Revista Tecnológica ESPOL, Vol. Xx, N. xx, pp-pp, (Abril, 2007)

Análisis y Diseño de un Proyecto de Video Vigilancia Inalámbrica en los Laboratorios del Bloque "A" y Parqueadero Norte del Campus Peñas

Maricela Córdova Pardo[1] , Jessica Cruz Yaulema[1] , Fernanda Fueltala Narváez[1] , Ing. Néstor Arreaga[2]
Licenciatura en Sistemas de Información[1]
Maestría en Sistemas de Información Gerencial[2]
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Peñas, Malecón 100 y Loja, Apartado 09-01-5863. Guayaquil, Ecuador
marycp@hotmail.com , jacruz@espol.edu.ec , ffueltal@espol.edu.ec , narreaga@espol.edu.ec

Resumen

El presente proyecto tiene como objetivo proporcionar la información necesaria para comprender y diseñar una instalación de vídeo vigilancia en red, que permitirá disponer de una herramienta que facilite el control del mobiliario, equipos y demás, de forma fácil y segura.
El proyecto de Video Vigilancia consiste en el diseño de una red inalámbrica capaz de transmitir imágenes y video en tiempo real, a través de la tecnología Wi-Fi bajo el estándar 802.11a en la frecuencia de 5 ghz, considerando el Internet como un medio de acceso remoto por parte de los usuarios finales, y la utilización de herramientas para la notificación por correo electrónico y grabación de video como medio de respaldo.
También se describe los mecanismos de seguridad a emplear tomando en cuenta aspectos como la autenticación de usuarios y la implementación de VPN's, minimizando los riesgos de una intrusión.
El proyecto ofrece una introducción general a la composición, operación y beneficios de este sistema, los factores a considerar para su implementación y los componentes que la convierten en un sistema de altas prestaciones, de bajo coste y alto rendimiento.

Palabras Claves: *vigilancia, inalámbrica, wi-fi, autenticación, VPN.*

Abstract

The present project has like objective to provide information necessary to understand and to design installation of video monitoring in network, that will allow to have a tool that facilitates the control of the furniture, equipment and others, of easy and safe form.
The project of Video Monitoring consists of the design of a radio network able to transmit images and video in real time, through the Wi-Fi technology under the standard 802.11a in the 5 frequency of ghz, considering the Internet like means of remote access on the part of the end users, and the use of tools for the notification by electronic mail and recording of video like endorsement means.
Also one describes the security mechanisms to use taking into account aspects like the authentication from users and the implementation from VPN's, diminishing the risks of a intrusion.
The project offers a general introduction to the composition, operation and benefits of this system, the factors to consider for its implementation and the components that turn it a system of high benefits, of low cost and high performance.

1. Introducción

Una red es un elemento indispensable en el desarrollo de actividades de una Institución, integra de forma adecuada cada uno de los recursos, facilitando su administración y uso.
En los últimos años se ha producido un crecimiento espectacular en lo referente al desarrollo y aceptación de las comunicaciones móviles y en concreto de las redes de área local (Wireless LANs).
La función principal de este tipo de redes es la proporcionar conectividad y acceso a las tradicionales redes cableadas, como si de una extensión de éstas últimas se tratara, pero con la flexibilidad y movilidad que ofrecen las comunicaciones inalámbricas. La tecnología LAN inalámbrica permite al cliente comunicación computacional sin cables para acceder a los servicios de área local
El crecimiento del vídeo en red para tareas de vigilancia y monitorización está siendo impulsado no sólo por un aumento general de la necesidad de seguridad, sino que también por su mayor rendimiento y los ahorros que proporciona, su flexibilidad en el acceso a la información y la facilidad de distribución de imágenes, por su capacidad de integración, escalabilidad y muchos otros factores.
Se proporcionará una introducción general a la composición, operación y beneficios de este sistema abordará los beneficios derivados de una solución digital, los factores a considerar cuando se implementa un sistema de este tipo y los componentes que la convierten en un sistema digital de altas prestaciones

2. Video Vigilancia Inalámbrica

El sistema de video vigilancia inalámbrica representa una solución alternativa a la mayoría de los desafíos que actualmente afectan a los usuarios a la hora de instalar sistemas de seguridad y vigilancia: distancia, falta de infraestructura de red, condiciones climatológicas, precio, etc.
Una aplicación de video vigilancia Inalámbrica crea secuencias de vídeo digitalizado que se transfieren a través de una red informática permitiendo la monitorización y visualización de imágenes desde cualquier localización remota a través de Internet.
Dada su escalabilidad, entre otras ventajas, la tecnología Inalámbrica está bien establecida no sólo para mejorar o revitalizar aplicaciones de vigilancia y monitorización remota existentes, sino también para un mayor número de aplicaciones. En una solución de video vigilancia inalámbrica, hay menos equipos que mantener que en un sistema analógico y por tanto, menos componentes susceptibles de desgaste. Proporciona características como:

- Alto grado de funcionalidad
- Totalmente Escalable
- Despliegue rápido y sencillo
- Flexibilidad
- Rentabilidad de la inversión

2.1. Equipos Necesarios

Los componentes necesarios para los sistemas de video vigilancia inalámbrica son.

- Cámara Inalámbrica
- Puntos de Acceso
- Adaptadores para los Clientes
- Antenas Inalámbricas

2.2. Funcionamiento

Se crea secuencias de vídeo digitalizado que son transferidas a través de una red inalámbrica o con cable, permitiendo la monitorización y la grabación dentro de un área.
Las cámaras de red se conectan directamente a una red IP como un cliente más de la red y se integran en aplicaciones sobre la red. Su función principal es la capturar imágenes, grabar video y almacenarlo en servidores, enviar alertas al correo electrónico, permitir a los usuarios tener cámaras en lugares remotos y visualizar, almacenar y analizar vídeo en directo de otra localización o de múltiples localizaciones sobre la red o Internet. El punto de acceso (AP) es el encargado de integrar la cámara a la red inalámbrica y permitir la comunicación con otros dispositivos como son computadores

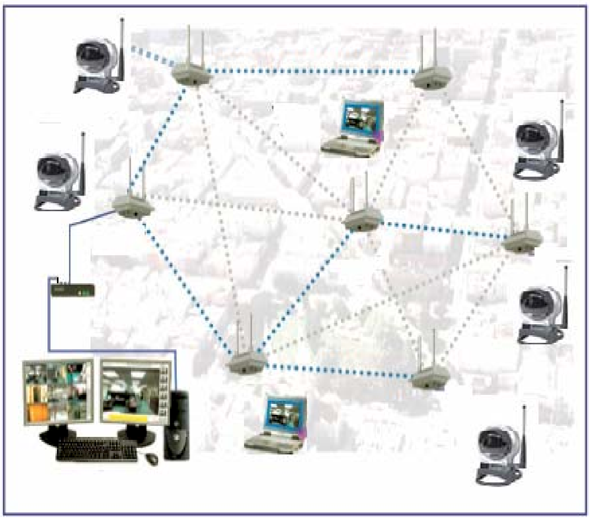

Figura 1. Vigilancia Inalámbrica

2.3. Aplicaciones

Los sistemas de vídeo vigilancia inalámbrica proporcionan soluciones rentables, flexibles y escalables, con un número ilimitado de aplicaciones. A continuación destacamos algunas de ellas:

- Distribución de Contenidos
- Complejos Educativos
- Transportes
- Entornos Públicos
- Comercios
- Industria
- Entidades Financieras
- Promoción Web

3. La Red Inalámbrica

La conforman múltiples puntos de acceso (AP's), los mismos que al ser ubicados estratégicamente, permiten extender la cobertura de la red en nuestro caso, poder cubrir todo el segundo piso del bloque A y el parqueadero norte.
En este modo, el usuario envía y recibe información a través de los AP.

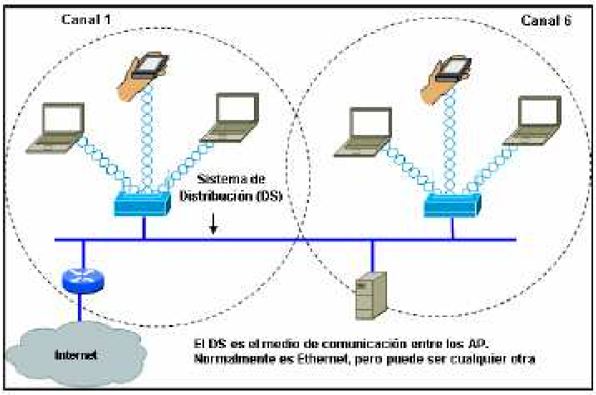

Figura 2. Topología de la Red

Para permitir a los clientes moverse físicamente dentro de una red inalámbrica, el área de cobertura debe traslaparse. En la figura 2 la célula 1 y la célula 2 traslapan sus áreas de cobertura. Cuando un cliente se mueve de la célula2 a la célula1, la información necesaria de red pasa entre el AP2 y AP1 manteniendo la conectividad LAN.

3.1. Área de Cobertura

La red de video vigilancia abarca el segundo piso del bloque A, en él se encuentran los laboratorios y auditorios de las diferentes áreas: LSI, CISCO, CELEX, LICRED y el parqueadero norte, donde se estacionan los vehículos de personas particulares, estudiantes y personal que labora en la universidad, el área a cubrir es de 4.208 metros cuadrados.

3.2. Técnicas de Despliegue Utilizadas

Para plantear un esquema de red inalámbrica, se realizó un rastreo del sitio, que se pretende cubrir, demostrando el nivel de interferencia de otros dispositivos que funcionen en el rango de frecuencias de 2.4Ghz y 5Ghz, tales como teléfonos inalámbricos y de otras redes Inalámbricas o WLAN's.
Esto también, permite identificar la ubicación de cada punto de acceso y las antenas necesarias para dar una cobertura adecuada de la celda y la capacidad del ancho de banda para evitar interferencias de canales entre puntos de acceso.
La herramienta que se ha utilizado para el análisis del proyecto es el software NetStumbler
La tabla que se muestra a continuación contiene el resumen de los datos obtenidos en base a las pruebas de análisis del sitio:

Tabla 1. Datos de Netstumbler

Ubicación	Signal + db	Noise+ db	Snr + db
Laboratorio B (CELEX)	-70	-100	30
Puerta de CELEX	-68	-100	32
Laboratorio LICRED	-69	-100	31
Laboratorio 1	-68	-100	22
Auditorio MSIG	-70	-100	30
Laboratorio 4	-65	-100	35
Laboratorio 3	-66	-100	34
Laboratorio 2	-70	-100	30
Parqueadero Norte	-64	-100	36

Los puntos de accesso se colocarán de acuerdo a estas consideraciones.

3.3. Diseño de la Red

Para cubrir el área de cobertura del bloque A y del parqueadero norte, los puntos de acceso se comunicarán entre sí bajo el estándar 802.11a en la frecuencia de 5 Ghz.
Con el objetivo de obtener velocidades promedio de 20 Mbps y disminuir la interferencia con redes inalámbricas cercanas a la nuestra, cada uno de los puntos de acceso serán configurados en los canales: 1, 5, 11 y distancias de 40 metros entre puntos de acceso.
Los puntos de acceso serán colocados en Parqueadero Norte, Laboratorio A y Laboratorio 4.
Las cámaras, computadores, se conectarán a la red de forma inalámbrica a través de los puntos de acceso bajo el estándar 802.11g en la frecuencia de 2.4Ghz.
La transferencia del contenido multimedia de la cámara inalámbrica, se realizara en el servidor local a la red.
En el servidor local, se instalarán: firewall, servicios de autenticación (RADIUS) y acceso a remoto seguro VPN, como medidas de seguridad de acceso, y la herramienta de administración y configuración de las cámaras Zone minder.
Los usuarios pueden tener acceso a la red de forma local, al conectarse inalámbricamente a la red, por lo que deberán contar con los siguientes requerimientos mencionados a continuación:

- Tener en el computador o laptop, una tarjeta wireless 802.11 a/b/g configurada con los parámetros de seguridad correspondientes definidos en las políticas de seguridad.
- Navegador web como Internet Explorer, Mozilla, Netscape, etc.
- Ubicarse dentro del área de cobertura.
- Aplicación de acceso y configuración de las cámaras inalámbricas: Zone Zinder

Una segunda opción es conectarse por medio de una red externa como Internet a través de VPN, por lo que es necesario:

- Instalar el cliente de la VPN en los computadores de los usuarios.
- Tener conexión a Internet.
- Navegador web como Internet Explorer, Mozzila, Netscape, etc.

3.4. Selección de Ubicación de los Equipos

La siguiente tabla indica la distribución de las cámaras y los puntos de acceso

Tabla 2. Ubicación de equipos

Equipo	Cant	Lugar
Cámara IP D-Link 5300G	2	Parqueadero Norte
Cámara IP D-Link 2120	1	Lab A – Celex
Cámara IP D-Link 2120	1	Lab B – Celex
Cámara IP D-Link 2120	1	Lab – Licred
Cámara IP D-Link 2120	1	Lab 1 – Cisco
Cámara IP D-Link 2120	1	Lab 3 – Cisco
Cámara IP D-Link 2120	1	Lab 4 – Cisco
Cámara IP D-Link 2120	1	Auditorio Msig
Cámara IP D-Link 2120	1	Lab 3 – Lsi
Cámara IP D-Link 2120	1	Auditorio – Lsi
Punto de Accesso Cisco Aironet 1240AG Serie 802.11a/b/g	1	Lab 4 - Cisco
Punto de Acceso Cisco Aironet 1240AG Series 802.11a/b/g	1	Lab A – Celex

Los dispositivos adicionales como lo es el servidor y switch, se ubicarán en el laboratorio LICRED, su instalación se deberá realizar considerando las normas de cableado estructucturado

4. Estudio Económico

Al realizar una comparación de costos para la implementación de un proyecto de video vigilancia, se puede ver que la adquisición de hardware y configuración para un sistema inalámbrico es superior en costos comparado a un sistema analógico, aunque a largo plazo se logra minimizar los costos de mantenimiento además de que los beneficios son significantes en cuanto al rendimiento y optimización de los recursos considerando que la maximización de los beneficios que ofrece un sistema de video vigilancia inalámbrico.

En la figura 3 se muestra la comparación de los costos de instalación de un sistema de video vigilancia inalámbrica ($9.470,41) y un sistema de video vigilancia analógica ($7.715,30).

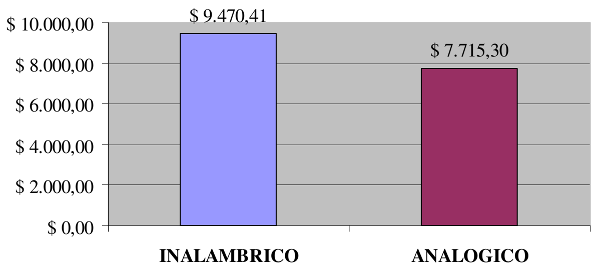

Figura 3. Cuadro Comparativo de Costos

4.1. Costo / Beneficios

Los costos de instalación de una red de vigilancia inalámbrica son superiores en comparación a los costos de instalación de una red de vigilancia analógica, ya que se consideran factores adicionales como son la seguridad en la transmisión, movilidad, no-convergencia de video, flexibilidad, lo que los convierte en equipos mas robustos.

Las redes inalámbricas ofrecen una solución de redes de vigilancia fiable que puede proporcionar seguridad al entorno externo más exigente. Los beneficios de implantar tecnologías de cámaras inalámbricas son los siguientes:

- Imagen tecnológica: La actualización e implementación de nuevas tecnologías, para cubrir necesidades que se presentan, ayudan al crecimiento de la imagen como institución competitiva dentro del medio educativo, permitiendo monitorizar y vigilar con altos niveles de rendimiento y capacidad para beneficio de la comunidad politécnica
- Accesibilidad remota: Puede acceder al vídeo en tiempo real en cualquier momento y desde cualquier ordenador. El vídeo puede almacenarse en ubicaciones remotas, por motivos de comodidad o seguridad, y la información puede transmitirse a través de la red LAN o por Internet. Esto significa que incluso las autoridades del Campus Prosperina pueden supervisar a distancia las áreas a cubrir del Campus Peñas.
- Mejorar la calidad de servicio: En cuanto a seguridad se refiere, al contar con una herramienta tecnológica que de soporte a las necesidades actuales y futuras en estas áreas.

5. Contenido Multimedia en la Red

- Notificación por correo electrónico: Las cámaras envían notificaciones a una dirección de correo electrónico cuando detectan algún movimiento en la grabación del video
- Acceso remoto controlado vía Web: proporciona facilidades a los administradores, para realizar configuraciones de las cámaras. El acceso no se verá limitado por el área de cobertura de la red inalámbrica, ya que al realizar una conexión segura como una VPN, se tendrán acceso a la aplicación en nuestro caso Zone Minder para realizar las configuraciones de modo seguro, sin poner en riesgo la integridad de la información y los recursos de la red
- Grabación de video: Permite que el usuario pueda revisar un incidente las veces que sea preciso, tanto imágenes aisladas como secuencias de video. La generación de video consiste en la transmisión de marcos de imágenes, dependiendo del ancho de banda de la red, con un ancho de banda de 1mbps la cantidad de máxima de marcos a transmitir es de 25 – 30, con ancho de banda menor a 1mbps el número de marcos disminuye

6. Seguridad

El desarrollo de una arquitectura de red segura tiene como objetivo la definición de un esquema de red aplicando medidas de seguridad informática, que una vez implementadas, minimizan los riesgos de una intrusión.
En una red de video vigilancia, usando la tecnología de redes inalámbricas basada en el estándar IEEE 802.11 ofrece beneficios incuestionables en el mundo empresarial: flexibilidad, movilidad, reducción de costes de infraestructura de red, mejor escalabilidad de la red entre otros. Sin embargo esta tecnología lleva una serie de riesgos que afectan directamente a la confidencialidad, integridad y disponibilidad de los activos e información empresarial.
Entre los riesgos mas comunes que se pueden encontrar en una red inalámbrica son:

- Intercepción y escucha del tráfico en tránsito
- Acceso no controlado a la red interna corporativa
- Denegación de servicio (DoS)

La seguridad Wireless consiste de cuatro facetas:

1. Soporte de Autenticación (Authentication Framework).- El mecanismo que aplica el algoritmo de autentificación para permitir comunicación segura de mensajes entre el cliente, el AP, y el servidor de autentificación.
2. Algoritmo de Autenticación (The Authentication Algorithm).- Algoritmo que valida las credenciales del usuario.
3. Algoritmo de Privacidad de Datos (The Date Privacy Algorithm).- Algoritmo que provee privacidad de datos a través de medios inalámbricos.
4. Algoritmo de Integridad de Datos (The Date Integrity Algorithm).- Algoritmo que provee integridad de datos a través de medios inalámbricos para asegurarle al receptor que los datos no fueron forzados

6.1. Niveles de Seguridad

La seguridad WLAN abarca dos niveles de seguridad: el acceso a la red y la protección de los datos (autenticación y encriptación, respectivamente).
Para garantizar el acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores se implementará el protocolo de autenticación para reconocimiento mutuo como es RADIUS
Y para implementar protección al tráfico de la red que permita que garanticen seguridad a la información se utilizará una VPN.

- Radius (Remote Access Dial-In User Server). Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP. Una de las características más importantes del protocolo es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y los datos se pueden utilizar con propósitos estadísticos.

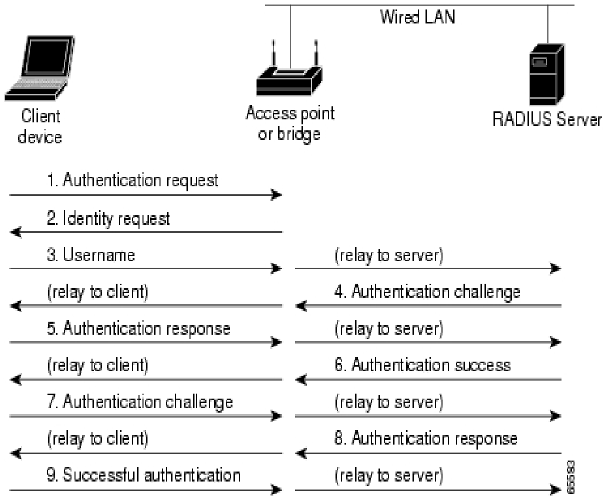

Figura 4. Funcionamiento de Radius

- VPN (Virtual Private Network) hace referencia a un protocolo especial que permite conectar una computadora a una red de forma segura. Una red privada virtual cifra las comunicaciones entre la computadora del usuario y el servidor VPN mediante un sistema que se conoce como tunelado. No importa el camino que se utilice en la comunicación (Internet, llamada directa por red telefónica, comunicación inalámbrica, etc.), que la información transmitida tendrá la garantía de no poder ser descifrada hasta que no llegue a su destino.

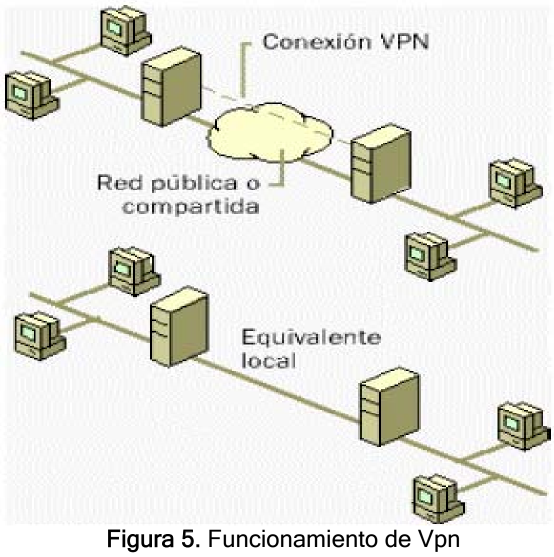

Figura 5. Funcionamiento de Vpn

6.2. Políticas de Seguridad

Las políticas de seguridad, son normas que determinan la ejecución de acciones ante los posibles ataques de acceso a la red por parte de intrusos, poniendo en riesgo la información, en nuestro caso las imágenes y video que se transmita.
Su aplicación y ejecución por parte de los usuarios finales garantiza una transmisión y acceso seguro.
Las políticas a considerar en la red de video vigilancia inalámbrica se definen a continuación.

Las políticas a considerar en la red se definen a continuación:

- Modificar la configuración predeterminada de las cuentas.
- Identificar puertos innecesarios.
- Modificar el SSID de los puntos de acceso.
- Asegurar cifrado en la información.
- Implementar Servidor RADIUS.
- Implementar VPN.
- Generar Ataques.
- Registrar las actividades de los usuarios en la red
- Controlar el área de transmisión.
- Controlar lo recursos con otros usuarios.

7. Conclusiones y Recomendaciones

Un sistema de video vigilancia inalámbrica, está capacitado para transmitir vídeo, audio y datos sin necesidad de una infraestructura física dedicada que conecte la cámara al monitor. Es una aplicación de seguridad fiable que puede desplegarse en poco tiempo en cualquier organización y se ajusta a una amplia variedad de presupuestos y necesidades de las organizaciones, pudiendo afrontar prácticamente cualquier desafío de mercado actual, desde comercios a banca a las más sofisticadas y desafiantes instalaciones de seguridad residenciales.

Aunque la solución expuesta en este documento, utiliza el Internet como medio de comunicación es necesario incorporar medidas correctas de seguridad como firewalls, protección por contraseña y sistemas sofisticados que proporcionan un mayor nivel de seguridad como VPN, servidores de autenticación. Las características de los equipos y compatibilidad garantizarán el buen uso y desempeño del sistema de video vigilancia inalámbrica.

La aplicación de políticas de seguridad descritas anteriormente, el uso adecuado de los equipos su instalación y correcto mantenimiento son muy importantes para el despliegue de una red inalámbrica que proporcionara este tipo de servicios.

Aunque el almacenamiento del vídeo proporciona numerosas ventajas para al gestión de la seguridad, es preciso hacerlo, en las limitaciones de la grabación y su visualización posterior, basándose en las potenciales legislaciones gubernativas relacionadas con la grabación de imágenes en general y las restricciones a la grabación en función de la localización.

8. Referencias

[1] Video en Red. Fecha de la última actualización 2006. Disponible en http://www.axis.com/

[2] Wireless Video Surveillance with Tropos MetroMesh Netwoks. Fecha de la última actualización Marzo 2006. Disponible en http://www.tropos.com/

[3] Enrique Pelaez, Federico Raue, “Análisis Diseño e Implementación de una Solución Técnica para Ampliar la Cobertura del Backbone la ESPOL Usando Dispositivos Inalámbricos”, Tesis, Facultad de Ingeniería Eléctrica y Computación, Escuela Superior Politécnica del Litoral, 2006.

[4] Alejandro Narváez, Angel Robles, Francisco Morán, “Red Inalámbrica de Área Local (WLAN) Aplicada a una Intranet, Campo de Estudio: Facultad de Filosofía de la Universidad de Guayaquil”, Tesis, Facultad de Ingeniería Eléctrica y Computación, Escuela Superior Politécnica del Litoral, 2005.

[5] Radius en Linux y Cisco. Fecha de la última actualización Agosto 2004. Disponible en http://www.freeradius.org/