SNMP	MIB I y MIB II
Antena	Dipolos 2.2 dBi integrados con diversidad en espacio
Seguridad	**Autenticación:** Estándares de seguridad · WPA · WPA2 (802.11i) · Cisco TKIP · MIC · IEEE 802.11 WEP de 40 bits y 128 bits **Tipos de 802.1X EAP:** · EAP-FAST · PEAP-GTC · PEAP-MSCHAPv2 · EAP-TLS · EAP-TTLS · EAP-SIM · Cisco LEAP **Cifrado:** · AES-CCMP (WPA2) · Cisco TKIP · WPA TKIP · IEEE 802.11 WEP de 40 bits y 128 bits
Dimensiones	4.1 in. (10.4 cm) ancho; 8.1 in. (20.5 cm) alto; 1.5 in. (3.8 cm) profundidad
Peso	10.5 oz. (297 g)
Memoria del sistema	16 MB RAM 8 MB FLASH
Requerimientos de alimentación	100-240 VAC 50-0Hz 33-57 VDC
Consumo de potencia	4.9 watts, RMS
Certificación Wi-Fi