UNIVERSIDAD TÉCNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TEMA:

"IMPLANTACIÓN DE UN SISTEMA DE RED INALAMBRICA EN EL CENTRO ASOCIADO DEL CANTÓN LA MANÁ DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI PARA LA INTERCONEXIÓN DE LAS DEPENDENCIAS Y CENTROS DE CÓMPUTO"

Tesis de Grado previa la obtención del Título de Ingenieros en Informática y Sistemas Computacionales

POSTULANTES:

Alvarez León Victor Patricio

Rosales Amores Cristian Fernando

DIRECTORA:

Dra. Anita Chancusi.

ASESOR:

Ing. Patricio Navas.

Latacunga, Junio 2008

AUTORÍA

Todos los contenidos plasmados en la presente Tesis de Grado, son de absoluta y exclusiva responsabilidad de los autores.

_____	_____
Alvarez León Victor	Rosales Amores Cristian
EGRESADO	**EGRESADO**

AGRADECIMIENTO

Deseo expresar mi agradecimiento a nuestra Directora de la Tesis, Dra. Anita Chacusi, por su calidez, sugerencias y confianza que hemos recibido de ella.

A nuestro Asesor, el Ing. Patricio Navas por su disposición y ayudas brindadas.

Nos sentimos en deuda con el Director de la Carrera, Ing. Yauli, un gran consejero en los momentos difíciles.

Desde luego, llegamos al final de este proyecto gracias al apoyo que nos otorgaron nuestros padres, esposas e hijos.

También tenemos presentes a todos nuestros amigos en especial al Ing. Jesús Gonzáles por siempre vivo en nuestros corazones, maestros y a quienes siempre nos han enseñado algo, quienes por cierto son muchos y no podríamos enumerarlos.

A todos nuestro mayor reconocimiento y gratitud.

Victor

Cristian

DEDICATORIA

Dedico la presente tesis con todo amor y cariño:

A ti Dios que me diste la oportunidad de vivir y de regalarme una familia maravillosa.

A mis padres, por el apoyo incondicional que me dieron a lo largo de mi carrera.

A los seres que más amo en este mundo: mi esposa, Maria del Carmen y mis hijos Melannie Victoria y Emilio Alejandro, por ser la fuente de mi inspiración y motivación para superarme cada día más y así poder luchar para que la vida nos depare un futuro mejor.

Victor

A mi esposa, hijas y familiares que con entero sacrificio y abnegación supieron entregarme esa confidencia ininterrumpida, esa relación clara y permanente de ayuda, para sembrar en mí el deseo de superación en este largo caminar; sus sabios consejos, su amor y su paciencia, me han impulsado hasta alcanzar y obtener mi anhelado título con esfuerzo y satisfacción.

Cristian

INDICE

Portada		i
Autoría		ii
Informe de la Directora de Tesis		iii
Agradecimiento		iv
Dedicatoria		v
Índice General		vi
Índice Tablas		x
Índice Gráficos		x
Resumen		xi
Sumary		xiii
Introducción…….…1		

CAPITULO I

1.	Estudio de la tecnología y seguridad inalámbrica……	4
1.1.	Wireless……..	4
1.1.1.	Conceptos…….	4
1.1.2.	Orígenes……	5
1.1.3.	Ámbito de aplicación……	6
1.1.4.	Estandarización de Wlan……...	8
1.2.	Wi-fi…….	10
1.2.1.	Wi-fi Alliance……	10
1.2.2.	Wi-fi: La solución a una multitud de problemas……...	10
1.2.3.	Arquitectura interna de las redes Wi-Fi……	11
1.3.	Posicionamiento tecnológico actual……..	13
1.4.	El desarrollo de la movilidad…….	14
1.5.	Aspectos de mercado wi-fi……	15
1.5.1.	Las estimaciones de las consultoras……..	15
1.5.2.	El problema de la seguridad……..	17
1.5.3.	La situación……	19
1.5.4.	Wardriving, warwalking, warchalking……..	20
1.5.5.	Modos de autenticación……	21
1.5.6.	Autentificación de sistema abierto……	21
1.5.7.	Autentificación de llave compartida……	21
1.6.	Métodos para implementar seguridad de una red…….	22

1.6.1. Aspectos básicos de la seguridad en una wlan…….. 22
1.6.2. Filtrado de direcciones MAC…… 23
1.6.3. WEP (Wired Equivalent Privacy)……..... 24
1.6.4. Las VPN……..... 24
1.6.5. 802.1x……... 25
1.6.6. WPA (Wi-Fi Protected Access)……... 25
1.7. Análisis DAFO de la tecnología wi-fi…….. 26

CAPITULO II

2. Análisis e interpretación de resultados…… 28
2.1. Resultado de la encuesta dirigida a estudiantes…… 28
2.2. Resultado de la encuesta dirigida a docentes…… 38
2.3. Resultado de la encuesta dirigida al personal administrativo… 48
2.4. Verificación de la hipótesis…… 58
2.5 Tecnología Wireless……. 58
2.5.1. Los Estándares Wlans: IEEE 802.11(A), 802.11(B), Y 802.11(G) ……. 59
2.5.2. Topología de la red wireless ……. 59
2.5.3. Tipos de Topologías wireless…… 60
2.5.3.1. Peer to Peer…… 60
2.5.3.2. Punto de Acceso…….. 61
2.5.4. Análisis de Hardware Wireless…….. 62
2.5.7. Antenas…… 63
2.5.7.1. Tipos de Antenas…….. 63
2.5.7.1.1. Antenas Direccionales (o Directivas)…….. 63
2.5.7.1.2. Antenas Omnidireccionales……. 64
2.5.7.1.3. Antenas Sectoriales…….. 65
2.5.8. ACCESS POINT (Punto de Acceso)…… 66
2.5.9. Tarjetas PCMCIA para portátiles……. 67
2.5.10. Requerimientos Técnicos……. 67
2.5.11. Servidor de cuarto de control…….. 67
2.5.12. Sistema operativo del servidor…… 67
2.5.13. Materiales para la red inalámbrica…….. 67

CAPITULO III

3. Propuesta: “IMPLANTACION DE UN SISTEMA DE RED INALAMBRICA EN EL CENTRO ASOCIADO DEL CANTÓN LA MANÁ DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI” …… 69

3.1. Presentación……... 69
3.2. Objetivo general…… 70
3.3. Objetivos específicos…… 70
3.4. Justificación……... 70
3.5. Desarrollo de la propuesta……. 71
3.5.1. Selección de los componentes de la red…….……. 72
3.5.1.1. Selección de la tecnología de la red……... 72
3.5.1.2. Selección de la topología de red…… 72
3.5.1.3. Selección de la antena a instalar…… 72
3.5.1.4. Selección del punto de acceso…….. 73
3.5.1.5. Diseño de la red wireless del campus…… 73
3.5.1.6. Direcciones IP……... 75
3.5.2. Implementar la seguridad de la red inalámbrica……. 76
3.5.2.1. Seguridad de usuarios…… 77
3.5.2.2. Características de RADIUS……. 77
3.5.2.2.1 Modelo cliente/servidor…….……. 77
3.5.2.2.2. Seguridad…… 78
3.5.2.2.3. Métodos de autentificación flexible…… 78
3.5.2.3. Funcionamiento de RADIUS……. 78
3.5.2.4. Freeradius…….. 80
3.5.2.5. Configuración del estándar 802.1x…… 80
3.5.2.5.1. Equipos que intervienen……. 80
3.5.2.5.2. Instalación del sistema operativo Linux CentOS v4.5…… 81
3.5.2.5.3. Configuración del servidor RADIUS……. 86
3.5.2.5.3.1. Archivos de configuración…….. 86
3.5.2.5.3.2. Configurando radiusd.conf…….. 86
3.5.2.5.3.3. Configurando users…….. 89
3.5.2.5.3.4. Configurando archivo eap.conf…… 89
3.5.2.5.3.5. Configurando archivo clients.conf…….. 90
3.5.2.5.3.6. Arrancar el servicio freeradius……. 90
3.5.2.5.3.7. Configuración de los equipos dlink AP-3200 y AP-2100..... 91
3.5.2.5.3.8. Configuración de 802.1x en el cliente…… 92
3.5.2.5.4. Configuración de un servidor dhcp…… 99
3.5.2.5.4.1. Configuración del archivo dhcpd.conf……..... 101
3.5.2.5.4.2. Arrancar el servicio dhcp……. 101
3.5.2.5.5. Configuración de un servidor intermediario…….. 101
3.5.2.5.5.1. Funcionamiento de un servidor intermedio……. 102
3.5.2.5.5.2. Características del servidor intermediario…… 102
3.5.2.5.5.3. Squid…… 103
3.5.2.5.5.4. Configuración del Squid…… 103

3.5.2.5.5.5. Acceso por autenticación en Squid…….. 104
3.5.2.5.5.5.1. Autenticación a través del módulo NCSA…… 104
3.5.2.5.5.6. Arrancar el servicio Squid……. 105
3.5.3. Costo de materiales utilizados en la implantación de red inalámbrica…… 105

Conclusiones y Recomendaciones
Conclusiones…… 107
Recomendaciones……. 109
Bibliografía…….. 110
Anexos

INDICE DE TABLAS

Tabla 1. Análisis DAFO de La Tecnología Wi-Fi ……. 27
Tabla 2. Ingreso de Contraseñas para acceso a la Red……..... 124

INDICE DE GRÁFICOS

Figura 1. Características de los estándares…….. 9
Figura 2. Distribución de las aplicaciones Wi-Fi…… 15
Figura 3. Estimación del número global de usuarios Wi-Fi, 2000-2008……. 16
Figura 4. Topología Peer to Peer…… 61
Figura 5. Topología Punto de Acceso……. 62
Figura 6. Antena Yagi 13dbi……... 64
Figura 7. Antena Omnidireccional……. 66
Figura 8. Antenas Sectoriales……. 66
Figura 9. Access Point…… 66
Figura 10. Tarjeta PCMCIA……. 67
Figura 11. Ubicación del Cuarto de Control y AP……. 74
Figura 12. Ubicación AP en el segundo piso…….. 75
Figura 13. Pantalla Inicial de Linux CentOS……. 81
Figura 14. Pantalla Configuración direcciones IP…….. 83
Figura 15. Configuración contraseña Súper Usuario…….. 84
Figura 16. Selección de Paquetes a instalar…… 85
Figura 17. Configuración AP-2100……..…….. 91

Figura 18. Configuración AP-3200……..…….. 92
Figura 19. Selección Panel de Control…….……... 93
Figura 20. Selección Conexiones de Red…….……... 93
Figura 21. Propiedades de Red……..…….. 94
Figura 22. Propiedades de conexiones de red inalámbrica……. 95
Figura 23. Ficha de Propiedades……. 96
Figura 24. Selección de Autenticación……..…….. 97
Figura 25. Propiedades de EAP……..……. 98
Figura 26. Propiedades de EAP MSCHAPv2……..…… 98
Figura 27. Ingreso de contraseña……..……... 99

RESUMEN

En los últimos años las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar.

Con las WLAN's la red, por sí misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red, y lo más importante incrementa la productividad y eficiencia en las entidades donde está instalada. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas.

Esta tesis presenta la implementación de una red inalámbrica para el Centro Asociado del Cantón La Maná de la Universidad Técnica de Cotopaxi, cuyo objetivo es tener acceso confiable a la red y a los servicios que presta el Centro Asociado.

Para su desarrollo se utilizó un sistema operativo basado en Linux el cual es robusto, estable, multiusuario, multitarea, multiplataforma y con gran capacidad para gestión de redes como es el CentOS 4.5. Así mismo, se realizó una implementación de servicios tales como DHCP (Protocolo de Configuración Dinámica de Máquinas), SQUID (Servidor Intermedio Proxy), RADIUS (Remote Authentication Dial In User Service) que es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP, cuyo objetivo es la de establecer los parámetros de seguridad requeridos para obtener una conexión segura.

La red inalámbrica que actualmente se encuentra instalada en el Centro Asociado del Cantón La Maná de la Universidad Técnica de Cotopaxi, fue probada en una aplicación de acceso al internet, conexión con la red cableada e intercambio de información entre redes, desde los puntos medios hasta los más extremos del campus universitario donde los resultados obtenidos de las pruebas realizadas muestran un buen balance entre la calidad de servicio y seguridad.

SUMARY

In the last year, the wireless Local Area Network (WLAN), are getting a lot of popularity that is increasing according to their service development and also because of the new applications that are discovered for them. The (WLAN) permit their users to accede to some information and resources in a real time without the necessity of being physically connected to a specific place.

With the WLANs, the network, by itself, it is mobile and eliminates the necessity to use cables and it establishes new applications adding flexibility to the network, and the most important, it increases the productivity and efficiency in the entities where it is installed. A user inside of a WLAN network can receive and transmit voice, data and videos inside of buildings, university grounds and also on Metropolitan Areas.

This thesis presents the implementation of a wireless network for the Associated Centre from Cotopaxi Technical University in La Maná Canton. Its goal is to have confident access to network and to the services that this Associated Centre presents.

For its development is used an operative system based on Linux which is robust, stable and multiuser, multitask, multiplatform and with a great capacity to manage networks like: the CentOS 4.5. Likewise, an implementation of services was made such as DHCP (Protocolo de Configuración Dinámica de Máquinas), SQUID (Servidor Intermedio Proxy), RADIUS (Remote Authentication Dial In User Service) that is a protocol of authentication and authorization for application of access to the mobility or IP network, its objective is to establish the security parameters to obtain a safe connection.

The wireless network that actually is installed in the Associated Center from Cotopaxi Technical University in La Maná Canton was proved in an application

of access to the internet, connection with the wired network and interchange of information among networks, since the middle points until the most extreme ones of the university field where the obtained results from the proofs, show a good balance between the quality of the service and the security.

INTRODUCCIÓN

Desde hace ya tiempo nos hemos dado cuenta que la tecnología ha ido creciendo constantemente. Desde la llegada de la computadora todo el mundo ha hecho lo posible por tratar de mantenerse a la vanguardia de la tecnología, con esto llego también el Internet lo cual fue un suceso muy importante para la administración de la información.

Todo tipo de empresas ya sean chicas, medianas o grandes, se han visto en la necesidad de estar al tanto de la tecnología. Y es por lo mismo que desde tiempo atrás las personas se han visto también en la necesidad de incluir en sus vidas cotidianas aparatos como dispositivos móviles, agendas electrónicas y computadoras portátiles.

Hoy en día el mercado de las tecnologías de información está muy fuerte, cada mes o incluso hasta en menos tiempo salen nuevos avances tecnológicos. Ahora bien, imagínese la maravilla de poder acceder al Internet en donde sea, en el trabajo, en la casa, en el café, en el aeropuerto, sin tener que preocuparnos por conexiones telefónicas y aun mejor sin tener que preocuparnos por los molestos cables.

Es por eso que el desarrollo de las redes inalámbricas es muy importante en la actualidad inalámbrica más utilizada hoy en día. WIFI es una abreviatura de Wireless Fidelity, también llamada WLAN (wireless lan o red inalámbrica)".

Como se puede observar es una gran ventaja el tener acceso a la información por medio de la red inalámbrica, pero un gran problema que se presenta es el de la seguridad. Si uno puede acceder a la información significa que también cualquier persona puede llegar a capturar información nuestra como cuentas, correos, contraseñas etc.

Por lo cual varios protocolos de seguridad se han desarrollado a lo largo de los años. El estándar WIFI, protocolo 802.11, además de controles como servidores

RADIUS complementando con servidores proxy como SQUID, utilizando sistemas operativos avanzados como nos brinda el LINUX CentOS.

Por todo lo anteriormente anotado la importancia de implementar una red inalámbrica en el Centro Asociado de la UTC, en el cantón La Maná, para la optimización de recursos, tratamiento de información confiable, logrando así tener un sistema de comunicación desde cualquier punto del Campus universitario, accediendo a todas las bondades de la red y una interconexión con la red cableada tanto en: datos, textos, imágenes, voz, vídeo, multimedia, etc., que beneficiará a autoridades, docentes y dicentes.

Para la elaboración de este proyecto, se realizaron algunos pasos como:

- Recopilar de toda la información de campo necesaria para conocer el estado actual del tema planteado.

- Analizar los fundamentos teóricos de las fuentes consultadas para fundamentar la investigación relacionada con el sistema de redes inalámbricas.

Cabe mencionar que se utilizó la Investigación de Campo, utilizando el Método Analítico y con la Encuesta como técnica.

Este trabajo investigativo consta de tres capítulos que son los siguientes:

El presente capítulo donde se hace una introducción que incluye, una exposición de los principales motivos que llevaron al desarrollo de la presente tesis. También en este capítulo se identifican algunos conceptos necesarios para la implantación de una red inalámbrica.

Además, se plantean los objetivos que se pretenden conseguir en la tesis.

El segundo capítulo tenemos la tabulación, análisis e interpretación de las encuestas realizadas en el Centro Asociado del Cantón La Maná de la Universidad Técnica de Cotopaxi, realizada tanto a los estudiantes, personal docente como administrativo; revisión de diversos estándares utilizados en la industria que pueden utilizarse para construir modelos de la planta bajo control; revisión de las tecnologías disponibles para ofrecer un acceso remoto seguro.

El tercer capítulo se presenta la implantación propuesta en la tesis. Este constituye la principal aportación teórica donde se explica la configuración del servidor bajo Linux CentOS como también los servicios y las seguridades que prestará la red inalámbrica.

Por último, se presentan las conclusiones y recomendaciones en las que se detallan las principales aportaciones del trabajo desarrollado.

CAPITULO I

1. ESTUDIO DE LA TECNOLOGIA Y SEGURIDAD INALÁMBRICA

1.1. Wireless

1.1.1. Conceptos

Por wireless se entiende literalmente conectividad inalámbrica, sin hilos. El contexto habitual en el que se emplea el término implica más significados, como el uso de radiofrecuencia (aunque no necesariamente, pues hay sistemas ópticos y de infrarrojos), la comunicación en cualquier sitio, la movilidad y sus aplicaciones asociadas o info-movilidad.[1]

Para el grupo investigador, una red inalámbrica es un sistema de comunicación de datos que utiliza tecnología de radiofrecuencia. En esta red se transmite y recibe datos sobre aire, minimizando la necesidad de conexiones alámbricas, es decir, combinan la conectividad de datos con la movilidad de usuarios.

La importancia de este conjunto de tecnologías reside en que permiten hacer algo cuando se necesita, en cualquier momento, desde cualquier lugar, incluso en movimiento y de una manera cómoda, al no estar la persona ceñida a las limitaciones inherentes a las comunicaciones con hilos. Además, hay otra serie de factores que están caracterizando el desarrollo espectacular de estos sistemas:[2]

[1] www.wikipedia.com

[2] http://www.alegsa.com.ar/Dic/wi-fi.php

- La facilidad del despliegue hacia el abonado en cualquier sitio: sistemas celulares, redes locales inalámbricas, sistemas fijos inalámbricos, comunicaciones por satélite.

- La propia extensión del concepto de abonado o usuario, ya que no sólo las personas, sino que también las cosas (máquinas de todo tipo) necesitan estar conectadas entre sí o a otros sistemas, para control o interacción en tiempo real.

- El fenómeno Internet como plataforma dominante para todo tipo de aplicaciones, móviles y multimedia incluidas.

- El fuerte empuje que se está dando desde el propio sector, fabricantes y operadores, como factor de crecimiento y creación de riqueza.

Por supuesto, esta rapidísima evolución comporta riesgos no sólo tecnológicos, sino también económicos o sociológicos, en aspectos tales como la info-discapacidad o la denominada "brecha digital". Resulta, por tanto, necesario hacer un esfuerzo para evitar la exclusión de personas con algún tipo de deficiencia, personas mayores o comunidades rurales y, en este sentido, la flexibilidad, comodidad y ubicuidad de los sistemas wireless pueden contribuir muy eficientemente a una mayor participación de todos en la denominada Sociedad de la Información.

1.1.2. Orígenes

El origen de las LAN inalámbricas se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, que consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE

(Institute of Electrical and Electronics Engineers), puede considerarse como el punto de partida en la línea evolutiva de esta tecnología.[3]

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread-spectrum"(frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en "spread-spectrum". IMS es una banda para uso comercial sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda.

La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezara a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.

1.1.3. Ámbito de Aplicación

Para el grupo investigativo, en la actualidad las redes WLAN han encontrado una gran variedad de nuevos escenarios de aplicación tanto en el ámbito residencial

[3] http://www.unincca.edu.co/boletin/indice.htm

como en entornos públicos, más allá de su origen corporativo. Estas nuevas aplicaciones son:[4]

- ***Escenario Residencial**:* Una línea telefónica terminada en un router ADSL al cual se conecta un AP para formar una red WLAN que ofrece cobertura a varios ordenadores en el hogar.[5]

- ***Redes Corporativas***: Una serie de Puntos de Acceso distribuidos en varias áreas de la empresa conforman una red WLAN autónoma o complementan a una LAN cableada. Son aplicaciones de alta densidad tráfico con altas exigencias de seguridad.

- ***Acceso público a Internet desde cafeterías, tiendas, etc*.** En estos establecimientos se ofrece a los clientes una tarjeta inalámbrica (NIC) que permiten acceso a Internet desde sus propios portátiles o PDA's. Es un escenario de acceso, involucrando un bajo número de Puntos de Acceso, parecido al residencial, pero que necesita mayores funcionalidades en el núcleo de red.

- ***Acceso público de banda ancha en entornos rurales***, hoteles, campus universitarios. En general este escenario necesita múltiples Puntos de Acceso para garantizar la cobertura del área considerada.

- Es necesario distinguir entre dos tipos de redes: **las *redes sin ánimo de lucro o redes libres*** que ofrecen un servicio gratuito a una comunidad. El otro tipo de redes son las redes que ofrecen servicios de pago a clientes que residen o transitan por la zona de cobertura. Las redes públicas son del tipo de pago por servicios siempre hay un operador de telecomunicaciones detrás de su gestión. Un operador establecido (especialmente los móviles)

---

[4] http://209.85.215.104/search?q=cache:QCnj3FjIitMJ:www.knotik.com/fich_documentos/11_presentacin_sobre_wifi+escenario+residencial+%2Bwifi&hl=es&ct=clnk&cd=1&gl=ec

[5] http://www.canariaswireless.net/modules.php?name=News&file=article&sid=756

dispone de gran parte de la infraestructura necesaria para ofrecer un servicio de amplia cobertura. Actualmente existen varios tipos de operadores actuando en el sector WLAN: Operadores "Wireless ISP" que ofrecen cobertura local de banda ancha en pueblos o en pequeñas ciudades utilizando WLAN. Operadores "Wireless ISP" que ofrecen cobertura nacional en los puntos de alta densidad de trafico conocidos como "hot spots".

- ***WLAN para cobertura de "Hot Spots"***. Estas redes cubren áreas donde se concentra un gran número de usuarios de alto tráfico como son aeropuertos, estaciones de ferrocarril, centros de congresos, etc. La red a instalar requiere un elevado número de Puntos de Acceso así como importantes exigencias de seguridad, gestión de red, facilidades de facturación, etc.

- ***Acceso a Internet desde medios públicos de transporte***. Algunas compañías ferroviarias quieran ofrecer acceso de banda ancha desde sus trenes en movimiento, compañías aéreas que ofrecen acceso a Internet desde sus vuelos intercontinentales o incluso compañías de autobuses urbanos. En mucho de estos casos la solución está basada en un acceso Wi-Fi en el interior del avión que termina un enlace vía satélite con la red Internet. En las otras aplicaciones Wi-Fi forma parte tanto de la red de acceso como de la solución de transporte hacia la red fija.

1.1.4. Estandarización de Wlan

Precisamente ha sido la estandarización de los productos la que ha dado lugar al tremendo auge que está teniendo este tipo de tecnología. La estandarización ha permitido desvincularse de tecnologías propietarias, consiguiendo una plataforma abierta con productos de mayores prestaciones y a un precio mucho más ajustado.

El grupo investigador opina que, aunque las redes inalámbricas necesitan cumplir con determinadas normas que se aplican de igual forma al mundo de las redes cableadas, esta estandarización requiere del cumplimiento de una normativa específica que permita controlar su comportamiento con respecto al uso de los recursos radioeléctricos.

A mediados del año 1997, el IEEE ("Institute of Electrical and Electronics Engineers") hizo público el estándar 802.11 que definía las especificaciones para las WLAN, y poco después, a finales de 1999, vio la luz el estándar 802.11b que daría lugar posteriormente a la denominación Wi-Fi. Básicamente, esto significa que, vía radio, se mantienen las características de una conexión Ethernet cableada.

El grupo de trabajo 802.11 es el responsable del desarrollo de los estándares de redes de área local inalámbricas bajo los auspicios del Comité de Estándares del proyecto 802 de LAN/MAN del IEEE.

Estándar WLAN	802.11b	802.11a	802.11g	802.11h	HiperLAN2	Bluetooth
Organismo	IEEE(USA)	IEEE	IEEE	IEEE	ETSI(euro)	Bluetooth SIG
Finalización	1999	2002	Jun,2003	2003	2003	2002
Denominación	Wi-Fi	Wi-Fi5				
Banda frecuencias	2.4GHz (ISM)	5 GHz	2.4GHz (ISM)	5 GHz	5 GHz	2.4 GHz
Velocidad máx.	11 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	0.721Mbit/s
Throughput medio	5,5 Mbps	36 Mbps			45 Mbps	
Interfaz aire	SSDS/FH	OFDM	OFDM	OFDM	OFDM	DSSS/FHSS
Disponibilidad	>1000	algunos	algunos	algunos	(2004)	Muchos
Otros aspectos				TPC, DFA		
Nº de canales	3c no solapados	12 no solapados	3 no solapados	19 no solapados		

Figura 1. Características de los estándares

1.2. WI-FI

1.2.1. WI-FI Alliance

Wi-Fi Alliance (anteriormente WECA, "Wireless Ethernet Compatibility Alliance") es una organización internacional, sin ánimo de lucro, formada en 1999 para certificar la interoperabilidad de productos inalámbricos de redes de área local basados en la especificación del IEEE 802.11. Actualmente la Wi-Fi Alliance tiene más de 200 miembros alrededor del mundo, que representan a un nutrido grupo de relevantes empresas y más de 1.000 productos han recibido la certificación Wi-Fi® desde que el proceso de certificación empezase en Marzo de 2.000. El objetivo de los miembros de la Wi-Fi Alliance es enriquecer la experiencia de los usuarios a través de la interoperabilidad de sus productos.[6]

Antiguamente la agrupación era conocida como WECA, pero cambió su nombre en octubre de 2002.

1.2.2. WI-FI: La Solución a una Multitud de Problemas

Las soluciones ofrecidas por la telefonía celular han estado disponibles ya desde hace tiempo ofreciendo a los usuarios la capacidad de trasladarse, mientras permanecen conectados, dentro de grandes áreas geográficas y a costos elevados. Las redes Wi-Fi ofrecen la misma posibilidad sin la desventaja del alto costo, pero sobre áreas geográfica limitadas. Los sistemas Wi-Fi ofrecen velocidades de transmisión de datos superior en un factor de 2 a 3 órdenes de magnitud, respecto a los sistemas 2.5G celulares. El bajo costo de instalación y operación de las redes Wi-Fi crea enormes oportunidades para su aplicación de una manera estándar a problemas que hasta el momento no han sido resueltos o han requerido soluciones a medida y costosas.

Desde el punto de vista del grupo investigativo las redes Wi-Fi solucionan una multitud de problemas para los usuarios, pudiendo ser estos estudiantes,

[6] http://www.wi-fi.org/

residenciales y de negocios, pero la mayoría de estas soluciones emergen de la libertad de obtener acceso a la red sin estar atados a cables.

1.2.3. Arquitectura Interna De las Redes WI-FI

El elemento fundamental de la arquitectura de las redes 802.11 es la celda, la cual se puede definir como el área geográfica en el cual una serie de dispositivos se interconectan entre sí por un medio aéreo. En general, esta celda estará compuesta por estaciones y un único punto de acceso. Las estaciones son adaptadores que permiten la conversión de información, generalmente encapsulada bajo el protocolo Ethernet, existente en terminales o equipos clientes, y su envío y recepción dentro de la celda. El punto de acceso es el elemento que tiene la capacidad de gestionar todo el tráfico de las estaciones y que puede comunicarse con otras celdas o redes. Es a todos los efectos un bridge que comunica a nivel 2 (enlace) los equipos, tanto de su celda de cobertura, como a otras redes a las cuales estuviese conectado. A esta configuración se le denomina Grupo de Servicio Básico BSS ("Basic Service Set").[7]

El grupo investigador opina que las redes inalámbricas basadas en el estándar IEEE 802.11, son una tecnología que aporta beneficios considerables en términos de flexibilidad, escalabilidad y movilidad, pero que tiene un gran impacto en la infraestructura operaciones y seguridad de la información de las organizaciones.

El BSS es, por tanto, una entidad independiente que puede tener su vinculación con otros BSS a través del punto de acceso mediante un Sistema de Distribución (DS, "Distribution System"). El DS puede ser interrogado (comunica el BSS con una red externa), cableado (con otros BSS a través de cable como por ejemplo una

[7] http://209.85.215.104/search?q=cache:-X2YT8f_6PsJ:casafutura.diatel.upm.es/rrssmd/trabajos/2004/powerpoint/13.-%2520Redes%2520Wi-Fi%2520(M.ALcaraz).pdf+arquitectura+interna+redes+wifi&hl=es&ct=clnk&cd=1&gl=ec

red Ethernet fija convencional), o también inalámbrico, en cuyo caso se denomina Sistema de distribución inalámbrica ("Wireless Distribution System").

Sobre este concepto básico surge una serie de alternativas:

- ***BSS independiente (IBSS, "Independent Basic Service Set").*** Es una celda inalámbrica en la cual no hay sistema de distribución y, por tanto, no tiene conexión con otras redes.

- ***Modo Ad-hoc.*** Es una variante del IBSS en el cual no hay punto de acceso. Las funciones de coordinación son asumidas de forma aleatoria por una de las estaciones presentes. El tráfico de información se lleva a cabo directamente entre los dos equipos implicados, sin tener que recurrir a una jerarquía superior centralizadora, obteniéndose un aprovechamiento máximo del canal de comunicaciones. La cobertura se determina por la distancia máxima entre dos equipos, la cual suele ser apreciablemente inferior a los modos en que hay un punto de acceso. Es un modo de empleo infrecuente por las connotaciones de aislamiento que conlleva aunque puede ser muy útil cuando el tráfico existente se reparte entre todos los equipos presentes.

- ***Modo infraestructura.*** El punto de acceso realiza las funciones de coordinación. Todo el tráfico tiene que atravesarlo, por lo que hay una clara pérdida de eficiencia cuando dos estaciones dentro de un mismo BSS desean comunicarse entre sí (los paquetes de información son enviados una vez al punto de acceso y otra vez al destino). Es una arquitectura apropiada cuando la mayor parte del tráfico se origina o finaliza en las redes exteriores a las cuales está conectado el punto de acceso. La cobertura alcanza una distancia cercana al doble de la distancia máxima entre punto de acceso y estación. Es el modo que se emplea habitualmente para conectar una red inalámbrica con redes de acceso a Internet (ADSL –

"Asymmetrical Digital Subscriber Line"- , RDSI –Red Digital de Servicio Integrados-,..) y redes locales de empresa.

- ***BSS extendido (ESS, "Extended Service Set").*** Es un caso específico del modo infraestructura, representado por un conjunto de BSS asociados mediante un sistema de distribución. Esto permite una serie de prestaciones avanzadas opcionales como el roaming entre celdas.

Para poder identificar de manera inequívoca a las celdas inalámbricas se les asigna un nombre de red consistente en una cadena con longitud máxima de 32 caracteres denominado "Service Set Identifier", SSID. Para poder agregarse a una determinada celda es requisito indispensable que el equipo tenga en su configuración interna el mismo SSID. Si se desea que la estación se conecte a cualquier celda inalámbrica presente, se deberá poner como parámetro "ANY".

Inmediatamente el equipo analizará todas las celdas que están presentes y se conectará a una de ellas adoptando su SSID, generalmente con el criterio de la que mayor nivel de señal posea.

1.3. Posicionamiento Tecnológico Actual

El desarrollo científico-tecnológico en el ámbito de las telecomunicaciones se orienta hacia la consecución de una mayor rapidez y eficiencia en los procesos, una mayor comodidad para el usuario, un mayor control de la naturaleza y el entorno.

Dentro del desarrollo tecnológico, es posible destacar los dos elementos que más han influido beneficiosamente en los últimos años:

- ***La mejora del acceso***, especialmente en sus componentes de capacidad y ubicuidad, representadas en particular por la banda ancha, las nuevas tecnologías de difusión y la movilidad.

- ***La interoperabilidad de redes y servicios***, en particular mediante el empleo de los servicios abiertos y del paradigma IP.

Son estos tres conceptos: banda ancha, movilidad y servicios abiertos los que van a marcar el éxito de una tecnología.

1.4. El Desarrollo de la Movilidad

Los investigadores opinan que una red inalámbrica permite conectar varios dispositivos o equipos a una red sin necesidad de usar cables. Gracias a las tecnologías inalámbricas, es posible acceder a recursos compartidos, en especial Internet, desde diferentes ubicaciones: esto se llama "movilidad".

Actualmente, el trabajo del día a día en las empresas requiere, por un lado, un acceso permanente a Internet o a la red corporativa y, por otro, que los empleados puedan acceder a ella de forma transparente cualquiera que sea su situación.[8]

El cable no permite movilidad y por tanto, los trabajadores se encuentran limitados a su ordenador y a la conexión por cable que éste tiene hacia Internet o la Intranet empresarial.

Las ventajas económicas respecto al cable se empiezan a apreciar desde el principio. Así, por ejemplo, cablear toda una oficina requiere de un mayor tiempo y, por supuesto, unos costes elevados. Esto no ocurre con la tecnología inalámbrica. La conexión de todos los equipos a la red inalámbrica puede hacerse en cuestión de horas (dependiendo del tamaño de la oficina) y los costes de esta

[8] http://www.ieco.clarin.com/notas/2008/02/11/01605261.html

implementación son menores, ya que la necesidad de mano de obra es menor, al igual que el número de los materiales empleados.

Además, ante un cambio de sede social, todos estos cables y conexiones no podrán ser utilizados en la nueva oficina, con lo que la inversión realizada no se recuperará. Sin embargo, todos los dispositivos que conforman una red inalámbrica pueden ser trasladados sin ningún tipo de problema, por lo que no volverá a tener que realizar ese gasto: la inversión está garantizada.

1.5. Aspectos de Mercado WI-FI

1.5.1. Las Estimaciones de las Consultoras [9]

Entre las predicciones tecnológicas para 2004, todas las grandes consultoras coinciden en señalar el desarrollo de las tecnologías Wi-Fi como una de las que presentan mayor potencial de crecimiento.

Lo que se refiere a la distribución de las aplicaciones Wi-Fi, se estima que los ordenadores personales (portátiles y de sobremesa) será el principal destino de las mismas, pero no desestima el impacto que tendrán en teléfonos móviles y PDAs.

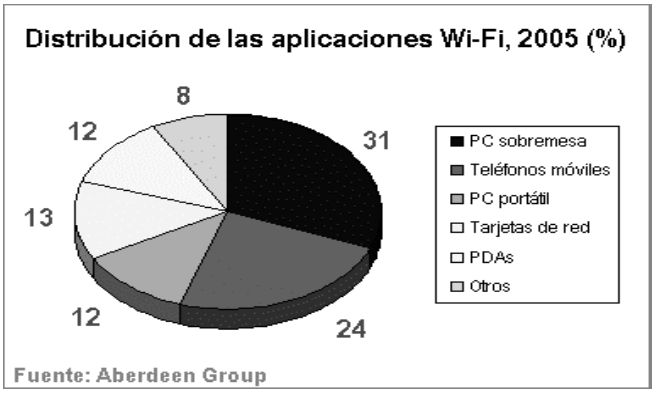


Figura 2. Distribución de las aplicaciones Wi-Fi

[9] http://www.baquia.com/noticias.php?id=7771

Según un informe de la consultora y analista de mercados Pyramid Research, fechado en julio de 2003, en la actualidad, alrededor de 50 millones de usuarios utilizan soluciones Wi-Fi a nivel mundial, y en cinco años se prevé que esta cifra crezca de forma exponencial. El número de usuarios llegará a los 700 millones para 2008.

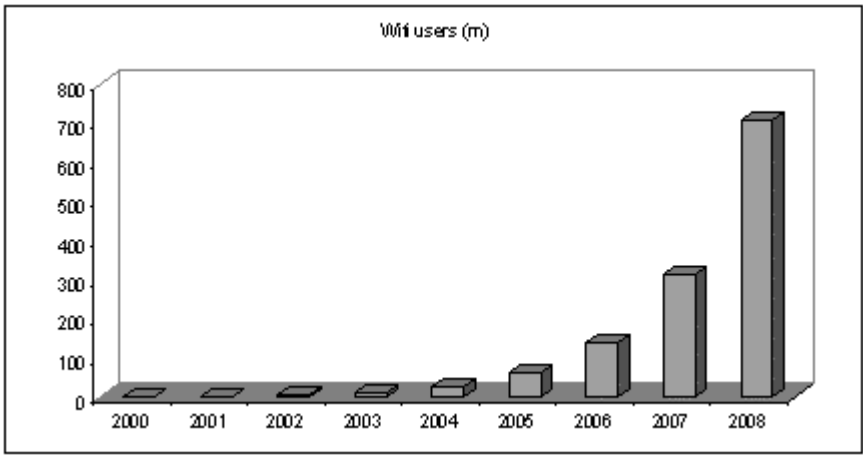


Figura 3. Estimación del número global de usuarios Wi-Fi, 2000-2008

De las tablas anteriores se pueden extraer las siguientes conclusiones:

- El crecimiento general del mercado Wi-Fi es enorme.
- La explosión de las aplicaciones privadas frente a las públicas.
- El mercado Norteamericano representa hoy en día, más del 50% del total, tanto en número de usuarios como de puntos de acceso.

Por otro lado, y haciendo referencia a las comunicaciones inalámbricas, se advierte que Wi-Fi se constituirá como una de las tecnologías más fuerte, alternativa que generará un volumen de negocio de unos 1.589 millones de euros durante el presente año. Según esto, en el estudio se señala que serán las redes WLAN privadas o semiprivadas, tales como las de ayuntamientos o

universidades, las que registren un mayor aumento, el cual vendrá favorecido por la calidad de servicio y la seguridad .

1.5.2. El Problema de la Seguridad.[10]

Si la instalación está abierta, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar la conexión a Internet, sino también acceder a la red interna o analizar toda la información que viaja por la red y obtener así nuestras contraseñas, cuentas de correo, el contenido de nuestras conversaciones por MSN, etc.

Para el grupo investigador, los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio las mismas que pueden viajar más allá de las paredes y filtrarse en habitaciones, casas, oficinas contiguas o llegar hasta la calle.

- ***Puntos ocultos:*** Este es un problema específico de las redes inalámbricas, pues suele ser muy común que los propios empleados de la empresa por cuestiones de comodidad, instalen sus propios puntos de acceso. Este tipo de instalaciones, si no se controlan, dejan huecos de seguridad enormes en la red. El peor de estos casos es la situación en la cual un intruso lo deja oculto y luego ingresa a la red desde cualquier ubicación cercana a la misma. La gran ventaja que queda de este problema es que es muy fácil su identificación siempre y cuando se propongan medidas de auditorías periódicas específicas para las infraestructuras Wi-Fi de la empresa, dentro del plan o política de seguridad.

- ***Falsificación de AP:*** Es muy simple colocar una AP que difunda sus SSID, para permitir a cualquiera que se conecte, si sobre el mismo se emplean técnicas de “Phishing”, se puede inducir a creer que se está

[10] http://www.wikilearning.com/curso_gratis/seguridad_en_wifi_tecnico-problemas_concretos_de_seguridad_en_wifi/4171-4

conectando a una red en concreto. Existen varios productos ya diseñados par falsificar AP, en la terminología WiFi se los suelen llamar “Rogue AP” o Fake AP”, el más común es un concocido srcipt en Perl denominado justamente “FakeAP”, que envía Beacons con diferentes ESSID y difernetes direcciones MAC con o sin empleo de WEP.

- ***Deficiencias en WEP (Características lineales de CRC32):*** Esta característica fue demostrada en teoría por Nikita Borisov, Ian Goldberg y David Wagner. El ICV permite verificar la integridad de un mensaje, por lo tanto, el receptor aceptará el mensaje si su ICV es válido (Recuerdo que es un simple CRC32). Esto presenta dos problemas:

- ***Deficiencias en el método de autenticación:*** Si un atacante captura el segundo y tercer mensaje de administración en una autenticación mutua. El segundo posee el desafío en texto plano y el tercero contiene el mensaje criptografiado con la clave compartida. Con estos datos, posee todos los elementos para autenticarse con éxito sin conocer el secreto compartido (Con esto sólo logra autenticarse, luego queda el acceso a la red).

- ***Debilidad en WPA***: Un estudio realizado por Robert Moskowitz, director de ICSA Labs, indica que el sistema utilizado por WPA para el intercambio de la información utilizada para la generación de las claves de cifrado es muy débil. Según este estudio, WPA en determinadas circunstancias es incluso más inseguro que WPE. Cuando las claves preestablecidas utilizadas en WPA utilizan palabras presentes en el diccionario y la longitud es inferior a los 20 caracteres, el atacante sólo necesitará interceptar el tráfico inicial de intercambio de claves. Sobre este tráfico, realizando un ataque de diccionario, el atacante puede obtener la clave preestablecida, que es la información necesaria para obtener acceso a la red. Es decir, a diferencia de WEP en que es necesario capturar un volumen significativo de tráfico para poder identificar las claves, en WPA

únicamente capturando el tráfico de intercambio de claves para poder realizar este ataque de diccionario. No es un problema nuevo, pues fue apuntado durante la verificación inicial del protocolo. Es solo una muestra que una implementación inadecuada puede afectar negativamente cualquier sistema de cifrado. Como hemos indicado, el problema solo es explotable bajo una serie de circunstancias muy concretas. Este problema puntual no es, en absoluto, una indicación de la debilidad de WPA. Únicamente es un recordatorio de la necesidad de utilizar claves convenientemente largas y que incluyan caracteres especiales.

1.5.3. La Situación

Una de las debilidades normalmente atribuidas a las tecnologías inalámbricas, y más en concreto a la tecnología Wi-Fi, es la falta de seguridad. Nos referimos, no tanto a la seguridad física sino, a la seguridad de la información, su integridad y a la no accesibilidad a terceros. Como elemento clarificador de la situación anterior valga lo siguiente:

Recientemente HP Services ha presentado un estudio que muestra la deficiente protección de los puntos de acceso inalámbricos. La compañía examinó en la práctica el estado de las redes wireless y su nivel de seguridad en determinadas zonas de la Comunidad de Madrid. Con el fin de comprobar in situ los bajos índices existentes, la compañía encargada de hacer este estudio montó a los medios de prensa en un autobús que recorrió parte del paseo madrileño de la Castellana y sus inmediaciones. En un plazo de una hora, y mediante el uso de un software específico, se captaron más de 80 redes, una gran mayoría de las cuales no contaban con los requisitos mínimos de seguridad (nivel de cifrado).

El estudio realizado con un ordenador portátil, tarjeta Wi-Fi, una antena omnidireccional y una direccional y un GPS (tras deshabilitar la obtención de dirección IP para evitar cualquier tipo de intrusión) detectó 747 puntos

inalámbricos que podrían corresponder a unas 518 organizaciones, de las cuales un 10% son grandes empresas (cuatro o más puntos de acceso), un 76% pymes (menos de cuatro) y un 15% usuarios particulares (un único punto). De todas ellas, el 68 por ciento no tenían configurada la seguridad. Por segmentos, más de la mitad de las grandes cuentas no disponía de los sistemas de seguridad más básicos, mientras que sólo el 31 por ciento de las pymes detectadas tenían activados sus sistemas de seguridad.

Como conclusión, queda de manifiesto que, en esta situación, cualquier usuario externo pueda utilizar libremente estas redes tanto corporativas como pertenecientes a usuarios domésticos.

1.5.4. Wardriving, Warwalking, Warchaking.[11]

Son palabras anglosajonas inventadas por "hackers" expertos que informan al público en Internet sobre la localización y configuración de redes inalámbricas Wi-Fi. Gran cantidad de aficionados se han dedicado a recorrer a pie (warwalking) y en coche (wardriving) los distintos países dotados de un ordenador portátil o PDA equipados con un cliente inalámbrico Wi-Fi, una antena direccional y un GPS. Así elaboran mapas disponibles en Internet donde se indica la situación de todas las redes inalámbricas encontradas y su nivel de seguridad (ver http://www.wifimaps.com). Han llegado a inventar un código de signos de estilo "grafitti" para marcar las zonas de cobertura informando si la red es segura o es fácil entrar a ella (warchalking).

Actualmente existen diversas iniciativas en marcha y se cuentan por decenas de miles el número de Hot-spots distribuidos por el mundo. A través de Internet podemos encontrar localizadores de Hot-spots que nos sitúan geográficamente los

11 http://209.85.215.104/search?q=cache:wDlGxrJmsWUJ:www.coit.es/pub/ficheros/informewificoit_definitivo_2464518b.pdf+WARDRIVING,+WARWALKING,+WARCHALKING&hl=es&ct=clnk&cd=3&gl=ec&lr=lang_es

puntos donde poder conectarnos, el operador que da el servicio, cómo acceder al mismo, e incluso sus tarifas. Igualmente se dispone de software específico que instalado en un PC portátil, permite localizar, detectar e incluso conectarse a la red Wi-Fi.

1.5.5. Modos de Autenticación

Antes de que una estación terminal pueda asociarse con un AP y conseguir acceso a la WLAN, debe llevar a cabo la autentificación. Dos tipos de autentificación de clientes están definidos en 802.11: sistema abierto y llave compartida.

1.5.6. Autentificación de Sistema Abierto

Es una forma muy básica de autentificación que consiste de una simple solicitud de autentificación que contiene la ID de la estación y una respuesta de autentificación que contiene el éxito o fracaso. En caso de éxito, se considera que ambas estaciones están mutuamente autentificadas.

1.5.7. Autentificación de Llave Compartida

Está basada en el hecho de que ambas estaciones tomando parte en el proceso de autentificación tiene la misma llave "compartida". Se asume que esta llave ha sido trasmitida a ambas estaciones a través de un canal seguro que no es WM. En implementaciones típicas, esto podría ser configurado manualmente en la estación cliente y en el AP. El primero y el cuarto frame de autentificación de llave compartida son similares a aquellos encontrados en sistemas de autentificación abierta. La diferencia es que en el segundo y el tercer frame, la estación de autentificación recibe un paquete de texto que es un reto (creado usando el Generador de Números Pseudo Aleatorios de WEP- Pseudo Random Number Generador PRNG) desde el AP, lo encripta usando la llave compartida, y luego lo manda de regreso al AP. Si después de la desencripción, el texto de reto es igual,

entonces la autentificación de un sentido es exitosa. Para obtener la autentificación mutua, el proceso se repite en la dirección opuesta. El hecho de que la mayor parte de los ataques hechos contra WLAN's 802.11b están basados en capturar la forma encriptada de una respuesta conocida hace de esta forma de autentificación una elección pobre.

Les da a los atacantes exactamente la información necesaria para derrotar la encriptación WEP y es por lo que la llave de autentificación compartida nunca es recomendada. Es mejor utilizar la autentificación abierta, la cual permitirá la autentificación sin la llave WEP correcta. Se mantendrá seguridad limitada porque la estación no estará preparada para enviar o recibir información de forma correcta con una llave WEP no válida.

1.6. Métodos para Implementar Seguridad de una Red Inalámbrica

Durante la investigación se determinó que el avance de la tecnología ha permitido conexiones de "alta velocidad" y ha facilitado a los usuarios la interconexión de sus equipos. Sin embargo la seguridad en este tipo de redes se ha descuidado considerablemente, aunque se ofrecen los mecanismos necesarios para protegerlas; este decremento de la seguridad es debido en gran parte al desconocimiento por parte de los usuarios que activan estas redes.

1.6.1. Aspectos Básicos de la Seguridad en una Wlan [12]

Es un hecho ya consumado la creciente demanda e implantación de todo tipo de redes wireless en entornos corporativos, PYMES, y en el ámbito familiar; este tipo de redes ofrecen un gran abanico de ventajas frente a las tradicionales redes cableadas. Facilidad de instalación, amplia cobertura, movilidad, sencilla ampliación, etc.… son algunas de ellas; es precisamente gracias a estas

[12] http://www.monografias.com/trabajos14/segur-wlan/segur-wlan.shtml

características que las redes inalámbricas deben el gran apogeo que viven en este momento.

Sin embargo estas ventajas conllevan una contrapartida en forma de problemas de seguridad que, si bien es cierto que se están dando a conocer, no son siempre tenidos en cuenta por los administradores de dichas redes. A estas alturas está claro y demostrado que las redes wireless son inseguras de forma intrínseca y que es necesaria una mayor dedicación a su seguridad que con las redes cableadas, esta situación además se ve agravada si las redes wireless están conectadas a Internet, por lo que cualquier infraestructura WI-FI debe considerar paliar estas deficiencias con la incorporación de soluciones específicas que garanticen a todos los niveles una seguridad óptima.

1.6.2. Filtrado de Direcciones MAC

La primera medida de seguridad implementada en las redes wireless fue, y sigue siendo, el filtrado de conexiones por dirección MAC ("Medium Access Control"). Para ello se crea una lista de direcciones MAC o listas de control de acceso (ACL, "Access Control List") en los puntos de acceso.[13]

Cada uno de estos puntos puede contar con una relación de las direcciones MAC de cada uno de los clientes que queremos que se conecten a nuestra red inalámbrica. Cada adaptador cuenta con una dirección que la identifica de forma inequívoca, y si el punto de acceso no la tiene dada de alta, simplemente no recibirá contestación por su parte.

Hay que tener en cuenta que éste no es el método más seguro para proteger la entrada a la red inalámbrica. Para empezar habrá que actualizar esta ACL cada

[13] http://www.adslayuda.com/foro/routers-adsl/conceptronic-c54apra-cadslr4/t56702-filtrado-mac.html

vez que se de de alta un nuevo adaptador inalámbrico, eliminando aquellos que se quieren dejar de utilizar.

1.6.3. WEP (Wired Equivalent Privacy)

El cifrado de la información es una de las técnicas más utilizadas, y para ello ya se lleva un tiempo empleando sistemas como WEP (Privacidad Equivalente a Cableado). Podríamos definir este sistema como la generación de una clave que se comparte entre el cliente y el punto de acceso, y que permite o deniega la comunicación entre ambos dispositivos. WEP utiliza un sistema con una clave de 64 ó 128 bits, que pueden ser hexadecimales o ASCII, mediante la que se autentifica el acceso y se encripta la información que se trasmite entre ambos dispositivos.

Aunque en teoría este sistema debería ser suficiente, lo cierto es que existen métodos para averiguar esta clave utilizando determinadas herramientas software, además del problema que se deriva de utilizar una misma clave para todos los usuarios.

1.6.4. Las VPN

Sin embargo, para conseguir que el nivel de confianza en las WLAN se equipare a las redes cableadas, algunos usuarios han optado por otra alternativa para reforzar la seguridad, implementando soluciones de seguridad de red convencionales adaptadas al entorno wireless.

En este modelo, es donde entran en juego el establecimiento de túneles IPSec (“Internet Protocol Security”). Este mecanismo, que asegura el tráfico de datos por una VPN (“Virtual Private Network”), utiliza algoritmos para la encriptación de datos, otros algoritmos para la autenticación de paquetes y certificados digitales para la validación de usuarios.

1.6.5. 802.1x

Cuando aumentan las necesidades en cuanto a niveles de seguridad y número de usuarios que es necesario administrar, además de la encriptación, es necesario añadir por otro mecanismo de seguridad como es la autenticación. La autenticación es el proceso por el cual se controla el acceso de los usuarios a la red. Para este propósito, el IEEE creó el grupo 802.1x con objeto de obtener un estándar de autenticación para redes (cableadas o no). RADUIS ("Remote Authenticated Dial-In User Service") es la infraestructura recomendada por la Wi-Fi Alliance como sistema de gestión centralizada que da una solución de autenticación para entornos con un elevado número de usuarios.[14]

Teniendo en cuenta que este tipo de entornos utilizará normalmente estructuras mixtas (cable tradicional y WLAN), la utilización de este protocolo permitirá mejorar la capacidad de autenticación del usuario inalámbrico, proporcionando un nivel de seguridad superior, escalable y una gestión centralizada.

A través de este sistema se podrá obtener un Certificado de Cliente Universal para permitir la autenticación mutua (autenticación del cliente al AP y del AP al cliente), gestión de clave protegida a través del soporte para RADIUS-EAP-TLS, así como la integración en entornos RADIUS existentes que soporten el protocolo MD-5 con sistemas de autenticación múltiples con protocolo EAP ("Extensible Authentication Protocol").

1.6.6. WPA (WI-FI Protected Access)

Este sistema creado para corregir las deficiencias del sistema previo WEP. Los investigadores han encontrado varias debilidades en el algoritmo (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques

[14] http://es.wikipedia.org/wiki/802.1x

estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).[15]

Wi-Fi Alliance ha certificado más de 175 productos con WPA desde septiembre de 2003. La organización ha empezado a requerir WPA para todos los productos certificados y ya no considera WEP como un mecanismo seguro.

1.7. Análisis DAFO de la Tecnología WI-FI

Llegados a este punto podemos realizar un pequeño análisis apoyado en la metodología DAFO que nos permita continuar posicionando a la tecnología Wi-Fi.

AMENAZAS	**OPORTUNIDADES**
Sector tecnológico en recesión/evolución.	La alta demanda del mercado.
Fuerte competencia en entorno urbano.	Acceso a subvenciones en entorno rural.
El entorno rural no genera claros beneficios.	Aplicaciones/servicios para entorno rural.
No aparece la “killer application” para datos.	Entrada en la Administración pública local.
Marco regulatorio indefinido.	Alianzas/Complemento a otras tecnologías.
UMTS/ operadores móviles.	Introducción a nuevos mercados/clientes.
Desorden en su desarrollo, despliegue	Desarrollo de aplicaciones.
Falta de profundidad en la ejecución de Soluciones	Desarrollo de calidad de servicio.

[15] http://es.wikipedia.org/wiki/Wi-Fi_Protected_Access

FORTALEZAS	**DEBILIDADES**
El acceso a Internet. La capacidad de banda ancha. Rápido despliegue de redes inalámbricas. No se requieren grandes inversiones. Evolución de estándares en el seno del IEEE. Soporte del sector informático.	Tecnología radio: interferencias y seguridad. Estándar IEEE 802.11 en evolución. Escasa penetración de ordenadores portátiles. Imagen de algo barato y sin calidad. No está definida la figura del operador. No está estandarizada/regulada la solución voz. En ocasiones, crecimiento incontrolado e ilegal. Seguridad.

Tabla 1. Análisis DAFO de La Tecnología Wi-Fi.

CAPITULO II

2. ANALISIS E INTERPRETACION DE RESULTADOS

Luego de la aplicación de la encuesta se organizaron los datos en cuadros y gráficos, los mismos que se explican a continuación:

2.1. Resultados de la Encuesta Dirigidos a los Estudiantes

1.- ¿Conoce Ud. Sobre Redes Inalámbricas?

Tabla No. 1

ITEM	F	%
SI	101	45%
NO	121	55%
TOTAL	222	100

Análisis e Interpretación

Como se muestra en el grafico, de todos los alumnos consultados hay un 45% que tiene algún conocimiento de lo que son las Redes Inalámbricas y un 55% que desconocen del tema.

Como podemos ver los resultados nos demuestra la falta de conocimiento de las bondades que brinda la tecnología inalámbrica y la necesidad de socializar el tema.

2.- ¿El Centro Asociado ofrece servicios informáticos?

Tabla No. 2

ITEM	F	%
SI	167	75%
NO	55	25%
TOTAL	222	100

Análisis e Interpretación

En lo que respecta a esta pregunta, un 75% de estudiantes manifiesta que SI se brinda servicios informáticos en el Centro Asociado y un 25% nos indica que NO.

Este resultado nos indica que falta una correcta información por parte de los encargados del Centro de Cómputo del Centro Asociado, en lo que ha servicios se refiere.

3.- ¿El Centro Asociado ha prestado servicios informáticos hasta el momento eficientes a la comunidad universitaria?

Tabla No. 3

ITEM	F	%
SI	77	35%
NO	145	65%
TOTAL	222	100

Análisis e Interpretación

De las respuestas obtenidas a esta pregunta se desprende que un 65% de los alumnos manifiesta que los servicios informáticos que actualmente brinda el Centro Asociado NO son eficientes, mientras tanto que un 35%, nos indica que son eficientes.

Se deduce que no hay un adecuado empleo de las bondades que existen en el Laboratorio Informático del Centro Asociado, o falta de conocimiento por parte de los alumnos.

4.- ¿Cuáles son los problemas más importantes que se han presentado al usar el Laboratorio Informático del Centro Asociado?

Tabla No. 4

ITEM	F	%
Aglomeración personas	46	21%
Falta de Computadores	111	50%
Daño en la Red	65	29%
TOTAL	222	100

Análisis e Interpretación

Como nos indica el gráfico uno de los problemas que se presenta con mayor incidencia al utilizar el laboratorio informático, es la falta de computadores que actualmente posee el Centro Asociado, seguido de daños en la red y la aglomeración de personas.

Según estos resultados se deduce que al momento no existe un laboratorio completamente equipado en lo que a computadoras, espacio y una adecuada instalación de red se refiere, por lo que es necesario la adquisición de nuevos y mejores equipos así como también, una correcta implantación de redes.

5.- ¿Dónde utiliza actualmente el servicio de Internet?

Tabla No. 5

ITEM	F	%
Centro Asociado	16	7%
Centros de Computo	185	83%
Hogar	21	10%
TOTAL	222	100

Análisis e Interpretación

De esta pregunta se desprende que la mayoría de alumnos en un 83%, utiliza los Centros de Cómputo que existe en la ciudad de La Maná, un 21% lo realiza desde sus hogares, mientras que solo un 16% utiliza el Laboratorio Informático del Centro Asociado, para acceder a los servicios que brinda el Internet.

Esto nos indica la urgente necesidad de implementar una red eficiente, la misma que ayudará a que los alumnos utilicen el Internet que brinda el Laboratorio Informático del Centro Asociado.

6.- ¿Con qué frecuencia usted utiliza el Centro de Cómputo del Centro Asociado?

Tabla No. 6

ITEM	F	%
Siempre	17	8%
Frecuentemente	68	31%
Raro	47	21%
Nunca	90	40%
TOTAL	222	100

Análisis e Interpretación

Con admiración vemos en el gráfico que un elevado 90% de la población estudiantil no utiliza el Laboratorio Informático existente en el Centro Asociado y solamente un 8% nos indica que siempre lo hace.

Haciendo un análisis de ésta pregunta, nos damos cuenta que la respuesta a la ausencia de alumnos en el Laboratorio Informático del Centro Asociado, corresponde a la deficiencia de equipos de cómputo, una adecuada distribución de los mismos, así como también la implementación de redes eficientes.

7.- ¿El servicio de Internet en el Centro Asociado para realizar sus actividades cotidianas es?

Tabla No. 7

ITEM	F	%
Muy Bueno	13	6%
Aceptable	121	54%
Malo	88	40%
TOTAL	222	100

Análisis e Interpretación

Vemos según el gráfico que solo un 13% de la población estudiantil opina que el servicio de Internet es Muy Bueno, no así un 40% piensa que es malo, y un 54% nos indica que es aceptable.

Esto refleja que la mayoría de la población que accede al Internet del Laboratorio del Centro Asociado se ha encontrado con un deficiente o regular servicio de Internet.

8.- ¿Considera usted que los servicios informáticos prestados actualmente en el Centro Asociado deben ser modernizados?

Tabla No. 8

ITEM	F	%
SI	210	95%
NO	12	5%
TOTAL	222	100

Análisis e Interpretación

De lo expresado en el gráfico un elevado 95% de la población estudiantil considera que los servicios que brinda el Laboratorio Informático del Centro Asociado deben ser modernizados mientras que un 5% opina que no.

De esto se desprende que con urgencia se necesita una modernización integral en el Laboratorio Informático del Centro Asociado.

9.- ¿Considera usted que sería beneficioso poder acceder a los servicios informáticos en todo momento y desde cualquier punto del campus universitario del Centro Asociado?

Tabla No. 9

ITEM	F	%
SI	205	92%
NO	17	8%
TOTAL	222	100

Análisis e Interpretación

Según los porcentajes expresados en el gráfico, una gran población representada por el 92% considera que seria beneficioso el acceso al Internet desde cualquier punto del Centro Asociado, mientras que un 8% opina que no.

Según este resultado consideramos que la necesidad del acceso al Internet y a los recursos informáticos desde cualquier punto del Centro Asociado seria adecuado y beneficioso para un normal desarrollo de la población estudiantil.

10.- ¿Considera usted que el uso de la tecnología informática y la implantación de una Red Inalámbrica en el Centro Asociado permitirá solucionar las dificultades de conexión y prestación de servicios?

Tabla No. 10

ITEM	F	%
SI	211	95%
NO	11	5%
TOTAL	222	100

Análisis e Interpretación

Según los porcentajes expresados en el gráfico, una pequeña cantidad de la población estudiantil representada en un 5%, considera que no es necesaria la implantación de una red inalámbrica, mientras que la gran mayoría representada en un 95% considera el beneficio de esta implantación en el Centro Asociado.

Se desprende que la implantación de una Red Inalámbrica en el Centro Asociado solventará las necesidades expresadas por los alumnos y que con urgencia se necesita en el Centro Asociado.

2.2 Resultados de la Encuesta Dirigidos a los Docentes

1.- ¿Conoce Ud. Sobre Redes Inalámbricas?

Tabla No. 1

ITEM	F	%
SI	19	46%
NO	22	54%
TOTAL	41	100

Análisis e Interpretación

Como se muestra en el gráfico, de todos los docentes consultados hay un 46% que tiene algún conocimiento de lo que son las Redes Inalámbricas y un 54% que desconocen del tema.

Como podemos ver los resultados nos demuestra la falta de conocimiento de las bondades que brinda la tecnología inalámbrica y la necesidad de socializar el tema.

2.- ¿El Centro Asociado ofrece servicios informáticos?

Tabla No. 2

ITEM	F	%
SI	17	41%
NO	24	59%
TOTAL	41	100

Análisis e Interpretación

En lo que respecta a esta pregunta, un 41% de los docentes manifiesta que SI se brinda servicios informáticos en el Centro Asociado y un 59% nos indica que NO.

Este resultado nos indica que falta una correcta información por parte de los encargados del Centro de Cómputo del Centro Asociado, en lo que ha servicios se refiere.

3.- ¿El Centro Asociado ha prestado servicios informáticos hasta el momento eficientes a la comunidad universitaria?

Tabla No. 3

ITEM	F	%
SI	15	37%
NO	26	63%
TOTAL	41	100

Análisis e Interpretación

De las respuestas obtenidas a esta pregunta se desprende que un 63% de los docentes manifiesta que los servicios informáticos que actualmente brinda el Centro Asociado NO son eficientes, mientras tanto que un 37%, nos indica que son eficientes.

Se deduce que no hay un adecuado empleo de las bondades que existen en el Laboratorio Informático del Centro Asociado, o falta de conocimiento por parte de los docentes.

4.- ¿Cuáles son los problemas más importantes que se han presentado al usar el Laboratorio Informático del Centro Asociado?

Tabla No. 4

ITEM	F	%
Aglomeración de personas	9	22%
Falta de computadores	24	59%
Daño en la red	8	19%
TOTAL	41	100%

Análisis e Interpretación

Como nos indica el gráfico uno de los problemas que se presenta con mayor incidencia al utilizar el laboratorio informático, es la falta de computadores que actualmente posee el Centro Asociado, seguido por la aglomeración de personas y daños en la red.

Según estos resultados se deduce que al momento no existe un laboratorio completamente equipado en lo que a computadoras, espacio y una adecuada instalación de red se refiere, por lo que es necesario la adquisición de nuevos y mejores equipos así como también, una correcta implantación de redes.

5.- ¿Dónde utiliza actualmente el servicio de Internet?

Tabla No. 5

ITEM	F	%
Centro Asociado	4	10%
Centros de Computo	30	73%
Hogar	7	17%
TOTAL	41	100%

Análisis e Interpretación

De esta pregunta se desprende que la mayoría de docentes en un 73%, utiliza los Centros de Cómputo que existe en la ciudad de La Maná, un171% lo realiza desde sus hogares, mientras que solo un 11 utiliza el Laboratorio Informático del Centro Asociado, para acceder a los servicios que brinda el Internet.

Esto nos indica la urgente necesidad de implementar una red eficiente, la misma que ayudará a que los docentes utilicen el Internet que brinda el Laboratorio Informático del Centro Asociado.

6.- ¿Con qué frecuencia usted utiliza el Centro de Cómputo del Centro Asociado?

Tabla No. 6

ITEM	F	%
Siempre	0	0%
Frecuentemente	9	22%
Rara vez	21	51%
nunca	11	27%
TOTAL	41	100%

Análisis e Interpretación

Con admiración vemos en el gráfico que un 27% de la población de docentes no utiliza el Laboratorio Informático existente en el Centro Asociado y un 51% nos indica que rara vez lo hace.

Haciendo un análisis de ésta pregunta, nos damos cuenta que la respuesta a la ausencia de docentes en el Laboratorio Informático del Centro Asociado, corresponde a la deficiencia de equipos de cómputo, una adecuada distribución de los mismos, así como también la implementación de redes eficientes.

7.- ¿El servicio de Internet en el Centro Asociado para realizar sus actividades cotidianas es?

Tabla No. 7

ITEM	F	%
Muy Bueno	3	7%
Aceptable	26	64%
Malo	12	29%
TOTAL	41	100%

Análisis e Interpretación

Vemos según el gráfico que solo un 7% de la población de docentes opina que el servicio de Internet es Muy Bueno, no así un 29% piensa que es malo, y un 64% nos indica que es aceptable.

Esto refleja que la mayoría de la población de docentes que accede al Internet del Laboratorio del Centro Asociado se ha encontrado con un deficiente o regular servicio de Internet.

8.- ¿Considera usted que los servicios informáticos prestados actualmente en el Centro Asociado deben ser modernizados?

Tabla No. 8

ITEM	F	%
SI	35	85%
NO	6	15%
TOTAL	41	100%

Análisis e Interpretación

De lo expresado en el gráfico un elevado 85% de la población de docentes considera que los servicios que brinda el Laboratorio Informático del Centro Asociado deben ser modernizados mientras que un 15% opina que no.

De esto se desprende que con urgencia se necesita una modernización integral en el Laboratorio Informático del Centro Asociado.

9.- ¿Considera usted que sería beneficioso poder acceder a los servicios informáticos en todo momento y desde cualquier punto del campus universitario del Centro Asociado?

Tabla No. 9

ITEM	F	%
SI	33	80%
NO	8	20%
TOTAL	41	100

Análisis e Interpretación

Según los porcentajes expresados en el gráfico, una gran población representada por el 80% considera que seria beneficioso el acceso al internet desde cualquier punto del Centro Asociado, mientras que un 20% de los docentes opina que no.

Según este resultado consideramos que la necesidad del acceso al Internet y a los recursos informáticos desde cualquier punto del Centro Asociado seria adecuado y beneficioso para un normal desenvolvimiento de los docentes.

10.- ¿Considera usted que el uso de la tecnología informática y la implantación de una Red Inalámbrica en el Centro Asociado permitirá solucionar las dificultades de conexión y prestación de servicios?

Tabla No. 10

ITEM	F	%
SI	32	78%
NO	9	22%
TOTAL	41	100

Análisis e Interpretación

Según los porcentajes expresados en el gráfico, un grupo de docentes representado en un 22%, considera que no es necesaria la implantación de una red inalámbrica, mientras que la gran mayoría representada en un 78% considera el beneficio de esta implantación en el Centro Asociado.

Se desprende que la implantación de una Red Inalámbrica en el Centro Asociado solventará las necesidades expresadas por los docentes.

2.3. Resultados de la Encuesta Dirigidos al Personal Administrativo

1.- ¿Conoce Ud. Sobre Redes Inalámbricas?

Tabla No. 1

ITEM	F	%
SI	1	20%
NO	4	80%
TOTAL	5	100

Análisis e Interpretación

Como se muestra en el grafico, de todo el personal administrativo consultados hay un 20% que tiene algún conocimiento de lo que son las Redes Inalámbricas y un 80% que desconocen del tema.

Como podemos ver los resultados nos demuestra la falta de conocimiento de las bondades que brinda la tecnología inalámbrica y la necesidad de socializar el tema.

2.- ¿El Centro Asociado ofrece servicios informáticos?

Tabla No. 2

ITEM	F	%
SI	1	20%
NO	4	80%
TOTAL	5	100

Análisis e Interpretación

En lo que respecta a esta pregunta, un 20% del personal administrativo manifiesta que SI se brinda servicios informáticos en el Centro Asociado y un 80% nos indica que NO.

Este resultado nos indica que falta una correcta información por parte de los encargados del Centro de Cómputo del Centro Asociado, en lo que ha servicios se refiere.

3.- ¿El Centro Asociado ha prestado servicios informáticos hasta el momento eficientes a la comunidad universitaria?

Tabla No. 3

ITEM	F	%
SI	3	60%
NO	2	40%
TOTAL	5	100

Análisis e Interpretación

De las respuestas obtenidas a esta pregunta se desprende que un 40% del personal administrativo manifiesta que los servicios informáticos que actualmente brinda el Centro Asociado NO son eficientes, mientras tanto que un 60%, nos indica que son eficientes.

Se deduce que no hay un adecuado empleo de las bondades que existen en el Laboratorio Informático del Centro Asociado, o falta de conocimiento por parte de los docentes.

4.- ¿Cuáles son los problemas más importantes que se han presentado al usar el Laboratorio Informático del Centro Asociado?

Tabla No. 4

ITEM	F	%
Aglomeración de personas	0	0%
Falta de computadores	4	80%
Daño en la red	1	20%
TOTAL	5	100%

Análisis e Interpretación

Como nos indica el gráfico uno de los problemas que se presenta con mayor incidencia al utilizar el laboratorio informático, es la falta de computadores que actualmente posee el Centro Asociado, seguido por daños en la red.

Según estos resultados se deduce que al momento no existe un laboratorio completamente equipado en lo que a computadoras, espacio y una adecuada instalación de red se refiere, por lo que es necesario la adquisición de nuevos y mejores equipos así como también, una correcta implantación de redes.

5.- ¿Dónde utiliza actualmente el servicio de Internet?

Tabla No. 5

ITEM	F	%
Centro Asociado	2	40%
Centros de Computo	2	40%
Hogar	1	20%
TOTAL	5	100%

Análisis e Interpretación

De esta pregunta se desprende que el personal administrativo utiliza el internet en un 40% en el Laboratorio Informático del Centro Asociado, un 40% en los Centros de de Cómputo que existe en la ciudad de La Maná y un 20% lo realiza desde sus hogares

Esto nos indica la urgente necesidad de implementar una red eficiente, la misma que ayudará a que todo el personal administrativo utilice el Internet que brinda el Laboratorio Informático del Centro Asociado.

6.- ¿Con qué frecuencia usted utiliza el Centro de Cómputo del Centro Asociado?

Tabla No. 6

ITEM	F	%
Siempre	2	40%
Frecuentemente	0	0%
Rara vez	1	20%
nunca	2	40%
TOTAL	5	100%

Análisis e Interpretación

Con admiración vemos en el gráfico que un 27% de la población de personal administrativo no utiliza el Laboratorio Informático existente en el Centro Asociado y un 51% nos indica que rara vez lo hace.

Haciendo un análisis de ésta pregunta, nos damos cuenta que la respuesta a la ausencia de personal administrativos en el Laboratorio Informático del Centro Asociado, corresponde a la deficiencia de equipos de cómputo, una adecuada distribución de los mismos, así como también la implementación de redes eficientes.

7.- ¿El servicio de Internet en el Centro Asociado para realizar sus actividades cotidianas es?

Tabla No. 7

ITEM	F	%
Muy Bueno	0	0%
Aceptable	3	60%
Malo	2	40%
TOTAL	5	100%

Análisis e Interpretación

Vemos según el gráfico que un 0% de la población de personal administrativo opina que el servicio de Internet es Muy Bueno, un 40% piensa que es malo, y un 60% nos indica que es aceptable.

Esto refleja que la mayoría de la población de personal administrativo que accede al Internet del Laboratorio del Centro Asociado se ha encontrado con un deficiente o regular servicio de Internet.

8.- ¿Considera usted que los servicios informáticos prestados actualmente en el Centro Asociado deben ser modernizados?

Tabla No. 8

ITEM	F	%
SI	4	80%
NO	1	20%
TOTAL	5	100%

Análisis e Interpretación

De lo expresado en el gráfico un elevado 80% de la población de personal administrativo, considera que los servicios que brinda el Laboratorio Informático del Centro Asociado deben ser modernizados mientras que un 20% opina que no.

De esto se desprende que con urgencia se necesita una modernización integral en el Laboratorio Informático del Centro Asociado.

9.- ¿Considera usted que sería beneficioso poder acceder a los servicios informáticos en todo momento y desde cualquier punto del campus universitario del Centro Asociado?

Tabla No. 9

ITEM	F	%
SI	4	80%
NO	1	20%
TOTAL	5	100

Análisis e Interpretación

Según los porcentajes expresados en el gráfico, una gran población representada por el 80% considera que seria beneficioso el acceso al internet desde cualquier punto del Centro Asociado, mientras que un 20% del personal administrativo opina que no.

Según este resultado consideramos que la necesidad del acceso al Internet y a los recursos informáticos desde cualquier punto del Centro Asociado seria adecuado y beneficioso para un normal desenvolvimiento de los docentes.

10.- ¿Considera usted que el uso de la tecnología informática y la implantación de una Red Inalámbrica en el Centro Asociado permitirá solucionar las dificultades de conexión y prestación de servicios?

Tabla No. 10

ITEM	F	%
SI	4	80%
NO	1	20%
TOTAL	5	100

Análisis e Interpretación

Según los porcentajes expresados en el gráfico, un grupo de administrativos representado en un 20%, considera que no es necesaria la implantación de una red inalámbrica, mientras que la gran mayoría representada en un 80% considera el beneficio de esta implantación en el Centro Asociado.

Se desprende que la implantación de una Red Inalámbrica en el Centro Asociado solventará las necesidades expresadas por los administrativos.

2.4. Verificación de la Hipótesis

La hipótesis planteada inicialmente en la investigación es: "La implantación de un sistema de red inalámbrica en el centro asociado del cantón La Maná de la Universidad Técnica de Cotopaxi, permitirá la interconexión de los equipos computacionales inalámbricos con los equipos de la red cableada."

Luego de haber realizado las encuestas al personal docente, dicente y administrativo del centro asociado del cantón La Maná de la Universidad Técnica de Cotopaxi, podemos verificar tanto en la pregunta 9 y 10 (pág 56, 57), que según su interpretación tenemos un alto porcentaje que esta de acuerdo con la creación de una red inalámbrica ya que con ella los docentes, dicentes y administrativos, podrán acceder a las bondades que brinda la red inalámbrica sean estos Internet, compartir recursos, etc., desde cualquier punto del campus universitario

Con esta información determinamos que la hipótesis ha sido verificada.

2.5. Tecnología Wireless

El reciente desarrollo de las tecnologías de Wireless, Wimax, Wifi, Mobile-fi,Wlan, UMTS y cdma2000 que son específicas de las normas de la HZEL como son 802.16, denominada como Wimax la misma que realiza transmisiones a distancias entre 40 y 70kms con una tasa de transferencia de información de 124Mbit/s cabe destacar que esta tecnología según las normas y leyes de los países se necesita o no licencia para su uso. La norma 802.1 la/b/c perteneciente a Wifi la tecnología que actualmente tiene una tasa de transferencia entre 11 Mbit/s y 54 Mbit/s y su alcance es de 300m, esta tecnología no necesita licencia para su uso ya que trabaja en un espectro que es de uso general. La norma 802.20 denominada Mobile-Fi utilizado para transmisiones en un rango hasta de 20 km con una tasa de transferencia de 16Mbit/s esta tecnología necesita de licencia para

su funcionamiento. La norma del UMTS y cdma2000 que tiene una tasa de transferencia de 2Mbit/s y un rango de 10 kilómetros, esta tecnología también necesita permisos o licencias para su uso y/o funcionamiento.

2.5.1. Los Estándares Wlans: IEEE 802.11(A), 802.11(B), Y 802.11(G)

El Instituto de Ingenieros Eléctricos Electrónicos (IEEE) ratificó el estándar 802.11 en el año 1997 permitiendo velocidades de transmisión de 2Mbps. En 1999, el IEEE aprobó ambos estándares: el 802.11a y el 802.1b. Las letras después del número "802.11" indican el orden en que los estándares fueron propuestos y no el orden en que los productos estuvieron disponibles en el Mercado. El estándar 802.11a especifica radios que operan en la banda de frecuencia de 5 GHz a velocidades de hasta 54 Mbps. [16]

El estándar 802.1b especifica operación en la banda de 2.4 GHz permitiendo alcanzar velocidades de hasta 11 Mbps en tres canales sin sobreposición. Las implementaciones comerciales resultaron que los equipos que venían operando en la banda de 2.4 GHz fueran de más fácil implementación, y por lo tanto los productos 802.1b aparecieron primero en el mercado a fines del año 1999.

2.5.2. Topología de la Red Wireless

La interconexión de nodos en una red compuesta de más de cinco nodos puede realizarse de muchas maneras. En cuanto el número de nodos aumente también va aumentando las posibles maneras de interconectar la red. Sin embargo una estructura aleatoria no es la más indicada por muchos motivos.

Normalmente cuando se diseña una red se estudia de antemano su tráfico, el número de máquinas conectadas, las necesidades de los usuarios y varias cosas más para organizar la estructura para dar el mejor servicio posible. Las redes

[16] http://www.radioptica.com/Radio/estandares_WLAN.asp

wireless al crecer de una manera no controlada requerirán un diseño o ajuste posterior para que se estructura mantenga cierta orden.

2.5.3. Tipos de Topologías Wireless

Será importante durante las primeras fases de crecimiento de la red discutir la adición de nuevos nodos y el mejor punto de conexión como decidir en una herramientas de monitorización de varios aspectos de la red que se podría utilizar para comparar el comportamiento de sus diferentes partes.[17]

La versatilidad y flexibilidad de las redes inalámbricas es el motivo por el cual la complejidad de una LAN implementada con esta tecnología sea tremendamente variable. Esta gran variedad de configuraciones ayuda a que este tipo de redes se adapte a casi cualquier necesidad.

Estas configuraciones se pueden dividir en dos grandes grupos, las redes peer to peer y las que utilizan Puntos de Acceso.

2.5.3.1. Peer To Peer

También conocidas como redes ad-hoc, es la configuración más sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas. En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

[17] dis.um.es/~lopezquesada/documentos/IES_0506/RAL_0506/doc/prac2ut1.doc

Figura 4. Topología Peer to Peer

2.5.3.2. Punto de Acceso

Estas configuraciones utilizan el concepto de celda, ya utilizado en otras comunicaciones inalámbricas, como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva. A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión es posible combinar las celdas de estas señales para cubrir de forma casi total un área más extensa. La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados Puntos de acceso, que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso.

Los Puntos de acceso son colocados normalmente en alto, pero solo es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos de metros.

La técnica de Punto de acceso es capaz de dotar a una red inalámbrica de muchas más posibilidades. Además del evidente aumento del alcance de la red, ya que la utilización de varios puntos de acceso, y por lo tanto del empleo de varias celdas que colapsen el lugar donde se encuentre la red, permite lo que se conoce como roaming es decir que los terminales puedan moverse sin perder la cobertura y sin sufrir cortes en la comunicación. Esto representa una de las características más interesantes de las redes inalámbricas.

Figura 5. Topología Punto de Acceso

2.5.4. Análisis del Hardware Wireless

Las LAN Wi-Fi proporcionara a las empresas mejoras generales en la productividad, basadas en la movilidad del usuario y las ventajas resultantes en la eficiencia organizacional e individual. Sin embargo, todo esto depende de la selección de los componentes adecuados que soportarán las aplicaciones deseadas y necesarias movilidad, rangos, seguridad y otras características de red.

2.5.7. Antenas

Las antenas son dispositivos utilizados para recoger o radiar ondas electromagnéticas. Aumentan la zona de influencia/cobertura de nuestras tarjetas inalámbricas, de manera que en lugar de dar cobertura a unos pocos metros, podemos alcanzar cientos de metros sin problemas.

2.5.7.1. Tipos de Antenas

Disponemos de tres tipos de antenas para redes inalámbricas:

2.5.7.1.1. Antenas Direccionales (o Directivas)

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un toco que emite un haz de luz concreto y estrecho pero de forma intensa (más alcance).

Las antenas direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

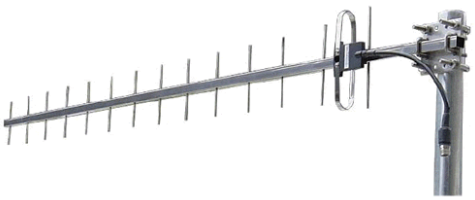


Figura 6. Antena Yagi 13dbi

2.5.7.1.2. Antenas Omnidireccionales

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional seria como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco es decir con menor alcance.

Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales. El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

Figura 7. Antena Omnidireccional

2.5.7.1.3. Antenas Sectoriales

Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con un haz de luz más ancho de lo normal.

Para tener una cobertura de 560° (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120° ó 4 antenas sectoriales de 80°. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

Figura 8. Antenas Sectoriales

2.5.8. ACCESS POINT (Punto de Acceso)

Es el dispositivo que hace de puente entre la red cableada y la inalámbrica.

Punto de acceso es un dispositivo que podemos añadir a una red existente para dotarla de conectividad inalámbrica.

Si ya disponemos de un router podemos simplemente conectar el punto de acceso a una de sus salidas para así conectar cualquier dispositivo inalámbrico con el resto de la red.

Figura 9. Access Point

2.5.9. Tarjetas PCMCIA para Portátiles

Tarjetas de red, o TR, que serán los que tengamos integrados en nuestro ordenador, o bien conectados mediante un conector PCMCÍA ó USB si estamos en un portátil o en un slot PCI si estamos en un ordenador de sobremesa.

Sustituyen a las tarjetas de red Ethernet o Token Ring a las que estábamos acostumbrados. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos trabajando. La velocidad de transmisión / recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.

Figura 10. Tarjeta PCMCIA

2.5.10. Requerimientos Técnicos

Para la elaboración del proyecto se necesitará:

2.5.11. Servidor de Cuarto de control

Pentium IV, CPU 3.00 Ghz., HD 160, 512 Mb. RAM, CD-RW.

2.5.12. Sistema Operativo del Servidor

Linux CentOS 4.5

2.5.13. Materiales para la Red Inalámbrica:

- Un Switch

- Dos Access Point
- Canaletas de pared
- Dos antena omnidireccionales
- Cable UTP Cat. 5

CAPITULO III

3. PROPUESTA: "IMPLANTACIÓN DE UN SISTEMA DE RED INALAMBRICA EN EL CENTRO ASOCIADO DEL CANTÓN LA MANÁ DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI".

3.1. Presentación

Dado el continuo desarrollo de la Universidad en el cantón La Maná se hace muy difícil, acceder a nuevos y mejores servicios o a una eventual reubicación de las oficinas y unidades de trabajo, o aspectos que se van creando de acuerdo a los requerimientos de la misma; ya que técnica y económicamente no es factible reutilizar el material para una nueva redistribución de puntos de acceso a la red LAN.

Al existir una gran cantidad de alumnos, es muy difícil que cada uno de ellos acceda a los equipos y servicios que brinda la red existente y es por eso que la opción mediata sería la instalación de una red inalámbrica, ya que también desde el punto de vista económico, los equipos informáticos inalámbricos son cada vez más accesibles para el común de las personas.

Se puede manifestar también que no existe limitación alguna para la instalación o implantación de una red inalámbrica, ya que actualmente ni el espesor, ni el material con el cual están fabricados los edificios no es una preocupación ya que esta tecnología trabaja utilizando como medio de transporte las ondas electromagnéticas para enlazar mediante un adaptador los diferentes componentes de la red.

3.2. Objetivo General

- Implantar un sistema de Red Inalámbrica en el Centro Asociado del Cantón La Maná de la Universidad Técnica de Cotopaxi, para la interconexión de los equipos computacionales inalámbricos con los equipos de la red cableada.

3.3. Objetivos Específicos

- Recopilar toda la información de campo necesaria para conocer el estado actual del tema planteado, y de esta manera buscar la solución más adecuada.

- Analizar los fundamentos teóricos de las fuentes consultadas para fundamentar la investigación relacionada con el sistema de redes inalámbricas.

- Realizar la implantación de un sistema de redes inalámbricas para el Centro Asociado del cantón La Maná de la Universidad Técnica de Cotopaxi, para la interconexión de los equipos computacionales inalámbricos con los equipos de la red cableada utilizando las normas establecidas por la IEEE.

3.4. Justificación

En la Universidad Técnica de Cotopaxi como en otras instituciones de la localidad se han desarrollado tanto en lo teórico como en lo práctico al instalar tecnología inalámbrica de punta en el edificio nuevo de la matriz, demostrando que su aplicación ha logrado descongestionar el acceso a los servicios informáticos y a su vez brindar un servicio de calidad a una mayor cantidad de usuarios.

Para la realización de este tema, se dispone de material bibliográfico tal como Normas IEEE, 802.11, ondas de radio, disponible en las distintas bibliotecas que dispone nuestra provincia así como también se puede acceder en librerías de renombre; además de trabajos prácticos publicados en el Internet que nos brindan el soporte suficiente para el desarrollo del proyecto.

Contamos con el aval de las autoridades de la Universidad, así como del Centro Asociado La Maná.

La universidad cuenta con docentes capacitados para desarrollo de proyectos de investigación científica los que facilitaría una secuencia metodológica, además existe la predisposición por parte del grupo investigador.

Con estos antecedentes es posible la realización de este trabajo práctico en el Centro Asociado La Maná, ya que serán beneficiados tanto el nivel administrativo, docente y dicente por cuanto los servicios informáticos estarán a la disposición dentro del área especificada.

3.5. Desarrollo de la Propuesta

La tecnología Inalámbrica (WIRELESS) ha sido descrita por los analistas como uno de los sectores de más alto crecimiento en la industria de la computación. WLAN provee acceso a los recursos de la red sin la complicación de los cables, ofreciendo flexibilidad, conveniencia y productividad.

Este proyecto que nace con la finalidad de crear redes de transmisión de datos inalámbricas (sin cables) que den cobertura a todo el área de Campus Universitario.

Se podrá acceder a la red cualquier persona que se encuentre en el radio de cobertura y previamente se haya autentificado, además que disponga de un

ordenador equipado con tecnología wireless.

3.5.1. Selección de los Componentes de la Red

3.5.1.1. Selección de la Tecnología de la Red

Una vez realizado el análisis de las diversas tecnologías Wireless se llego a la conclusión que en el campus universitario se necesita una WLAN de alto desempeño.

3.5.1.2. Selección de la Topología de Red

Ya que el campus universitario conforman tanto estudiantes como personal docente y administrativo se traslada de un lugar a otro se ve la necesidad de disponer conexión constante y esto se alcanza por medio de la topología AP o basada en Puntos de Acceso que es similar a la de la tecnología celular esto nos permite extender la red inalámbrica al disponer de diversos puntos de acceso y también aumentar el número de usuarios que pueden acceder a la red. Cabe destacar que esta topología nos permite desplazarnos con libertad con nuestros equipos sin tener que cambiar de 1P, lo que se conoce como ROAMING.

3.5.1.3. Selección de la Antena a Instalar

Las direccionales se suelen utilizar para unir dos puntos a largas distancias mientras que las omnidireccionales se utilizan para dar señal extensa en los alrededores. Las sectoriales se suelen utilizar cuando se necesita un balance de las dos cosas, es decir, llegar a largas distancias y a la vez, a un área extensa.

Si necesita dar cobertura de red inalámbrica en toda un área próxima (una planta de un edificio o un parque por ejemplo) lo más probable es que utilice una antena omnidireccional. Si tiene que dar cobertura de red inalámbrica en un punto muy

concreto (por ejemplo un PC que está bastante lejos) utilizará una antena direccional finalmente, si se necesita dar cobertura amplia y a la vez a larga distancia, utilizará antenas sectoriales.

Luego de realizar el análisis de los diferentes tipos de antenas existentes para la cobertura de redes Wireless; dado que debe ser cubierto un área próxima hemos decidido que la antena D-Link ANT24-0700 de tipo omnidireccional es la que nos presta mayores beneficios y para mejor aprovechamiento de sus beneficios utilizaremos dos de este tipo.

3.5.1.4. Selección del Punto de Acceso

Después de estudiar las diversas alternativas de cada una de las empresas tomadas en cuenta para nuestro estudio se llego a la conclusión que los equipos D-LINK DWL-2100 y DWL-3200 que satisfacen las necesidades del campus universitario, para realizar esta selección tomamos en cuenta la administración remota por FTP, Telnet, http, además de un sinnúmero de alternativas de seguridad además es el que mas gama de accesorios posee.

El AP DWL-2100 se utilizará para afianzar el trabajo que realizará el AP DWL-3200, en su área de cobertura y acceso de los usuarios.

3.5.1.5. Diseño de la Red Wireless de Campus

En el esquema actual de la red wireless se muestra los puntos de conexión al switch ubicados en el campus universitario, este a su vez posee un puerto para los access point de la red wireless.

Figura 11. Ubicación del Cuarto de Control y AP

Figura 12. Ubicación AP en el segundo piso

3.5.1.6. Direcciones IP

Cada grupo Proxy necesita de un rango de direcciones IP para posibilitar la conexión de los nodos con los equipos de los clientes, la conexión de los nodos entre sí y finalmente para posibilitar la conexión con otros entes externos e Internet.

Es importante establecer la asignación de direcciones tanto para el servidor de la red Proxy como para cada una de sus dependencias.

Es necesario asegurar que las direcciones IP no coinciden entre equipos porque así se haría imposible la interconexión.

Para esto se utilizará un servidor proxy que se encargará de asignar direcciones a cada computador en forma automática, como veremos más adelante.

3.5.2. Implementar la Seguridad de la Red Inalámbrica

La seguridad en las redes inalámbricas es sumamente importante, por la facilidad con que cualquiera puede encontrarlas y acceder a ellas.

Cualquier persona con una computadora portátil puede encontrar fácilmente el punto de acceso inalámbrico de la red inalámbrica, pudiendo así ingresar ha archivos, utilizar la conexión a proxy, obtener datos importantes que se transfieran en la red inalámbrica, etc.

Para el presente proyecto utilizaremos El Servidor RADIUS que es un protocolo de autentificación comúnmente utilizado por el estándar de seguridad del 802.1x (usado en redes inalámbricas). De todas maneras, este no fue creado inicialmente para ser un método de seguridad en redes inalámbricas. Sin embargo mejora el estándar de encriptación WEP, en conjunto con otros métodos de seguridad como EAP-PEAP.

Al hablar de Radius resulta conveniente conocer el marco AAA, que implica una serie de conceptos básicos de los que se encarga el protocolo. AAA son las siglas de Authentication, Authorization y Accounting.

Autenticación, es el proceso de verificar si la identidad de una persona o una máquina es efectivamente la que declara. Busca establecer una relación de confianza entre los interlocutores. Cuando hablamos de autenticar usuarios el primer ejemplo que se nos viene a la cabeza es el del nombre de usuario y la contraseña, aunque no todo es tan simple. Infraestructuras tan completas como los certificados digitales son soluciones más actuales y complejas al problema de la autenticación.

Autorización, involucra la utilización de reglas y plantillas para decidir si un usuario previamente autenticado goza de privilegios suficientes para acceder o no a un recurso. Por ejemplo, los permisos en un sistema de ficheros que determinan si un usuario puede leer, escribir o incluso ejecutar un archivo.

Cuentas, entorno a la arquitectura AAA se encuentran las cuentas de usuario, que miden y documentan los recursos que un usuario utiliza durante su acceso.

3.5.2.1. Seguridad de Usuarios

Con frecuencia la parte más complicada de una política de seguridad es concienciar a los usuarios de la necesidad de medidas básicas de prevención contra ataques. Demasiados usuarios opinan que las historias de crackers que atacan PCs sólo suceden en las películas o en organizaciones militares de alta seguridad; nada más lejos de la realidad; en cualquier universidad ocurren a diario incidentes de seguridad, de los que solo una pequeña parte se detecta (y muchos menos se solucionan). Es muy recomendable para el administrador de la red imprimir una hoja con las medidas de seguridad básicas o la política del sistema, y entregar una copia a cada usuario al crear su cuenta.

3.5.2.2. Características de Radius

Las principales características del radius son:

3.5.2.2.1 Modelo Cliente/Servidor

Un servidor de acceso a la red (Network Access Server (NAS)) opera como un cliente de RADIUS. El cliente es el responsable de pasar la información del usuario al servidor RADIUS designado, y luego actuar en la respuesta que el retornara.

El servidor RADIUS es responsable de recibir el requerimiento de conexión del usuario, autentificar al usuario, y retornar toda la información de configuración necesario para el cliente entregue el servicio al usuario.

Un servidor RADIUS puede actuar como cliente proxy a otros servidores RADIUS, u otro tipo de servidores de autentificación.

3.5.2.2.2. Seguridad

Las transacciones entre cliente y servidor RADIUS deben estar autentificadas a través del uso de un secreto compartido, este nunca debe ser mandado sobre la red. En resumen, cualquier password de usuario debe ser mandada encriptado entre el cliente y el servidor RADIUS, para eliminar la posibilidad de que alguien capture una password de usuario de una red insegura.

3.5.2.2.3. Métodos de Autentificación Flexible

El servidor RADIUS debe ser capaz de soportar una variedad de métodos de autentificación. Cuando se utiliza el modelo de nombre de usuario y la password, puede soportar PPP PAP o CHAP, login tipo UNIX, y otros métodos de autentificación.

3.5.2.3. Funcionamiento de Radius

En esta parte se comenta todo el procedimiento AAA del servidor RADIUS, partiremos desde el punto en que el usuario ingresa sus datos de usuario y password.

Estos datos de usuario son recibidos por el cliente, este es el encargado de crear un paquete llamado “Access-Request” que contiene los atributos de nombre de

usuario, password, el ID del cliente y el ID de la puerta por la cual el usuario esta accesando. Aquí se protegen los datos, como la password vía un algoritmo MD5, basado en RSA.

Esta solicitud es mandada al servidor RADIUS vía red. Si no hay respuesta se reintenta, hay marcas de tiempo en los paquetes mandados. El cliente también tiene la posibilidad de probar con servidores alternativos, pero después de un determinado número de intentos al servidor principal, también se puede aplicar un modelo round-robin en casos de muchas consultas simultáneas.

Cuando un servidor RADIUS recibe una solicitud este el cliente. Una solicitud de un cliente que no tenga un secreto compartido será descartada silenciosamente. Si el cliente valido, el servidor RADIUS consulta su base de datos de usuarios para encontrar que nombre de usuario coincide con la solicitud. Esto siempre incluye verificar la password, pero puede también especificar el cliente o el puerto por el cual le esta permitido tener acceso.

Si cualquier atributo presente no concuerda, el servidor RADIUS manda un "Access- Reject" indicando que el usuario es no valido.

Si se verifican los datos entregados, el servidor RADIUS crea un "Access-Accept", aquí se adjuntan una serie de parámetros, como el tipo de servicio que se debe entregar y todos los valores necesarios para dar el servicio solicitado.

Todas esta solicitudes y respuestas trabajan sobre UDP, el cual le brinda la posibilidad de ser más rápido a la hora de atender una solicitud, además no tiene los timeout del TCP, pero fuerza a tener retransmisiones artificiales cuando un paquete se pierde.

3.5.2.4. Freeradius

Freeradius proyecto iniciado en 1999 por Alan DeKok y Miquel van Smoorenburg (quien colaboró anteriormente en el desarrollo de Cistron RADIUS), es una alternativa libre hacia otros servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que le componen. Puede operar tanto en sistemas con recursos limitados así como sistemas atendiendo millones de usuarios.

Freeradius inició como un proyecto de servidor RADIUS que permitiera una mayor colaboración de la comunidad y que pudiera cubrir las necesidades que otros servidores RADIUS no podían. Actualmente incluye soporte para LDAP, SQL y otras bases de datos, así como EAP, EAP-TTLS y PEAP. Actualmente incluye soporte para todos los protocolos comunes de autenticación y bases de datos.

3.5.2.5. Configuración del Estándar 802.1x

3.5.2.5.1. Equipos que Intervienen

Para este proyecto se utilizan:

- Un computador Pentium IV
- Un Access Point 3200
- Un Access Point 2100
- Un switch 3COM de 24 puertos
- Cable UTP Cat. 5e
- Dos antenas omnidireccionales D-Link ANT24-0700
- 30 mts. Manguera flexible
- 10 mts canaleta de pared

3.5.2.5.2. Instalación del Sistema Operativo Linux CentOS V4.5

Inserte el disco de instalación de CentOS y en cuanto aparezca el diálogo de inicio (boot), pulse la tecla **ENTER** o bien ingrese las opciones de instalación deseadas.

Figura 13. Pantalla Inicial de Linux CentOS

a. Si desea verificar la integridad del disco a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla ENTER, considere que esto puede demorar varios minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione **«Skip»** y pulse la tecla ENTER..

b. Haga clic sobre el botón **«Next»** en cuanto aparezca la pantalla de bienvenida de CentOS.

c. Seleccione **«Spanish»** como idioma para ser utilizado durante la instalación.

d. Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«Spanish»** corresponde a la disposición del teclado Español España. Al terminar, haga clic sobre el botón **«Siguiente»**.

e. Haga clic sobre el botón **«Siguiente»** y espere a que el sistema intente detectar instalaciones previas de CentOS.

f. Seleccione el tipo de instalación **«Personalizada»** para realizar esta con un mayor control de las opciones disponibles. Al terminar, haga clic sobre el botón **«Siguiente»**.

g. Utilice **«Particionamiento Automático»**, a menos de que disponga de muy poco espacio en disco duro. Al terminar, haga clic sobre el botón **«Siguiente»** para ingresar a la herramienta para particiones del disco duro. Si está conforme con la tabla de particiones creada, haga clic sobre el botón **«siguiente»** para pasar a la siguiente pantalla.

h. Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de corrida 1, o cualquiera otro, haga clic en la casilla **«Usar la contraseña del gestor de arranque»**.

i. Para configurar los parámetros de red del sistema, haga clic sobre el botón **«Modificar»** para la interfaz eth0, y especifique la dirección IP y máscara de subred que utilizará en adelante el sistema. Al terminar, haga clic sobre el botón **«Aceptar»**.

j. En la ventana emergente para modificar la interfaz eth0, desactive la casilla **«Configurar usando DHCP»** y especificamos la dirección IP en 192.168.0.222 y máscara de subred 255.255.255.0. Al terminar, haga clic sobre el botón **«Aceptar»**, y luego clic en **«Siguiente»**.

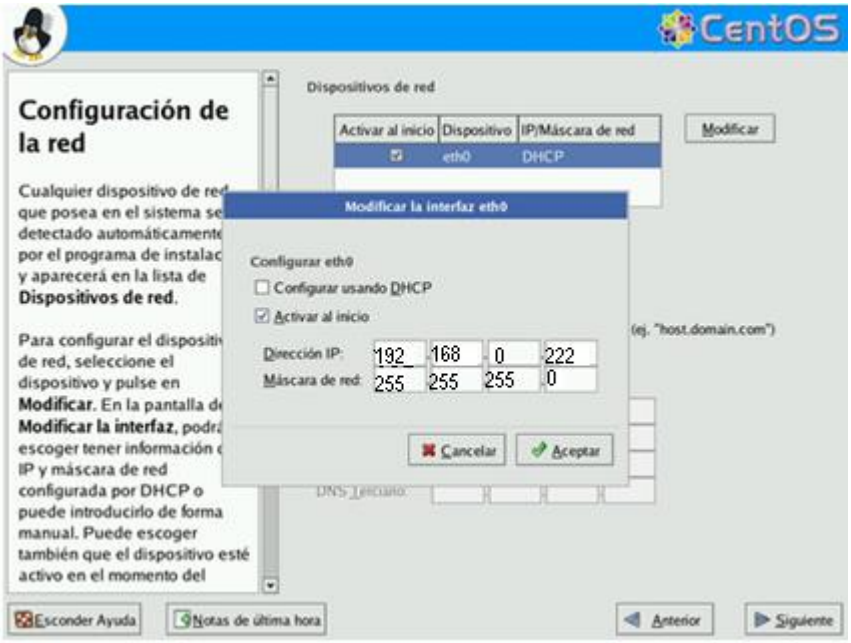


Figura 14. Pantalla Configuración direcciones IP

k. No configure el cortafuegos, de clic en **«Siguiente»**.

l. Haga clic sobre el botón **«Proceder»** a fin de saltar la configuración del cortafuegos.

m. Agregue el soporte para idiomas adicionales de acuerdo al país donde se hospedará el sistema. Si elimina «Spanish (Spain)», se eliminará la documentación y soporte para español genérico, por lo que lo es conveniente dejar dicha casilla habilitada. Finalmente, seleccione el idioma predeterminado a utilizar en el sistema. Al terminar, haga clic sobre el botón «Siguiente».

n. Seleccione la casilla «El sistema horario usará UTC», que significa que el reloj del sistema utilizará UTC (Tiempo Universal Coordinado), que es el sucesor de GMT (b>Greenwich Mean Time, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Haga clic con el ratón sobre **Guayaquil/Territorio Continental** o seleccione en el siguiente campo la zona horaria que corresponda a la región donde se hospedará físicamente el sistema.

o. Asigne una clave de acceso al usuario root. Debe escribirla dos veces a fin de verificar que está coincide con lo que realmente se espera. haga clic sobre el botón «Siguiente».

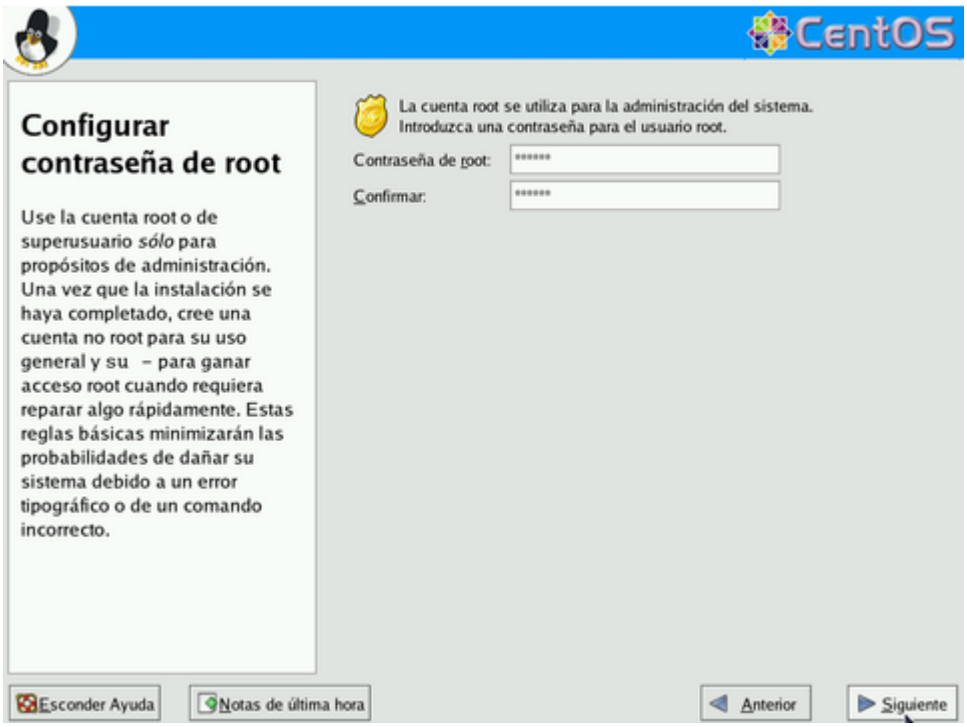


Figura 15. Configuración contraseña Súper Usuario

p. En la siguiente pantalla podrá seleccionar los grupos de paquetes que quiera instalar en el sistema. En este caso seleccionamos: Sistema X Windows, Escritorio GNOME, KDE, Internet Gráfico. Al terminar, haga clic sobre el botón «Siguiente».

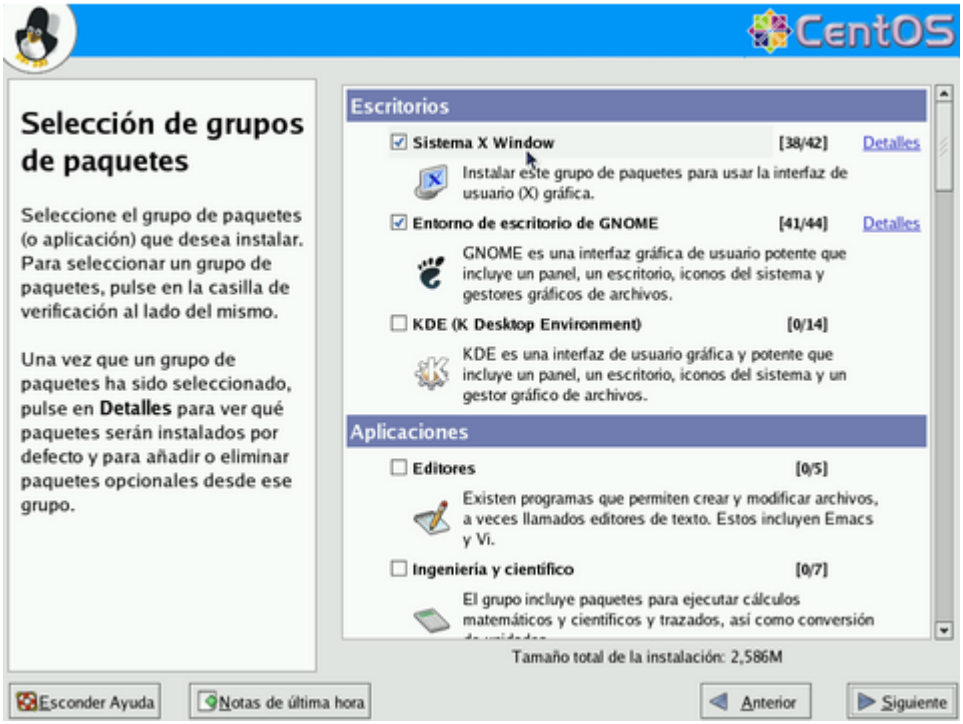


Figura 16. Selección de Paquetes a instalar

q. Una vez hecho lo anterior, haga clic sobre el botón «Siguiente» a fin de iniciar el proceso.

r. Se iniciará de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo.

s. Espere a que se terminen los preparativos del proceso de instalación.

t. Iniciará la instalación de los paquetes necesarios para el funcionamiento del sistema operativo. Espere algunos minutos hasta que concluya el proceso.

u. Una vez concluida la instalación de los paquetes, haga clic sobre el botón «Reiniciar».

3.5.2.5.3. Configuración del Servidor Radius

Para configurar una red wifi segura usando certificados de cliente y servidor para la autenticación se utilizará como servidor RADIUS el Linux CentOS y como software RADIUS usaremos FreeRADIUS, que viene instalado en el sistema operativo.

3.5.2.5.3.1. Archivos de Configuración

Todos los archivos de configuración de FreeRADIUS se encuentran en: /etc/raddb/

radiusd.conf - Archivo general de configuración de FreeRADIUS.

eap.conf – Archivo de configuración de las directivas EAP a utilizar. Es un include de radiusd.conf

clients.conf – Descripción y credenciales de los diferentes dispositivos que consultan al RADIUS (AP´s).

users – Archivo donde se especifican las credenciales de los usuarios de la red.

3.5.2.5.3.2. Configurando RADIUSD.CONF

```
prefix = /usr/local
exec_prefix = ${prefix}
sysconfdir = ${prefix}/etc
localstatedir = ${prefix}/var
sbindir = ${exec_prefix}/sbin
logdir = ${localstatedir}/log/radius
raddbdir = ${sysconfdir}/raddb
radacctdir = ${logdir}/radacct
# Location of config and logfiles.
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/radiusd
#
log_file = ${logdir}/radius.log
#
libdir = ${exec_prefix}/lib
#
```

```
pidfile = ${run_dir}/radiusd.pid
#
max_request_time = 30
#
delete_blocked_requests = no
#
cleanup_delay = 5
#
max_requests = 1024
#
bind_address = *
#
port = 0
#
hostname_lookups = no
#
allow_core_dumps = no
#
regular_expressions = yes
extended_expressions = yes
#
log_stripped_names = yes
#
log_auth = yes
#
log_auth_badpass = yes
log_auth_goodpass = yes
#
usercollide = no
#
lower_user = no
lower_pass = no
#
nospace_user = no
nospace_pass = no
checkrad = ${sbindir}/checkrad
# SECURITY CONFIGURATION
security {
max_attributes = 200
reject_delay = 1
status_server = no
}
# PROXY CONFIGURATION
proxy_requests = no
# CLIENTS CONFIGURATION
$INCLUDE ${confdir}/clients.conf
```

```
# SNMP CONFIGURATION
snmp = no
# THREAD POOL CONFIGURATION
thread pool {
start_servers = 5
max_servers = 32
min_spare_servers = 3
max_spare_servers = 10
max_requests_per_server = 0
}
# MODULE CONFIGURATION
modules {
$INCLUDE ${confdir}/eap.conf
mschap {
authtype = MS-CHAP
}
files {
usersfile = ${confdir}/users
acctusersfile = ${confdir}/acct_users
preproxy_usersfile = ${confdir}/preproxy_users
compat = no
}
}
# Instantiation
instantiate {
}
#
authorize {
files
mschap
eap
}
# Authentication.
authenticate {
Auth-Type MS-CHAP {
mschap
}
eap
}
#
preacct {
}
#
accounting {
}
#
```

```
session {
}
#
post-auth {
}
#
pre-proxy {
}
#
post-proxy {
}
```

3.5.2.5.3.3. Configurando USERS

“test” Auth-Type := EAP , User-Password == "test"

“mobile” Auth-Type := EAP , User-Password == "mobile"

3.5.2.5.3.4. Configurando Archivo EAP.CONF

```
eap {
default_eap_type = tls
timer_expire = 60
ignore_unknown_eap_types = no
cisco_accounting_username_bug = no
# Supported EAP-types
# EAP-TLS
tls {
private_key_password = laclave
private_key_file = ${raddbdir}/certs/servidor-prueba.key
certificate_file = ${raddbdir}/certs/servidor-prueba.crt
CA_file = ${raddbdir}/certs/demoCA/cacert.pem
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
fragment_size = 1024
include_length = yes
```

```
}
peap {
default_eap_type = mschapv2
}
mschapv2 {
}
}
```

3.5.2.5.3.5. Configurando Archivo CLIENTS.CONF

```
client 192.168.0.50 {
secret = testing123
shortname = UTC
}
client 192.168.0.55 {
secret = testing123
shortname = UTC
}
```

3.5.2.5.3.6. Arrancar el Servicio Freeradius

Para subir el servicio ejecutamos:

```
# /usr/local/sbin/radiusd -f -X
….
Listening on authentication *:1812
Listening on accounting *:1813
Ready to process requests.
```

Hacemos que FreeRADIUS se inicie cada vez que arranca el sistema operativo:

```
# chkconfig radiusd on
```

3.5.2.5.3.7. Configuración de los equipos Dlink AP-3200 y AP-2100

Como muestra la Figura 16 para el AP-2100 y Figura 17 para el AP-3200, debemos ingresar un nombre al Access Point, dar un nombre a la red (ESSID= UTC), seleccionar el canal (por defecto está el 6), seleccionar el método de autenticación WPA e ingresar los datos del servidor RADIUS. Recordar que la "shared secret" corresponde a la definida en el archivo clients.conf de FreeRadius y para este cliente. Aplicamos los cambios y el Access Point se reiniciara.

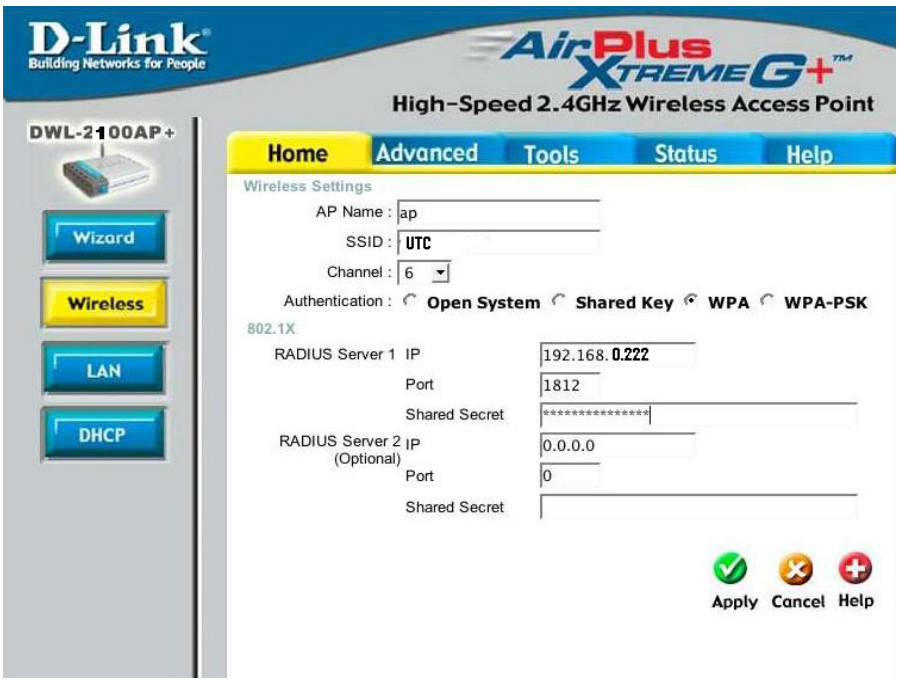


Figura 17. Configuración AP-2100

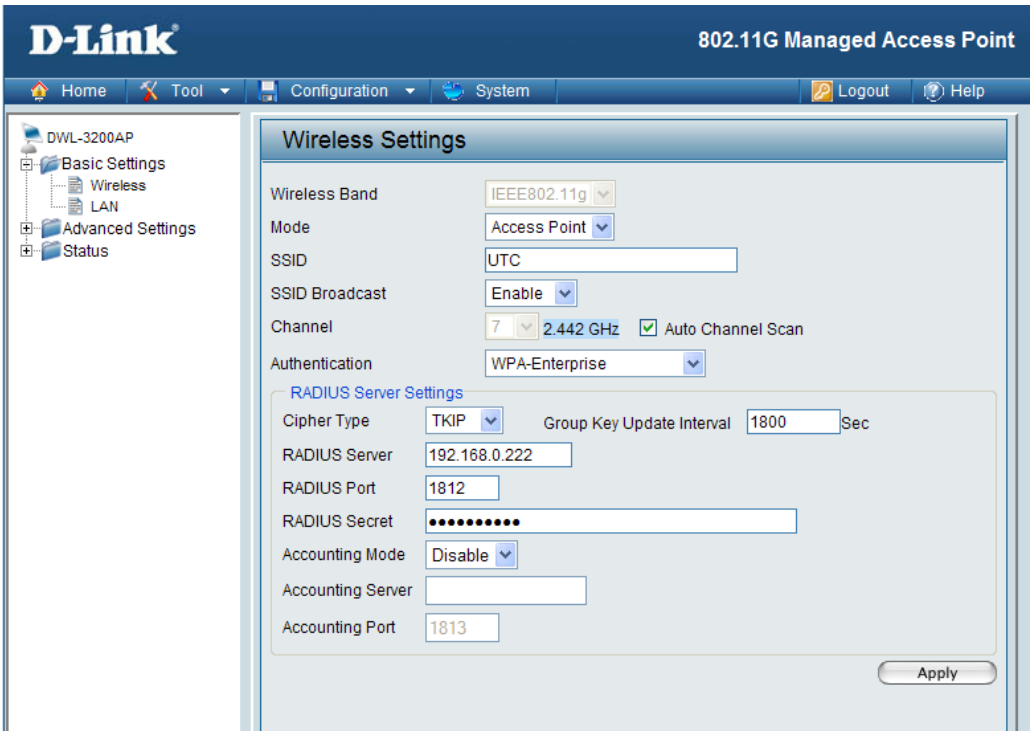


Figura 18. Configuración AP-3200

3.5.2.5.3.8. Configuración de 802.1x en el Cliente

Para configurar los clientes debemos tener en cuenta las siguientes especificaciones:

- Sistema Operativo: Windows XP con Service Pack 2.
- Tener previamente instalada una tarjeta wireless (inalámbrica) Tipo b ó g.
- Habilitar físicamente la tarjeta inalámbrica.

Abrir Conexiones de Red

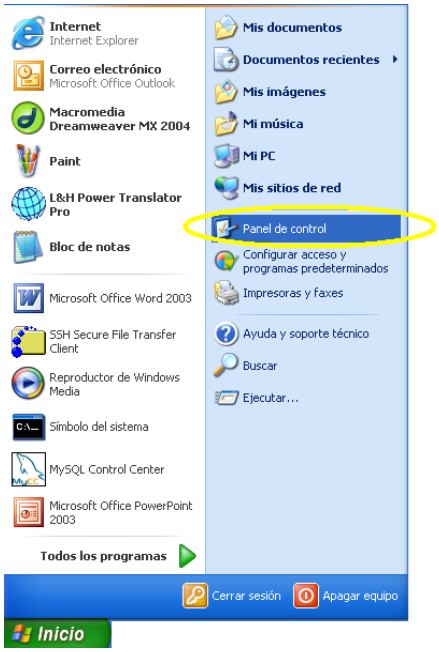


Figura 19. Selección Panel de Control

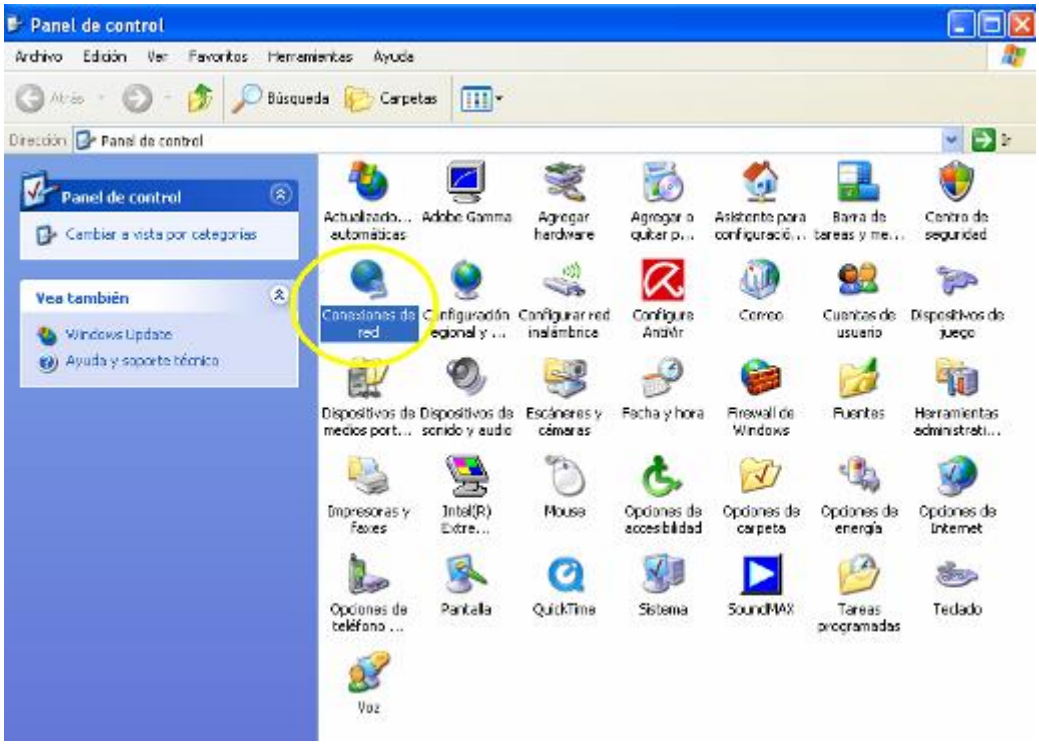


Figura 20. Selección Conexiones de Red

Escogemos la “conexión de redes inalámbricas” click derecho “propiedades “y se nos muestra una pantalla con el detalle de propiedades, escogemos la pestaña “redes inalámbricas”

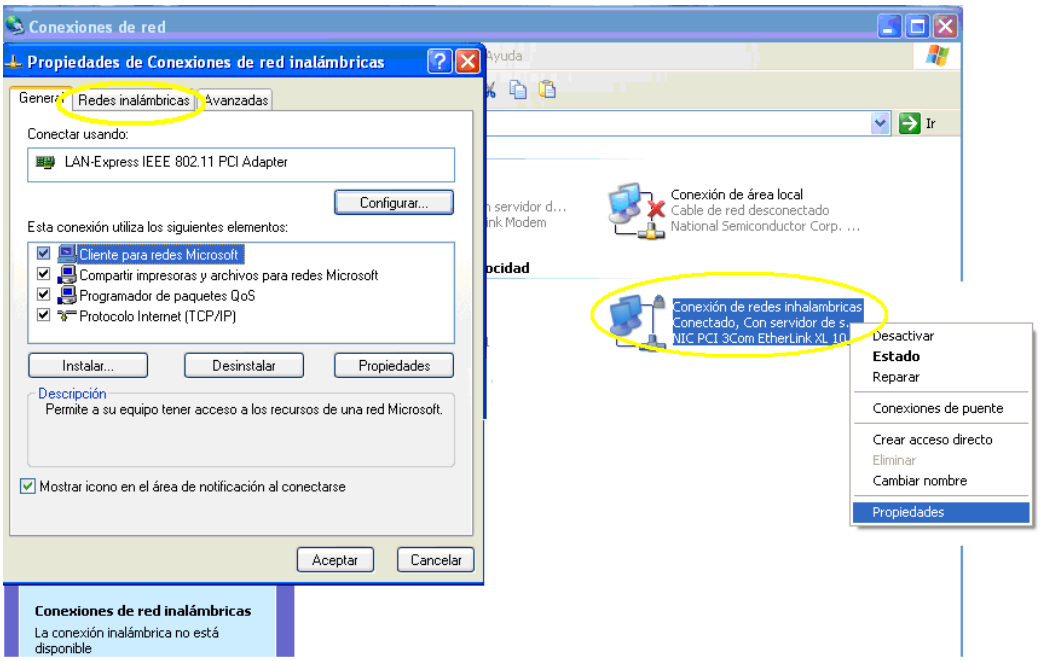


Figura 21. Propiedades de Red

Se nos muestra entonces la siguiente pantalla, hacemos click en “Agregar”, pero antes marcamos lo indicado en la figura.

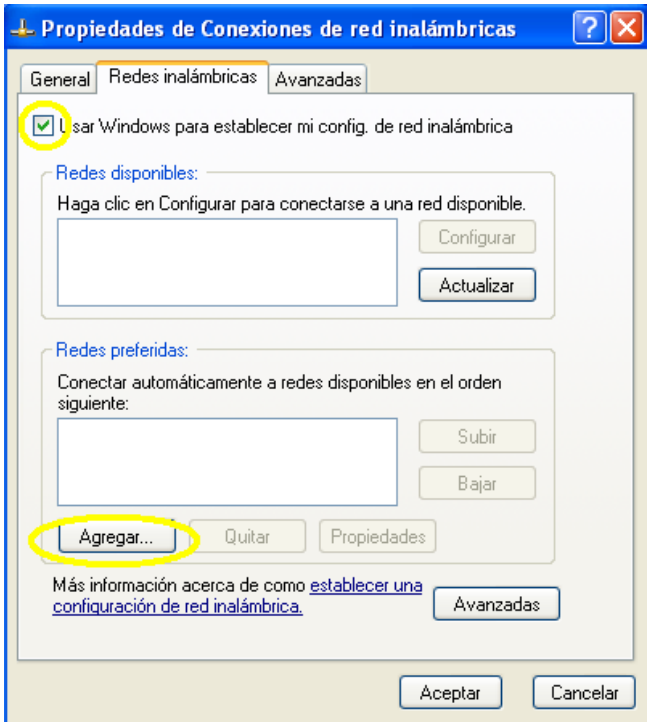


Figura 22. Propiedades de conexiones de red inalámbrica

Se nos muestra la siguiente pantalla, En la pestaña "Asociación" marque las casillas marcadas y además ingrese en "Nombre de red (SSID)" la palabra UTC, y hacemos clic en "Aceptar"

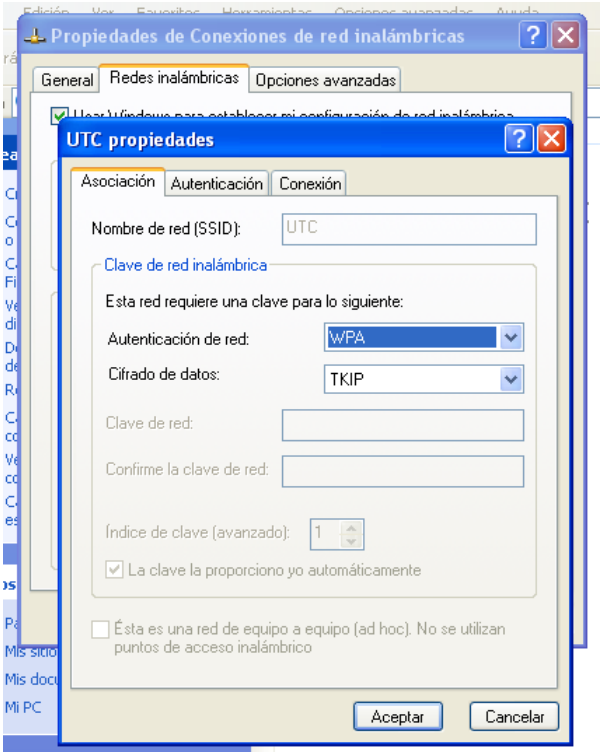


Figura 23. Ficha de Propiedades

Ahora en la misma pantalla escogemos la otra Pestaña "Autenticación ", marque las casillas marcadas y en "Tipo de EAP" escoja la opción EAP protegido (PEAP).

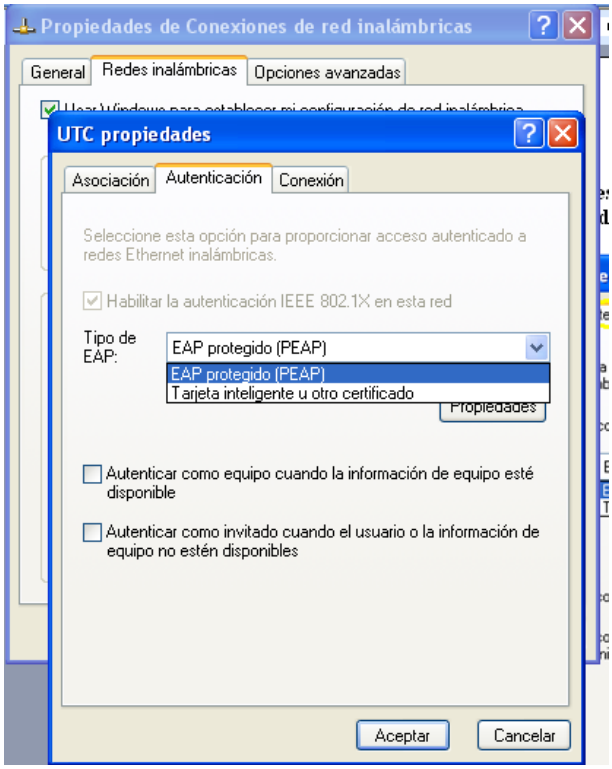


Figura 24. Selección de Autenticación

Una vez escogido la opción EAP protegido (PEAP), en la misma pantalla escogemos la opción “Propiedades” y se nos muestra la siguiente pantalla

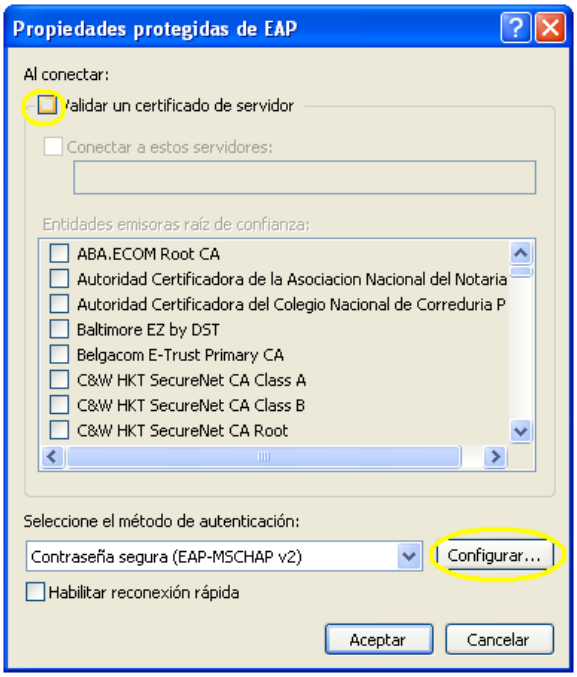


Figura 25. Propiedades de EAP

Desmarcamos la opción "Validar un certificado de servidor" y hacemos click en "Configurar", se nos muestra la siguiente sub-pantalla

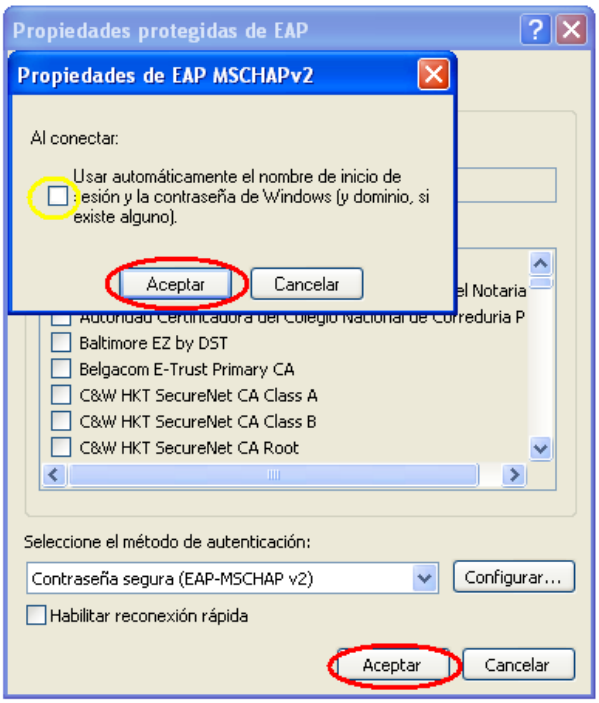


Figura 26. Propiedades de EAP MSCHAPv2

Hacemos click en “Aceptar” (marcado con rojo) de la subpantalla y en todos los otros “Aceptar” que se van mostrando.

Activamos físicamente la tarjeta inalámbrica. Finalmente el momento que se activa la tarjeta inalámbrica aparece un cuadro de dialogo solicitando las credenciales.

Figura 27. Ingreso de contraseña

Nombre de Usuario	Mobile
Contraseña	Mobile
Dominio de inicio de sesión	<<ESTE CAMPO VA VACIO>>

Tabla 2. Ingreso de Contraseñas para acceso a la Red

3.5.2.5.4. Configuración de un Servidor DHCP

DHCP (acrónimo de Dynamic Host Configuration Protocol que se traduce como Protocolo de configuración dinámica de servidores) es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red (dirección IP; máscara de subred, puerta de

enlace, etc.) a partir de un servidor DHCP. Su propósito principal es hacer más fáciles de administrar las redes grandes. DHCP existe desde 1993 como protocolo estándar y se describe a detalle en el RFC 2131.

Sin la ayuda de un servidor DHCP, tendría que configurarse de forma manual cada dirección IP de cada anfitrión que pertenezca a la red del Centro Asociado del cantón La Maná de la Universidad Técnica de Cotopaxi. Un servidor DHCP entonces supervisa y distribuye las direcciones IP de la red asignando una dirección IP a cada anfitrión que se una. Cuando, una computadora portátil se configura para utilizar DHCP, a ésta le será asignada una dirección IP y otros parámetros de red necesarios para unirse a cada Red de Área Local donde se localice.

Existen tres métodos de asignación en el protocolo DHCP:

- **Asignación manual:** La asignación utiliza una tabla con direcciones MAC (acrónimo de Media Access Control Address, que se traduce como dirección de Control de Acceso al Medio). Sólo los anfitriones con una dirección MAC definida en dicha tabla recibirán el IP asignada en la misma tabla. Esto se hace a través de los parámetros hardware ethernet y fixed-address.

- **Asignación automática:** Una dirección de IP disponible dentro de un rango determinado se asigna permanentemente al anfitrión que la requiera.

- **Asignación dinámica:** Se determina arbitrariamente un rango de direcciones IP y cada anfitrión conectado a la red está configurada para solicitar su dirección IP al servidor cuando se inicia el dispositivo de red, utilizando un intervalo de tiempo controlable (parámetros default-lease-time y max-lease-time) de modo que las direcciones IP no son permanentes y se reutilizan de forma dinámica.

3.5.2.5.4.1. Configuración del Archivo DHCPD.CONF

```
ddns-uptdate-style interim;
ignore client-updates;
subnet 192.168.0.0 netmask 255.255.255.0 {
        option routers 192.168.0.222;
        option subnet-mask 255.255.255.0;
        option domain-name-servers utc.lamana.edu.ec;
        option ip-forwarding off;
        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;
}
```

3.5.2.5.4.2. Arrancar el Servicio DHCP

Para subir el servicio ejecutamos:

```
# service dhcpd start
```

Hacemos que dhcp se inicie cada vez que arranca el sistema operativo:

```
# chkconfig dhcpd on
```

3.5.2.5.5. Configuración de un Servidor Intermediario

Un Servidor Intermediario (Proxy) se define como una computadora o dispositivo que ofrece un servicio de red que consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red.

3.5.2.5.5.1. Funcionamiento de un Servidor Intermedio

- Cliente se conecta hacia un Servidor Intermediario (Proxy).
- Cliente solicita una conexión, fichero u otro recurso disponible en un servidor distinto.
- Servidor Intermediario (Proxy) proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.
- En algunos casos el Servidor Intermediario (Proxy) puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

3.5.2.5.5.2. Características del Servidor Intermediario

Los Servidores Intermediarios (Proxies) generalmente se hacen trabajar simultáneamente como muro cortafuegos operando en el Nivel de Red, actuando como filtro de paquetes, como en el caso de iptables, o bien operando en el Nivel de Aplicación, controlando diversos servicios, como es el caso de TCP Wrapper. Dependiendo del contexto, el muro cortafuegos también se conoce como BPD o Border Protection Device o simplemente filtro de paquetes.

Una característica común de los Servidores Intermediarios (Proxies) es funcionar como caché de contenido de Red (principalmente HTTP), proporcionando en la proximidad de los clientes un caché de páginas y ficheros disponibles a través de la Red en servidores HTTP remotos, permitiendo a los clientes de la red local acceder hacia éstos de forma más rápida y confiable.

Cuando se recibe una petición para un recurso de Red especificado en un URL (Uniform Resource Locator) el Servidor Intermediario busca el resultado del URL dentro del caché. Si éste es encontrado, el Servidor Intermediario responde al cliente proporcionado inmediatamente el contenido solicitado. Si el contenido solicitado no estuviera disponible en el caché, el Servidor Intermediario lo traerá

desde servidor remoto, entregándolo al cliente que lo solicitó y guardando una copia en el caché. El contenido en el caché es eliminado luego a través de un algoritmo de expiración de acuerdo a la antigüedad, tamaño e historial de respuestas a solicitudes (hits) (ejemplos: LRU, LFUDA y GDSF).

3.5.2.5.5.3. SQUID

Squid es un Servidor Intermediario (Proxy) de alto desempeño que se ha venido desarrollando desde hace varios años y es hoy en día un muy popular y ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix®. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo sustento lógico libre, está disponible el código fuente para quien así lo requiera.

Entre otras cosas, Squid puede funcionar como Servidor Intermediario (Proxy) y caché de contenido de Red para los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, caché transparente, WWCP, aceleración HTTP, caché de consultas DNS y otras muchas más como filtración de contenido y control de acceso por IP y por usuario.

3.5.2.5.5.4. Configuración del SQUID

Squid se instala de manera predeterminada a menos que especifique lo contrario, durante la instalación del sistema operativo, y viene incluido en todas las distribuciones actuales de Linux CentOS.

Squid utiliza el fichero de configuración localizado en /etc/squid/squid.conf, y podrá trabajar sobre este utilizando cualquier editor de texto, en este proyecto utilizamos el VI.

En el archivo squid.conf cambiamos las siguientes líneas de instrucción:

```
# Default: http_port 3128
http_port 192.168.0.222:3128
cache_mem 16 MB
cache_dir ufs /var/spool/squid 700 16 256
acl utc src 192.168.0.0/255.255.255.0
acl sitiosdenegados url_regex "/etc/squid/sitiosdenegados"
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
http_access allow utc password !sitiosdenegados
```

3.5.2.5.5.5. Acceso por Autenticación en SQUID

Es muy útil el poder establecer un sistema de autenticación para poder acceder hacia Internet, pues esto permite controlar quienes si y quienes no accederán a Internet sin importar desde que máquina de la red local lo hagan. Sera de modo tal que tendremos un control por nombre de usuario y clave de acceso.

3.5.2.5.5.5.1. Autenticación a Través del Módulo NCSA

Squid puede utilizar el módulo ncsa_auth, de la NCSA (National Center for Supercomputing Applications), y que ya viene incluido como parte del paquete principal de Squid en la mayoría de las distribuciones actuales. Este módulo provee una autenticación muy sencilla a través de un fichero de texto simple cuyas claves de acceso fueron creadas con htpasswd.

Se requerirá la creación previa de un fichero que contendrá los nombres de usuarios y sus correspondientes claves de acceso (cifradas). El fichero puede localizarse en cualquier lugar del sistema, con la única condición que sea asequible para el usuario squid.

Se creo un fichero /etc/squid/claves:

touch /etc/squid/claves

A continuación deberemos dar de alta las cuentas que sean necesarias, utilizando el mandato htpasswd -mismo que viene incluido en el paquete httpd-2.0.x-. Para el presente proyecto se creo la siguiente clave:

htpasswd /etc/squid/claves joseperez

Lo anterior solicitará teclear una nueva clave de acceso para el usuario joseperez y confirmar tecleando ésta de nuevo. Repita con el resto de las cuentas que requiera dar de alta.

Todas las cuentas que se den de alta de este modo son independientes a las ya existentes en el sistema. Al dar de alta una cuenta o cambiar una clave de acceso lo estará haciendo EXCLUSIVAMENTE para el acceso al servidor Proxy. Las cuentas son independientes a las que se tengan existentes en el sistema como serían intérprete de mandatos, correo y Samba.

Lo siguiente será especificar que programa de autenticación para lo cual digitamos la siguiente orden:

 # auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves

3.5.2.5.5.6. Arrancar el Servicio SQUID

Para subir el servicio ejecutamos:
service squid start

Hacemos que squid se inicie cada vez que arranca el sistema operativo:

chkconfig squid on

3.5.3. Costo de materiales utilizados en la implantación de cableado estructurado

Ver anexo No. 1

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Con la investigación desarrollada se realizó la implantación de una red Inalámbrica para el Centro Asociado del Cantón La Maná de la Universidad Técnica de Cotopaxi, que permite que los estudiantes, profesores y personal administrativo que se encuentran en el sector de aulas, laboratorios, biblioteca y área recreativa que pertenecen al Campus Universitario, puedan acceder a diferentes servicios que proporciona la conectividad inalámbrica como Internet de banda ancha, acceso a red cableada, e intercambio de información.

- Una vez realizada la implantación de este tipo de red podemos decir que es una herramienta útil y eficiente para la comunicación móvil, además de facilitar la instalación de los dispositivos sin necesidad de ningún tipo de cableado ni la modificación arquitectónica del área en donde se va a implantar la red.

- Otro de los beneficios de este tipo de tecnología inalámbrica es que permite la incorporación de nuevos usuarios a la red de una manera rápida y permitiendo gran flexibilidad en la ubicación de los equipos.

- Con el desarrollo de la investigación se afianzó el conocimiento en redes, en especial en redes inalámbricas, a su vez se consolidó el conocimiento en configuración y puesta en marcha de Access Point y sus diversos modos de administración.

- Se contó con la bibliografía suficiente tanto física como virtual, la misma que nos permitió llegar a cumplir los objetivos propuestos.

- Durante el desarrollo de la investigación el Centro Asociado brindó todo el apoyo necesario como fue de tipo técnico como humano; así como también por parte de las autoridades de la Universidad.

- Es necesario mencionar que no existió ningún inconveniente para la realización de la propuesta de diseño de la red inalámbrica y que todos los objetivos fueron cumplidos sin ningún percance.

Recomendaciones

Una vez concluido el proceso investigativo, recomendamos:

- Para la administración de la red se deberá considerar aspectos como la atención a fallas, configuración de tarjetas PCMCIA y seguridad por lo que se deberá contar con los servicios de profesionales capacitados para el soporte de usuarios y la administración de la red inalámbrica.

- Para un mejor funcionamiento y mayor tiempo de vida útil de los equipos es aconsejable realizar un mantenimiento frecuente tanto físico como de software, para evitar molestias a futuro.

- Hacer una revisión de la parte eléctrica de la universidad, para que no haya picos de voltaje en el cuarto de control**.**

- Se debe incentivar a los estudiantes para que continúen con este tipo de trabajos prácticos que va en beneficio tanto de la institución como de las futuras generaciones de profesionales.

- Se debe considerar el orientar al estudiantado sobre las bondades que ofrecen las nuevas tecnologías como en este caso, redes inalámbricas las cuales al momento se encuentran en apogeo.

BIBLIOGRAFÍA

Bibliografía Citada:

1. Colegio de Ingenieros De Telecomunicaciones, (2004) "WLAN basadas en el estándar IEEE 802.11", Madrid, Pág. 25.

2. ESPÍN DEL POZO, Javier. RUIZ LUDEÑA José Luís. "Topologías de redes", Pág. 89.

3. ENCICLOPEDIA DE INFORMACIÓN. http://www.wikipedia.org.

4. GÓMEZ LÓPEZ J. (2008). "Guía de campo de WI-FI". Edit. Ra-Ma, Pág. 123.

5. SÁNCHEZ NAVARRO, José Daniel. (2002). "Tipos de redes". Editorial McGraw Hill, Pág. 115.

6. REID, NEIL & SEIDE, "Manual de Redes Inalámbricas" (2004) Editorial McGraw-Hill , Pág 45, 145

Bibliografía Consultada

7. Abad Domingo, Alfredo (Editorial McGraw-Hill), Redes de Area Local

8. BAÑARES, José Luis. (2004). "Sistemas de Comunicación y Redes".

9. CARBALLAR, J.A. (Editorial Ra-ma), WI-FI. INSTALACIÓN, SEGURIDAD Y APLICACIONES

10. CARBALLAR, J.A. “Wi-fi. Instalación, Seguridad y Aplicaciones”, 2007, Editorial Ra-ma

11. José A. Carballar Falcón (Editorial Ra-ma), WI-FI. CÓMO CONSTRUIR UNA RED INALÁMBRICA, 2ª EDICIÓN.

12. Prentice-Hall, L.W. Couch II “Sistemas de Comunicación Digitales y Analógicos”. 2002

13. RODRIGUEZ, Jorge. (2000). “Introducción a las Redes de Área Local”.

Bibliografía Básica

14. ADMINISTRACIÓN BÁSICA DE LINUX
http://www.adrformacion.com/cursos/linuxad/leccion3/tutorial2.html

15. CONFIGURACION DE REDES INALAMBRICAS Y DISPOSITIVOS
http://igor.tamarapatino.org/escritos/conf/wireless/implantacion.html

16. CONFIGURACIONES SQUID PROXY
http://www.linuxparatodos.net/portal/staticpages/index.php?page=19-0-como-squid-general

17. LAS REDES DE AREA LOCAL.
http://www.monografias.com/trabajos15/las-redes/las-redes.shtml

18. RESTRICCIONES ACCESO WEB
http://www.linuxparatodos.net/portal/staticpages/index.php?page=19-2-como-squid-restriccion-web

ANEXOS 1

COSTO DE MATERIALES UTILIZADOS EN LA IMPLANTACIÓN DE RED INALÁMBRICA

Cantidad	Producto	P. Unitario	Total
1	Switch 3COM, 24 puertos	145,00	145,00
50	Cable UTP Cat. 5e	0.60	30,00
2	Access Point D-LINK	225,00	450,00
2	Antenas omnidireccionales de 7dbi	50,00	100,00
1	Discos Instalación CentOS	25,00	25,00
1	Tarjeta de red CNET	15,00	15,00
Subtotal			**765,00**
IVA			**91.80**
TOTAL			**856.80**

SUMINISTROS

Cantidad	Producto	P. Unitario	Total
2	Resmas de papel bond A4	3,5	7,00
4	Esferográficos	0,3	1,20
10	Carpetas de cartón	0,3	3,00
300	Impresiones	0,15	45,00
800	Copias	0,03	24,00
5	Anillados	1	5,00
Subtotal			**85,20**
IVA			**10,22**
TOTAL			**95,42**

VIATICOS

Cantidad	Producto	P. Unitario	Total
	Pasajes		72,00
	Alimentación		48,00
	Hospedaje		120,00
Subtotal			**240,00**
IVA			**24,00**
TOTAL			**264,00**

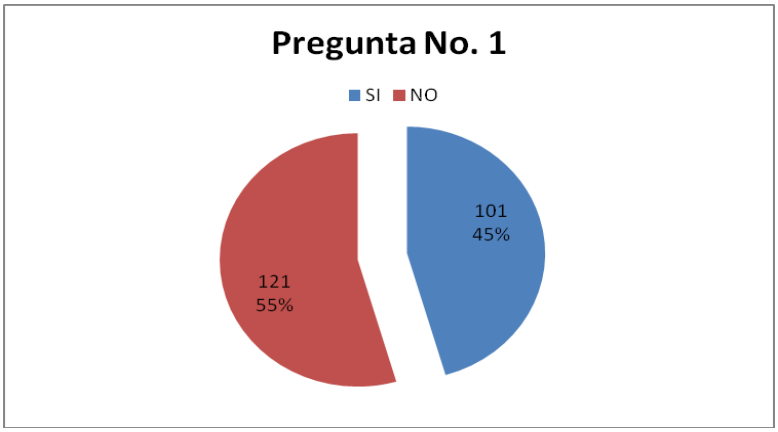
Costo total: $ 1.216,22 (mil doscientos dieciséis dólares con 22/100)

ANEXO 2

RESULTADOS DE LA ENCUESTA DIRIGIDOS A LOS ESTUDIANTES

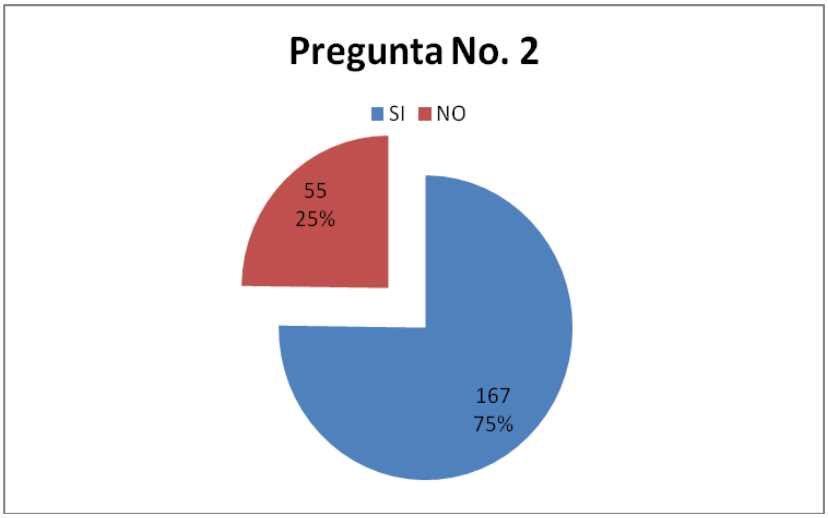
1. ¿Conoce Ud. Sobre Redes Inalámbricas?

Representación Gráfica



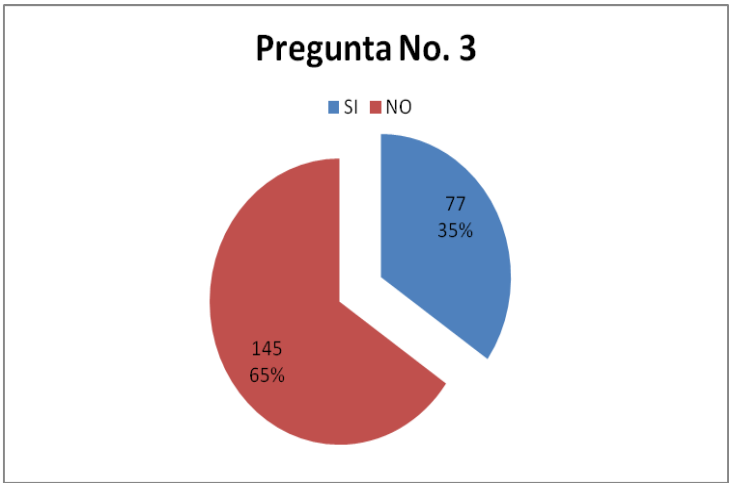
2.- ¿El Centro Asociado ofrece servicios informáticos?

Representación Gráfica



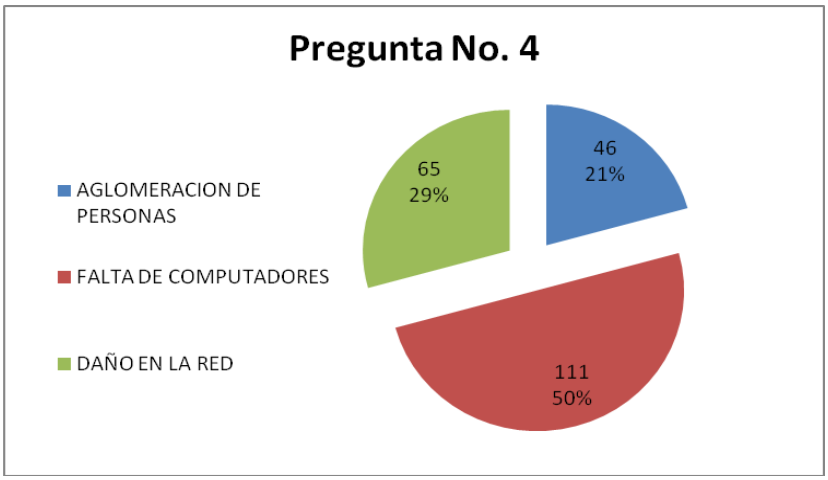
3.- ¿El Centro Asociado ha prestado servicios informáticos hasta el momento eficientes a la comunidad universitaria?

Representación Gráfica



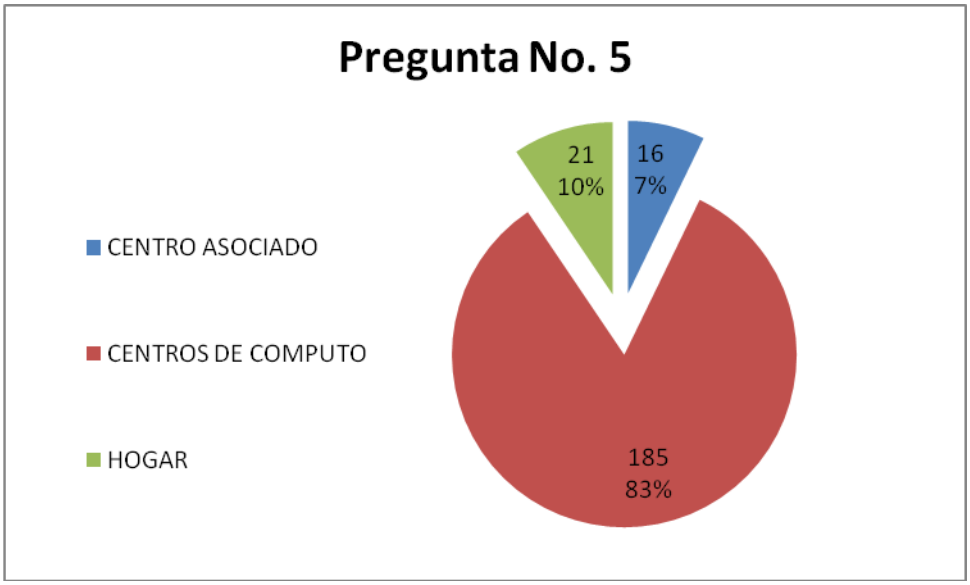
4.- ¿Cuáles son los problemas más importantes que se han presentado al usar el Laboratorio Informático del Centro Asociado?

Representación Gráfica



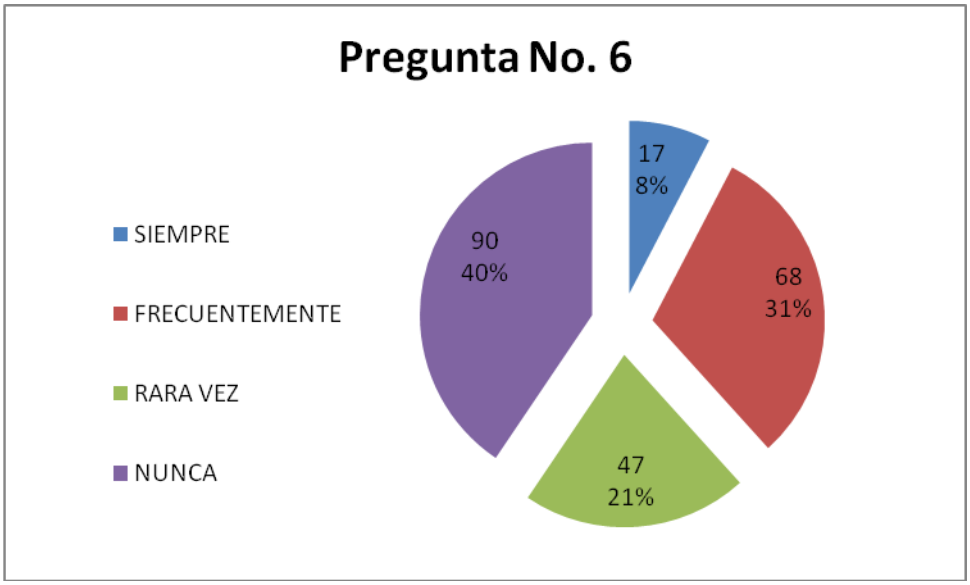
5.- ¿Dónde utiliza actualmente el servicio de Internet?

Representación Gráfica



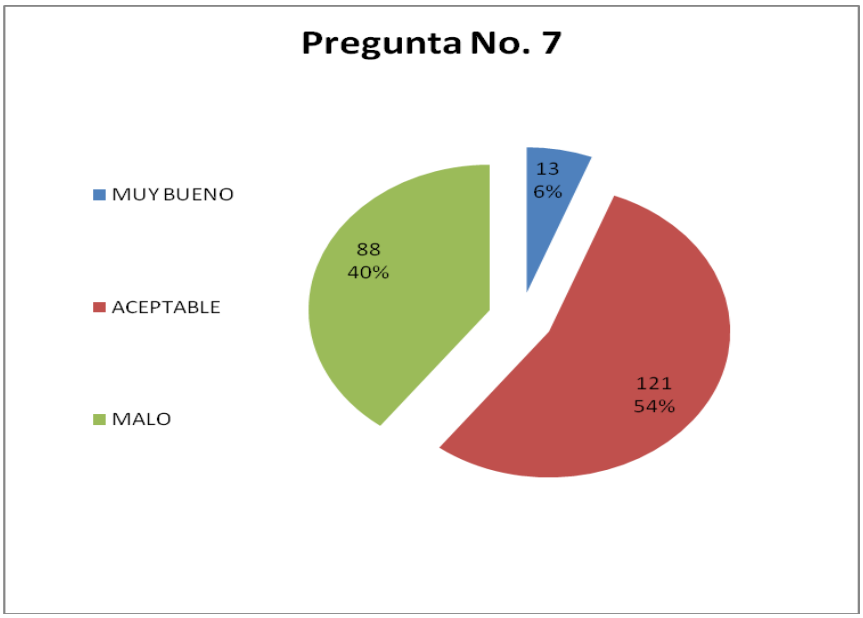
6.- ¿Con qué frecuencia usted utiliza el Centro de Cómputo del Centro Asociado?

Representación Gráfica



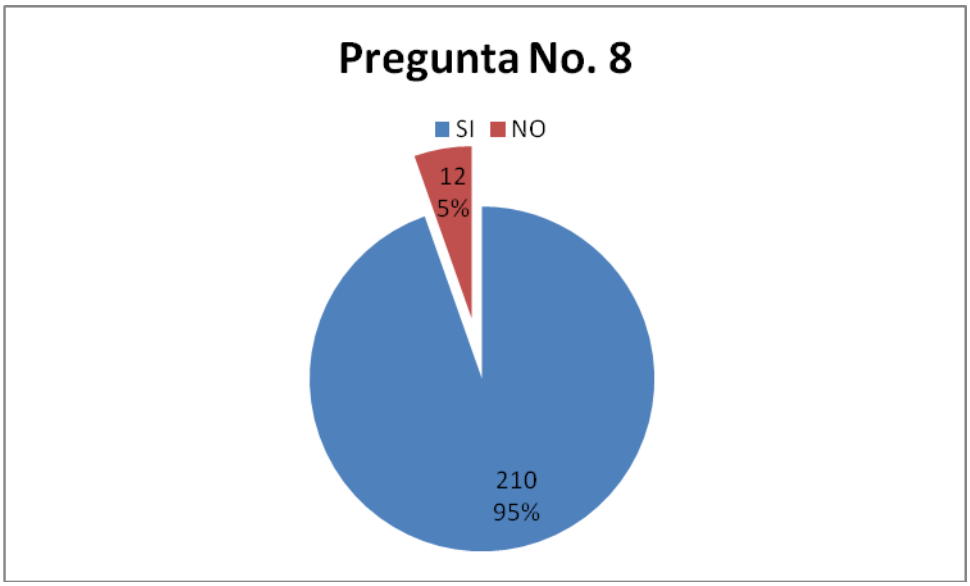
7.- ¿El servicio de Internet en el Centro Asociado para realizar sus actividades cotidianas es?

Representación Gráfica



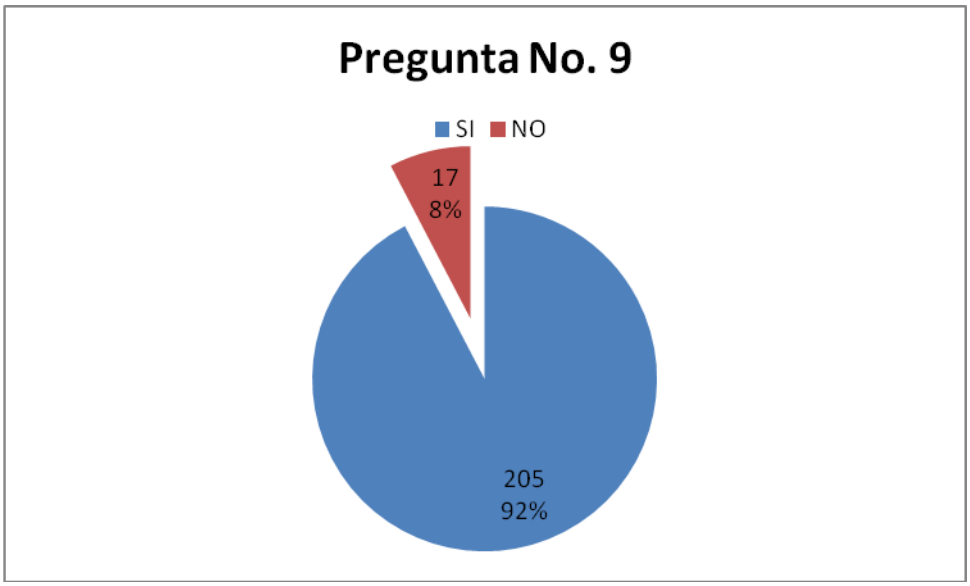
8.- ¿Considera usted que los servicios informáticos prestados actualmente en el Centro Asociado deben ser modernizados?

Representación Gráfica



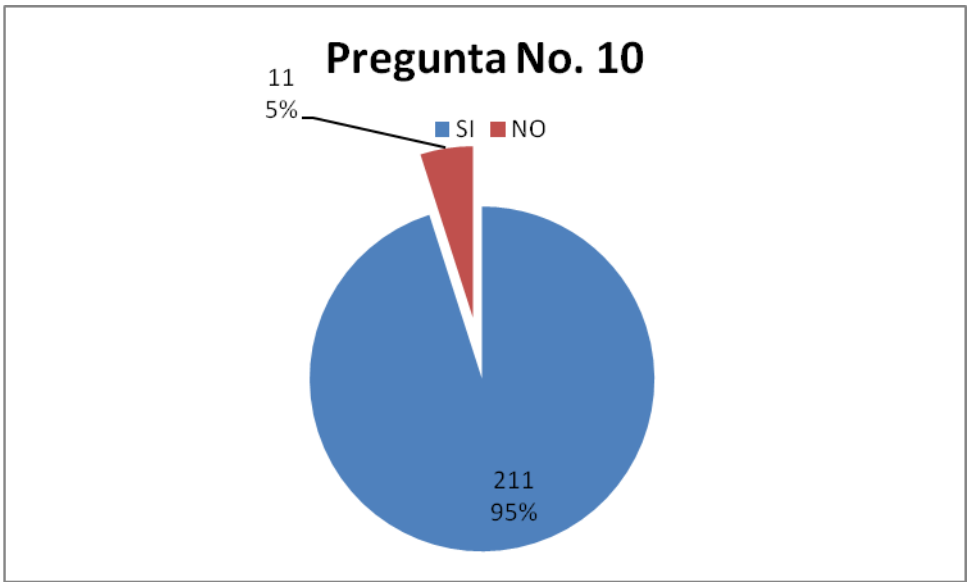
9.- ¿Considera usted que sería beneficioso poder acceder a los servicios informáticos en todo momento y desde cualquier punto del campus universitario del Centro Asociado?

Representación Gráfica



10.- ¿Considera usted que el uso de la tecnología informática y la implantación de una Red Inalámbrica en el Centro Asociado permitirá solucionar las dificultades de conexión y prestación de servicios?

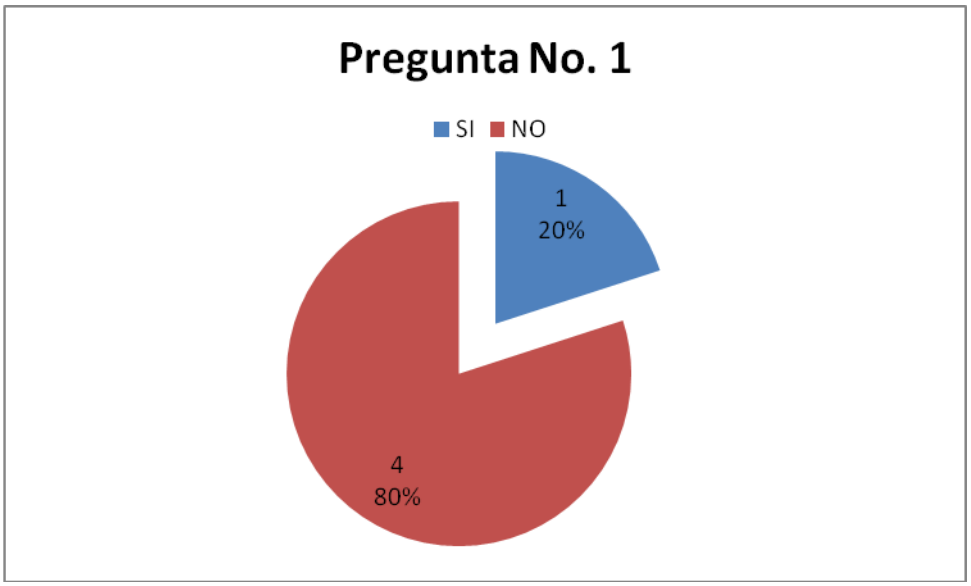
Representación Gráfica



2.2 RESULTADOS DE LA ENCUESTA DIRIGIDOS A LOS DOCENTES

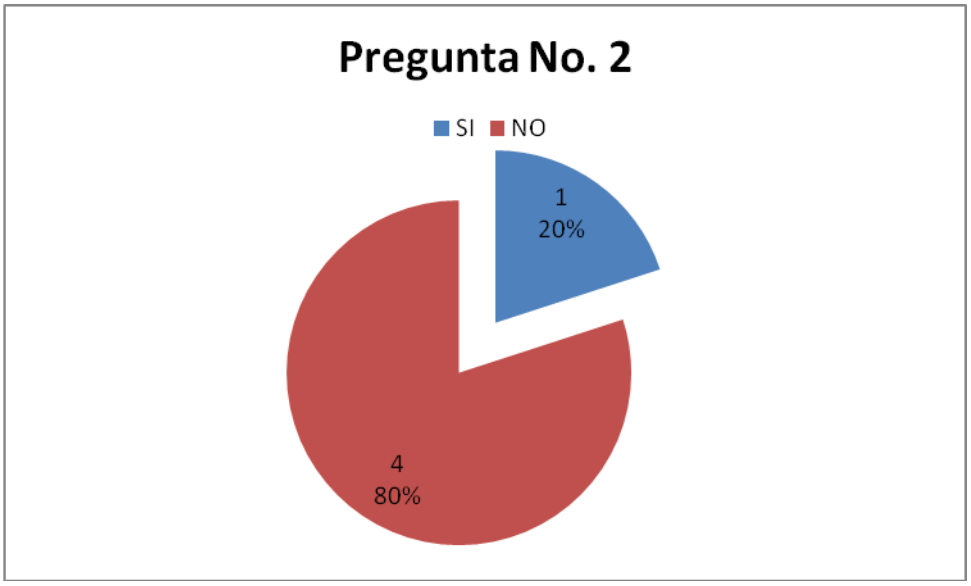
1.- ¿Conoce Ud. Sobre Redes Inalámbricas?

Representación Gráfica



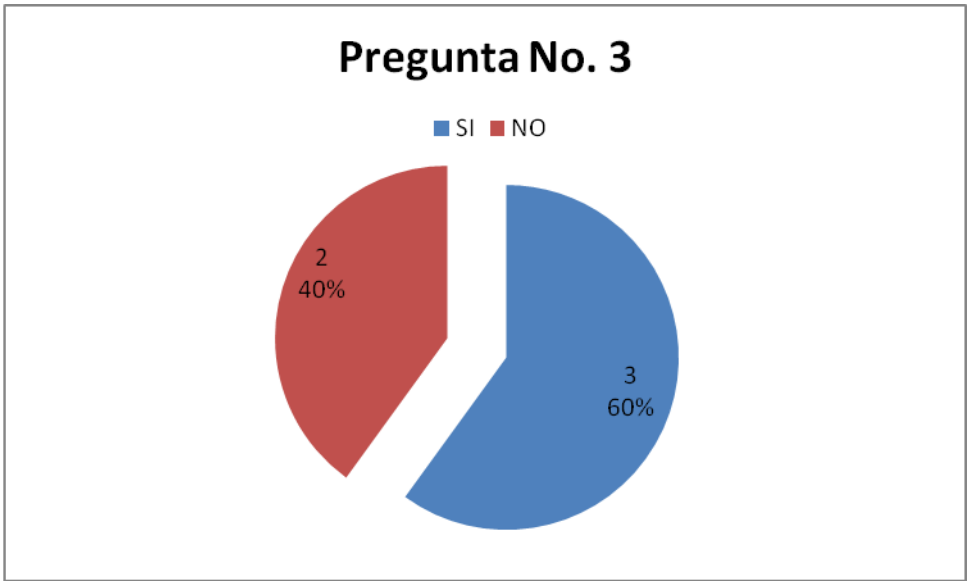
2.- ¿El Centro Asociado ofrece servicios informáticos?

Representación Gráfica



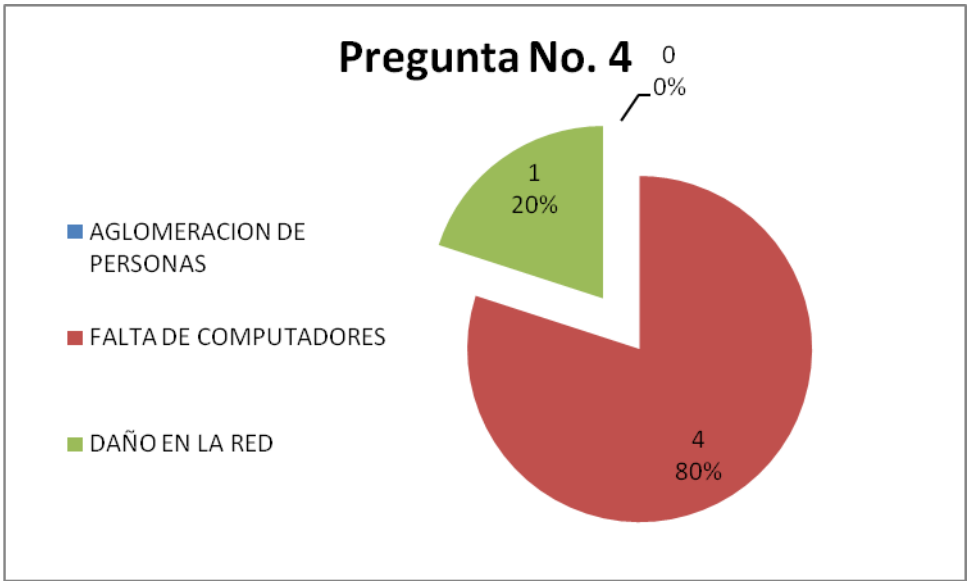
3.- ¿El Centro Asociado ha prestado servicios informáticos hasta el momento eficientes a la comunidad universitaria?

Representación Gráfica



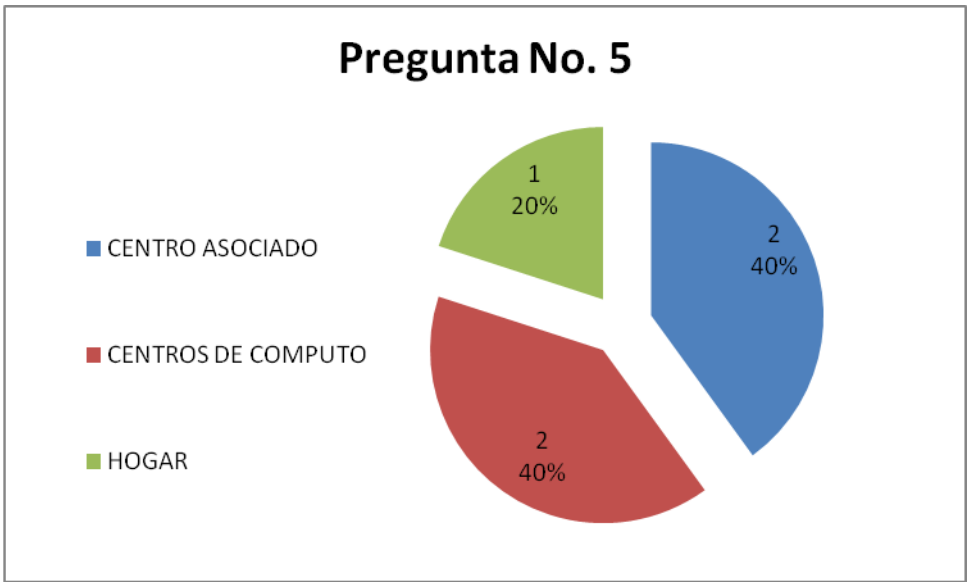
4.- ¿Cuáles son los problemas más importantes que se han presentado al usar el Laboratorio Informático del Centro Asociado?

Representación Gráfica



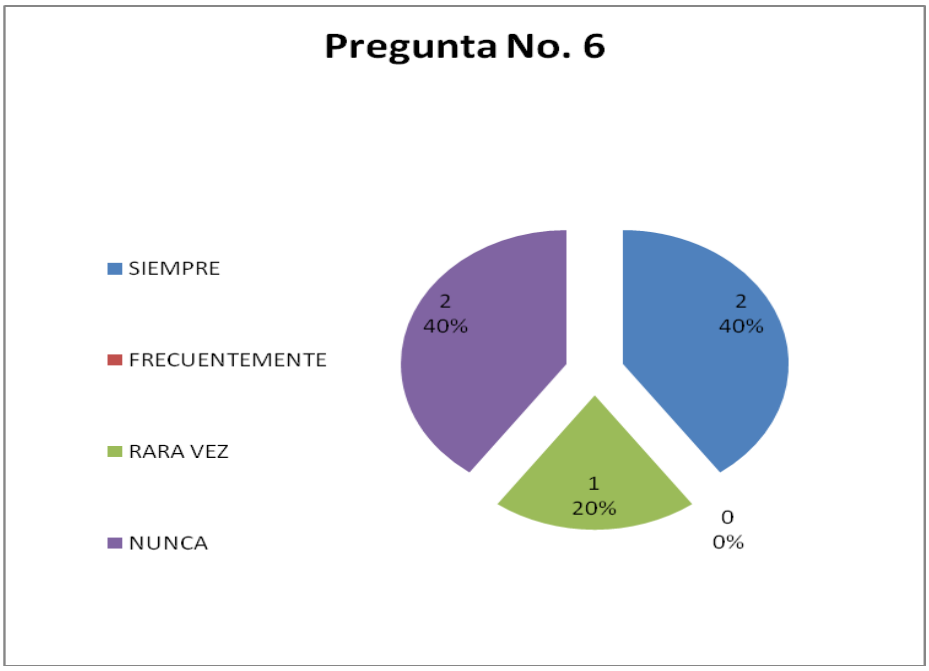
5.- ¿Dónde utiliza actualmente el servicio de Internet?

Representación Gráfica



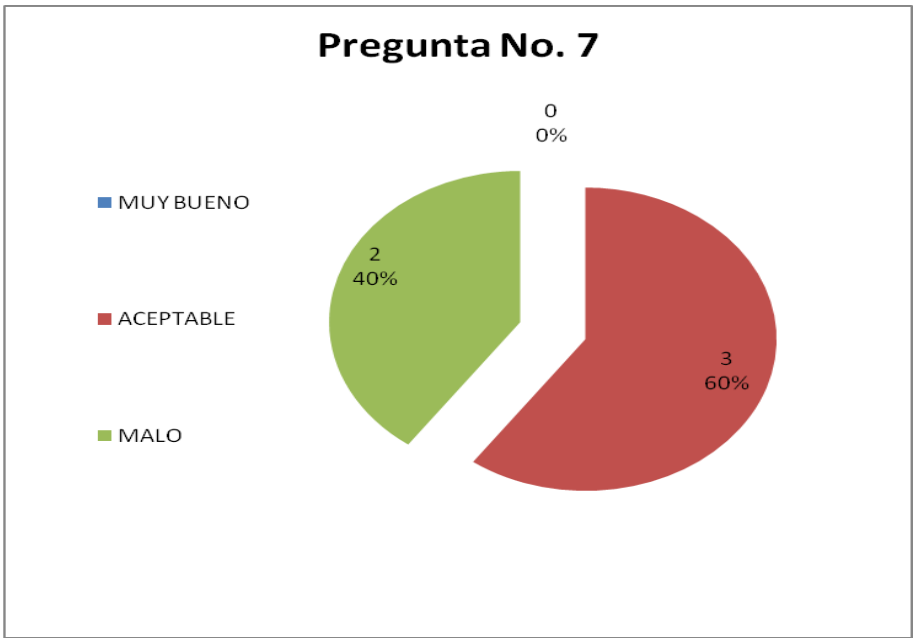
6.- ¿Con qué frecuencia usted utiliza el Centro de Cómputo del Centro Asociado?

Representación Gráfica



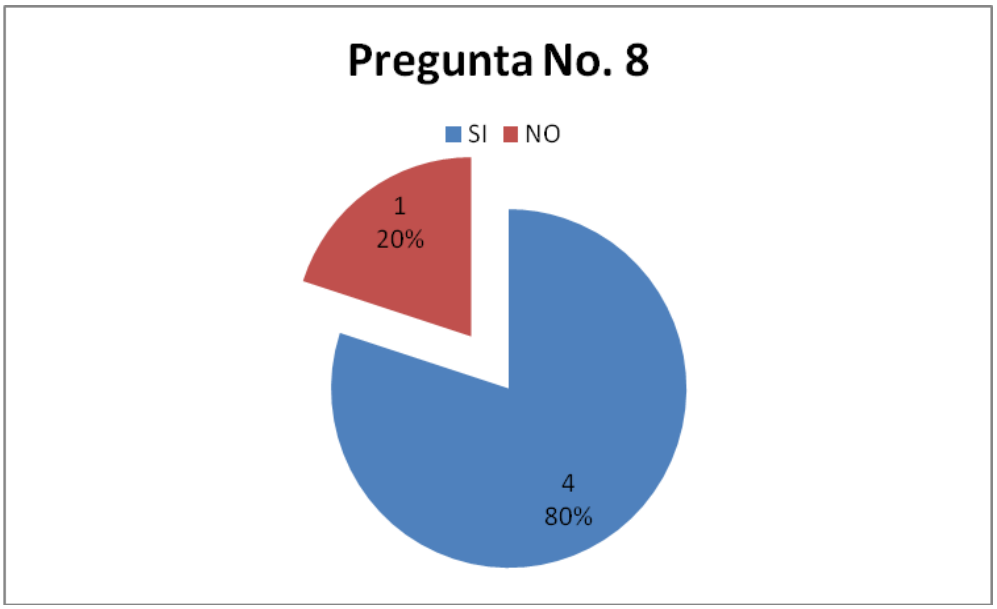
7.- ¿El servicio de Internet en el Centro Asociado para realizar sus actividades cotidianas es?

Representación Gráfica



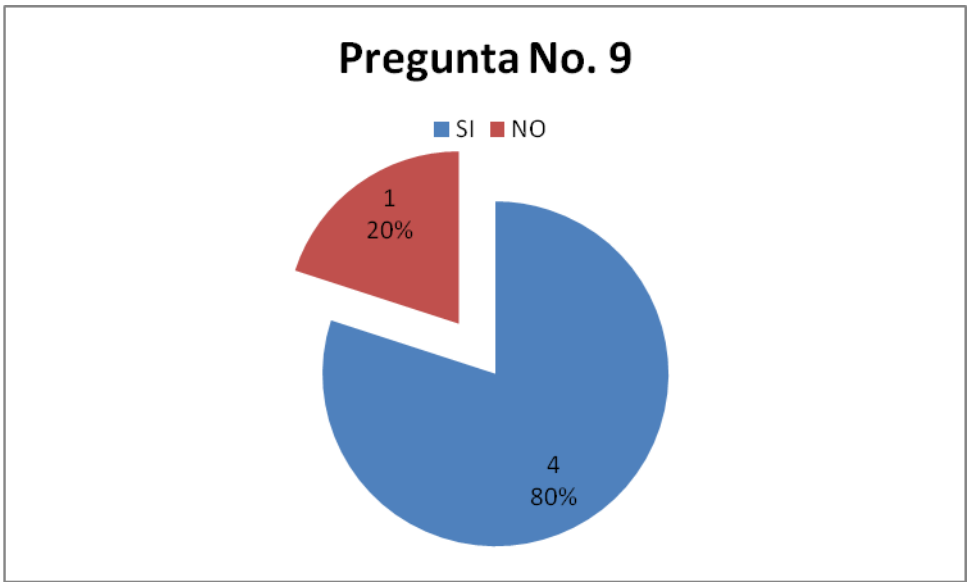
8.- ¿Considera usted que los servicios informáticos prestados actualmente en el Centro Asociado deben ser modernizados?

Representación Gráfica



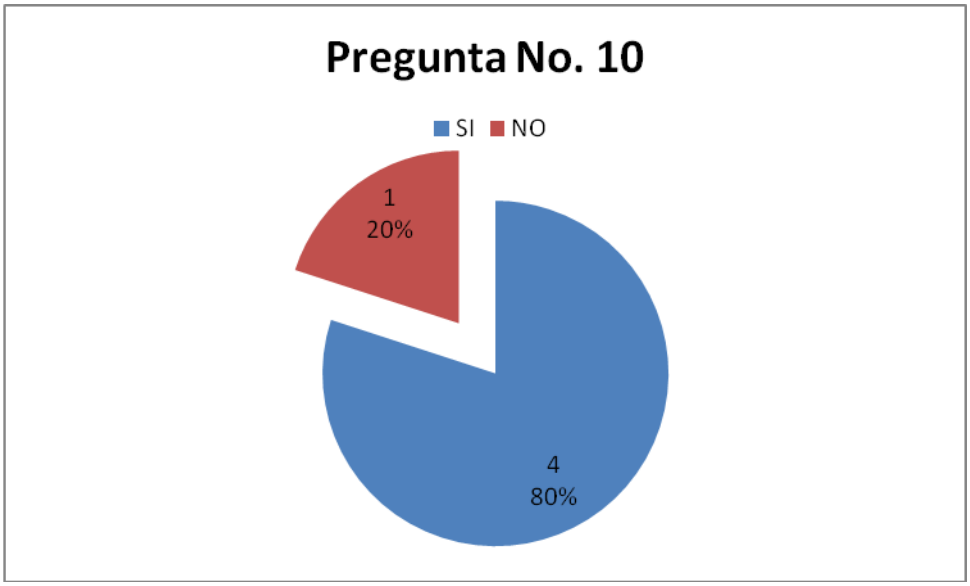
9.- ¿Considera usted que sería beneficioso poder acceder a los servicios informáticos en todo momento y desde cualquier punto del campus universitario del Centro Asociado?

Representación Gráfica



10.- ¿Considera usted que el uso de la tecnología informática y la implantación de una Red Inalámbrica en el Centro Asociado permitirá solucionar las dificultades de conexión y prestación de servicios?

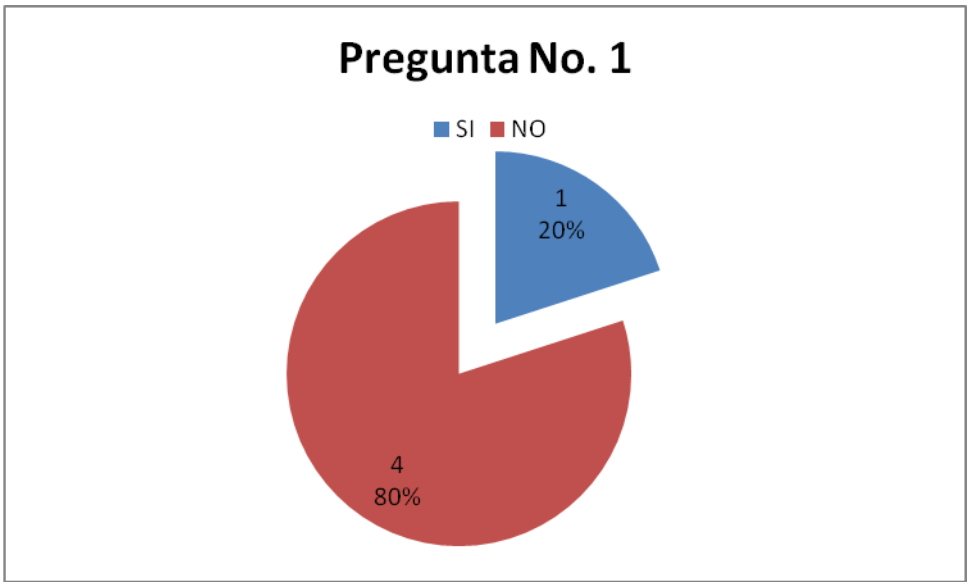
Representación Gráfica



RESULTADOS DE LA ENCUESTA DIRIGIDOS AL PERSONAL ADMINISTRATIVO

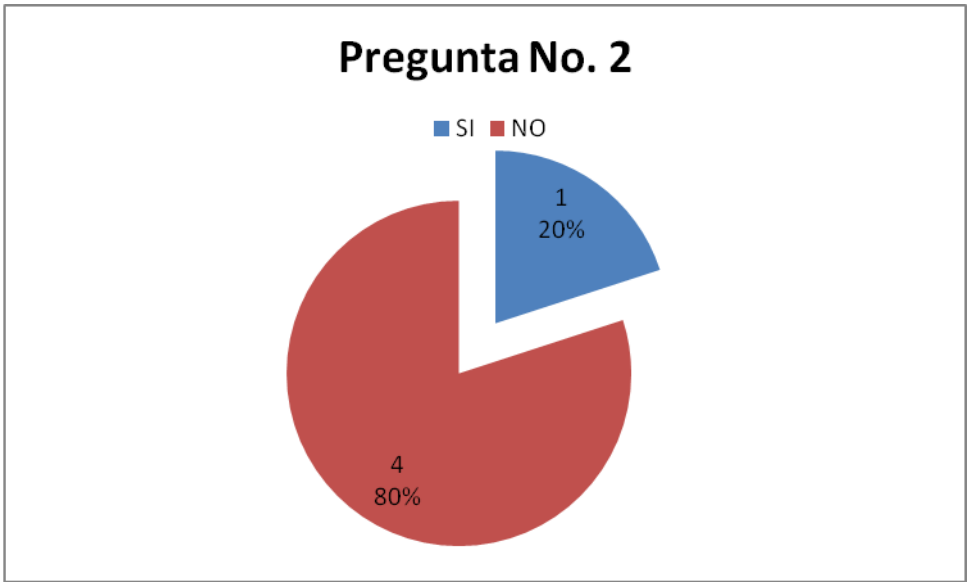
1.- ¿Conoce Ud. Sobre Redes Inalámbricas?

Representación Gráfica



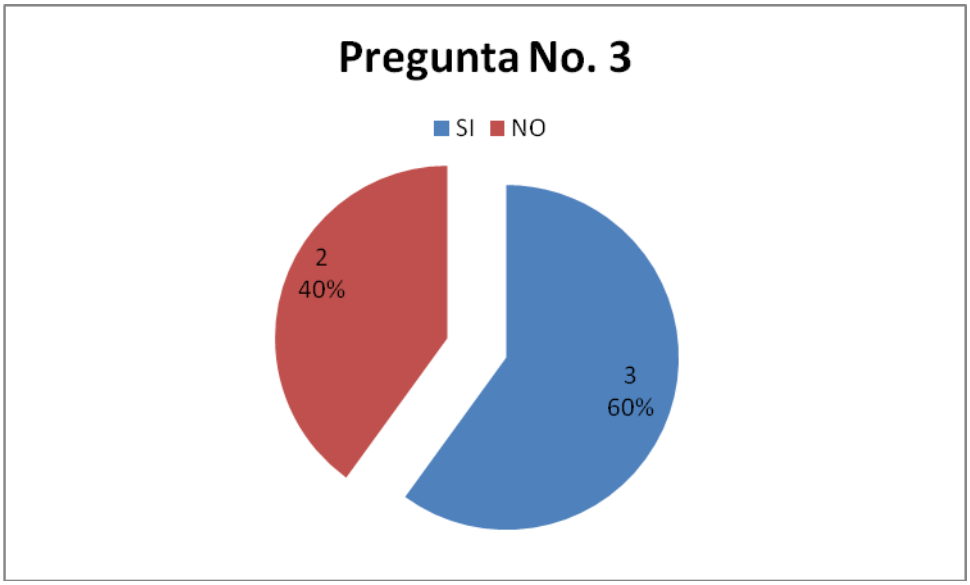
2.- ¿El Centro Asociado ofrece servicios informáticos?

Representación Gráfica



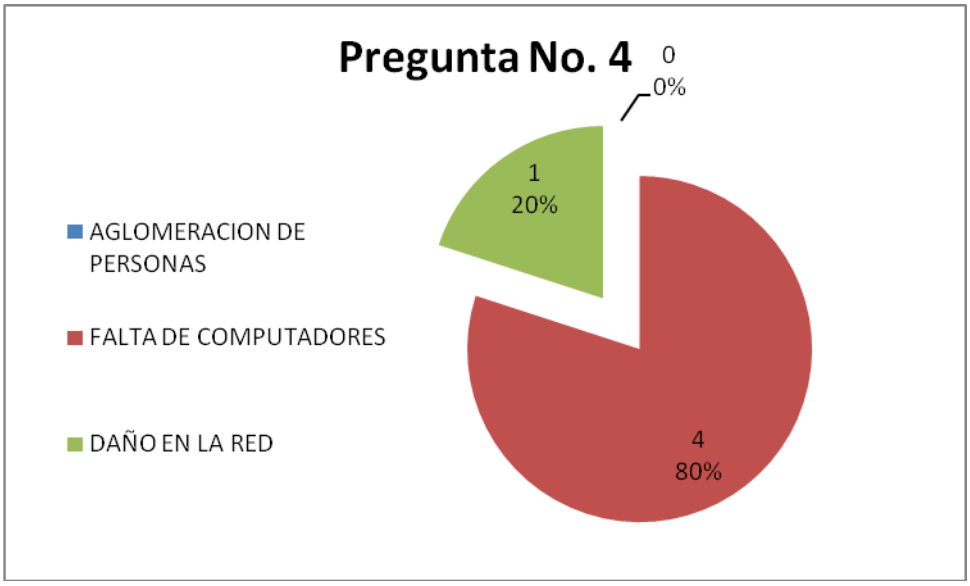
3.- ¿El Centro Asociado ha prestado servicios informáticos hasta el momento eficientes a la comunidad universitaria?

Representación Gráfica



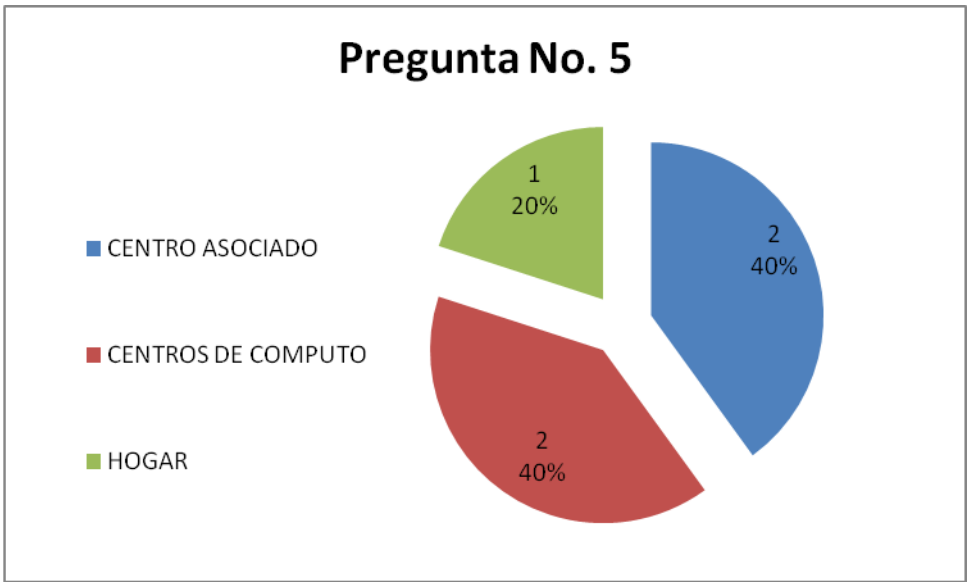
4.- ¿Cuáles son los problemas más importantes que se han presentado al usar el Laboratorio Informático del Centro Asociado?

Representación Gráfica



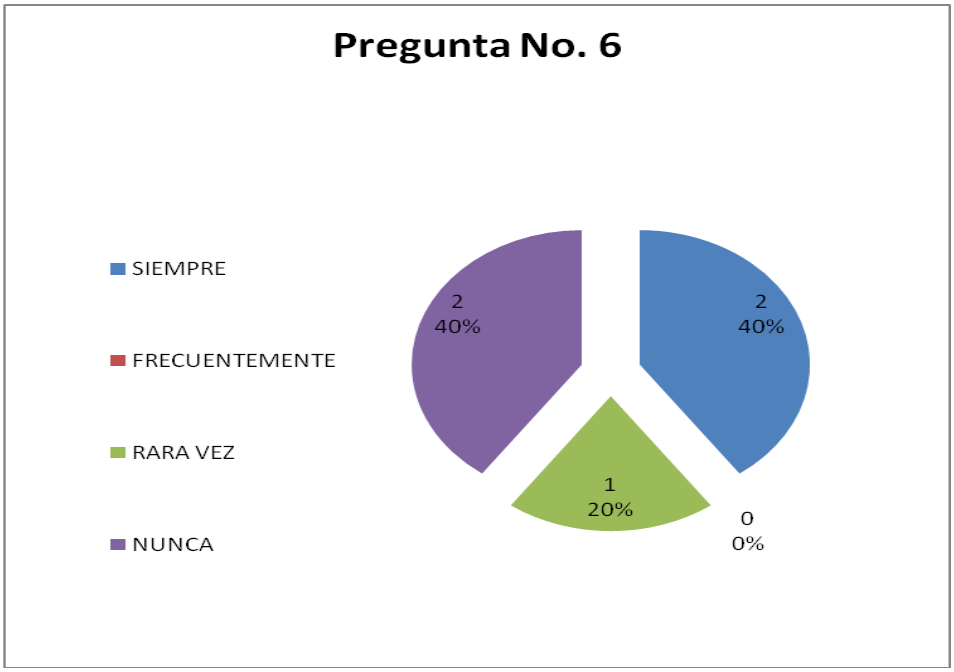
5.- ¿Dónde utiliza actualmente el servicio de Internet?

Representación Gráfica



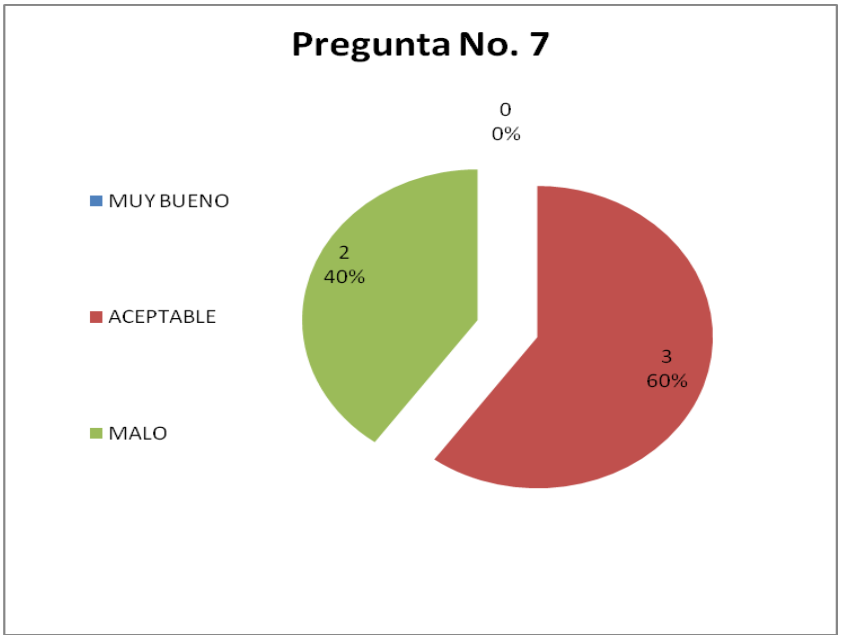
6.- ¿Con qué frecuencia usted utiliza el Centro de Cómputo del Centro Asociado?

Representación Gráfica



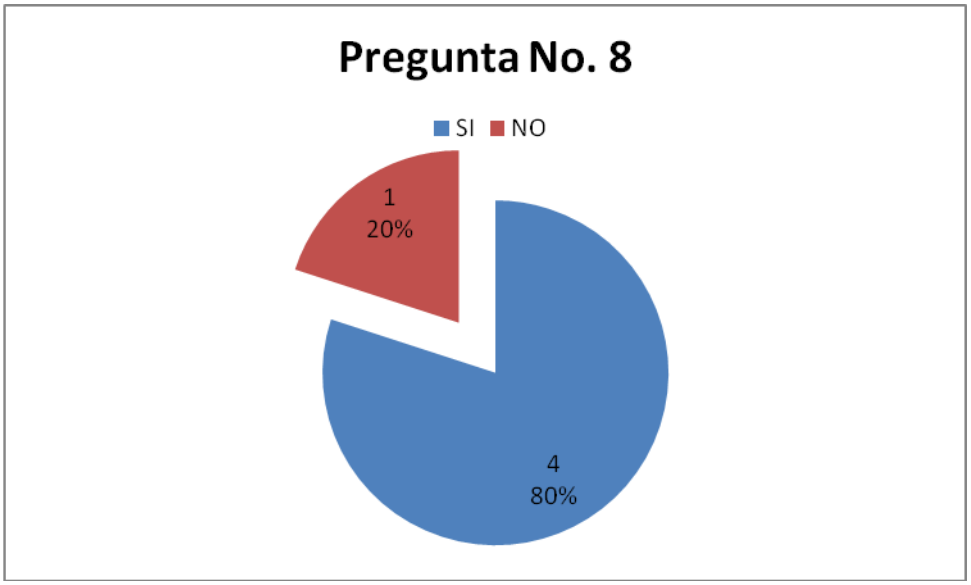
7.- ¿El servicio de Internet en el Centro Asociado para realizar sus actividades cotidianas es?

Representación Gráfica



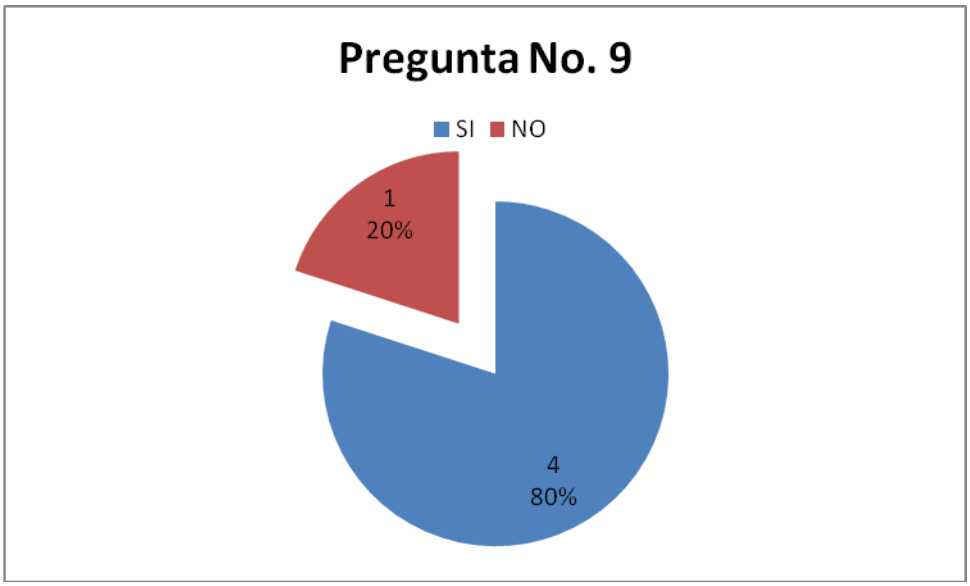
8.- ¿Considera usted que los servicios informáticos prestados actualmente en el Centro Asociado deben ser modernizados?

Representación Gráfica



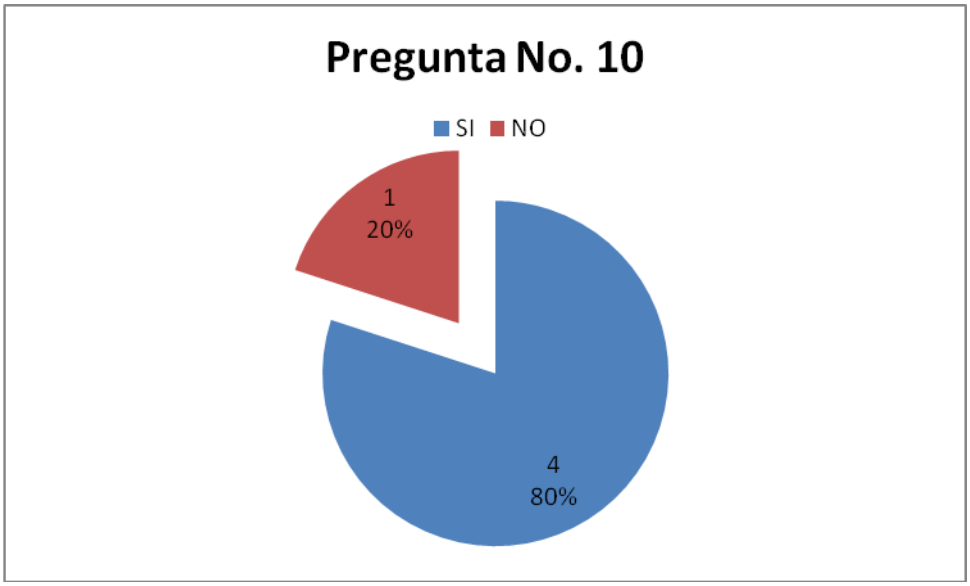
9.- ¿Considera usted que sería beneficioso poder acceder a los servicios informáticos en todo momento y desde cualquier punto del campus universitario del Centro Asociado?

Representación Gráfica



10.- ¿Considera usted que el uso de la tecnología informática y la implantación de una Red Inalámbrica en el Centro Asociado permitirá solucionar las dificultades de conexión y prestación de servicios?

Representación Gráfica



ANEXO 3

FOTOGRAFÍAS DE LA IMPLANTACIÓN


8 12:37 PM


Abercrombie
SONY
8 1:34 PM


8 2:11PM


8 2:11PM


8 3:16 PM


Triunfa
5 8:57 PM


6 11:41 AM


6 11:41 AM

6 11:42 AM

ANEXO 4

CRONOGRAMA