ESCUELA POLITÉCNICA DEL EJÉRCITO
DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA

"DISEÑO IMPLEMENTACIÓN Y ADMINISTRACIÓN DE UNA RED INALÁMBRICA PARA LA GESTIÓN DE SERVICIOS DE TELECOMUNICACIONES DE LA UNIDAD EDUCATIVA LICEO DEL VALLE".

LUISA DANIELA MACAS PALLO
JUAN CARLOS BRITO VALLEJO

SANGOLQUI – ECUADOR

2008

CERTIFICACIÓN

CERTIFICAMOS QUE EL PRESENTE PROYECTO DE GRADO FUE REALIZADO EN SU TOTALIDAD POR LOS SEÑORES JUAN CARLOS BRITO VALLEJO Y LUISA DANIELA MACAS PALLO, BAJO NUESTRA DIRECCIÓN.

…….	**……**
Ing. Carlos Romero	**Ing. Julio Larco**
DIRECTOR	**CODIRECTOR**

Sangolquí, 06 de octubre del 2008

RESUMEN DEL PROYECTO DE GRADO

El presente trabajo contiene toda la documentación correspondiente Diseño Implementación y administración de una red inalámbrica para la gestión de servicios de telecomunicaciones de la Unidad Educativa Liceo del Valle.

Está dividido en 8 capítulos que plasman los conocimientos teóricos, técnicos y prácticos para desarrollar la implementación de una red wireless con servicios de Internet, VoIP y video-vigilancia basada sobre plataforma Linux, lo cual constituye en la actualidad una de las soluciones de mayor relevancia e importancia dentro de la integración del mercado de servicios de red y comunicaciones.

El capítulo 1 detalla una explicación de la situación inicial del Liceo del Valle, un análisis de su infraestructura física y tecnológica y el planteo de la necesidad y su solución.

En el capítulo 2 se explica la plataforma Linux y la implementación del servidor de comunicaciones con todos los servicios como dhcp, dns, mail, web, red, proxy, etc.

El capítulo 3 analiza de manera teórica el entorno wireless y los dispositivos necesarios para montar la red.

El capítulo 4 abarca la tecnología de VoIP y vigilancia IP, estandares, definiciones, características y equipos.

El capítulo 5 detalla las herramientas de software empleadas para el diseño de la red, dimensionamiento de equipos, análisis de interferencia y características que brinden calidad a la WLAN implementada.

El capítulo 6 corresponde a un análisis financiero de costos, inversión y tiempos de recuperación de la inversión.

El capítulo 7 trata netamente de criterios técnicos para el montaje de toda l red y las pruebas de funcionamiento de los equipos.

Y finalmente en el capítulo 8 se enuncian conclusiones y recomendaciones de todo lo anteriormente detallado.

DEDICATORIA

A mis padres Vilma y Carlos, a mi hermana Cristina, y a mi esposa Cristina, dedico este proyecto por ser las personas que me han Apoyado de manera positiva en mi vida.

J.C.B.V

Este proyecto va dedicado a mi familia, mi madre Paulina, mi hermano Francisco, mis tías Sandrita e Isabel y en general a mi familia, a mis amigos, a mi ángel y a Dios

DANY

AGRADECIMIENTO

Agradecemos muy sinceramente a todas las personas quienes hicieron posible la realización de nuestro trabajo, por toda la colaboración y la ayuda desinteresada, que fue un aporte fundamental para la culminación del presente Proyecto de Grado.

A los Ingenieros Carlos Romero y Julio Larco, quienes nos han brindado las herramientas y conocimientos necesarios para orientar nuestro proyecto, por todo el tiempo y predisposición para ayudarnos. Para ellos, nuestro agradecimiento.

A la Ing. Doris Yánez, por habernos facilitado los equipos necesarios para la implementación de la parte práctica del proyecto, además de haber aportado con todos los conocimientos sobre los equipos y su manejo.

Al Ing. Patricio Cevallos, por permitirnos ejecutar nuestro proyecto en su prestigiosa institución, quien nos abrió sus puertas y nos brindó toda su colaboración.

A los Ingenieros Pablo Zurita y Andrés Zurita por parte de Enlace Digital, por habernos apoyado de manera incondicional tanto personal como económicamente, especialmente con la parte física en cuanto a equipos instalados para nuestro proyecto, gracias por su respaldo.

Nuestro más sincero reconocimiento a todas estas personas, a quienes ponemos a consideración este proyecto.

Daniela y Juan Carlos

“Agradezco a Dios, que siempre es mi guía y ejemplo de vida, lo que me ayudado ha seguir adelante hasta la culminación de esta meta.

A mis padres, que han sido mi apoyo y fuerza fundamental en quienes siempre encontrado cariño, confianza y toda la ayuda que he necesitado, les agradezco de manera especial por sus enseñanzas y valores que han fomentado en mi para hacerme alguien de bien, lo que me ha motivado a conseguir mis objetivos.

A toda mi familia, por su preocupación y confianza en mi.

A mi querida esposa, quien con su paciencia y comprensión me ha enseñado lo que significa la constancia y la entrega, en el desarrollo y culminación de todos mis proyectos propuestos, gracias por ser el pilar fundamental de mi vida.

Finalmente, a todos las personas que de una u otra manera han aportado en este proyecto, sinceramente MUCHAS GRACIAS…”

J.C.B.V.

Agradezco a Dios por ser una luz en mi vida que me ayuda a seguir adelante frente a problemas y adversidades de la vida, a mi ángel que desde el cielo me guía, me cuida y me da fuerzas para vivir el día a día. Gracias mamita.

A mi familia en general, a mi madre que ha sido, es y será en mi vida un apoyo incondicional para todos y cada uno de los proyectos en mi vida, su paciencia, dedicación y amor durante toda mi vida. A mi hermano que es mi compañero en casa, a mis tías que siempre han estado pendientes de mí y con sus palabras de aliento han colaborado en los ánimos de seguir adelante y lograr todo lo que ahora tengo en la vida.

A mis amigos que han ayudado a forjar este sueño de tantos años y en especial a quienes con su esfuerzo, cariño, amor y paciencia caminaron junto a mi, los últimos pasos en la realización de este proyecto.

DANY

PRÓLOGO

El presente proyecto ha sido desarrollado con la finalidad de proveer a la institución Educativa Liceo del Valle de una nueva infraestructura tecnológica, la cual constituye un apoyo en la modernización de los procedimientos operativos, de manera que posea un mejor desarrollo y eficiencia

Todo lo aquí expuesto ha sido desarrollado de manera práctica con una aplicación completa de procedimientos de Ingeniería, los cuales están basados en análisis previos para posteriormente realizar la implantación sobre la base de un diseño correctamente concebido.

El documento presente se enfoca de manera especial para quienes se encuentren interesados en la investigación de telecomunicaciones y redes de información, así como también parte de administración de sistemas operativos poco conocidos. Es decir el proyecto va dirigido tanto a la parte de aplicación de teoría en dispositivos ya desarrollados, como en posibles nuevos campos de investigación.

Acerca del contenido aquí expuesto, se ha tratado temas relacionados con redes de datos y telecomunicaciones, basados en la transmisión inalámbrica y cableada; especificaciones de VoIP, servidores de aplicaciones y circuito cerrado de seguridad con el uso de cámaras IP. Los puntos anteriores fueron integrados para converger hacia una solución global para el mejoramiento de la eficiencia y eficacia de los procedimientos desarrollados dentro de la Unidad Educativa Liceo del Valle.

El presente proyecto tiene, en su parte más significativa, el desarrollo de telefonía IP basada en dispositivos mixtos, es decir hemos logrado comunicación entre redes IP y analógicas, así como también entre dispositivos de los tipos antes mencionados. Mediante la programación de varios equipos, presentamos una solución de comunicación IP completamente óptima y de alta calidad y desempeño que ha cumplido con las expectativas de la institución educativa.

Todo el documento se encuentra provisto de texto completamente claro y explicativo, así como también gráficos y tablas que exponen de mejor manera los contenidos aquí presentados.

Finalmente, el desarrollo, diseño e implementación de este proyecto ha colaborado de manera significativa para mejorar los procedimientos operativos de la institución educativa, así como también ha provisto de nuevos conocimientos en los campos de redes y telecomunicaciones. Adicionalmente se ha establecido un desarrollo completo del proyecto considerando aspectos técnicos, financieros y de diseño que de no considerarlos, difícilmente se hubiera concluido con éxito. El principal aporte esta basado en el incentivo a la investigación y desarrollo de nuevas soluciones de ingeniería, aún no conocidas.

CAPÍTULO 1

INTRODUCCIÓN

CAPÍTULO 2

SERVIDOR DE APLICACIONES BAJO LINUX

CAPITULO 3

WIRELESS

CAPITULO 4

VOZ SOBRE IP Y VIDEO –VIGILANCIA

CAPÍTULO 5

DISEÑO

CAPÍTULO 6

ANÁLISIS ECONÓMICO

CAPÍTULO 7

IMPLEMENTACIÓN

CAPÍTULO 8

CONCLUSIONES Y RECOMENDACIONES

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ANEXOS

GLOSARIO DE TÉRMINOS

ACCESS POINT	Un punto de acceso inalámbrico en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.
BIND	*Berkeley Internet Name Daemon*
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FCC	Agencia del gobierno de los Estados Unidos responsable de las regulaciones dentro de las cuales esta la de las comunicaciones interestatales
FQDN	Full Cuallified Domain Name
GNOME	Es un entorno de escritorio para sistemas operativos de tipo Unix bajo tecnología X Window. Forma parte oficial del proyecto GNU
GNU	Proyecto nacido en 1984 para desarrollar un sistema operativo similar a UNIX, pero bajo el concepto de software libre
IEEE	Instituto de Ingenieros Eléctricos Electrónicos
IDE	Integrated Drive Electronics, disco con la electrónica integrada
NFS	Network File System. Sistema de archivos en red
FTP	File Tranfer Protocol. Protocolo de transferencia de archivos

QoS	Quality of Service. Calidad de Servicio que permite asegurar una óptima transferencia de paquetes
RAM	Random Access Memory. Memoria de acceso directo
RHCE	Certificado de Ingeniería de Red Hat
RPM	Red Hat Package Manager Gestionador de paquetes de Red Hat
TCP/IP	Protocolo de Control de Transmisión/Protocolo Internet
TI	Tecnologías de la Información
TGZ	Es la extensión de los ficheros compactados con TAR y luego comprimidos con GZIP
USB	Universal Serial Bus
WEP	Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite
WIRELESS	Transmisión de información a través de un medio no guiado, de manera inalámbrica

CAPÍTULO 1

INTRODUCCIÓN

1.1 ANTECEDENTES

Debido al vertiginoso crecimiento y desarrollo de las tecnologías de red y comunicaciones tanto a nivel mundial como nacional, es cada vez mayor la demanda de alta calidad y variedad en los servicios por parte de los usuarios.

Actualmente la convergencia de los servicios de voz, video y datos, bajo el formato IP, requieren medios de transmisión de alto desempeño que optimicen y a la vez abaraten costos de implementación, operación y mantenimiento.

La tecnología wireless representa una muy opcionada alternativa como medio de transmisión en la actualidad, sustituyendo parte importante del cableado estructurado, presentando además, gran variedad de dispositivos multifuncionales de red con un buen desempeño y alta escalabilidad.

Para contar con una red óptima es importante mencionar la evolución de las redes wireless, las cuales anteriormente no contaban con mucha demanda debido a que no poseían un funcionamiento adecuado y constantemente se presentaban problemas de interconectividad entre equipos, siendo además una barrera importante los obstáculos presentes en el enlace.

Ahora se cuenta con nuevas tecnologías como antenas de mayor irradiación de señal que logran cada vez mayor alcance a pesar de la existencia de distancias significativas

Hablando de telefonía, la comunicación vía Internet actualmente es el mayor medio a nivel mundial, se han desarrollado diferentes tecnologías para aprovechar este servicio, entre ellas la telefonía de Voz sobre IP, un medio en pleno desarrollo que brinda calidad a

menor costo, especialmente para llamadas a nivel internacional, por lo que se considera oportuno implementar este servicio en el proyecto.

Las instituciones educativas, hoy por hoy cuentan con sistemas inteligentes de alta tecnología en sus inmediaciones y es obvio pensar que, en lo que se refiere al ámbito de las comunicaciones no podría ser de otra manera. El presente plan va a ser implementado en la unidad educativa Liceo del Valle con usuarios que tienen la necesidad de un servicio confiable y seguro de Internet de banda ancha, correo electrónico, VoIP y video vigilancia para cada una de sus dependencias.

En cuanto compete a seguridad es un tema en boga en estos días, cada vez la mayoría de instalaciones de cualquier índole, requieren este servicio y una buena opción es la video-vigilancia acoplada a un formato IP.

Es por ello, que el conjunto de dispositivos y servicios mencionados anteriormente cuenta con una alta demanda en el mercado actual y por ende constituye una solución tecnológica que brindará servicios innovadores para el Liceo del Valle.

1.2 SITUACIÓN ACTUAL: LOGÍSTICA E INFRAESTRUCTURA

Físicamente, el Liceo del Valle se encuentra ubicado en Sangolquí vía a Pifo en el Km. 1

Las instalaciones del Liceo del Valle se hallan asentadas sobre un área distribuida en parte administrativa, primaria, secundaria, uso múltiple y preescolar.

El terreno sobre el cual se encuentra asentado es irregular, ubicándose en la parte más alta del mismo el edificio administrativo, continuando hacia abajo con primaria. El edificio de secundaria es el más extenso en construcción y se encuentra a la misma altura de terreno que la parte del ambiente de uso múltiple.

Por último, preescolar funciona en el lugar más bajo del terreno y más alejado del resto de edificios.

1.2.1 Infraestructura Física

En general, el área construida por la Unidad Educativa Liceo del Valle se compone de cinco edificios principales, parqueaderos, vías de acceso y un bar. La edificación en donde funciona la parte administrativa cuenta con dos plantas, mientras que el resto de edificios únicamente funcionan en una planta.

Figura. 1.1. Vista frontal de secundaria

A continuación se muestra el plano de implantación general de las instalaciones del Liceo del Valle, en el cual se muestran claramente las edificaciones compuestas por Administración, aulas primaria, aulas secundaria, aulas preescolar, uso múltiple y artes:

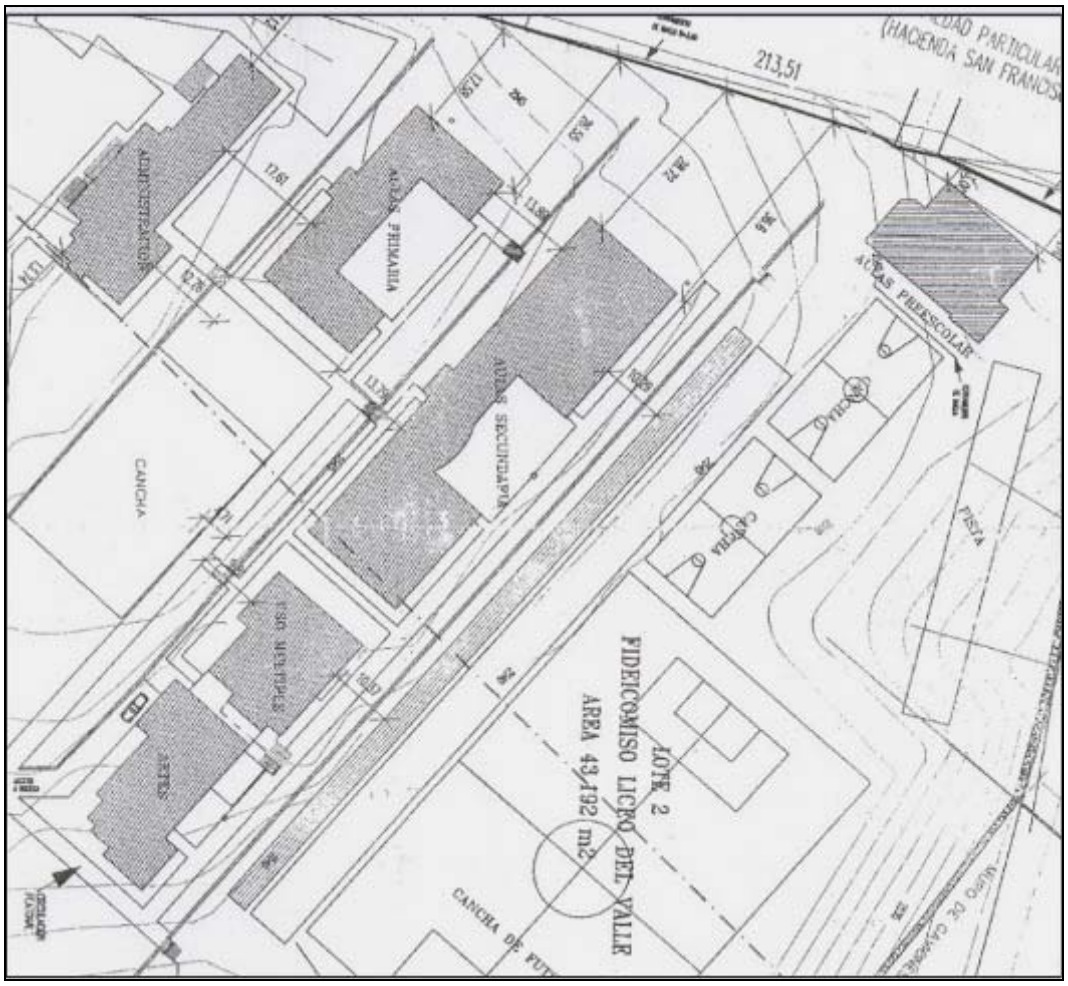


Figura. 1.2. Plano general de la Unidad Educativa Liceo del Valle

A continuación se indica la fachada frontal del edificio de administración:

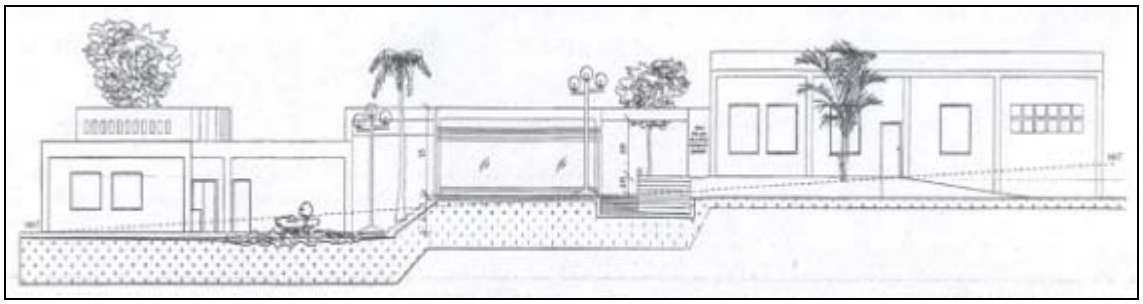


Figura. 1.3. Administración vista frontal

El edificio de administración se encuentra ubicado en la parte más alta del terreno sobre el cual se asientan las instalaciones del Liceo del Valle.

Dicha edificación cuenta con dos plantas. En la superior funcionan las oficinas de administración junto con los laboratorios de computación. La segunda planta cuenta con 10

oficinas en donde se desempeñan las funciones de rectorado, administración, sistemas, secretariado y contabilidad. Adicionalmente existen 2 aulas de computación, las cuales se encuentran provistas por computadores para uso de los estudiantes.

En la parte inferior se encuentran los laboratorios de Física, Química y la biblioteca.

La única conectividad de red con la que cuenta este edificio es la que se encuentra en el área de contabilidad, las computadoras aquí ubicadas comparten los datos de un sistema contable.

La siguiente imagen muestra la fachada frontal de la edificación en donde funcionan las aulas de primaria.

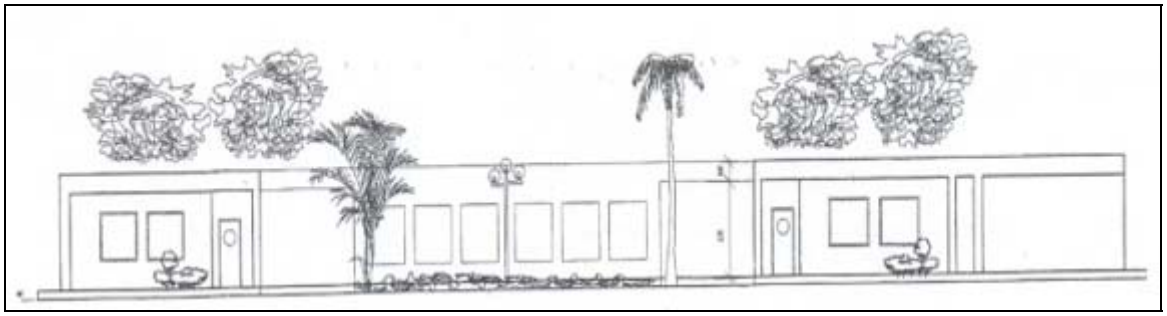


Figura. 1.4. Vista frontal primaria

Dicho edificio cuenta con una sola planta, el cual posee aulas para proveer instrucción primaria a los estudiantes. Adicionalmente tiene 2 oficinas dedicadas al área de inglés y la inspección de primaria.

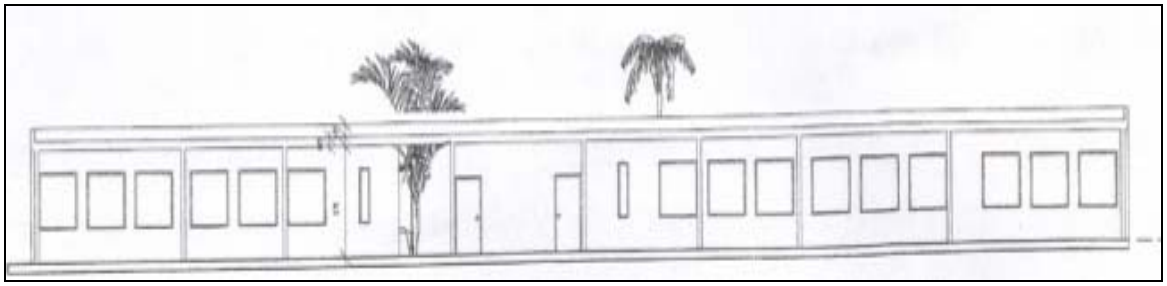


Figura. 1.5. Vista lateral Primaria

En la imagen anterior se muestra la fachada frontal de la edificación en donde funcionan las aulas de instrucción secundaria. Al igual que primaria, dicha edificación funciona en una sola planta.

También posee ambientes adicionales tales como oficinas administrativas, sala de profesores y aulas de dibujo, pintura e inglés.

Tanto primaria como secundaria no poseen ningún tipo de conectividad de red ni servicio de Internet.

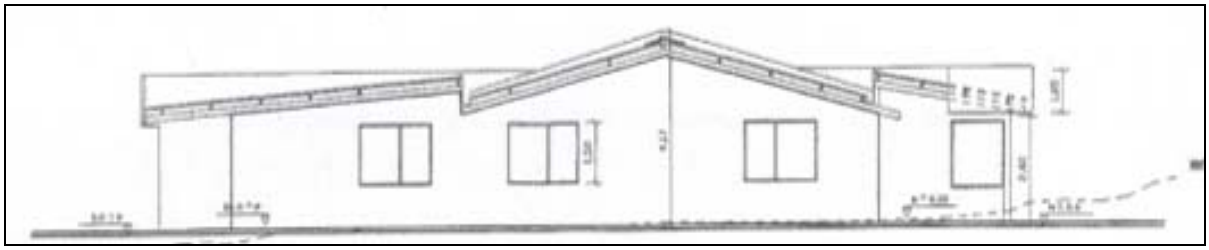


Figura. 1.6. Vista posterior Primaria

La imagen anterior corresponde a la edificación en la cual funcionan las instalaciones de las aulas de preescolar. Al igual que en los casos anteriores, también cuenta con oficina de inspección y sala de profesores.

El ambiente de Uso múltiple, el cual se muestra en el siguiente gráfico, funciona junto al bar y a las aulas de artes. Es usado para presentaciones programadas por la institución educativa.

En una oficina adicional, y anexa a uso múltiple, se encuentra una pequeña oficina en la cual funciona el departamento de Educación Física

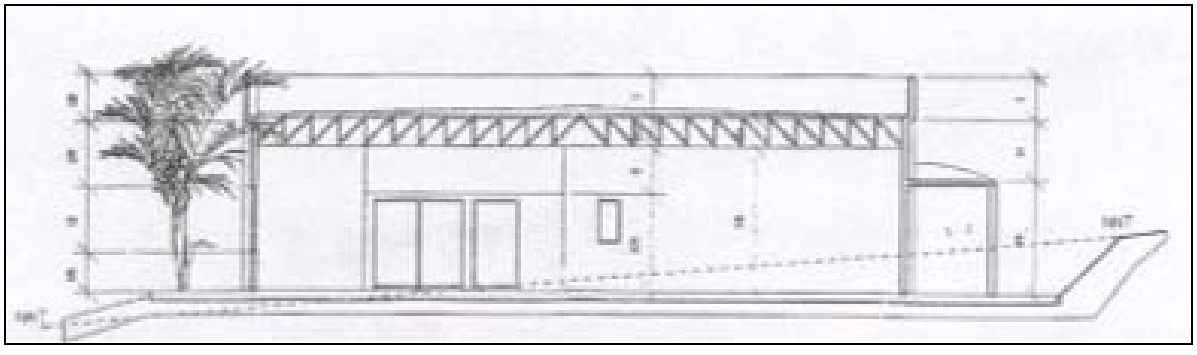


Figura. 1.7. Vista Frontal Aula Múltiple

1.2.2 Infraestructura Tecnológica

Actualmente las instalaciones del Liceo del Valle cuentan con infraestructura tecnológica que se encuentra basada únicamente en el uso de computadores, los cuales no poseen conectividad de red entre ellos. Por otra parte tampoco cuentan con servicio de Internet ni conectividad inalámbrica.

Los siguientes cuadros muestran un resumen de los computadores que posee el Liceo del Valle. En el primero se indica el sistema operativo de los equipos junto con su ubicación y tipo. En el segundo se detalla el hardware que contiene cada uno de ellos:

Tabla. 1.1. Sistema operativo de PC's existentes en liceo

Orden	Ubicación	Sistema Operativo	Tipo	Departamento
1	Aula multiple	Windows XP	PC escritorio	Educación Física
2	Secundaria Derecha	Windows XP	PC escritorio	Orientación Vocacional
3	Secundaria Izquierda	Windows XP	PC escritorio	Sala de profesores secundaria
4	Secundaria Izquierda	Windows XP	PC escritorio	Sala de profesores secundaria
5	Secundaria Izquierda	Windows XP	PC escritorio	Inspección general
6	Secundaria Izquierda	Windows XP	PC escritorio	Inglés
7	Secundaria Izquierda	Windows XP	PC escritorio	Inglés
8	Preescolar	Windows XP	PC escritorio	Preescolar
9	Primaria	Windows XP	PC escritorio	Secretaría Primaria
10	Administración	Windows XP	Laptop	Gerencia
11	Administración	Windows XP	Laptop	Vicerrectorado
12	Administración	Windows XP	Laptop	Sistemas
13	Administración	Windows XP	PC escritorio	Rectorado

14	Administración	Windows XP	PC escritorio	Vicerrectorado
15	Administración	Windows XP	PC escritorio	Tesorería
16	Administración	Windows XP	PC escritorio	Contabilidad
17	Administración	Windows XP	PC escritorio	Información
18	Administración	Windows XP	PC escritorio	Secretaría Secundaria
19	Administración	Windows XP	PC escritorio	Sistemas
20	Administración	Windows XP	PC escritorio	Sistemas
21 – 32	Laboratorio 1	Windows XP	PC escritorio	Sistemas
33 – 45	Laboratorio 2	Windows XP	PC escritorio	Sistemas
46	Administración	Windows XP	PC escritorio	Biblioteca
47	Administración	Windows XP	PC escritorio	Almacén
48	Administración	Windows XP	PC escritorio	Biblioteca
49	Administración	Linux CentOS 4.2	PC escritorio	Sistemas

Tabla. 1.2. Hardware en PC's existentes en liceo

Orden	Ubicación	Disco Duro	Procesador	Memoria RAM	Tipo
1	Aula múltiple	40 GB	PIII 800 MHz	128 MB	Clon
2	Secundaria Derecha	40 GB	PIII 800 MHz	128 MB	Clon
3	Secundaria Izquierda	40 GB	PIII 800 MHz	128 MB	Clon
4	Secundaria Izquierda	40 GB	PIII 800 MHz	128 MB	Clon
5	Secundaria Izquierda	40 GB	PIII 800 MHz	128 MB	Clon
6	Secundaria Izquierda	40 GB	PIII 800 MHz	128 MB	Clon
7	Secundaria Izquierda	40 GB	PIII 800 MHz	128 MB	Clon
8	Preescolar	40 GB	PIII 800 MHz	128 MB	Clon
9	Primaria	40 GB	PIII 800 MHz	128 MB	Clon
10	Administración	40 GB	PIV 1.6 GHz	512 MB	Clon
11	Administración	100 GB	PIV 1.6 GHz	1 GB	Clon
12	Administración	100 GB	PIV 1.6 GHz	1 GB	Clon
13	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon

14	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
15	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
16	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Compaq
17	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
18	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
19	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
20	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
21 - 32	Laboratorio 1	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
33 - 44	Laboratorio 2	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
45	Laboratorio 2	40 GB	PIV Celeron 2.4 GHz	512 MB	Compaq
46	Administración	40 GB	PIII 800 MHz	128 MB	Clon
47	Administración	40 GB	PIII 800 MHz	128 MB	Clon
48	Administración	40 GB	PIV Celeron 2.4 GHz	512 MB	Clon
49	Administración	80 GB	PIV 2.8 GHz	512 MB	Clon

1.3 PROYECTO DE RED CONVERGENTE DE SERVICIOS

En la sección 1.2 ha quedado reflejado que la institución educativa cuenta con un sistema incompleto de infraestructura tecnológica. Sin embargo no debe entenderse que el Liceo del Valle se ha despreocupado en su equipamiento, puesto que cuenta con un importante número de equipos de computación, los cuales se presentan como computadores de mediana y alta tecnología.

El Liceo del Valle se ha preocupado por brindar servicios de calidad a sus estudiantes, administrativos y docentes, por lo cual ha invertido en la construcción de un área para cada ambiente de instrucción, tales como preescolar, primaria, secundaria y administración.

La institución educativa ha establecido una política institucional de prioridades en las cuales ha incluido la implementación de soluciones tecnológicas conformando una red convergente de servicios.

La necesidad de brindar fuentes de consulta actualizadas tanto a estudiantes como a docentes mediante el uso de Internet, ha sido la principal preocupación de la institución educativa a fin de brindar una instrucción de calidad en todas sus áreas. Junto a este servicio se incluye la implementación de seguridad mediante el uso de cámaras y tecnología de voz sobre IP.

Con todos estos servicios, el Liceo del Valle establecerá un sistema de alta calidad y estará a la vanguardia en cuanto a servicios tecnológicos de redes y telecomunicaciones se refiere.

1.3.1 Necesidad específica

La buena gestión del Liceo del Valle, su crecimiento como institución educativa, la incorporación de nuevos laboratorios, así como la inclusión de distintas actividades, han aumentado la cantidad de trabajo tanto en su parte docente como administrativa.

El plan estratégico del Liceo del Valle pretende brindar servicios de calidad como institución educativa tanto en el aspecto de la enseñanza así como en la implementación de soluciones tecnológicas para de esta manera mejorar los métodos de aprendizaje de sus estudiantes así como también facilitar la labor de enseñanza del personal docente.

Por otra parte, la institución educativa pretende mejorar los servicios de comunicaciones e implementar soluciones para navegación en Internet y seguridad con video vigilancia.

Queda, entonces, bien identificada la necesidad del Liceo del Valle, estando establecida en tres parámetros claramente definidos: Internet, video vigilancia y comunicaciones.

En la actualidad la parte administrativa utiliza un tipo de conexión dial-up para tener acceso a navegación por Internet constituyéndose en un método obsoleto y que no brinda las características y ventajas necesarias para un adecuado uso de las aplicaciones de la Web.

Cada vez se necesitan mayores recursos tecnológicos para poseer servicios de calidad que nos permitan acceder a diferentes fuentes de conocimiento, en el caso de la navegación por Internet, así como también en para la parte de telecomunicaciones y video vigilancia.

Todas las razones anteriormente expuestas, han hecho que la institución educativa Liceo del Valle decida implementar soluciones tecnológicas para el mejoramiento de su calidad de enseñanza así como también para mejorar el desempeño de su personal docente y administrativo para de esta manera brindar servicios de calidad y excelencia en el campo educativo.

1.3.2 Solución

La unidad educativa Liceo del Valle ha decidido implementar los servicios de Internet, Video-vigilancia y Voz sobre IP para las instalaciones de la parte administrativa, primaria, secundaria y preescolar.

Para esto ha decidido utilizar los servicios de la empresa Enlace Digital, la cual se encargará del diseño e implementación del proyecto.

Como primer punto se instalará un sistema de cableado estructurado en las oficinas administrativas, el cual cumplirá con todas las normas establecidas en este aspecto y además contará con las respectivas certificaciones.

El plan de trabajo continúa con la contratación de un proveedor de servicios de Internet, la cual contará con la asesoría de la empresa responsable del desarrollo del proyecto. Como actividad paralela, se efectuará la instalación y configuración de un

servidor de Internet, el cual poseerá adicionales tales como seguridad informática, correo electrónico, sistema de nombres de dominio, entre otros.

Continuando con la solución propuesta, se implementará un sistema para acceso inalámbrico mediante el cual los computadores ubicados en las inmediaciones de la institución educativa tendrán acceso al servicio de Internet.

Adicionalmente se colocará un sistema de cámaras de seguridad IP en puntos estratégicos de acuerdo a criterio de los administradores del Liceo del Valle. Dichas cámaras serán inalámbricas y aprovecharán la ventaja de poseer el sistema de conectividad gíreles antes mencionado.

La seguridad mediante las cámaras estará basada en grabaciones de tipo programado o por movimiento, según los requerimientos que se establezcan.

Como punto final se implementará un sistema de conectividad en telecomunicaciones utilizando una nueva tecnología, la de Voz sobre IP. Esto tendrá un funcionamiento utilizando teléfonos tipo IP con central telefónica y una puerta de salida para las comunicaciones tanto a nivel nacional como internacional.

Todos estos sistemas implementados funcionarán como una solución convergente que implementará redes y telecomunicaciones brindando de esta manera servicios que contarán con tecnología de punta y facilitarán la labor de docentes y administrativos y paralelamente proporcionará un nivel de aprendizaje superior a los estudiantes de tan prestigiosa institución educativa

CAPÍTULO 2

SERVIDOR DE APLICACIONES BAJO LINUX

2.1 GENERALIDADES DE LINUX

2.1.1 Definición e Importancia

Definición

Llamamos sistema operativo al administrador de todos los recursos disponibles de una computadora. Estos recursos pueden ser: el disco duro, la impresora, el monitor. Incluso la memoria es un recurso que es preciso administrar Linux es un sistema operativo; robusto, estable, multiusuario, multitarea, multiplataforma y con gran capacidad para gestión de redes diseñado por miles de programadores y usuarios expertos de todo el mundo. Al tener disponible el código abierto a cualquier modificación, son los programadores los que van adaptando el sistema a los tiempos y a las necesidades de cada momento. Por ello se define como un software libre. El fundador de dicho sistema es Linus Torvalds, y el código libre está regido por la licencia GNU[1].

Dos características muy peculiares lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente. El sistema lo forman el núcleo del sistema (kernel) mas un gran numero de programas / librerías que hacen posible su utilización.

El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de Linus Torvalds, la persona de la que partió la idea de este proyecto, a principios de la década de los noventa. Día a día, mas y mas programas / aplicaciones están disponibles para este

[1] *GNU (*Proyecto nacido en 1984 para desarrollar un sistema operativo similar a UNIX, pero bajo el concepto de software libre*)*

sistema, y la calidad de los mismos aumenta de versión a versión. La gran mayoría de los mismos vienen acompañados del código fuente y se distribuyen gratuitamente bajo los términos de licencia de la GNU Public License. En los últimos tiempos, ciertas casas de software comercial han empezado a distribuir sus productos para Linux y la presencia del mismo en empresas aumenta rápidamente por la excelente relación calidad-precio que se consigue con Linux.

Pero no sólo el sistema operativo Linux ofrece su código a los programadores, muchos software complementarios son también de libre distribución, por lo que en Internet podemos encontrar multitud de programas gratuitos, y que permiten a sus usuarios y programadores llevar a cabo todas las mejoras posibles en todo momento.

Importancia

El sistema operativo Linux es muy importante debido a sus múltiples aplicaciones y a que es de libre distribución. Además que es una excelente alternativa para reactivar equipos que de otra manera sólo serían inservibles.

Una característica muy peculiar hace la diferencia del resto de los sistemas que se puede encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo.

La cantidad de servidores en Internet operados por sistemas Linux y Apache (más de 60% de los servidores en Internet operan con Linux, según expertos), nos dan una idea de lo que se puede lograr con un software gratuito. De hecho, muchas empresas tienen algún servidor Linux para generar una intranet, un servidor de archivos o impresoras.

Algunas de las características que hacen que Linux sea tan interesante son estas:

- Multitarea
- Multiusuario
- Multiprocesador
- Multiplataforma
- Consolas virtuales múltiples

- Soporte para varios sistemas de archivo comunes
- TCP/IP[2], incluyendo ftp, telnet, NFS[3], etc.
- Diversos protocolos de red incluidos en el kernel: TCP, IPv4, IPv6, AX.25, X.25, IPX, DDP, Netrom, etc.

Se tiene también acceso al código fuente, esto nos permite hacer los cambios que se puedan requerir en el sistema (como crear aplicaciones específicas, mejorar algún problema en Linux etc.) lo que no sucede con otros sistemas operativos.

2.1.2. Historia

Linux hace su aparición a principios de la década de los noventa, alrededor del año 1991 y por aquel entonces un estudiante de informática de la Universidad de Helsinki, llamado Linus Torvalds empezó (como una afición y sin poderse imaginar a lo que llegaría este proyecto) a programar las primeras líneas de código de este sistema operativo llamado LINUX, un Sistema Operativo tipo Minix para su 386. (Linus originariamente quiso ponerle "Freax" a su proyecto, pero el nombre que prosperó fue el que hoy se conoce).

El sistema ha sido diseñado y programado por multitud de programadores alrededor del mundo. El núcleo del sistema sigue en continuo desarrollo bajo la coordinación de Linus Torvalds.

En los últimos tiempos, ciertas casas de software comercial han empezado a distribuir sus productos para Linux y la presencia del mismo en empresas aumenta rápidamente por la excelente relación calidad-precio que se consigue con Linux

La primera versión oficial, la 1.0, apareció en marzo de 1994; soportaba sólo máquinas i386 con un único procesador. Exactamente un año después, apareció Linux 1.2 (marzo de 1995) y fue la primera versión con soporte para distintas plataformas (Alpha, Sparc y Mips), pero todavía modelos de un solo procesador. Linux 2.0, aparecido en junio de 1996, no sólo soportaba nuevas arquitecturas; también introdujo a Linux en el mundo de máquinas multiprocesador (SMP: *Symmetrical Multi-Processing*, o "Multi-Proceso Simétrico"). Tras 2.0, las revisiones importantes han ido tardando más en aparecer (Linux

[2] *TCP/IP (*Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo Internet*)*
[3] *NFS (*Network File System*)*

2.2 en enero de 1999 y 2.4 en enero de 2001), y con cada nueva entrega se ha ampliado el rango de hardware al igual que la escalabilidad. (Linux 2.4 también fue notable al acercarse al escritorio, con soporte en el kernel para ISA Plug-and-Play, USB, PC Card y otras novedades.) Linux 2.6, finalizada el 17/12/03, no sólo trae ampliaciones por ese lado: también será un salto importante al mejorar el soporte tanto para sistemas mucho más grandes como para dispositivos más pequeños (PDAs y similares).

2.1.3. Principales distribuciones: ventajas y desventajas de cada una de ellas

Una distribución Linux, o distribución GNU/Linux (abreviada con frecuencia distro) es un conjunto de aplicaciones reunidas por un grupo, empresa o persona para permitir instalar fácilmente un sistema Linux (también llamado GNU/Linux). En general, se destacan por las herramientas para configuración y sistemas de paquetes de software a instalar.

Existen numerosas distribuciones Linux. Cada una de ellas puede incluir cualquier número de software adicional (libre o no), como algunos que facilitan la instalación del sistema y una enorme variedad de aplicaciones, entre ellos, entornos gráficos, suites ofimáticas, servidores Web, servidores de correo, servidores FTP[4], etcétera.

La base de cada distribución incluye el núcleo Linux, con las bibliotecas y herramientas del proyecto GNU y de muchos otros proyectos/grupos de software, como BSD.

Usualmente se utiliza la plataforma Xfree86 o la Xorg para sostener interfaces gráficas Entre las principales distribuciones Linux y sus características, tenemos:

DISTRIBUCION RED HAT ENTERPRISE

Esta es una distribución que tiene muy buena calidad, contenidos y soporte a los usuarios por parte de la empresa que la distribuye. Es necesario el pago de una licencia de soporte. Enfocada a empresas.

Para muchos el nombre de Red Hat equivale a Linux, ya que probablemente se trata de la compañía de Linux más popular del mundo. Entre sus principales características están

[4] *FTP (File Transfer Protocol)*

su curiosa mezcla de conservadurismo y paquetes punteros mezclados sobre muchas aplicaciones desarrolladas en casa.

Actualmente Red Hat ha dividido el negocio en dos áreas distintas, por una parte promociona el proyecto Fedora para usuarios finales, el cual saca tres versiones al año, manteniendo los paquetes de Red Hat para usuarios corporativos, que se mantienen más tiempo, y garantizan su estabilidad.

Red Hat Linux se ha convertido en la distribución Linux dominante en servidores en todo el mundo. Otra de las razones del éxito de Red Hat es la gran variedad de servicios populares que ofrece la compañía. Los paquetes de software son fácilmente actualizables usando la Red Hat Network, un repositorio oficial de software e información. Una larga lista de servicios de soporte son accesibles en la compañía y, aunque no siempre baratos, tienes virtualmente asegurado un excelente soporte de personal altamente cualificado. La compañía ha desarrollado incluso un programa de certificación para popularizar su distribución, el RHCE (Certificado de Ingeniería de Red Hat), academias y centros examinadores están disponibles en casi todas partes del mundo.

Todos estos factores han contribuido a que Red Hat sea una marca reconocida en el mundo de la industria de las TI[5].

- Pros: Ampliamente usada, excelente soporte de la comunidad, muchas innovaciones.
- Contras: Menor soporte para la versión gratuita (fedora), soporte multimedia pobre, requiere licenciamiento pagado.
- Sistema de paquetes: RPM
- Descarga Gratuita: Si

DISTRIBUCION FEDORA

Esta es una distribución patrocinada por RedHat y soportada por la comunidad. Fácil de instalar.

[5] *TI (Tecnologías de la Información)*

El objetivo del proyecto Fedora es conseguir un sistema operativo de propósito general y basado exclusivamente en software libre con el apoyo de la comunidad Linux. Los ingenieros de Red Hat continúan participando en la construcción y desarrollo de este proyecto e invitan y fomentan la participación de miembros de la comunidad Linux.

Originalmente, Red Hat Linux fue desarrollado exclusivamente dentro de Red Hat, con la sola realimentación de informes de usuarios que recuperaban fallos y contribuciones a los paquetes de software incluidos; y no contribuciones a la distribución como tal. Esto cambió dando origen al Proyecto Fedora que está orientado a la comunidad de usuarios y así mismo, sirve de base para que Red Hat Enterprise Linux se desarrolle con más efectividad y adopte las nuevas características que se añaden en el Proyecto Fedora.

- Pros: 100% libre, bastante actualizada, instalación de software sencilla usando paquetes rpm.
- Contras: incluye solo las partes mas básicas del sistema operativo
- Sistema de paquetes: RPM[6]
- Descarga gratuita: Si

DISTRIBUCION DEBIAN

Otra distribución con muy buena calidad. El proceso de instalación es quizás un poco mas complicado, pero sin mayores problemas. Gran estabilidad antes que últimos avances.

Esta distribución es posiblemente la más estable y confiable, aunque no la más actualizada. Mientras que la rama estable es perfecta para servidores con funciones críticas, muchos usuarios prefieren usar las ramas de pruebas o inestable, más actualizadas, en sus ordenadores personales. Debian es también famosa por su reputación de ser difícil de instalar, a menos que el usuario tenga un profundo conocimiento del hardware de la computadora. Compensando este fallo está "apt-get" un instalador de paquetes Debian.

- Pros: 100% libre, bien probada, bastante actualizada, instalación de software sencillísima usando apt-get.

[6] *RPM (*Red Hat Package Manager Gestionador de paquetes de Red Hat*)*

- Contras: No tiene tantos paquetes como otras distribuciones.
- Sistema de paquetes: DEB
- Descarga gratuita: Si

DISTRIBUCION S.U.S.E

SuSE es otra compañía orientada a los escritorios, aunque variedad de otros productos para empresas están disponibles. La distribución ha recibido buenas críticas por su instalador y la herramienta de configuración YaST, desarrollada por los desarrolladores de la propia SuSE. La documentación que viene con las versiones comerciales, ha sido repetidas veces evaluada como la más completa, útil y usable con diferencia a la de sus competidores. SuSE Linux 7.3 recibió el premio "Producto del año 2001" que entrega el Linux Journal. La distribución tiene un gran porcentaje de mercado en Europa y América del norte, pero no se vende en Asia y otras partes del mundo.

Novell ha comprado a esta compañía ha seguido la misma estrategia que redhat, dejando SuSE para SOHO (Small Office, Home Office, en español, pequeñas oficinas y usuarios domésticos)

- Pros: Atención profesional en cada detalle, herramienta de configuración de fácil uso (YaST), posibilidad de integrar con el directorio activo de Novell.
- Contras: Solo disponible en algunas partes del mundo en las tiendas de software o mediante instalación FTP, incluye componentes propietarios, que no permiten su redistribución.
- Sistema de paquetes: RPM
- Descarga gratuita: SuSE no proporciona imágenes ISO para descarga, no obstante la versión Profesional de su distribución es accesible para la instalación FTP normalmente 1 o 2 meses más tarde de la versión oficial. La instalación mediante FTP no es difícil, pero requiere una buena conexión.

DISTRIBUCION SLACKWARE

Esta distribución es de las primeras que existió. Tuvo un periodo en el cual no se actualizo muy a menudo, pero eso es historia. Es raro encontrar usuarios de los que empezaron en el mundo Linux

hace tiempo, que no hayan tenido esta distribución instalada en su ordenador en algún momento.

Slackware Linux es la distribución más antigua que sobrevive hoy en día. No ofrece extras vistosos, y se mantiene con un instalador basado en texto, y sin herramientas de configuración gráfica. Mientras otras distribuciones intentan desarrollar interfaces fáciles de usar para muchas utilidades comunes, Slackware no ofrece nada amistoso, y toda la configuración se realiza mediante los archivos de configuración

Es extremadamente estable y segura, muy recomendada para servidores. Los administradores con experiencia en Linux encuentran que es una distribución con pocos fallos, ya que usa la mayoría de paquetes en su forma original, sin demasiadas modificaciones propias de la distribución, que son un riesgo potencial de añadir nuevos fallos. Es raro que se produzcan lanzamientos de nuevas versiones (aproximadamente una al año), aunque siempre se pueden encontrar paquetes actualizados para descargar después del lanzamiento oficial

- Pros: Alta estabilidad y ausencia de fallos, sigue fielmente los principios de UNIX.
- Contras: Toda la configuración se realiza mediante la edición de ficheros de texto, autodetección de hardware limitada.
- Sistema de paquetes: TGZ [7]
- Descarga gratuita: Si

DISTRIBUCION GENTOO

Esta distribución es una de las únicas que últimamente han incorporado un concepto totalmente nuevo en Linux. Es un sistema inspirado en BSD-ports. Se puede compilar/optimizar el sistema completamente desde cero. La primera versión estable de Gentoo fue anunciada en Marzo del 2002.

Gentoo Linux es una distribución basada en código fuente, la única en esta lista. Mientras que los sistemas de instalación proveen de varios niveles de paquetes

[7] *TGZ (*Es la extensión de los ficheros compactados con TAR y luego comprimidos con GZIP *)*

precompilados, para obtener un sistema Linux básico funcionando, el objetivo de Gentoo es compilar todos los paquetes de código en la máquina del usuario. La principal ventaja de esto es que todo el software se encuentra altamente optimizado para la arquitectura de la computadora.

También, actualizar el software instalado a una nueva versión es tan fácil como teclear un comando, y los paquetes, mantenidos en un repositorio central, se mantienen bastante actualizados. En la otra cara de la moneda, instalar Gentoo y convertirla en una distribución completa, con los últimos entornos gráficos, multimedia y de desarrollo es un trabajo largo y tedioso, cuenta varios días incluso en una máquina rápida.

- Pros: Fácil instalación de paquetes de software individuales, altamente actualizada.
- Contras: Instalación larga y tediosa, ocasionalmente inestable y con riesgos de romperse, no aconsejada para servidores con funciones críticas, cierta experiencia en sistemas Unix.
- Sistema de paquetes: SRC
- Descarga gratuita: Si

DISTRIBUCION UBUNTU

Distribución basada en Debian, con lo que esto conlleva y centrada en el usuario final y facilidad de uso.

Constituye una distribución muy orientada al escritorio, pero con bastante estabilidad. Fundamentalmente comparte las ventajas de debian (exceptuando que tiene ligeramente menos paquetes, y que estos no están tan probados), añadiéndole el hecho de tener una distribución bastante actualizada.

- Pros: 100% libre, Web y recursos de la comunidad excelentes, instalación de software sencillísima usando apt-get.
- Contras: La versión estable no está actualizada.
- Sistema de paquetes: DEB
- Descarga gratuita: Si

DISTRIBUCION CENTOS

CentOS (acrónimo de **C**ommunity **ENT**erprise **O**perating **S**ystem) es un clon a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de RHEL.

Es una distribución de calidad empresarial, pero sin necesidad de pagar por los servicios de actualizaciones o soporte. Disponer de CentOS es una alternativa muy válida para poder tener servidores de desarrollo o preproducción sin tener que pagar suscripciones por cada sistema

- Pros: Distro Linux gratuito orientado a los usuarios que necesiten un sistema operativo de nivel empresarial. Una activa y creciente comunidad de usuarios, desarrollo rápido, probado y corregido, una extendida red de replicas (mirrors), múltiples y gratuitas vías de soporte, foros, etc.

- Contras: No tienen soporte comercial, es decir que aplicaciones propietarias tal vez no se ejecuten de buena manera en estas distros, y cierto hardware igualmente no va a funcionar correctamente.

- Sistema de paquetes: RPM

- Descarga gratuita: Si

DISTRIBUCION MANDRIVA

Mandriva Linux (anteriormente Mandrake Linux) es una distribución que en su inicio se basó en la distribución de la empresa Red Hat, Red Hat Linux, para después seguir su propio desarrollo. Enfocada a usuarios principiantes e intermedios, usando las versiones mas recientes de sus aplicaciones y librerías. Lo más destacado de esta distribución son sus asistentes de configuración.

- Pros: Instalador fácil de utilizar. Detección de hardware y utilidades de particionamiento de disco consideradas por muchos como las mejores de la industria. Distribución altamente actualizada de Linux

- Contras: Existen más errores y quizás menos estabilidad que con otras distribuciones.

- Sistema de paquetes: RPM

- Descarga gratuita: Si

Tabla. 2.1. Resumen de distribuciones Linux

Distribución	Formato de paquetes	Descarga gratuita	Escritorio predeterminado	Disco(s)	Recomendable para
Red Hat Enterprise	RPM	NO	GNOME	4	Empresas
Fedora	RPM	SI	GNOME	4	Principiantes
Debian	DEB	SI	GNOME	14	Usuarios Avanzados
Suse	RPM	SI	KDE	5	Principiantes y empresas
Slackware	TGZ	SI	KDE	2	Usuarios avanzados
Gentoo	SRC	SI	----	1	Usuarios Avanzados
Ubuntu	DEB	SI	GNOME	1	Todos
CentOS	RPM	SI	KDE	4	Empresas
Mandrila	RPM	SI	KDE	4	Principiantes

Al haber realizado un análisis de las diferentes distribuciones de Linux se ha decidido utilizar el sistema operativo CentOS para el proyecto de tesis, puesto que es una distribución a nivel empresarial y acorde con sus características cumple con los requerimientos necesarios para la implementación del mismo.

La versión a ser usada en el servidor es CentOS 4.5

2.1.4 Principales Aplicaciones

Hay numerosas aplicaciones para Linux:

- Navegador Web: Ofrece navegación más segura por Internet Mozilla o bien Mozilla Firefox.
- Cliente de Correo: Mozilla Thunderbird o bien Evolution.
- Administrador de archivos similar al Explorer de Windows: Konqueror y Nautilus (integrados en KDE y Gnome, respectivamente).

- Entorno ofimático completo: Esta claro que una de las cosas que necesitamos realizar con el ordenador es la utilización de hojas de cálculo, la edición de textos para trabajos, etc. Los softwares más comunes que se utilizan para este tipo de aplicaciones son: OpenOffice., Koffice. y Staroffice
- Visor de PDF: Acrobat Reader, Xpdf, Gpdf.
- Creación de PDF: OpenOffice.
- Autoría de DVDs y Cds: Una de las cosas que nos empieza a meter más en el mundo de Linux es cuando conseguimos sustituir todo lo que hacíamos antes en Windows, pues bien, grabar CDs es un paso importante en la independencia de nuestro Linux sobre Windows. Se lo puede realizar mediante el uso del software K3b
- Reproducción de ficheros de sonido: Reproductor de archivos de música MP3. Una de las opciones que se puede utilizar es el software llamado XMMS .
- Reproducción de DivX, VCD, DVD: Mplayer, xine.
- Creación de páginas Web: Quanta+.
- Compartición P2P: aMule, BitTorrent, MLDonkey
- Tratamiento gráfico: Ya sea para realizar complejos retoques fotográficos o para lo más simple se necesita un programa de dibujo. En Linux se tiene varias y muy buenas opciones tales como los softwares The Gimp y Krita.
- Mensajería instantánea: aMSN (MSN), Gaim.
- Ejecución de aplicaciones Windows: Wine, WineX (Cedega).
- Bases de datos
- Emuladores
- Servidores: al ser Linux un sistema operativo que nació y se actualiza en el Internet, ha servido como servidor para el mismo. A continuación se detalla algunas de las principales aplicaciones que puede desempeñar como servidor:

-Red: Asignación de direcciones IP estáticas y dinámicas, gateway, tarjetas de red virtuales, enrutamiento entre redes.

-DHCP: Asignación dinámica de direcciones IP a todos los usuarios de la red

-DNS: Servicio de traducción de nombres de dominio en zonas forward y reverse

-Web: Servidor Apache http para publicación de páginas Web

-Proxy: Servicio que permite dar acceso a Internet a los usuarios de la red a través de un puerto determinado

-Correo Electrónico: Envío y recepción de correos electrónicos hacia un dominio determinado

-FTP: Protocolo de transferencia de archivos

-Seguridades: Firewall de tipo corporativo, Antivirus, MailScanner, Antispam

-Monitoreo: Accesos desde y hacia la red, aplicaciones, puertos

2.2 INSTALACIÓN DEL SISTEMA OPERATIVO CENTOS 4.3

El primer paso para realizar la instalación del sistema operativo CentOS 4.3 es necesario descargar el software de Internet

Debido a que se trata de un software de distribución gratuita, este se lo puede obtener directamente desde el sitio Web de CentOS en Internet.

Los pasos a seguir para la obtención del software son los siguientes:

- Ingresar al sitio Web www.centos.org (ver figura 2.1)
- Colocar el cursor sobre el link download y escoger la opción Mirrors

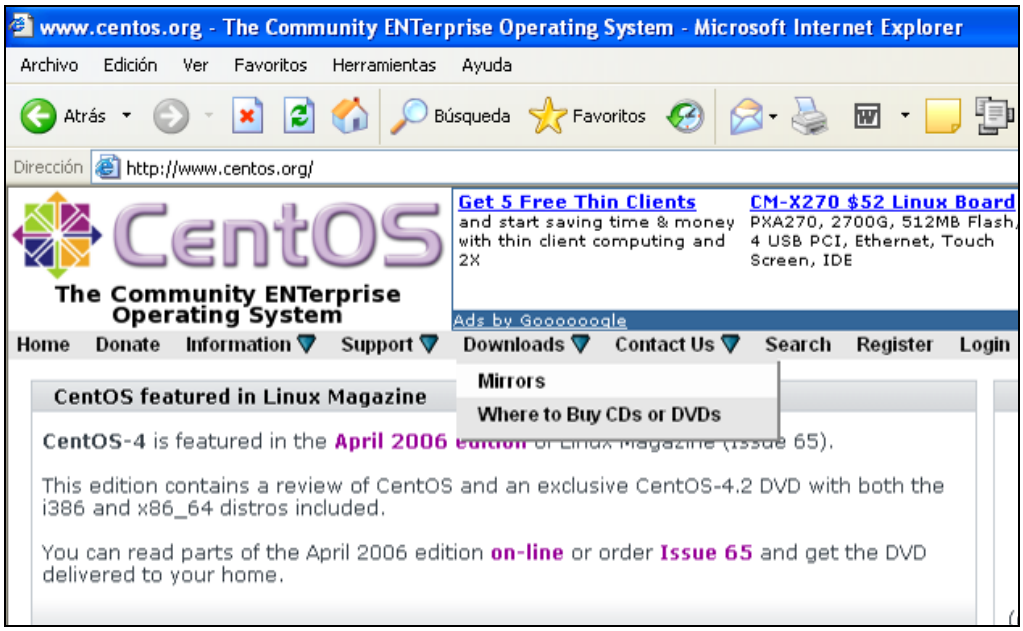


Figura. 2.1. Página Web para descargar el software CentOS 4.5

- Escoger la versión de CentOS 4 como se indica a continuación:

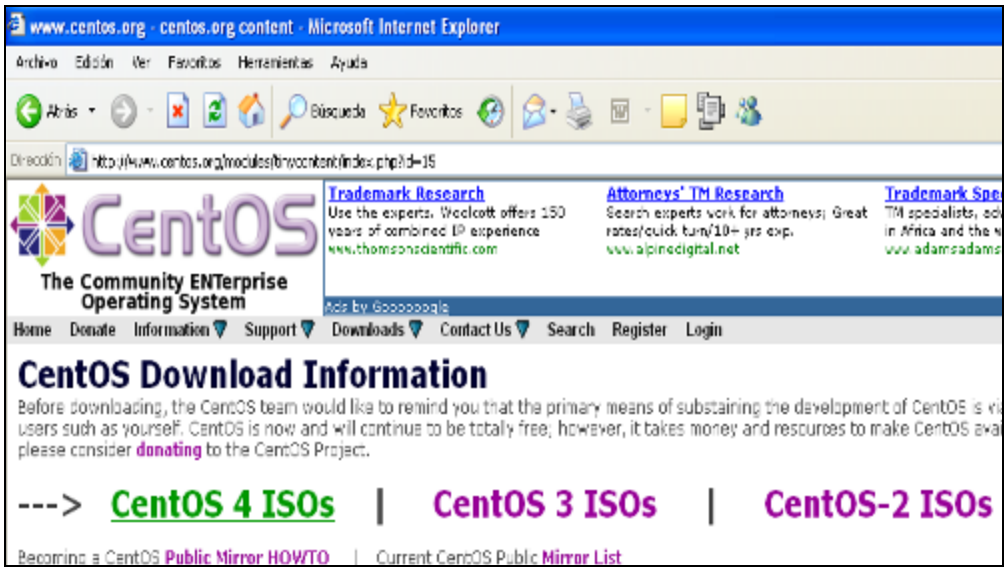


Figura. 2.2. Diferentes versiones de CentOS

- Se escoge el tipo de plataforma i386 debido a que se constituye en la más apropiada para el tipo de plataforma de hardware disponible

Figura. 2.3. Tipo de plataforma

- En la figura 2.4, se presentan varios links desde donde se puede descargar el software. Se escoge para el caso la dirección http://mirrors.kernel.org/centos/4.3/isos/i386/ debido a que el sitio Web kernel.org brinda total confiabilidad para la descarga del sistema operativo.

Figura. 2.4. Links de sitios Web para descarga de CentOS 4.5

- De la lista se escogen los archivos siguientes para la descarga:

  - CentOS-4.3-i386-bin1of4.iso
  - CentOS-4.3-i386-bin2of4.iso
  - CentOS-4.3-i386-bin3of4.iso
  - CentOS-4.3-i386-bin4of4.iso

  Ver figura 2.5

Los cuales corresponden a la serie completa de archivos para la instalación del sistema operativo, sin necesidad de conectarse a Internet durante la misma.

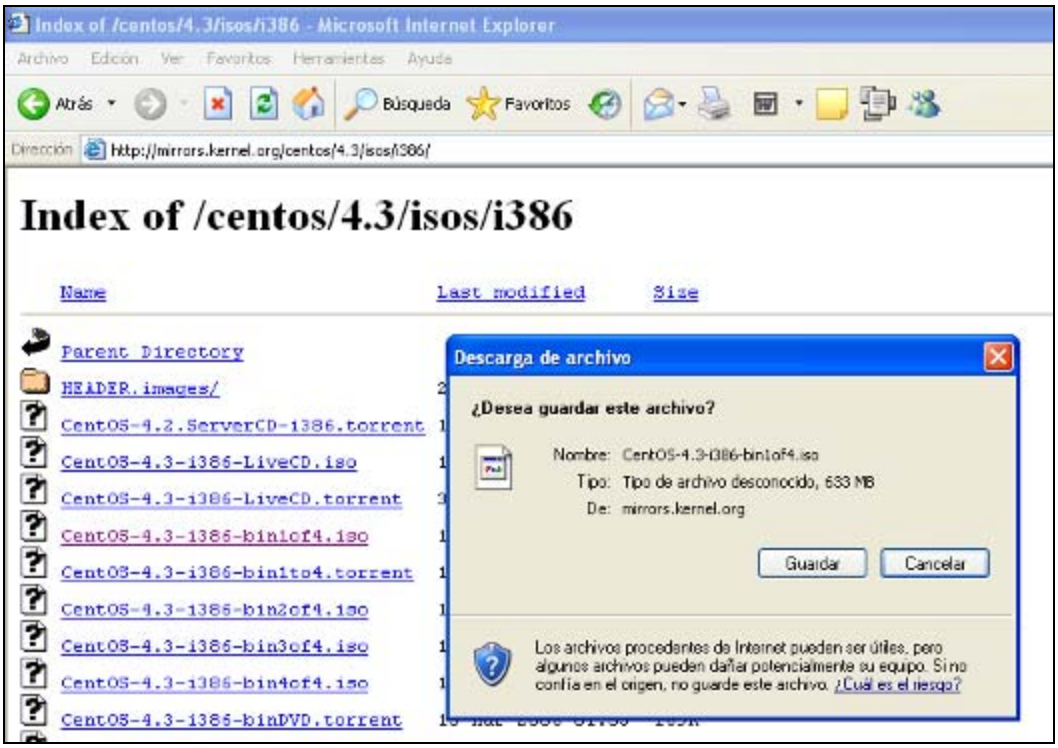


Figura. 2.5. Descarga de archivos de CentOS 4.5

Debido a la considerable cantidad de MB[8] a ser descargados, se puede correr el riesgo de que se interrumpa la descarga de archivos por factores externos como cortes de energía eléctrica o fallas en la conexión a Internet o a su vez por conflictos del sistema operativo Windows provocando que se pierdan toda la información hasta un cierto punto obtenida y teniendo que reanudar la descarga desde un inicio.

Como solución a esto se puede bajar los archivos de CentOS 4.3 utilizando un sistema operativo Linux anteriormente instalado con la ventaja de que si se tiene una interrupción en la descarga, se la puede reanudar desde el punto en donde se provocó dicha interrupción.

Para poder descargar se ingresa como administrador, se escoge la carpeta en donde guardar la información y luego se ejecuta el comando ***wget*** seguido por la dirección url del sitio Web de descarga y un punto al final de tal manera que se indica que los archivos se guarden en la carpeta a la cual se ingresó previamente, así:

[8] *MB (*Megabytes *)*

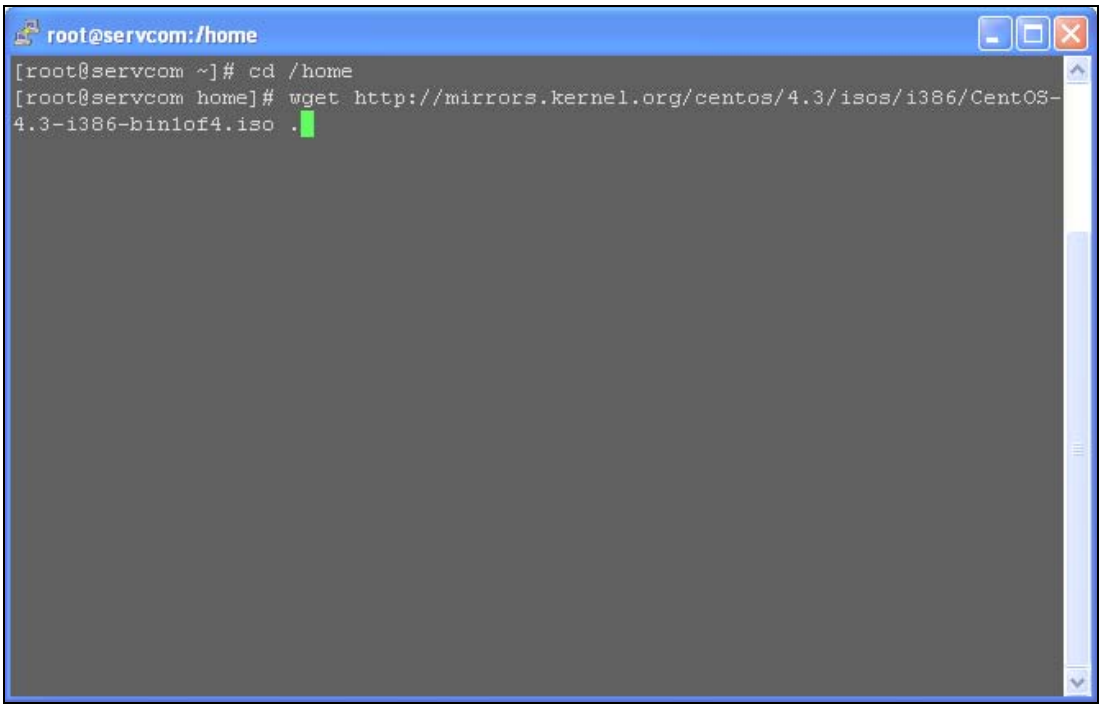


Figura. 2.6. Descarga de archivos de CentOS 4.3 utilizando Linux

Una vez obtenidos los cuatro archivos .iso desde el Internet, se debe quemar un cd por cada uno de ellos, para esto se puede utilizar cualquier programa que me permita guardar dicha información en un cd-rom.

Instalación del sistema operativo:

Una vez creados los cd's de instalación, se tendrá al CD 1 como disco de arranque, de tal manera que para realizar la instalación únicamente se debe colocar el cd # 1 de CentOS 4.3 en una unidad de CD-ROM. De forma automática (tomando en cuenta que el boot en el BIOS se lo haga desde la unidad de CD) iniciará la instalación del sistema operativo, presentado una pantalla como la que se indica a continuación:

Figura. 2.7. Pantalla de inicio de instalación de CentOS 4.3

Una vez que se realiza la secuencia de inicio de instalación del sistema operativa y carga algunos módulos para el inicio de la instalación, se presenta una pantalla la cual permite realizar la un chequeo de el correcto estado de cada uno de los cd's de instalación.

Puesto que es la primera vez que se va a instalar el sistema operativo, es recomendable realizar el test de los cd's para posteriormente evitar problemas en la instalación.

Para iniciar la prueba de los discos de instalación, se debe escoger la opción *OK* y de manera automática iniciará el chequeo, como se indica en la figura 2.8. Una vez finalizada cada prueba de un cd, se presenta un informe, indicando si existen errores o no. El proceso se repite para los restantes 3 discos.

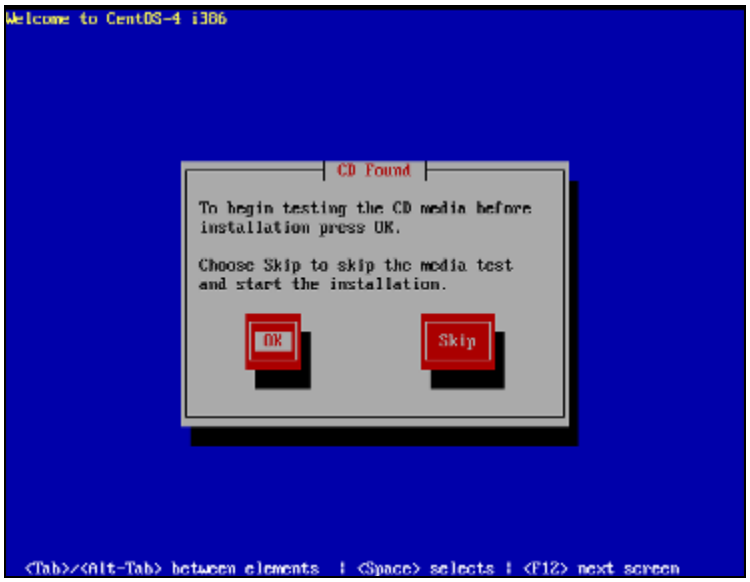


Figura. 2.8. Chequeo del estado de los CDs de instalación

Una vez finalizado el test de los discos, se presenta la pantalla de inicio de instalación del sistema operativo CentOS 4.3. Todas las pantallas que se muestran a continuación cuentan con una ayuda en la parte izquierda, la cual puede ser ocultada según sea el caso.

En la pantalla que se presenta en la figura 2.9, se debe dar clic en *Next* para continuar con la instalación.

Figura. 2.9. Pantalla de inicio de instalación de CentOS 4.3

Como siguiente paso, se escoge el idioma que se usará durante la instalación. En este caso y para facilidad, se toma la opción *Spanish (Español)* y se hace clic en *Next.*

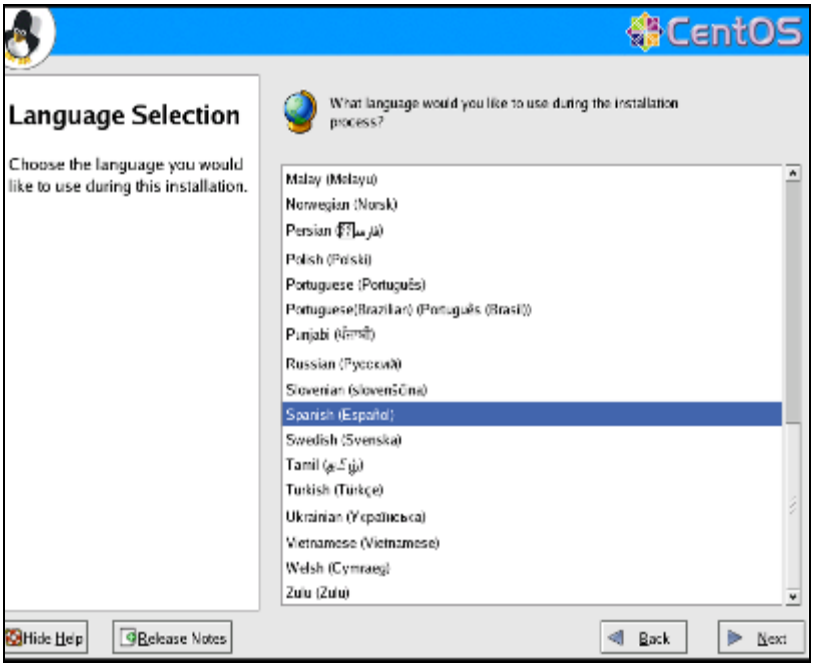


Figura. 2.10. Pantalla para escoger el lenguaje para la instalación

Como siguiente paso, se escoge el tipo de teclado, en este caso va a ser *Spanish* y se da clic en *Siguiente*.

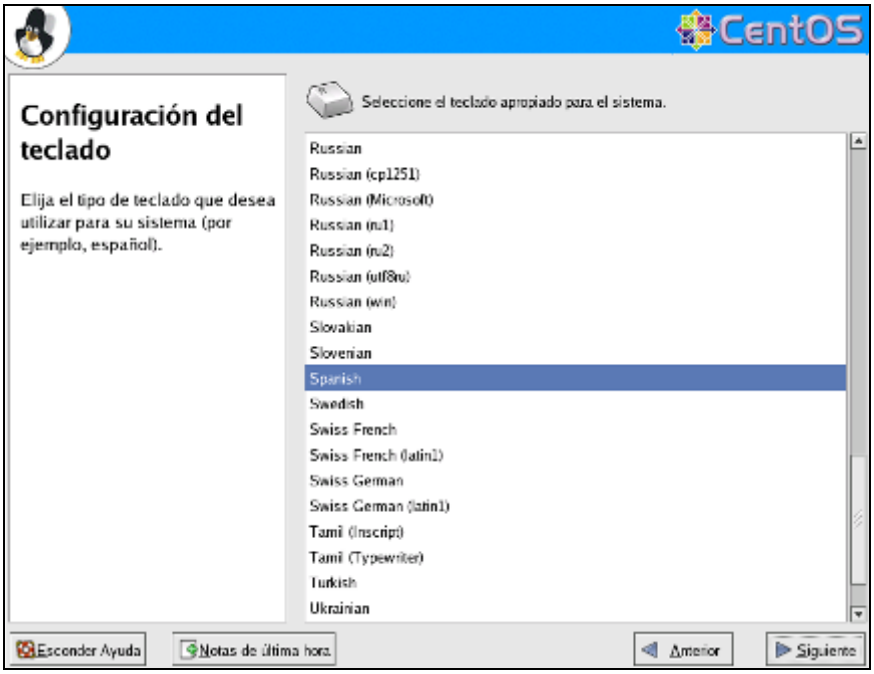


Figura. 2.11. Pantalla para escoger el idioma del teclado

A continuación se escoge el tipo de instalación. Para el desarrollo del proyecto se deberá escoger el tipo de instalación como "*Servidor*", puesto que brinda herramientas adicionales, las cuales serán utilizadas para la configuración de distintos tipos de servicios que se explicarán más adelante.

Se da clic en *Siguiente* para continuar la instalación.

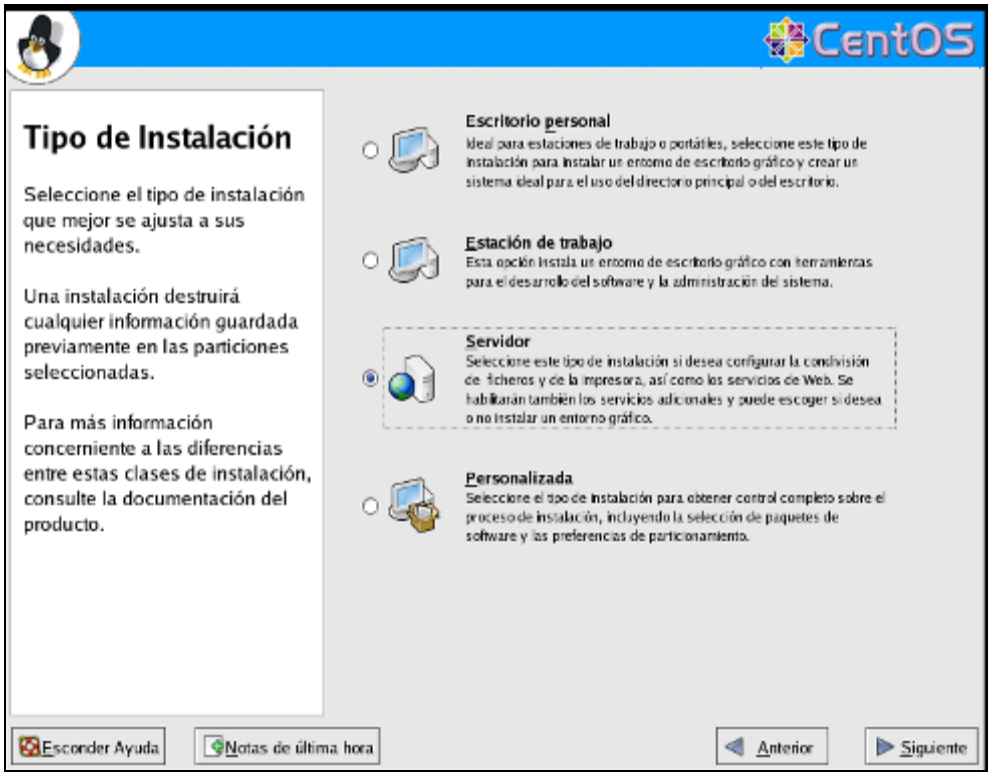


Figura. 2.12. Tipo de instalación

Como siguiente paso, se debe escoger el tipo de particionamiento. Existen 2 tipos:

- El particionamiento automático, el cual establece tres tipos de particiones a saber: /boot (partición para el arranque del sistema operativo), / (partición raíz) y swap (partición de memoria virtual que debe ser el doble de la memoria RAM[9] del PC).
- El particionamiento manual Disk Druid, mediante el cual se puede realizar un tipo de división del disco duro, teniendo un mejor criterio para la instalación del sistema.

[9] *RAM (*Random Access Memory (Memoria de acceso directo *)*

El tipo de particionamiento a realizarse es del tipo Disk Druid. En el próximo punto se explicará el criterio escogido para la realización de cada una de las particiones determinadas.

Para continuar se da clic en *Siguiente*

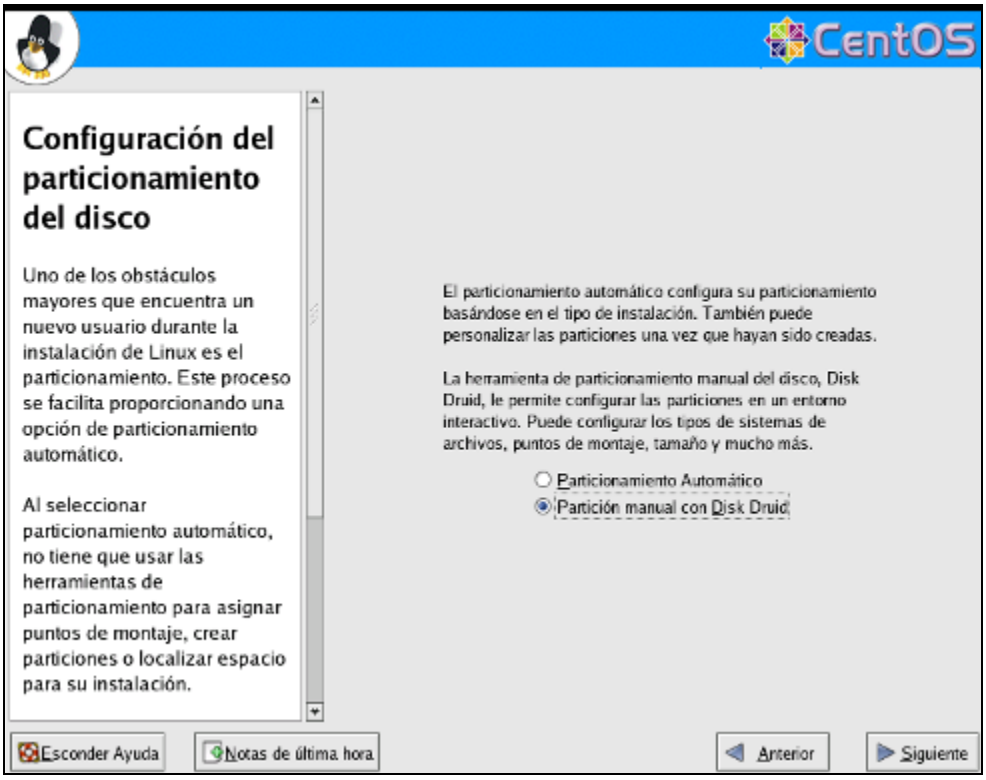


Figura. 2.13. Tipo de particionamiento

Como siguiente paso se tiene una pantalla inicial para comenzar con la configuración del disco duro. Como se puede ver en la parte superior se indica la cantidad de espacio en disco duro disponible, para el desarrollo del proyecto se utilizará un disco de 80 GB de capacidad.

Los dispositivos de almacenamiento en linux se nombran de la siguiente manera:

Si se cuenta con un disco duro tipo IDE, el primer disco será nombrado como hda. En caso de poseer particiones en este disco cada una tendrá un número para ser identificada, así: hda1, hda2, hda3, etc.

En caso de utilizar discos duros tipo scocy, estos serán llamados como sda. De la misma manera las particiones serán sda1, sda2, sda3, etc.

En caso de poseer más de un disco duro en el computador, serán nombrados hda, hdb, hdc, etc. ó sda, sdb, sdc, etc. según sea en caso como disco IDE[10] o scocy.

Para iniciar el particionamiento, se debe dar clic en el link que indica la pestaña *"New"* para de esta manera crear un a nueva partición.

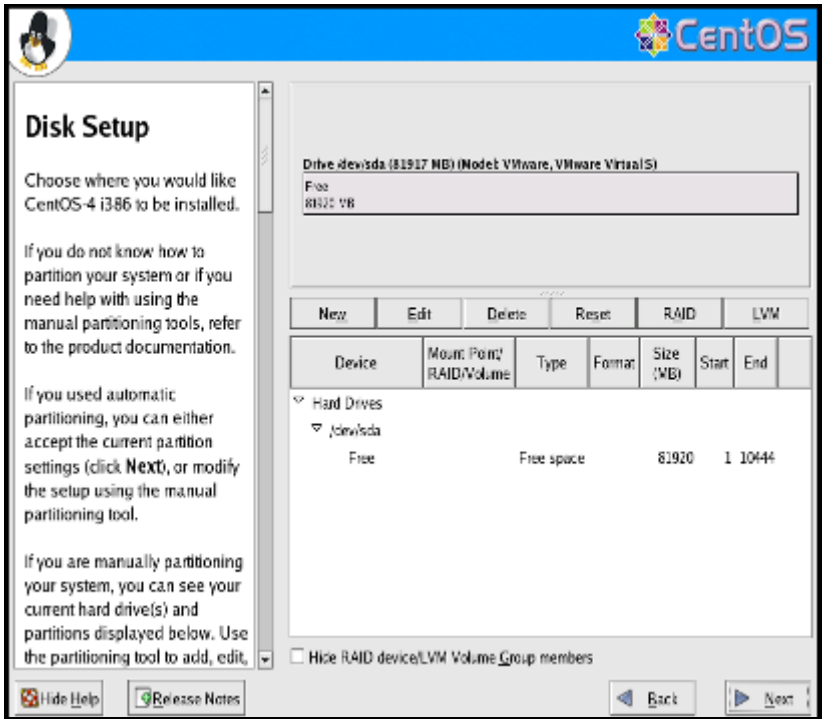


Figura. 2.14. Inicio del proceso de particionamiento

Al hacer clic en "*New*" se despliega una pantalla como la que se muestra abajo.

Aquí inicia el proceso de particionamiento del disco. En primer lugar se debe escoger el punto de montaje, es decir la partición a crearse como tal.

Como primera partición se selecciona / , la cual constituye la raíz del sistema operativo. (tal como C:\ en Windows). A continuación se escoge el tipo de sistema de archivos, en este caso va a ser de tipo ext3 (tal como ntfs o fat en Windows).

[10] *IDE (*Integrated Drive Electronics, disco con la electrónica integrada)

Luego se establece el tamaño de la partición, en este caso es de 20000 MB.

Se da clic en OK y se continúa para crear la siguiente partición.

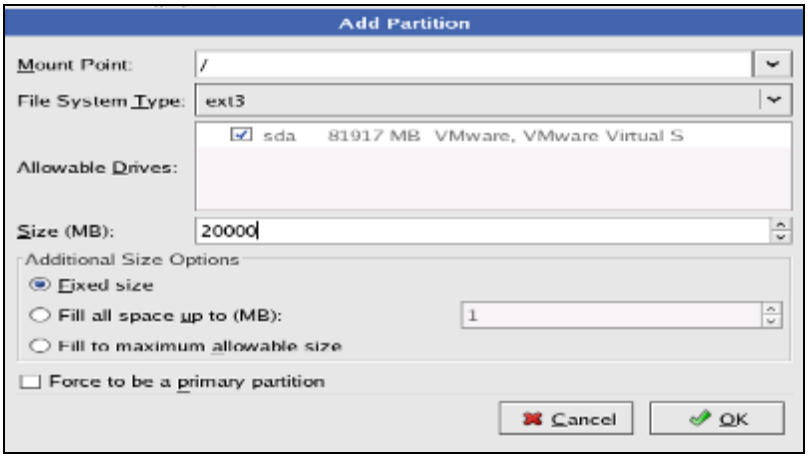


Figura. 2.15. Partición raíz

La siguiente partición a ser creada es la de arranque del sistema operativo (/boot), la cual posee los archivos necesarios para el correcto inicio de CentOS.

Debido a que no se posee archivos que vayan a ocupar un espacio considerable en el disco duro, se ha colocado un tamaño de 500 MB para esta partición.

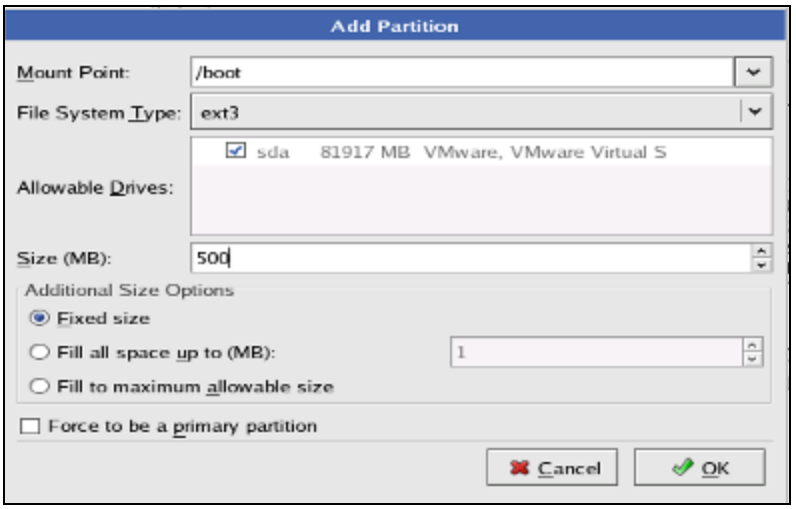


Figura. 2.16. Partición /boot

Como siguiente paso se debe crear la partición /home que para el caso de Windows se podría comparar con la carpeta Documents and Settings.

Aquí se encontrarán las carpetas de todos los usuarios creados en el sistema. Todos estos usuarios poseerán restricciones para realizar cambios importantes en el servidor.

Los usuarios creados podrán posteriormente ser utilizados para cuentas de correo electrónico o para almacenar en cada una de sus carpetas personales distinto tipo de información en caso de poseer un servidor de archivos.

El espacio asignado para esta partición es de 20000 MB.

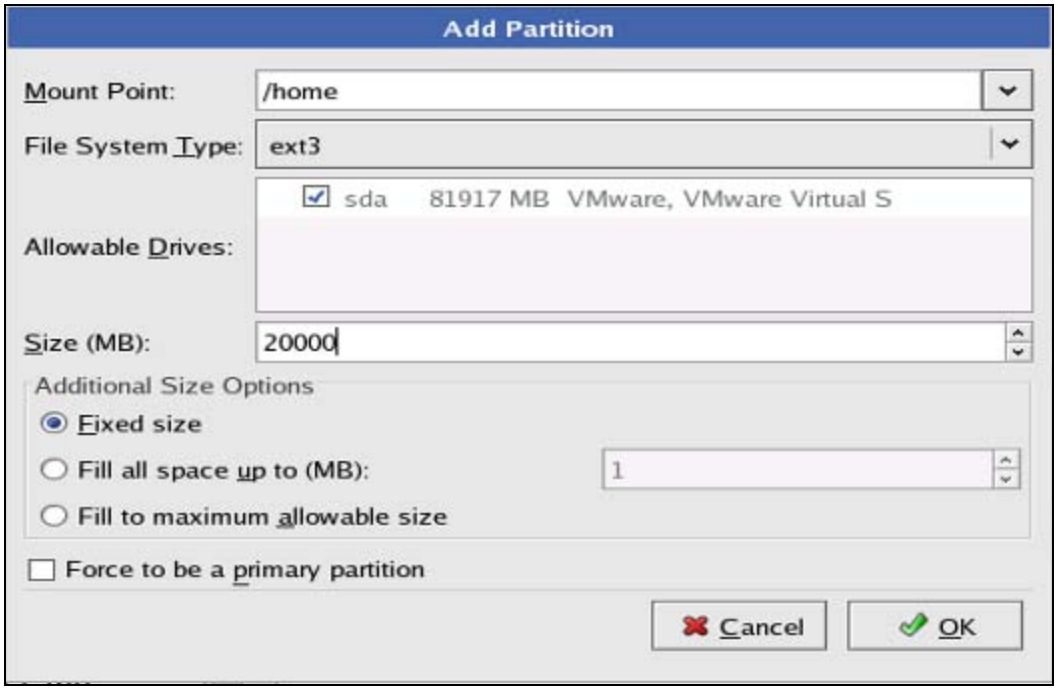


Figura. 2.17. Partición /home

A continuación se crea una de las particiones más importantes del sistema operativo: el sistema de archivos swap.

Esta partición se la podría comparar con la memoria virtual de Windows.

Su función es evitar que el sistema Linux se “cuelgue”. Actúa de tal manera que una vez que son llevados a cabo muchos procesos y la memoria RAM llegue a su límite, entra en funcionamiento la memoria swap, la cual es parte del disco duro.

El sistema operativo seguirá funcionando pero de manera más lenta, debido a que la memoria RAM funciona en el rango de los microsegundos; y la swap funciona en el rango de los milisegundos.

La partición swap debe poseer un tamaño equivalente al doble de la memoria RAM instalada en el computador

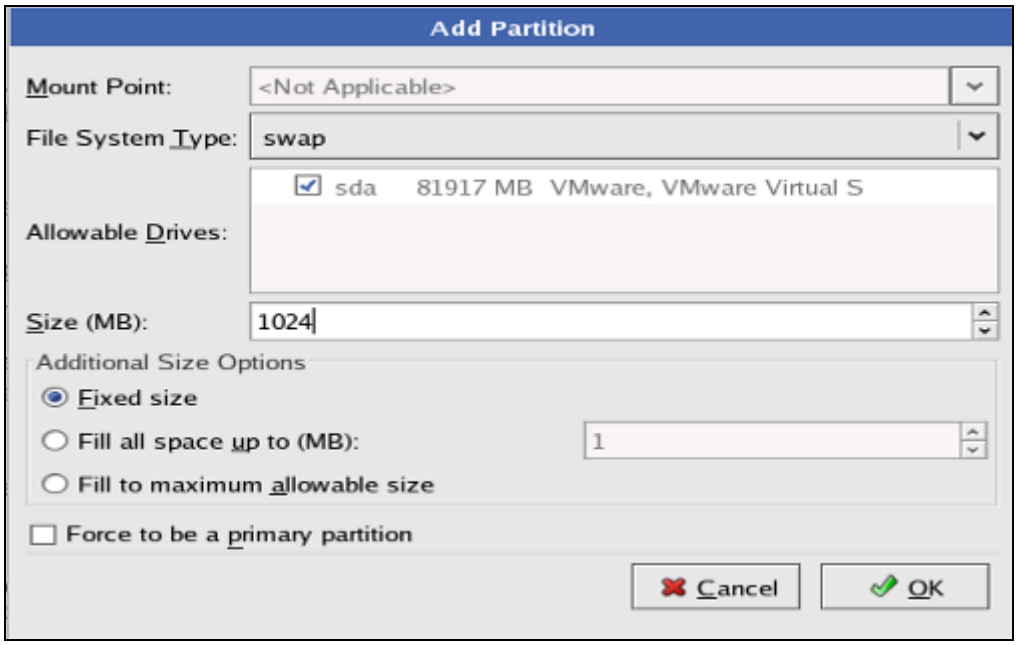


Figura. 2.18. Partición de memoria virtual swap

Como partición final, se crea la llamada tipo /var. En ella se almacenará información acerca de los logs del sistema, servidor de dominio (dns) y los correos electrónicos recibidos por los usuarios entre las características más importantes.

Debido a que es la última de las particiones, se establece un tamaño que corresponde al resto del espacio libre en el disco duro.

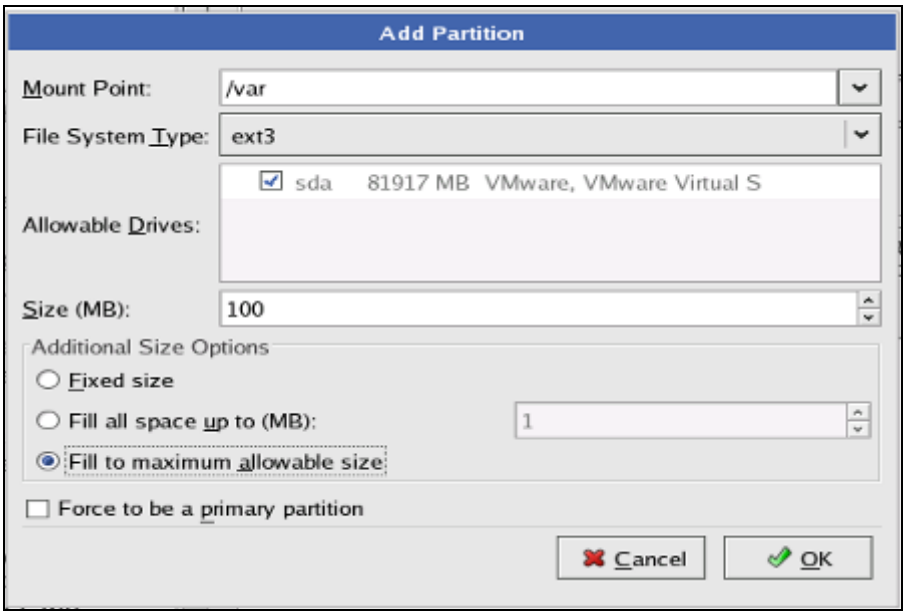


Figura. 2.19. Partición /var

Para culminar el proceso de particionamiento, se visualiza un resumen de las particiones, indicando el tipo (primaria o extendida), el punto de montaje, el tipo de sistema de archivos y el tamaño de cada una de ellas.

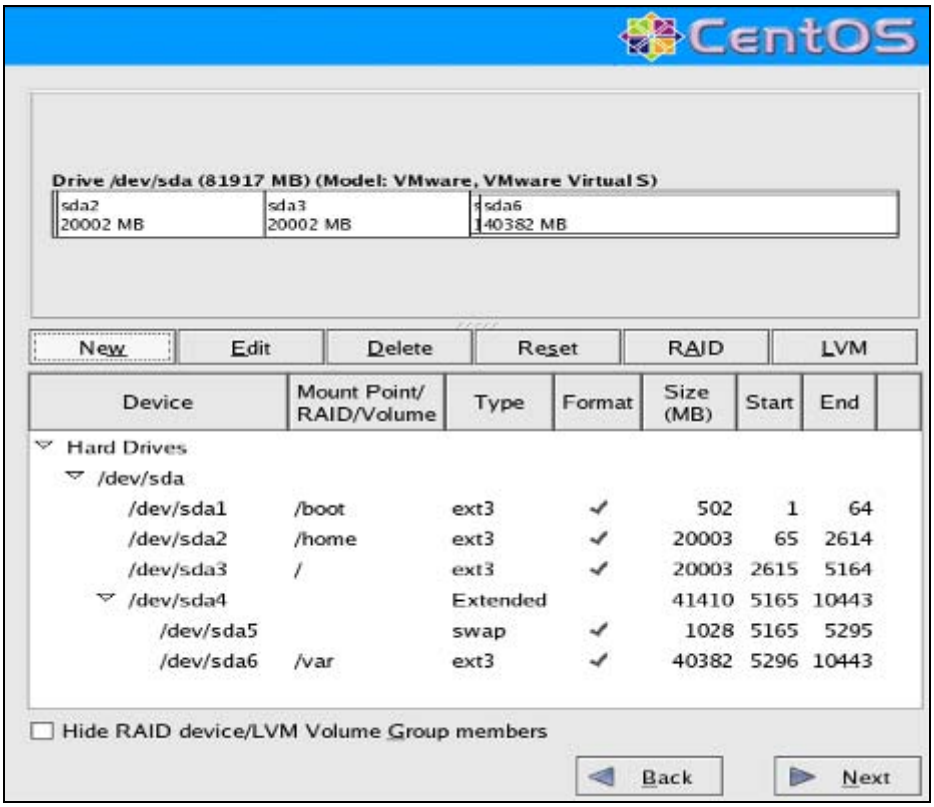


Figura. 2.20. Resumen de particiones

La siguiente configuración que se debe realizar referente al gestor de arranque. Por defecto CentOS trae un solo gestor de arranque llamado GRUB, cuya labor principal es presentar una pantalla de inicio antes del arranque del sistema operativo. Adicionalmente mediante este gestor de arranque se puede establecer entre otras cosas el nivel de inicio del sistema operativo y permite el cambio de contraseña de administrador en caso de olvido.

Debido a esto, es importante establecer una contraseña para el gestor de arranque, lo cual se realiza de manera muy sencilla.

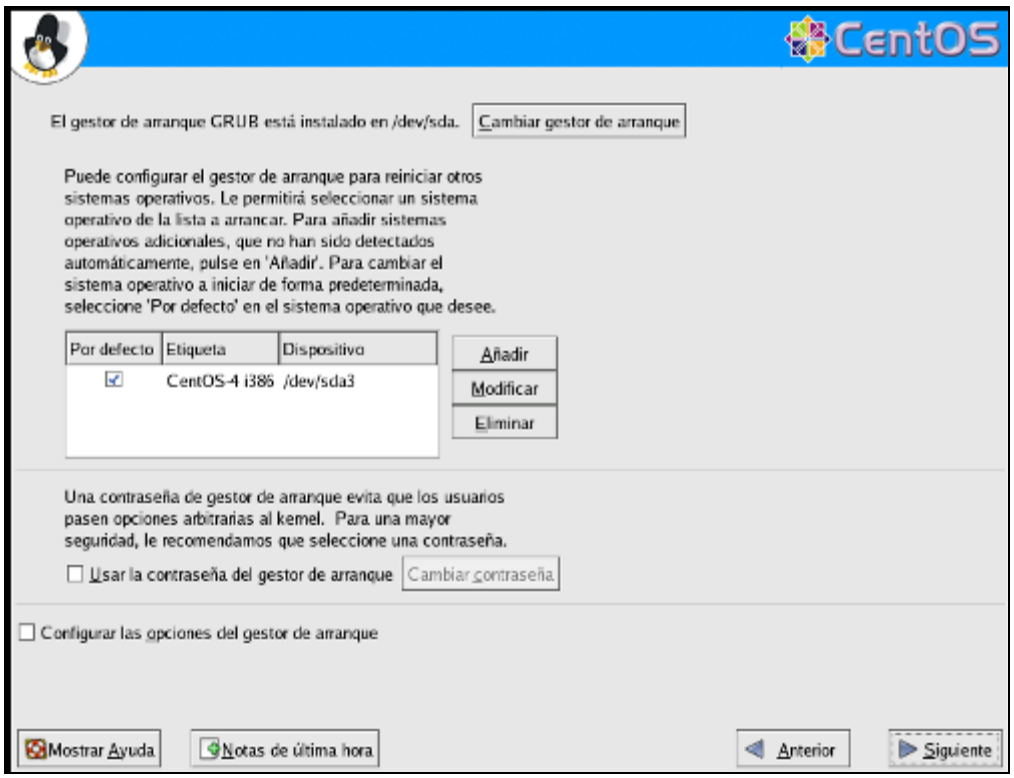


Figura. 2.21. Gestor de arranque

La siguiente pantalla muestra la configuración del firewall que proporciona el sistema por defecto. En este caso, inicialmente, no se va a habilitar ningún tipo de cortafuegos (firewall) debido a que es demasiado básico para proporcionar un tipo de seguridad adecuado. Posteriormente, se configurará el firewall utilizando otro tipo de software más especializado.

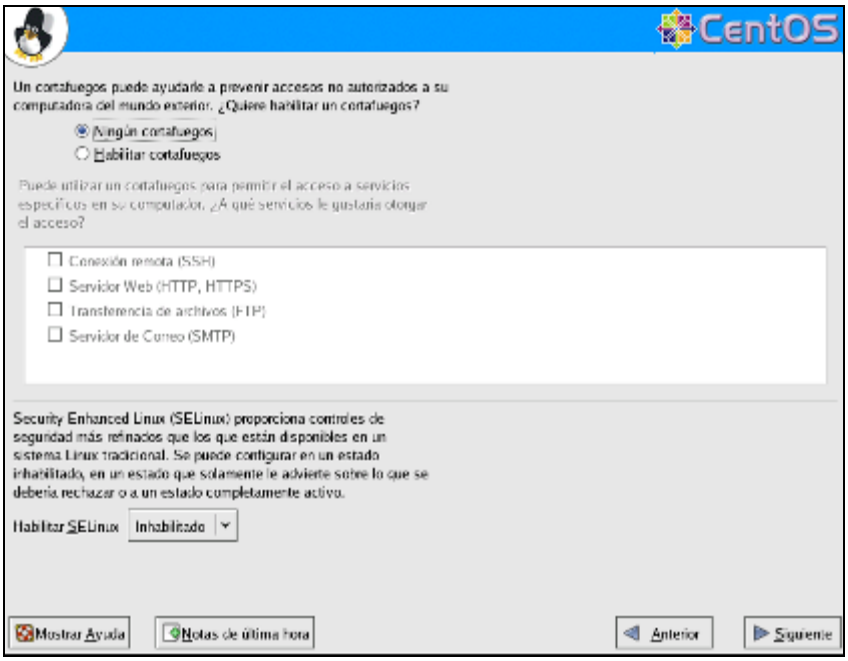


Figura. 2.22. Cortafuegos (Firewall)

En la siguiente pantalla se escoge el idioma por defecto que se instalará en el sistema. Para la instalación a realizarse se debe seleccionar dos tipos, el español y el inglés, esto debido a que algunas de las ayudas se presentan en español y será mucho más fácil el entendimiento de los mismos; y el inglés se lo instala debido a que muchos de los softwares adicionales a ser instalados, requieren soporte para idioma inglés.

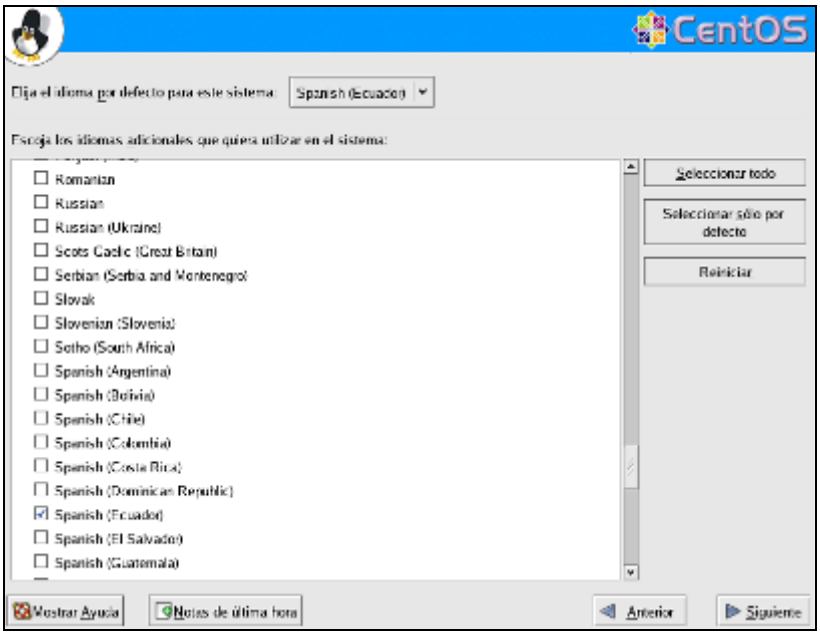


Figura. 2.23. Idioma del sistema operativo

La siguiente configuración a realizar corresponde al tipo de zona horaria a ser escogido. Se da clic en "*Siguiente*" para continuar

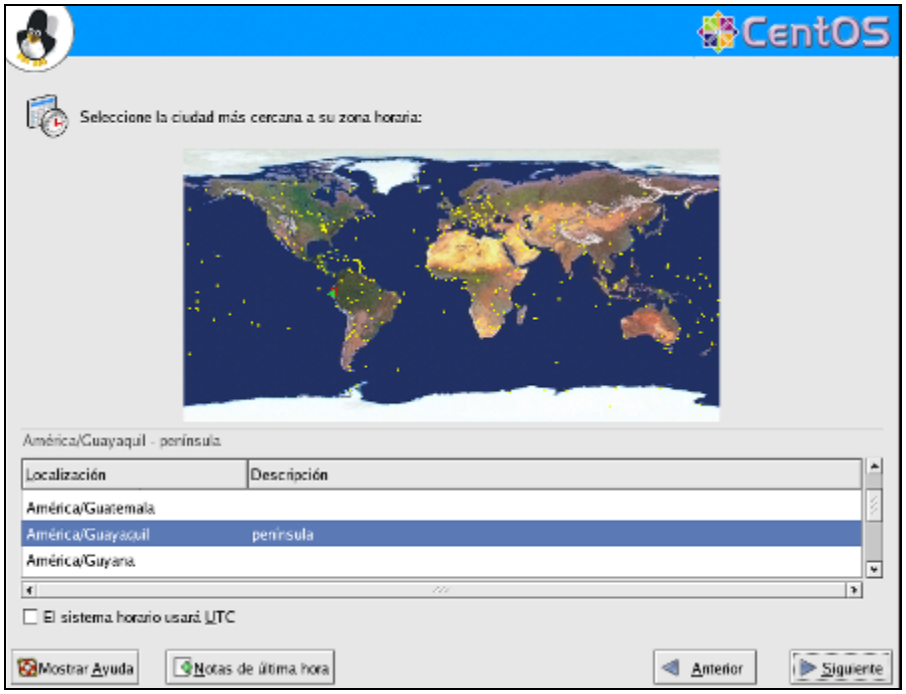


Figura. 2.24. Zona horaria

A continuación se debe ingresar la contraseña que utilizará el administrador (root) del equipo para poder ingresar al sistema.

Cuando un usuario administrador inicia el sistema, este tiene todos los privilegios para realizar cualquier tipo de modificación en el mismo, debido a esto se recomienda colocar una contraseña de difícil descifrado en caso de que exista alguna pretensión de intrusos en el sistema.

Clic en "*Siguiente*" para continuar

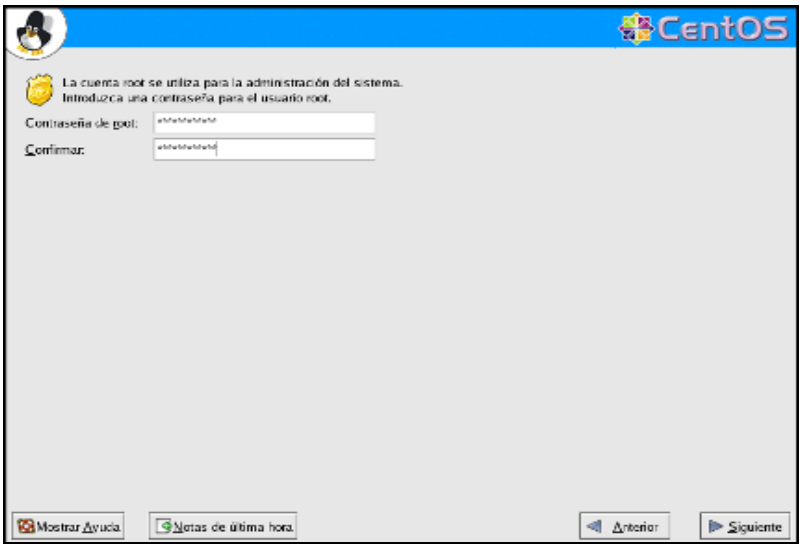


Figura. 2.25. Definir contraseña de root (administrador)

Como siguiente paso se debe escoger el tipo de aplicaciones a ser instaladas para el funcionamiento del sistema operativo.

CentOS permite escoger de cada uno de los paquetes a ser instalados y los divide en diferentes secciones como se verá a continuación:

El primer tipo de aplicación que se instala corresponde al tipo de escritorio gráfico a ser utilizado. En este caso se puede escoger entre tres diferentes a saber: el sistema X Window, el entorno GNOME y el entorno KDE.

Para la instalación a ser realizada, se escoge el sistema KDE, debido a que el sistema X Window es demasiado básico y posee muchos impedimentos. El sistema GNOME es parecido al KDE con la diferencia que ocupará mucho más espacio en el disco duro, lo cual no conviene para un entorno gráfico que será muy poco utilizado.

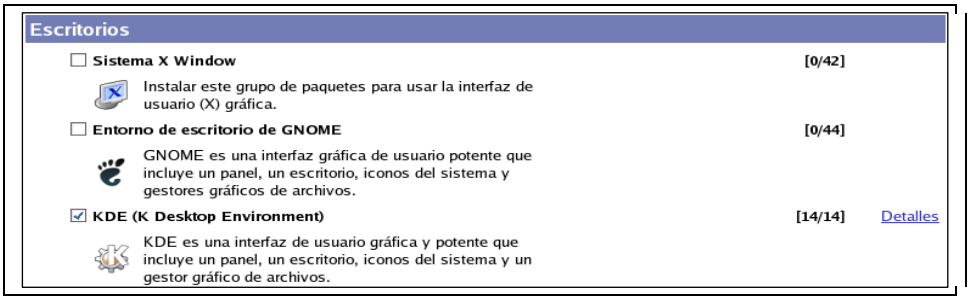


Figura. 2.26. Definición del tipo de escritorio a instalarse

A continuación se escoge el tipo de aplicaciones a ser instaladas, para el caso de servidor se deberá evitar instalar todo lo que corresponda a paquetes de ofimática, sonido, gráficos, juegos, etc. Una instalación recomendada en cuanto a estos paquetes es la que se indica a continuación. Cada usuario o administrador de este tipo de sistemas poseerá su criterio para seleccionar las aplicaciones según su parecer.

Figura. 2.27. Definición de las aplicaciones a instalarse

Con un criterio más centrado en el tipo de servicios que brindará el servidor de aplicaciones, se deberá escoger los paquetes correspondientes al ítem *"Servidores"*.

Para el presente proyecto, se necesitarán las aplicaciones indicadas a continuación:

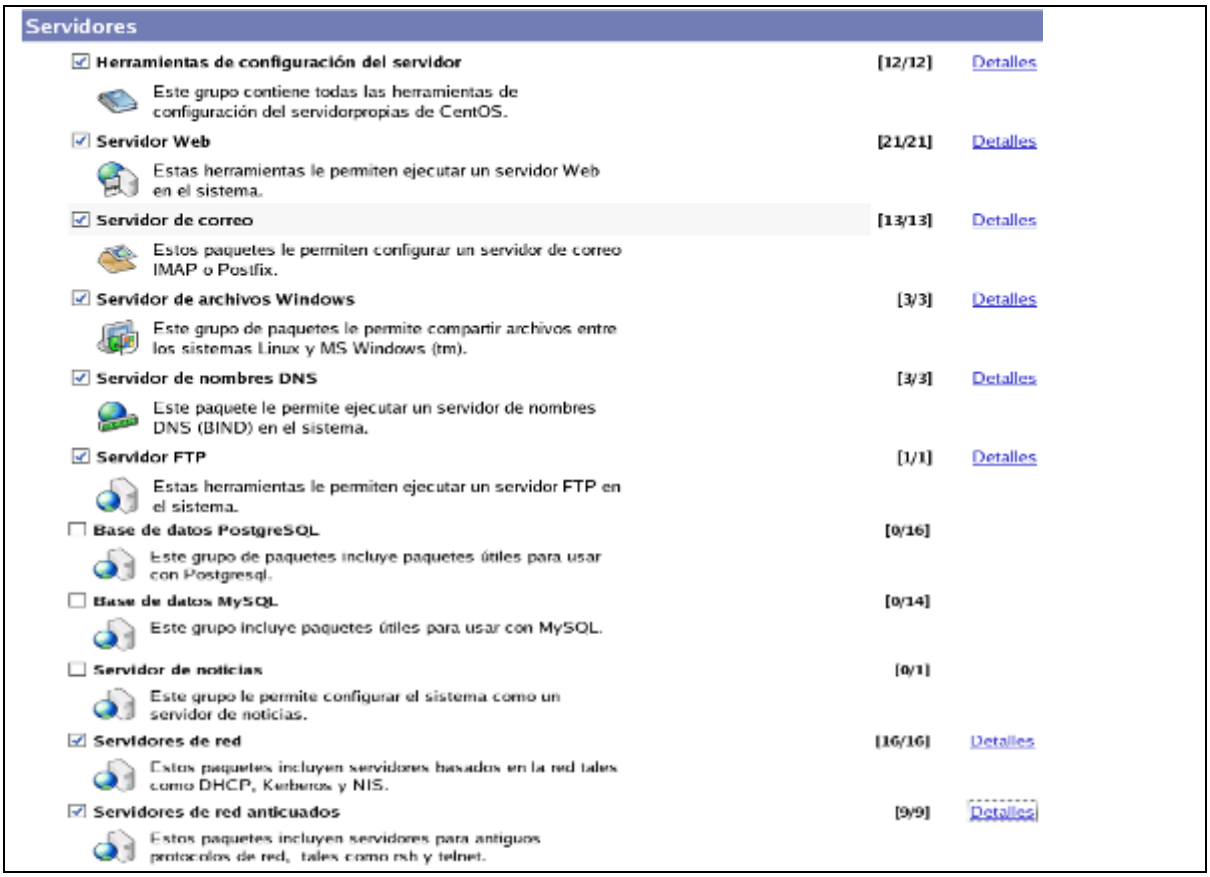


Figura. 2.28. Definición de los tipos de servidores a instalarse

Adicionalmente se deberán seleccionar herramientas de desarrollo, las cuales principalmente servirán para introducir en el sistema diferentes tipos de librerías, las cuales posteriormente servirán para poder instalar software adicional y evitar problemas debido a la falta de alguna de las mismas. Se escoge el *"Desarrollo de software para KDE"* debido a que es el tipo de software a instalarse tal como se indicó en el primer punto al iniciar escogiendo las diferentes aplicaciones.

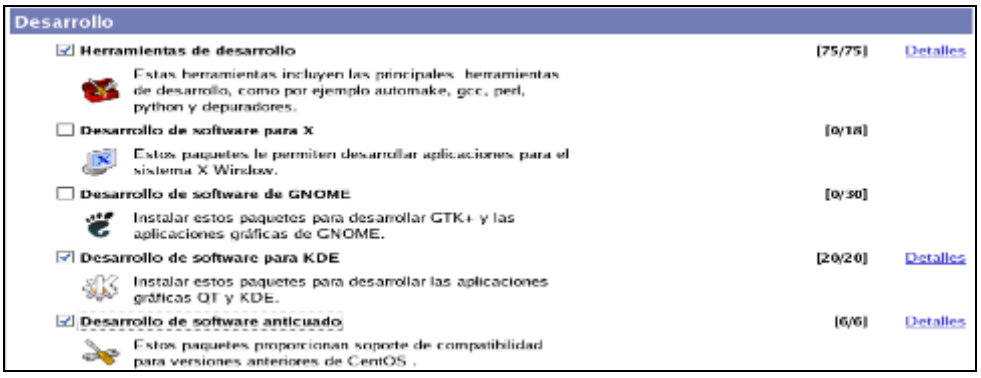


Figura. 2.29. Definición de las herramientas de desarrollo a instalarse

También se debe seleccionar paquetes del sistema, tales como herramientas de administración y herramientas del sistema.

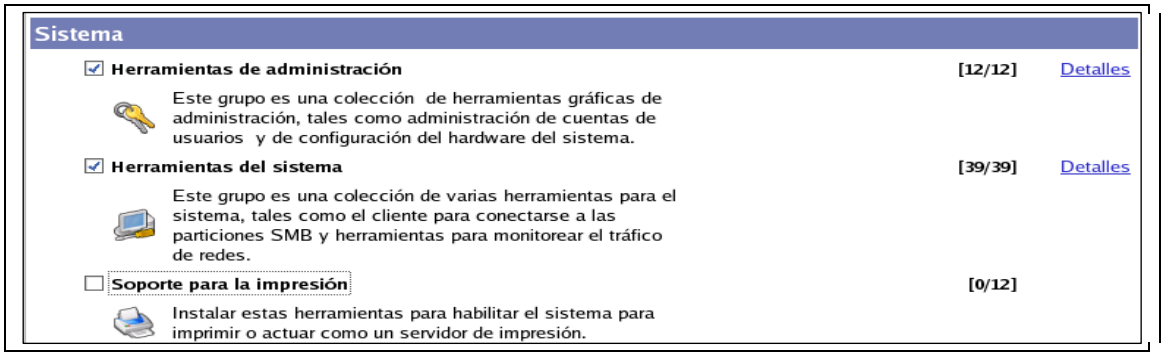


Figura. 2.30. Definición de las herramientas de sistema a instalarse

Como último punto se presenta una *"Miscelánea"*, en la cual se puede escoger una instalación total de los paquetes, así como también un tipo de instalación mínima para el funcionamiento del sistema operativo.

En este caso no se debe seleccionar ninguna de las opciones debido a que se ha escogido por separado a cada una de las aplicaciones a ser instaladas.

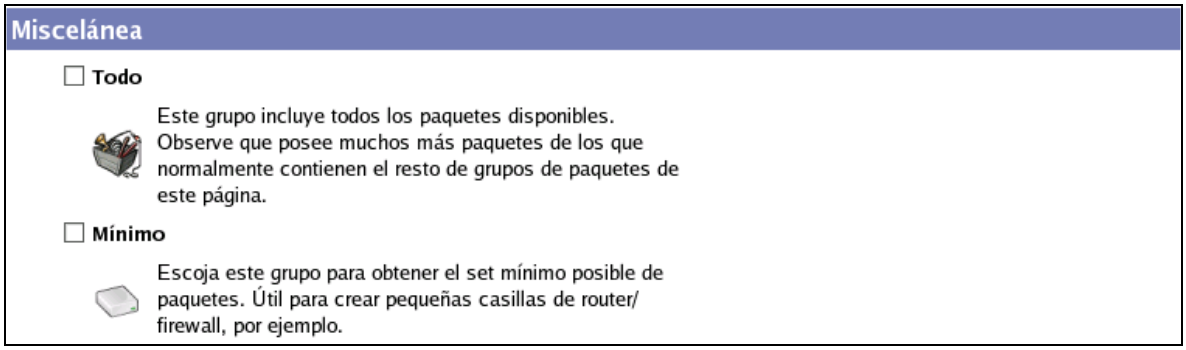


Figura. 2.31. Miscelánea de la instalación

A continuación únicamente se debe dar clic en *"Siguiente"* para dar inicio a la instalación.

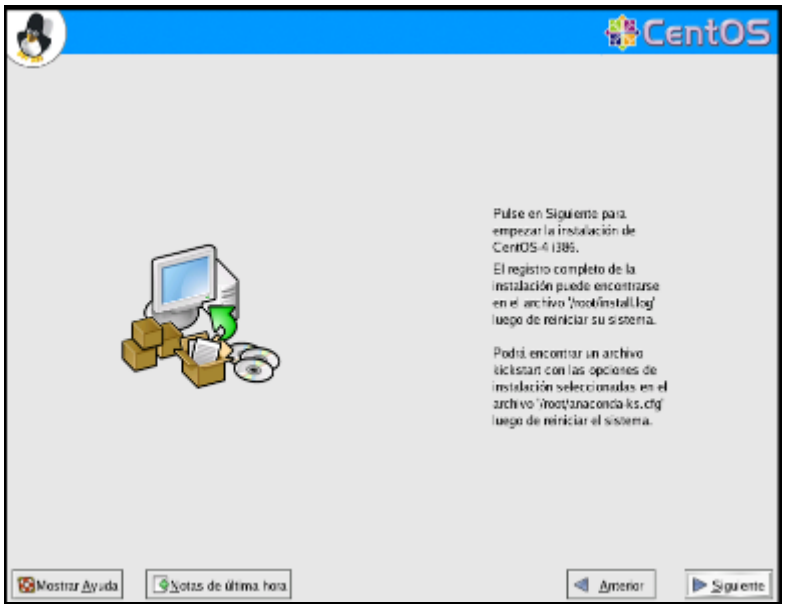


Figura 2.32 Inicio de la instalación

Luego el sistema presenta un resumen de los medios (CD's) que van a ser necesitados para la instalación. Esto corresponde según la cantidad de paquetes que se haya escogido.

Figura 2.33 Medios requeridos para la instalación

La instalación inicia formateando cada una de las particiones creadas anteriormente. A lo largo de la misma, el sistema pedirá el ingreso de los diferentes discos. Una vez finalizada la instalación, CentOS automáticamente se reiniciará.

Una vez completada la instalación, se puede empezar con la configuración del servidor de aplicaciones.

2.2.1 Requerimientos del Hardware

Hardware recomendado para operar:

- **Memoria RAM:** 256 MB (Mínimo).
- **Espacio en Disco Duro:** 2 GB (Minimo) - 10 GB (Recomendado).
- **Procesador**: Intel Pentium III/IV/Celeron, AMD[11] II/III, AMD Duron, AMD Athlon/XP/MP.

2.2.2. Instalación de Software adicional

La instalación de software adicional se lo hace con la finalidad de contar con servicios adicionales en el servidor de aplicaciones, tales como monitoreo, administración, etc.

En este punto se va a explicar como realizar la instalación de diferentes paquetes con los que cuenta Linux.

El primero y más sencillo de instalar es de extensión rpm. Para instalarlo se debe descargar el paquete deseado mediante la opción *wget* explicada anteriormente y ejecutar el comando:

rpm –ivh <nombredelpaquete.rpm>

donde:
rpm: tipo de paquete a ser instalado
i: comando para instalar
v: imprime mensajes del progreso de la instalación
h: muestra el progreso de la instalación mediante signos #

Un ejemplo de instalación de paquetes rpm sería:

[11] *AMD (*Advanced Micro Devices*)*

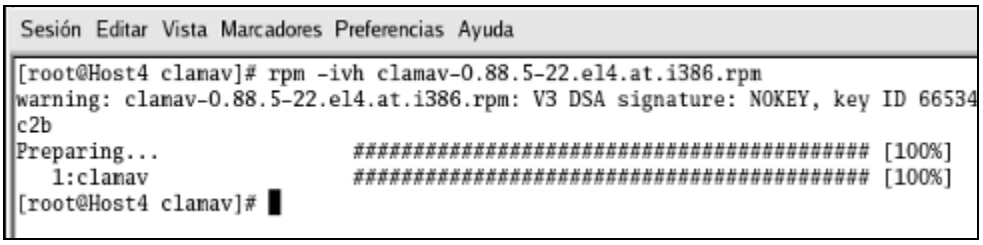


Figura 2.34 Instalación de paquetes RPM

Todos los paquetes rpm deben ser del tipo de arquitectura i386 para tener una correcta instalación de cualquier software adicional.

Como segunda opción para realizar una instalación de software adicional en Linux, se tiene los paquetes de tipo *tar.gz*.

Este tipo extensión es comparable con los archivos tipo .zip o .rar de Windows.

Una vez que obtenemos un archivo de estas características, se debe descomprimir de tal manera que se extraiga todos los archivos y carpetas contenidos en él y se pueda trabajar con su contenido.

Para realizar dicha extracción se debe ejecutar lo siguiente:

tar –xvzf <archivo.tar.gz>

donde:

tar: comando básico para ejecutar acciones en archivos con extensión *.tar.gz.*

x: extrae archivos comprimidos

v: listado de archivos procesados

z: filtra el archivo comprimido a través de gzip

f: Crea automáticamente una carpeta para la descompresión de archivos

Un ejemplo de extracción de paquetes .tar.gz sería:

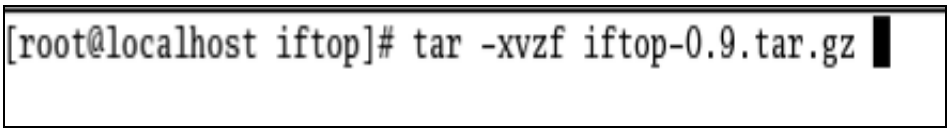


Figura 2.35 Extracción de paquetes tar.gz

Una vez extraídos los archivos y carpetas incluidas, automáticamente se crea una carpeta la cual contiene toda la información para poder instalar el software.

Figura 2.36 Paquetes extraídos

En este caso la carpeta creada es llamada iftop-0.9, dentro de ella se encuentran detalladas las instrucciones para la instalación del software. Una instalación típica que se suele hacer se explica a continuación:

Dentro de la carpeta se encuentra lo siguiente:

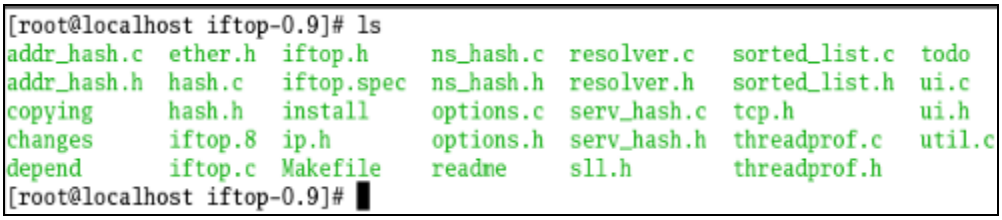


Figura 2.37 Contenido de paquetes extraídos

Todo lo necesario para instalar el software se encuentra explicado en el archivo *install.*

Para este caso, como ejemplo, (puede haber variaciones en otro tipo de softwares) se deben ejecutar los siguientes comandos:

./Makefile

make

make install

Con esto el software queda instalado de manera correcta. Hay que fijarse que no se produzcan errores al instalar debido a falta de paquetes adicionales o librerías faltantes, en cuyo caso habrá que instalar primero.

Como paquetes adicionales que funcionan similar a los de tipo tar.gz están los de tipo tar.bz y tar.bz2.

Al igual que tar.gz, estos archivos también se encuentran comprimidos pero en otro tipo de formato. Por ejemplo para descomprimir archivos de tipo *tar.bz2* se debe ejecutar el comando:

tar xvjf <archivo.tar.bz2>

La diferencia con tar.gz está en que para este tipo se utiliza xvzf y para tar.bz2 se usa xvjf.

Para archivos tar.bz se debe ejecutar lo siguiente:

tar zvjf <archivo.tar.bz>

Una vez que se extraen los archivos incluidos, se debe chequear el documento *install* en donde se explicará el procedimiento para la correcta instalación de un software determinado.

2.2.3 Creación de respaldos

Para la creación de respaldos, se va a considerar realizar un backup de los principales archivos de configuración del sistema operativo, es decir aquellos archivos sensibles de los cuales dependa el correcto funcionamiento del servidor de aplicaciones.

En caso de pérdida de archivos, borrado por error o una modificación incorrecta irrecuperable, automáticamente se podrá recurrir a los archivos anteriores.

Estos respaldos se los realizará de manera automática todos los días laborables de la semana a las 14h00.

Los archivos a ser respaldados se indican a continuación:

Tabla. 2.2. Archivos de respaldo

Archivo	Ubicación	Funcionalidad
squid.conf	/etc/squid	Servidor Proxy
dhcpd.conf	/etc	Servidor dhcp
sendmail.cf	/etc/mail	Servidor de correo electrónico
sendmail.mc	/etc/mail	Servidor de correo electrónico
network	/etc/sysconfig	Servicios de red
resolv.conf	/etc	Servicios de red
ifcfg-eth0	/etc/sysconfig/network-scripts	Servicios de red
ifcfg-eth1	/etc/sysconfig/network-scripts	Servicios de red
iptables	/etc/sysconfig	Firewall, nat y enmascaramiento
dansguardian.conf	/etc/dansguardian	Restricción de accesos Web indebidos
httpd.conf	/etc/httpd/conf	Servidor Web
named.conf	/etc	Servidor DNS

La actualización automática se realiza de la siguiente manera:

Como primer paso se crea un pequeño script, el cual debe estar ubicado en */etc/init.d* debido a que aquí se encuentran todos los servicios que Linux ejecuta.

Este será considerado como un servicio más de Linux y se podrá ejecutar manualmente mediante el comando:

/etc/init.d/respaldos start

El archivo creado tiene el nombre de *respaldos* y cuenta con los permisos necesarios para su ejecución.

Para establecer todos los permisos de lectura, escritura y ejecución tanto a dueño, grupo y otros se ejecuta lo siguiente:

chmod 777 respaldos

donde:

chmod: comando para establecer permisos a un archivo

777: establece que el archivo tendrá todos los permisos

La configuración del script respaldos se muestra a continuación:

```
#!/bin/bash
cp /etc/squid/squid.conf /home/respaldos
cp /etc/dhcpd.conf /home/respaldos
cp /etc/mail/sendmail.cf /home/respaldos
cp /etc/mail/sendmail.mc /home/respaldos
cp /etc/sysconfig/network /home/respaldos
cp /etc/resolv.conf /home/respaldos
cp /etc/sysconfig/network-scripts/ifcfg-eth0 /home/respaldos
cp /etc/sysconfig/network-scripts/ifcfg-eth1 /home/respaldos
cp /etc/sysconfig/iptables /home/respaldos
cp /etc/dansguardian/dansguardian.conf /home/respaldos
cp /etc/httpd/conf/httpd.conf /home/respaldos
cp /etc/named.conf /home/respaldos
```

Figura 2.38 Script de configuración para respaldos

Como se puede ver claramente, todos los comandos únicamente realizan la función de copiar los archivos de configuración a la carpeta /home/respaldos.

Adicionalmente, para establecer que los respaldos se ejecuten automáticamente se debe configurar una tarea programada.

En los sistemas operativos Linux, esto se lo hace mediante un software llamado *crontab*. Para poder acceder a la configuración del mismo, se debe ejecutar, como root, el comando: *crontab –e*

A continuación se obtendrá un editor en el que se puede añadir líneas al fichero de crontab, una por cada tarea que se desee programar.

Cuando se añada una entrada al crontab, se lo hace mediante una sola línea y con el siguiente formato:

[minutos] [hora] [día] [mes] [dia_de_semana] [comando]

Entonces, para el caso planteado, se ejecutará la línea de comando del crontab como se muestra a continuación:

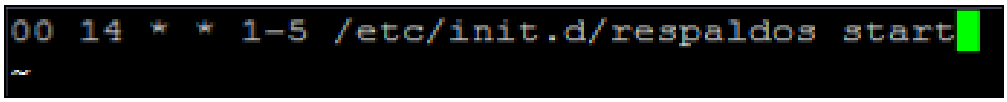


Figura 2.39 Configuración Crontab

En donde se indica que los respaldos se realizarán de lunes a viernes (1-5) a las 14h00.

2.2.4 Actualización del servidor

La actualización del servidor de aplicaciones es uno de los aspectos más importantes que se debe realizar. Este servicio se configura de tal manera que se ejecute de forma automática todas las noches por defecto a las 4 horas.

El servicio, el cual viene incluido en los paquetes de instalación de Linux, se llama yum.

Para poder realizar todo tipo de actualizaciones, el servidor debe estar conectado a Internet, puesto que dichas actualizaciones se las descarga de los sitios Web de CentOS.

Por tanto el servicio yum debe estar activado para realizar las tareas antes mencionadas.

Es recomendable cuando se instala el sistema operativo Linux, realizar una actualización total, para esto se ejecuta como root lo siguiente:

yum check-update

Automáticamente el servidor se conectará con los repositorios de CentOS y chequeará las actualizaciones disponibles.

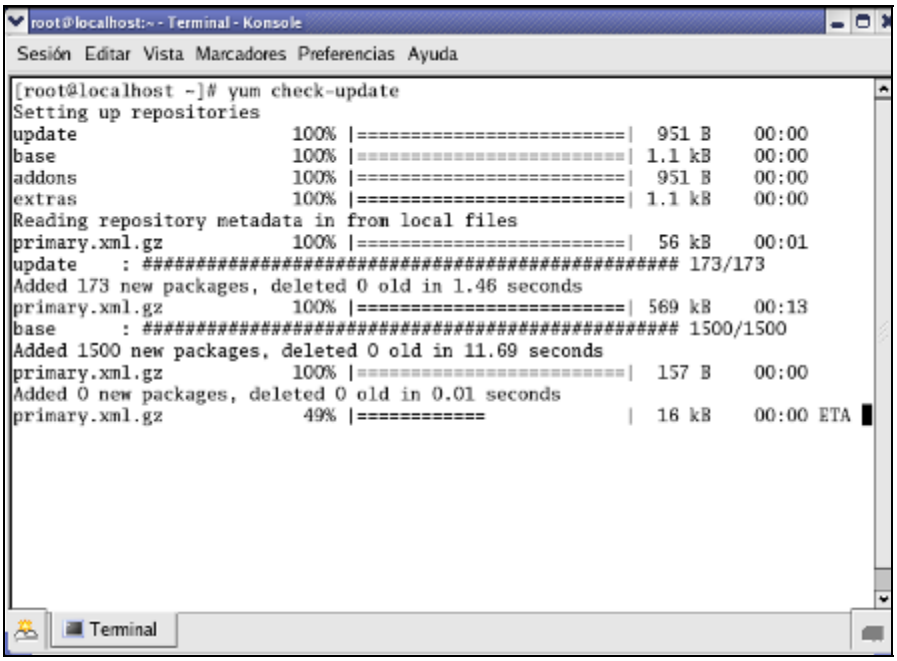


Figura 2.40 Chequeo de actualizaciones

Como siguiente paso se ejecuta el comando *yum update* de tal manera que el servidor empiece a descargar las actualizaciones antes chequeadas e instalarlas en el sistema operativo.

Eventualmente se podrá crear una tarea programada para que el servidor se actualice a una fecha y hora determinada, como se explicó en el ítem anterior.

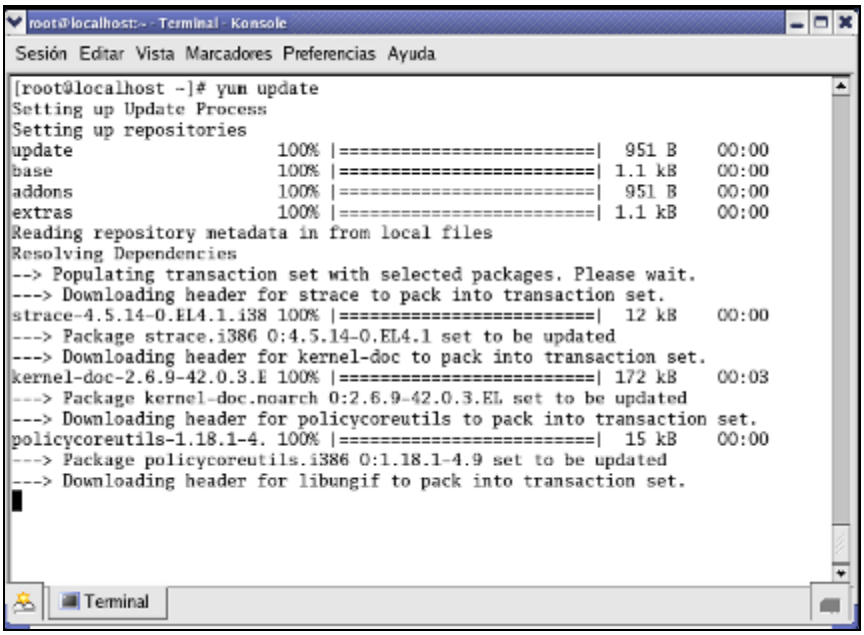


Figura 2.41 Actualizaciones yum

Otra manera mediante la cual se puede realizar el proceso de actualización es mediante el manejo del software *up2date*.

La versión incluida en el sistema no requiere de registrarse en Red Hat, simplemente definir en /etc/sysconfig/rhn/sources los depósitos apt-get o yum que mejor se crea convenientes y ejecutar up2date para instalar cualquier paquete de software incluido en cualquiera de los depósitos.

El primer paso a seguir es ejecutar el comando *up2date –l* con la finalidad de listar los paquetes disponibles para instalar.

Al ejecutar dicho comando se presentará una pantalla como la que se indica a continuación:

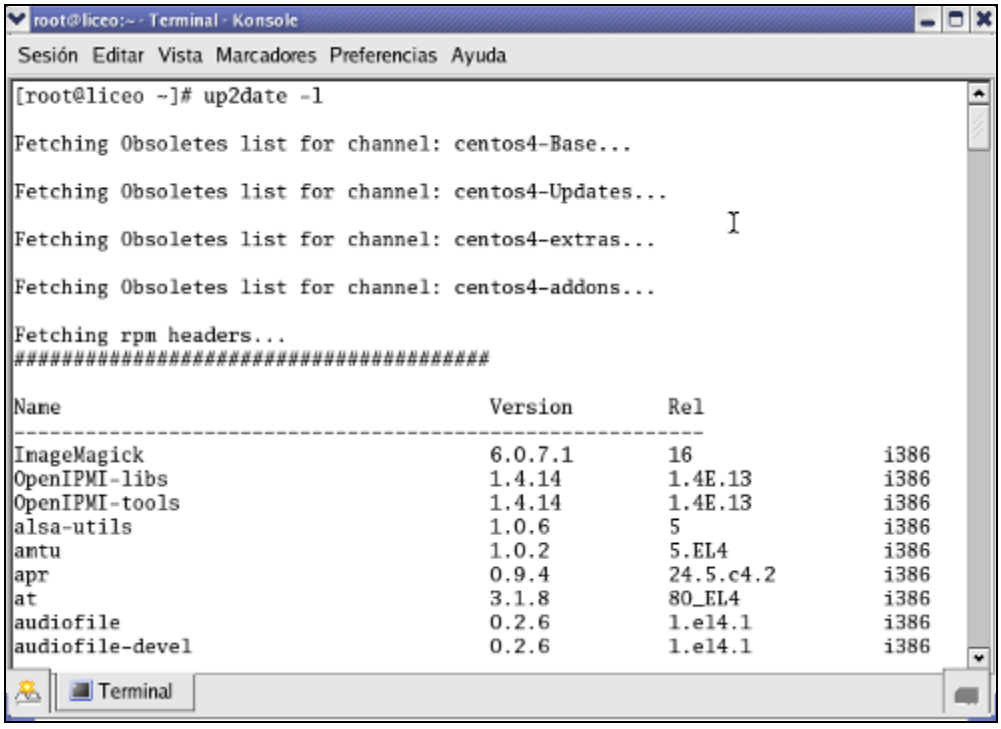
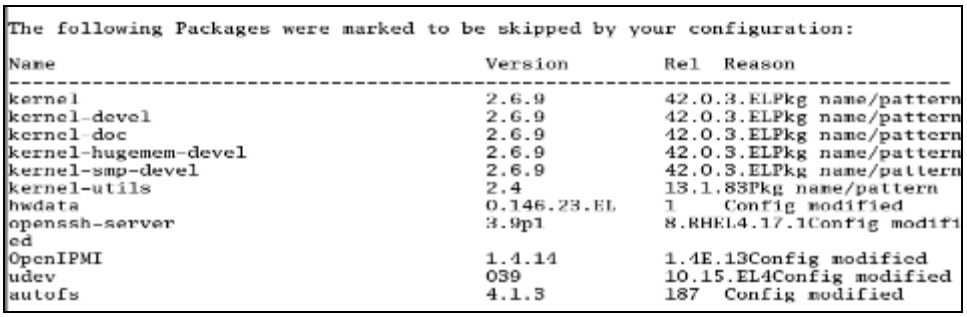


Figura 2.42 Paquetes disponibles para instalar

Una vez que el programa accede a los repositorios de CentOS, muestra una lista de paquetes a ser actualizados y adicionalmente otra lista de paquetes que son marcados para realizar una posterior revisión de la configuración, como se muestra a continuación:



```
The following Packages were marked to be skipped by your configuration:

Name                                    Version        Rel  Reason
-------------------------------------------------------------------------------
kernel                                  2.6.9          42.0.3.ELPkg name/pattern
kernel-devel                            2.6.9          42.0.3.ELPkg name/pattern
kernel-doc                              2.6.9          42.0.3.ELPkg name/pattern
kernel-hugemem-devel                    2.6.9          42.0.3.ELPkg name/pattern
kernel-smp-devel                        2.6.9          42.0.3.ELPkg name/pattern
kernel-utils                            2.4            13.1.83Pkg name/pattern
hwdata                                  0.146.23.EL    1    Config modified
openssh-server                          3.9p1          8.RHEL4.17.1Config modifi
ed
OpenIPMI                                1.4.14         1.4E.13Config modified
udev                                    039            10.15.EL4Config modified
autofs                                  4.1.3          187  Config modified
```

Figura 2.43 Paquetes para posterior revisión

Una vez realizado lo anterior, se debe ejecutar el comando *up2date –u* para iniciar con la actualización de los paquetes antes listados.

Eventualmente se podrá crear una tarea programada para que el servidor se actualice a una fecha y hora determinada.

2.3 SERVICIOS

2.3.1 Red

2.3.1.1 Descripción

Uno de los aspectos más importantes a ser considerados en la configuración del servidor de aplicaciones bajo plataforma Linux constituyen los servicios de red, puesto que a partir de una red correctamente configurada las aplicaciones adicionales poseerán una muy buena base para su correcto funcionamiento.

Para realizar la comunicación y transmisión de datos entre varios computadores se utiliza el direccionamiento IP dentro de lo que constituye la parte lógica para establecer conectividad entre PC's. Una **dirección IP** es un número que identifica de manera lógica y jerárquicamente a una interfaz de una computadora dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen una *dirección IP fija o también llamada estática*. Los servidores de correo, dns, ftp públicos, servidores web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se facilita su ubicación. Las máquinas

tienen una gran facilidad para manipular y jerarquizar la información numérica, y son altamente eficientes para hacerlo y ubicar direcciones IP, sin embargo, los seres humanos debemos utilizar otra notación más fácil de recordar y utilizar, tal es el caso URLs[12] y resolución de nombres de dominio DNS como se explicará con mayor detalle más adelante.

Existen 3 clases de direcciones IP. En la siguiente tabla se muestra un resumen acerca de dichas clases la cual incluye información adicional como se muestra a continuación:

Tabla. 2.3. Clases de direcciones IP

Clase	Rango	Número de redes	Número de hosts	Máscara de red	Broadcast
A	1.0.0.0 – 126.255.255.255	126	$2^{24} – 2$	255.0.0.0	x.255.255.255
B	128.0.0.0 – 191.255.255.255	16382	$2^{16} - 2$	255.255.0.0	x.x.255.255
C	192.0..0.0 – 223.255.255.255	2097150	$2^{8} - 2$	255.255.255.0	x.x.x.255
D	224.0.0.0 – 239.255.255.255				
E	240.0.0.0 – 255.255.255.255				

Las clases D y E son para direcciones de multicast y reservadas para uso futuro respectivamente.

No se ha considerado el rango desde 127.0.0.0 a 127.255.255.255 debido a que está reservado y son llamadas direcciones de loopback, las cuales son utilizadas para pruebas de funcionamiento correcto de las tarjetas de red de los computadores.

Adicionalmente se ha establecido otro tipo de clasificación de direcciones IP, en este caso son llamadas públicas y privadas.

Las direcciones IP públicas, como su nombre lo indica, se encuentran destinadas para su uso a nivel de aplicaciones y sitios de Internet hacia los cuales se puede acceder libremente. Estas se encuentran a lo largo de toda la gran red denominada Internet

[12] *URL (*las siglas URL en inglés quieren decir "Uniform Resource Locator," y se refiere al texto que identifica a una página web*)*

Las direcciones IP privadas, por el contrario, tienen su uso en redes de dicho tipo, es decir, se manejan a nivel interno como por ejemplo en hogares o sitios de trabajo.

Las direcciones IP públicas son únicas e irrepetibles, provocando cada vez una mayor escasez de las mismas; es por eso que en la actualidad se encuentra en estudio una nueva implementación de direccionamiento llamado IP versión 6.

Por el contrario, las direcciones IP privadas pueden ser repetidas sin ningún inconveniente en cualquier red de tipo privado, debido a que estas direcciones no son vistas desde la red Internet.

El rango de las direcciones IP privadas se detalla a continuación:

Tabla. 2.4. Rango de direcciones IP privadas

Clase	Tipo	Rango
A	Privado	10.0.0.0 a 10.255.255.255
B	Privado	172.16.0.0 a 172.31.255.255
C	Privado	192.168.0.0 a 192.168.255.255

Las direcciones IP públicas son todas aquellas que no se encuentran estipuladas como privadas y adicionalmente que se encuentren fuera del rango de multicast y las destinadas para uso futuro.

Para la configuración del servidor de aplicaciones, se ha considerado dos interfaces de red con dos tipos de direcciones: una pública para la salida a Internet y aplicaciones, y una privada para uso interno en la red.

La interfaz de red interna poseerá una dirección IP privada 192.168.100.1 y la interfaz de red externa poseerá una dirección IP pública 200.107.15.50.

2.3.1.2 Configuración del servicio

Existen 3 partes que se necesitan configurar en el servidor Linux para tener una correcta configuración de red. Como primer paso se deben configurar las interfaces de red, esto de lo hace ingresando a los archivos de configuración ifcfg-eth0 para el caso de la red interna e ifcfg-eth1 para acceder al Internet.

Estos 2 archivos se encuentran en:

/etc/sysconfig/network-scripts

Se accede a la configuración de cada uno de ellos utilizando el editor de texto **vi,** así:

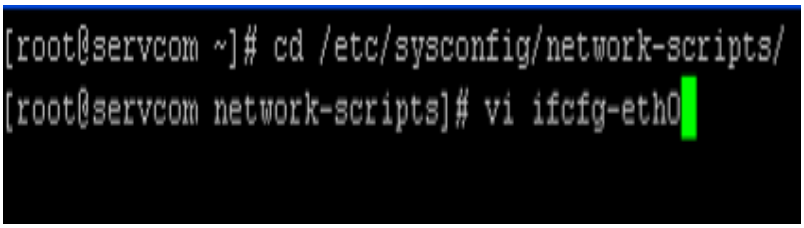


Figura. 2.44. Acceso a la configuración de eth0

Como primer paso se va a configurar la interfaz de red interna eth0 mediante la cual todas las computadoras del Liceo del Valle tendrán conectividad directa para salida a Internet.

Una vez que se ha colocado el comando *vi ifcfg-eth0* se mostrará una pantalla como la que se indica a continuación:

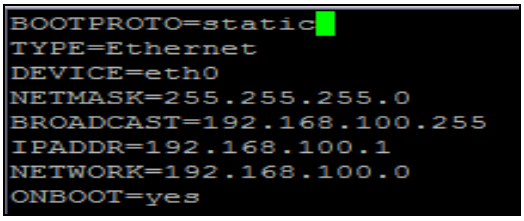


Figura. 2.45. Configuración tarjeta de red eth0

En donde:

BOOTPROTO: Tipo de configuración para la tarjeta de red (estático o mediante dhcp)

TYPE: Tipo de interfaz (En este caso Ethernet)

DEVICE: dispositivo eth0

NETMASK: Máscara de red

BROADCAST: Dirección de Broadcast

IPADDR: Dirección IP de la interfaz de red eth0

NETWORK: Red a la que pertenece la interfaz eth0

ONBOOT: Con el parámetro *yes* la interfaz de activará en cada inicio del sistema operativo

A continuación se determinarán los parámetros de configuración de la interfaz de red externa eth1 (la que se conecta directamente al dispositivo del ISP para la salida al Internet).

Para poder ingresar al archivo de configuración de la interfaz de red externa se debe digitar el comando *vi ifcfg-eth1* como usuario administrador dentro del directorio */etc/sysconfig/network-scripts/*, así:

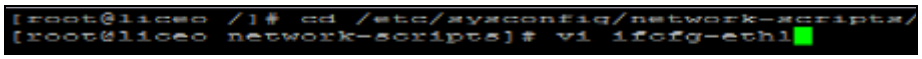


Figura. 2.46. Acceso a la configuración de eth1

Una vez colocado este comando, se presentará una pantalla como la que se indica a continuación:

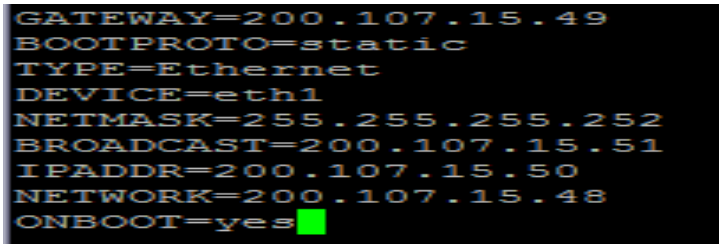


Figura. 2.47. Configuración tarjeta de red eth1

Todos los parámetros aquí configurados son dados por el proveedor de Internet. La única diferencia con la interfaz anterior está en que se ha incluido la puerta de enlace:
GATEWAY: Puerta de enlace para salida a Internet.

Como parámetros adicionales se deben configurar los DNS, direcciones IP que son dadas también por el ISP[13]. Para configurar estos parámetros se debe ingresar a */etc* y modificar el archivo *resolv.conf*, así:

[13] *ISP (*Internet Service Provider Proveedor de servicios de Internet*)*

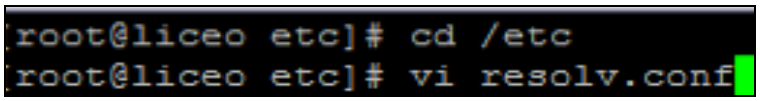


Figura. 2.48. Acceso a la configuración de los DNS

Se presentará la siguiente información:

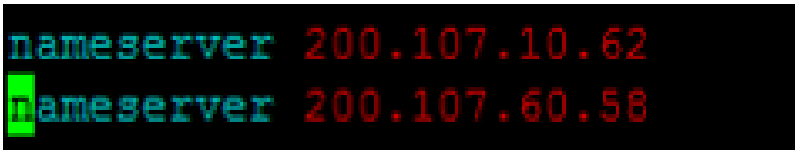


Figura. 2.49. Configuración DNS

En donde se encuentran colocadas las direcciones IP de los DNS las cuales son dadas por el ISP.

Una vez que son colocados todos estos parámetros se puede dar por terminada la configuración de la red tanto para el funcionamiento a nivel LAN como para la salida a Internet.

Es necesario reiniciar los servicios de red de la siguiente manera:

service network restart

Como una prueba se puede hacer un ping hacia una página Web en Internet y adicionalmente a una dirección IP de una PC en la red LAN.

En caso de existir errores se debe revisar uno a uno los archivos de configuración indicados anteriormente.

2.3.2 DHCP

2.3.2.1 Descripción

DHCP es un de protocolo de asignación de direcciones IP en forma dinámica que por medio de un servidor provee los parámetros de configuración a las computadoras conectadas a la red informática que los requieran (máscara, puerta de enlace y otros).

DHCP se basa en el modelo Cliente-Servidor. Utiliza un protocolo de comunicaciones muy sencillo (basado en UDP sobre IP).

Funciona normalmente en servidores y también se encuentra en dispositivos de red como routers, access points, equipos VPN[14], etc. que les permiten a usuarios múltiples acceder a Internet.

DHCP usa un concepto de "alquiler" o cantidad de tiempo que una dirección IP estará válida para un computador. Este tiempo de arrendamiento dependerá en qué tanto requerirá el usuario la conexión a Internet en esa ubicación en particular. Es especialmente útil en instalaciones donde los usuarios de los PC cambian con frecuencia. Con tiempos cortos, el DHCP[15] puede configurar dinámicamente las redes en las cuales hay más computadores que direcciones IP. El protocolo también soporta IP estáticos para equipos que necesitan una dirección IP fija, como un servidor Web.

2.3.2.2 Configuración del servicio

Para realizar la configuración del servicio DHCP[15] el primer paso es instalarlo, lo cual se realizó en el proceso de instalación del sistema operativo como se explicó anteriormente.

A continuación, se modifica el archivo de texto llamado **dhcpd.conf** en la carpeta **/etc** como se muestra a continuación:

- Como usuario administrador (root) se ingresa a la carpeta /etc así:

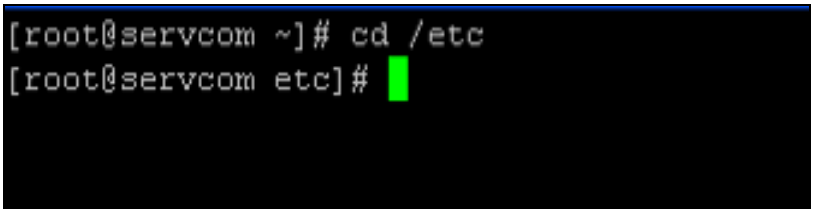


Figura. 2.50. Ingreso a la carpeta /etc

- Se edita el archivo de texto dhcpd.conf

[14] VPN (Virtual Private Networks, en castellano red privada virtual)
[15] *DHCP (*Dynamic Host Configuration Protocol*)*

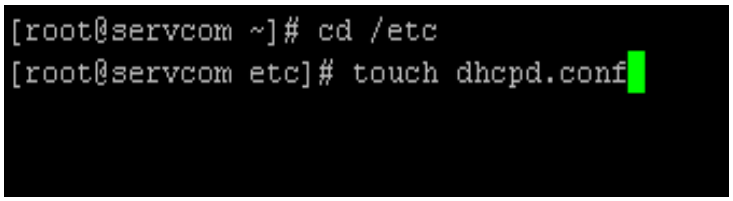


Figura. 2.51. Creación del archivo dhcpd.conf

- Se ingresa al archivo para poderlo configurar, se lo hace de la siguiente manera:

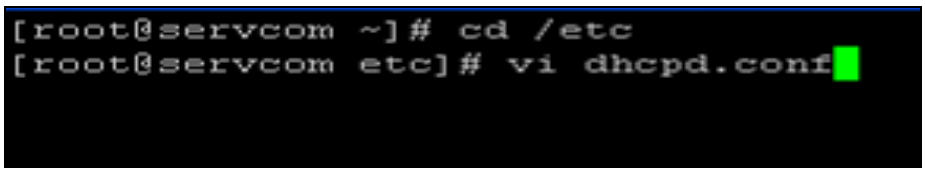


Figura. 2.52. Ingreso al archivo dhcpd.conf

Una vez que se ingresa al archivo de configuración, los comandos que se asocian a este servicio se muestran a continuación:

option domain-name "liceo.com";
option domain-name-servers 157.100.98.2, 157.100.98.4;
default-lease-time 86400;
max-lease-time 172000;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.100.255;
option routers 192.168.100.1;
ddns-update-style ad-hoc;
subnet 192.168.100.0 netmask 255.255.255.0{
range 192.168.100.170 192.168.100.220;
}

A continuación se explicará el significado de los comandos indicados:

option domain-name	nombre del dominio
option domain-name-servers	Servidores DNS
default-lease-time	tiempo por defecto de arrendamiento de unaIP
max-lease-time	máximo tiempo de arrendamiento de una IP
option subnet-mask	mascara de subred

option broadcast-address	dirección IP de broadcast
option routers	dirección IP del servidor de aplicaciones
ddns-update-style interim;	se incluye por defecto para el funcionamiento
subnet 192.168.0.0	subred a ser usada en la red interna
netmask 255.255.255.0	máscara de subred
range	rango de direcciones IP a distribuirse

Se pueden asignar direcciones IP fijas a clientes determinados en la red, como por ejemplo, se va a asignar la IP 192.168.0.101 a una PC del laboratorio, se lo hace de la siguiente manera:

```
host CCPC1{
    hardware ethernet 00:11:5B:44:E7:03;
    fixed-address 192.168.100.101;
 }
```

Para poder asignar una IP fija mediante el servicio dhcp a una PC determinada, se lo hace mediante la autenticación por dirección MAC, lo cual se encuentra indicado por medio del parámetro *hardware-ethernet.*

La línea indicada *host* corresponde al nombre del computador al cual se le dará una dirección IP fija. Se puede colocar cualquier nombre según nuestro criterio.

La configuración total del archivo *dhcpd.conf* incluye la asignación de direcciones IP fijas a 26 computadores adicionales dentro de la red del Liceo del Valle, lo cual se lo hace de la misma manera que lo indicado con el *host CCPC1.*

El principal objetivo de realizar este tipo de configuraciones es para posteriormente establecer parámetros de restricciones de navegación.

Una vez realizadas todas las configuraciones indicadas anteriormente, se guarda el archivo y se inicia el servicio dhcp de la siguiente manera:

service dhcpd start

2.3.3 DNS

2.3.3.1 Descripción

En la década de los 70, la red Arpanet, antecesora de Internet, estaba formada por un número pequeño de servidores. En un sencillo archivo HOST.TXT figuraban los pocos centenares de servidores que la componían. Para realizar cambios en este fichero, los administradores de los diferentes servidores enviaban las modificaciones por correo electrónico y recibían el nuevo fichero HOST.TXT actualizado por FTP. El organismo encargado de mantener el fichero era SRINIC. Con el crecimiento de Arpanet la capacidad de NIC para mantener el fichero original se vió desbordada. Además apareció el problema de servidores con nombre duplicado. En 1984 se creó el sistema de nombres de dominio DNS (Domain Name System), documentado en las RFC 882 y 883.

El servicio DNS (Domain Name System) es un conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Como ejemplo del sistema de nombres de dominio se puede citar al sitio Web www.google.com, el cual corresponde a la dirección IP 64.233.179.104.

De esta manera se evita recordar un sin número de direcciones IP públicas que existen en Internet y facilita el uso del mismo mediante la traducción de dichas direcciones a nombres conocidos y mucho mas fáciles de recordar.

El sistema de nombres de dominios en Internet es un sistema distribuido, jerárquico, replicado y tolerante a fallas. Aunque parece muy difícil lograr todos esos objetivos, la solución no es tan compleja en realidad. El punto central se basa en un árbol que define la jerarquía entre los dominios y los sub-dominios. En un nombre de dominio, la jerarquía se lee de derecha a izquierda. Por ejemplo, en google.com.ec, el dominio más alto es ec.

Cada componente del dominio (y también la raíz) tiene un servidor primario y varios servidores secundarios. Todos estos servidores tienen la misma autoridad para responder por ese dominio, pero el primario es el único con derecho para hacer modificaciones en él. Por ello, el primario tiene la copia maestra y los secundarios copian la información desde él. El servidor de nombres es un programa que típicamente es una versión de BIND (*Berkeley Internet Name Daemon*).

La raíz del sistema de dominios es servida por algunos servidores ``bien conocidos''. Todo servidor de nombres debe ser configurado con la lista de los servidores raíz bien conocidos (en general lo vienen de fábrica). Estos servidores dicen qué dominios de primer nivel existen y cuales son sus servidores de nombres. Recursivamente, los servidores de esos dominios dicen que sub-dominios existen y cuales son sus servidores.

A un nombre de dominio que incluye todos los nodos hasta el raíz se le denomina nombre de dominio completamente cualificado (FQDN Full Cuallified Domain Name). En Internet por debajo del raíz los primeros nodos corresponden normalmente a países u organizaciones internacionales. Cada país tiene su propio dominio, y además existen otros para otro tipo de organizaciones. En el caso de Estados Unidos, la mayoría de los dominios pertenecen por razones históricas a los dominios edu, com, mil y gov. Otros dominios que dependen del raíz son:

· int para organizaciones internacionales, como la OTAN (nato.int)
· org para organizaciones no gubernamentales
· net para otras redes que se han unido a Internet
· arpa para la transición de Arpanet a Internet

y los diferentes países, identificados por el código de dos letras ISO3166, salvo Gran Bretaña, que usa uk. Dentro de cada dominio hay una organización que decide la estructura de dominios. Por ejemplo en Ecuador es NIC.ec.

2.3.3.2 Dominios: Tipos y contratación.

Los tipos de dominios que poseen un mayor uso en la red se detallan a continuación:

Dominios .com: Son los más acertados para empresas u organizaciones con ánimo de lucro. La red está llena de .com, por lo que registrando un dominio este tipo, una determinada organización adquirirá un aspecto de globalidad.

Dominios .org: Para todo tipo de organizaciones sin ánimo de lucro.

Dominios .net: Usados mayoritariamente por empresas de Internet y Telecomunicaciones.

Dominios .edu: Usados para fines educativos

Dominios .mil: Exclusivamente para todo tipo de organizaciones militares.

Dominios .gov: Para los gobiernos

Dominios estatales

Dominios .ec: Relativos al territorio ecuatoriano.

Dominio .au: Australia

Dominio .fr: Francia

Dominio .de: Alemania

Dominio .uk: Reino Unido. , etc.

Otros dominios

En esta categoría se incluyen los nuevos dominios que se han incorporado recientemente a Internet:

Dominios genéricos Multilingües: Son dominios .com, .org y .net que llevan eñes, acentos, u otros caracteres especiales.

Dominios .tv: Usados en empresas de vídeo, cine y televisión principalmente.

Dominios .info: Destinados principalmente para empresas de información, periódicos, revistas, etc.

Dominios .biz: Proviene de la pronunciación del inglés "business", por lo que están dedicados a actividades comerciales y de negocios. Es lo mismo que el .com, pero para la zona de Europa.

Dominios .cc: Esta extensión tiene un especial interés para aquellos que pretenden conseguir un dominio global y no tienen posibilidad de conseguir el .com que desean.

Dominios .ws: Las siglas .ws se identifican con Web Site, por lo que se trata de una magnífica opción para todo tipo de sitios web. Además, debido a su novedad, es mucho más probable conseguir el dominio deseado.

Dominios .name: Proviene del inglés "name" que significa "nombre", por lo que se trata de una opción totalmente nueva para registrar un nombre propio o un apodo.

Dominios .pro: Para uso específico reservado a profesionales de determinadas categorías, agrupados en subdominios. Ejemplo: .med.pro (médicos). Deberán acreditar su pertenencia al colegio u organización profesional correspondiente.

Dominios .aero: De uso restringido para la industria de los servicios aéreos: compañías aéreas, aeronáuticas, aeropuertos y servicios aéreos.

Dominios .coop: Reservado a las cooperativas y hace falta demostrar la cualidad de cooperativa a través de las organizaciones locales correspondientes.

Dominios .museum: Dominio de uso restringido para los museos. Permite en un segundo nivel el nombre del museo que se trate. (prado.museum, picasso.museum)

2.3.4 Web

2.3.4.1 Descripción

Un servidor web es un programa que implementa el protocolo HTTP (*hypertext transfer protocol*). Este protocolo está diseñado para transferir hipertextos, páginas web o páginas HTML (hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

Sin embargo, el hecho de que HTTP y HTML estén íntimamente ligados no debe dar lugar a confundir ambos términos. HTML es un formato de archivo y HTTP es un protocolo.

Un servidor Web es un programa que ejecuta de forma continua en un ordenador, manteniéndose a la espera de peticiones por parte de un cliente (un navegador de Internet)

y que contesta a estas peticiones de forma adecuada, sirviendo una página Web que será mostrada en el navegador o mostrando el mensaje correspondiente si se detectó algún error.

Al iniciar una petición hacia una página Web determinada, se debe distinguir entre las aplicaciones ejecutadas en el lado del cliente y las ejecutadas en el lado del servidor:

Aplicaciones en el lado del cliente: el cliente Web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java o Javascript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Normalmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje javascript y java, aunque pueden añadirse más lenguajes mediante el uso de plugins

Aplicaciones en el lado del servidor: el servidor Web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código HTML; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor suelen ser la opción por la que se opta en la mayoría de las ocasiones para realizar aplicaciones Web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad adicional, como sí ocurre en el caso de querer ejecutar aplicaciones javascript o java. Así pues, cualquier cliente dotado de un navegador Web básico puede utilizar este tipo de aplicaciones.

Uno de los servidores Web más populares del mercado, y el más utilizado actualmente, es Apache, de código abierto y gratuito, disponible para Windows y GNU/Linux, entre otros.

2.3.4.2 Configuración del servicio

Apache es un servicio que por fortuna solo es necesario instalar e iniciar. No requiere modificaciones adicionales para su funcionamiento básico. Para añadir el servicio a los servicios que inician junto con el sistema, solo basta ejecutar:

chkconfig httpd on

Para iniciar el servicio por primera vez, solo basta utilizar:

service httpd start

Para reiniciar el servicio, considerando que se interrumpirán todas las conexiones establecidas en ese momento, solo basta utilizar:

service httpd restart

Si el servicio ya está trabajando, también puede utilizar **reload** a fin de que Apache vuelva a leer y cargar la configuración sin interrumpir el servicio, y, por ende, las conexiones establecidas.

service httpd reload

Para detener el servicio, solo basta utilizar:

service httpd stop

2.3.5 Proxy

2.3.5.1 Descripción

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (p.ej.: una página Web) en una cache que permita acelerar sucesivas consultas coincidentes.

Un proxy HTTP es una máquina que recibe peticiones de páginas Web de otra máquina. El proxy, negocia esta petición, a su vez, con el servidor Web adecuado, obtiene la página solicitada y retorna el resultado.

Como se indicó anteriormente un servidor proxy puede tener un caché con las páginas recibidas, de modo que si otra máquina solicitase una dirección ya visitada con anterioridad por cualquier máquina de la red, le enviará la copia local que reside en el caché. Eso permite un uso eficiente del ancho de banda y un menor tiempo de respuesta.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Los proxies Web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA[16]. Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

Proxies transparentes

Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración.

Un proxy transparente combina un servidor proxy con NAT de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de Internet.

[16] *PDA (*Personal Digital Assistant, (Ayudante personal digital)*)*

2.3.5.2 Configuración del servicio

La configuración básica del servicio Proxy Squid se la debe realizar en el archivo de configuración *squid.conf* ubicado en */etc/squid.*

Existen un gran número de parámetros, de los cuales se recomienda configurar los siguientes:

http_port:

De acuerdo a las asignaciones hechas por IANA[17] y continuadas por la ICANN[18], los Puertos Registrados (rango desde 1024 hasta 49151) recomendados para Servidores Intermediarios (Proxies) pueden ser el 3128 y 8080 a través de TCP.

De modo predefinido Squid utilizará el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.

Se debe localizar la sección de definición de http_port, y especificar:

 # Default: http_port 3128

http_port 3128

cache_dir

Este parámetro se utiliza para establecer que tamaño se desea que tenga el caché en el disco duro para Squid.

De modo predefinido Squid utilizará un caché de 100 MB, de modo tal se encontrará la siguiente línea:

cache_dir ufs /var/spool/squid 100 16 256

Se puede incrementar el tamaño del caché hasta donde lo desee el administrador. Mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se utilizará menos el ancho de banda. La siguiente línea establece un caché de 1000 MB:

[17] *IANA (*Internet Assigned Number Authority. Autoridad de Asignación de Números en Internet)

[18] ICANN (Internet Corporation for Assigned Names and Numbers o Corporación de Internet para la Asignación de Nombres)

cache_dir ufs /var/spool/squid 1000 16 256

Los números 16 y 256 significan que el directorio del caché contendrá 16 directorios subordinados con 256 niveles cada uno.

Es muy importante considerar que si se especifica un determinado tamaño de caché y éste excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente.

cache_mem

El parámetro cache_mem establece la cantidad ideal de memoria para lo siguiente:

- Objetos en tránsito.
- Objetos frecuentemente utilizados.
- Objetos negativamente almacenados en el caché.

datos de estos objetos se almacenan en bloques de 4 Kb. El parámetro cache_mem especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad

De modo predefinido se establecen 8 MB. Se puede especificar una cantidad mayor si así se considera necesario, dependiendo esto de los hábitos de los usuarios o necesidades específicas adicionales.

Si se posee un servidor con al menos 128 MB de RAM, se recomienda establecer 16 MB como valor para este parámetro:

cache_mem 16 MB

Controles de acceso

Es necesario establecer Listas de Control de Acceso que definan una red o bien ciertas máquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.

Listas de control de acceso

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:

acl [nombre de la lista] src [lo que compone a la lista]

Si se desea establecer una lista de control de acceso que abarque a toda la red local, basta definir la IP correspondiente a la red y la máscara de la subred. Por ejemplo, si se tiene una red donde las máquinas tienen direcciones IP 192.168.0.**x** con máscara de subred 255.255.255.0, se puede utilizar lo siguiente:

acl redlocal src 192.168.1.0/255.255.255.0

Reglas de Control de Acceso

Estas definen si se permite o no el acceso hacia Squid. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso.

La sintaxis básica es la siguiente:
http_access [deny o allow] [lista de control de acceso]

En el siguiente ejemplo se considera una regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada redlocal establecida como 192.168.0.0/24:
acl redlocal src 192.168.0.0/255.255.255.0
http_access allow redlocal

También pueden definirse reglas valiéndose de la expresión !, la cual significa no. Pueden definirse, por ejemplo, dos listas de control de acceso, una denominada lista1 y otra denominada lista2, en la misma regla de control de acceso, en donde se asigna una expresión a una de estas. La siguiente establece que se permite el acceso a Squid a lo que comprenda lista1 excepto aquello que comprenda lista2
http_access allow lista1 !lista2

Caché con aceleración

Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché de Squid. Si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet.

Esta función permite navegar rápidamente cuando los objetos ya están en el caché de Squid y además optimiza enormemente la utilización del ancho de banda.

La configuración de Squid como Servidor Intermediario (Proxy) Transparente solo requiere complementarse utilizando una regla de iptables (la cual se explicará más adelante) que se encargará de redireccionar peticiones haciéndolas pasar por el puerto 3128.

Proxy Acelerado (Transparente)

En la sección HTTPD-ACCELERATOR OPTIONS deben habilitarse los siguientes parámetros:

httpd_accel_host virtual

httpd_accel_port 80

httpd_accel_with_proxy on

httpd_accel_uses_host_header on

La configuración de proxy transparente permite a los usuarios evitarse la colocación del servidor proxy y del puerto en cada browser de cada computador

Una vez terminada la configuración, se debe ejecutar el siguiente mandato para iniciar por primera vez Squid:

service squid start

2.3.5.3 Políticas de restricción de acceso a Internet

- **Por dirección MAC**

Todas las políticas de restricción adicionales deberán ser colocadas en la sección de listas de control de acceso así como también se ha de poner las respectivas reglas de control de acceso por cada lista.

Para establecer restricción por MAC address se ha de colocar como lista de control de acceso lo siguiente:

acl pc_mac arp 00:07:95:C4:DF:7E

y como regla (allow o deny):

http_access allow pc_mac

- **Por días y horas**

Para establecer restricción por días y horas se ha de colocar como lista de control de acceso lo siguiente:

acl acceso_hor_dia time M-T-W-H-F 9:00-17:00

y como regla (allow o deny):

http_access allow acceso_hor_dia

- **Por clave de acceso**

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.

Debe procederse a crear un fichero */etc/squid/passwd*, así:

touch /etc/squid/passwd

Este fichero debe hacerse legible y escribible solo para el usuario *squid*:

chmod 777 /etc/squid/passwds

chown squid:squid /etc/squid/passwd

A continuación deberemos dar de alta las cuentas que sean necesarias, utilizando el mandato *htpasswd, así:*

htpasswd /etc/squid/passwd dany

Una vez realizado esto, se deberá ingresar la clave de acceso para el usuario *"dany"*, la cual es pedida automáticamente luego de ingresado el comando anterior.

Se debe repetir el mismo proceso por cada cuenta de usuario a ser creada.

Lo siguiente será especificar que programa de autenticación se utilizará. Se debe localizar la sección que corresponde a la etiqueta *auth_param basic program* en el archivo squid.conf. Por defecto no está especificado programa alguno. Considerando que *ncsa_auth* se localiza en */usr/lib/squid/ncsa_auth*, se procede a añadir el siguiente parámetro:

auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd

/usr/lib/squid/ncsa_auth corresponde a la localización de el programa para autenticar y */etc/squid/passwd* al fichero que contiene las cuentas y sus claves de acceso.

El siguiente paso corresponde a la definición de una *Lista de Control de Acceso*. Se debe especificar una denominada *passwd* la cual se configurará para utilizar obligatoriamente la autenticación para poder acceder a Squid. Debe localizarse la sección de Listas de Control de Acceso y añadirse la siguiente línea:

acl password proxy_auth REQUIRED

Habiendo hecho lo anterior, se debe colocar la lista y la regla de control de acceso de la siguiente manera:

acl redliceo src 192.168.100.0/255.255.255.0
acl password proxy_auth REQUIRED
http_access allow redliceo password

Hay que tomar en cuenta que este tipo de configuración para acceso mediante clave no funciona con proxy transparente, es decir que se deberá configurar en cada computador del usuario la IP y el puerto del servidor proxy en cualquier browser que se utilice.

- **Por acceso a páginas Web determinadas**

Para este tipo de acceso se debe primero crear un archivo en /etc/squid, en el cual se establecerán los sitios Web a los cuales tendrá acceso un usuario determinado, así:

touch /etc/squid/sitios_permitidos

las páginas Web en este archivo se deberán colocar de la siguiente manera:

.pichincha.com
.iess.gov.ec
.sri.gov.ec

A continuación se deberá crear las listas de control de acceso y la regla de control de acceso, así:

acl redliceo src 192.168.100.0/255.255.255.0
acl liceo_dominios dstdomain”/etc/squid/sitios_permitidos”

http_access allow redliceo liceo_dominios

En este caso la red liceo tendrá acceso únicamente a los sitios determinados en el archivo *sitios_permitidos.*

En caso de necesitar que la redliceo ingrese a todas las páginas Web excepto las indicadas en un archivo llamado *sitios_denegados* se deberá colocar las listas y la regla de control de acceso de la siguiente manera:

acl redliceo src 192.168.100.0/255.255.255.0
acl liceo_dominios dstdomain"/etc/squid/sitios_denegados"
http_access allow redliceo !liceo_dominios

Hay que tomar en cuenta el signo ! delante de *liceo_dominios* en la regla de control de acceso. Este signo representa la negación del acceso de la *redliceo* a las páginas Web colocadas en el archivo sitios_denegados

2.3.6. Correo Electrónico (Sendmail)

2.3.6.1 Descripción

Correo electrónico, o en inglés e-mail, es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos (normalmente por Internet). Junto con los mensajes también pueden ser enviados ficheros como paquetes adjuntos.

Para que una persona pueda enviar un correo a otra, ambas han de tener una dirección de correo electrónico. Esta dirección la tiene que dar un proveedor de correo, que son quienes ofrecen el servicio de envío y recepción. El procedimiento se puede hacer desde un programa de correo o desde un correo Web.

El envío de un mensaje de correo es un proceso largo y complejo. Éste es un esquema de un caso típico:

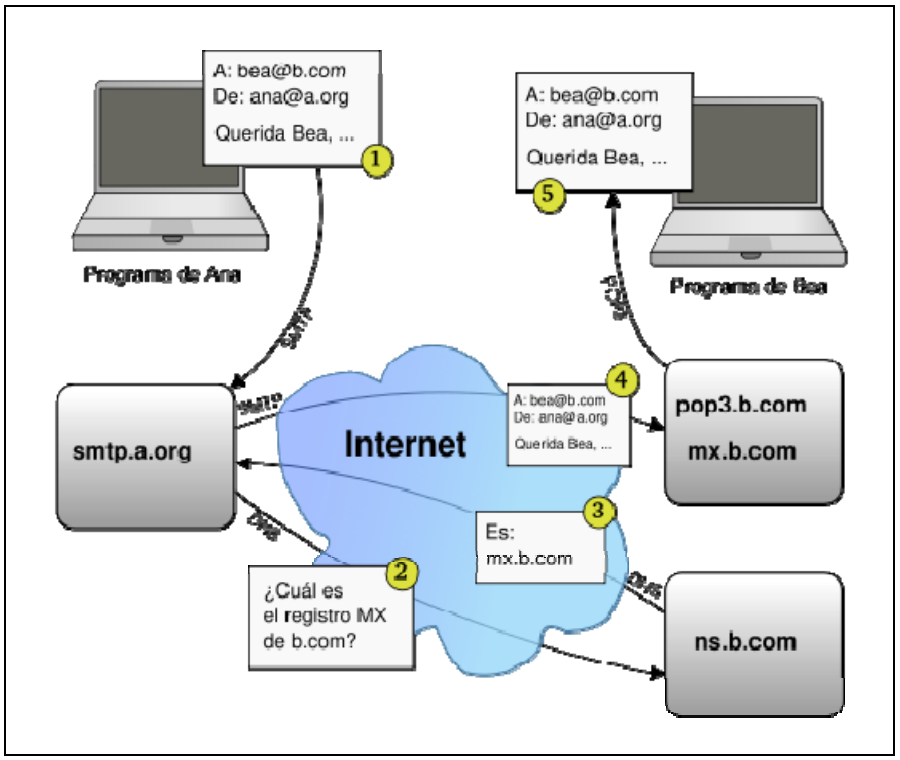


Figura. 2.53. Esquema de envío de e-mail

En este ejemplo ficticio, *Ana* (**ana@a.org**) envía un correo a *Bea* (**bea@b.com**). Cada persona está en un servidor distinto (una en a.org, otra en b.com), pero éstos se pondrán en contacto para transferir el mensaje. Por pasos:

1. *Ana* escribe el correo en su programa cliente de correo electrónico. Al darle a *Enviar*, el programa contacta con el servidor de correo usado por *Ana* (en este caso, smtp.a.org). Se comunica usando un lenguaje conocido como protocolo SMTP[19]. Le transfiere el correo, y le da la orden de enviarlo.

2. El servidor SMTP ve que ha de entregar un correo a alguien del dominio b.com, pero no sabe con qué ordenador tiene que contactar. Por eso consulta a su servidor DNS (usando el protocolo DNS), y le pregunta que quién es el encargado de gestionar el correo del dominio b.com. Técnicamente, le está preguntando el registro MX asociado a ese dominio.

[19] *SMTP(*Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo)

3. Como respuesta a esta petición, el servidor DNS contesta con el nombre de dominio del servidor de correo de *Bea*. En este caso es mx.b.com; es un ordenador gestionado por el proveedor de Internet de *Bea*.

4. El servidor SMTP (smtp.a.org) ya puede contactar con mx.b.com y transferirle el mensaje, que quedará guardado en este ordenador. Se usa otra vez el protocolo SMTP.

5. Más adelante *Bea* aprieta el botón "*Recibir nuevo correo*" en su programa cliente de correo. Esto empieza una conexión, mediante el protocolo POP3[20] o IMAP[21], al ordenador que está guardando los correos nuevos que le han llegado. Este ordenador (pop3.b.com) es el mismo que el del paso anterior (mx.b.com), ya que se encarga tanto de recibir correos del exterior como de entregárselos a sus usuarios. En el esquema, *Bea* recibe el mensaje de *Ana* mediante el protocolo POP3.

Ésta es la secuencia básica, pero pueden darse varios casos especiales:

- Si ambas personas están en la misma red (una Intranet de una empresa, por ejemplo), entonces no se pasa por Internet. También es posible que el servidor de correo de *Ana* y el de *Bea* sean el mismo ordenador.

- *Ana* podría tener instalado un servidor SMTP en su ordenador, de forma que el paso 1 se haría en su mismo ordenador. De la misma forma, *Bea* podría tener su servidor de correo en el propio ordenador.

- Una persona puede no usar un programa de correo electrónico, sino un webmail. El proceso es casi el mismo, pero se usan conexiones HTTP al webmail de cada usuario en vez de usar SMTP o IMAP/POP3.

- Normalmente existe más de un servidor de correo (MX) disponible, para que aunque uno falle, se siga pudiendo recibir correo.

[20] *POP3 (*Post Office Protocol 3, Protocolo 3 de Correo)
[21] *IMAP (*Internet Message Access Protocol, Protocolo de Red de Acceso a Mensajes Electrónicos)

2.3.6.2 Configuración del servicio

El primer paso será crear usuarios a través de un método diferente a la manera tradicional, debido a que para utilizar el método de autenticación para SMTP, Sendmail utilizará SASL. Por tal motivo, el alta de cuentas de usuario de correo deberá de seguir el siguiente procedimiento:

useradd -s /sbin/nologin jcbv

Se debe asignar una clave de acceso en el sistema para permitir autenticar a través de los métodos PLAIN y LOGIN para autenticar SMTP y a través de los protocolos POP3 e IMAP:

passwd jcbv

Establecer dominios a administrar en el fichero /etc/mail/local-host-names del siguiente modo:

dominio.com
mail.dominio.com

Establecer dominios permitidos para poder enviar correo en:

```
vi /etc/mail/relay-domains
```

Por defecto, no existe dicho fichero, hay que generarlo. Para fines generales tiene el mismo contenido de /etc/mail/local-host-names a menos que se desee excluir algún dominio en particular.

dominio.com
mail.dominio.com

Definir lista de control de acceso en:

```
vi /etc/mail/access
```

Incluir solo las IPs locales del servidor, y la lista negra de direcciones de correo, dominios e IPs denegadas. Hay que considerar que cualquier IP que vaya acompañada de RELAY se le permitirá enviar correo sin necesidad de autenticar, lo cual puede ser útil si se utiliza un cliente de correo con interfaz HTTP (Webmail) en otro servidor.

No es conveniente estar autenticando la cuenta de root a través de la red para revisar los mensajes originados por el sistema. Se debe definir alias para la cuenta de root a donde re-direccionar el correo en el fichero /etc/aliases del siguiente modo:

root: jcbv

Configuración de funciones de Sendmail

Modificar el fichero /etc/mail/sendmail.mc y desactivar o habilitar funciones:

vi /etc/mail/sendmail.mc

El parámetro confSMTP_LOGIN_MSG permite establecer el mensaje de bienvenida al establecer la conexión al servidor. Es posible ocultar el nombre y la versión de sendmail, esto con el objeto de agregar seguridad por secreto. Funciona simplemente haciendo que quien se conecte hacia el servidor no pueda saber que software y versión del mismo se está utilizando y con ellos dificultar a un delincuente o abusador de servicio el determinar que vulnerabilidad específica explotar:

```
define(`confSMTP_LOGIN_MSG',`$j ; $b')dnl
```

Lo anterior regresará algo como lo siguiente al realizar una conexión hacia el puerto 25 del servidor:

$ telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to nombre.dominio.
Escape character is '^]'.
220 nombre.dominio ESMTP ; Tue, 21 Jun 2007 04:25:13 -0500
quit
221 2.0.0 nombre.dominio closing connection
Connection closed by foreign host.

Esta configuración se puede poner justo antes de la línea correspondiente al parámetro confAUTH_OPTIONS.

De modo predefinido Sendmail escucha peticiones a través de la interfaz de retorno del sistema a través de IPv4 (127.0.0.1) y no a través de otros dispositivos de red. Solo se necesita eliminar la restricción de la interfaz de retorno para poder recibir correo desde Internet o la LAN modificando la siguiente línea:

DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl

Se debe eliminar de dicho parámetro el valor Addr=127.0.0.1 y la coma (,) que le antecede, del siguiente modo:

DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl

De modo predefinido, como una forma de permitir el correo del propio sistema en una computadora de escritorio o una computadora portátil, está se utiliza el parámetro FEATURE(`accept_unresolvable_domains'). Sin embargo se recomienda desactivar esta función a fin de impedir aceptar correo de dominios inexistentes (generalmente utilizado para el envío de correo masivo no solicitado o Spam), solo basta comentar esta configuración precediendo un dnl, del siguiente modo:

dnl FEATURE(`accept_unresolvable_domains')dnl

Enmascaramiento

Se deben habilitar las siguientes líneas y adaptar valores para definir la máscara que utilizará el servidor:

MASQUERADE_AS(`dominio.com')dnl
FEATURE(masquerade_envelope)dnl
FEATURE(masquerade_entire_domain)dnl

A continuación se debe modificar el fichero /etc/dovecot.conf y habilitar los servicios de imap y/o pop3 del siguiente modo (de modo predefinido están habilitados imap e imaps):

Protocols we want to be serving:
imap imaps pop3 pop3s

```
protocols = imap pop3
```

El servicio se agrega al arranque del sistema y se inicia del siguiente modo:

```
chkconfig dovecot on
service dovecot start
```

Para reiniciar servicio de Sendmail solo bastará ejecutar:

```
service sendmail restart
```

2.3.6.3 Acceso mediante Web (Webmail) y Microsoft Outlook

Para tener acceso Web al servidor de correo, se debe configurar un software llamado Squirrelmail, el cual introduce una interfaz gráfica para acceso mediante browser

Se debe cambiar el directorio /usr/share/squirrelmail/config/ y ejecutar el guión de configuración que se encuentra en el interior:

```
cd /usr/share/squirrelmail/config/
./conf.pl
```

Lo anterior le devolverá una interfaz de texto muy simple de utilizar, como la mostrada a continuación:

```
SquirrelMail Configuration : Read: config.php (1.4.3)
---------------------------------------------------------
Main Menu --
1. Organization Preferences
2. Server Settings
3. Folder Defaults
4. General Options
5. Themes
6. Address Books (LDAP)
7. Message of the Day (MOTD)
8. Plugins
9. Database


D. Set pre-defined settings for specific IMAP servers

C. Turn color on
S Save data
Q Quit

Command >>
```

Aquí se deben ingresar las preferencias en cuanto a la configuración se refiere de acuerdo al menú mostrado.

Se debe reiniciar el servicio de apache:

service httpd start

Para probar el funcionamiento se debe acceder con cualquier navegador Web hacia:

http://127.0.0.1/webmail/

Lo anterior mostrará lo siguiente:

Figura. 2.54. Acceso a cuenta de correo vía web

Se debe ingresar un usuario y contraseña creados anteriormente para tener acceso al servicio de Mail via Web

De igual manera, se puede configurar para recibir los correos electrónicos en Microsoft Outlook, así:

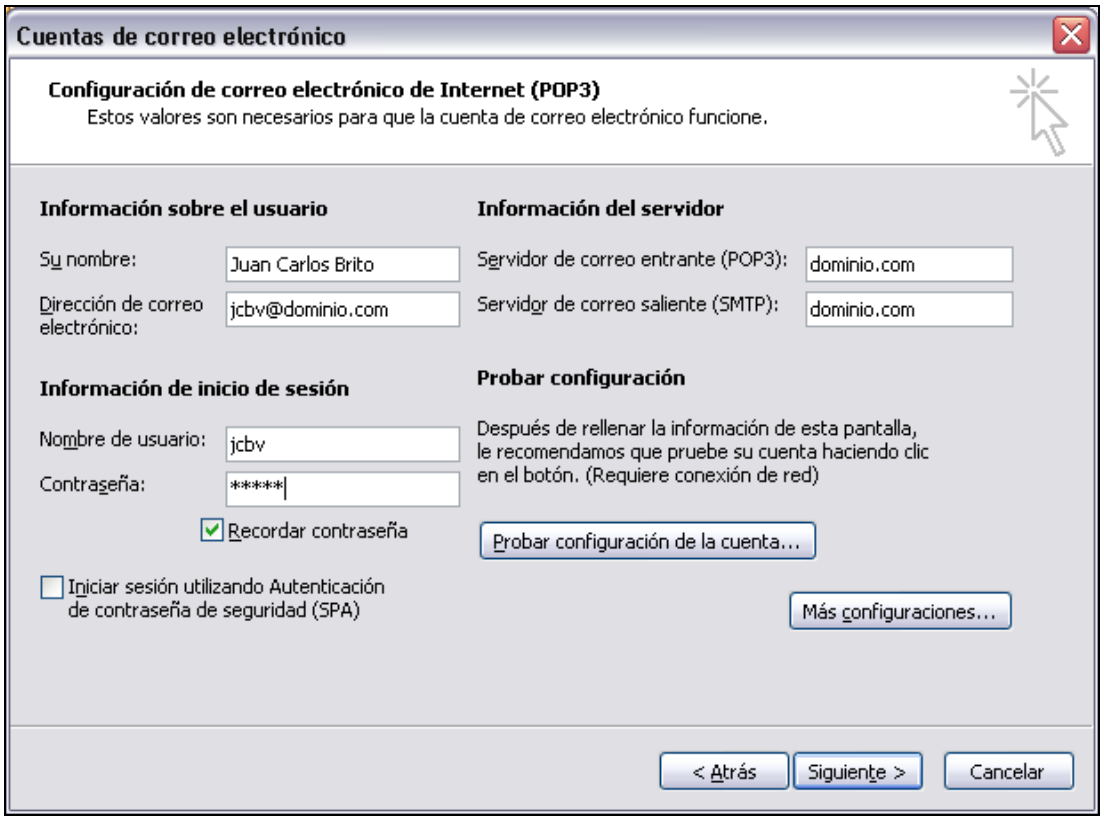


Figura. 2.55. Configuración de cuenta de correo en Microsoft Office Outlook

2.3.7 FTP

2.3.7.1 Descripción

FTP (**F**ile **T**ransfer **P**rotocol) o Protocolo de Transferencia de Archivos (o ficheros informáticos) es uno de los protocolos estándar más utilizados en Internet siendo el más idóneo para la transferencia de grandes bloques de datos a través de redes que soporten TCP/IP. El servicio utiliza los puertos 20 y 21, exclusivamente sobre TCP. El puerto 20 es utilizado para el flujo de datos entre cliente y servidor. El puerto 21 es utilizando para el envío de órdenes del cliente hacia el servidor. Prácticamente todos los sistemas operativos y plataformas incluyen soporte para FTP, lo que permite que cualquier computadora conectada a una red basada sobre TCP/IP pueda hacer uso de este servicio a través de un cliente FTP.

2.3.7.2 Configuración del servicio

VSFTPD (Very Secure FTP Daemon) es un sustento lógico utilizado para implementar servidores de archivos a través del protocolo FTP. Se distingue principalmente porque sus valores por defecto son muy seguros y por su sencillez en la configuración, comparado con otras alternativas como Wu-ftpd. Actualmente se presume que VSFTPD es quizá el servidor FTP más seguro del mundo.

Se debe utilizar un editor de texto y modificar el fichero */etc/vsftpd/vsftpd.conf*. A continuación se analizarán los parámetros a modificar o añadir, según se requiera:

anonymous_enable

Se utiliza para definir si se permitirán los accesos anónimos al servidor. Se ha de establecer como valor YES o NO de acuerdo a lo que se requiera.

anonymous_enable=YES

local_enable

Establece si se van a permitir los accesos autenticados de los usuarios locales del sistema. Se ha de establecer como valor YES o NO según se requiera.

local_enable=YES

write_enable

Establece si se permite el mandato write (escritura) en el servidor. Se ha de establecer como valor YES o NO de acuerdo a lo que se requiera.

write_enable=YES

ftpd_banner

Este parámetro sirve para establecer el banderín de bienvenida que será mostrado cada vez que un usuario acceda al servidor. Se puede establecer cualquier frase que se considere conveniente.

ftpd_banner=Bienvenido al servidor FTP

anon_max_rate

Se utiliza para limitar la tasa de transferencia en bytes por segundo para los usuarios anónimos, algo sumamente útil en servidores FTP de acceso público. En el siguiente ejemplo se limita la tasa de transferencia a 64 Kb por segundo para los usuarios anónimos:

anon_max_rate=64536

local_max_rate.

Hace lo mismo que anon_max_rate, pero aplica para usuarios locales del servidor. En el siguiente ejemplo se limita la tasa de transferencia a 1024 Kb por segundo para los usuarios locales:

local_max_rate=1048576

max_clients

Establece el número máximo de clientes que podrán acceder simultáneamente hacia el servidor FTP. En el siguiente ejemplo se limitará el acceso a 5 clientes simultáneos.

max_clients=5

Para ejecutar por primera vez el servicio se debe ejecutar el comando:

service vsftpd start

Para hacer que los cambios hechos a la configuración surtan efecto se debe ejecutar el comando:

service vsftpd restart

Para detener el servicio se ha de utilizar:

service vsftpd stop

2.3.7.3 Creación de cuotas de disco

Cuotas de disco se refiere a un espacio del disco duro asignado a un usuario determinado.

Para poder asignar sistemas de archivos para que funcionen con cuotas de disco se debe iniciar el sistema en nivel de corrida 1 (mono usuario), ya que se requiere no haya procesos activos utilizando contenido de la partición a la cual se le aplicará la cuota de disco.

Durante la instalación se debe asignar una partición dedicada para, por mencionar un ejemplo, el directorio `/home`.

Con la finalidad de añadir el soporte para cuotas en las particiones anteriormente mencionadas, se debe añadir en el fichero /etc/fstab los parámetros usrquota y grpquota a las líneas que definen la configuración de la partición /home:

LABEL=/home /home ext3 defaults,usrquota,grpquota 1 2

Se debe remontar la partición para que surtan efecto los cambios:

mount -o remount /home

Se deben crear los ficheros aquota.user, aquota.group, quota.user y quota.group, los cuales se utilizarán en adelante para almacenar la información y estado de las cuotas en cada partición.

cd /home

touch aquota.user aquota.group quota.user quota.group

A continuación se debe ejecutar

quotacheck –avug

La primera vez que se ejecuta el mandato anterior es normal marque advertencias refiriéndose a posibles ficheros truncados que en realidad no eran otra cosa sino ficheros de texto simple vacíos a los cuales se les acaba de convertir en formato binario. Si se ejecuta de nuevo *quotacheck - avug*, no deberá mostrar advertencia alguna.

Para activar la cuota de disco configurada, solo bastará ejecutar:

quotaon /home

Luego se debe iniciar el sistema e nivel 3 o 5 a fin de aplicar cuota de disco a algunos usuarios.

edquota

Es importante conocer que significa cada columna mostrada por el comando edquota.

Blocks: Bloques. Corresponde a la cantidad de bloques de 1 Kb que está utilizando el usuario.

Inodes: Inodos. Corresponde al número de ficheros que está utilizando el usuario. Un inodo (también conocido como Index Node) es un apuntador hacia sectores específicos de disco duro en los cuales se encuentra la información de un fichero. Contiene además la información acerca de permisos de acceso así como los usuarios y grupos a los cuales pertenece el fichero.

Soft: Limite de gracia. Limite de bloques de 1 KB que el usuario puede utilizar y que puede rebasar hasta que sea excedido el periodo de gracia (de modo predeterminado son 7 días).

Hard: Limite absoluto. Limite que no puede ser rebasado por el usuario bajo circunstancia alguna.

Para asignar cuotas de disco a cualquier usuario o grupo solo hará falta utilizar *edquota* citando el nombre del usuario al cual se le quiere aplicar:

edquota usuario

Lo anterior deberá devolver algo como lo siguiente a través de vi u otro editor de texto simple:

Disk quotas for user usuario (uid 501):

Filesystem	*blocks*	*soft*	*hard*	*inodes*	*soft*	*hard*
/dev/hda3	*0*	*0*	*0*	*0*	*0*	*0*

Cuota absoluta

Suponiendo que se quiere asignar una cuota de disco de 6 MB para el usuario «*usuario*» en `/dev/hda3`, se utilizaría lo siguiente:

Disk quotas for user usuario (uid 501):

Filesystem	*blocks*	*soft*	*hard*	*inodes*	*soft*	*hard*
/dev/hda3	*0*	*0*	*6144*	*0*	*0*	*0*

El usuario siempre podrá rebasar una cuota de gracia pero nunca una cuota absoluta.

Cuota de gracia

El sistema tiene de modo predeterminado un periodo de gracia de 7 días que se puede modificar con el mandato edquota -t, donde se puede establecer un nuevo periodo de gracia por días, horas, minutos o segundos.

Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds

Filesystem	*Block grace period*	*Inode grace period*
/dev/hda3	*7days*	*7days*

La cuota de gracia establece los límites de bloques o inodos que un usuario tiene en una partición. Cuando el usuario excede el límite establecido por la cuota de gracia, el sistema advierte al usuario que se ha excedido la cuota del disco sin embargo permite al usuario continuar escribiendo hasta que trascurre el tiempo establecido por el periodo de gracia, tras el cual al usuario se le impide continuar escribiendo sobre la partición. Suponiendo que quiere asignar una cuota de gracia de 6 MB en `/dev/hda3`, la cual podrá ser excedida hasta por 7 días, se utilizaría lo siguiente:

Disk quotas for user fulano (uid 501):

Filesystem	*blocks*	*soft*	*hard*	*inodes*	*soft*	*hard*
/dev/hda7	*0*	*6144*	*0*	*0*	*0*	*0*

2.3.8 Servicios de VoIP y video- vigilancia

2.3.8.1 Parámetros en el servidor

Los parámetros a considerarse para la configuración en el servidor de aplicaciones corresponden a la creación de reglas PAT (Port Address Translation), de tal manera que se pueda tener acceso a la visualización de las cámaras IP desde cualquier lugar del mundo, utilizando un puerto público a elección. Es necesario adicionalmente contar con un servidor de dominio correctamente configurado y apuntando hacia una dirección IP pública estática, la cual debe ser provista por el ISP.

2.3.8.2 Configuración

Para tener acceso a la visualización de las cámaras IP, se debe crear una regla de iptables como la indicada a continuación:

Siendo eth1 la tarjeta de red externa,

Para el acceso a una de las cámaras, se deberá ejecutar lo siguiente en cualquier tipo de browser:

http://www.dominio.com:8082

2.4 SERVICIOS AGREGADOS

2.4.1 Traffic – Shaping

- **Control de tráfico en la red de acuerdo a direcciones IP, servicios, puertos, aplicaciones.**

El control de tráfico en la red se realizará mediante la utilización del software llamado *cbq*, Este servicio, a diferencia del resto, no constituye un paquete instalador (sea tipo rpm o tar.gz) sino que los programadores lo han generado para que sea copiado

directamente en la ruta */etc/init.d,* lugar en el cual se encuentran el resto de servicios instalados.

Se lo puede descargar desde el internet realizando una búsqueda del archivo llamado *cbq.init,* el cual contiene toda la programación necesaria para su correcto funcionamiento.

Una vez descargado, se lo debe copiar en la ruta antes especificada.

Para su configuración se debe crear un archivo nuevo (no se debe modificar el cbq.init), el cual deberá poseer un nombre que tenga el formato: *cbq-1234.csc.* Es decir debe contener la palabra cbq más un guión y un número hexadecimal de 2 bytes en el rango de 0002 a FFFF y adicionalmente una extensión cualquiera. En este caso se ha colocado como ejemplo la *csc*.

Dicho archivo configurable deberá ser ubicado en la ruta */etc/sysconfig/cbq.*

Una vez realizado esto, se debe abrir el archivo y colocar los parámetros de configuración como se muestran y explican a continuación:

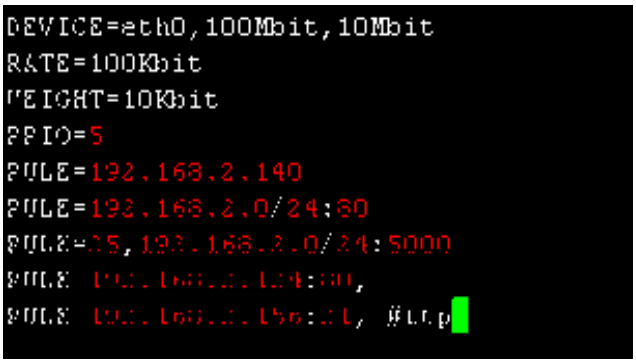


Figura. 2.56. Configuración del archivo cbq

DEVICE = NIC en la cual se va a controlar el ancho de banda. Se debe especificar las características en velocidades de la tarjeta de red

RATE = Regla en la cual se incluye el ancho de banda a ser proporcionado

WEIGHT = Picos máximos a los cuales puede llegar un usuario controlado (Corresponde a un valor especificado en el 10% del parámetro RATE).

PRIO = Valor 5 por defecto.

A continuación se explicarán las principales reglas mediante las cuales se puede establecer diferentes parámetros de control de acceso.

RULE=10.1.1.0/24:80

Selecciona el tráfico que va hacia el Puerto 80 en la red 10.1.1.0

RULE=10.2.2.5

Selecciona el tráfico que va hacia cualquier puerto en un PC con la IP 10.2.2.5

RULE=:25,10.2.2.128/26:5000

Selecciona el tráfico que va desde cualquier punto en el puerto 50 hacia el puerto 5000 en la red 10.2.2.128.

RULE=10.5.5.5:80,

Selecciona el tráfico que va desde el puerto 80 del PC con la dirección IP 10.5.5.5

Adicionalmente se pueden establecer parámetros de rango de tiempo en los cuales se establece el control de ancho de banda, así:

TIME=<from>-<to>;<rate>/<weight>[/<peak>]

TIME=18:00-06:00;256Kbit/25Kbit

2.4.2 Calidad de Servicio (QoS)

Para la aplicación de criterios de calidad de servicio del servidor, es necesario identificar cuáles paquetes son de aplicación en tiempo real como la voz y la videoconferencia, videovigilancia o monitoreo.

La calidad de servicio o QoS es un conjunto de protocolos y tecnologías garantizan la entrega de datos a través de la red en un momento dado. De este modo, se asegura que las aplicaciones que requieran un tiempo de latencia bajo o un mayor consumo de ancho de

banda, realmente dispongan de los recursos suficientes cuando los soliciten. Por ello, uno de las principales metas de QoS es la priorización. Esto es, el dar más relevancia a unas conexiones frente a otras.

Algunos de los beneficios que podemos obtener al implantar QoS en un determinado sistema son:

● Control sobre los recursos: se puede limitar el ancho de banda consumido por transferencias de FTP y dar más prioridad a un servidor de bases de datos al que acceden múltiples clientes.

● Uso más eficiente de los recursos de red: al poder establecer prioridades dependiendo del tipo de servicio, umbrales de tasas de transferencia.

● Menor latencia: en aplicaciones de tráfico interactivo como SSH, telnet... que requieren un tiempo de respuesta corto.

Existen varias estrategias y técnicas para llevar a cabo la aplicación de QoS, tanto software como Hardware, comerciales y de código abierto (libres). La implementación de este servicio de cola bajo Linux permite ordenar el tráfico de red

Para proceder a la implantación práctica de un sistema QoS para gestionar el ancho de banda, hay que comprender cual es el camino que recorre un paquete desde que ingresa o se genera en el servidor hasta que sale a Internet u otra red; así como las diferentes disciplinas de cola también conocidas como qdiscs (Queue Disciplines) que clasifican los paquetes.

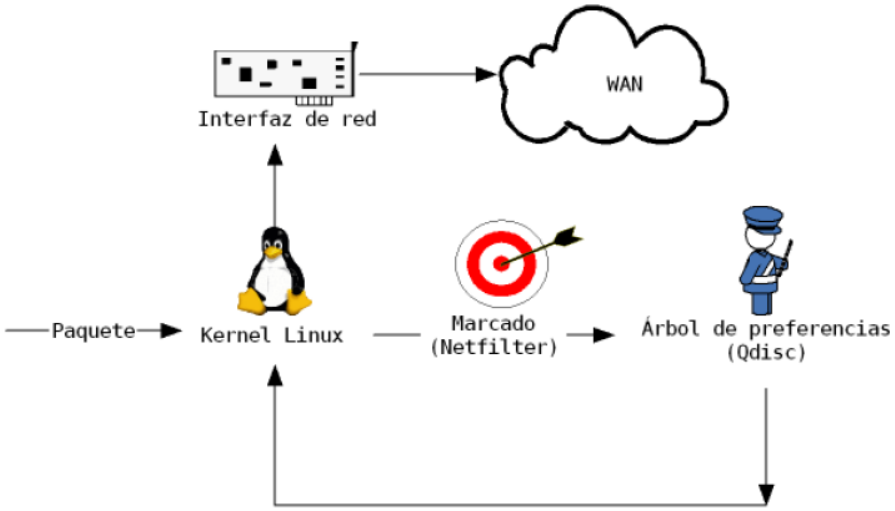


Figura. 2.57. Diagrama de paquetes con disciplinas de cola

En la figura ___ se puede observar de forma esquemática cual es el proceso que sigue un paquete de datos desde que llega hasta la máquina local y/o abandona la misma:

● El paquete llega al kernel linux de la máquina.

● Netfilter (iptables) se encarga de poner una marca al paquete que se establezca dentro de la configuración. Es similar al código postal del sistema de correos: un identificador para posteriormente poder clasificar el envío. Se pueden hacer marcados en base al puerto de destino, a la cabecera IP, la dirección IP origen del paquete.

● El árbol de preferencias: aquí es donde reside el corazón del mecanismo de control de tráfico. Con el encolamiento se determina de que forma se envían los datos, mediante el uso de disciplinas de cola. Las disciplinas de cola no son más que una estructura de clases en las que hay dependencia de padre-hijo entre sus miembros.

Para implementar QoS en Linux:

Se requiere parchear el kernel. Se descomprime los archivos .tar.gz, por ejemplo, en el directorio home, y situarse en el lugar donde se haya descomprimido el kernel de linux. Normalmente se instala las fuentes del kernel en /usr/src/linux. Para parchear simplemente hay que introducir el comando

patch -p1 < /ruta_al_parche:

Una vez parcheado el kernel, se ejecuta *make menuconfig* para entrar en el menú n de configuración del kernel y realizar los cambios requeridos, y además, muy importante, marcar las opciones necesarias para que funcione:

- Networking Options: Network packet filtering
- IP: Netfilter configuration:
  - Netfilter MARK match support
  - Connection state match support
  - Packet filtering
  - Packet mangling
  - MARK target support
  - Connection tracking
  - Layer7 match support

Se debe escoger también la opción QoS and Fair Queing dentro de Networking Options, como también aquellas cosas que se vaya a usar posteriormente, como por ejemplo HTB Packet Scheduler, si se quiere usar htb.

Una vez terminado de configurar el kernel, salir del menú de configuración y compilarlo, junto a los módulos.

Con el kernel listo, aplicado los parches correspondientes para usar ESFQ, IMQ y Layer7. Ahora sólo queda aplicar los parches al código fuente de iproute2 e iptables. El proceso es similar al anterior, usando el comando *patch:*

Una vez parcheado hacer *make && make install* para compilar iptables e instalarlo. El proceso para iproute2 es similar.

Con el kernel, iproute2 e iptables convenientemente parcheados y compilados, reiniciar la máquina para arrancar con el nuevo kernel (configurar grub) para empezar a definir las políticas de tráfico.

El comando tc

El comando tc "Traffic Control", herramienta incluida dentro del paquete iproute2, será el programa para crear el árbol de bandas del que se ha hablado anteriormente. Su sintaxis es la siguiente:

Para gestionar qdiscs: tc qdisc [add | change | replace | link] dev DEV [parent qdisc-id | root] [handle qdisc-id] qdisc [qdisc specific parameters]

Para gestionar las clases: tc class [add | change | replace] dev DEV parent qdiscid [classid class-id] qdisc [qdisc specific parameters]

Para gestionar los filtros: tc filter [add | change | replace] dev DEV [parent qdisc-id | root] protocol protocol prio priority filtertype [filtertype specific parameters] flowid flow-id

Muestra las qdiscs: tc [-s | -d] qdisc show [dev DEV]

Muestra el tráfico de las clases: tc [-s | -d] class show dev DEV

Muestra los filtros: tc filter show dev DEV

Primero crearemos la qdisc raiz. Es la principal y siempre tiene que estar presente; es la que está asociada a la tarjeta de red. La tarjeta de red de salida a internet es eth1. Crear la banda principal (root) con nombre 1:. Por defecto enviará los paquetes a la clase 13.

tc qdisc add dev eth0 root handle 1: htb default 13

Con root se indica que se va a crear la *qdisc* raíz, que tendrá el identificador 1:. Se Sigue creando l árbol, en base a los objetivos correspondientes.

tc class add dev eth0 parent 1: classid 1:1 htb rate 300kbit ceil 300kbit

Se ha definido una banda dependiente de root (parent 1:) con algoritmo htb. Esta clase no dejará pasar paquetes a más velocidad de 300kbit. Ceil hace referencia al **máximo posible** de transferencia, y rate al **mínimo garantizado.**

Hay que tomar en cuenta que la qdisc no puede prestar ancho de banda si sobra, mediante el comando *prio* indicar el canal con mayor prioridad. Realizar también el filtrado correspondiente en *iptables*.

2.5. SEGURIDADES

2.5.1 Cortafuegos (Firewall)

Filtrado de paquetes entrantes y salientes por direcciones IP (host), por servicios, por puertos, por aplicaciones.

El servicio de cortafuegos, es de suma utilidad puesto que evita que intrusos y servicios indeseables ingresen al sistema. Es muy importante tener configurado un servicio de firewall para brindar una correcta protección al servidor.

El cortafuegos instalado en el servidor corresponde al servicio brindado por el software guarddog, el cual permite configurar un nivel de seguridad de acuerdo a diferentes parámetros. Para poder ingresar al firewall, se debe acceder al servidor en modo gráfico, y abrir una consola de administración presionando las teclas Alt + F2 y digitando la palabra "*konsole*" en la pantalla mostrada. A continuación se desplegará la consola en la cual se debe digitar el comando guarddog y automáticamente se abre el software**.** Así:

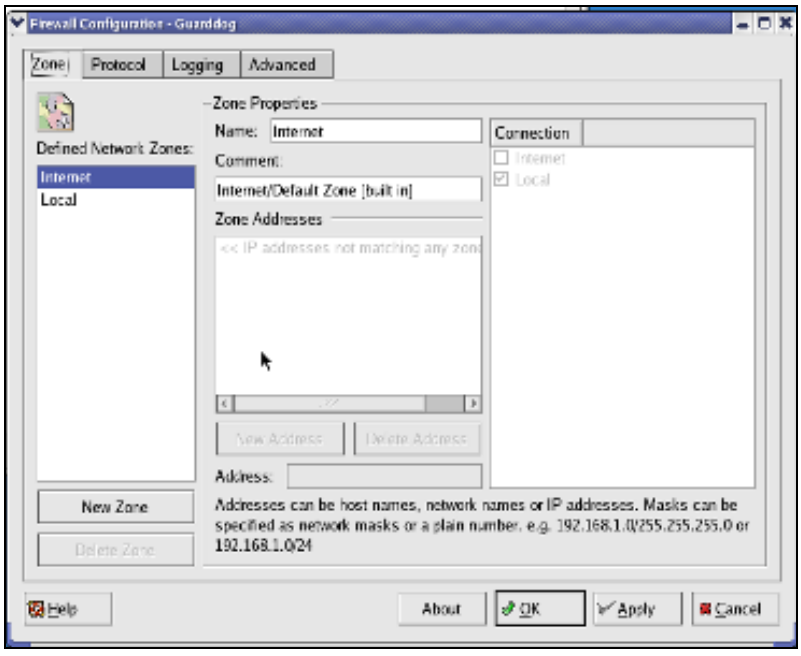


Figura. 2.58. Configuración firewall, software guarddog

Inicialmente se tiene 2 zonas: Internet y Local. La primera no requiere explicación alguna, la segunda se refiere al servidor de aplicaciones.

Se debe agregar entonces la zona faltante, es decir a la red LAN, así:

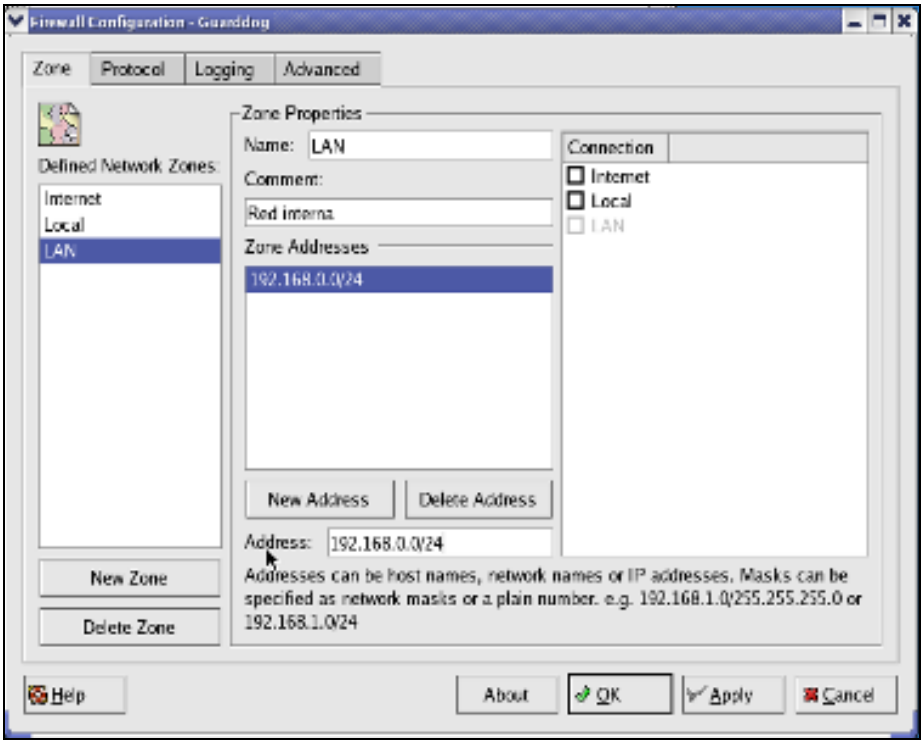


Figura. 2.59. Parámetros LAN de configuración de firewall

A continuación se escoge la pestaña *"Protocol"*, en la cual se muestran las zonas de red definidas en el ítem anterior. Adicionalmente se muestra una serie de protocolos de red, los cuales posee una breve explicación en la parte inferior izquierda.

También se indica la nomenclatura para indicar si un protocolo es rechazado o permitido.

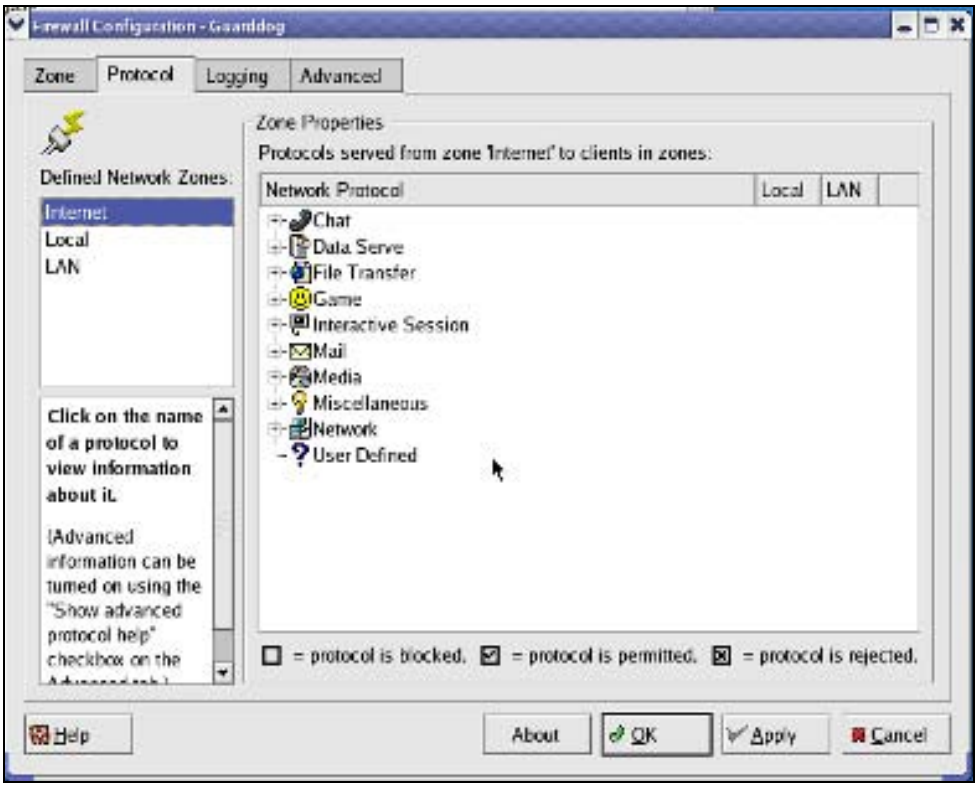


Figura. 2.60. Selección de protocolos

La aceptación o rechazo de los protocolos indicados en la lista se lo maneja de la siguiente forma: En la parte derecha se indican las zonas *"Internet"* y *"LAN"* y en la izquierda se encuentra señalada la zona *"Local"* Entonces se establece la vía de aceptación o rechazo en dos partes: desde "Internet" hacia "Local" y desde "LAN" hacia "Local".

De igual manera, se establece la aceptación o rechazo de protocolos de red para el resto de zonas en diferentes vías, de acuerdo al criterio del administrador de red quien configura el servicio.

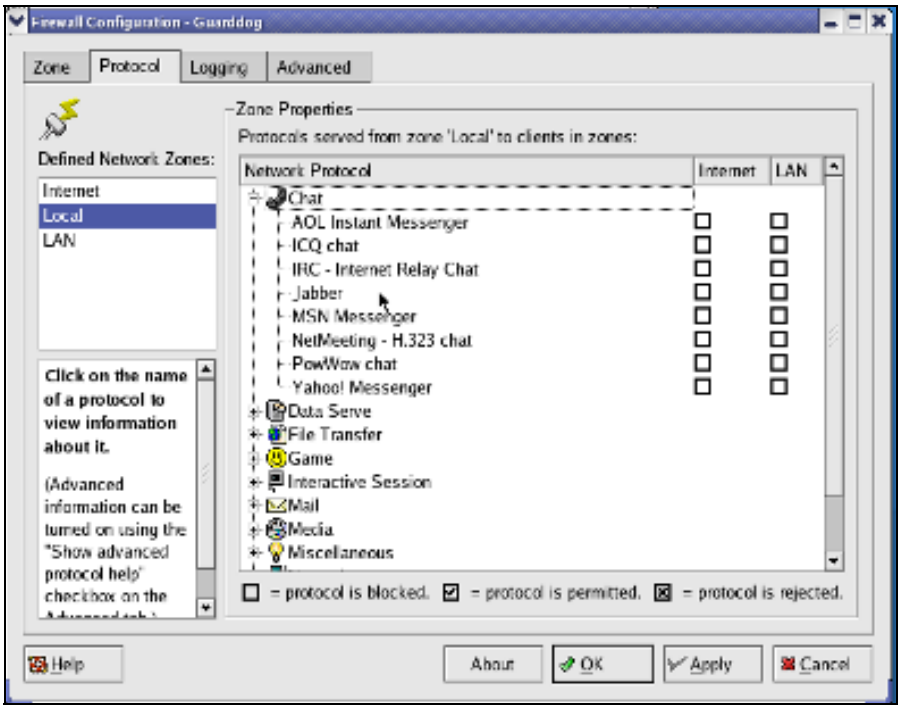


Figura. 2.61. Filtrado de protocolos de red

En la tercera pestaña se muestra la aceptación o no de los logs del firewall, los cuales se presentarán de manera automática en la parte texto del sistema Linux. Queda a criterio del usuario la aceptación o rechazo de la presentación de dichos logs.

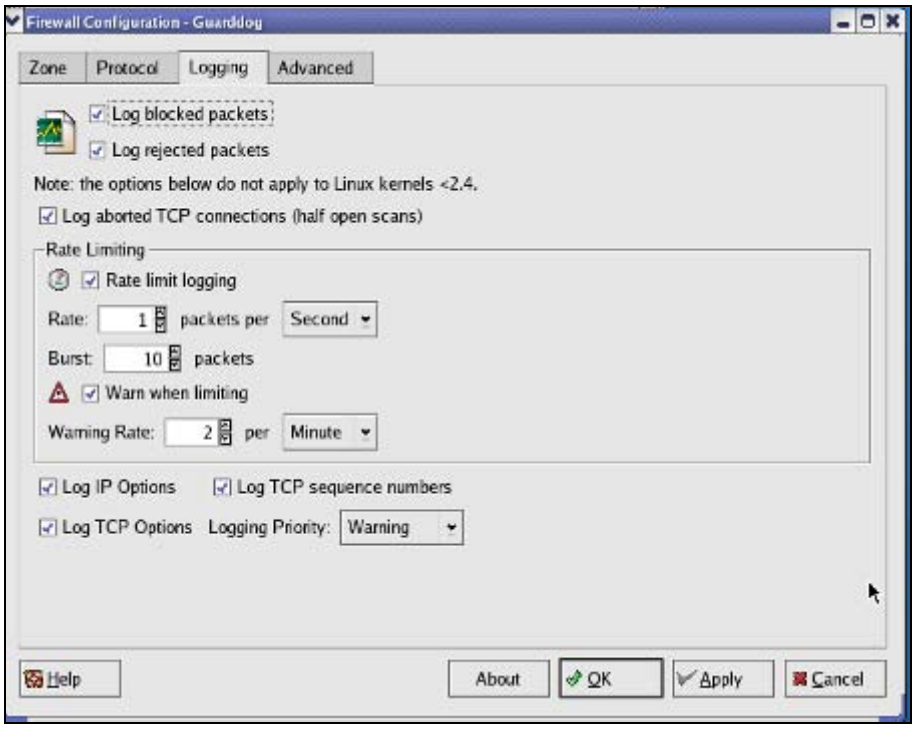


Figura. 2.62. Configuración de logs del firewall

Adicionalmente se puede crear protocolos definidos por el usuario, los cuales corresponderán a un puerto determinado.

Se crea un nombre del protocolo y el puerto que maneja. De esta forma automáticamente este nuevo criterio se introducirá en la lista de protocolos a ser aceptados o rechazados.

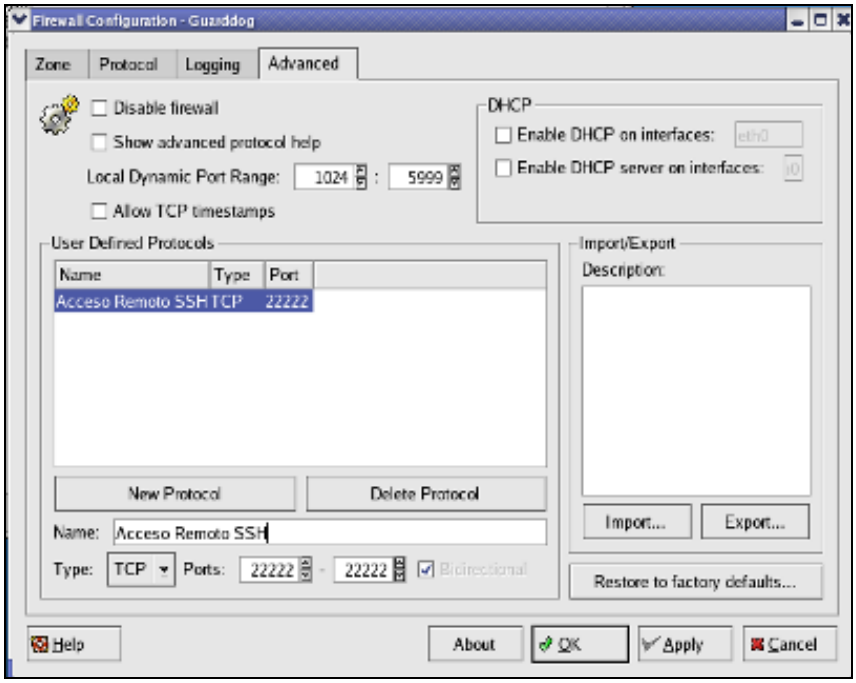


Figura. 2.63. Creación de protocolos propietarios de usuario

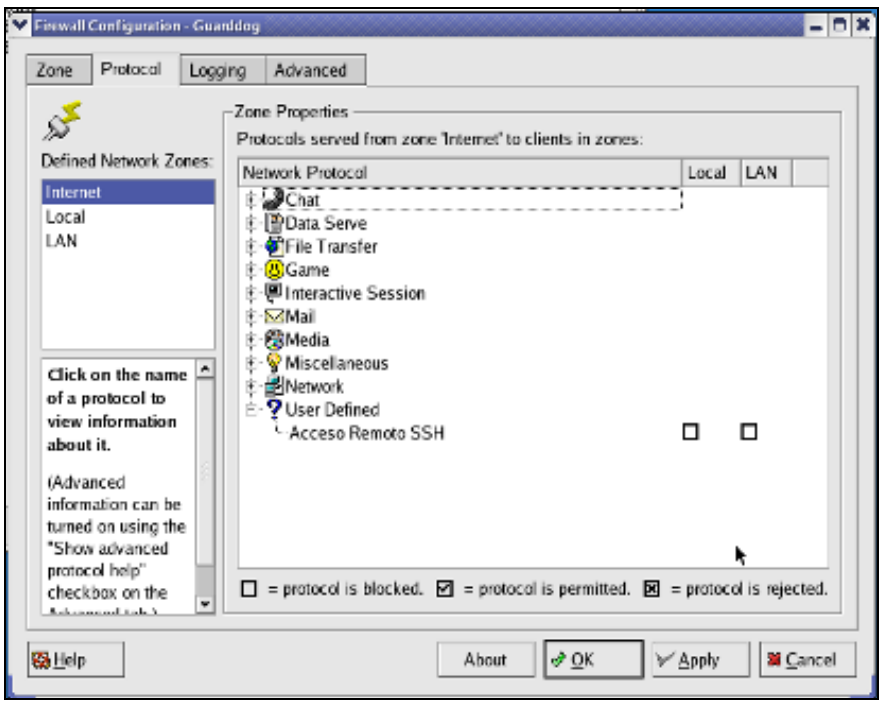


Figura. 2.64. Establecimiento de permiso para protocolo creado

Redireccionamiento de puertos y enmascaramiento de paquetes

El redireccionamiento de puertos y enmascaramiento de paquetes se lo hará utilizando el servicio de iptables. Existen dos instrucciones a ser ejecutadas para realizarlos.

A continuación se detallan y explican las mismas:

El redireccionamiento de puertos se lo utiliza para que todas las conexiones hacia Internet (puerto 80) pasen primero por el Proxy, el cual puede controlar loa accesos a Internet o restringirlos según criterio del administrador. La instrucción debe ser ejecutada como root y se muestra a continuación:

iptables –t nat –A PREROUTING –i eth0 –p tcp –m tcp –dport 80 –j REDIRECT –to-ports 3128

En este caso hay que tomar en cuenta que el tráfico considerado es de tipo tcp y que la interfaz de red eth0 corresponde a la NIC interna. (la cual posee la IP privada).

El enmascaramiento de paquetes de red se lo realiza para que, junto con squid, la red cuente con un sistema de proxy transparente.

La instrucción se muestra a continuación:

iptables –t nat –A POSTROUTING –s 192.168.0.0/24 –j MASQUERADE

2.5.2. – Antivirus

2.5.2.1 Estudio introductorio acerca de virus, troyanos, gusanos, spam y adware/spyware. Formas de transmisión, consejos de seguridad.

Los virus, gusanos y troyanos son programas malintencionados que pueden provocar daños en el equipo y en la información del mismo. También pueden hacer más lento Internet e, incluso, pueden utilizar su equipo para difundirse a amigos, familiares, colaboradores y el resto de la Web. La buena noticia es que con un poco de prevención y algo de sentido común, es menos probable ser víctima de estas amenazas.

Virus

Un virus es código informático que se adjunta a sí mismo a un programa o archivo para propagarse de un equipo a otro. Infecta a medida que se transmite. Los virus pueden dañar el software, el hardware y los archivos.

El virus es un código escrito con la intención expresa de replicarse. Un virus se adjunta a sí mismo a un programa host y, a continuación, intenta propagarse de un equipo a otro. Puede dañar el hardware, el software o la información.

Al igual que los virus humanos tienen una gravedad variable, desde el virus Ébola hasta la gripe de 24 horas, los virus informáticos van desde molestias moderadas hasta llegar a ser destructivos. La buena noticia es que un verdadero virus no se difunde sin la intervención humana. Alguien debe compartir un archivo o enviar un mensaje de correo electrónico para propagarlo.

Gusano

Un gusano, al igual que un virus, está diseñado para copiarse de un equipo a otro, pero lo hace automáticamente. En primer lugar, toma el control de las características del equipo que permiten transferir archivos o información. Una vez que un gusano esté en su sistema, puede viajar solo. El gran peligro de los gusanos es su habilidad para replicarse en grandes números. Por ejemplo, un gusano podría enviar copias de sí mismo a todos los usuarios de su libreta de direcciones de correo electrónico, lo que provoca un efecto dominó de intenso tráfico de red que puede hacer más lentas las redes empresariales e Internet en su totalidad. Cuando se lanzan nuevos gusanos, se propagan muy rápidamente. Bloquean las redes y posiblemente provocan esperas largas (a todos los usuarios) para ver las páginas Web en Internet.

Un gusano puede consumir memoria o ancho de banda de red, lo que puede provocar que un equipo se bloquee.

Debido a que los gusanos no tienen que viajar mediante un programa o archivo "host", también pueden crear un túnel en el sistema y permitir que otro usuario tome el control del equipo de forma remota.

Troyano

Del mismo modo que el caballo de Troya mitológico parecía ser un regalo pero contenía soldados griegos que dominaron la ciudad de Troya, los troyanos de hoy en día son programas informáticos que parecen ser software útil pero que ponen en peligro la seguridad y provocan muchos daños. Un troyano reciente apareció como un mensaje de correo electrónico que incluye archivos adjuntos que aparentaban ser actualizaciones de seguridad de Microsoft, pero que resultaron ser virus que intentaban deshabilitar el software antivirus y de servidor de seguridad.

Los troyanos se difunden cuando a los usuarios se les engaña para abrir un programa porque creen que procede de un origen legítimo. Para proteger mejor a los usuarios, Microsoft suele enviar boletines de seguridad por correo electrónico, pero nunca contienen archivos adjuntos.

Los troyanos también se pueden incluir en software que se descarga gratuitamente. Nunca descargue software de un origen en el que no confíe.

Formas de transmisión

Prácticamente todos los virus y muchos gusanos no se pueden transmitir a menos que se abra o se ejecute un programa infectado.

Muchos de los virus más peligrosos se difundían principalmente mediante archivos adjuntos de correo electrónico, los archivos que se envían junto con un mensaje de correo electrónico. Normalmente se puede saber que el correo electrónico incluye un archivo adjunto porque se muestra el icono de un clip que representa el archivo adjunto e incluye su nombre. Algunos tipos de archivos que se pueden recibir por correo electrónico habitualmente son fotos, cartas escritas en Microsoft Word e, incluso, hojas de cálculo de Excel. Un virus se inicia al abrir un archivo adjunto infectado (normalmente se hace clic en el icono de archivo adjunto para abrirlo).

Sugerencia: nunca abra nada que esté adjunto a un mensaje de correo electrónico a menos que espere el archivo y conozca el contenido exacto de dicho archivo.

Si recibe un correo electrónico con un archivo adjunto de un desconocido, elimínelo inmediatamente. Por desgracia, en ocasiones tampoco resulta seguro abrir archivos adjuntos de personas que conoce. Los virus y los gusanos tienen la capacidad de robar la información de los programas de correo electrónico y enviarse a todos los incluidos en la libreta de direcciones. Por lo tanto, si recibe un correo electrónico de alguien con un mensaje que no entiende o un archivo que no esperaba, póngase siempre en contacto con la persona y confirme el contenido del archivo adjunto antes de abrirlo.

Otros virus se pueden propagar mediante programas que se descargan de Internet o de discos repletos de virus que dejan los amigos o incluso que se compran en una tienda. Existen formas menos habituales de contraer un virus. La mayoría de las personas se contagian de virus si abren y ejecutan archivos adjuntos de correo electrónico desconocidos.

Presencia de virus

Al abrir y ejecutar un programa infectado, es posible que no sepa que ha contraído un virus. Su equipo puede hacerse más lento o bloquearse y reiniciarse cada pocos minutos. En ocasiones, un virus ataca los archivos que necesita para iniciar un equipo. En este caso, puede presionar el botón de encendido y estar mirando una pantalla vacía.

Todos estos síntomas son signos habituales de que el equipo tiene un virus, aunque se pueden deber a problemas de hardware o software que nada tengan que ver con un virus.

Preste atención a los mensajes que indiquen que ha enviado correo electrónico con virus. Puede significar que el virus ha incluido su dirección de correo como el remitente de un correo electrónico infectado. Esto no significa necesariamente que tenga un virus. Algunos virus tienen la capacidad de falsificar las direcciones de correo electrónico.

A menos que tenga instalado software antivirus actualizado en el equipo, no existe un modo seguro de saber si tiene un virus.

Spam

Es el correo electrónico no solicitado o no deseado, que se envía a múltiples usuarios con el propósito de hacer promociones comerciales o proponer ideas. Generalmente, suelen

ser: publicidad, ofertas o enlaces directos una página web. Estos mensajes son enviados a cientos de miles de destinatarios cada vez.

El correo basura es molesto y roba recursos del sistema. Su distribución causa la perdida de ancho de banda en la Red, y multiplica el riesgo de infección por virus.

Las personas o empresas que envían este tipo de emails, construyen sus listas usando varias fuentes. Normalmente, utilizan programas que recogen direcciones de correo desde Usenet, o recopilan las mismas de otras listas de distribución.

Muchos de los mensajes no solicitados nos ofrecen la opción de eliminarnos. La experiencia demuestra que este método es una trampa, y que sólo sirve para verificar que la dirección de correo existe realmente, y se encuentra activa. Por otro lado, si respondemos alguno de estos emails, el resultado es idéntico, seremos colocados automáticamente en una nueva lista de distribución, confirmando nuestra dirección.

Spyware

Los programas espía se instala en un ordenador sin el conocimiento del usuario, para recopilar información del mismo o de su ordenador, enviándola posteriormente al que controla dicha aplicación.

Existen dos categorías de spyware: software de vigilancia y software publicitario. El primero se encarga de monitorizar todo el sistema mediante el uso de transcriptores de teclado, captura de pantallas y troyanos. Mientras, el segundo, también llamado “Adware”, se instala de forma conjunta con otra aplicación o mediante controles ActiveX, para recoger información privada y mostrar anuncios.

Este tipo de programas registran información sobre el usuario, incluyendo, contraseñas, direcciones de correo, historial de navegación por Internet, hábitos de compra, configuración de hardware y software, nombre, edad, sexo y otros datos secretos.

Al igual que el correo basura, el software publicitario, usa los recursos de nuestro sistema, haciendo que sea este el que pague el coste asociado de su funcionamiento.

Además, utiliza el ancho de banda, tanto para enviar la información recopilada, como para descargar los banners publicitarios que nos mostrará.

Los mayores responsables de la difusión de spyware son los populares programas de intercambio de archivos (P2P) disponibles en la actualidad, tipo Kazaa, eDonkey o eMule.

Consejos de seguridad

1. No abrir ningún adjunto de e-mail proviniendo de alguien desconocido o desconfiado.

2. No abrir ningún mensaje si no sabe a que se refiere, por más que venga de parte de un conocido o compañero. La mayoría de los virus se propagan por e-mail. Es mucho más fácil prevenir que reparar, así que sería mejor pedir una confirmación de parte del remitente.

3. No abrir los adjuntos de los mensajes que presentan un asunto sospechoso o inesperado. Si quiere abrirlos, asegúrese de guardarlos primeramente en su disco duro y después analícelos con una solución antivirus actualizada.

4. Eliminar cualquier mensaje no deseado. No reenviarlos o responder a sus respectivos remitentes. Este tipo de mensajes está contemplado como spam, al no ser solicitado o esperado y considerando también que sobrecarga el tráfico en Internet.

5. No copiar ningún fichero si desconoce o desconfía su origen.

6. Tener cuidado al descargar ficheros desde Internet. Primeramente debe averiguar los orígenes y asegurarse que dichos ficheros han sido ya analizados con un programa antivirus en el sitio de descarga. Si no está seguro de estos elementos, copie el archivo en su disco duro o en un disquete y luego analícelo con su propio antivirus.

7. Utilizar un antivirus de confianza y actualizarlo permanentemente. Seleccione un antivirus que incluye un módulo residente para monitorizar su actividad mientras está usando el ordenador.

8. Actualizar con regularidad su antivirus, si tiene uno instalado en su sistema. 500 virus nuevos se descubren cada mes. Las actualizaciones del antivirus deben incluir por lo menos los archivos con las firmas de virus, pero sería preferible que también actualice los motores de análisis.

9. Hacer copias de seguridad a menudo. Si un virus llega a destruir un fichero importante, podrá reemplazarlo. Se recomienda almacenar estas copias en una ubicación separada, en otro ordenador o bien en soporte magnético.

10. Si tiene dudas acerca de un fichero o mensaje, no descargar, ejecutar o abrirlo.

2.5.2.2 Instalación y configuración del antivirus ClamAV

ClamAV Antivirus, con una rápida exploración detecta más de 44 mil virus, gusanos y troyanos lo cual incluye virus para MS Office

Posee capacidad para examinar contenido de ficheros ZIP, RAR, Tar, Gzip, Bzip2, MS OLE, MS Cabinet, MS CHM y MS SZDD.

Además posee una avanzada herramienta de actualización con soporte para firmas digitales y consultas basadas sobre DNS

La instalación de ClamAV se lo puede realizar descargando el programa, ya sea en formato tar, bz, bz2 o rpm.

Una vez descargado se realiza la instalación del mismo de acuerdo a la extensión del paquete como se encuentra explicado en el ítem 2.2.2

Para realizar la configuración se debe editar el archivo clamd.conf, el cual se encuentra ubicado en */etc.*

vi /etc/clamd.conf

Aquí se debe cambiar el valor de usuario “clamav” a “root”, así:

Figura. 2.65. Inicialización del antivirus por parte del usuario "root"

También se debe editar el archivo de configuración freshclam.conf, el mismo que se encuentra ubicado en /etc

vi /etc/freshclam.conf

Se debe descomentar el parámetro Checks y colocar el valor 12 para actualizar la base de datos del antivirus cada 2 horas de manera automática

Figura. 2.66. Configuración de actualización de antivirus

Para forzar la actualización del antivirus se debe ejecutar el comando *freshclam* como usuario root.

El comando *clamd* ejecuta el demonio del antivirus.

Posteriormente se debe indicar que los demonios del antivirus se ejecuten automáticamente al iniciar el sistema, así:

chkconfig freshclam on
chkconfig clamd on

Para iniciar los servicios se debe ejecutar:

service clamd start

service freshclam start

Para realizar un escaneo del sistema en busca de posibles infecciones se debe ejecutar el comando clamdscan seguido del directorio a ser analizado, así:

clamdscan -v /home/

2.5.2.3 Instalación y configuración de MailScanner para Linux Mail Servers.

Para instalar MailScanner, solo bastará ejecutar:

yum -y install mailscanner

Configuración de MailScanner

Se debe utilizar cualquier editor de texto y modificar /etc/MailScanner/MailScanner.conf con la finalidad de configurar los siguientes parámetros:

Se puede configurar MailScanner para que devuelva los mensajes de sistema en español, así:

%report-dir% = /etc/MailScanner/reports/**es**

La identificación de la organización solo es de carácter informativo y sirve para identificar si un mensaje infectado pertenece a un servidor u otro.

%org-name% = empresa

El parámetro %org-long-name% es utilizado para definir que mostrar en la firma localizada al final de los reportes enviados por MailScanner.

%org-long-name% = Empresa S.A.

Definir antivirus a utilizar

MailScanner puede detectar automáticamente los antivirus a utilizar dejando el valor auto en el parámetro Virus Scanners, de modo que detectará cualquiera de los siguientes:

Tabla. 2.5. Antivirus disponibles para linux

• Sophos.	• Mcafee.	• Command.
• Bitdefender.	• DRweb.	• Kaspersky.
• eTrust.	• Inoculate.	• Inoculan.
• Nod32.	• F-Secure.	• F-Prot.
• Panda.	• Rav.	• Antivir.
• ClamAV.	• Trend.	• Norman.
• Css.	• AVG.	• Vexira.

Para agilizar el inicio de MailScanner se pueden definir los antivirus necesarios. ClamAV es el antivirus recomendado por tratarse de libre distribución.

Virus Scanners = clamav

Se puede utilizar más de un antivirus. Solo se necesitará instalar las versiones apropiadas para el sistema operativo y añadirlos en MailScanner como lista horizontal separada por espacios.

Virus Scanners = clamav nod32 sophos trend

Se puede poner en cuarentena los elementos adjuntos infectados en los mensajes de correo electrónico:

Quarantine Infections = yes

Control de Spam

De modo predefinido está activo el soporte de exploración de correo en búsqueda de correo masivo no solicitado (Spam).

Spam Checks = yes

Quienes se dedican al envío de correo masivo no solicitado han aprendido que pueden hacer que su mensaje pase los filtros enviando un mensaje con muchos destinatarios, uno de los cuales podría tener configurado tener todo en lista blanca en las opciones de SpamAssassin en el directorio de inicio del usuario. De este modo, si un mensaje llega con más de un número determinado de destinatarios (20 de modo predefinido), éste se será tratado como cualquier otro mensaje sin aún si el destinatario ha

decidido poner todo en lista blanca o si el remitente está en la lista blanca en el fichero /etc/MailScanner/rules/spam.whitelist.rules.

Ignore Spam Whitelist If Recipients Exceed = 20

Control de SPAM a través de DNSBL o listas negras

MailScanner permite también realizar filtrado de correo contra listas negras como SpamCop y Spamhaus.

Modificar el fichero /etc/MailScanner/spam.lists.conf y definir o confirmar las listas negras a utilizar:

ORDB-RBL relays.ordb.org.
spamhaus.org sbl.spamhaus.org.
spamhaus-XBL xbl.spamhaus.org.
combinación de las dos anteriores:
SBL+XBL sbl-xbl.spamhaus.org.
spamcop.net bl.spamcop.net.
NJABL dnsbl.njabl.org
SORBS dnsbl.sorbs.net.

En el fichero /etc/MailScanner/MailScanner.conf configurar lo siguiente:

Spam List = ORDB-RBL SBL+XBL spamcop.net NJABL SORBS

Control de Spam a través de SpamAssassin

MailScanner puede utilizar SpamAssassin para una más eficiente detección de correo masivo no solicitado. Puede activarse o desactivarse esta funcionalidad a través del parámetro Use SpamAssassin asignando yes o no.

Use SpamAssassin = yes

SpamAssassin utiliza un sistema de calificación para etiquetar o no como correo masivo no solicitado. Se asigna un valor numérico a partir de 1 (valor recomendado es 6), con o sin decimales, para el parámetro Required SpamAssassin Score. Cada vez que se identifica en un mensaje contiene alguna característica que pudiera clasificarlo como correo masivo no solicitado, se asignan fracciones de punto que se van sumando. Cuando

un mensaje rebasa el valor asignado para Required SpamAssassin Score éste es etiquetado de inmediato como correo masivo no solicitado.

Required SpamAssassin Score = 6

Puede especificarse también a través del parámetro High SpamAssassin Score que los mensajes que rebasen la puntuación establecido como valor de este se eliminen directamente en lugar de solo etiquetarlos como correo masivo no solicitado. El valor prefinido (y recomendado) es 10.

High SpamAssassin Score = 10

El parámetro Spam Actions define que política a aplicar para el correo electrónico que se clasifica como Spam, calificado a partir del valor definido en Required SpamAssassin Score, pero inferior al valor definido a High SpamAssassin Score.

Tabla 2.6 Comandos de SpamAssassin

deliver	Entrega del mensaje de modo normal.
delete	Eliminar el Mensaje.
bounce	Envía un masaje de rechazo al remitente. Este valor solo puede utilizarse con el parámetro Spam Actions, no puede utilizarse con el parámetro High Scoring Spam Actions.
store	Almacenar el mensaje en el directorio de cuarentena.
forward usuario@dominio.com	Reenviar copia del mensaje a usuario@dominio.com
striphtml	Convierte el contenido HTML a texto simple. Se requiere especificar el valor deliver para que tenga efecto.
attachment	Convierte el mensaje a adjunto, de modo que el usuario tendrá que realizar un paso adicional para mirar el contenido.
notify	Se envía una breve notificación al usuario que le indica que no le fue entregado un mensaje por haber sido clasificado como correo masivo no solicitado, permitiendo solicitar recuperar el mensaje si acaso éste fuese un mensaje esperado.
header "nombre: valor"	Añade la cabecera con cualquier nombre (sin espacios) con el valor especificado.

Suponiendo se aplicarán las siguientes políticas:

• Si el mensaje es calificado al menos el valor definido en Required SpamAssassin Score, pero inferior al valor definido en High SpamAssassin Score, se entregará al usuario como mensaje adjunto y añadirá la cabecera "X-Spam-Status: Yes".

• Si el mensaje es calificado al menos con el valor definido en High SpamAssassin Score, se eliminará automáticamente.

Los valores para Required SpamAssassin Score y High SpamAssassin Score corresponderían del siguiente modo:

```
Spam Actions = deliver attachment header "X-Spam-Status: Yes"
High Scoring Spam Actions = delete
```

Listas Blancas

Pueden especificarse listas blancas de direcciones o nombres de dominio que no se desee etiqueten como correo masivo no solicitado (Spam) en el fichero /etc/MailScanner/rules/spam.whitelist.rules del siguiente modo, donde yes significará que el correo proveniente de dichas direcciones nunca se etiquetará como correo masivo no solicitado (Spam):

```
# This is where you can build a Spam WhiteList
# Addresses matching in here, with the value
# "yes" will never be marked as spam.
#From:          152.78.         yes
#From:          130.246.        yes
FromOrTo:       default         no
From:           200.76.185.250  yes
From:           192.168.0.      yes
```

En el ejemplo anterior, todo el correo proveniente de 200.76.185.250 y cualquier dirección IP de la red 192.168.0.0/24 quedará exento de etiquetarse como correo masivo no solicitado (Spam).

Se debe desactivar y detener el servicio de sendmail, el cual será controlado en adelante por el servicio MailScanner:

```
chkconfig sendmail off
chkconfig MailScanner on
service sendmail stop
service MailScanner start
```

2.6 MONITOREO DE ANCHO DE BANDA.

2.6.1 IFTOP

Como primer paso se debe realizar la instalación del programa. Es recomendable descargarlo del sitio www.pbone.net que brinda paquetes de instalación rpm.

Se lo debe descargar de acuerdo a la distribución de Linux que se tenga e instalarlo como fue explicado en secciones anteriores.

Este servicio funciona con la finalidad de establecer un control en cuanto al monitoreo de la red; tanto interna como externa.

El software iftop funciona en la parte de texto y se ingresa como usuario administrador así:

iftop –i <interfaz de red>

Por ejemplo si se necesita monitorear la interfaz de red eth0, se deberá colocar como usuario root lo siguiente:

```
Iftop –i eth0
```

A continuación se presentará una pantalla como la que se muestra a continuación:

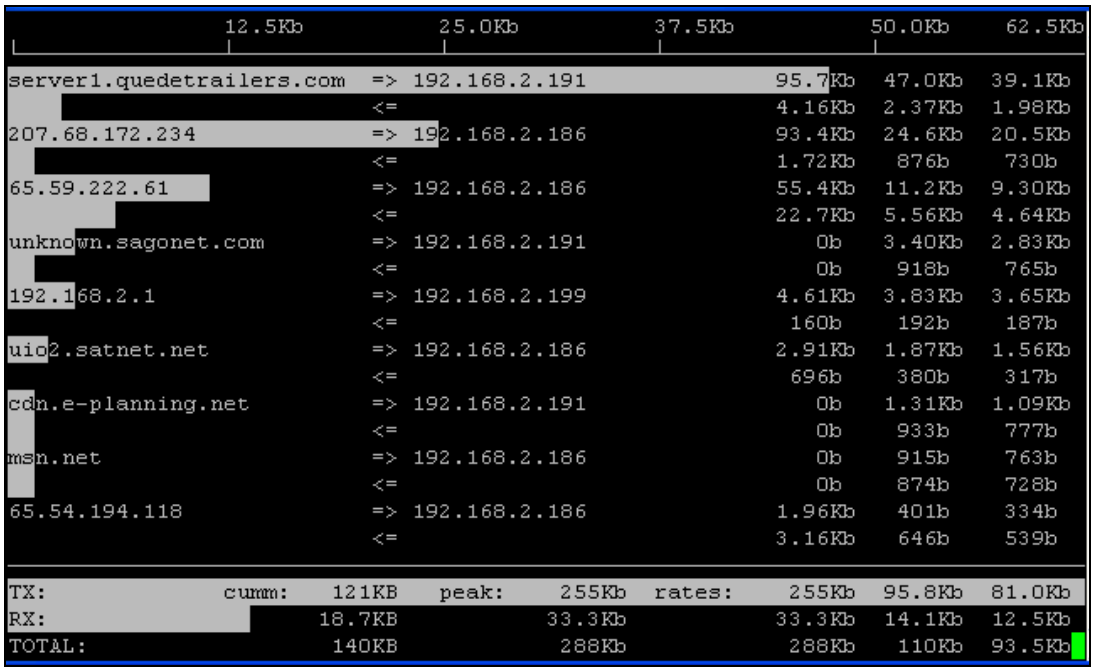


Figura. 2.67. Monitorización de interfaces del servidor

Aquí se muestra el tráfico producido en la interfaz interna de red. Se ve claramente la dirección IP de un equipo en una red ingresando a un sitio Web determinado y el consumo de ancho de banda utilizado.

Existen 5 columnas: la primera muestra el sitio Web visitado, la segunda la dirección IP de la PC que está navegando, las tres últimas el ancho de banda consumido en diferentes instantes de tiempo

En la parte baja se muestra el ancho de banda total proporcionado por el proveedor de servicios tanto en transmisión como en recepción.

Para salir de este programa se debe presionar la letra q

2.6.2 NTOP

NTOP es un software que permite analizar el tráfico de la red de manera gráfica vía Web.

Se lo puede descargar desde el sitio de repositorios de paquetes rpm www.pbone.net

Se lo instala y configura como todo programa en Linux. Se ejecuta el comando respectivo para la instalación de paquetes rpm y se configura el servicio e el archivo respectivo, en este caso se encuentra ubicado en */etc* y su nombre es *ntop.conf.*

Una vez realizadas las configuraciones según criterio del administrador, se procede a iniciar el servicio y a acceder al mismo.

El acceso se lo realiza utilizando cualquier tipo de browser de la siguiente manera:

http://<ip del servidor>:3000/

El acceso se lo realiza utilizando el puerto 3000, según lo especificado en el archivo de configuración.

A continuación se muestra la pantalla principal del software en la cual se indican las estadísticas del tráfico global.

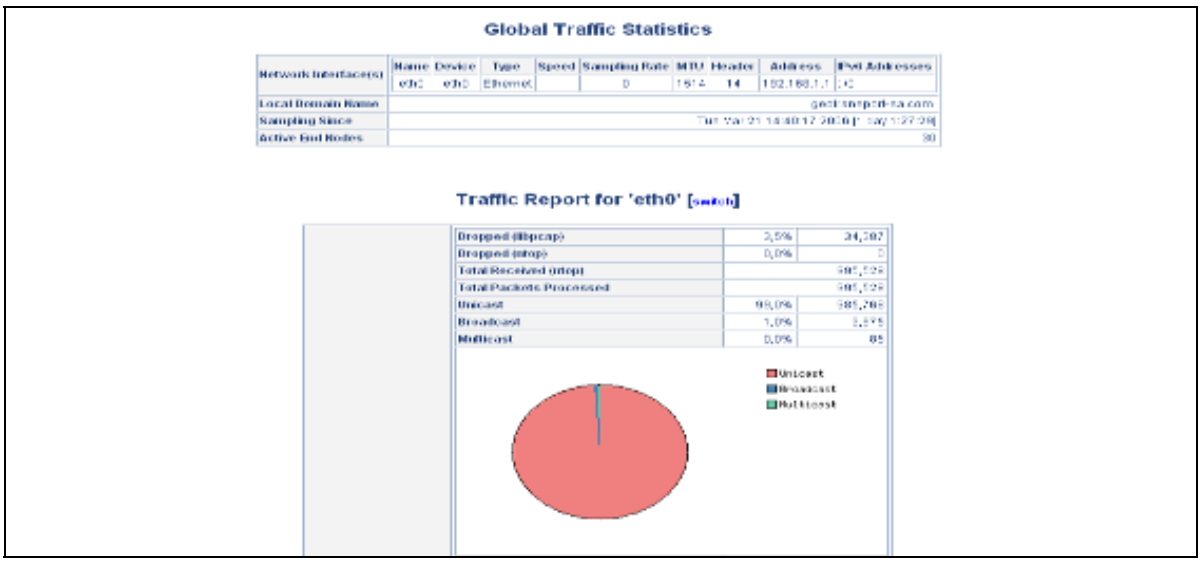


Figura. 2.68. Estadísticas del NTop

2.7 ADMINISTRACIÓN

2.7.1 Webmin

Para realizar la administración gráfica del servidor vía Web, se debe instalar el paquete llamado Webmin, en cualquiera de sus extensiones tal como está indicado en le apartado 2.2.2.

En caso de escoger la instalación de paquetes rpm, se debe tener en cuenta que harán falta algunas librerías, la cuales deberán ser instaladas previamente. Estas son:

perl-Authen-PAM
perl-Convert-VER
perl-Mon
perl-Net-SSLeay

Todas se las puede descargar del sitio Web http://dag.wieers.com

Una vez instalado no requiere mayor configuración. Un dato importante que se debe considerar es que se trata de acceso a sitio Web seguro https y que el puerto de ingreso es el 10000.

Para poder ingresar a la configuración del servidor vía Web, se debe colocar en un browser lo siguiente:

https://<dirección IP del servidor>:10000

El acceso se lo puede realizar desde la red interna LAN o desde un sitio remoto, siempre y cuando el servidor posea una dirección IP pública y se encuentren habilitados los permisos necesarios para el acceso al servidor por el puerto 10000 como se explicó en la configuración del firewall en el punto 2.5.1.

Una vez que se realiza el acceso se debe ingresar como usuario root con su respectiva contraseña, así:

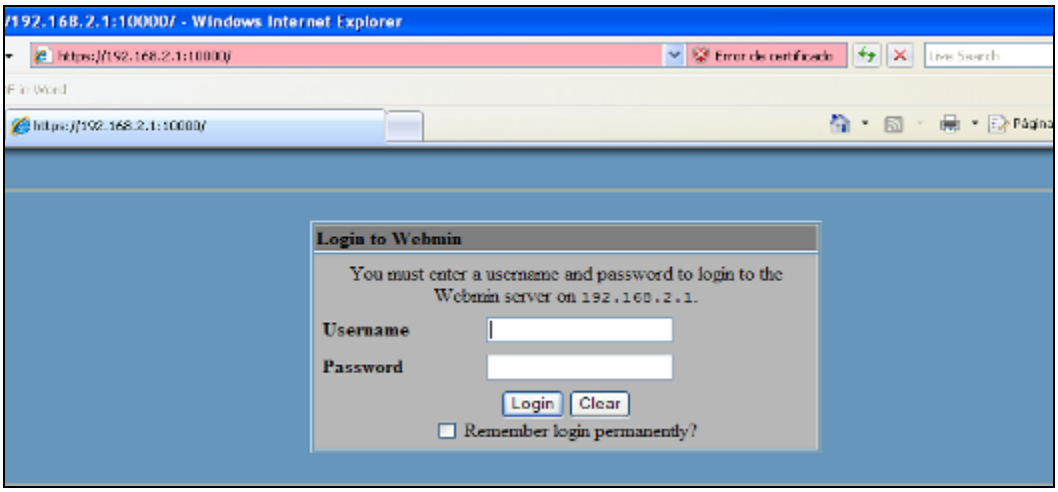


Figura. 2.69. Usuario y password de Webmin

Una vez ingresado, se presenta una pantalla, en la cual se puede realizar la administración del servidor. En la parte superior se tiene unos íconos que indican el tipo de servicio al cual se quiere acceder:

Figura. 2.70. Menú principal de Webmin

En la pantalla que se indica arriba, se tiene las opciones generales para la administración del webmin. Aquí se puede configurar principalmente lo que se refiere a presentación y lenguaje del webmin, usuarios del mismo, entre otros.

En la opción sistema lo más importante es la creación de usuarios y grupos. Para acceder a esta opción, se debe dar clic en la ficha *Usuarios y Grupos*, y de manera muy

sencilla se puede crear un usuario nuevo. Dicho usuario funcionará para acceder a los servicios de mail y ftp.

Figura. 2.71. Ficha sistema del webmin

Una vez ingresado a la opción Usuarios y Grupos, se escoge la ficha *Crear un nuevo usuario* y se despliega un cuadro como el que se muestra a continuación:

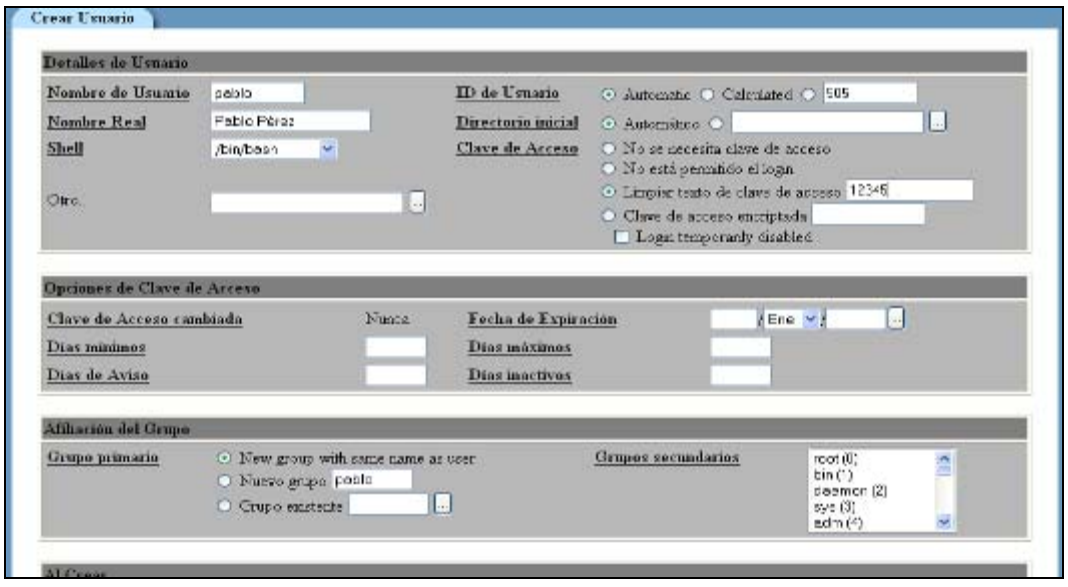


Figura. 2.72. Creación de usuarios

Se debe colocar cada campo como se indica en la figura, para que todo funcione correctamente.

Cada usuario deberá tener un *Nombre de Usuario* diferente, al igual que el *Nombre Real,* el *ID de Usuario;* y, la *Clave de Acceso.*

El campo *Shell* deberá ser siempre /bin/bash, con la finalidad de que el servicio ftp funcione para cada uno de los usuarios a ser considerados para el uso de este servicio.

Los otros valores se los puede dejar por defecto, a menos que los requerimientos del administrador sean diferentes.

Una vez ingresados los datos se escoge la ficha *Crear* para ingresar al nuevo usuario.

De la misma manera, se puede crear grupos de usuarios, así:

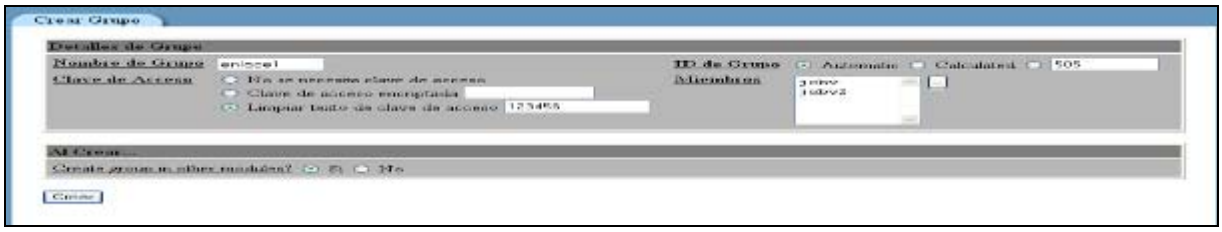


Figura. 2.73. Creación de grupos

A continuación se explicará la parte correspondiente a la ficha servidores. Los principales aspectos a ser considerados aquí son:

- Administración del acceso remoto ssh
- Administración del servicio DHCP

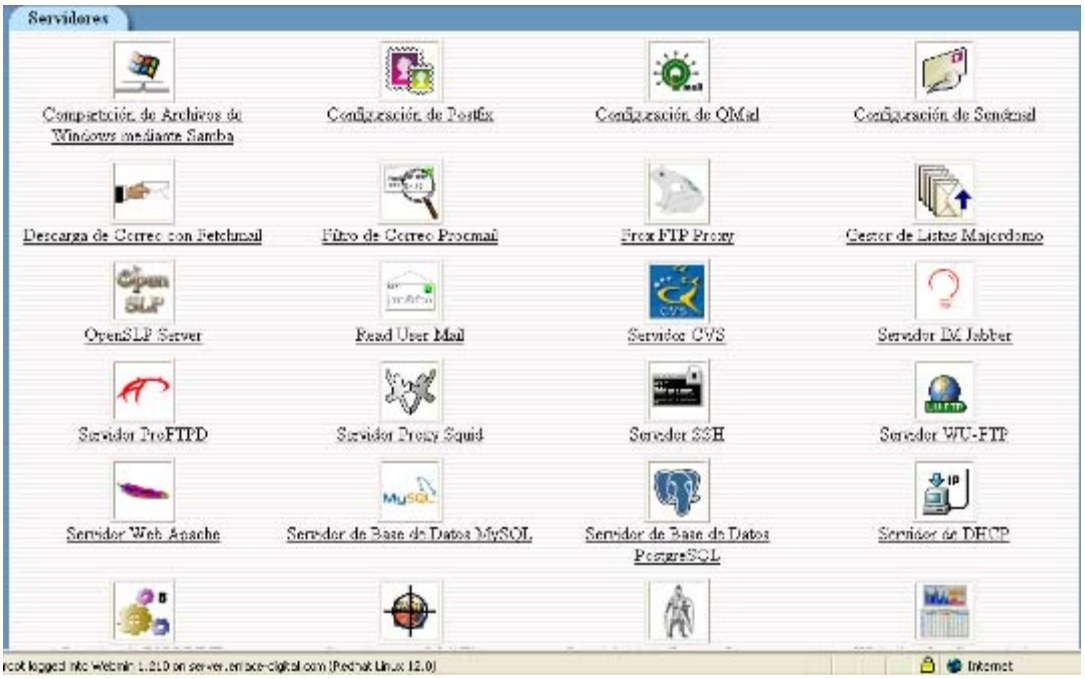


Figura. 2.74. Opciones de la ficha servidores

Para la administración del acceso remoto ssh se debe establecer el cambio de dirección IP y de puerto mediante el cual se producirá la conexión remota. Esto se lo hace escogiendo la ficha indicada como *Servidor ssh* en el menú de la lista de servidores.

Una vez aquí se escoge la opción *En red,* se coloca la dirección IP del equipo que va a tener acceso al servidor de manera remota y el puerto según criterio del administrador de red. Como es conocido el puerto ssh por defecto va a ser el 22, pero es recomendable cambiarlo por seguridad con un puerto público a partir del 1024 hasta el 65536

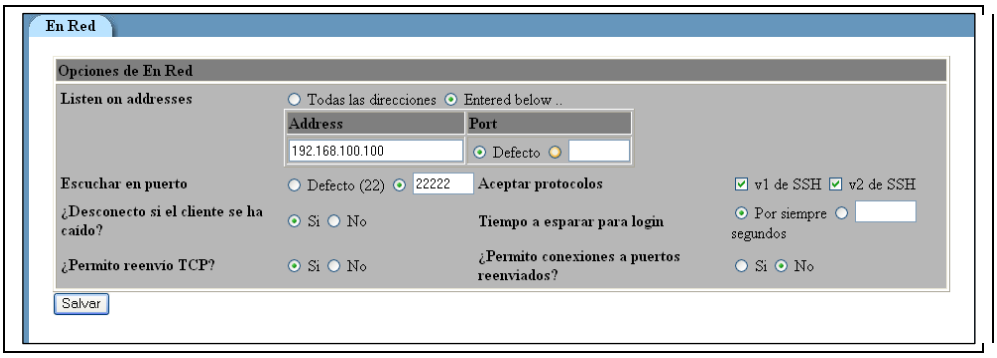


Figura. 2.75. Opciones del servicio ssh

En segunda instancia se presenta la administración del servicio dhcp, la cual se la puede realizar escogiendo la ficha indicada como *Servidor de DHCP* en el menú de la lista de servidores.

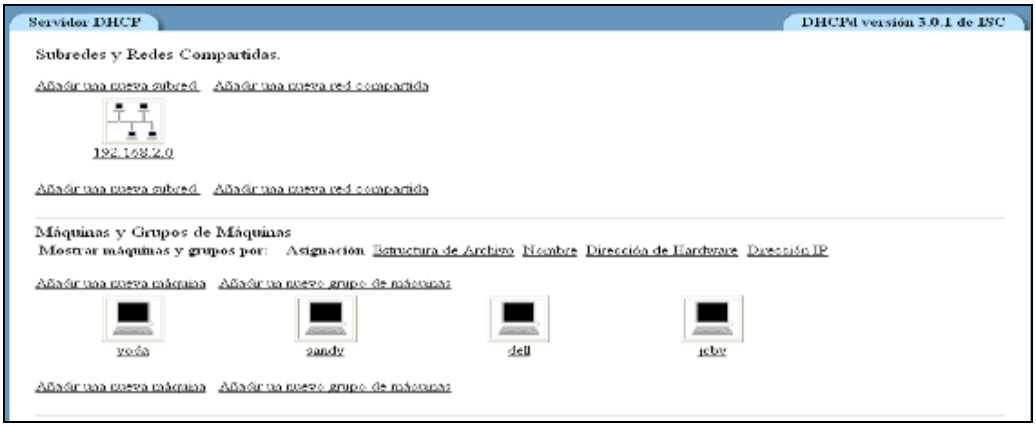


Figura. 2.76. Opciones del servicio dhcp

Aquí se puede establecer subredes de acuerdo a los requerimientos del administrador, se puede añadir hosts que tengan direcciones IP fijas y adicionalmente establecer el rango de direcciones del servidor dhcp.

Ahora se explicará la configuración de la red mediante el uso de Webmin. Aquí lo más importante constituye el hecho de que se puede mirar las interfaces de red conectadas Escogiendo la ficha *Configuración de Red,* se presenta el siguiente cuadro:

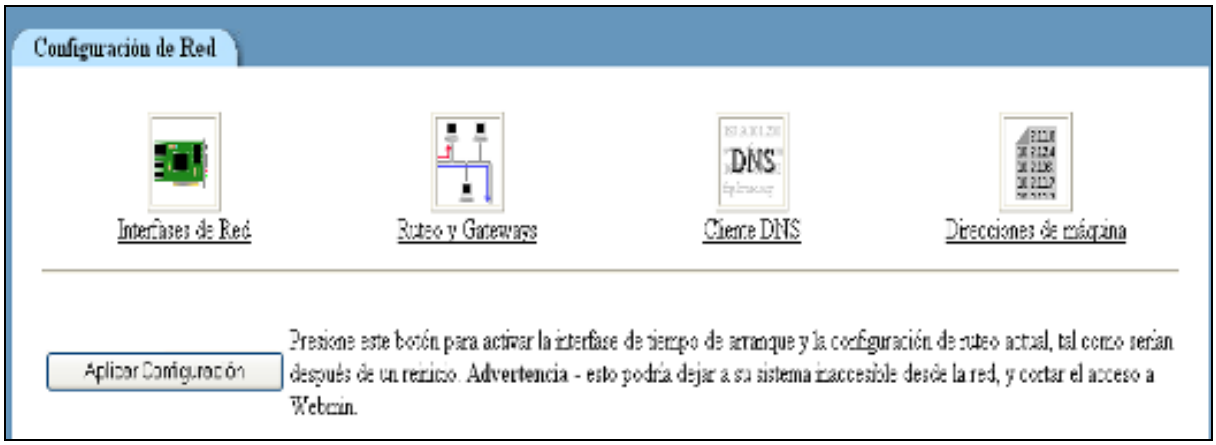


Figura 2.77. Configuración de red

En la pestaña interfaces de red, se puede constatar el estado de las tarjetas de red con sus direcciones respectivas como se muestra a continuación:

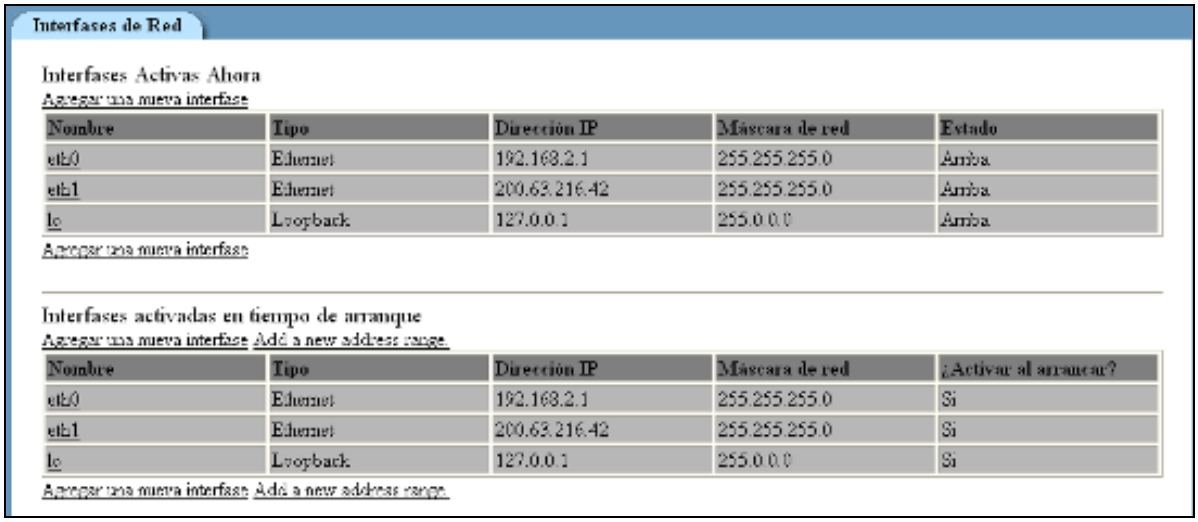


Figura. 2.78. Interfaces de red

Otro aspecto importante en la ficha de *Red*, constituye el monitoreo del ancho de banda. Esta herramienta brinda da estadísticas del comportamiento de la red en bytes, con la posibilidad de escoger el día y la hora sobre la cual se requiera realizar el monitoreo:

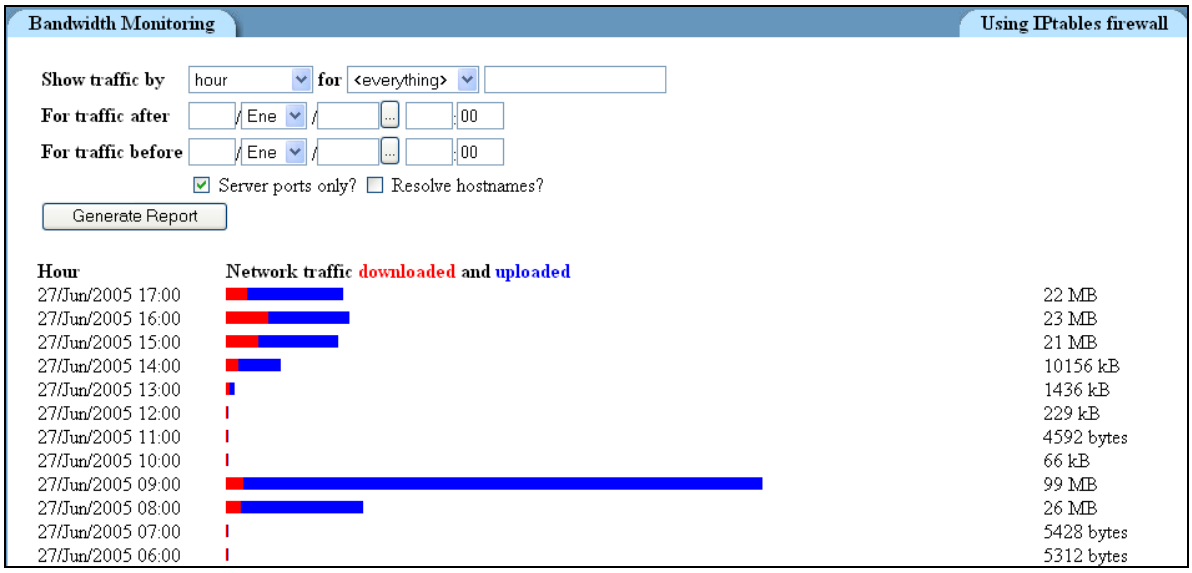


Figura. 2.79. Monitoreo del ancho de banda

Una vez terminados los aspectos más importantes de la configuración de la red, se explicará el último punto que constituye la opción *Otros*. El principal punto es la ficha "*Estado de Sistema y de Servidor"*, aquí se puede establecer el monitoreo de los diferentes servicios levantados en el servidor, con la gran ventaja de poder recibir un correo en caso de que alguno de los servicios deje de funcionar:

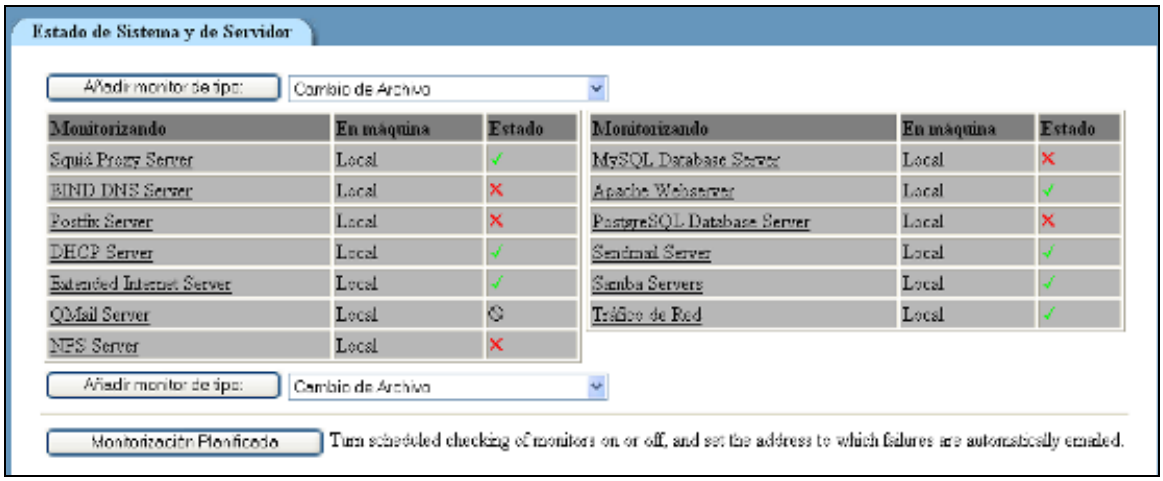


Figura. 2.80. Estado de Sistema y Servidor

Para poder recibir un mensaje de correo que alerte de algún problema con el servidor, hay que escoger la opción *Monitorización Planificada* y llenar los datos requeridos de la siguiente manera: (se debe especificar la dirección de correo a la que nos interese recibir los mensajes).

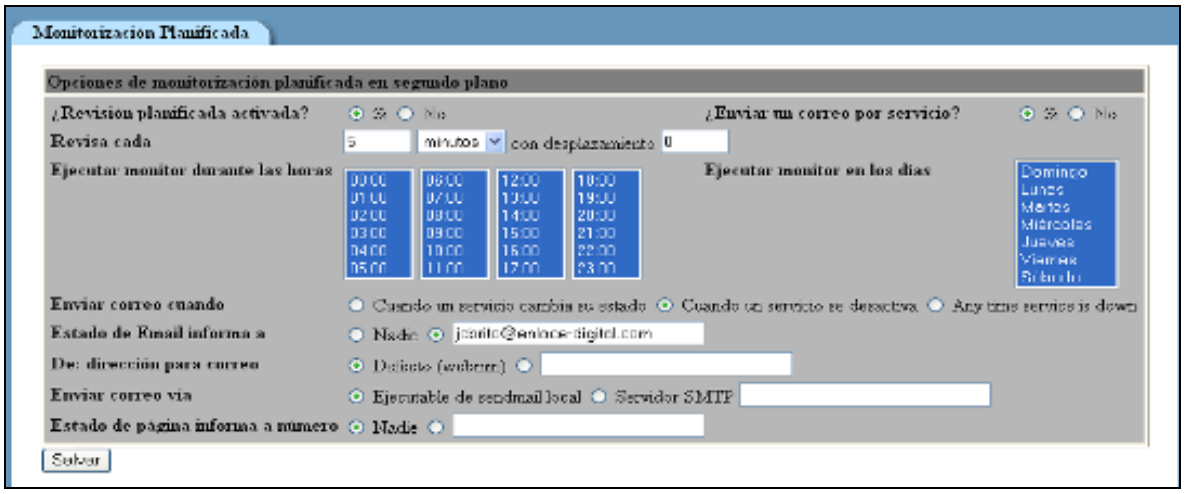


Figura. 2.81. Monitorización Planificada

2.7.2 SSH

Administración remota en modo texto

Una forma muy útil de realizar la administración del servidor, constituye el hecho de poderla realizar mediante el uso del servicio ssh[22].

Para poder ingresar de forma remota, debemos utilizar el programa llamado *putty* que de manera sencilla se lo puede descargar desde el sitio Web:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Una vez que se ejecuta este software, para ingresar al servidor desde cualquier sitio de la red LAN o desde Internet, se debe colocar la dirección IP del servidor seguida del puerto especificado en la configuración ssh. (Por lo regular el puerto 22)

[22] *SSH (*Protocolo de conexión segura a los servidores*)*

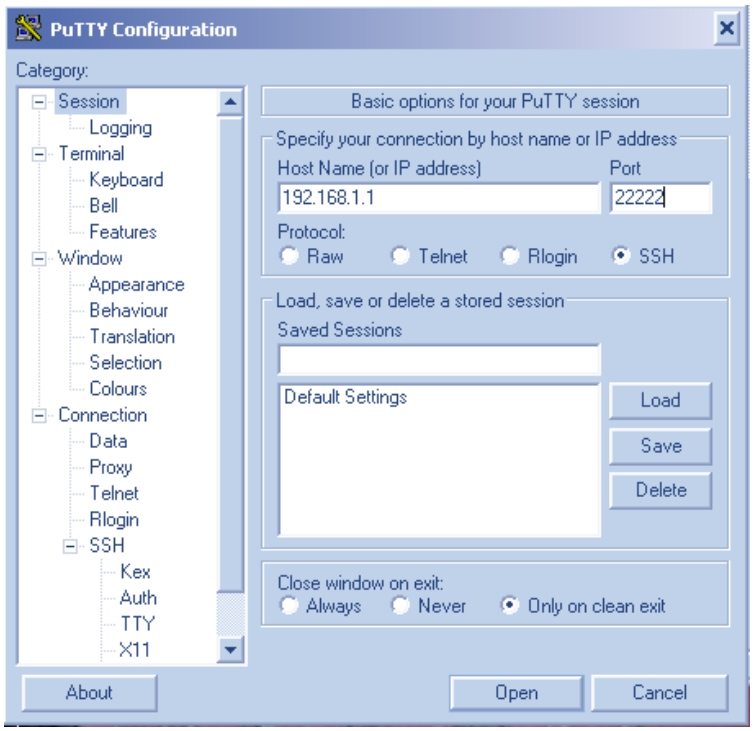


Figura. 2.82. Software PuTTY de administración y monitoreo del servidor

Al hacer clic sobre la ficha *open,* se presentará una pantalla como la siguiente:

Figura. 2.83. Pantalla de inicio del putty

Una vez aquí, se debe ingresar un nombre de cualquier usuario diferente de root (administrador) que se encuentre creado en el servidor y que cuente con los permisos necesarios para el ingreso.

Cuando se ha conseguido el ingreso como un usuario sin privilegios, para acceder al servidor como administrador se debe colocar el siguiente comando:

su –

Posteriormente pedirá el password de root. Al ingresarlo de manera correcta se tendrá acceso total al servidor de aplicaciones.

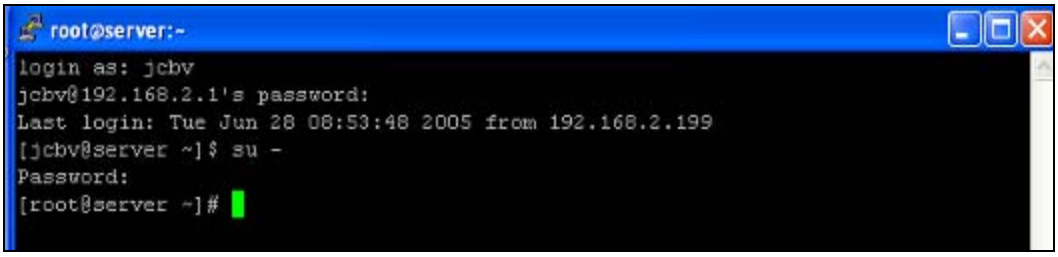


Figura. 2.84. Ingreso al servidor como administrador

2.7.3 WinSCP

Herramienta Windows para acceso al servidor

La herramienta de acceso WinSCP, permite ingresar al servidor Linux para realizar operaciones de transferir archivos entre los sistemas operativos Windows y cualquier versión de Linux.

Para poder tener acceso a este servicio se debe instalar el software en cualquier PC con sistema operativo Windows y ejecutarlo como se muestra a continuación:

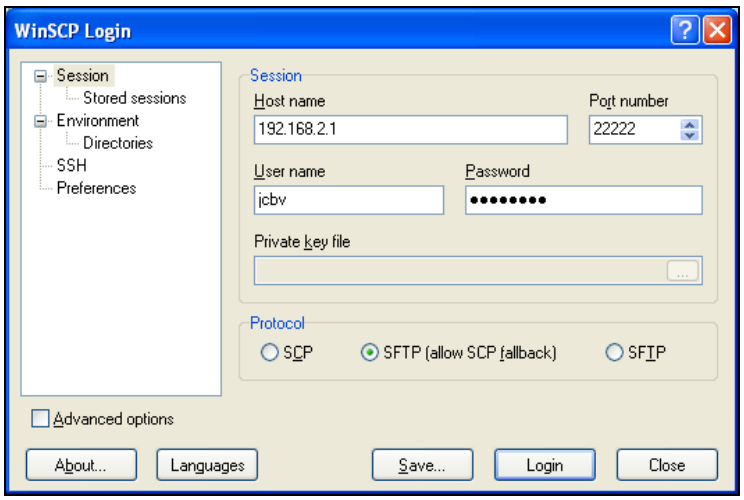


Figura. 2.85. Herramienta de acceso WinSCP

En esta imagen, se puede apreciar claramente que para realizar el acceso al servidor se debe colocar la IP y el puerto de acceso junto con un usuario sin privilegios, así como su contraseña.

Posteriormente se presentará una pantalla como la que se indica a continuación:

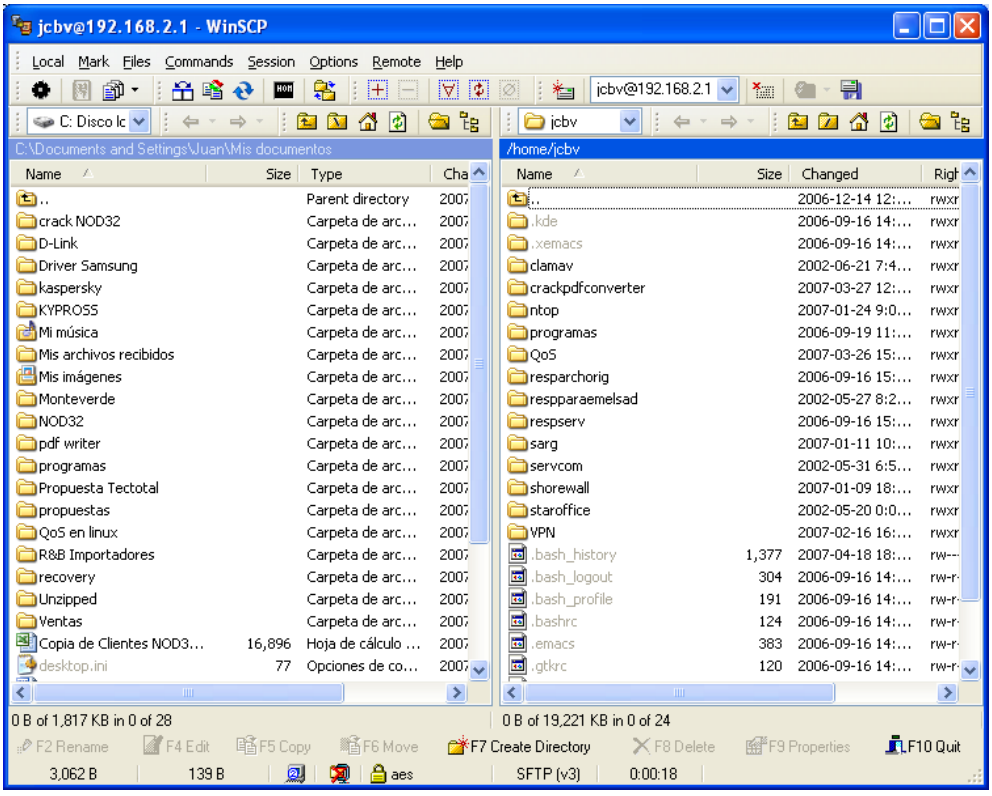


Figura. 2.86. Visualización de directorios Windows y Linux

Aquí se tiene dos tipos de ambientes. En el uno se puede apreciar el disco local C con todos sus archivos y carpetas y en el otro la carpeta del usuario en Linux.

Se pueden copiar o cortar e incluso eliminar todo tipo de archivos, siempre y cuando se tengan los permisos necesarios tanto en Windows como en Linux.

CAPITULO 3

WIRELESS

3.1 INTRODUCCIÓN A REDES WIRELESS LAN

3.1.1 Wireless como medio de red

La tecnología wireless ha ganado un amplio campo de aplicación en los últimos años, ya sea por una necesidad de su uso o por su versatilidad en cuanto a movilidad del usuario. El entorno wireless es una opción de red, a veces apropiada y otras veces necesaria. Realmente la mayoría de las redes sin cables constan de componentes wireless que se comunican con una red que utiliza cableado, es una red de componentes mezclados llamada red híbrida.

Consiste en un tipo de comunicación basado en el protocolo IEEE 802.11 o WI-FI que define el empleo de las capas más bajas del modelo OSI. En general los protocolos 802.x definen la tecnología de la red; las WLAN no utilizan un medio de propagación físico, sino se utiliza la modulación de ondas electromagnéticas de alta frecuencia, baja potencia que usan una banda específica y las cuales se propagan por el espacio sin un medio físico que una los extremos de la transmisión.

Con respecto al alcance máximo del área de cobertura, las distancias son equiparables a las conseguidas con cableado (alrededor de 100 metros) si bien se pueden conseguir mayores distancias utilizando antenas. El alcance máximo es teórico ya que en la práctica, se ve reducido por las causas como interferencias electromagnéticas y elementos arquitectónicos.

Figura. 3.1. Cobertura mundial de las redes Wireless

Los sistemas WLAN utilizan para su funcionamiento las bandas de frecuencia 902-928 Mhz , 2.400-2.483 Ghz y 5725-5850 Ghz, también conocidas como ISM (Industrial, Científica, Médica), por las que no hace falta pagar ninguna licencia y se pueden usar libremente.

Estas condiciones de libertad de utilización, sin necesidad de licencia, han propiciado que el número de equipos, especialmente computadoras, que utilizan las ondas para conectarse, a través de redes inalámbricas haya crecido notablemente.

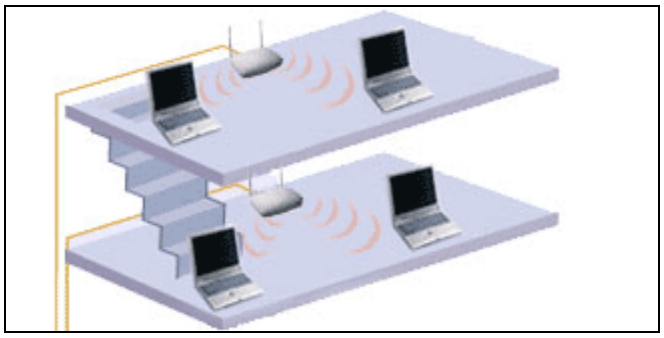


Figura. 3.2. Transmisión Wireless

Las redes WLAN (Wireless Local Area Network) o Red de Área Local Inalámbrica se diferencian de las convencionales principalmente en la capa física, y en la capa de enlace de datos (MAC[23]), según el modo de referencia OSI[24]. La capa física indica como

[23] *MAC (Media Access Control Address)*
[24] *OSI (Open System Interconnection)*

son enviados los bits de una estación a otra, la capa MAC se encarga de describir cómo se empaquetan y verifican los bits de manera que no tengan errores.

Las redes wireless están llamando la atención porque sus componentes pueden:

- Ofrecer conexiones temporales a una red cableada existente.
- Ayudar a proporcionar respaldo a una red existente.
- Ofrecer algún grado de portabilidad.
- Extender las redes más allá de los límites de las conexiones físicas

3.1.2. Tecnologías wireless

Las redes wireless se pueden dividir en tres categorías, basándose en su tecnología:

- LAN.
- LAN extendidas.
- Computación móvil.

La diferencia fundamental entre estas categorías radica en las facilidades de transmisión. Las LAN y las LAN extendidas wireless utilizan transmisores y receptores propiedad de la compañía en donde funciona la red. La computación móvil utiliza medios de transporte público, como las compañías telefónicas de servicios de larga distancia, junto con compañías telefónicas locales y sus servicios públicos, para transmitir y recibir señales.

3.1.2.1 LAN

Excepto por el medio utilizado, una red wireless típica opera de forma similar a una red cableada: en cada una de los equipos se instala una tarjeta de red wireless con un transceptor, es decir que realiza tanto funciones de transmisión como de recepción con comunicación semiduplex, es decIr enviar señales en ambos sentido pero no simultáneamente. Los usuarios se comunican con la red como si estuvieran utilizando equipos con cables.

Puntos de acceso

El transceptor, dispositivo que realiza funciones tanto de transmisión como de recepción usando componentes de circuitos comunes para ambas funciones, a veces

Técnicas de transmisión

Las LAN wireless utilizan cuatro técnicas para transmitir datos:

- Transmisión infrarroja.
- Transmisión láser.
- Transmisión por radio de banda estrecha (frecuencia única).
- Transmisión por radio de amplio espectro.

Transmisión infrarroja: Todas las redes wireless infrarrojas operan utilizando un rayo de luz infrarroja para llevar los datos entre los dispositivos. Estos sistemas necesitan generar señales muy fuertes, porque las señales de transmisión débiles son susceptibles de interferencias desde fuentes de luz, como ventanas. Este método puede transmitir señales a altas velocidades debido al gran ancho de banda de la luz infrarroja. Una red infrarroja normalmente puede transmitir a 10 Mbps.

Hay cuatro tipos de redes infrarrojas:

- **Redes de línea de visión:** transmite sólo si el transmisor y el receptor tienen una línea de visión despejada entre ellos.

- **Redes infrarrojas de dispersión:** En esta tecnología, las transmisiones emitidas rebotan en paredes y suelo y, finalmente, alcanzan el receptor. Éstas son efectivas en un área limitada de unos 30,5 metros.

- **Redes reflectoras:** Los transceptores ópticos situados cerca de los equipos transmiten a una posición común que redirige las transmisiones al equipo apropiado.

- **Telepunto óptico de banda ancha:** ofrece servicios de banda ancha y es capaz de ofrecer requerimientos multimedia de alta calidad que pueden alcanzar los ofrecidos por una red cableada.

Tienen dificultad para transmitir a distancias mayores de 30,5 metros (100 pies). También están supeditados a interferencias de la fuerte luz ambiental que se encuentra en los entornos comerciales.

Trasmisión láser: La tecnología láser es similar a la infrarroja, ya que necesita una línea de visión directa y cualquier persona o cosa que interfiera el rayo láser bloqueará la transmisión.

Transmisión por radio de banda estrecha (frecuencia única) . Este método es similar a la transmisión desde una estación de radio. El usuario sintoniza el transmisor y el receptor a una cierta frecuencia. Ésta no necesita situarse en la línea de visión, porque el rango de transmisión es de 3.000 metros (9.842 pies). Sin embargo, como la señal es de alta frecuencia, está supeditada a la atenuación del acero y los muros. La radio de banda estrecha es un servicio de suscripción. Este método es relativamente lento; la transmisión está en el rango de los 4,8 Mbps.

Transmisión por radio de amplio espectro. Transmite señales en un rango de frecuencias. Esto ayuda a evitar los problemas de las comunicaciones de banda estrecha.

Las frecuencias disponibles se dividen en canales, conocidos como hops o saltos, que se pueden comparar con una etapa de un viaje que incluye la intervención de una serie de paradas entre el punto de inicio y el destino. Los adaptadores de amplio espectro sintonizan en un hop específico por una cantidad de tiempo predeterminada, y después pasan a un hop diferente. Una secuencia de saltos determina la coordinación. Los equipos de la red están todas sincronizadas para coordinar el hop. Este tipo de señalización ofrece una cierta seguridad incorporada, ya que el algoritmo de salto de frecuencia de la red tendría que conocerse para obtener el flujo de datos.

Para aumentar la seguridad y evitar que los usuarios no autorizados escuchen la emisión, el emisor y el receptor pueden cifrar la transmisión.

La tecnología de radio de amplio espectro ofrece una red realmente wireless. Por ejemplo, dos o más equipos equipados con adaptadores de red de amplio espectro y un sistema operativo con capacidades de red predeterminadas pueden actuar como una red de trabajo sin cables de conexión. Además, las redes wireless se pueden vincular a una red existente añadiendo una interfaz apropiada a uno de los equipos de la red.

Aunque algunas implementaciones de radio de amplio espectro pueden ofrecer velocidades de transmisión de 4Mbps a distancias de unos 3,22 kilómetros (dos millas) en exteriores y 244 metros (800 pies) en interiores, la velocidad típica de 250 Kbps (Kilobits por segundo) hace que este método sea bastante más lento que otras opciones de red wireless.

Transmisión punto a punto

Utiliza una tecnología punto a punto que transfiere datos desde un equipo a otro en lugar de comunicarse entre varios equipos y periféricos. Sin embargo, los componentes adicionales como transceptores de host y transceptores únicos están disponibles. Éstos se pueden implementar en equipos individuales o en equipos que ya están en una red para formar una red de transferencia de datos wireless.

Esta tecnología implica la transferencia de datos serie wireless con estas características:

- Utiliza un enlace de radio punto a punto para la transmisión de datos rápida y libre de errores.
- Atraviesa paredes, techos y suelos.
- Soporta índices de datos desde 1,2 a 38,4 Kbps hasta 61 metros (200 pies) en interiores o unos 0,5 kilómetros (0.30 millas) con transmisión a la vista.

Este tipo de sistema transfiere datos entre equipos, o entre equipos y otros dispositivos como impresoras o lectores de código de barras.

3.1.2.2 LAN extendidas

Otros tipos de componentes wireless pueden funcionar en un entorno LAN extendido, de forma similar a su contrapartida cableada. Por ejemplo, un bridge LAN wireless puede conectar redes separadas hasta 4,8 kilómetros (tres millas).

Conexión wireless multipunto

Un bridge wireless es un componente que ofrece una forma sencilla de poder conectar edificios sin utilizar cables. De la misma forma que un puente ofrece un camino

entre dos puntos, un bridge wireless ofrece una camino de datos entre dos edificaciones. Con variaciones que dependen de condiciones atmosféricas y geográficas, esta distancia puede ser superior a 4,8 kilómetros (tres millas).

Aunque es costoso, tal componente se podría justificar porque elimina el gasto de las líneas alquiladas.

Bridge wireless de gran alcance

Si los bridges wireless no llegan lo suficientemente lejos, otra alternativa a considerar son los bridges wireless de gran alcance. Éstos también utilizan tecnología de radio de amplio espectro para ofrecer bridges Ethernet y Token Ring, pero para una distancia superior a 40 kilómetros (unas 25 millas).

Como con los bridge wireless originales, el coste de los bridge de gran alcance se podría justificar porque elimina la necesidad de la línea T1 o enlaces de microondas.

Una línea T1 es una línea de comunicaciones de alta velocidad que puede tener comunicaciones digitales y acceso a Internet a una velocidad de 1,544 Mbps.

3.1.2.3 Computación móvil

Los empleados que están de viaje pueden utilizar esta tecnología con equipos portátiles o asistentes digitales personales (PDA) para intercambiar mensajes de correo electrónico, archivos u otra información. Aunque esta forma de comunicación tiene sus ventajas, es lenta. La velocidad de transmisión oscila entre los 8 kbps y los 19,2 kbps. La velocidad es menor cuando se incluye la corrección de errores. La computación móvil incorpora adaptadores wireless que utilizan tecnología telefónica celular para conectar equipos portátiles con redes cableadas. Los equipos portátiles utilizan pequeñas antenas para comunicarse con las torres de radio en áreas circundantes. Los satélites en órbita cercanos a la tierra recogen las señales de baja potencia de los dispositivos de red móviles y portátiles.

3.1.3 Topología de red

La topología de red corresponde a la disposición lógica de los dispositivos de red

Las redes inalámbricas pueden construirse con o sin Punto de Acceso (AP), esto es lo que nos determina si es una "Ad-Hoc" o una "Infraestructura".

- Topología Ad-Hoc. Red *peer to peer*.

Al igual que las redes cableadas Ethernet, en las cuales compartimos el medio (cable) y se pueden realizar varias "conversaciones" a la vez entre distintos Host, el medio de las redes WLAN (aire) dispone de un identificador único para cada una de esas "conversaciones" simultaneas que se pueden realizar, es una dirección MAC (48 bits).

En el caso de las redes Ad-Hoc, este número MAC es generado por el adaptador inalámbrico que crea "la conversación", y es un identificador MAC aleatorio.

Cuando un adaptador Wireless es activado, primero pasa a un estado de "escucha", en el cual, durante unos 6 segundos está buscando por todos los canales alguna "conversación" activa. Si encuentra alguno, le indicará al usuario a cual se quiere conectar.

En el supuesto de que no se pueda conectar a otro Host que ya estuviera activo, pasa a "crear la conversación", para que otros equipos se puedan conectar a él.

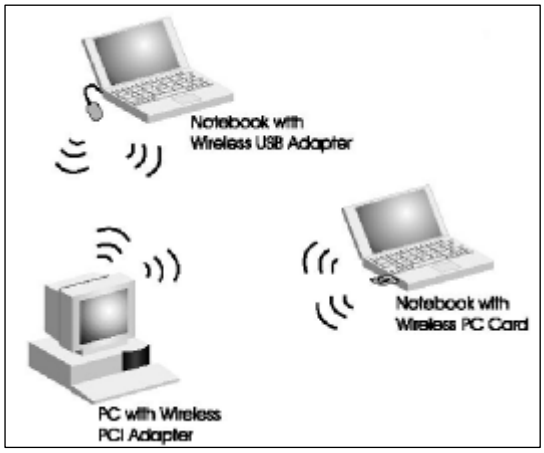


Figura. 3.3. Topología punto a punto

BSSID:

Para una determinada WLAN con topología Adhoc, todos los equipos conectados a ella (Host) deben de ser configurados con el mismo Identificador de servicio básico (Basic Service Set, BSSID)

Modo Adhoc: como máximo puede soportar 256 usuarios.

- Topología Infraestructura,

En el cual existe un nodo central (Punto de Acceso WiFi) que sirve de enlace para todos los demás (Tarjetas de Red Wifi). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del access point.

Ahora la MAC que identifica a esta "conversación" es la MAC del AP (MAC real)

El modo Infraestructura como máximo puede soportar 2048 nodos/usuarios. Pero si se hace un uso del ancho de banda "intensivo", como con juegos o multimedia, de 6 a 8 usuarios es el máximo recomendable.

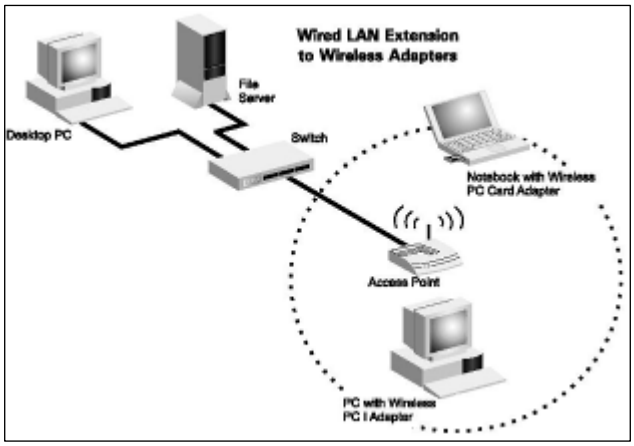


Figura. 3.4. Topología infraestructura

Modos de topología infraestructura

Todos los dispositivos, independientemente de que sean tarjetas de red o access point tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo:

- **Modo Managed**, es el modo en el que la tarjeta de red se conecta al access point para que éste último le sirva de "concentrador". La tarjeta de red sólo se comunica con el access point.

- **Modo Master**. Este modo es el modo en el que trabaja el access point, pero en el que también pueden entrar las tarjetas de red si se dispone del firmware[25] apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como access point realmente tarjetas de red a las que se les ha añadido cierta funcionalidad extra vía firmware o vía SW[26]. Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro y bajo una distribución especial de linux llamada LINUXAP - OPENAP.

Esta afirmación se ve confirmada al descubrir que muchos access point en realidad lo que tienen en su interior es una placa de circuitos integrados con un Firmware añadido a un adaptador PCMCIA[27] en el cual se le coloca una tarjeta PCMCIA idéntica a las que funcionan como tarjeta de red.

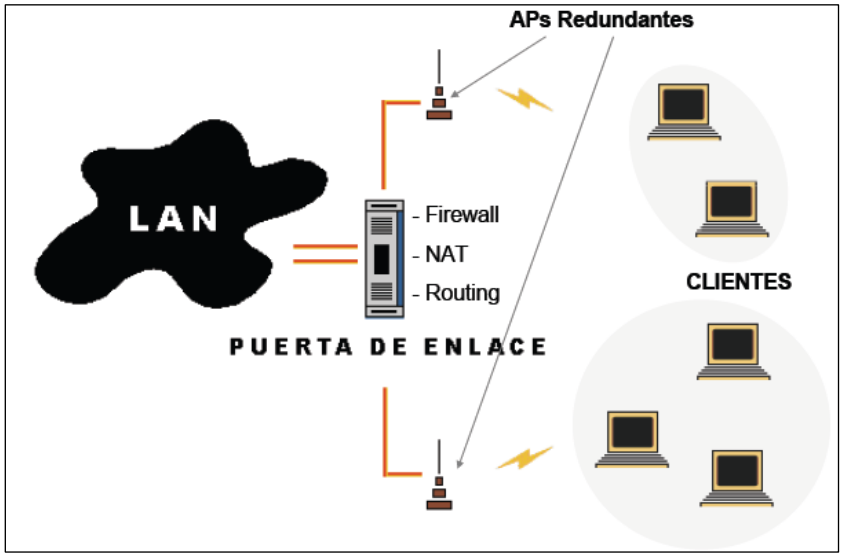


Figura. 3.5. Ejemplo de topología Wireless

[25] *Firmware (es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria tipo ROM, que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.)*
[26] *SW (Software)*
[27] *PCMCIA (Personal Computer Memory Card International Association)*

3.1.4. Dispositivos Wireless

En esencia, las características de una red inalámbrica son las mismas que las de las redes convencionales. De hecho, son completamente compatibles, hasta el punto que los r*outers wireless* suelen incorporar conexiones RJ45 para conectar equipos a través de cable. También existen dispositivos que permiten realizar puentes entre ambas tecnologías. Son los denominados puntos de acceso, que funcionan a modo de switch inalámbrico (permiten que equipos con receptores wireless entren dentro de la red de cableado).

También existen modelos que realizan la operación inversa: recogen la señal del aire para incorporarla a una red cableada, así como repetidores de señal para conectar puntos demasiado distantes. Desde aquí, cualquier dispositivo de red ya se encuentra disponible para la tecnología WiFi: servidores de impresión y juegos y receptores de todo tipo de interfaces (PCMCIA, PCI[28] o USB[29]), si bien cada vez es más normal que los equipos nuevos incluyan algún tipo de receptor integrado en la placa base. En cuanto al acceso a Internet, los fabricantes han pensado también en los usuarios con ADSL, de modo que resulta fácil encontrar *routers* compatibles con esta tecnología que nos permiten contar con acceso a Internet desde cualquier punto de la casa o la oficina sin necesidad de realizar cableado alguno.

En los últimos meses, han aparecido en el mercado novedosos productos cuyo éxito o fracaso se hará patente a corto plazo. Es el caso de las cajas wireless para discos duros, que permiten habilitar una unidad para ser compartida en toda la red. De hecho, existen pequeños aparatos localizadores de redes inalámbricas. Con diversas formas, y discretamente camuflados a modo de llavero, con sólo pulsar un botón estos dispositivos nos informan de la presencia de alguna red WiFi y de su nivel de intensidad en el punto en el que nos encontramos.

Las mayoría de soluciones inalámbricas soportan la modalidad de **Infraestructura** (configuración punto de acceso), la modalidad **Ad-Hoc** (configuración sin punto de acceso), la modalidad **Bridging** para realizar conexiones Building to Building en modalidad inalámbrica, la modalidad **Cliente Inalámbrico** para poder transformar

[28] *PCI (Peripheral Component Interconnect)*
[29] *USB (Universal Serial Bus)*

prácticamente cualquier dispositivo en inalámbrico y la modalidad de **Repetidor** que nos ayudará a expandir las áreas de cobertura de los puntos de acceso. Entre algunos de ellos tenemos:

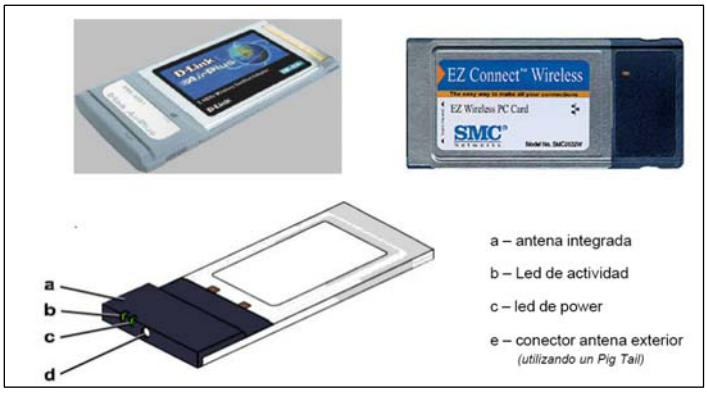


Figura. 3.6. Tarjetas PCMCIA para portátiles

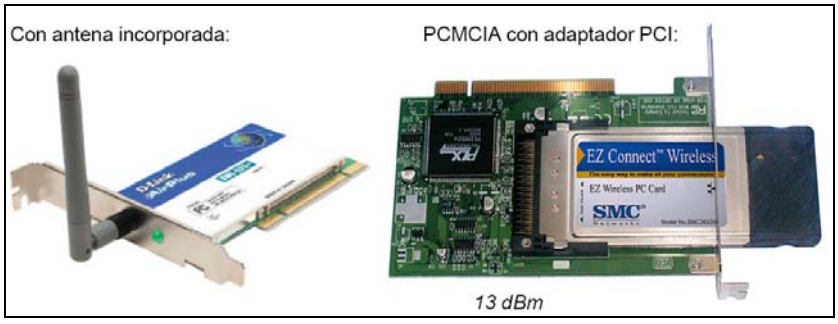


Figura. 3.7. Tarjetas PCI para PC's de escritorio

Figura. 3.8. Adaptadores USB

Figura. 3.9. Puntos de acceso, similares a HUB o concentradores

Ante el crecimiento de la tecnología Wi-Fi a un nivel cada vez más popular, las empresas fabricantes de dispositivos tecnológicos de redes no se quedaron atrás y comenzaron a producir aparatos con este tipo de tecnología. Unos de los poseedores de estas dotes más usados son los celulares: los más modernos ya poseen tecnologías como Bluetooth y Wi-Fi, que les permiten conectarse a las redes caseras Wireless para compartir sus recursos y tomar de la red otros disponibles, como *ring tones*, fondos de pantalla, música MP3 y hasta documentos de paquetes de oficina.

Figura. 3.10. Tarjeta wi-fi

Otras de las nuevas estrellas de la tecnología Wireless son los teclados: varios de los más modernos ya vienen sin cables y nos evitan la conexión cableada a la PC. En este rubro, también se hicieron presentes los mouse que ya están allí sin su antiguo cable con conector PS/2 o serial.

Figura. 3.11. Teclado y Mouse inalámbrico

Existen otros como son los servidores de impresión inalámbricos, o las cámaras inalámbricas, pero solamente son aplicaciones de wireless, no son dispositivos que permitan crear redes WLAN.

3.1.5 Mercado de las redes Wireless LAN

En cuanto compete a campo tecnológico, la industria ha tenido un vertiginoso avance en la creación de nuevos servicios y soluciones que tienen como base la convergencia de redes y la infraestructura asociada a las mismas.

No importa que una empresa sea multinacional, de tamaño mediano o microempresa. No importa el sector en el que se esté operando. En mayor o menor medida, las nuevas tecnologías, Internet y el comercio electrónico (e-business) afectarán o ya han afectado a los negocios en su estrategia o en la manera cómo se plantea el trabajo interno y las relaciones comerciales.

Los dispositivos móviles constituyen un paso más, y representan un medio más a disposición de las empresas que saben que para crecer, para ser más competitivas y mejorar sus procesos, deben acercarse a las nuevas tecnologías e incorporarlas en su

negocio en la medida de lo justo y necesario para que éstas les faciliten el desarrollo empresarial.

Las ventas de aparatos con conexión inalámbrica se incrementarán gracias a factores como la extensión de los estándares, el aumento de la interoperabilidad, la creciente demanda de aparatos portátiles o la aparición de nuevas aplicaciones.

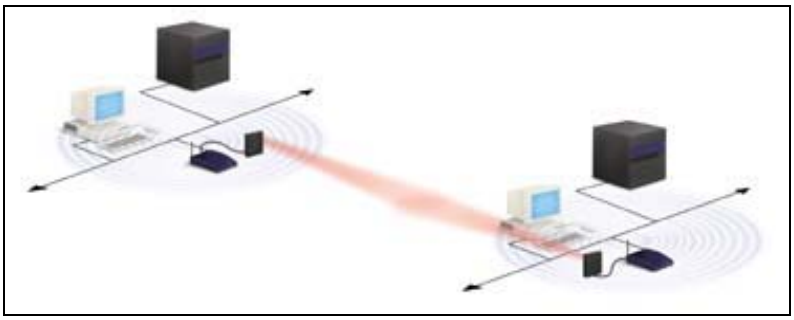


Figura. 3.12. Red WLAN

Por el lado de la oferta, la intensa competencia en un mercado en el que todavía no existen claros dominadores conduce a un progresivo abaratamiento de los precios.

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

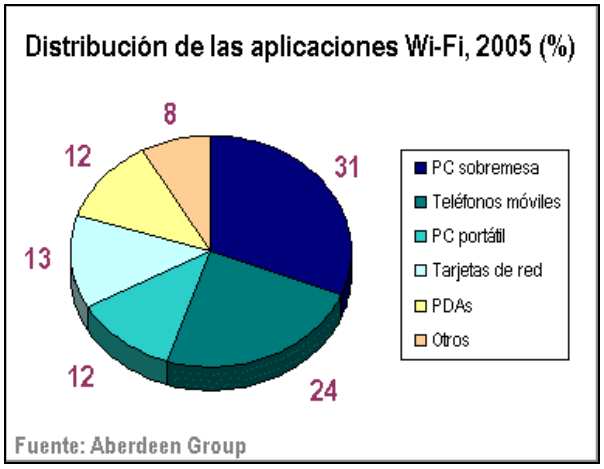


Figura. 3.13. Mercado de las redes WLAN

La aparición en el mercado de los laptops y los PDA (Personal Digital Assistant), y en general de sistemas y equipos de informática portátiles es lo que ha generado realmente la necesidad de una red que los pueda acoger, o sea, de la WLAN.

De esta manera, la WLAN hace posible que los usuarios de ordenadores portátiles puedan estar en continuo movimiento, al mismo tiempo que están en contacto con los servidores y con los otros ordenadores de la red, es decir, la WLAN permite movilidad y acceso simultáneo a la red.

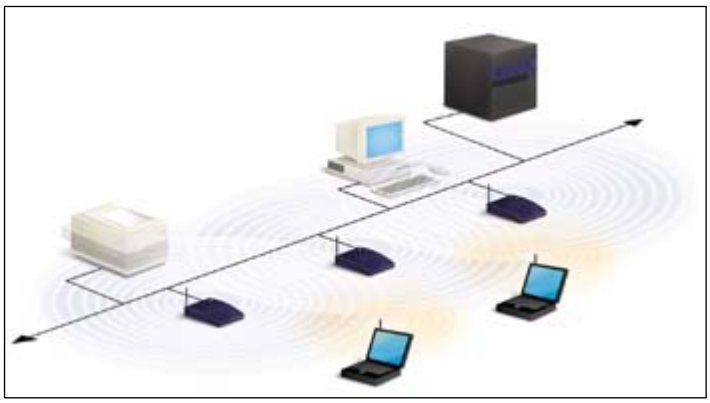


Figura. 3.14. Movilidad de equipos Portátiles dentro de una WLAN

En una LAN convencional, cableada, si una aplicación necesita información de una base de datos central tiene que conectarse a la red mediante una estación de acogida , pero no puede estar en movimiento continuo y libre. La WLAN puede ser autocontenida o bien puede actuar como una extensión de la red de cable Ethernet o Token-Ring.

3.1.5.1 Ventajas de WLANs sobre las redes alámbricas

Movilidad: Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red alámbrica.

Simplicidad y rapidez en la instalación: La instalación de una red inalámbrica puede ser tan rápida y fácil y además que puede eliminar la posibilidad de tender cable a través de paredes y techos.

Flexibilidad en la instalación: La tecnología inalámbrica permite a la red ir donde la alámbrica no puede ir.

Costo de propiedad reducido: Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN alámbrica, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.

Escalabilidad: Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

3.1.5.2 Algunos problemas asociados con la tecnología inalámbrica

Los hornos de microondas utilizan radiaciones en el espectro de 2.45 Ghz. Es por ello que las redes y teléfonos inalámbricos que utilizan el espectro de 2.4 Ghz. pueden verse afectados por la proximidad de este tipo de hornos, que pueden producir interferencias en las comunicaciones.

Otras veces, este tipo de interferencias provienen de una fuente que no es accidental. Mediante el uso de un perturbador o inhibidor de señal se puede dificultar e incluso imposibilitar las comunicaciones en un determinado rango de frecuencias.

3.1.6 Principales aplicaciones

Para implementar una red wireless es necesario tomar en cuenta varios parámetros como:

- Medio físico
- Ancho de banda necesario.
- Longitud y extensión de la red.
- Seguridad.
- Número de usuarios.
- Posibilidades de ampliación.

- Nuevas soluciones de mercado y tendencias inminentes.
- Coste y Tiempo.

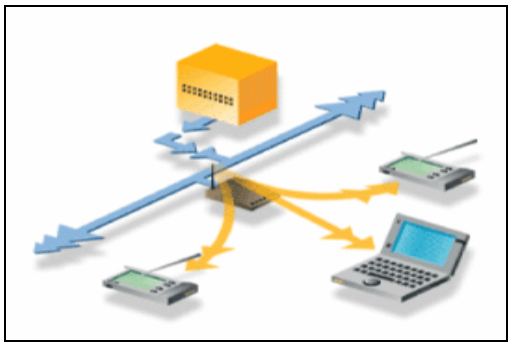


Figura. 3.15. Esquema de red wireless

El mercado de las soluciones inalámbricas alcanzó en el año 2002 un volumen de negocio de unos 1.600 millones de dólares y según todas las previsiones, se espera que experimente un crecimiento anual del 20%, a pesar de algunos factores en su contra que frenan este desarrollo como los problemas de seguridad y la diversidad de estándares.

Originalmente las redes WLAN fueron diseñadas para el ámbito empresarial. Sin embargo, en la actualidad han encontrado una gran variedad de escenarios de aplicación, tanto públicos como privados: entorno residencial y del hogar, grandes redes corporativas, PYMES[30], zonas industriales, campus universitarios, entornos hospitalarios, ciber-cafés, hoteles, aeropuertos, medios públicos de transporte, entornos rurales, etc. Incluso son ya varias las ciudades en donde se han instalado redes inalámbricas libres para acceso a Internet.

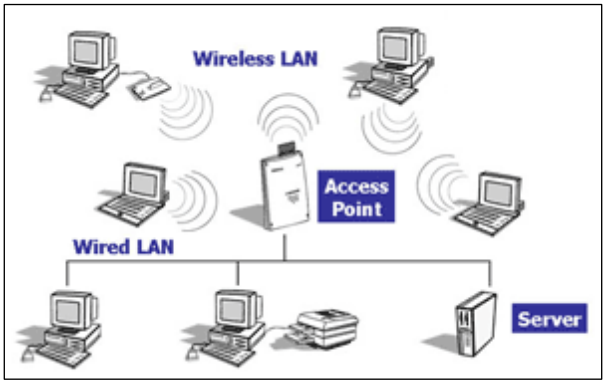


Figura. 3.16. Disposición de un access point dentro de una red wireless

[30] PYMES (Un tipo de empresa con un número reducido de trabajadores, y cuya facturación es moderada.)

La tendencia a la movilidad y la ubicuidad hacen cada vez más utilizados los sistemas inalámbricos, y el objetivo es ir evitando los cables en todo tipo de comunicación, no solo en el campo informático sino en televisión, telefonía, Seguridad, Domótica, etc.

Figura. 3.17. Tendencia a movilidad

La tecnología de redes inalámbricas ofrece movilidad y una instalación sencilla, además permite la fácil ampliación una red.

Un fenómeno social que ha adquirido gran importancia en todo el mundo como consecuencia del uso de la tecnología inalámbrica son las comunidades wireless que consisten en agrupaciones que buscan la difusión de redes alternativas a las comerciales.

La dificultad intrínseca en la instalación de las redes con cable es un factor que empujará a una mayor aceptación de los entornos sin cable. La conexión sin cable puede ser especialmente útil para redes:

- En sitios concurridos, como áreas de recepción y salas de espera.
- Para usuarios que están constantemente moviéndose, como médicos y enfermeras en hospitales.
- Áreas y edificios aislados.
- Departamentos donde la ubicación física cambia frecuentemente y de forma no predecible.

- Estructuras, como construcciones históricas, donde el cableado representa un reto.

Actualmente, las redes locales inalámbricas (WLAN) se encuentran instaladas mayoritariamente en algunos entornos específicos, como almacenes, bancos, restaurantes, fábricas, hospitales y transporte. Las limitaciones que, de momento, presenta esta tecnología ha hecho que sus mercados iniciales hayan sido los que utilizan información tipo "bursty" (períodos cortos de transmisión de información muy intensos seguidos de períodos de baja o nula actividad) y donde la exigencia clave consiste en que los trabajadores en desplazamiento puedan acceder de forma inmediata a la información a lo largo de un área concreta, como un almacén, un hospital, la planta de una fábrica o un entorno de distribución o de comercio al por menor; en general, en mercados verticales.

El previsible aumento del ancho de banda asociado a las redes inalámbricas y, consecuentemente, la posibilidad del multimedia móvil, permitirá atraer a mercados de carácter horizontal que surgirán en nuevos sectores, al mismo tiempo que se reforzarán los mercados verticales ya existentes. La aparición de estos nuevos mercados horizontales está fuertemente ligada a la evolución de los sistemas PCS[31] (Personal Communications Systems), en el sentido de que la base instalada de sistemas PCS ha creado una infraestructura de usuarios con una cultura tecnológica y hábito de utilización de equipos de comunicaciones móviles en prácticamente todos los sectores de la industria y de la sociedad.

Esa cultura constituye un gran motor generador de demanda de más y más sofisticados servicios y prestaciones, muchos de los cuales han de ser proporcionados por las WLAN. De hecho, según datos de la CTIA (Celular Telephone Industry Associations), los clientes de los proveedores de servicios por radio se muestran en general satisfechos con los servicios recibidos, pero esperan más tanto en términos de servicio como de precio, tanto en el contexto celular como PCS.

[31] *PCS (Personal Communications Services)*

3.2 ACCESS POINT

3.2.1 Conceptos básicos

Se trata de un dispositivo inalámbrico que mediante sistema de radio frecuencia se encarga de recibir información de diferentes estaciones móviles. Este dispositivo capta la información de las estaciones y las transmite a un servidor, que puede ser único o formar parte de una red, cableada, más extensa. Su alcance aproximado es de 100 metros.

Figura. 3.18. Access Point

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. Este o su antena son normalmente colocados en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena.

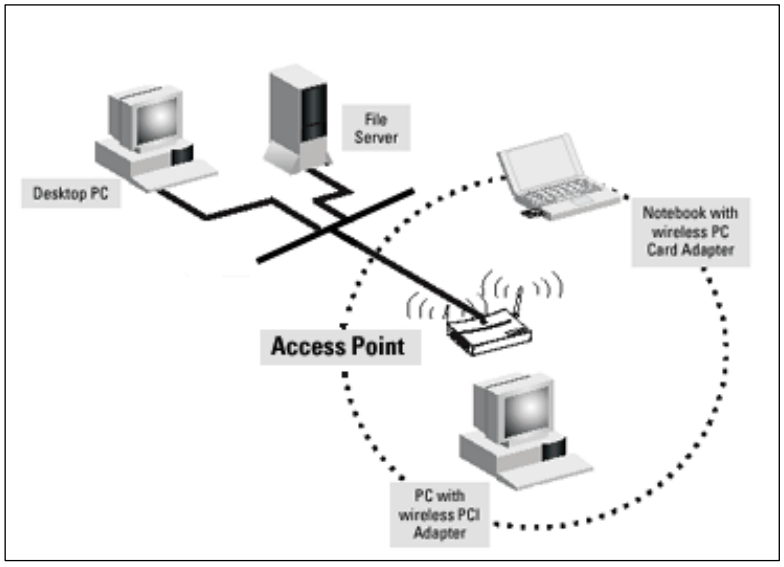


Figura. 3.19. Conexión de un AP en la red

Esta maravilla de la técnica surgida hace pocos años soluciona muchos problemas pues, al evitar estar "atados" a un cable, permite movilidad, comodidad, estética, ahorros de instalaciones, etc.

3.2.2 Tecnología Wi-Fi

WiFi (Wireless Fidelity) es un nombre comercial desarrollado por un grupo de comercio industrial llamado WiFi Alliance (Inicialmente: 3Com – Aironet [hoy parte de CISCO] – Harris – Lucent – Nokia y Symbol technologies, hoy más de 150 miembros), el nombre “oficial” de esta alianza es **WECA** (Wireless Ethernet Compatibility Alliance) y son los primeros responsables de 802.11b.

WiFI describe los productos de WLAN basados en los estándares 802.11 y está pensado en forma más “Amigable” que la presentación eminentemente técnica que ofrece IEEE.

En un principio, la expresión Wi-Fi era utilizada únicamente para los aparatos con tecnología 802.11b, el estándar dominante en el desarrollo de las redes inalámbricas, de aceptación prácticamente universal, que funciona en una banda de frecuencias de 2,4 GHz

y permite la transmisión de datos a una velocidad de hasta 11Mbps (aunque la velocidad real de transmisión depende en última instancia del número de usuarios conectados a un punto de acceso). Con el fin de evitar confusiones en la compatibilidad de los aparatos y la interoperabilidad de las redes, el término Wi-Fi se extendió a todos los aparatos provistos con tecnología 802.11 (ya sea 802.11a, 802.11b, 802.11g, 802.11i, 802.11h, 802.11e, con diferentes frecuencias y velocidades de transmisión).

Una Wireless LAN WI-FI se basa en una arquitectura de celdas, cada una de las cuales es llamada “Basic Service Set” (BSS). Una BSS es un conjunto de estaciones WI-FI fijas o móviles. Para acceder a la transmisión, el medio es controlado por cierto conjunto de reglas llamado “coordination function”. WI-FI define una función de coordinación distribuida o “distributed coordination function” (DCF) y “point coordination function” (PCF)

Alternativamente, una infraestructura BSS puede ser parte de una extensa red, a esto se lo llama “extended service set” (ESS). Un ESS es el conjunto de una o más infraestructuras BSS conectadas vía distribution system, cuya naturaleza no esta especificada por el estándar, de hecho las estaciones conectadas a un sistema de distribución son los AP.

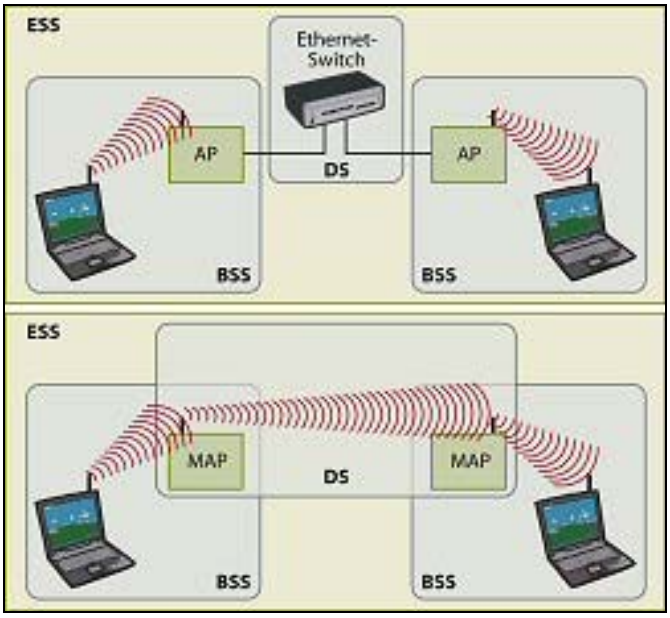


Figura. 3.20. Estructura típica de una red WI-FI

La tecnología WiFi ha nacido como una tecnología con la que poder unir puntos en los que la infraestructura tradicional no llega, además de poder acceder sin cables ofreciendo una total libertad de movimientos, siendo posible su instalación en todo tipo de establecimientos.

La tecnología Wi-Fi hace posible que los usuarios accedan a Internet y a las redes locales de su empresa a través de banda ancha y de forma inalámbrica, tanto desde su propio lugar de trabajo como desde entornos públicos o privados de uso público.

También existen servicios Wi-Fi orientados a aquellos entornos privados de uso público (aeropuertos, hoteles, escuelas de negocios, recintos feriales etc.) que quieran posibilitar a sus empleados y clientes el acceso en banda ancha y sin cables a Internet y a las aplicaciones de sus propias empresas.

3.2.2.1 Operación básica de WI-FI

Al accionar una estación WI-FI, se exploran los canales disponibles para poder activar una red donde las señales empiezan a transmitirse. Si se selecciona una red, de cualquier tipo de topología analizada anteriormente en el ítem 3.1.3. Posteriormente, se autentica a sí mismo y con el access point AP, viene entonces la asociación, si la seguridad WEP o WPA es activada, se debe realizar un paso futuro de autenticación.

Luego de este proceso cualquiera de las estaciones puede participar en la red. WI-FI provee diferentes acuerdos para brindar calidad de servicio QoS[32], los rangos van desde priorizar el mejor esfuerzo (best effort) en la estructura de red y garantizar el servicio.

Las estaciones de trabajo pueden descubrir nuevas redes acorde a la potencia que genere cada una de ellas con sus equipos y asociarse con una de estas nuevas redes. Así, las estaciones además pueden deambular entre redes que comparten un sistema de distribución común, es decir con la capacidad de roaming que mantiene celdas de cobertura, es decir perpetuar el servicio cuando una estación cambia de un AP a otro.

[32] *QoS (Quality of Service)*

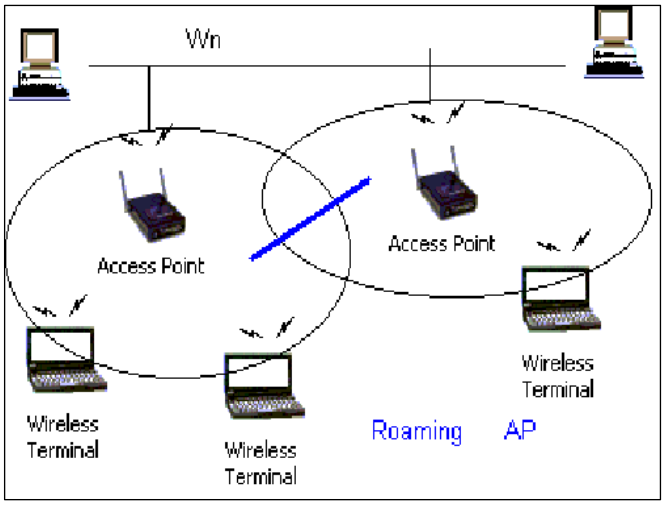


Figura. 3.21. Cobertura roaming de los AP

Finalmente una estación puede estar inactiva para ahorro de energía, y puede desasociarse y desautenticarse del AP si lo desea.

3.2.3 Estándares 802.11 a, b, g

Este estándar desarrollado por el Instituto de Ingeniería Eléctrica y Electrónica IEEE 802.11, describe las normas a seguir por cualquier fabricante de dispositivos Wireless para que puedan ser compatibles entre si.

En 1990, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN. Pero no es hasta 1994 cuando aparece el primer borrador.

El protocolo **IEEE 802.11** o **WI-FI** es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local LAN.

Figura. 3.22. Estándar para Wireless Ethernet

3.2.3.1 Los estándares de WLAN

Para seleccionar una de las alternativas de conectividad inalámbrica contempladas bajo el estándar IEEE 802.11, es fundamental analizar brevemente la historia, estado actual y desarrollo con el fin de encontrar la más acorde al servicio a brindarse.

Entre los principales estándares se encuentran:

Tabla. 3.1. Cuadro comparativo de estándares WLAN

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras– Temporales), y AES (Estándar de Encriptación Avanzado).

Protocolos

802.11 legacy

La versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión *teóricas* de 1 y 2 mega bit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM (Industrial, Scientific and Medical) a 2,4 GHz. IR sigue siendo parte del estándar, pero no hay implementaciones disponibles.

El estándar original también define el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la calidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. El estandar 802.11b funciona en la banda de 2.4 GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP(Transmission Control Protocol) y 7.1 Mbit/s sobre UDP.

802.11a

En 1997 la IEEE (Instituto de Ingenieros Eléctricos Electrónicos) crea el Estándar 802.11 con velocidades de transmisión de 2Mbps.

En 1999, el IEEE aprobó ambos estándares: el 802.11a y el 802.11b.

En 2001 hizo su aparición en el mercado los productos del estándar 802.11a.

La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 Ghz y utiliza 52 subportadoras orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2.4 Ghz tiene gran uso (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos), el utilizar la banda de 5 GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

Transmisión

Exteriores

Valor Máximo A 30 metros 54 Mbps

Valor Mínimo A 300 metros 6 Mbps

Interiores

Valor Máximo A 12 metros 54 Mbps

Valor Mínimo A 90 metros 6 Mbps

802.11h

La especificación 802.11h es una modificación sobre el estándar 802.11 para WLAN desarrollado por el grupo de trabajo 11 del comité de estándares LAN/MAN del IEEE (IEEE 802) y que se hizo público en octubre de 2003. 802.11h intenta resolver problemas derivados de la coexistencia de las redes 802.11 con sistemas de Radares y Satélites en la banda de los 5 GHz (802.11a).

El desarrollo del 802.11h sigue unas recomendaciones hechas por la ITU que fueron motivadas principalmente a raíz de los requerimientos que la Oficina Europea de Radiocomunicaciones (ERO) estimó convenientes para minimizar el impacto de abrir la banda de 5 GHz, utilizada generalmente por sistemas militares, a aplicaciones ISM (ERC/DEC[33]/(99)23).

[33] *ERC/DEC/(99)23(European Radiocommunications Comitee)*

Con el fin de respetar estos requerimientos, 802.11h proporciona a las redes 802.11a la capacidad de gestionar dinámicamente tanto la frecuencia, como la potencia de transmisión.

Selección Dinámica de Frecuencias y Control de Potencia del Transmisor

DFS (*Dynamic Frequency Selection*) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz con el fin de evitar interferencias co-canal con sistemas de radar y para asegurar una utilización uniforme de los canales disponibles.

TPC (*Transmitter Power Control*) es una funcionalidad requerida por las WLAN que operan en la banda de 5GHz para asegurar que se respetan las limitaciones de potencia transmitida que puede haber para diferentes canales en una determinada región, de manera que se minimiza la interferencia con sistemas de satélite.

802.11g

En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 Ghz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión. .

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Actualmente se venden equipos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas apropiadas.

802.11n

En enero de 2004, el IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn)[34] para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 600 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operación de las redes sea mayor con este nuevo estándar gracias a la tecnología MIMO Multiple Input – Multiple Output, que permite utilizar varios canales a la vez para enviar y recibir datos gracias a la incorporación de varias antenas. Existen también otras propuestas alternativas que podrán ser consideradas y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que no es hasta principios de 2007 que no se acabe el segundo boceto. No obstante ya hay dispositivos que se han adelantado al protocolo y ofrecen de forma no oficial éste estándar (con la promesa de actualizaciones para cumplir el estándar cuando el definitivo esté implantado).

802.11e

Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso:

- (EDCA) Enhanced Distributed Channel Access y
- (HCCA) Controlled Access.

802.11i

Esta dirigido a batir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1x, TKIP (Protocolo de Claves Integra – Seguras – Temporales), y AES (Estándar de Encriptación Avanzado).

[34] *Tgn (Task Group 'n' Synchronization)*

Protocolo propietario

802.11 Super G

Hoy en día el estándar 802.11 Super G, con una banda de 2.4 Ghz y 5 Ghz, alcanza una velocidad de transferencia de 108 Mbps. De la empresa D-Link

Futuros estándares

El futuro para las WI-FI será probablemente MIMO que corresponde a IEEE 802.11n, estándar de capa física el cual actualmente está en desarrollo

Hasta hace poco los dispositivos 802.11, tenían una sola antena. Y si tenían mas, solo usaban una (siempre la mejor). Con la tecnología MIMO (Multiple Input-Multiple Output) se consigue que cada una de las antenas pueda recibir o transmitir de forma simultánea, para mejorar el rendimiento.

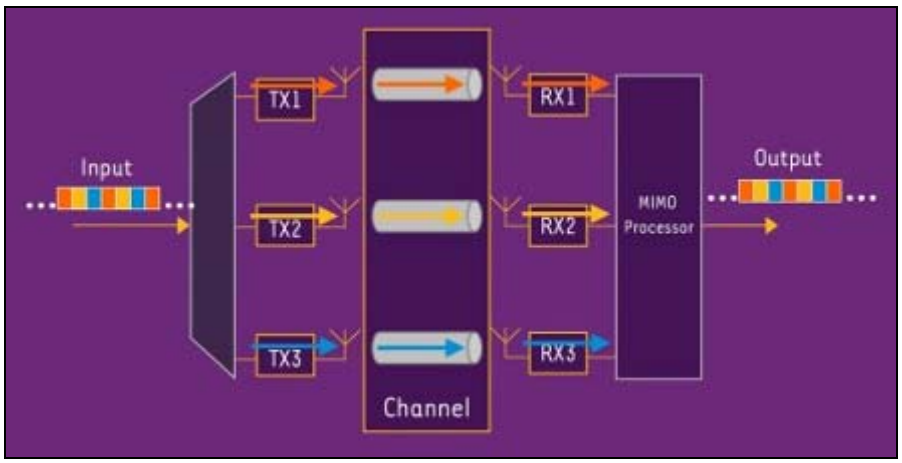


Figura. 3.23. Arquitectura MIMO

Además corrige de manera más eficiente las interferencias, y por lo tanto, la calidad de la señal recibida. Esta tecnología está siendo implementada en productos con 802.11 g, pero su potencial vendrá dado el día que se apruebe definitivamente el esperado 802.11n.

Por último otra ventaja que ofrece es la de poder trabajar con equipos de 802.11b y g sin adecuar su velocidad al más lento. Simplemente entabla la comunicación con cada uno a la velocidad especificada por el estándar.

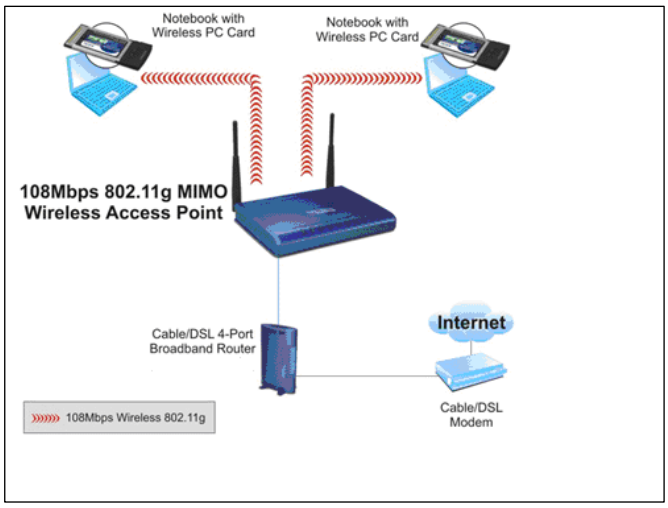


Figura. 3.24. Red implementada con equipo MIMO

Son diversos los fabricantes y los productos que se han adaptado a esta mejora del WIFI, ofreciendo compatibilidad hacia los productos inferiores.

Figura. 3.25. Router wireless MIMO

3.2.4 Canales de transmisión y radiofrecuencia

El término radiofrecuencia, también denominado espectro de radiofrecuencia o RF, se aplica a la porción del espectro electromagnético en el que se pueden generar ondas electromagnéticas aplicando corriente alterna a una antena.

3.2.4.1 Bandas de Frecuencia

Las ondas de radio reciben también el nombre de “corrientes de radiofrecuencia” (RF) y se localizan en una pequeña porción del denominado “espectro radioeléctrico” correspondiente al espectro de ondas electromagnéticas.

El espectro radioeléctrico o de ondas de radio comprende desde los 3 kHz de frecuencia, con una longitud de onda de 100 000 m (100 km), hasta los 30 GHz de frecuencia, con una longitud de onda de 0,001 m (1 mm)

Las WLAN transmiten utilizando radio frecuencias (RF) en el mismo espectro que utilizan las radios AM/FM. Algunas tecnologías WLAN utilizan los 2,4 GHz Industriales, Científicos y Médicos (ISM), mientras que otras lo hacen a través de la banda de 5 GHz UNII (Unlicensed National Information Infrastructure).

El alcance de las señales de radio varía con la frecuencia. En general, las frecuencias más bajas atraviesan los obstáculos más fácilmente, con lo cual su tendencia es a llegar a sitios más lejanos. En contraste, las altas frecuencias son más fácilmente reflejadas por muros o edificios. El conocimiento de las características de propagación de las ondas de radio es esencial para conocer a fondo las características de las WLAN.

Las ondas de radio provienen de señales de corriente alterna de alta frecuencia que se transmiten a lo largo de un cable para finalmente ser radiadas por antenas. La antena convierte esta señal en una señal “wireless”, proceso denominado como transmisión. Otra antena convierte la señal recibida en una señal de corriente alterna, a esto se denomina recepción.

Las señales RF se transmiten desde una antena en todas direcciones, sin embargo se diseña la antena para focalizar y redireccionar las ondas.

Las bandas de frecuencia son el resultado de la división del espectro electromagnético, con el objeto de delimitar el acceso de usuarios a determinadas bandas.

En los Estados Unidos y otros países, las bandas de frecuencia son de 900 MHz, 2.4 GHz y, en algunos casos, de hasta 5 GHz. Si bien estas bandas de frecuencia no requieren licencia, los equipos que las utilicen deben estar certificados por los reguladores del país donde se encuentren.

La Federal Communication Commission (FCC) es la agencia del gobierno de los Estados Unidos responsable de las regulaciones dentro de las cuales esta la de las comunicaciones interestatales. Para las WLANs, la FCC ha establecido las bandas de frecuencia de radio permitidas, límites de potencia de salida, tecnologías de transmisión, uso en interiores y exteriores, y regulaciones geográficas.

Los aparatos que no poseen licencia utilizan una potencia baja y su alcance es limitado. Estos dispositivos deben ser muy resistentes a las interferencias, debido al hecho de que no se garantiza que los usuarios posean acceso exclusivo a estas frecuencias sin licencia y, por lo tanto, pueden sufrir intrusiones.

Tabla. 3.2. Rango de frecuencias

Nombre	Abreviatura inglesa	Banda ITU	Frecuencias	Longitud de onda
			Inferior a 3 Hz	> 100.000 km
Extra baja frecuencia Extremely low frequency	ELF	1	3-30 Hz	100.000 km – 10.000 km
Super baja frecuencia Super low frequency	SLF	2	30-300 Hz	10.000 km – 1000 km
Ultra baja frecuencia Ultra low frequency	ULF	3	300–3000 Hz	1000 km – 100 km
Muy baja frecuencia Very low frequency	VLF	4	3–30 kHz	100 km – 10 km
Baja frecuencia Low frequency	LF	5	30–300 kHz	10 km – 1 km
Media frecuencia Medium frequency	MF	6	300–3000 kHz	1 km – 100 m
Alta frecuencia High frequency	HF	7	3–30 MHz	100 m – 10 m
Muy alta frecuencia Very high frequency	VHF	8	30–300 MHz	10 m – 1 m
Ultra alta frecuencia Ultra high frequency	UHF	9	300–3000 MHz	1 m – 100 mm
Super alta frecuencia Super high frequency	SHF	10	3-30 GHz	100 mm – 10 mm
Extra alta frecuencia Extremely high frequency	EHF	11	30-300 GHz	10 mm – 1 mm
			Por encima de los 300 GHz	< 1 mm

Las redes Wireless prevalecen en gran medida ante el problema de la línea de visión, ya que pasan a una frecuencia más alta que otros aparatos en el espectro electromagnético. Estas redes funcionan a unos 2.4 GHz y, en algunos casos, a mayor frecuencia. Aun así, se encuentran muy por debajo del espectro de luz visible.

Gracias al uso de esa frecuencia, la longitud de la onda es tan imperceptible que logra traspasar objetos sólidos.

Es por esto que las redes inalámbricas funcionan perfectamente sobre distancias cortas en espacios interiores, aunque en ocasiones algunos obstáculos pueden interferir en la transmisión.

Por consiguiente, a continuación se verá los materiales sólidos que más interfieren en las redes Wireless.

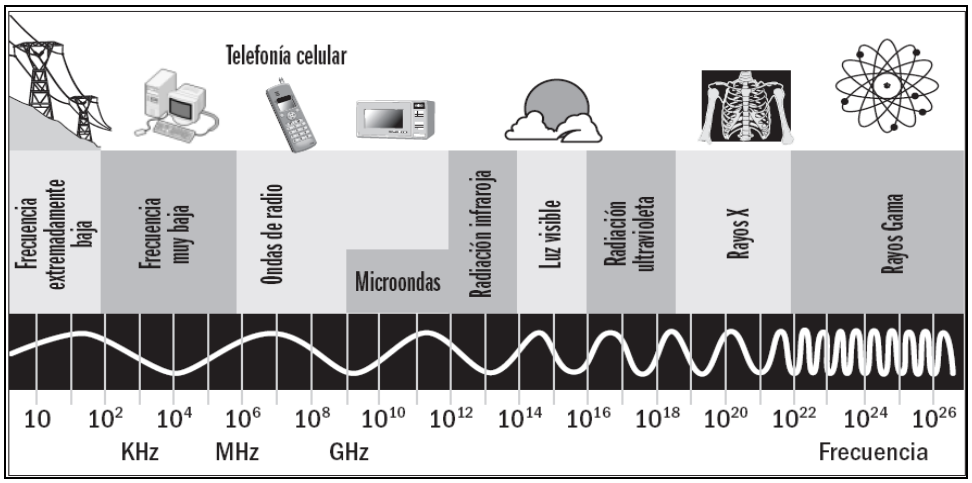


Figura. 3.26. Espectro Electromagnético

3.2.4.2 Interferencia y atenuación

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por la acción de materiales ambientales. La inspección en el lugar ayuda a identificar los elementos que afecten en forma negativa a la señal.

En la siguiente tabla, se enumeran los materiales nocivos que debemos considerar con el propósito de realizar una instalación.

Tabla. 3.3. Materiales que provocan interferencia en las señales inalámbricas

MATERIAL	EJEMPLO	INTERFERENCIA
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Árboles y plantas	Media
Agua	Lluvia / Niebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metales	Vigas, armarios	Muy Alta

Debido a que las redes inalámbricas operan en un espectro de frecuencias utilizado comúnmente por otras tecnologías, pueden encontrarse interferencias que influyan negativamente en el rendimiento de nuestra red.

Las ondas de radio no recorren las mismas distancias en todas las direcciones. Las paredes, las puertas, los huecos de ascensores, las personas y otros obstáculos suponen distintos grados de atenuación de la señal que provocan que el patrón de la radiación de radiofrecuencia (RF) sea irregular e imprevisible. La atenuación consiste simplemente en una reducción de la intensidad de la señal durante la transmisión. La atenuación se registra en decibelios (dB). Un decibelio es diez veces el logaritmo de la potencia de señal en una entrada determinada dividido por la potencia de señal en una salida de un medio especificado. Por ejemplo, una pared de una oficina (de grosor medio) que cambie la propagación de una señal de RF de un nivel de potencia de 200 milivatios (entrada) a 100 milivatios (salida) supone una atenuación de 3 dB. A continuación se proporcionan algunos ejemplos de valores de atenuación de una construcción típica de oficina:

Tabiques de pladur: 3 dB
Vidrieras con marco metálico: 6 dB
Tabique de hormigón ligero: 4 dB
Ventana de oficina: 3 dB
Puerta metálica: 6 dB
Puerta metálica en pared de ladrillo: 12,4 dB

Otros factores que reducen el alcance y afectan al área de cobertura son las paredes de hormigón de fibra vulcanizada, los revestimientos de aluminio, las tuberías y el cableado eléctrico, los hornos microondas y los teléfonos inalámbricos.

Las siguientes son algunas de las tecnologías que más frecuentemente encontraremos en el hogar o en la oficina, y que pueden causar inconvenientes:

- Bluetooth
- Hornos microondas
- Algunos teléfonos inalámbricos (los que operan en 2,4 GHz o más)

• Otras redes WLAN

3.2.4.3. Transmisión de datos en las ondas de radio

Aparte del hecho de utilizar una parte del espectro electromagnético que puede traspasar objetos sólidos, otro aspecto importante de las redes inalámbricas es saber la manera en que se transmiten datos a través de las ondas de radio y como son clasificadas por el receptor.

Para enviar datos a través de ondas de radio se utiliza un estándar de comunicación. Esto consiste en un conjunto de normas establecidas por instituciones reguladoras-certificadoras de telecomunicaciones a fin de que los dispositivos se comuniquen correctamente.

Las ondas de Radio son un tipo de ondas electromagnéticas, lo cual confiere tres ventajas importantes:

- No es necesario un medio físico para su propagación, las ondas electromagnéticas pueden propagarse incluso por el vacío.
- La velocidad es la misma que la de la luz, es decir 300.000 Km/seg.
- Objetos que a nuestra vista resultan opacos son transparentes a las ondas electromagnéticas.

No obstante las ondas electromagnéticas se atenúan con la distancia, de igual forma y en la misma proporción que las ondas sonoras. Pero esta desventaja es posible minimizarla empleando una potencia elevada en la generación de la onda, además que tenemos la ventaja de la elevada sensibilidad de los receptores.

Generación y propagación de las ondas

Las ondas de radio son generadas aplicando una corriente alterna de radiofrecuencia a un antena. La antena es un conductor eléctrico de características especiales que debido a la acción de la señal aplicada genera campos magnéticos y eléctricos variables a su alrededor, produciendo la señal de radio en forma de ondas electromagnéticas.

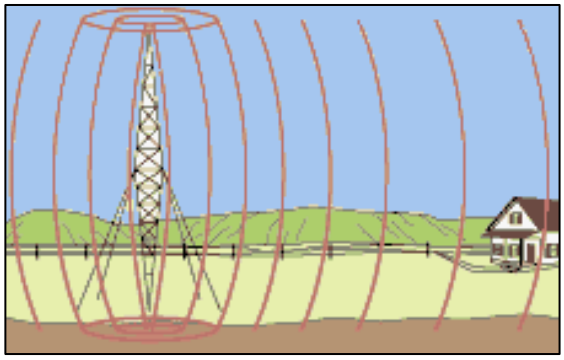


Figura. 3.27. Espectro Electromagnético

Estas ondas se transmiten desde un punto central (la antena emisora) de forma radial y en todas direcciones, pero podemos diferenciar tres formas de transmisión:

- Onda de tierra: en principio las ondas de radio se desplazan el línea recta, atravesando la mayoría de los objetos que estén en su camino con mayor o menor atenuación. Las pérdidas por dicha atenuación dependen de la frecuencia de la transmisión y de las características eléctricas de la tierra o el material atravesado. En términos generales a menor frecuencia mayor es el alcance de la onda y cuanta menor sea la densidad del material más fácil será atravesarlo.

Parte de esta onda es reflejada por la superficie terrestre.

- Onda visual o directa: es refractada en la baja atmósfera (refractación troposférica) debido a los cambios en la conductividad relativa en sus capas.
- Onda espacial: la atenuación en el aire es muy pequeña, lo que hace que la onda pueda alcanzar las capas altas de la atmósfera (ionosfera) y ser reflejada en su mayor parte de vuelta a tierra.

El mayor inconveniente que tendremos es que la transmisión de estos tres frentes no se hace a la misma velocidad, ya que las ondas reflejadas se retrasan con respecto a la onda directa, produciéndose un desfase que genera ruido (e incluso llegando a anular la onda si el desfase es de 180 grados). Para reducir este efecto hay que elevar la antena, ya que aumentando la altura se disminuye el ángulo de desfase.

Otro inconveniente es que en onda media la onda espacial no regresa a tierra durante el día pero sí durante la noche, debido a que la altura de la ionosfera se reduce. En cuanto a onda corta tenemos adicionalmente el inconveniente que a partir de una frecuencia crítica las ondas no son reflejadas a tierra y escapan al espacio.

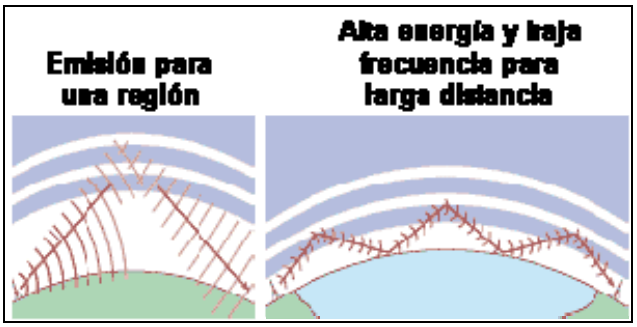


Figura. 3.28. Transmisión a larga distancia

Basándonos en el efecto de refracción en la ionosfera y en la capa terrestre es posible transmitir a largas distancias. Para ello debemos emplear ondas de gran energía y de baja frecuencia.

3.2.4.4 Solapamiento de señales

Más allá de los diferentes estándares de comunicación que tiene este tipo de tecnología, hay algo que todos tienen en común: la forma en que ordenan las señales de datos que se solapan. En lugares de una densidad de población alta, se puede llegar a encontrar un gran número de aparatos inalámbricos que están enviando señales al mismo tiempo utilizando un grupo similar de frecuencias.

Los dispositivos wireless usan dos tipos diferentes de estrategias para resolver este solapamiento de señales:

• **FH o FHSS** (*espectro extendido con salto de frecuencias*): en este estándar, las frecuencias cambian alrededor de 1.600 veces por segundo. Este tipo de estándar posee un gran número de patrones de salto para que las redes que utilicen este espectro y se encuentren en un lugar cercano unas a otras, no tengan posibilidad de usar la misma frecuencia en forma simultánea.

• **DS o DSSS** (*espectro extendido de frecuencia directa*): este espectro divide una franja del ancho de banda en canales separados y no transmite durante un largo tiempo en una misma frecuencia del canal. Debido a que utiliza canales distintos en una misma zona, hay redes que pueden llegar a solaparse sin que las señales de unas y otras se interfieran.

Estas dos formas de transmisión de espectro extendido resisten las interferencias, ya que no hay una sola frecuencia en uso constante.

El salto de frecuencia puede ser también resistente a la posibilidad de espionaje, ya que los patrones de salto pueden evitar casi todos los analizadores de espectro.

3.2.5 Criterios de selección de equipos y funcionamiento acorde a la aplicación.

Existen en la actualidad decenas de marcas de Access Point y cientos de modelos. La tarea de seleccionar el Punto de Acceso adecuado para las necesidades de cada organización no es nada sencilla.

Hay Access Points "Robustos" (Fat) y "Básicos" o "Delgados" (Thin). Los hay del estándar 802.11b/g, del estándar 802.11a y últimamente del estándar 802.11n. Hay algunos que incorporan muchas funciones para la seguridad WIFI.

Dentro de los parámetros más importantes al momento de elegir un AP, se encuentran los siguientes:

• *Estándar de transmisión de datos*, cual de los estándares 802.11x es el más adecuado para la red con la mejor relación precio/prestaciones. Asociado con el estándar está el problema de las velocidades de transmisión y el alcance de cada punto de acceso.

• *Seguridad WI-FI*, tomando en cuenta que soporten el estándar de seguridad 802.1x de la IEEE y que permitan la autenticación y autorización del usuario.

• *Tipo de producto*, hay una gran competencia entre los fabricantes y cada uno busca una estrategia para competir. Unos optan por los bajos precios y ofrecen productos delgados que prácticamente sólo son una antena y el driver elemental necesario para su

configuración. Otros fabricantes han optado por puntos de acceso muy robustos que incluyen muchísimas funciones y software muy potentes que permiten diversas configuraciones y que, por ejemplo, serán fáciles de actualizar cuando aparezcan novedades tecnológicas

- *Garantía del fabricante,* con el fin de analizar la funcionalidad de la red a través del tiempo y el crecimiento futuro.

- *Funcionalidad roaming*, para una buena cobertura de la red WLAN.

- *Certificación WI-FI del producto*, para contar con un respaldo del equipo a ser usado.

- *Convergencia de equipos en uno solo*, saber con que otras funciones cuentan y si cumplen tareas de otros elementos activos de red.

- *En general características técnicas*, como potencia de transmisión, sensibilidad y ganancia de las antenas.

3.2.6 Seguridad y Encriptación

Las redes inalámbricas se comunican mediante un medio compartido, es decir, todos los dispositivos asociados a la red son capaces de "ver" todos los datos que se transmiten por la red, les vayan destinados o no, e incluso pueden suplantar la personalidad de otro dispositivo.

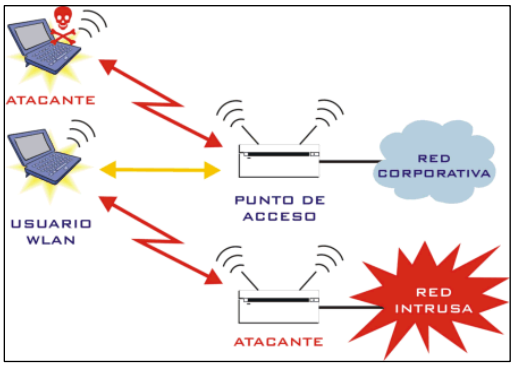


Figura. 3.29. Ataque a una red WLAN sin seguridades

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología Wi-Fi es la seguridad. Un muy elevado porcentaje de redes son instaladas por administradores de sistemas y redes por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan.

3.2.6.1 Mecanismos de Seguridad

• El estándar 802.11 define una serie de mecanismos básicos que tienen como objetivo proporcionar una seguridad equivalente a la de una red tradicional cableada. Para ello se busca dos objetivos básicos:

• **Autentificación**: el objetivo es evitar el uso de la red (tanto en la WLAN como la LAN a la que conecta el AP) por cualquier persona no autorizada. Para ello, el Punto de Acceso solo debe aceptar paquetes de estaciones previamente autentificadas.

• **Privacidad**: consiste en encriptar las transmisiones a través del canal radio para evitar la captura de la información. Tiene como objetivo proporcionar el mismo nivel de privacidad que en un medio cableado.

Con estos objetivos en mente se definen los mecanismos básicos de 802.11. Posteriormente se han observado deficiencias en estos mecanismos que los debilitan, y debido a ello se han desarrollado nuevos mecanismos, adicionales o en sustitución de los anteriores.

Cuando un dispositivo desea conectarse a una red WLAN, primero debe conocer el SSID (*Service Set ID*). Este actúa como un identificador de la red. En el estándar 802.11 se especifica que este identificador se retransmitir en difusión (*broadcast*) cada pocos segundos, anunciando de esta forma la red. Esto permite la conexión de clientes de manera sencilla, pero a su vez permite la identificación de redes sin dificultad.

Existen varias alternativas para garantizar la seguridad de estas redes:

Listas de control de acceso basadas en direcciones MAC:

Una de las medidas más comunes que se utilizan para poner seguridades en una red wireless es restringir las máquinas que podrán comunicarse con el Punto de Acceso haciendo filtrado por dirección MAC en éste. Para esto se suele crear una tabla en el punto de acceso que contiene todas las MACs de los clientes que están autorizados para conectar.

Aunque esto pueda parecer una medida de seguridad efectiva, no lo es, ya que es muy fácil cambiar la dirección MAC que aparece en los paquetes que un cliente envía, y hacernos pasar por uno de los equipos que sí que tienen acceso a la red.

No emitir Beacon Frames (o emitirlos sin el ESSID):

Una medida de seguridad bastante común es "ocultar" el ESSID[35] (el nombre de la red), es decir, hacer que el AP no mande beacon frames, o en su defecto no incluya el ESSID en éstos.

En este caso, para descubrir el ESSID solo habría que capturar datos de la red y esperar a que un cliente se conectara, y veríamos el ESSID en la trama Probe Request del cliente (en el caso de que no se manden Beacon Frames), o en la trama Probe Response del Punto de Acceso.

Utilizar 802.1x para la autenticación ante la red:

Especifica los mecanismos necesarios para llevar a cabo un control de acceso por puerto en redes 802. Este estándar, ha tenido una gran aceptación, y su implementación está disponible en varias formas por parte de los fabricantes.

802.1x define el control de acceso por puerto. Para ello, cuando un dispositivo quiere acceder a una red a través de un AP, este solicita unas credenciales al mismo. Esta solicitud se realiza usando EAP (*Extensible Authentication Protocol*). Una vez recibidas las credenciales por parte de la estación, el AP reenvía las mismas a un servidor de autentificación RADIUS, que realiza la autentificación del usuario y autoriza su acceso.

[35] *ESSID (Extended **S**ervice **S**et **ID**entifier)*

Debido a que EAP es un protocolo genérico, puede transportar diferentes tipos de autentificación, con diferentes prestaciones cada uno de ellos.

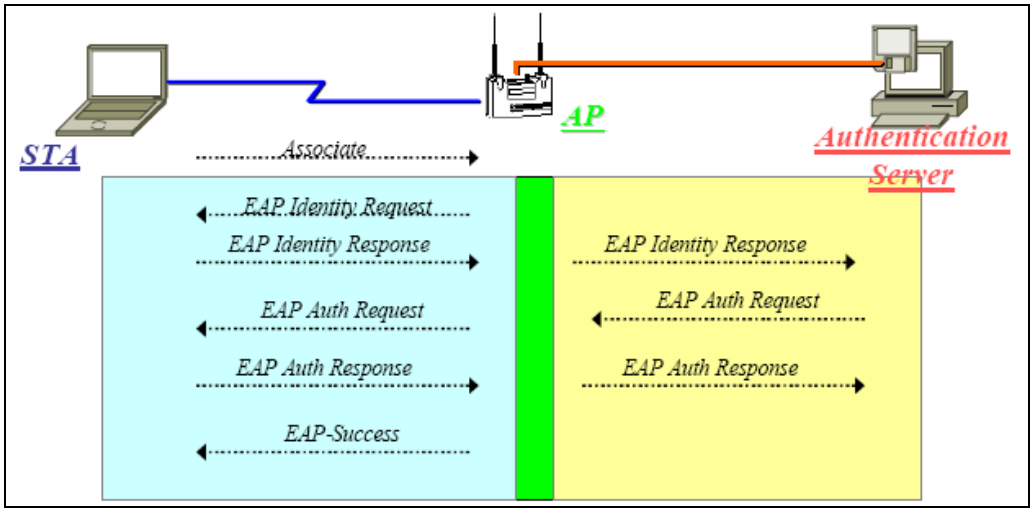


Figura. 3.30. Modelo 802.1X

Este sistema de autenticación obliga a instalar un programa en el ordenador que haga de cliente de 802.1x si el sistema operativo no lo soporta de forma nativa, y no soluciona el problema del cifrado de los datos, ya que sólo es una solución para la autenticación.

Contraseñas no estáticas:

Periódicas: -OTP (One Time Password): Contraseñas de un solo uso, conocidas como token flexibles.

Utilizar WEP para cifrar los datos:

Para proteger los datos que se envían a través de las WLANs, el estándar 802.11b define el uso del protocolo WEP (Wired Equivalent Privacy). WEP intenta proveer de la seguridad de una red con cables a una red Wireless, encriptando los datos que viajan sobre las ondas radioeléctricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace).

El protocolo WEP está basado en el algoritmo de encriptación RC4 (ARC4 o ARCFOUR), y utiliza claves de 64bits o de 128 bits, que en realidad son de 40 y 104 bits, ya que los otros 24 bits van en el paquete como Vector de Inicialización (IV).

En la figura se muestra el formato del paquete, que en el caso de que esté encriptado mediante WEP solo se realiza esta operación sobre los campos de datos e ICV.

Este último consiste en un CRC de 32 bits para comprobar la integridad de los datos. Es importante destacar que la implementación de WEP es opcional según el estándar, y por ello inicialmente no se implementó en muchos equipos.

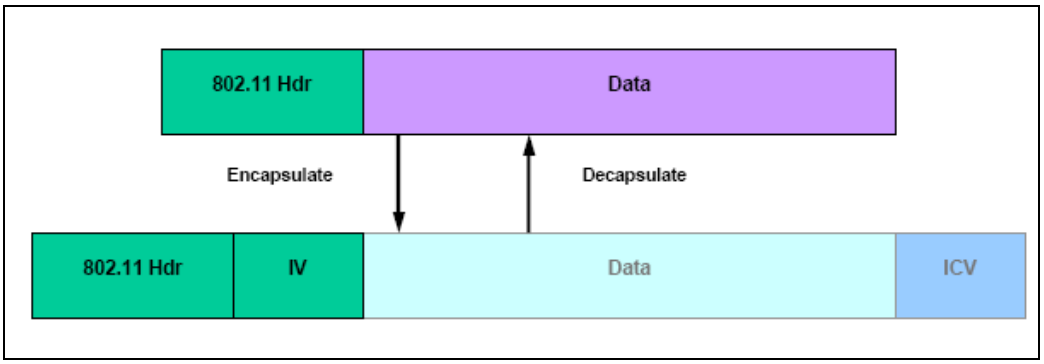


Figura. 3.31. Formato del paquete encriptado con WEP

Aunque esto pueda parecer suficientemente seguro, no lo es, ya que se ha encontrado numerosas vulnerabilidades en el mecanismo de encriptación que hacen desaconsejable su uso, ya que sólo hay que capturar el tráfico (que viaja por un medio compartido) y desencriptarlo con alguna de las herramientas ampliamente difundidas por Internet para tal fin.

La solución: REDES PRIVADAS VIRTUALES

Una VPN es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

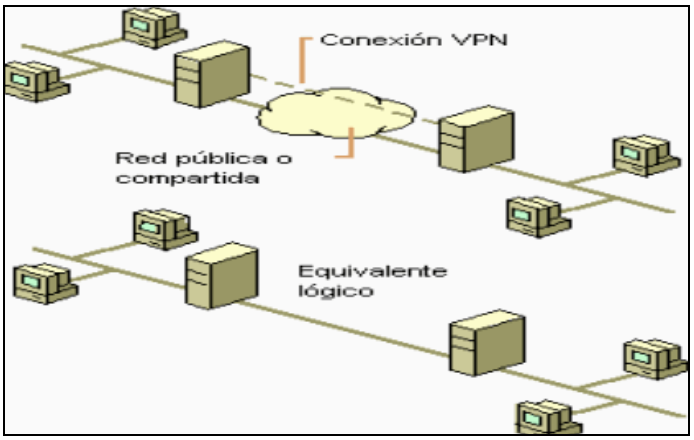


Figura. 3.32. Estructura de una VPN

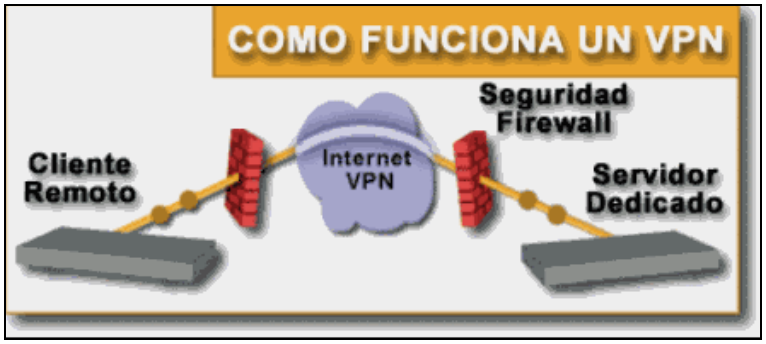


Figura. 3.33. Funcionamiento de una VPN

En la figura anterior se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de Internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado y lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar mis oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como Internet, IP, Ipsec, Frame Relay, ATM[36] como lo muestra la figura siguiente.

[36] *ATM (Asynchronous Tranfer Mode)*

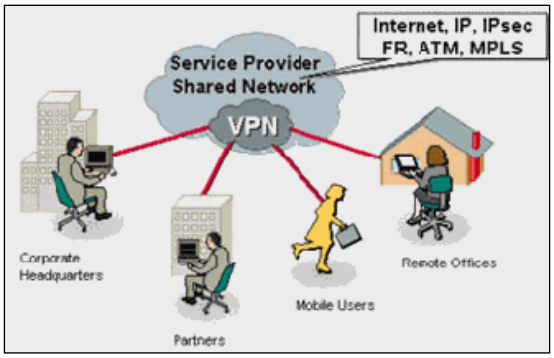


Figura. 3.34. Protocolos de las redes privadas virtuales

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se ha vuelto un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

3.2.6.2. Problemas concretos de seguridad en WI-FI

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 WiFi de la empresa, dentro del plan o política de seguridad.

Falsificación de AP (Punto de Acceso)**:** 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 conectando a una red en concreto.

Deficiencias en WEP: Ya existen varias herramientas automáticas para descifrarlo.

ICV[37] independiente de la llave: Se trata de un control de integridad débil, cuya explotación permite inyectar paquetes en la red.

Tamaño de IV demasiado corto: Como se mencionó, es el principal problema del protocolo WEP.

Deficiencias en el método de autenticación: Si no se configura adecuadamente una red WiFi posee débil método de autenticación, lo cual no permite el acceso, pero si hacerse presente en la misma.

Debilidades en el algoritmo key Scheduling de RC4: Este es el algoritmo de claves que emplea WEP, y con contraseñas débiles existen probabilidades de romperlo. Esto fue la sentencia definitiva para WEP.

Debilidad en WPA: Nuevamente existe un tema de seguridad con el empleo de claves débiles (esto lo soluciona la versión dos de WPA).

3.2.7 Configuración

Para acceder a las configuraciones del Access Point (AP), lo usual es conectarse a la interfaz Web que la mayoría posee. Existen 2 maneras de hacerlo: en forma inalámbrica; o con el cable de red tradicional.

Cabe destacar que dentro de las características y funciones que puede incluir un access point tenemos:

- Bridging
- NAT
- Servidor DHCP[38]
- Repetidor
- Sistemas de distribución wireless? (WDS)
- Privacidad
- Autentificación

[37] *ICV (Integrity Check Value)*
[38] *DHCP(Dynamic Host Configuration Protocol)*

- Enrutado IP más complejo

3.2.7.1 Definir y Configurar la Conexión al AP

Para conectarse en forma inalámbrica, basta con encender el AP, activar la conexión inalámbrica del computador y conectarse a la red WIFI que ofrezca el AP. Por lo general, la red WIFI se llamará "default", que es el nombre que traen configurado de fábrica.

En caso de usar un cable de red ethernet, se debe conectar el puerto Ethernet del AP con el del computador, usando un cable cruzado, o en su defecto empleando un switch o un hub y un par de cables directos.

Un AP siempre trae un número IP configurado de fábrica (p.ej. 192.168.1.1). Por lo tanto, se debe configurar la interfaz de red del PC (la que se esté usando, inalámbrica o Ethernet) con cualquier IP del mismo segmento, para luego conectarse a él.

Conexión a la Página de Configuración del AP

Una vez definida la configuración IP del PC, se accede al dispositivo vía http, por medio de un navegador (Explorer, Mozilla, Netscape, etc.) con el fin de conectarse a la página de configuración del AP. Esto produce el despliegue de una ventana donde se solicita un nombre de usuario y contraseña.

Configuración avanzada

Algunos tipos de Access Point (AP) incluyen funcionalidades de *router* de banda ancha (ADSL[39] o Cable). Por un lado permite conectar y compartir una conexión de banda ancha y por otro interconectar localmente a los PC's con tarjetas de red inalámbrica.

Por otra parte, donde existe banda ancha, es posible encontrar 2 escenarios: conexión de banda ancha monousuario; y conexión de banda ancha multiusuario. Dependiendo de esto, el AP podrá utilizarse adicionalmente como *router* para compartir la banda ancha.

[39] *ADSL* ***(Asymmetric Digital Subscriber Line)***

Configuración del AP para Conexiones de Banda Ancha Monousuario

Bajo este esquema, la conexión con el AP debe hacerse según el diagrama que se muestra:

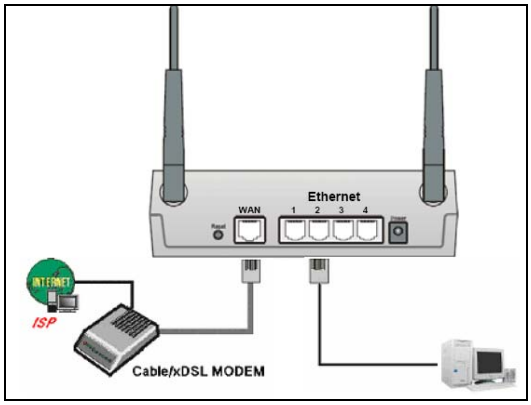


Figura. 3.35. Conexionado del AP con conexión BA monousuario.

Como se aprecia, el cable tipo ethernet de la conexión de banda ancha debe llegar al puerto WAN del AP. Para estos casos, se deberán averiguar las configuraciones IP que utiliza el proveedor del servicio para la configuración de los parámetros adecuados en el AP.

Por otra parte, para que el AP comparta la conexión Internet, se debe definir una configuración específica para la red local (LAN). Para esto, se debe escoger la numeración IP de la red privada (p.ej 192.168.1.x) y asignar una dirección IP fija al AP.

Una vez asignada la dirección IP de la red local (LAN), se requiere asignar direcciones IP del mismo segmento (p.ej 192.168.1.2, 192.168.1.3, …) a los computadores cliente. Esto se puede realizar en forma manual (configurando uno por uno cada computador) o utilizando el servidor DHCP que incorpora el AP.

Configuración del AP Para Conexiones de Banda Ancha Multiusuario

Bajo este esquema, la conexión con el AP debe hacerse según el siguiente diagrama:

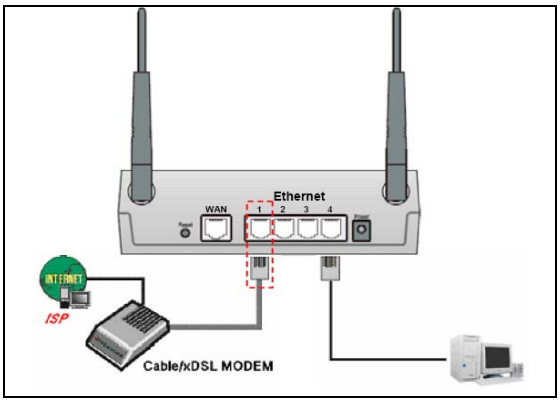


Figura. 3.36. Conexionado del AP con conexión BA Multiusuario.

Para este caso, el AP actúa sólo como un hub inalámbrico, por lo que no es necesario modificar la configuración de red que trae por defecto.

Sólo en los casos en que el equipo del proveedor no ofrece servicio DHCP a los computadores cliente, se podría utilizar el servidor DHCP que trae el AP. Para estos casos, es necesario averiguar la numeración IP que utiliza el proveedor y los rangos de IP que ha asignado a esa red en particular. Posteriormente, se debe asignar uno de los IP a la interfaz LAN del AP y los restantes utilizarlos para configurar el servicio DHCP.

3.3.- ANTENAS

3.3.1 Definición e Importancia

Las antenas son dispositivos utilizados para recoger o radiar ondas electromagnéticas. Convierte la onda guiada por la línea de transmisión (el cable o guía de onda) en ondas electromagnéticas que se pueden transmitir por el espacio libre.

Está constituida por un conjunto de conductores diseñados para radiar (transmitir) un campo electromagnético cuando se le aplica una fuerza electromotriz alterna.

De manera inversa, en recepción, si una antena se coloca en un campo electromagnético, genera como respuesta a éste una fuerza electromotriz alterna.

Las antenas deben de dotar a la onda radiada con un aspecto de dirección. Es decir, deben acentuar un solo aspecto de dirección y anular o mermar los demás. Esto es necesario ya que solo nos interesa radiar hacia una dirección determinada.

Las antenas también deben dotar a la onda radiada de una polarización. La polarización de una onda es la figura geométrica descrita, al transcurrir el tiempo, por el extremo del vector del campo eléctrico en un punto fijo del espacio en el plano perpendicular a la dirección de propagación.

Para todas las ondas, esa figura es normalmente una elipse, pero hay dos casos particulares de interés y son cuando la figura trazada es un segmento, denominándose linealmente polarizada, y cuando la figura trazada es un círculo, denominándose circularmente polarizada.

El tamaño de las antenas está relacionado con la longitud de onda de la señal de radiofrecuencia transmitida o recibida, debiendo ser, en general, un múltiplo o submúltiplo exacto de esta longitud de onda. Por eso, a medida que se van utilizando frecuencias mayores, las antenas disminuyen su tamaño.

Asimismo, dependiendo de su forma y orientación, pueden captar diferentes frecuencias, así como niveles de intensidad.

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.

Se han realizado pruebas de campo y se han establecido comunicación entre dispositivos Wireless a más de 70 Km. (con antenas parabólicas de alta ganancia).

3.3.1.1 Parámetros de una antena

Las antenas se caracterizan eléctricamente por una serie de parámetros, estando los más habituales descritos a continuación.

- **Ancho de banda**

Es el margen de frecuencia de funcionamiento de la antena. Normalmente se da a 3dB, es decir, el intervalo entre las frecuencias que las que el nivel de energía radiado cae a la mitad. Varía mucho entre los tipos de antenas, siendo uno de los parámetros que más condicionan su elección.

El ancho de banda de la antena se define como el rango de frecuencias sobre las cuales la operación de la antena es satisfactoria. Esto, por lo general, se toma entre los puntos de media potencia, pero a veces se refiere a las variaciones en la impedancia de entrada de la antena.

- **Directividad**

Es la relación entre la potencia radiada en la dirección de máxima radiación y la radiaciación total de la antena promediada a lo largo del área de la esfera. Este parámetro sólo depende del diagrama de radiación y no de la eficiencia ni potencia radiada.

- **Ganancia**

Es la directividad menos las pérdidas en la antena. Refleja el comportamiento real de la antena al tener en cuenta su geometría a través de la directividad y los materiales que la componen, tanto conductores como dieléctricos, incluidos en las pérdidas.

La ganancia de las antenas se da normalmente en decibelios sobre la antena isotrópica [dBi]. Es decir, la ganancia en potencia comparada con un antena isotrópica (antena ideal que emite por igual en todas direcciones).

Científicamente se toma como referencia la antena *isotrópica*, que es una antena ideal que radia uniformemente en todas direcciones. Evidentemente no existe tal antena pero, matemáticamente, es muy fácil calcular el campo electromagnético que produciría una antena de ese tipo.

La ganancia de algunas antenas viene expresada en [dBd], que expresa su ganancia comparada con la de una antena dipolo, el dipolo consiste en dos elementos conductores rectilíneos colineares de igual longitud, alimentados en el centro, y de radio mucho menor

que el largo.. En este caso debemos añadir 2.14 para obtener la ganancia correspondmente en [dBi].

En la práctica la antena que se usa como referencia suele ser el dipolo, que ya tiene una ganancia de 2,8 dB sobre la antena isotrópica. Esto se debe a que el dipolo es una antena muy simple y fácil de construir, por lo cual se pueden hacer comparaciones directas entre dos antenas sin tener que recurrir a la antena isotrópica que no existe y por tanto no es comparable directamente.

Cuanta más ganancia tiene una antena mas directiva será (la energía se dirige en una dirección específica), y al mismo tiempo menos señales cercanas (ruido) se recibirán, con lo que se mejora la relación señal ruido.

- **Impedancia de entrada**

Es el parámetro circuital de la antena. Excitada con una cierta tensión, absorbe una corriente dada por $I = \frac{V}{Z}$. La impedancia suele ser compleja, anulándose la parte imaginaria en la resonancia (para el caso de antenas resonantes).

- **Anchura de haz**

Es un parámetro de radiación, ligado a la ganancia. Se suele indicar a 3dB y es el intervalo angular dentro del cual la potencia relativa radiada por la antena es superior a la mitad de la ganancia.

- **Polarización**

Se refiere a la polarización de la onda radiada por la antena en la dirección de máxima ganancia. Se llama diagrama copolar al diagrama de radiación con la polarización deseada y diagrama contrapolar (*Crosspolar*, en inglés) al diagrama de radiación con la polarización contraria.

Las antenas pueden funcionar con polarización lineal o polarización circular, según el tipo y aplicación. A partir de las dos polarizaciones lineales se puede generar la circular y viceversa. Y dentro de la polarización lineal se encuentra la vertical y la horizontal.

3.3.1.2 Frecuencias utilizadas

Según los estándares 802.11 las frecuencias que podemos utilizar para comunicaciones Wireless son aquellas destinadas a libre uso a 2'4GHz y 5GHz.

La banda de 5GHz está destinada a usos militares. La segunda restricción importante es que el límite de potencia está en 100mW sin amplificación, a la espera también de que se amplíe a 1W.

- **Frecuencia de 2.4Ghz**

La primera frecuencia que se homologó para poder ser utilizada para comunicaciones digitales inalámbricas es la de 2'4GHz. Se escogió esta frecuencia porque es una banda destinada a uso libre de radioaficionados, con las limitaciones que hemos comentado anteriormente, y que dependiendo de los países dispone de más o menos canales, ya que no todos los países siguen al pie de la letra las recomendaciones de la ITU.

La banda de 2'4GHz está dentro de la zona de lo que se llaman microondas. Esta banda tiene la peculiaridad que a estas frecuencias existe muy poco ruido. Además al tratarse de frecuencias próximas a las de la luz visible tienen un comportamiento bastante similar a ésta, con la pequeña ventaja de que al ser longitudes de onda más largas objetos pequeños como vegetación o tabiques son bastante transparentes a la señal, esto permite que no siempre se deba tener visión directa entre emisor y receptor. Con otros elementos también existen reflexiones especulares, esto hace que queden "iluminadas" zonas que a simple vista no tendrían porque tener señal.

Los principales enemigos de las ondas electromagnéticas en las que viajan las señales son los metales. Los metales son totalmente opacos, esto hace que un edificio de hormigón armado nos pueda bloquear la señal si se encuentra entre el emisor y el receptor. Algo parecido pasa con los automóviles por esto llevan la antena de la radio y del móvil fuera, aunque si los cristales no llevan plomo permitan tener algo de cobertura en el habitáculo.

Otra pared importante para la señal es la torre del ordenador, ya que es una gran pantalla electromagnética para evitar que señales externas afecten al funcionamiento del

ordenador, de este modo siempre será mucho más efectiva una antena que se pueda colocar encima de la torre que no una que esté justo detrás (como la mayoría de tarjetas PCI Wireless).

- **Nueva banda a 5GHz**

A medida que las tecnologías Wireless fueron avanzando se vio la necesidad de tener más ancho de banda. Así fue como se homologó la banda de 5GHz. La elección de esta frecuencia no es gratuita, ya que es aproximadamente el doble de la de 2'4GHz.

Por su forma una antena está destinada a una frecuencia en concreto: su longitud es proporcional a la longitud de onda de la frecuencia que se desea transmitir o recibir. De este modo la antena ya será el primer filtro que facilitará la entrada de señales de las frecuencias requeridas y atenuará otras frecuencias no deseadas. Los mínimos de atenuación se encuentran en múltiples de la frecuencia principal. Así la antena de 2'4GHz será muy buena a esta frecuencia y bastante buena a 5GHz que es el doble de la frecuencia principal.

Como ejemplo de ello se puede citar los teléfonos móviles duales. Estos teléfonos permitían utilizar la frecuencia hasta entonces utilizada para GSM de 950MHz y además la nueva frecuencia de GSM-1800: 1800MHz, casi el doble, como en el caso del Wireless.

Esta estrategia permite crear una nueva tecnología totalmente compatible con una tecnología anterior, aprovechando así el ancho de banda de ambas tecnologías. En su época una estación base de GSM permitía 600 llamadas simultáneas, y GSM-1800 permitía 3000, de este modo las nuevas instalaciones se hacían con GSM-1800 pero dejaban totalmente funcionales las instalaciones antiguas de GSM.

- **Ocupación de frecuencias**

Cuando se utiliza un canal para conectar dos ordenadores (o un ordenador y un Access Point) este canal queda inutilizable para ninguna otra conexión. El número de canales que tenemos en la banda de Wireless es limitado, así nadie podrá utilizar el canal que se está usando en cualquier parte donde llegue la señal.

Para dimensionar las antenas a ser instaladas, se debe considerar la ganancia en función de la distancia existente entre ambos equipos, ya que al emplear una antena de alta ganancia para una distancia corta, no se permite a nadie reutilizar la frecuencia del canal en el radio de cobertura de la antena. Si en la zona nadie más utiliza Wireless no pasará nada, pero cada día son más las personas que utilizan esta tecnología, sobretodo en las grandes ciudades.

Hay otro aspecto importante a la hora de comprar la mayor antena del mercado: la seguridad. En las comunicaciones telemáticas la seguridad nunca es absoluta, así que un modo bastante eficaz de evitar que otros puedan acceder a las comunicaciones de una red privada, es hacer que la señal se difunda de la forma más restringida posible. Así, puede ser útil usar antenas de la potencia justa para llegar al destino, o si se interconecta dos edificios y la señal tiene que salir al espacio público quizá la mejor opción será usar antenas direccionales apuntadas entre ellas. Esta será una buena solución para la interconexión de Access Points de distintas redes: backbone

3.3.1.3 Banda ISM de 2.4 Ghz

Las redes sin cables que utilizan el estándar 802.11b operan en la banda ISM. Hay otros equipos que también utilizan esta banda, entre los que se incluyen los hornos microondas, algunos equipos médicos y los teléfonos sin cables. El estándar IEEE 802.11b define como deben configurarse las redes WLAN, y como pueden minimizarse las interferencias provenientes de otros servicios que operen en la misma frecuencia.

Tabla. 3.4. Radiación acorde a la ubicación de la antena

Nº canal	US/Canada	Europa	Francia	España	Japón
1	2412	2412	-	-	2412
2	2417	2417	-	-	2417
3	2422	2422	-	-	2422
4	2427	2427	-	-	2427
5	2432	2432	-	-	2432
6	2437	2437	-	-	2437
7	2442	2442	-	-	2442
8	2447	2447	-	-	2447
9	2452	2452	-	-	2452
10	2457	2457	2457	2457	2457
11	2462	2462	2462	2462	2462
12	-	2467	2467	-	2467
13	-	2472	2472	-	2472
14	-	-	-	-	2484

Un receptor de WLAN puede utilizar cualquiera de estos canales y puede saltar automáticamente de canal en canal si encuentra interferencias. Una antena para 802.11b para los EEUU y Canadá deberá radiar bien entre los 2410 y los 2460MHz.

3.3.2 Tipos

Existe una amplia gama de antenas para diversas aplicaciones outdoor o de campo, el establecimiento de una red inalámbrica requiere diversos tipos de antenas y accesorios de acuerdo a las distancias y aplicaciones, las antenas y accesorios son robustas, de alto rendimiento, bajo costo y fáciles de instalar que junto a los bridges, routers y estaciones base proporcionan a los clientes una solución inalámbrica completa para cualquier instalación.

Existen tres tipos de antenas para redes inalámbricas:

- **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 foco 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. 3.37. Antena direccional

Son directivas y solo emiten/reciben con un ancho de haz definido por la construcción de la antena.

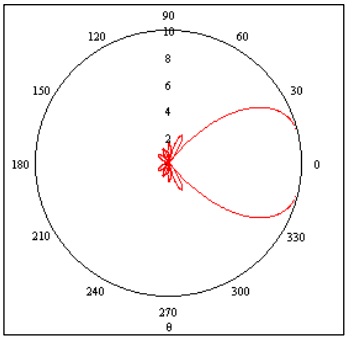


Figura. 3.38. Patrón de radiación

- **Antena 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 sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance.

Figura. 3.39. Antena omnidireccional

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. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional

Dan cobertura con un diagrama de radiación circular (360º). Se supone que dan servicio por igual independientemente de su colocación, pero debido a que las frecuencias en las que estamos trabajando son próximas a microondas, los diagramas no son circulares, son óvalos, como se muestra en la figura.

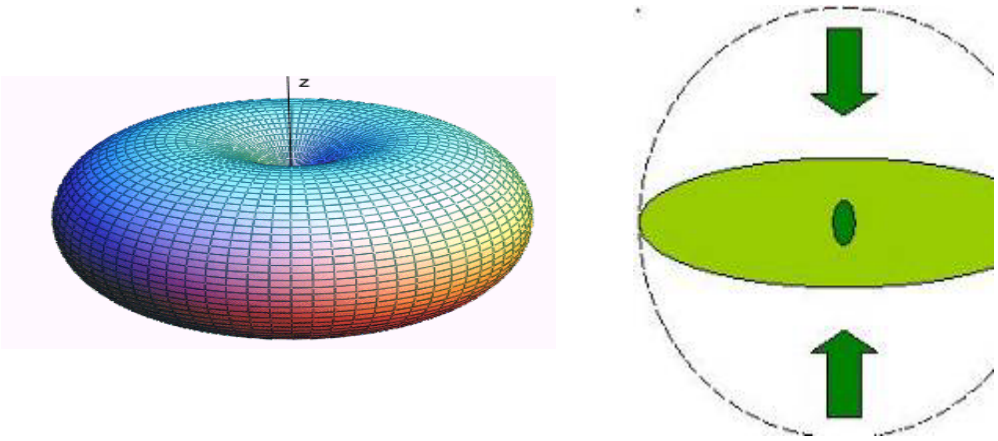


Figura. 3.40. Diagrama de radiación de una antena omnidireccional

- **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.

Figura. 3.41. Antena sectorial

Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120º ó 4 antenas sectoriales de 80º. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

3.3.2.1 Apertura vertical y apertura horizontal

La apertura es cuanto se abre el haz de la antena. El haz emitido o recibido por una antena tiene una abertura determinada verticalmente y otra apertura determinada horizontalmente.

En lo que respecta a la apertura horizontal, una antena omnidireccional trabajará horizontalmente en todas direcciones, es decir, su apertura será de 360º. Una antena direccional oscilará entre los 4º y los 40º y una antena sectorial oscilará entre los 90º y los 180º.

La apertura vertical debe ser tenida en cuenta si existe mucho desnivel entre los puntos a unir inalámbricamente. Si el desnivel es importante, la antena deberá tener mucha apertura vertical. Por lo general las antenas, a más ganancia (potencia por decirlo de algún

modo) menos apertura vertical. En las antenas direccionales, por lo general, suelen tener las mismas aperturas verticales y horizontales

3.3.2.2 Selección de la antena más adecuada

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

Si se necesita dar cobertura de red inalámbrica en toda un área próxima (una planta de un edificio o un parque por ejemplo) lo más recomendable es usar una antena omnidireccional. Si se tiene que dar cobertura de red inalámbrica en un punto muy concreto (por ejemplo un PC que está bastante lejos) se utilizará una antena direccional, finalmente, si se necesita dar cobertura amplia y a la vez a larga distancia, se utilizará antenas sectoriales.

Otro punto importante a saber es la distancia nominal que se obtiene según los dBi que tenga la antena:

Tabla. 3.5. Distancia nominal de radiación en dBi's

dBi	Distancia nominal (en Metros)
2.5	300
5.0	600
7.5	1200
10	2400

Como se puede observar, en la tabla 3.5, por cada 2.5 dBi que tenga la antena se duplica la distancia.

3.3.3 Formas de irradiación de ondas

Cada antena tiene su propia forma de irradiar una señal. Hay antenas que irradian más en una dirección que en otra, hay otras que tienden a irradiar casi por igual en todas las direcciones, y hay antenas que irradian solo en ciertas direcciones.

La forma característica que tiene una antena de emitir la señal es lo que se conoce como su patrón de irradiación. Un radiador isotrópico emite su señal en forma de una esfera perfecta, las antenas Yagui poseen un patrón elíptico, más alongado hacia el frente.

En un patrón de irradiación hay direcciones en las se emite mucha energía y, direcciones en las que no se emite energía del todo. Estos vienen a formar las llamadas direcciones sordas de las antenas, en donde prácticamente no se reciben señales.

Los patrones de irradiación de una antena por lo general son brindadas por el fabricante en las especificaciones, en forma de gráfico como el siguiente:

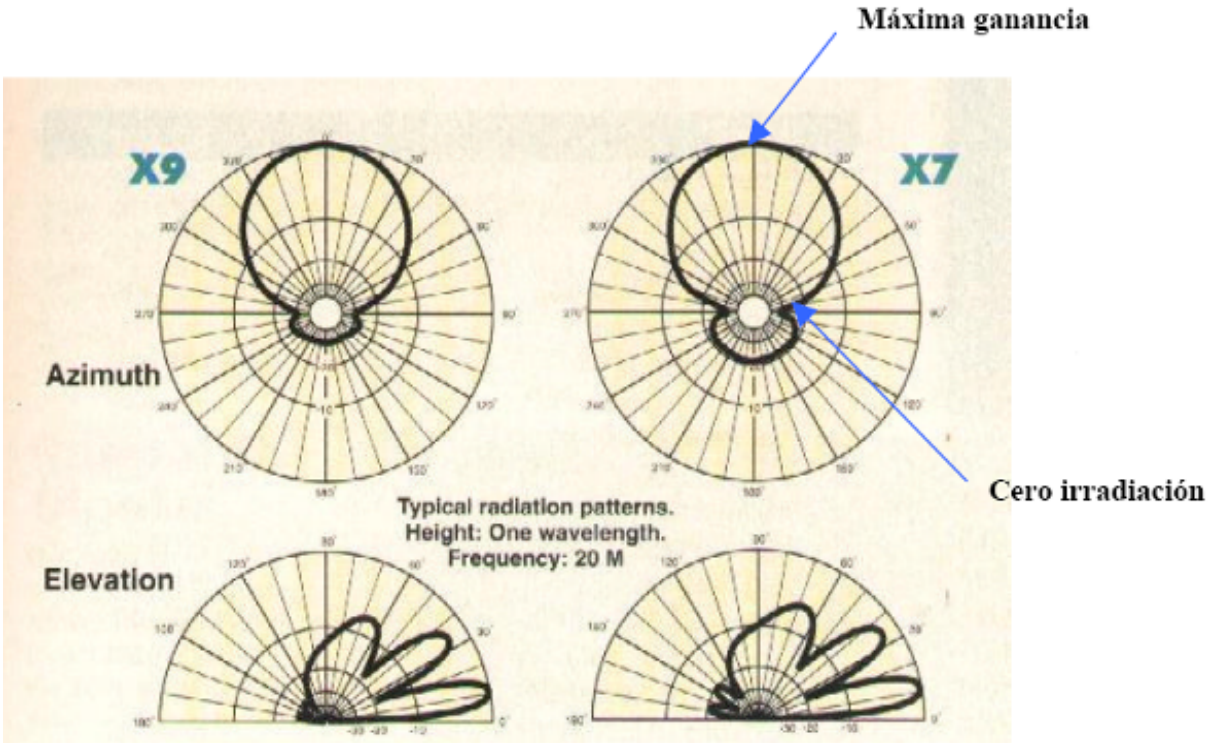


Figura. 3.42. Patrones de irradiación

El gráfico nos muestra en la parte superior el llamado patrón azimutal, que sería la forma de irradiar de la antena vista desde arriba. El gráfico inferior nos muestra el patrón de irradiación vertical o en elevación, el cual muestra la forma de irradiar vista desde lado. Los puntos donde la curva (la elipse) se aleja más del centro del gráfico son las direcciones que tienen mayor ganancia, mientras que los puntos donde la curva toca el centro son direcciones de cero radiación.

Estos dos patrones son muy importantes a la hora de seleccionar una antena, el primero nos muestra que tan direccional es la antena, y el segundo nos muestra que tan bajo es su ángulo de irradiación.

En términos generales, el patrón de irradiación de una antena es también su patrón de recepción. Cuando una antena emite, actúa como un lente, concentrando la señal en ciertas direcciones. Cuando una antena recibe, actúa como un embudo, concentrando la señal de solo ciertas direcciones.

Los patrones de irradiación de las antenas son de muchos tipos, desde el simple patrón esférico del radiador isotrópico hasta patrones con lóbulos múltiples como el que se muestra en la figura. El patrón no solo depende de la antena, sino también de la altura sobre el suelo de la misma y de la presencia de otros objetos conductores cercanos.

Figura. 3.43. Patrón de radiación lobular

Diagramas de radiación

El diagrama de radiación de una antena se define como la representación grafica de las características de radiación en función de la dirección angular. Se utilizara habitualmente un sistema de coordenadas esférico.

Las tres variables de un sistema esférico son (r, q , f)

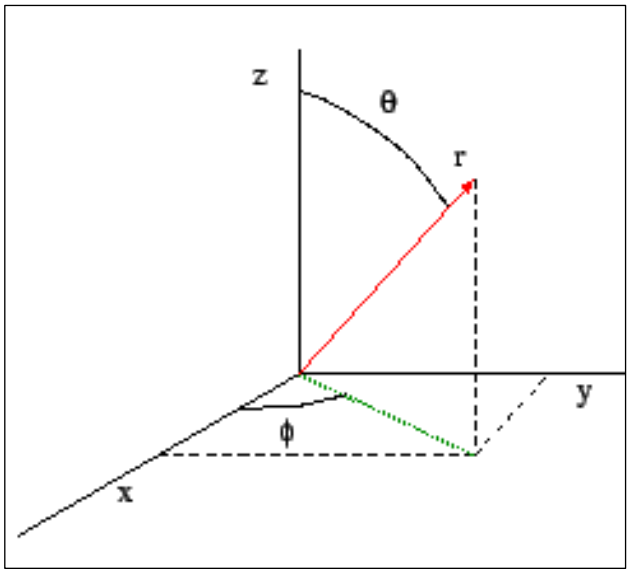


Figura. 3.44. Sistema esférico

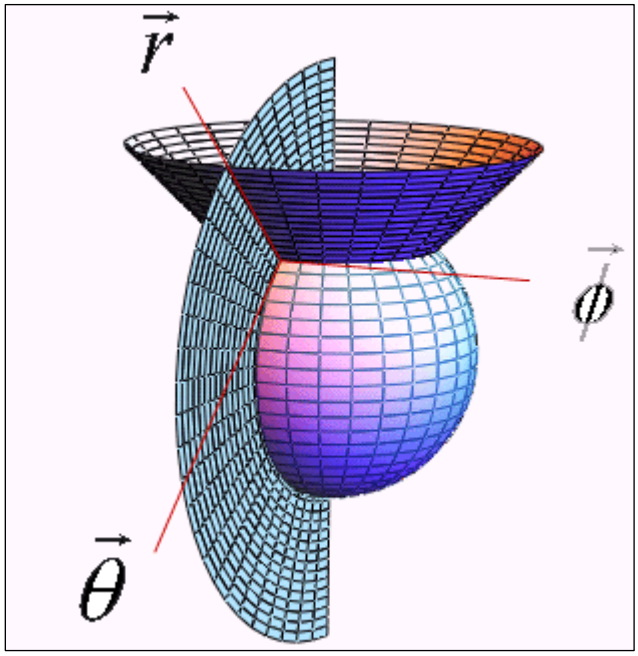


Figura. 3.45. Sistema coordenado esférico

Los patrones de radiación se ven afectados por la altura sobre el suelo, la conductividad de la tierra y los objetos alrededor. La medida de los patrones por lo tanto es difícil y por lo general se hace en laboratorios y con antenas modelo, que interpoladas a las frecuencias deseadas, definen todos los parámetros requeridos.

3.3.4 Principales aplicaciones

La aplicación fundamental de las antenas es la transmisión, recepción de información empleando para ello radiación electromagnética.

Para codificar la información se emplea una señal base denominada portadora. Esta es una señal de gran potencia y frecuencia capaz de ser emitida por la antena. Sobre la portadora se aplica otra señal, la modulante, que se encarga de transmitir la información propiamente dicha a la portadora.

3.3.4.1 Telegrafía, radiodifusión y televisión

Es su uso inicial, las antenas se emplearon para transmisiones de telegrafía sin hilos. La evolución tecnológica pronto derivó en la aparición de la radio, y posteriormente la televisión. Las transmisiones telegráficas, de radio iniciales emplearon frecuencias relativamente reducidas, a las que se asocian longitudes de onda largas. Esto hace de estas emisiones relativamente inmunes a obstáculos, y con la capacidad de recorrer grandes distancias. De hecho, es posible aprovechar la reflexión de la señal en la ionosfera para aumentar el alcance. La televisión por su parte, requiere de frecuencias muy altas, ya que debe transmitir una mayor cantidad de información. Estas frecuencias muy altas son más sensibles a obstáculos, y más direccionales, lo que obliga a emplear repetidores y amplificadores a distancias relativamente reducidas. Hay que tener en cuenta que el alcance del VHF está limitado a la línea visual.

3.3.4.2 Comunicaciones punto a punto

La principal aplicación de las antenas es sin duda la transmisión de información, sea del tipo de sea, comunicaciones por teléfono, transferencia de datos entre redes de ordenadores, canales de televisión, etc. El parámetro crítico en este campo es el ancho de banda, la capacidad de transmitir una gran cantidad de información en poco tiempo. Para

conseguir esto es necesario emplear frecuencias muy elevadas. Por tanto, actualmente las microondas son el tipo de radiación empleado.

3.3.4.3 Aplicaciones INDOOR:

En estas aplicaciones (antena integrada a la Tarjeta de Red Inalámbrica) la distancia entre la tarjeta de red inalámbrica y el AP puede llegar a los 300 mts cuando no existen paredes / obstáculos en la trayectoria entre la tarjeta de red wireless y el AP.

Cuando existen obstáculos en la trayectoria, estas distancias se achican acorde a cuan grande sea el obstáculo en cuestión. Valores típicos pueden ubicarse dentro los 100 mts.

3.3.4.4 Aplicaciones OUTDOOR:

En estas aplicaciones se recomienda que la trayectoria entre la tarjeta de red inalámbrica y el AP este totalmente libre de obstáculos. A este requisito se lo denomina "Línea de Vista".

En estas aplicaciones los rangos de cobertura pueden llegar a varios kilómetros (por ejemplo: 5Km) según la configuración total de la red.

Dentro de las variables que determinan la cobertura de un Sistema Outdoor se puede mencionar:

- Longitud y tipo de Cable instalado entre la tarjeta de red y su antena Externa. Longitudes de 5 mts y cable 9913 es lo común en estas instalaciones.

- Ganancia de la antena de la tarjeta de red. Usualmente se trabaja con antenas cuya ganancia oscila entre 7 dBi a 24 dBi de acuerdo a la distancia entre la tarjeta y el Nodo donde se instala el AP (Access Point).

- Ganancia de la antena del Nodo donde se ubica el AP (Access Point). Dicha ganancia oscila entre los 6 dBi a los 13 dBi. La antena puede ser Omnidireccional o sectorizada.

- Uso de Amplificadores Bidireccionales junto a la Antena del Nodo. Este dispositivo activo incrementa la cobertura de un sistema.

- Longitud y tipo de cable instalado entre la Antena del Nodo y el AP (Access Point)

3.3.4.5 Otros

Además de las aplicaciones en las que la antena emite información modificada, hay otras en las que su papel es más pasivo, limitándose a emitir pulsos de características determinadas, y recibirlos para su posterior análisis. Este análisis abre las puertas a multitud de aplicaciones como;

- Radar
- Meteorología
- Radioayudas a la navegación
- Reconstrucción de superficies, elaboración de mapas
- Radioastronomía

3.3.5 Instalación

Las antenas externas se conectan a los equipos wireless mediante un cable. Salvo que sea muy corto, lo normal es que el cable que une el dispositivo wireless con la antena sea un cable de tipo coaxial, similares a los de antena de televisión pero con una impedancia diferente. Corresponde a 50 ohmios en comparación a los 75 ohmios que suelen ser los típicos de televisión. Los cables coaxiales se caracterizan porque disponen de un conector central (normalmente denominado activo) rodeado de una malla metálica concéntrica que le protege de las interferencias, que son muchas, en el campo radioeléctrico en que operan habitualmente, las tarjetas y los punto de acceso inalámbricos.

Para conectar el cable a la antena y a los dispositivos inalámbricos, se utilizan los conectores. Tanto la antena como algunos equipos wireless disponen de un conector donde se deben colocar sus correspondientes conectores de los extremos de cable.

Para poder llevar a cabo esta operación, existen unos conectores conocidos como de tipo macho y otros como de tipo hembra que se conectan entre sí.

Figura. 3.46. Conector N macho

Tanto el cable, como cada conector, añaden perdidas a las señales de radio wireless. Para evitar estas perdidas, aparte de utilizar cables y conectores de calidad hay que procurar utilizar un cable lo mas corto posible y el número de conectores imprescindible. El número de conectores dependerá de las tarjetas y antenas que se disponga, la calidad dependerá del valor a invertir y la longitud vendrá determinada por el tipo de cable que se quiera usar, por el alto costo que pueda tener, por la distancia a la antena, en definitiva por su pérdida.

Si se tiene una buena antena pero por estar demasiado lejos a la tarjeta WIFI, posiblemente se llegue a perder la ganancia obtenida en la antena. Por lo tanto, es importante valorar todos estos aspectos.

Además, se debe intentar evitar en la medida que sea posible utilizar conectores para extender la longitud de cableo, para adaptar diferentes tipos de cables o conectores. Reducir siempre a la máxima expresión y no hacer nunca empalmes entre cables.

PIGTAIL

El Pigtail, no es más que un pequeño cable, que sirve de adaptación entre la tarjeta WIFI (o el AP) y la antena o el cable que vaya hacia la antena. Este Pigtail tiene 2 conectores: el propietario de cada tarjeta en un extremo, y por el otro un conector N estándar en la mayoría de los casos.

Figura. 3.47. Conector N

Es utilizado para cambiar el tipo de conector que posee el equipamento. Equivale a un "Triple" eléctrico, que convierte de enchufes de 3 a 2 patas.

Generalmente los conectores más habituales son los RSMA, RTNC.

Figura. 3.48. N-Macho y RP-SMA

3.4.- Localización y chequeo de averías

La habilidad para encontrar las fallas y repararlas no es solamente una tradición; es fundamental para la existencia del servicio.

El instrumento más utilizado para comprobar si una antena funciona o no es el medidor de ROE. Aunque no es el elemento más idóneo, ya que puede inducir a error, es el más económico y el más común de los que se emplean.

El medidor de ROE consiste en una línea coaxial a la que se aproximan dos conductores que captan una pequeña parte de la potencia que circula por el cable. Mediante

unos diodos convenientemente conectados, se detecta la potencia que circula hacia la antena y la que retorna de ella. Si se ajusta la lectura de potencia hacia la antena en un punto determinado (que lo da uno de los diodos), el otro indicador dará la ROE directamente, ya que la escala está graduada en ROE.

En cuanto al chequeo de averías, se recomienda brindar a estos equipos un constante mantenimiento. Existen 2 tipos de mantenimiento, que toda infraestructura lo necesita: Eventual y Exhaustivo.

Eventual: Revisión periódica de las instalaciones, verificando el correcto funcionamiento, detectar las posibles anomalías que se puedan presentar y deterioros no contemplados.

Exhaustivo: Servicio de atención de averías de 24 horas

CAPITULO 4

VOZ SOBRE IP Y VIDEO –VIGILANCIA

4.1.- VOZ SOBRE IP

4.1.1Generalidades

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VoIP, Telefonía IP, Telefonía por Internet, Telefonía Broadband y Voz sobre Broadband es el enrutamiento de conversaciones de voz sobre Internet o a través de alguna otra red basada en IP.

Los Protocolos que son usados para llevar las señales de voz sobre la red IP son comúnmente referidos como protocolos de Voz sobre IP o protocolos IP. Ellos pueden ser vistos como implementaciones comerciales de la Red experimental de Protocolo de Voz (1973) inventado por ARPANET.

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP.

Si a todo lo anterior, se le suma el fenómeno Internet, junto con el potencial ahorro económico que este tipo de tecnologías puede llevar acarreado, la conclusión es clara: El VoIP (Protocolo de Voz Sobre Internet - Voice Over Internet Protocol) es un tema en boga y estratégico para las empresas.

La telefonía sobre IP abre un espacio muy importante dentro del universo que es Internet.

Es la posibilidad de estar comunicados a costos más bajos dentro de las empresas y fuera de ellas, es la puerta de entrada de nuevos servicios apenas imaginados y es la forma de combinar una página de presentación de Web con la atención en vivo y en directo desde un call center, entre muchas otras prestaciones. Lentamente, la telefonía sobre IP está ganando terreno... y todos quieren tenerla.

4.1.1.1 Definición e Importancia

DEFINICIÓN

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

La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportadas vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

Las llamadas mediante la tecnología VoIP se podrán realizar desde cualquiera de los terminales telefónicos hacia cualquier número de teléfono público o privado de la red, el sistema se encargará de enrutar cada llamada a través de la red telefónica o de la red de datos privada o a través de Internet, según corresponda en cada caso.

IMPORTANCIA

Ventajas ante la telefonía convencional

Una llamada telefónica normal requiere una enorme red de centrales telefónicas conectadas entre si mediante fibra óptica y satélites de telecomunicación, además de los cables que unen los teléfonos con las centrales. Las enormes inversiones necesarias para

crear y mantener esa infraestructura la tenemos que pagar cuando realizamos llamadas, especialmente llamadas de larga distancia. Además, cuando se establece una llamada tenemos un circuito dedicado, con un exceso de capacidad que realmente no estamos utilizando.

Por contra, en una llamada telefónica IP se comprime la señal de voz y se utiliza una red de paquetes sólo cuando es necesario. Los paquetes de datos de diferentes llamadas, e incluso de diferentes tipos de datos, pueden viajar por la misma línea al mismo tiempo. Además, el acceso a Internet cada vez es más barato, muchos ISPs[40] (Proveedor de Servicios de Internet) lo ofrecen gratis, sólo tienes que pagar la llamada, siempre con las tarifas locales más baratas. También se empiezan a extender las tarifas planas, conexiones por cable, ADSL[41], etc.

En general, el servicio de telefonía vía VoIP es gratuito o cuesta muchísimo menos que el servicio equivalente tradicional y similar a la alternativa que los proveedores del servicio de la Red Pública Telefónica Conmutada (PSTN) ofrecen. Las llamadas de VoIP a VoIP entre cualquier proveedor son generalmente gratis, en contraste con las llamadas de VoIP a PSTN que generalmente cuestan al usuario de VoIP.

Hay dos tipos de servicio de PSTN a VoIP: Llamadas Locales Directas: DID[42] y Números de acceso.

DID conecta a quien hace la llamada directamente al usuario VoIP mientras que los Números de Acceso requieren que este introduzca el número de extensión del usuario de VoIP. Los Números de acceso son usualmente cobrados como una llamada local para quien hizo la llamada desde la PSTN (Red Pública Telefónica Conmutada) y gratis para el usuario de VoIP.

[40] *ISP (Proveedor de Servicios de Internet)*
[41] *ADSL (Asymmetric Digital Subscribe Line)*
[42] *DID (Direct Inward Dialing)*

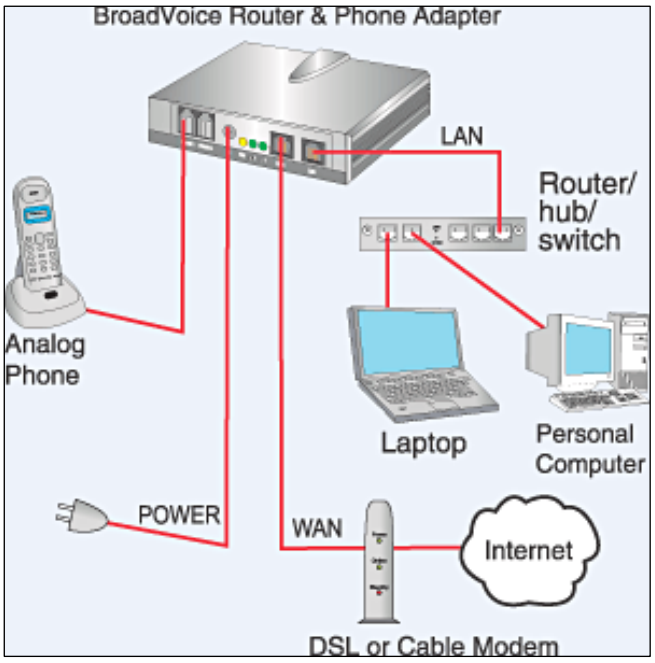


Figura. 4.1. Solución típica basada en VoIP

Funcionalidad

VoIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas tradicionales:

•Las llamadas telefónicas locales pueden ser automáticamente enrutadas a un teléfono VoIP, sin importar en donde se esté conectado a la red. Llevando un teléfono VoIP en un viaje, y donde quiera que se esté conectado a Internet, se podrá recibir llamadas.

•Números telefónicos gratuitos para usar con VoIP están disponibles en Estados Unidos de América, Reino Unido y otros países de organizaciones como Usuario VoIP.

•Los agentes de Call Center usando teléfonos VoIP pueden trabajar en cualquier lugar con conexión a Internet lo suficientemente rápida.

•Algunos paquetes de VoIP incluyen los servicios extra por los que PSTN (Red Telefónica Conmutada) normalmente cobra un cargo extra, o que no se encuentran disponibles en algunos países, como son las llamadas de 3 a la vez, retorno de llamada, remarcación automática, o identificación de llamadas.

Movilidad

Los usuarios de VoIP pueden viajar a cualquier lugar en el mundo y seguir haciendo y recibiendo llamadas de la siguiente forma:

•Los subscriptores de los servicios de las líneas telefónicas pueden hacer y recibir llamadas locales fuera de su localidad. Por ejemplo, si un usuario tiene un número telefónico en la ciudad de Nueva York y está viajando por Europa y alguien llama a su número telefónico, esta se recibirá en Europa. Además si una llamada es hecha de Europa a Nueva York, esta será cobrada como llamada local, por supuesto, debe de haber una conexión a Internet disponible, como WiFi (Wireless Fidelity) para hacer esto posible.

•Los usuarios de Mensajería Instantánea basada en servicios de VoIP pueden también viajar a cualquier lugar del mundo y hacer y recibir llamadas telefónicas.

•Los teléfonos VoIP pueden integrarse con otros servicios disponibles en Internet, incluyendo videollamadas, intercambio de datos y mensajes con otros servicios en paralelo con la conversación, audio conferencias, administración de libros de direcciones e intercambio de información con otros (amigos, compañeros, etc).

4.1.1.2 Evolución de la tecnología VoIP

La voz sobre IP (VoIP), empieza a ser una realidad en muchas empresas por la rápida amortización y el ahorro de costes que proporciona.

La convergencia de voz y datos, con servicios unificados dentro de la empresa, está todavía por empezar, pese a los notables desarrollos que se han producido en los últimos años. Lo más usual es aprovechar la red de datos de banda ancha, como la ADSL, para canalizar llamadas de voz y dejar la unificación para más adelante.

En numerosas empresas se está produciendo una evolución silenciosa de sus redes internas. El objetivo común es reducir la factura telefónica de las llamadas de voz nacionales e internacionales, que representan un elevado porcentaje del total pagado a los operadores. La migración hacia la telefonía IP se hace al margen de los operadores, con

instalaciones privadas, aunque la intensa competencia entre operadores de voz hace que también se puedan contratar servicios unificados a precios interesantes.

El tráfico internacional de telefonía IP representó en el 2003 el 5.5% de las llamadas internacionales, casi el doble que en el anterior, según la Unión Internacional de Telecomunicaciones (UIT) en un informe publicado recientemente.

La consultora IDC prevé que este mercado se duplicará cada año hasta alcanzar los 59.000 millones de dólares en el 2007. Entonces, el tráfico de voz a través de IP será una cuarta parte del total.

La fricción proviene de dos sistemas de tarificación diferentes: el tradicional, basado en el uso y en función del tiempo y la distancia, y el de la tarifa plana que promueve Internet. Se dice que los operadores del mundo desarrollado disponen aún de un margen de 5 a 10 años para reequilibrar las tarifas, mientras que los países en desarrollo no pueden hacerlo.

La regulación del mercado de telefonía IP varía según el país y el tipo de servicio ofrecido. En este sentido, Estados Unidos es el país más avanzado y tres grandes operadores ya ofrecen un servicio de alta calidad.

En la Unión Europea se permite telefonía IP porque existe un cierto retraso de la señal, pero está por decidir la legislación que se aplicará cuando la tecnología avance y la señal se transmita prácticamente en tiempo real.

La popularidad de la voz sobre IP (VoIP) creció a pasos agigantados el año pasado, tanto el número de redes instaladas como el dinero invertido en la compra de este tipo de productos e, incluso, la capacidad de las soluciones se han más que duplicado durante el pasado año. Sin embargo, los problemas de interoperitividad podrían obstaculizar el progreso de estas tecnologías.

Hace pocos años, la voz sobre IP era el dominio de unos pocos, como 3Com, Cisco, Clarent, Nuera Communications e Hypercom. Pero esta tecnología está siendo adoptada

por un amplio número de fabricantes de telecomunicaciones y networking tradicionales, que en un principio vieron la voz sobre IP como una amenaza a su base instalada convencional.

Con todo, la interoperatividad entre los productos VoIP sigue siendo el problema fundamental para la generalización masiva de esta tecnología. No obstante, poco a poco comienza a verse el futuro dentro de la comunidad de fabricantes sobre los distintos estándares. Se puede llegar a afirmar según diversas revistas tecnológicas que coexistirán diferentes normas,

Por lo tanto, se puede decir que aparecerán nuevas categorías de productos, aumento de sus capacidades, caída de los precios en la gama alta, la reorganización de los estándares y la creación de las alianzas de interoperatividad entre fabricantes.

La convergencia de las redes telefónicas y las redes de datos es una de las tendencias tecnológicas más importantes de esta década. El potencial de esta unión es de una gran envergadura, siendo capaz de provocar notables mejoras y ahorros en las redes de comunicaciones de las corporaciones. Lo que se tiende en estos momentos es ofrecer al mercado productos y soluciones que aprovechen la infraestructura de red IP, con el propósito de mejorar la efectividad y productividad de las comunicaciones en las empresas.

Hasta hace pocos años, la mayoría de las corporaciones poseía una PBX[43]de tecnología propietaria para la red telefónica y una red LAN completamente separada para el transporte de datos

En los últimos tiempos se han ido haciendo cada vez más populares los sistemas CTI[44] que relacionan las redes de voz y de datos, pero en un contexto limitado, sin llegar a utilizar un formato de transporte común.

[43] *PBX (Private Branch Exchange)*
[44] *CTI (Integración Telefónica Computacional)*

La integración de la infraestructura telefónica y de datos permite simplificar la administración de los recursos de red y facilita la expansión en capacidad. La ventaja real de la fusión datos-telefonía es su potencial para soportar nuevas aplicaciones hacia el usuario

El impulso tecnológico que hará posible la integración de las redes de voz y de datos es el crecimiento y la difusión de las redes IP, tanto a nivel LAN (Local Area Network) como a nivel WAN (Wide Area Network). En la siguiente década, la conectividad IP alcanzará un grado de penetración similar al enchufe de electricidad en el hogar o la empresa

El networking IP entrega algunas ventajas fundamentales que impactan en los servicios telefónicos y que es conveniente identificar:

1. Las redes IP hacen desaparecer los límites físicos asociados a los teléfonos y funcionalidades telefónicas tradicionales. Dentro de poco será posible acceder simultáneamente a todos los servicios tradicionales y a la capacidad de responder llamadas desde cualquier lugar del mundo, sin que la parte originadora dependa de su posición geográfica. Esto permite ofrecer un servicio flexible para viajeros frecuentes y sitios remotos.

2. El protocolo IP es independiente de la capa de enlace, permitiendo que los usuarios finales elijan el formato de enlace más adecuado a las restricciones de costo y localización. IP puede viajar sobre ATM[45], ethernet, frame relay, ISDN[46] o incluso mediante líneas analógicas.

3. Un conjunto de estándares universales relacionados a las redes IP permitirá a muchos proveedores ofrecer productos compatibles. Estos estándares harán posible la competencia entre múltiples fuentes de servicios de red y hardware. La competencia minimizará los costos y maximizará los nuevos servicios para el usuario final.

[45] *ATM (Modo de transferencia asíncrona)*
[46] *ISDN (Integrated Services Digital Network)*

4. Con la expansión de los servicios de datos, los usuarios finales requerirán un incremento en la seguridad de las redes y el hardware. Los principales proveedores de soluciones LAN/WAN están ya en estos momentos integrando nuevos desarrollos de hardware y software orientados a mejorar la calidad de servicio y confiabilidad. A medida que la telefonía y otros servicios en tiempo real comiencen a ser parte de esta infraestructura, los diseñadores de hardware y software de red incorporarán las restricciones de estas aplicaciones a la confiabilidad y uptime del sistema

La convergencia de las redes de datos y las redes telefónicas será un detonante decisivo para la evolución de la industria de PBX's. La tendencia más importante prevista será la migración desde una estructura predominantemente compuesta por sistemas propietarios a una industria más abierta y con sistemas compatibles sobre el formato IP. La nueva industria PBX IP incluirá cuatro grandes áreas de negocio:

1. Infraestructura IP: Básicamente compuesta por la conectividad IP provista principalmente por los proveedores de equipamiento LAN/WAN.

2. Control de llamada (sistemas operativos y servidores): Sistemas operativos LAN con la capacidad de proveer servicios y funcionalidades telefónicas tradicionales.

3. Dispositivos de usuario: Softwares y teléfonos IP, capaces de ser conectados a redes IP directamente con niveles de calidad similares a la red telefónica tradicional.

4. Aplicaciones avanzadas: Aprovechando la natural integración de los sistemas telefónicos y de datos, han surgido y surgirán aplicaciones de mayor sofisticación que los servicios telefónicos clásicos tales como IVR[47] (respuesta de voz interactiva) y call centers (centro de llamadas).

Es importante tener en cuenta que la calidad y confiabilidad de la infraestructura de red IP y de la arquitectura PBX IP son aspectos claves en la penetración de esta nueva tecnología, ya que dichos atributos deben ser comparables con los niveles de la red telefónica. Una red IP dimensionada adecuadamente a la demanda de tráfico y la

[47] *IVR (Respuesta de voz interactiva)*

inclusión de PBX IP[48] permiten obtener niveles de servicio similares a una red telefónica tradicional. Algunas de las funcionalidades incluidas en la PBX IP son:

- Resistencia a cortes de abastecimiento de energía
- Configuración redundante en el servidor para aumentar la confiabilidad en el control de llamada
- Enrutamiento de llamada alternativo cuando los enlaces IP o los enlaces telefónicos no están disponibles

Unos ejemplos de adaptación son los siguientes:

- PBX IP detrás del sistema PBX tradicional existente: Esta configuración extiende la cobertura del sistema telefónico privado haciendo uso de la red IP como transporte. La PBX IP se conecta a la PBX tradicional mediante un gateway y el centro de procesamiento de llamada se instala en un servidor NT[49] en el centro de datos de la empresa. Bajo esta configuración, se mantienen todas las funcionalidades telefónicas y el ambiente de operación es transparente para el usuario.

- Oficinas remotas sobre la red IP: Esta aplicación es similar a la anterior en cuanto a funcionalidades, con la diferencia que se incluyen interfaces WAN IP[50] para conectar en red a determinados sitios remotos. El procesamiento de llamada puede permanecer centralizado o bien puede ser instalado en el sitio remoto como fuente secundaria

- Utilizar la red de banda ancha existente para canalizar las llamadas de voz.

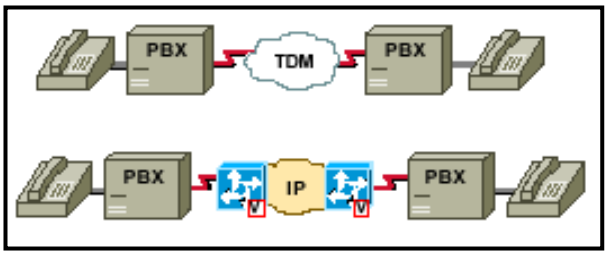


Figura. 4.2. Sistema convencional de telefonía acoplado a la telefonía IP

[48] *PBX IP (Private Branch Exchange based on Internet Protocol)*
[49] *NT (New Technology)*
[50] *WAN IP (Wide Area Network based on Internet Protocol)*

Grado de implantación de esta tecnología

La tecnología VoIP crece cada año, tanto en número de usuarios como en inversiones realizadas por las empresas. Esta tecnología ha ido evolucionando año a año hasta lo que es ahora, aunque todavía le queda un largo camino por recorrer.

Todo empezó en 1995, año en que se empezó a introducir esta tecnología. Para finales de 1996 la telefonía IP aún era considerada una radio para aficionados de Internet, una aplicación que muy pocas personas utilizaban, con PC's con micrófonos y shareware de voz sobre IP. Para entonces la calidad del servicio era de pésima calidad.

Ya en 1997 apareció nuevo software para VoIP para clientes, pero la calidad que esperaban estos no era la misma que ofrecían las llamadas tradicionales, lo que desalentó a los clientes. Esta tecnología de VoIP era prácticamente inexistente en el mundo empresarial, y los primeros dispositivos de acceso que pasan las llamadas hacia y desde Internet u otras redes IP (gateways) estaban muy lejos de ser lo que son.

Los años 1997 y 1998 fueron los años del gateway y del gatekeeper respectivamente. Además, durante estos años se lograron unas normas de interoperabilidad, lo que hizo que los proveedores de equipos y servicios pudiesen concentrarse en desarrollar aplicaciones de valor agregado que se necesitan para llevar la demanda de la voz sobre IP a ser una alternativa de bajo costo ante los servicios tradicionales de larga distancia. Con todo ello la voz sobre Internet empieza a ser una realidad cotidiana en muchas empresas por la rápida amortización y el ahorro de costes que proporciona.

Hasta ahora básicamente son sólo las empresas las que adoptan el cambio por la reducción de costos que ello conlleva. Como ejemplo se puede decir, que si una empresa coloca un gateway la inversión se amortiza antes de un año con llamadas provinciales, y en tres meses en las empresas que llaman tres horas al día con su oficina situada en América o Asia.

Pero la convergencia de voz y datos, con servicios unificados dentro de la empresa, es aún insuficiente, pese a los notables desarrollos que se han producido en los últimos años.

El avance de esta tecnología es muy grande año a año. Cada año aparecen nuevos productos con más capacidades y más recursos lo que posibilita su implantación. Cada año, el tráfico de telefonía IP aumenta el doble respecto al anterior, por lo que dentro de unos años, siguiendo ese crecimiento, el tráfico de voz sobre IP habrá crecido extraordinariamente desde su implantación.

A nivel de usuario pero, esta tecnología no esta lo suficientemente implantada, y es aquí por donde tiene más camino por hacer. Las actuales conexiones a Internet imposibilitan tener una conversación con la misma calidad que con la telefonía tradicional, y sólo mediante conexiones de banda ancha la calidad es parecida.

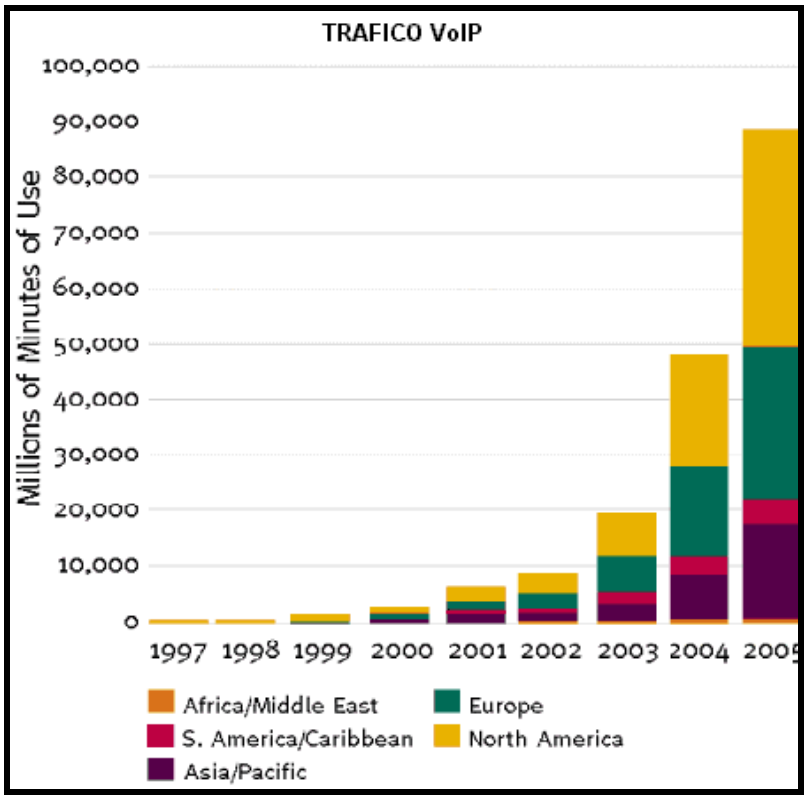


Figura. 4.3. Implantación de VoIP.

4.1.2 Proveedores de servicio VoIP

El primer paso de hacer una llamada de teléfono por VoIP es suscribirse a un servicio. VoIP permite que el usuario tenga un número telefónico estándar y que pueda conectarse con cualquier otro número telefónico estándar, no importando si la persona a quien se está llamando utiliza VoIP o el servicio telefónico tradicional. Para esto se requiere del servicio de un proveedor de VoIP que suministre una conexión entre sus llamadas a través del Internet y la red de telefonía tradicional.

Algunos servicios de telefonía por Internet solamente permiten que el usuario llame a otros usuarios del mismo servicio. Por éste y otros motivos, es importante investigar y entender las opciones y contrato del proveedor de VoIP antes de subscribirse.

Una vez que se contrata el servicio, el proveedor del servicio de VoIP enviará un adaptador de teléfono para banda ancha, que se enchufa directamente a la conexión a Internet. Luego se conecta el aparato telefónico existente al adaptador telefónico. Finalmente, todo lo que hay que hacer es levantar el auricular y marcar el número.

La calidad de la voz es buena. Aunque en realidad, hoy en día no hay proveedor de Voip con voz de mala calidad, siempre y cuando se use conexión de banda ancha

Sobre los últimos tres años ha llegado a ser cada vez más difícil recopilar una descripción de todos los servicios de funcionamiento mundiales de VoIP o abastecedores de banda ancha para telefonía.

Encontrar y comparar los servicios de VoIP en el Internet es ya una misión propia. Algunos de los muchos, establecidos servicios de VoIP son fáciles de encontrar en centenares de sitios de Internet. Con sus presupuestos extensos de la comercialización y bombardeo diario de los lanzamientos de prensa, han establecido una dominación del mercado en un período del tiempo corto. Hay, sin embargo, cientos de pequeños y nuevos servicios de VoIP con el mismo servicio al cliente y niveles de calidad, incluso más barato de las tasas de VoIP y paquetes mensuales con llamadas ilimitadas de VoIP .

Hace unos pocos meses un nuevo grupo de proveedores de servicio de VoIP han estado introduciendo su marca en el mercado de VoIP. Estos proveedores están ofreciendo las llamadas VoIP gratis a un amplio rango de destinos y están capturando una cuota de mercado significativa Siendo el primer servicio de VoIP en ofrecer estas llamadas VoIP Buster es el mas conocido, pero justo recientemente, una compañía hermana, VoIP Stunt en Alemania fue lanzada con llamadas libres a 39 destinos.

La telefonía IP es un servicio que desde la puesta en marcha de skype se ha convertido en una revolución. Desde mi punto de vista será superada muy pronto en el ámbito web 2.0, pero debido a la conmoción que ha ocasionado en las compañias telefónicas merece una atención principal por los medios y usuarios. Desde ebay, yahoo, google, Skype a las telefónicas tradicionales tienen el ojo puesto en la telefonía IP como plan de marketing.

Una relación de diferentes lugares VoiIP con características básicas se da a continuación:

- Skype (http://www.skype.com), tras su exitosísima salida al mundo real ahora acaba de terminar la fase beta de skype 2.0 con notorias mejoras respecto al inicial: videochat on line, posibilidad de crear grupos de contactos, muestra la hora en la que viven nuestros contactos (para evitar llamadas intempestivas), mejor barra de herramientas e idiomas. Con skypeout (se puede llamar a telefonía convencional).

- Voipbuster (http://www.voipbuster.com/). Es uno de los más modernos pero tiene la ventaja que para algunos paises (España entre ellos) el llamar a teléfonos fijos es gratuito si se adquiere un bono (con comprar un euro es suficiente) sino tiene un límite de llamada a fijos de un minuto, sin embargo no parece que puedan recibir llamadas de telefonía convencional.

- Voipstunt (http://www.voipstunt.com/): Telefonía a fijo totalmente gratis para algunos paises, es el más nuevo y el que más servicio gratuito tiene, no parece que puedan recibir llamadas de telefonía convencional. Es de la misma empresa que voipbuster: betamax.

- Gizmo (http://www.gizmoproject.com/): telefonía gratuita a EEUU y a costes bajos a otros paises, incorporando mensajería, mapas, etcétera. Tienen el servicio call-out para llamar a telefonía convencional.

- P4Gphone (http://www.4gphone.com) Telefonía IP, incluso con equipos de telefonía para la completa instalación. Tienen ofertas integradas de paquete de telefonía y terminales a precios competitivos.

- DialPad (http://www.dialpad.com/): la apuesta de yahoo por la telefonía IP. Tiene posibilidad de planes y prepago con sustanciosos ahorros. Parece no admitir llamadas de telefonía convencional.

- Sip2go (http://sip2go.com): Telefonía Ip de bajo coste incluso para móviles: Tiene un número telefónico (número de teléfono global) para la recepción de llamadas convencionales.

- Vonage (http://www.vonage.com/) : Incluye un sistema dentro de sus paquetes de tarifas que engloba fax y comunicaciones via email, p2p etc, en cualquier lugar del mundo así como llamada a telefonía convencional. muy barato para EEUU, Canadá y Puerto Rico.

- Netzerovoice (http://www.netzerovoice.com/): Se puede recibir llamadas y actuar como una pequeña centralita: para llamar a cualquier tipo de teléfono tienen tarifas y paquetes especiales.

- Voiceeclipse (http://www.voiceeclipse.com/):Telefonía IP que incluye paquetes con terminales para diferentes usos personalizados (tiene coste de alta) y permite en sus paquetes la recepción de llamadas telefónicas convencionales.

- Skypho (http://www.skypho.net/): La apuesta italiana en VoIP. Número telefónico accesible desde telefonía tradicional de manera gratuita y posibilidad de adquirir teléfonos usb o Voip.

- Wavago (http://www.wavigo.com/DLESP.html): en fase de pruebas que se consumarán en el 2007.

- Stanaphone (https://www.stanaphone.com/): telefonía IP con caracter empresarial y de negocio, incluyen un paquete con fax, etc.

- TotalCall (http://totalcallip.com). Con planes interesantes para quien habla a menudo con EEUU. No parece contemplar la recepción de llamadas de telefonía convencional.

- Jajah (http://www.jajah.com/en/index.asp). Uno de los mas modernos y baratos, incorpora ventajas como correo de voz, encriptación, acceso a usuarios de skype, etc, merece la pena echarle un vistazo y sus tarifas no son altas.

PROVEEDORES A NIVEL NACIONAL

1.- Proveedor VoIP: Bonacom

Ubicación: [Oficina General] - **Ecuador / Guayaquil**

[Punto de presencia] - USA / MIAMI

Categorías VoIP: Proveedor de VoIP Internacional al por mayor

Servicios VoIP: Soluciones Call Routing VoIP

2.- Proveedor VoIP: Inter2fone

Ubicación:[Oficina General] - USA / Miami

[Punto de presencia] - USA / Miami,

[Punto de presencia] - **Ecuador / Quito**

Categorías VoIP: Hardware, Proveedor de servicio Hosted VoIP bilingüe, Proveedor Internacional al por mayor de VoIP, Proveedor del servicio de Telefonía por Internet, SIP[51] Billing, Consultoria Voip , Voip Termination ISP, Wireless Broadband

VoIP Services: Call Routing VoIP Soluciones, H.323 Wireless/ GSM[52] VoIP Soluciones, Servicio de Instalación y soporte, dispositivos IP, Outsourced Billing, PC to

[51] *SIP (Session Initiation Protocol)*

[52] *GSM (Global System for Mobile Communications)*

Phone, Phone To PC, Phone To Phone, Servicio de Administración de Proyectos, SIP Softswitch & CPE[53], SIP VoIP Gateway, System Integration, Termination

Descripción: Inter2fone tiene sus oficinas centrales en Miami, Florida USA y sus oficinas regionales en Ecuador y en Suiza. Fue inicialmente formado como una división de FIX GROUP para atender servicios de VoIP para el mercado Latinoamericano.

3.- Proveedor VoIP: Omicron Technologies

Ubicación: [General office] - Ecuador / Quito

Categorías VoIP: Hardware, Proveedor Internacional al Por Mayor de VoIP, Internet Telephony Service Provider, Servicio de Internet VoIP y videoconferencia, Provider, Voip consulting

Servicios VoIP: Fax a Fax, dispositivos IP, PC to Phone, Phone To PC, Phone To Phone, Voz y video conferencia, Web Call

Telefonía sobre IP: Situación Legal.

Siempre que aparecen innovaciones y nuevas opciones en contra de prácticas establecidas o situaciones que se consideran predefinidas, existe el riesgo de que caer en un limbo cultural, legal o de otro tipo, a menudo provocado por intereses afectados por las innovaciones que rompen monopolios o cambian estructuras.

Esto ha sucedió a lo largo de la historia de la humanidad y ha dado lugar a figuras inquisitorias con las consecuencias que la misma historia nos muestra.

La telefonía IP no cuenta con una regulación legal definida a nivel mundial centrándose la discusión en aspectos como:

-Se trata de Telecomunicaciones o transmisión de datos. (Aquí esta determinación implica si paga impuestos como en Ecuador del 29% o no y qué tipo de licencias se requieren para prestar el servicio.)

[53] *CPE (Customer Premises Equipment)*

Las normas legales de formas diversas tratan específicamente de proteger monopolios establecidos por operadoras a menudo ineficientes que encarecen los servicios sin beneficio para el usuario.

Si existe una alternativa práctica, cómoda y accesible para los usuarios, entonces lo que cabe es impulsarla, incentivarla y dotarla de normas que le permitan crecer. Lo contrario es lo que se pretende en muchos países incluido Ecuador, de colocarle barreras para impedir su desarrollo y evitar que los usuarios se beneficien de los avances de la tecnología y la técnica modernas so pretexto de proteger a las empresas de telecomunicaciones existentes..

El tipo de regulación que se necesita tiene que estar acorde con el mercado, con las necesidades de los usuarios y con el desarrollo tecnológico.

Respecto del mercado deben primar las consideraciones de libre competencia y desarrollo. Los usuarios deben contar con normas básicas de protección y mecanismos de atención a sus necesidades. En el aspecto tecnológico debe primar la neutralidad tecnológica y protegerse las innovaciones.

El caso concreto en varios países ha sido el cierre de los sitios que prestan el servicio de VoIP para el público, aun cuando este servicio sigue prestándose desde los llamados cyber cafés o cafés net, e incluso de tiendas o pequeños locales o domicilios a los cuales acuden los usuarios en busca de comunicaciones a costos menores y mejor atención.

Las empresas en sus comunicaciones internacionales usan con éxito y enormes ventajas de ahorros en costos, la telefonía IP, el fax por IP y otros servicios son ampliamente usados en Ecuador y en el mundo.

La telefonía tradicional internacional tiene un importante reto que no puede resolverse por vía legal o imposiciones legales. Tienen que innovar y ofrecer servicios similares para competir.

La caída de los ingresos provenientes principalmente de comunicaciones de larga distancia no es resultado solamente del uso del a tecnología VoIP sino principalmente del aparecimiento del email como alternativa de comunicación instantánea, más barata y accesible.

Las telecomunicaciones empleando diversos mecanismos para abaratarlas han sido permanentemente objetadas por las instituciones estatales como ilegales, desde el callback hasta el bypass, que emplean circuitos más económicos. Esto en algún momento puede justificarse por la necesaria protección a nuestras empresas de telecomunicaciones, pero el caso de la telefonía IP es sustancialmente diferente pues implica un beneficio para el usuario y resuelve un problema social de importantes repercusiones.

4.1.3 Dispositivos de VoIP

Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, permiten construir las aplicaciones VoIP. Estos elementos son:

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- Gateways (pasarelas RTC[54] / IP).
- Gatekeeper.
- Unidades de audioconferencia múltiple (MCU Voz).
- Servicios de Directorio.

[54] *RTC (Red telefónica conmutada)*

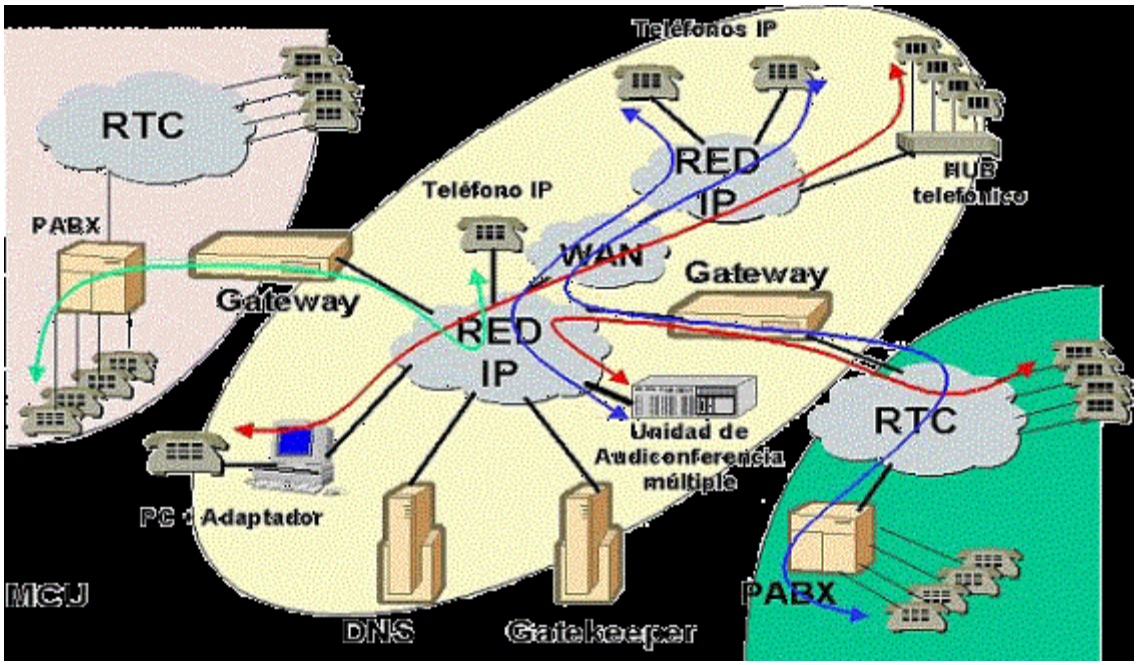


Figura. 4.4. Elementos de una red VoIP

Las funciones de los distintos elementos son fácilmente entendibles a la vista de la figura, si bien merece la pena recalcar algunas ideas.

GATEKEEPER

El Gatekeeper es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de aquel. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.

GATEWAY

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica. Se puede considerar al Gateway como una caja que por un lado tiene un interface LAN y por el otro dispone de uno o varios de los siguientes interfaces:

•FXO[55]. Para conexión a extensiones de centrales ó a la red telefónica básica.

FXO es un dispositivo de computador que permite conectar éste a la RTB, y mediante un software especial, realizar y recibir llamadas de teléfono. Sirve sobre todo

[55] *FXO (Foreign Exchange Office)*

para implementar centrales telefónicas (PBX) con un ordenador. Existen dispositivos que se **FXO** en los gateway de VoIP, como en tarjetas de ordenadores.

•FXS[56]. Para conexión a enlaces de centrales o a teléfonos analógicos.

Las tarjetas FXS sirven para conectar teléfonos analógicos normales a un computador, y mediante un software especial, realizar y recibir llamadas hacia el exterior, o hacia otros interfaces FXS.

•E&M[57]. Para conexión específica a centrales.

E&M es una interfaz en un dispositivo VoIP que le permite ser conectado a las líneas troncales analógicas de un PBX.

•BRI (Basic Rate Interface) Acceso básico RDSI (Red Digital de Servicios Integrados) (2B+D).

•PRI (Primary Rate Interface) Acceso primario RDSI (30B+D).

•G703/G.704. (E&M digital) Conexión especifica a centrales a 2 Mbps.

Los distintos elementos pueden residir en plataformas físicas separadas, o se pueden encontrar varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos Gatekeeper y Gateway.

Gateway de Voz sobre IP

El término gateway de VoIP en ocasiones también se suele utilizar para hacer referencia a otros elementos funcionales, que se posicionan entre redes IP para desarrollar determinadas funciones de mapping, por ejemplo en la capa IP. Entidades específicas como proxies VoIP, transcodificadores VoIP, traductores de direcciones de red VoIP, etc., caen en esta categoría de gateways de VoIP.

Los gateways de interconexión en este contexto son básicamente dispositivos lógicos, aunque también pueden ser, y de hecho son, dispositivos físicos, como se verá

[56] *FXS (Foreign Exchange Station)*
[57] *E&M (*recEive and transMit)

posteriormente. Tienen una serie de atributos que caracterizan el volumen y tipos de servicios que pueden proveer, por ejemplo:

• Capacidad, expresa el volumen de servicio que puede brindar el gateway, estando relacionado directamente con el número de puertos que tiene (igual al número máximo de llamadas simultáneas) y la velocidad del enlace de acceso.

• Protocolos de señalización soportados, tanto relativos a redes de VoIP como relativos a redes SCN[58].

• Codecs de voz utilizados.

• Algoritmos de encriptado que soporta.

• Rango de direccionado, que es el rango o abanico de números telefónicos a los que se tiene acceso en la GSTN[59] desde la red IP. En relación con la tarificación, este rango de direccionado puede o no estar fraccionado.

En general, los gateways de interconexión tienen que proporcionar los siguientes mecanismos o funciones:

• Adaptación de señalización, básicamente tiene que ver con las funciones de establecimiento y terminación de las llamadas,

• Control de los medios, se relaciona con la identificación, procesamiento e interpretación de eventos relacionados con el servicio generados por usuarios o terminales,

• Adaptación de medios, según requerimientos de las redes.

El gateway de interconexión también desarrolla la función control de medios, que se ocupa de "manejar" toda la información de control generada por el terminal. Para el caso de comunicaciones de voz, la información de control del nivel de usuario más a

[58] *SCN (Switched Circuit Network)*
[59] *GSTN (General Switched Telephone Network)*

destacar, son los tonos multifrecuencia (DTMF[60]) que produce un teclado telefónico convencional (por ejemplo, para interactuar con un servidor de voz). Dadas las características de estas señales, en el sentido que están en el rango audible pero no son señales de voz, sino tonos, es necesario prestar particular atención para su trasvase por la conexión híbrida que representa la pasarela de interconexión. Las técnicas de compresión de voz de baja velocidad introducen considerable distorsión en los tonos DTMF, provocando la recepción y correspondiente decodificación incorrecta en los receptores. Entonces, esto requiere que las señales de audio y los tonos DTMF sean separados en el gateway (si no lo ha sido ya en el emisor) y conducidas de forma independiente al receptor.

- Hay dos posibles soluciones para el transporte de los tonos DTMF: Transporte "dentro de banda": consiste en transportar estos tonos, digitalizados y paquetizados, con los protocolos RTP/UDP[61], mediante un formato de carga útil dedicado.

- Transporte "fuera de banda": conlleva a utilizar un canal de control de medios seguro (no UDP, sino TCP) para el transporte de las señales DTMF.

El transporte de los tonos DTMF "dentro de banda" se ve afectado por la falta de garantía en la entrega de paquetes que el protocolo UDP ofrece, con nefastas consecuencias para el funcionamiento del servicio en caso de pérdida de un paquete asociado a un tono DTMF. Tiene la ventaja de que los tonos permanecen sincronizados en el tiempo con respecto a la voz.

En cambio, el transporte "fuera de banda" si bien gana en seguridad respecto a la entrega segura de los paquetes, pierden las señales su referencia exacta en el tiempo en relación con el stream de voz. Esta es precisamente la solución adoptada en la Recomendación H.323, mediante el canal H.245.

[60] *DTMF (Dual Tone Multi Frequency)*
[61] *RTP/UDP (Real Time Protocol/ User Datagram Protocol)*

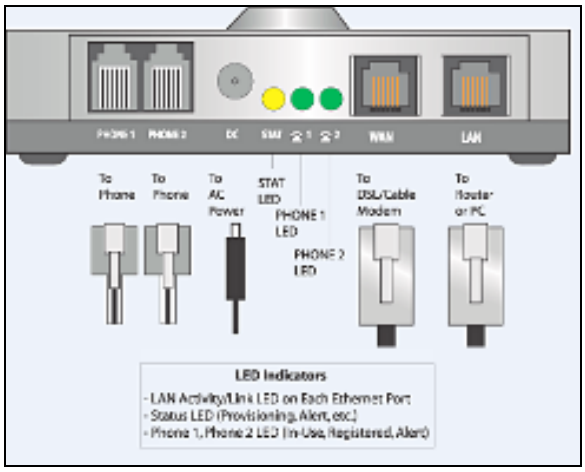


Figura. 4.5. Adaptador de analógico a VoIP.

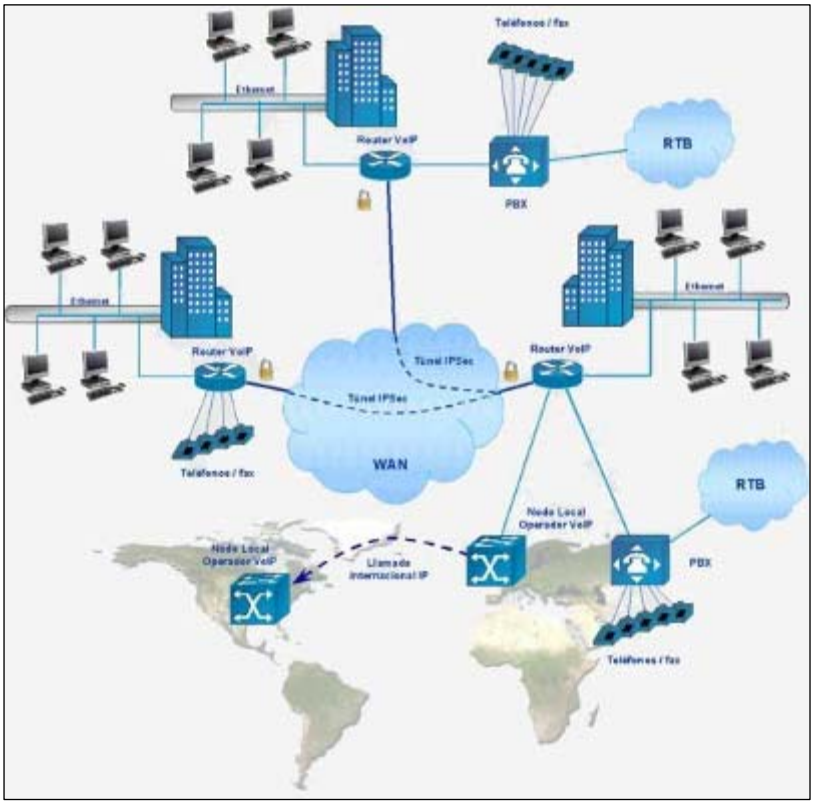


Figura. 4.6. Conexión de dispositivos de VoIP

Teléfonos IP

Los teléfonos IP pasan como teléfonos de escritorio convencionales, pero se conectan con el Internet (vía Lan Ethernet o Wireless) hasta en ocasiones mejor que la red básica de telefonía. Son independientes de los PCs.

Adaptadores análogos del teléfono

Estos adaptadores (ATAs) permiten convertir cualquier teléfono análogo en un teléfono listo para usarse en la red IP, con ello se puede recibir y realizar llamadas sin tener encendido un computador.

Microteléfonos de la PC, Speakerphones y adaptadores del teléfono

Los microteléfonos se conectan al computador vía la tarjeta de los sonidos o un puerto del USB y trabajan junto con un softphone para proveer un servicio completo de VoIP. También existen altavoz-teléfonos handsfree basados en conexión USB, y adaptadores del teléfono que sean similares a ATAs.

Todos estos dispositivos trabajan sin ningún software especial o vienen con software libre. Muchos trabajan en los sistemas de MacOS y de Linux así como Windows.

Hardware del asterisco

El asterisco es un PABX abierto de VoIP, que funciona en el sistema operativo de Linux. Es un producto extremadamente de gran alcance capaz de las funciones más avanzadas del PABX incluyendo voz-correo, llamadas de conferencia, trunking, y mucho más. Para conectar los teléfonos directamente a este hardware, o conectarlo con el PSTN, se requieren tarjetas de interconexión.

Entradas de los medios del grado del negocio

Las entradas de los medios son convenientes para los negocios que requieren un número significativo de líneas de VoIP - como opción independiente o enganchado hasta un PABX existente. Estas entradas hacen el trabajo de ATAs múltiples en una unidad así como funciones adicionales de enrutamiento

Muchas de estas unidades están disponibles en configuraciones de H.323 y de MGCP[62] a petición

[62] *MGCP(Media Gateway Control Protocol)*

4.1.3.1 Características de funcionamiento

VoIP convierte la señal de voz de su teléfono en una señal digital que puede viajar a través del Internet. Si llama a un número telefónico regular, la señal entonces se reconvierte en el otro extremo. Dependiendo del tipo de servicio de VoIP, se puede hacer llamadas de VoIP desde una computadora, un teléfono especial para VoIP, o un teléfono tradicional con o sin adaptador. Además, la existencia de nuevos puntos de acceso a Internet de alta velocidad o "*hot spots*" en lugares públicos como aeropuertos, parques, y cafés permiten conectarse a Internet y usar el servicio de VoIP vía inalámbrica. Si el proveedor de servicio de VoIP asigna un número de teléfono regular, entonces se podrá recibir llamadas de teléfonos regulares que no necesitan ningún equipo especial y seguramente se podrá marcar de forma regular.

Aquí un ejemplo de cómo funciona el servicio de VoIP:

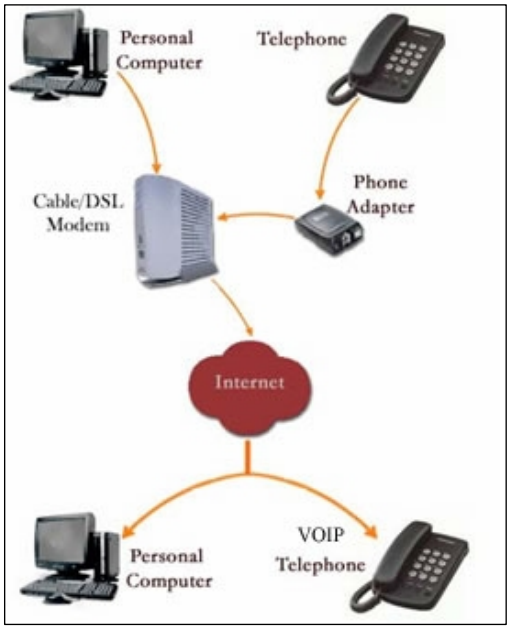


Figura. 4.7. Servicio de VoIP

Requerimientos de una red para soportar VoIP

A continuación se mencionan aspectos importantes que se deben tener en la red IP para implantar este servicio en tiempo real

•Manejar peticiones RSVP[63] que es un protocolo de reservación de recursos.

•El costo de servicio debe estar basado en el enrutamiento para las redes IP.

•Donde se conecta con la red pública conmutada un interruptor de telefonía IP debe soportar el protocolo del Sistema de Señalización 7 (SS7). SS7 se usa eficazmente para fijar llamadas inalámbricas y con línea en la PSTN y para acceder a los servidores de bases de datos de la PSTN. El apoyo de SS7 en interruptores de telefonía IP representa un paso importante en la integración de las PSTN y las redes de datos IP.

•Se debe trabajar con un comprensivo grupo de estándares de telefonía (SS7, Recomendación H.323) para que los ambientes de telefonía IP y PBX/PSTN/ATM vídeo y Gateway telefónica puedan operar en conjunto en todas sus características

Arquitectura de red

El propio Estándar define tres elementos fundamentales en su estructura:

•*Terminales*: Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.

•*Gatekeepers*: Son el centro de toda la organización VoIP, y serían el sustituto para las actuales centrales. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.

•*Gateways*: Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.

Con estos tres elementos, la estructura de la red VoIP podría ser la conexión de dos delegaciones de una misma empresa. La ventaja es inmediata: todas las comunicaciones entre las delegaciones son completamente gratuitas. Este mismo esquema se podría aplicar para proveedores, con el consiguiente ahorro que esto conlleva.

•*Protocolos*: Es el lenguaje que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es muy importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

[63] *RSVP (ReSerVation Protocol)*

- Por orden de antigüedad (de más antiguo a más nuevo):
  - H.323 - Protocolo definido por la ITU-T[64]
  - SIP - Protocolo definido por la IETF[65]
  - Megaco (También conocido como H.248) y MGCP - Protocolos de control
  - Skinny Client Control Protocol - Protocolo propiedad de Cisco
  - MiNet - Protocolo propiedad de Mitel
  - CorNet-IP - Protocolo propiedad de Siemens
  - IAX - Protocolo original para la comunicación entre PBXs Asterisk (obsoleto)
  - Skype - Protocolo propietario peer-to-peer utilizado en la aplicación Skype
  - IAX2 - Protocolo para la comunicación entre PBXs Asterisk en reemplazo de IAX
  - Jingle - Protocolo abierto utilizado en tecnología Jabber

VoIP presenta una gran cantidad de ventajas, tanto para las empresas como para los usuarios comunes.

El Estándar VoIP (H323)

Definido en 1996 por la ITU proporciona a los diversos fabricantes una serie de normas con el fin de que puedan evolucionar en conjunto.

El estándar H.323 especifica los componentes, protocolos y procedimientos que proveen los servicios de comunicación multimedia sobre redes de paquetes sin garantía de calidad de servicio, tanto para sesiones multipunto como punto a punto. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol). Además, H.323 también define la señalización necesaria para comunicaciones multimedia sobre redes IP (entre otras). Para el transporte de medios utiliza los protocolos RTP[66]/RTCP[67].

Los terminales y equipos H.323 soportan aplicaciones con requerimientos de tiempo real (voz y vídeo), así como aplicaciones de datos y combinaciones de ellas

[64] *ITU-T (International Telecommunications Union Telecommunication Standardization Sector)*
[65] *IETF (Internet Engineering Task Force)*
[66] *RTP Real Time Transport Protocol*
[67] *RTCP Real Tine Communications Protocol.*

(videotelefonía..etc). Los terminales H.323 pueden ser terminales explícitamente diseñados a este fin o pueden estar integrados en PC's.

Características principales

Por *su estructura el estándar proporciona las siguientes ventajas:*

- Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento. Las redes soportadas en IP presenta las siguientes ventajas adicionales:

  - Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.
  - Es independiente del hardware utilizado.
  - Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.
  - Permite la integración de Video y TPV[68]

Actualmente, las redes desplegadas para la transmisión de voz sobre IP son en su mayor parte propietarias, utilizando mecanismos de señalización, control y codificación de la voz propios de los suministradores, y con muy poca o sin ninguna interoperabilidad entre ellas. La norma H.323 de ITU viene a poner luz sobre este tema y es, a partir de ahora, prácticamente de obligado cumplimiento para los suministradores. Entre otras cosas, el hecho de que NetMeeting, un cliente H.323 desarrollado por Microsoft para Windows 95, 98, 2000 y Windows NT, se entregue de forma gratuita, es prácticamente una garantía de que esta es la norma que hay que cumplir.

[68] *TPV Transfer Protocol Vision.*

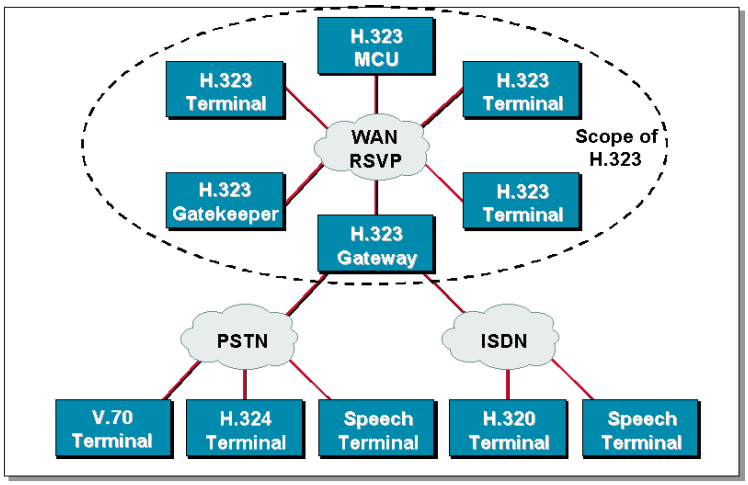


Figura. 4.8. Alcance de la norma H.323

La norma H.323 es muy compleja al integrar no sólo voz sobre IP, sino también comunicaciones multimedia. La presencia de un Gatekeeper como elemento centralizado de control de la red es uno de los aspectos fundamentales de la norma. Existen diferentes variantes de códecs (codificadores/compresores/descompresores/decodificadores) en la norma, pero se acordó a mediados de 1997 en un consorcio denominado IMTC, en el que están presentes Microsoft, Cisco, HP, etc., que el codec preferido para voz sobre IP es el apoyado por Microsoft, *G.723.1,* que funciona a 6,4 kbit/s totales (total de ambos sentidos), más el overhead causado por cabeceras de IP y UDP (unos 10 kbit/s es el resultante). Cisco, de momento, sigue utilizando G.729a, que resulta menos exigente en cuanto a capacidad de proceso.

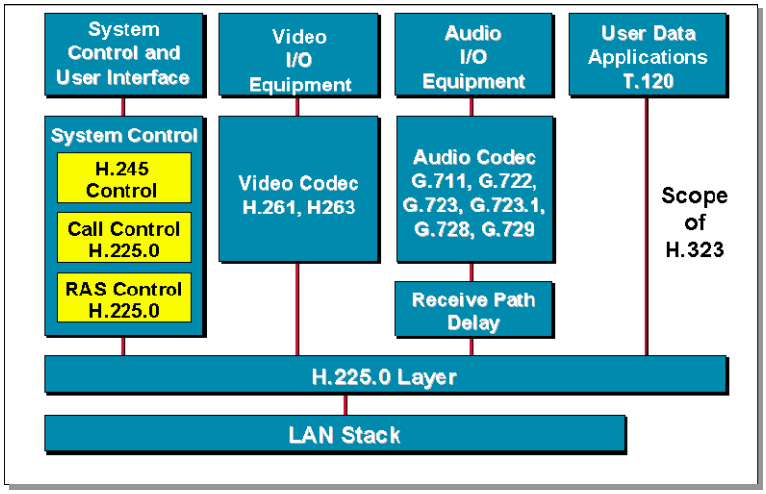


Figura. 4.9. Normas adicionales incluidas en H.323

El mayor problema que enfrenta la voz sobre IP, es el de los retrasos acumulados en el tránsito de los paquetes y en el propio proceso de codificación. En la Internet global, los retrasos pueden llegar a ser del orden de dos segundos, impidiendo cualquier posibilidad de una conversación normal. La causa principal de estos retrasos es la pérdida de paquetes, que en muchos casos puede llegar a un 40%. La única manera de mantener este tipo de cifras bajo control es trabajar en una red privada, dimensionada para este tipo de tráfico, o introducir conceptos de calidad de servicio (QoS). Esta es la razón por la que la mayor parte de proveedores de voz por Internet disponen de una red dedicada para este propósito, ya que de otra manera no se puede conseguir la calidad requerida por los usuarios, sobre todo si pertenecen al mundo empresarial.

Protocolo SIP

SIP (**S**ession **I**nitiation **P**rotocol) es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet. Fue desarrollado inicialmente en el grupo de trabajo IETF MMUSIC (Multiparty Multimedia Session Control) y, a partir de Septiembre de 1999, pasó al grupo de trabajo IETF SIP.

Algunas organizaciones de estandarización que lo están usando actualmente, o considerando utilizarlo en un futuro inmediato:

- Grupo de trabajo IETF PINT.
- 3GPP[69] para redes móviles de tercera generación.
- Softswitch Consortium.
- IMTC y ETSI Tiphon están trabajando en la interoperabilidad entre SIP y H.323.
- Especificación PacketCable DCS (Distributed Call Signaling).
- SpeechLinks, para enlaces web activados por la voz.

Protocolo H.248 (MEGACO)

H.248 (también conocido como protocolo Megaco) es el estándar que permite que un media gateway controller (MGC) controle a media gateways (MG). H.248 es el resultado de la cooperación entre la ITU y el IETF. Antes de lograr esta cooperación

[69] *3GPP (3rd Generation Partnership Project)*

existían varios protocolos similares compitiendo entre si, principalmente MGCP (la combinación de SGCP[70] e IPDC[71]) y MDCP. H.248 se considera un protocolo complementario a H.323 y SIP, un MGC controlará varios MGs utilizando H.248, pero será capaz de comunicarse con otro MGC utilizando H.323 o SIP.

Parámetros de la VoIP

Este es el principal problema que presenta hoy en día la penetración tanto de VoIP como de todas las aplicaciones de IP. Garantizar la calidad de servicio sobre una red IP, por medio de retardos y ancho de banda, actualmente no es posible; por eso, se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

- *Códecs*:

La voz ha de codificarse para poder ser transmitida por la red IP. Para ello se hace uso de Códecs que garanticen la codificación y compresión del audio o del video para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el Códec utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos.

Entre los códecs utilizados en VoIP encontramos los G.711, G.723.1 y el G.729 (especificados por la ITU-T)

- *Retardo* o *latencia*:

Una vez establecidos los retardos de procesado, retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.

- *Calidad del servicio*:

La calidad de servicio se está logrando en base a los siguientes criterios:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.

[70] *SGCP (Simple Gateway Control Protocol)*
[71] *IPDC (Internacional Programme for the Development of Communication)*

- Compresión de cabeceras aplicando los estándares RTP/RTCP.
- Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son: CQ (Custom Queuing): Asigna un porcentaje del ancho de banda disponible. PQ (Priority Queuing): Establece prioridad en las colas. WFQ (Weight Fair Queuing): Se asigna la prioridad al tráfico de menos carga. DiffServ: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.
- La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

4.1.3.2 Criterios de selección de equipos

Dentro de los parámetros que se deben tomar en cuenta para la elección de un equipo de VoIP a ser implementado se encuentran:

- Tipo de gateway
- Puerto de conexión a Internet
- Interfaz LAN
- Protocolo de comunicación
- Tipos de protocolo que soporta para conexión con otros dispositivos
- Compatibilidad con otros equipos
- Servicios incorporados en los equipos
- Funcionalidad
- Escalabilidad
- Seguridades
- Ancho de banda

Para poder elegir adecuadamente el tipo de equipo a utilizarse es necesario tomar algunos parámetros de dimensionamiento como: tipo de aplicación, ancho de banda de la red en la cual se va a implementar el servicio, demanda de usuarios, disponibilidad de QoS en la red,etc.

Los equipos VoIP en algun punto (teléfono IP o gateway FXS) codifican una señal analógica utilizando un protocolo que separa la voz en paquetes de datos. Cada protoclo

tiene un grado de compresión de datos distinto. Puede hacerse una analogía con la resolución de la imagen de una cámara digital. Si existe mucha compresión, la imagen no saldrá nítida. Análogamente en VoIP, si existe mucha compresión, baja la calidad del sonido.

Estos protocolos o Codecs han ido evolucionando y varían en calidad de sonido, y en el ancho de banda requerido. Los equipos VoIP en general soportan múltiples protocolos.

Por ejemplo los modelos:

Cisco ATA-186 usa los codecs: G.723.1, G.711a, G.711u, G.729ª
Cisco 7960 usa los codecs: G.711a, G.711u, G.729ª

Algunos codecs requieren el pago de royalties para poder ser usados La mayoría de los equipos manejan varios CODEC. Al conectarse con otro ATA "negocian" el CODEC más avanzado que soporten ambos. En general se debe calcular que con los CODECS avanzados, para mantener una conversación con excelente calidad se debe contar con un ancho de banda de 20 a 25 kB por canal de llamada.

El ancho total requerido se calcula con la cantidad máxima de conversaciones simultáneas más un 30% de seguridad.

4.2.- VIDEO- VIGILANCIA

4.2.1 Generalidades

Los Sistemas de Seguridad y Vigilancia se están imponiendo en diversos lugares: los encontramos muy llamativos en los grandes Centros Comerciales o en los supermercados y los vemos, más sencillos o discretos, en los medianos y pequeños almacenes.

En los edificios y conjuntos residenciales es frecuente que el vigilante cuente con una cámara que le permita controlar a los usuarios y a los autos que ingresan al mismo.

En la mayoría de los casos se han venido implementando los Sistemas de Seguridad, para prevenir actos violentos y/o en algunos casos, desanimar a los violentos o maleantes en sus actos de robo, vandalismo o terrorismo. Se debe destacar que si el sistema ha sido diseñado para cumplir este objetivo, muy poco se logra si no se cuenta con un sistema de grabación o registro adecuado.

Los métodos tradicionales de grabación análoga, realizados en cintas, aunque no requieren una gran intervención del encargado de la vigilancia, son susceptibles tanto a la pérdida de la información, como a la interrupción de la grabación. El uso de cintas de mala calidad o la reutilización de ellas cuando un evento no se ha verificado aún, son incidencias lamentables que se repiten continuamente.

Los puntos citados anteriormente, unidos a la dificultad para acceder rápidamente a la información grabada en forma análoga, impiden con mucha frecuencia la identificación del culpable o maleante.

Con la tecnología digital aplicada a los Sistemas de Video-Vigilancia, la búsqueda de las imágenes se realiza en forma rápida, directa y eficiente. El medio digital que se está imponiendo con más fuerza, utiliza la herramienta que ya forma parte integral de nuestra vida cotidiana, en nuestro hogar y trabajo y es el computador.

Instalando un sencillo hardware y software especializado en el computador, se están habilitando los Sistemas de Video-Vigilancia, para que puedan ser utilizados por las áreas Administrativas y Gerenciales de la Empresa, o en los almacenes, o en sus hogares, brindándoles una eficaz herramienta de control y supervisión, que les permitirá visualizar las imágenes proyectadas por las cámaras y administrar fácilmente las opciones que les brinda el software escogido.

Los nuevos protocolos de compresión de vídeo junto con la aparición de la Banda Ancha por ADSL han hecho posible la transmisión de imágenes, a través de Internet. Esto unido a la aparición de nuevas cámaras de Vídeo IP gestionables remotamente, convierten en una solución idónea los sistemas de Vídeo Vigilancia a través de Internet.

4.2.1.1 Definición e Importancia

¿Imagina poder ver cómo la niñera cuida a su hijo en la casa o cómo lo tratan en el jardín infantil? ¿Ver qué hacen sus empleados mientras no está en la oficina? ¿Saber quién le rayó el carro en el parqueadero? ¿Apagar las luces o cerrar las puertas de su hogar desde el PC de su oficina? Todo esto es posible con un sistema de videovigilancia IP.

La Vigilancia IP Inalámbrica comprende dos tecnologías probadas, la de transmisión inalámbrica en exteriores y la de Vídeo Vigilancia en red que, combinadas crean una potente solución que representa una solución alternativa a la mayoría de los desafíos que actualmente afectan a los usuarios finales a la hora de instalar sistemas de seguridad y vigilancia: distancia, falta de infraestructura de red, condiciones climatológicas, precio y otras. La Vigilancia IP Inalámbrica representa un innovador avance pero, ¿Qué es exactamente? IP es la abreviatura de Internet Protocol, el protocolo de comunicaciones más común entre redes informáticas e Internet. Una aplicación de Vigilancia IP crea secuencias de vídeo digitalizado que se transfieren a través de una red informática permitiendo la monitorización remota allá donde llegue la red así como la visualización de imágenes y la monitorización desde cualquier localización remota a través de Internet.

Dada su escalabilidad, entre otras ventajas, la tecnología de Vigilancia IP está bien establecida no sólo para mejorar o revitalizar aplicaciones de vigilancia y monitorización remota existentes, sino también para un mayor número de aplicaciones. Y cuando se añade la potencia de la transmisión inalámbrica a la Vigilancia IP creamos incluso una solución más robusta: Un cable Ethernet (conexión de red) que puede conectar fácilmente cámaras de red a una solución de conectividad punto-a-multipunto, creando instantáneamente una WAN (red de área extensa) inalámbrica capaz de transmitir vídeo de alta resolución a una estación base en tiempo real. La combinación de la Vigilancia IP con la tecnología Inalámbrica crea una aplicación de seguridad que va más allá que cualquiera de las tecnologías disponibles y proporciona además las siguientes características:

- Fácil de desplegar

- Alto grado de funcionalidad
- Proporciona ahorros en instalación y operación
- Totalmente escalable

Funciones diversas como manipular imágenes, disminuir espacio en su almacenamiento o activación de alarmas, son solo algunas de las bondades de los programas que se ofrecen ahora en el mercado. Si el computador se utiliza en una red local (LAN), otros usuarios, con los permisos adecuados, podrán monitorear las imágenes. Si el computador o la red están conectados a Internet o a redes WAN, se podrá efectuar el monitoreo en forma remota.

Estando en un sitio de descanso, fuera de la ciudad o en un sitio muy lejano y se comprueba a través de Internet, que todo está funcionando armoniosamente en el trabajo o en el hogar, se puede continuar y hasta prolongar las vacaciones.

El computador, integrado a los Sistemas de Video-Vigilancia, está contribuyendo positivamente al desarrollo de esta tecnología. En nuevos y revolucionarios campos se están utilizando las cámaras de CCD[36]: en programas de investigación científica, en conservación y estudio de animales y en todo tipo de actividades diurnas y nocturnas, encaminadas al adecuado aprovechamiento de nuestros recursos, a la conservación animal y a la protección de las bellezas naturales, son solo algunas de las nuevas aplicaciones, derivadas todas de la utilización de los Sistemas de Video unidas al computador y de la transmisión de ellas a través de Internet, que además de enriquecernos multiplican su difusión.

4.2.1.2 Evolución de la tecnología

Los sistemas basados en la tecnología referida a las cámaras de seguridad, han venido actualmente a brindar un fuerte apoyo al tema de la seguridad integral, aludiendo entre sus virtudes ejercer una vigilancia preventiva, mediante el registro visual de sucesos. Su incorporación y aplicación en el mercado, va dirigida a asegurar un amplio espectro de ambientes y lugares, que van desde: Empresas de diversas rubros; Centros Comerciales; Supermercados; Aeropuertos; Condominios y Viviendas particulares; Vías

Públicas; Centros de Eventos; Trasporte Público; Gran Minería y Establecimientos Educacionales, entre otros. A modo de conocimiento respecto de la evolución que han experimentado estos sistemas durante el transcurso de los últimos años, podríamos catalogarlas en dos grandes eras: la análoga y la digital.

No obstante se cuenta actualmente en el mercado con los dos tipos de sistemas, la mayoría de las empresas e instituciones de variada índole aun cuentan con sistemas de seguridad basados en1 cámaras de vigilancia análoga (en muchos casos obsoletos). Sin embargo, dada la rápida evolución de las técnicas delictuales es recomendable reemplazar a la brevedad los sistemas análogos por los llamados digitales. Para obtener una mayor comprensión acerca de la evolución de los llamados sistemas digitales, con relación a sus virtudes y a las ventajas que para su seguridad representan, a continuación, se expone una breve reseña de sus progresos.

LA ERA ANÁLOGA:

Se inicia con el desarrollo de sistemas de seguridad basados en cámaras, multiplexadores, monitores de TV y VCR (Video Cassette Recorder o video grabadores VHS), nombre como se conocen, todos los que aún siguen siendo fabricados y comercializados en el mundo. A estos sistemas se les llama CCTV y su principal funcionalidad responde al monitoreo de imágenes obtenidas de las cámaras y la opcional grabación de estas en cintas VHS (Video Home System). Estos sistemas comenzaron a ser implementados en los años 50 en forma muy básica, durante los años 70 mejoraron significativamente y actualmente se han complementado con equipos tales como VCR y monitores. Dicha tecnología, se continúa usando masivamente en términos de prevención de seguridad, no obstante las notables desventajas aún están vigentes. En primer término constituyen un alto costo de mantenimiento respecto del inevitable deterioro en el tiempo con relación al recurso cintas, sin mencionar el constante reemplazo de las mismas a fin de no descontinuar las grabaciones, la alta sensibilidad a descargas magnéticas o electroestáticas, sin embargo prevalece en primera prioridad el alto costo de depender del factor humano, por cuanto constantemente se requiere de una persona que supervise los VCR, sumado a ello, la gran demanda de tiempo y la escasa posibilidad que implica contar con una grabación anterior ante un requerimiento relacionado con un evento especifico que se desee investigar.

LA ERA DIGITAL:

En los últimos 5 años, se ha potenciado el desarrollo de la tecnología DVR (Digital video Recorder), alternativa que ha venido en resolver la totalidad de los problemas presentados por el sistema análogo. Estos nuevos sistemas están principalmente basados en una plataforma computacional que permite la visualización/grabación de grupos de cámaras (en formatos de 4, 8, 16 cámaras como estándar) durante las 24 horas del día, manteniendo como característica relevante el almacenamiento digital de las imágenes obtenidas desde las cámaras en discos duros, de la misma forma en que un archivo se guarda en un PC. Esta función permite, entre otros beneficios, obtener una mayor calidad de las imágenes grabadas sin deterioro en el tiempo, grabación circular sin necesidad de reemplazar cintas (esto es, que dependiendo de la capacidad de los discos duros, se pueden almacenar varios días continuos de grabación que se van renovando en forma automática), y entre otros una fácil búsqueda automatizada de las imágenes grabadas sobre la base de fechas, horas, número de cámara, sistemas de alarmas, etc.

SISTEMAS DVR:

Características Relevantes

•Grabación seleccionada por el usuario: Continua, por calendario, activada por detección de movimiento, sensores y alarmas.

•Funcionamiento como Servidor de Cámaras: Los sistemas DVR permiten la conexión en forma remota y segura desde otros equipos con software cliente, como PC de escritorios, laptops y equipos compatibles con Pocket Pc, sobre redes Lan e Internet, tanto para la visualización de las imágenes en tiempo real y revisión de los videos grabados, como para la administración y la configuración de los DVR. A su vez, tan solo con una conexión Internet y un navegador Web como Internet Explorer, es posible realizar una conexión desde cualquier lugar del mundo para monitorear lo que está sucediendo en el lugar donde se encuentran instaladas las cámaras o buscar los registros anteriormente almacenados.

•Conexión a cámaras PTZ[72] o cámaras DOMO: Control de las características Pan-Tilt-Zoom que incluyen actualmente las cámaras modernas o profesionales, mediante el software DVR y sin necesidad de utilizar las controladoras convencionales.

•Múltiples herramientas para la búsqueda de imágenes grabadas y vastas funciones para el respaldo y exportación de estas, en medios como CD, DVD[73], etc.

•Excelente calidad de imagen en un archivo pequeño: Los actuales métodos de compresión existentes (MPEG-4[74], JPEG, etc.) permiten reducir el espacio requerido para la grabación de las imágenes, manteniendo una calidad superior a la obtenida en una grabación en cinta VHS.

•Notificaciones configurables por el usuario: Brinda la posibilidad de configurar el sistema para recibir una notificación vía e-mail o SMS cuando alguna cámara detecta movimientos o el disco duro está alcanzando un punto crítico, entre otras.

•Permiten concentrar diferentes servidores DVR en una sola estación de monitoreo.

•Alto nivel de seguridad en el acceso de usuarios al sistema.

Los sistemas DVR, por su autonomía respecto del recurso humano permiten un significativo ahorro de dinero, sumado a la fase mantenimiento, cuyo funcionamiento es autónomo y configurable de estas plataformas.

Insertos en la evolución más importante de los sistemas DVR actuales, mencionamos la extensa compatibilidad con las modernas cámaras DOMO e IP, la sólida integración con otros sistemas de control digital como por ejemplo: accesos de personas sobre la base de tarjetas magnéticas, registro de transacciones en cajas de recaudación o cajeros automáticos, etc. Estos sistemas, hoy en día, dado que acceden a elaborar algoritmos de reconocimiento digital de rostros y objetos, han brindado a sus usuarios excelentes resultados en lo que respecta a seguridad en lugares tales como: Aeropuertos;

[72] *PTZ (Pan Tilt Zoom)*
[73] *DVD Digital Video Disc)*
[74] *MPEG-4(Moving Pictures Experts Group)*

Estaciones de Trenes; Transporte Público; Zonas de tráfico común; Empresas de actividades múltiples, etc., por cuanto aportan herramientas imprescindibles para lograr un reconocimiento automatizado de delincuentes, terroristas, robos, hurtos, elementos perdidos e incluso posibles explosivos.

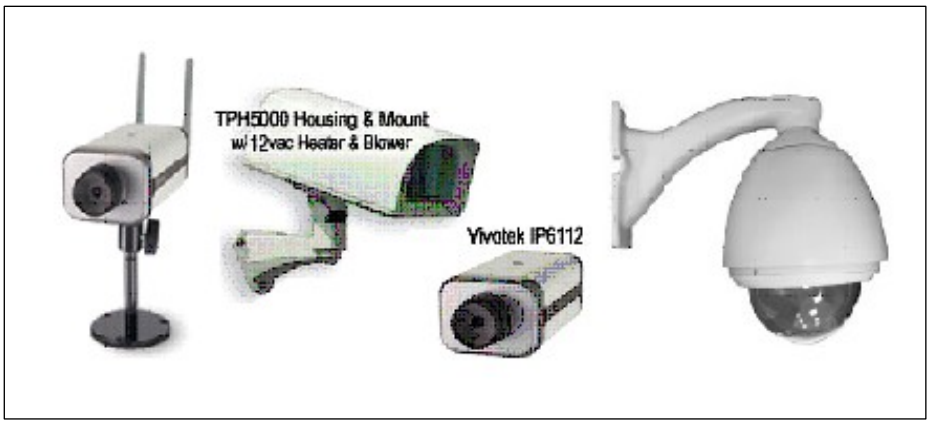


Figura. 4.10. Tipos de cámaras de videovigilancia

Los sistemas de tecnología análoga y la digital, dependen a su vez fundamentalmente del tipo de cámaras utilizadas, dispositivos que se encuentran en una diaria y constante evolución respecto del desarrollo de tecnologías más avanzadas que aporten una mejor calidad de imagen para los diferentes escenarios en donde sean utilizadas.

Con relación al tipo de cámaras a utilizar, es de vital importancia elegir la correcta que se adecue al ambiente a monitorear, en merito a que el mercado ofrece desde cámaras básicas de bajo costo, basadas en sensores CMOS con lentes incorporados, hasta sofisticados sistemas DOMO (cámaras montadas sobre bases motorizadas que permiten el movimiento horizontal y vertical), basadas en sensores CCD, con zoom óptico y digital, que incluyen visión nocturna y que soportan las mas exigentes condiciones climáticas.

4.2.2 Cámaras IP

Poder hacer seguimiento de cada una de las personas que atraviesa un punto de entrada de alta seguridad, o comprobar falsas alarmas en establecimientos desde el confort de su casa son entre muchas otras aplicaciones interesantes ahora son posibles gracias a la llegada de la tecnología de la cámara de red.

Comenzando con la primera webcam del mundo en 1991, preparada para monitorizar remotamente el nivel de café en la cafetera de la Universidad de Cambridge, el mercado y el uso de la tecnología de la cámara de red ha crecido considerablemente. Soluciones de seguridad en bancos, aeropuertos y casinos son sólo unos pocos ejemplos o aplicaciones profesionales basadas en cámaras de red, que son algo común en nuestros días.

Las cámaras son el componente esencial en todas las instalaciones de vídeo. Este dispositivo recoge la luz y la convierte en un conjunto de imágenes reconocible, que puede entonces enviarse a través de la red. Todas las cámaras generan imágenes estáticas que se envían a un visualizador con un ratio de imágenes por segundo. El ojo humano precisa aproximadamente 17 imágenes (o frames) por segundo para percibir el vídeo como en directo. La cámara en sí misma consiste en un chip que convierte la luz en señales eléctricas, y varios circuitos electrónicos como el DSP[75] (procesador digital de imágenes) entre otros.

Como se ha mencionado brevemente antes las cámaras analógicas han sido el estándar durante muchos años. De forma creciente, cada vez hay más cámaras de red instaladas.

La nueva generación de cámaras de Vídeo IP permite la transmisión de imágenes en tiempo real, así como su almacenamiento remoto y su comunicación electrónica. También pueden incorporar la tecnología WiFi, permitiéndonos su instalación en cualquier lugar sin necesidad de cableado.

4.2.2.1 Características de funcionamiento

Una cámara de red tiene su propia dirección IP y características propias de ordenador para gestionar la comunicación en la red. Todo lo que se precisa para la visualización de las imágenes a través de la red se encuentra dentro de la misma unidad. Una cámara de red puede describirse como una cámara y un ordenador combinados. Se conecta directamente a la red como cualquier otro dispositivo de red e incorpora software propio para servidor Web, servidor FTP, cliente FTP y cliente de correo electrónico.

[75] *CMOS(Complementary Metal Oxide Semiconductor)*

También incluye entradas para alarmas y salida de relé. Las cámaras de red más avanzadas también pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de vídeo analógico.

El componente cámara de la cámara de red captura la imagen, que puede ser descrita como luz de diferentes longitudes de onda, y la transforma en señales eléctricas. Estas señales son entonces convertidas del formato analógico al digital y son transferidas al componente ordenador donde la imagen se comprime y se envía a través de la red.

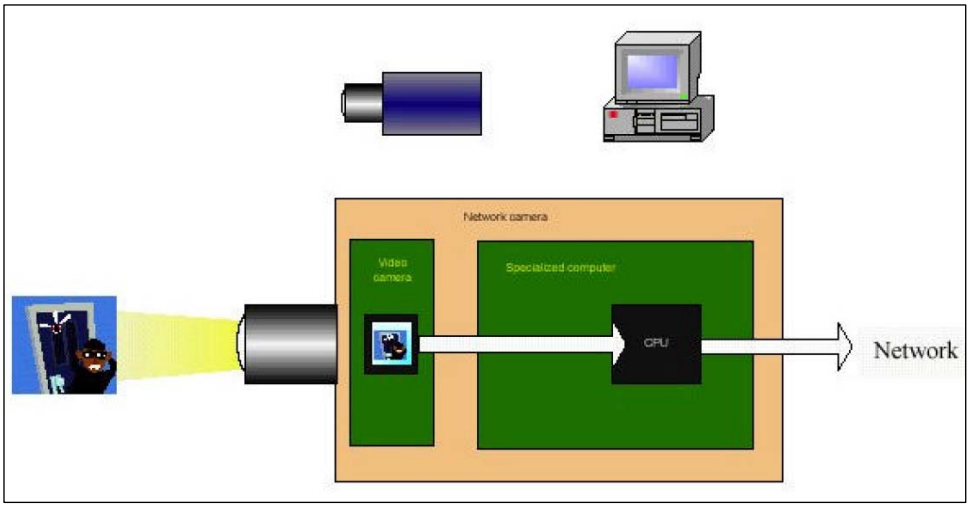


Figura. 4.11. Esquema general de funcionamiento de cámara de red

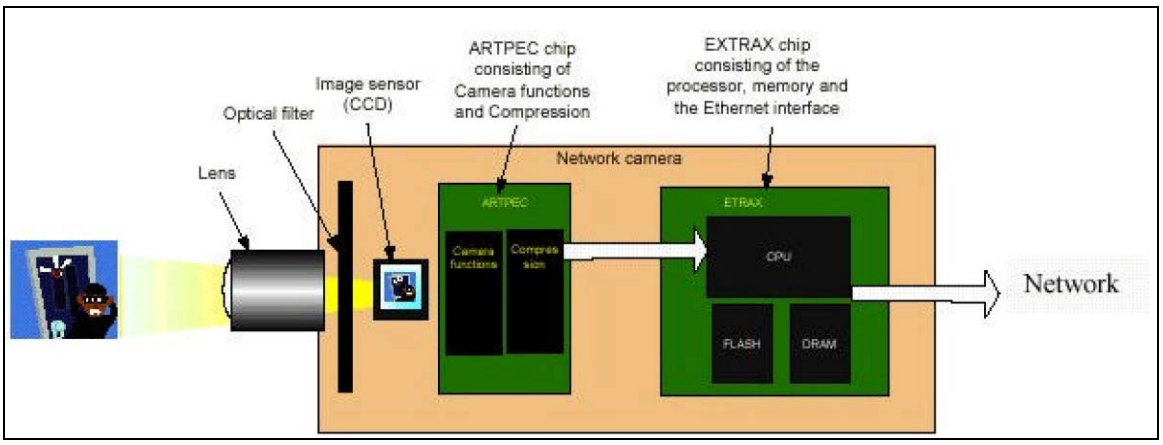


Figura. 4.12. Esquema interno de una cámara de red

La **lente** de la cámara enfoca la imagen en el **sensor de imagen** (CCD). Antes de llegar al sensor la imagen pasa por el **filtro óptico** que elimina cualquier luz infrarroja de

forma que se muestren los colores correctos. El sensor de imagen convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas señales eléctricas se encuentran ya en un formato que puede ser comprimido y transferido a través de redes.

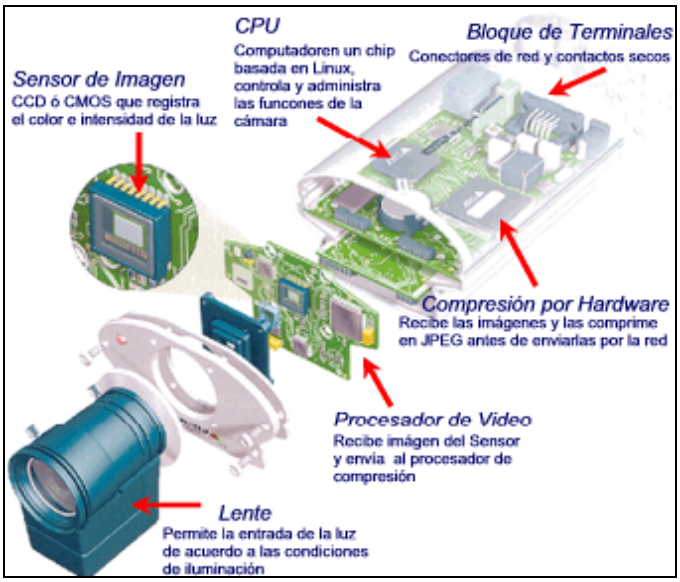


Figura. 4.13. Componentes internos de una cámara IP

Las funciones de cámara gestionan la exposición (el nivel de luz de la imagen), el equilibrio de blancos (el ajuste de los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen. Estas funciones las llevan a cabo el controlador de cámara y el chip de compresión de vídeo. La imagen digital se comprime en una imagen que contiene menos datos para permitir una transferencia más eficiente a través de la red.

La CPU, y la memoria flash y DRAM representan los “cerebros” o funciones de ordenador de la cámara y están específicamente diseñados para su aplicación en redes.

Juntos, gestionan la comunicación con la red y el servidor Web.

Es importante analizar los procesos de grabación y almacenamiento digital. En un sistema de vídeo IP hay múltiples procesos ejecutándose simultáneamente, el objeto de estudio para el caso serán relacionados con la compresión:

· **Codificación:** El proceso que se realiza en la cámara de red o el servidor de vídeo que codifica (digitaliza y comprime) la señal de vídeo analógico de manera que pueda transmitirse a través de la red.

· **Transmisión IP:** Transmisión sobre una red de datos basada en el protocolo IP, inalámbrica o con cableado, desde una fuente a hardware variado de grabación o visualizacción (por ejemplo un servidor de PC's).

· **Grabación:** Datos transferidos a discos duros estándar conectados a un dispositivo de almacenamiento como puede ser un servidor, NAS (Network Attached Server) o SAN (Storage Area Network).

· **Decodificación:** El vídeo codificado debe ser traducido, o decodificado, con el fin de ser visualizado/monitorizado. Este proceso se realiza en un PC o en otro sistema decodificador que se emplee para visualizar el vídeo.

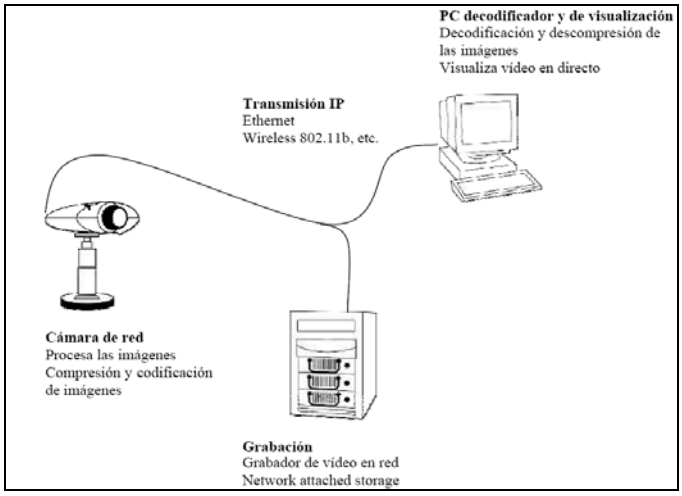


Figura. 4.14. Sistema de video en red

Técnicas de compresión

Cuando se digitaliza una secuencia de vídeo analógico cualquiera de acuerdo al estándar ITUR BT.601 (CCIR 601), se requiere un ancho de banda de 116 Mbit/segundo ó de 116 millones de bites cada segundo. Dado que la mayoría de las redes son sólo de 100 Mbit/segundo, no es posible ni deseable transmitir las secuencias de vídeo sin alguna

modificación. Para solucionar este problema se han desarrollado una serie de técnicas denominadas técnicas de compresión de vídeo e imágenes, que reducen el alto nivel de bits precisos para transmisión y almacenamiento.

La compresión de imágenes se aplica sobre una imagen individual haciendo uso de las similitudes entre píxels próximos en la imagen y de las limitaciones del sistema de visión humana. JPEG es un ejemplo de una técnica de compresión de imágenes.

La compresión de vídeo se aplica sobre series consecutivas de imágenes en una secuencia de vídeo, haciendo uso de las similitudes entre imágenes próximas. Un ejemplo de este tipo de técnicas es MPEG.

La efectividad de una técnica de compresión de imágenes viene dada por el ratio de compresión, calculado como el tamaño del fichero de la imagen original (sin comprimir) dividido por el tamaño del fichero de imagen resultante (comprimida). A mayor ratio de compresión se consume menos ancho de banda manteniendo un número de imágenes por segundo determinado. O si el ancho de banda se mantiene constante se aumenta el número de imágenes por segundo. Al mismo tiempo, un mayor nivel de compresión implica menor nivel de calidad de imagen para cada imagen individual.

Cuanto más sofisticada sea la técnica de compresión utilizada, más complejo y caro resultará el sistema. Lo que ahorre en ancho de banda y almacenamiento encarecerá los costes de latencia, codificación y complejidad del sistema. Otro factor adicional a considerar son los costes de las licencias y los honorarios asociados a un número de estándares de compresión.

Estos factores generalmente hacen que la compresión sofisticada resulte restrictiva para mantener robusto el sistema a la vez que se consiguen o mantienen bajos los costes del mismo

Tecnología de compresión

En las cámaras IP hay dos tipos de tecnología de compresión que se utilizan predominantemente: MJPEG y MPEG-4. Sin embargo, el 99% de las cámaras IP que actualmente se encuentran disponibles en el mercado se basan en la tecnología MJPEG.

MPEG-4 proporciona una calidad de vídeo mucho mejor pero, hasta hace poco, resultaba demasiado costoso poner en práctica esta tecnología para su incorporación en una cámara IP dedicada. Sin embargo, el coste, el rendimiento y el consumo de potencia del sensor de la cámara y del hardware de compresión MPEG-4 han alcanzado un punto en el que es posible integrarlo todo en las cámaras IP ahora disponibles. El precio y el rendimiento del hardware han experimentado una mejora debido a que ciertos fabricantes de vídeo IP han hecho inversiones en chips dedicados para la compresión MPEG-4.

La calidad del vídeo de estas cámaras nuevas, cuando se transmite por una red y se muestra en un monitor analógico, no puede distinguirse de un vídeo analógico conectado directamente a un monitor. Esto supone un gran avance en comparación con la discontinuidad de las imágenes de las antiguas cámaras IP de tecnología MJPEG.

No obstante, la ejecución de MPEG-4 puede presentar diferencias sustanciales. Es posible usar esta tecnología en el modo de “imagen-I exclusivamente”, que es básicamente idéntico a MJPEG pero cumple con la norma MPEG-4. En dicho caso, la cámara IP puede calificarse como MPEG-4 pero tener una calidad de vídeo similar a MJPEG.

El problema que presenta MJPEG es la necesidad de un gran ancho de banda para generar vídeo de buena calidad. Generalmente se trata de entre 10 y 30 veces más de lo que necesita una buena puesta en práctica de MPEG-4. Esto tiene un gran impacto en el ancho de banda y el almacenamiento. Tanto el suministro de la red como el coste de almacenamiento, tienen que ser al menos 10 veces mayores de lo que deberían ser.

A pesar de que las cámaras IP basadas en MJPEG generalmente son más económicas, el resto del sistema es muy costoso, lo que se traduce en un coste total del

sistema mayor que el resultante en caso de utilizar una tecnología de compresión de buena calidad

4.2.2.2 Tipos y características

Existe una gran variedad de cámaras de videovigilancia destinadas a cubrir las más diversas necesidades. Podemos encontrar cámaras para instalaciones de interior, con carcasa estanca para exterior, con infrarrojos para visión nocturna, ocultas en diferentes dispositivos, con carcasa irrompible antivandálica, con óptica intercambiable, con señal de vídeo inalámbrica o con servidor Web de vídeo incorporado para monitoreo desde Internet.

Hay cámaras que reúnen más de una característica al mismo tiempo, por ejemplo, podemos encontrar una cámara antivandálica que además tiene infrarrojos y es domo, una cámara con movimiento, zoom y visión nocturna, etc. También se puede convertir una cámara para interior en cámara para exterior añadiéndole una carcasa estanca con ventilación estándar.

Para mucha gente una cámara de red y una Webcam son lo mismo, sin embargo son dos cosas muy diferentes. Como se muestra claramente en los diagramas inferiores una cámara de red tiene su propia inteligencia y no necesita estar conectada a un ordenador para establecer una conexión a través de la red.

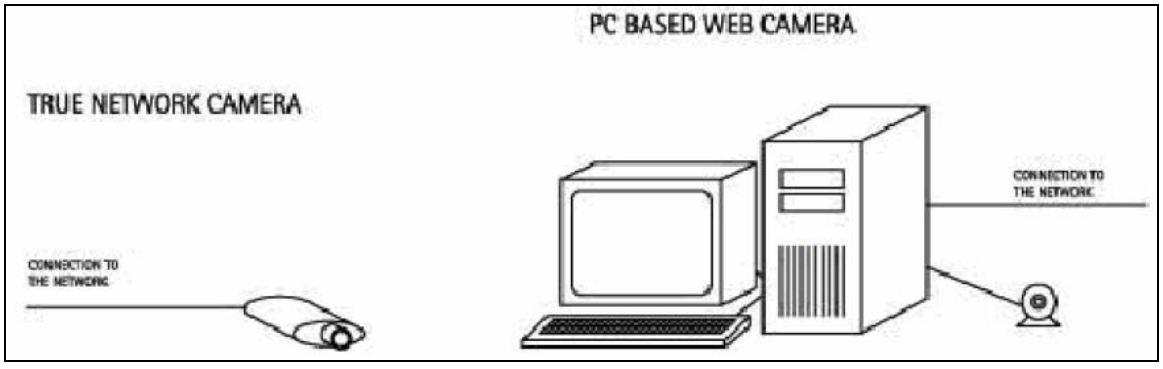


Figura. 4.15. Diferencias entre Web Cam y Cámara IP

TIPOS

Cámaras de red fijas

Una cámara de red fija proporciona una visión estática del área que está frente a la cámara. Además de la unidad de cámara se necesita una lente para que la cámara opere correctamente.

Figura. 4.16. Cámara fija

La lente ajusta la cantidad de luz que entra en la cámara, al igual que hace una cámara de fotos. La lente también enfoca la imagen en el sensor de imágenes (CCD). Antes de alcanzar el sensor, las imágenes pasan a través de un filtro óptico, que elimina cualquier luz infrarroja de manera que el color correcto sea el que se muestra. El sensor de imágenes convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas señales digitales eléctricas están ahora en un formato que pueden comprimirse y transferirse a través de la red.

Las cámaras de red proporcionan al usuario final muchos beneficios incluyendo una mayor funcionalidad respecto a las cámaras analógicas con un TCO (Coste total de propiedad) inferior. Las cámaras de red se conectan directamente a la red existente de manera que el cableado coaxial necesario para las cámaras analógicas ya no se precisa y los gastos de instalación son mínimos. Cuando existen ordenadores en el lugar ya no se precisa más equipamiento para ver las imágenes provistas por la cámara, y estas imágenes pueden visualizarse de la manera más simple desde un navegador web en el monitor de un ordenador, y de forma más compleja usando soluciones de seguridad profesionales con la ayuda de un software dedicado.

Cámaras IP domo fijas

Las cámaras domo fijas, también conocidas como mini domo, constan básicamente de una cámara fija preinstalada en una pequeña carcasa domo. La cámara puede enfocar fácilmente el punto seleccionado en cualquier dirección. La ventaja principal radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. Una de las limitaciones es que las cámaras domo fijas casi nunca disponen de objetivos intercambiables, y en caso de que ofrezcan una selección de objetivos, las posibilidades de intercambiarse se ven limitadas por el espacio en el interior de la carcasa domo

Figura. 4.17. Cámara domo fija

Cámaras con movimiento horizontal, vertical y zoom (Cámaras PTZ)

Una cámara de red PTZ básicamente combina en un único producto una cámara fija, una lente de zoom, un dispositivo que permite a usuarios remotos mover la cámara para cambiar su campo de visión y una interface de red. La cámara puede moverse tanto manual como automáticamente. En algunos casos se pueden usar lentes externas con las denominadas cámaras pan tilt (con movimiento horizontal y vertical).

Figura. 4.18. Cámara PTZ

Las cámaras PTZ se utilizan principalmente en interiores y en aquellos lugares donde resulte apropiado ver la dirección hacia la cual apunta la cámara. La mayoría de cámaras PTZ no disponen de un movimiento horizontal completo de 360 grados, y tampoco están hechas para un funcionamiento automático continuo, conocido como “recorrido protegido”. El zoom óptico oscila entre 18x y 26x.

Cámaras IP domo

Las cámaras IP domo disfrutan de las mismas ventajas que las cámaras domo fijas: son bastante discretas y, al mirar la cámara, no puede determinarse la dirección hacia la cual apunta. Una cámara IP domo, en comparación con una cámara PTZ, añade la ventaja de permitir una rotación de 360 grados. Asimismo ofrece la resistencia mecánica para un funcionamiento continuo en recorridos protegidos donde la cámara se desplaza de forma continua entre unas 10 posiciones predefinidas, un día tras otro. Con recorridos protegidos, una cámara puede abarcar una zona donde se precisarían 10 cámaras fijas para llevar a cabo el mismo trabajo. La principal desventaja es que sólo se puede supervisar una ubicación en un momento dado, dejando así las otras 9 posiciones sin supervisar. El zoom óptico oscila, normalmente, entre 18x y 30x. Sin embargo, para instalaciones en el exterior, los factores de zoom superiores a 20x resultan inadecuados debido a las vibraciones y movimientos causados por el viento.

Figura. 4.19. Cámara tipo domo

Cámaras IP PTZ no mecánicas

Con la introducción de las cámaras IP, apareció una nueva línea de cámaras PTZ, las llamadas cámaras PTZ no mecánicas. Gracias al sensor de megapíxels, la cámara puede abarcar entre 140 y 360 grados y el usuario puede obtener una visión panorámica, inclinada, alejada o de cerca con la cámara, en cualquier dirección, sin tener que realizar ningún movimiento mecánico. La ventaja primordial es que no se produce un desgaste de las piezas móviles. Ofrece además un movimiento inmediato a una nueva posición, lo que en una cámara PTZ tradicional puede tardar hasta 1 segundo. En la actualidad, las mejores cámaras PTZ no mecánicas utilizan un sensor de 3 megapíxeles. Con el fin de garantizar una buena calidad de imagen, el movimiento vertical y horizontal deberá limitarse a 140 grados y el zoom a 3x. Para un zoom o una cobertura mayor, la calidad de la imagen se verá seriamente perjudicada.

Se encuentran disponibles diversas variaciones de los tipos de cámaras descritos anteriormente, entre las que se incluyen:

•Versiones a prueba de agresiones, en función de la carcasa de protección que se use.

•Versiones resistentes a las condiciones climáticas, en función de la carcasa de protección que se use.

•Versiones de visión diurna/nocturna, lo que significa que la cámara puede cambiar automática o manualmente entre modo diurno con vídeo en color y modo nocturno con imágenes en blanco y negro en situaciones de poca luz que pueden mejorarse usando iluminadores de infrarrojos.

APLICACIONES

La tecnología de la cámara de red puede emplearse en literalmente miles de aplicaciones de valor añadido, y no necesariamente en aspectos de seguridad. Las cámaras de red proporcionan un enorme abanico de posibilidades de costo efectivo para monitoreo y vigilancia remota de personas, propiedades, lugares, activos, maquinaria y equipos, actividades turísticas, aseguramiento de bienes y personas con ayuda de información de alarmas y detectores de movimiento.

Prácticamente las posibilidades son ilimitadas y tienen la ventaja de que el video transmitido por la red puede ser consultado en cualquier lugar del mundo.

Algunas de las aplicaciones de monitoreo y vigilancia que actualmente están utilizando esta tecnología son:

- Monitoreo y vigilancia Urbana y lugares públicos.
- Monitoreo y vigilancia residencial con ó sin manejo de alarmas.
- Monitoreo y vigilancia de oficinas, fabricas y negocios.
- Monitoreo y vigilancia de escuelas y hospitales.
- Monitoreo y vigilancia de casinos.
- Monitoreo y vigilancia de Bancos, Casas de Bolsa, Aseguradoras, Casas de Cambio.
- Monitoreo y vigilancia de Obras de Construcción.

- Monitoreo y vigilancia de Museos.
- Monitoreo y vigilancia de Carreteras y vías de comunicación.
- Monitoreo y vigilancia de Equipo y Maquinaria.
- Monitoreo y vigilancia de enfermos, niños, ancianos y mascotas.

Estos son solo algunos ejemplos del uso actual pero en realidad las posibilidades de vigilancia y monitoreo son ilimitadas.

VENTAJAS

Frente a otros dispositivos

Existen una gran cantidad de ventajas a favor de una cámara de red cuando se compara ya sea con una cámara web basada en PC ó con una cámara de tecnología antigua como son las cámaras análogas.

En lo que se refiere a un Circuito Cerrado de Televisión, una cámara IP te aporta grandes ventajas:

• Posibilidad de acceso desde cualquier sitio del mundo. Un CCTV es, como su nombre indica, "cerrado", por ello hay que estar en el lugar del CCTV para poder ver las imágenes.

• Es más barato. Instalar cámaras IP es muy sencillo ya que es como instalar una red local LAN o conectarla directamente al Router (inalámbrico o con cables, existen ambas opciones). No se necesita las complicadas y caras instalaciones de CCTV.

• Ampliable. Es muy sencillo añadir más cámaras IP a un sistema, mientras que en un CCTV necesitamos duplicar sistemas de monitorización durante la ampliación del sistema.

Como dispositivo en si.

En primer lugar se puede mencionar que una cámara de red es una unidad independiente no requiere de ningún otro dispositivo ó computadora para la captura y

transmisión de imagen, que cuenta con su propio servidor web incluido que realiza todo este trabajo, lo único que se requiere es una conexión de red Ethernet estándar.

También una cámara de red tiene las siguientes ventajas:

Flexibilidad - Se puede conectar en cualquier lugar y se pueden utilizar dispositivos como módems, celulares, adaptadores inalámbricos ó la misma red cableada como medio de transmisión.

Funcionalidad - Todo lo que se necesita para transmitir video sobre la red esta incluido en la cámara.

Instalación - Solo se requiere asignar la IP para empezar a transmitir video.

Facilidad de Uso - Se puede administrar y ver el video en una computadora estándar con un navegador de internet.

Estabilidad - Ya que no requiere de componentes adicionales, se tienen una mayor estabilidad-

Calidad - Proporcionan imágenes de alta calidad en formato MJPEG ó MPEG4.

Costo - El costo es muy bajo ya que el costo total para transmitir video es el de la cámara

4.2.2.3 Criterios de selección de equipos

Existen varios parámetros muy importantes a considerar al momento de elegir el dispositivo a ser usado para video vigilancia dentro de una red inalámbrica. La calidad de la imagen es, evidentemente, una de las características más importantes de cualquier cámara, si no la más importante. Esto es doblemente cierto en las aplicaciones de vigilancia y supervisión, en las que puede haber vidas y bienes en juego.

Factores determinantes

A diferencia de las cámaras analógicas tradicionales, las cámaras de red no sólo disponen de capacidad de procesamiento para tomar y presentar las imágenes, sino también para administrar digitalmente el vídeo y comprimirlo para su transporte a través de la red.

Existe un lógico compromiso entre el nivel de compresión y la calidad de la imagen, pero, aún así, la calidad de la imagen puede variar considerablemente según la óptica y el sensor de imagen elegidos, la capacidad de procesamiento disponible y el nivel de complejidad de los algoritmos. En síntesis, es necesario tener en cuenta los siguientes factores:

- El tipo de sensor de imagen
- El rendimiento de la cámara en condiciones de iluminación escasa
- La posibilidad de sustituir y elegir la lente
- La resolución de la imagen
- Las necesidades de tamaño de archivo y de ancho de banda
- El tratamiento adicional de la imagen, como por ejemplo el balance de blancos, la compensación de centelleo, el aumento de la definición, etc.

Desde el nacimiento de las cámaras de red, ha proliferado la introducción tecnologías y patentes para mejorar la calidad de la imagen. Desde el punto de vista técnico, la superioridad de la calidad de imagen, al momento de la elección de una cámara IP, se apoya en tres pilares:

- Procesamiento de señal, algoritmos de mejora de la imagen y tecnología de compresión de vídeo avanzados

- Microprocesadores de procesamiento de la imagen y de red de vídeo diseñados a la medida del cliente

- Cuidada selección y combinación de los sensores de imagen y lentes más recientes y de mejor calidad.

Uso del ancho de banda

Otro factor importante al momento de elegir corresponde al ancho de banda, el utilizado por los productos de vigilancia IP depende de la configuración de éstos. Por ejemplo, el uso de ancho de banda de una cámara depende de factores tales como:

- El tamaño de la imagen
- La compresión
- La frecuencia de imagen (fotogramas por segundo)
- La complejidad de la imagen

Hay muchas formas de aprovechar al máximo el sistema de vigilancia IP y administrar el consumo de ancho de banda, entre ellas se incluyen las siguientes técnicas:

- **Conmutación de redes:** Mediante la conmutación de redes, una técnica de conexión utilizada con frecuencia hoy en día, puede dividirse un ordenador y una red de vigilancia IP físicos en dos redes lógicas autónomas. Las redes siguen conectadas físicamente, pero el conmutador de red las divide lógicamente en dos redes virtuales independientes.

- **Redes más rápidas:** El precio de los conmutadores y enrutadores baja constantemente, por lo que las redes con capacidad para gigabytes son cada día más asequibles. Al reducir el efecto de la limitación del ancho de banda, las redes más rápidas aumentan el valor potencial de la vigilancia remota sobre red.

- **Frecuencia de imagen condicionada a sucesos:** En la mayoría de las aplicaciones no es necesario disponer de 30 imágenes por segundo (ips) en todo momento en todas las cámaras. Las posibilidades de configuración y los sistemas inteligentes incorporados a las cámaras de red o el servidor de vídeo permiten establecer frecuencias de imagen menores (por ejemplo, 1-3 ips), reduciendo drásticamente el consumo de ancho de banda. En caso de alarma, si está activada la detección de movimiento, la frecuencia de imagen de la grabación puede aumentarse automáticamente hasta un nivel superior.

En la mayoría de los casos, la cámara sólo enviará vídeo a través de la red si merece la pena grabar las imágenes, lo que por regla general únicamente supone el 10% del tiempo. El 90% restante no se transmite nada a través de la red.

4.2.2.4 Configuración

Figura 4.20 Tipos de configuración de cámaras IP

Dependiendo del tipo de aplicación que vaya a tener la cámara se determina su configuración.

La cámara IP se puede conectar a una LAN/Intranet y a Internet. Se selecciona una de los cuatro tipos de configuración de la cámara IP. Los parámetros de red difieren según el tipo de configuración de la cámara IP. La cámara IP se puede instalar en la LAN/Intranet.

Dentro de las 4 tipos de configuración existen los detallados a continuación**:**

Conexión LAN/Intranet

La cámara corresponde a un nodo más dentro de la red, mediante el puerto Ethernet se conecta a un switch colocado con la finalidad de hacer más fluido el tráfico de red. Es la configuración más utilizada, brinda funcionalidades como: acceso para visualización de la imagen tanto para los usuarios de la red lan o wlan a la que pertenece la cámara como

mediante un navegador de internet desde cualquier parte del mundo estableciendo los permisos de puertos acordes al caso.

Conexión a Internet con un Router de banda ancha

Para esta configuración se requiere un Módem Router conectado directamente a la cámara IP, se la puede instalar independientemente sin PC en la red.

Conexión directa a Internet con un módem

La mayoría de los servicios xDSL utilizan PPPo. En su gran mayoría, las cámaras IP no son compatibles con PPPoE. Si la conexión a Internet precisa de PPPoE, se puede conectar mediante el Router compatible con PPPoE.

Conexión directa con un PC

Para aplicaciones de pruebas o fines limitados, existe la posibilidad de conectar una cámara IP mediante un cable cruzado a una PC. Basta con colocarlas en la misma red para visualizar la imagen.

Finalmente de manera general para poder configurar una cámara IP se requiere hacer una conexión cableada entre esta y una PC y mediante un browser ingresar a la configuración de la cámara y establecer datos básicos como dirección IP, intervalos de grabación, programación de horarios de grabación, captura de imágenes, calidad de la imagen.

CAPÍTULO 5

DISEÑO

5.1 DISEÑO DE LA INTRANET

5.1.1 Demanda en la institución educativa

La unidad educativa Liceo del Valle ante el vertiginoso crecimiento de la ciencia y tecnología ha tomado la decisión de implementar soluciones que vayan de acuerdo a dicho crecimiento.

En este sentido, la institución educativa ha concluido realizar la contratación de servicios outsourcing para el diseño e implementación de la solución tecnológica completa la cual comprende cableado estructurado, red inalámbrica, servidor de aplicaciones, video vigilancia y VoIP.

El Liceo del Valle para este efecto ha decidido contratar los servicios de la empresa Enlace Digital para el desarrollo y la puesta a punto de la solución planteada.

En el capítulo 1 se hizo referencia de la infraestructura tecnológica de la institución a manera de censo de usuarios que van a acceder al servicio, tomando en cuanta el número de computadores instalados, sistema operativo que poseen y su ubicación.

Teniendo en cuenta estos datos como partida se verá en fases posteriores la cantidad de equipos de red necesaria para interconectar a los usuarios y el tipo de tecnología además requerida para el fin, sin dejar a un lado un dimensionamiento de equipos y servicios en general para un incremento de la demanda de usuarios en un futuro.

Actualmente, en conjunto, la parte administrativa, primaria, secundaria y preescolar cuenta con 50 computadores; para lo cual se debe realizar el respectivo dimensionamiento en lo referente a equipos inalámbricos, ancho de banda a contratarse, entre otros.

Así mismo se deben hacer los estudios necesarios en cuanto a cobertura de la red inalámbrica, de tal manera que se tenga servicio de conectividad wireless a lo largo de todo el campus de la institución educativa.

Estos y otros aspectos que requieren mayor profundidad y que serán explicados a lo largo de este capítulo tienen referencia con el diseño de la solución tecnológica planteada.

5.1.2 Análisis de planos

La institución educativa Liceo del Valle actualmente se encuentra asentada en un terreno cuya extensión total es de 43192 m^2

Por otra parte el área física de construcción aproximada sobre la cual se encuentran funcionando todas sus dependencias (administración, primaria, secundaria, preescolar, artes y uso múltiple) es de 4000 m^2

En el capítulo 1 se analizó la infraestructura física del Liceo, para poder tomar en cuenta distancias, facilidades como accesibilidad y electricidad para la colocación de equipos, los planos del área en el cual se va a implementar un servicio de red sirve para decidir aspectos de interconexión, necesidad de cableado estructurado o de una red inalámbrica.

Para nuestro caso, las áreas de construcción, entre ellas, se encuentran separadas una distancia promedio de 30 metros, por lo que se ha decidido usar tecnología inalámbrica para tener cobertura de red en las áreas de primaria, secundaria, preescolar y uso múltiple, alejadas del área principal del Liceo, y costoso en cuanto a la opción de tendido de cableado estructurado se refiere.

Más adelante mediante software especializado se dará mayor uso a los planos proporcionados, realizando en base a ellos cálculos de distancias, interferencia y posibles pérdidas de señal se refiere.

5.1.3 Obstáculos e interferencias para transmitir

Dentro del alcance de una red inalámbrica es importante para su dimensionamiento, tomar en cuenta las condiciones de la infraestructura del lugar, que puedan afectar en la transmisión de las señales, convirtiéndose en obstáculos para un óptimo desempeño de los equipos.

Debido a la naturaleza de la tecnología de radio, las señales de radio frecuencia pueden desvanecerse o bloquearse por materiales medioambientales. La inspección in situ ayudar a identificar los elementos que afecten negativamente a la señal inalámbrica.

Tabla. 5.1. Tabla de interferencias acorde al material

Material	Ejemplo	Interferencia
Madera	Tabiques	Baja
Vidrio	Ventanas	Baja
Amianto	Techos	Baja
Yeso	Paredes interiores	Baja
Ladrillo	Paredes interiores y exteriores	Media
Hojas	Arboles y plantas	Media
Agua	Lluvia / Nebla	Alta
Cerámica	Tejas	Alta
Papel	Rollos de papel	Alta
Vidrio con alto contenido en plomo	Ventanas	Alta
Metal	Vigas, armarios	**Muy Alta**

Debido a que las redes inalámbricas operan en un espectro de frecuencias utilizado por otras tecnologías, pueden existir interferencias que pueden afectar negativamente al rendimiento

Es importante tomar además en cuenta que la presencia de otro tipo de tecnologías pueden interferir en la transferencia de las señales Las tecnologías que pueden producir interferencias son las siguientes:

- Bluetooth
- Hornos Microondas
- Algunos teléfonos DECT inalámbricos
- Otras redes WLAN

Pérdida de señal WIFI, interferencia y obstáculos

Las ondas de RF transmitidas por las redes inalámbricas WIFI son atenuadas e interferidas por diversos obstáculos y "ruidos". Al transmitir energía, esta es absorbida y reducida.

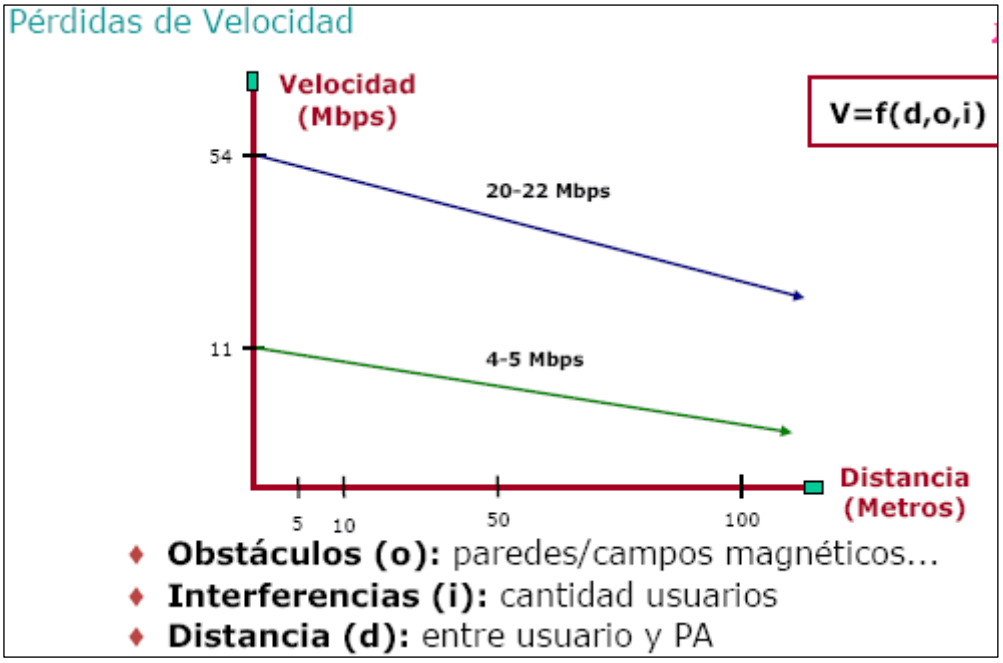


Figura. 5. 1 Gráfico perdida velocidad vs. distancia

En la figura 5.1 se puede observar un gráfico donde se muestra como en las redes inalámbricas WIFI van decreciendo las velocidades de transmisión a medida que incrementa la distancia al Punto de Acceso Inalámbrico**.** Esto se debe a que paredes y transmisiones de otros equipos van atenuando la señal.

Como se ve en la figura 5.1**,** las velocidades promedio del estándar 802.11b son de 4-5 Mbps y no de 11 Mbps como se suele creer. De la misma manera, las velocidades promedio del estándar Wifi 802.11g son 20-22 Mbps y no 54 Mbps.

En la figura 5.1 se muestra también un recuadro con una función que conviene recordar: La velocidad de transmisión de una red inalámbrica Wifi, será función de la distancia, los obstáculos y las interferencias.

Factores de atenuación e interferencia

Los factores de atenuación e interferencia de una red inalámbrica WIFI 802.11b o 802.11g son:

- Tipo de construcción
- Micro-ondas
- Teléfonos fijos inalámbricos
- Dispositivos Bluetooth
- Elementos metálicos como escaleras de emergencia y armarios
- Peceras
- Humedad ambiente
- Tráfico de personas

Hay que aclarar que la lista anterior es válida para el estándar wifi 802.11b y el estándar wifi 802.11g. En cuanto al estándar wifi 802.11a, si bien el concepto teórico de obstáculos e interferencias es similar, en la práctica existen varias diferencias, que en general son ventajas. Como se explicó esta tecnología utiliza una banda de frecuencia superior a 5 GHz que aún está muy poco "poblada" o utilizada. Por ejemplo, las interferencias de Micro-ondas, Dispositivos Bluetooth y Teléfonos fijos Inalámbricos, aquí

no existen y por lo tanto es más fácil estabilizar una red inalámbrica wifi que se base en el estándar wifi 802.11a.

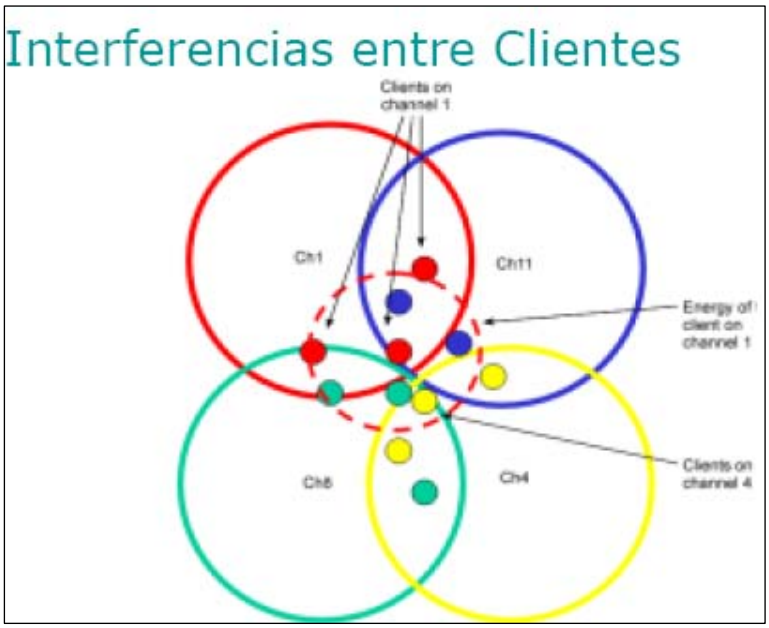


Figura. 5.2. Interferencia entre clientes acorde al canal que ocupan

En la figura 5.2 se ve un ejemplo de cómo pueden producirse las interferencias entre clientes de una red inalámbrica WIFI. Las ondas de RF de los clientes rojos que están transmitiendo en canal 1 se propagan también hacia donde están estaciones móviles que están asociadas a otros Access Point (el amarillo, el verde y el azul). Una situación que se puede dar, por ejemplo, es que un cliente "rojo" intente transmitir, para lo cual enviará un RTS y si el canal está libre recibirá un CTS. Ese CTS, va dirigido a todos los clientes "rojos". Si algún cliente de "otro color" capta el CTS, se quedará callado durante el Slot Time, lo que representa una ineficiencia y pérdida de tiempo en el sistema, que si se repite mucho, generará una pobre calidad de servicio de dicha red inalámbrica WIFI.

Análisis de obstáculos e interferencia para la Intranet del Liceo del Valle

Como fue mostrado en los planos, los materiales que pueden intervenir en la transmisión óptima de los datos son las paredes que separan las antenas wireless de las PCs y las antenas de los Access Point, por tanto, los materiales a consideran son ladrillo, bloque y cemento.

Para la colocación adecuada de los Access Point es necesario tomar en cuenta que la directividad de las antenas sea la más alta posible y que la ganancia de las antenas sea la suficiente para tener un buen nivel de la señal.

Se ha tomado algunos softwars para el diseño de la WLAN, y la colocación de los elementos activos. Para nuestro caso la pérdida por los materiales que intervienen en la transmisión de las señales sería:

- Ventana (metal), pérdida 5-8dB
- Pared 10 cm espesor, pérdida 10 dB
- Hormigón, pérdida 20-25 dB

Al tratarse de una construcción escolar que consta de aulas, construcciones de hormigón, ventanas de vidrio, puertas de madera, techo de acero y cemento, dentro de la siguiente tabla se puede encontrar las pérdidas promedio ocasionadas por dichas estructuras, aspecto importante a tomar en cuenta para el direccionamiento de las antenas a usarse en los access point y la potencia en dB requerida para optimizar la red:

Tabla. 5.2. Pérdidas promedio acorde a infraestructura

Material	Pérdida adicional (db)	Rango efectivo
Espacio en abierto	0	100%
Ventana (no metal)	3	70%
Ventana (metal)	5-8	50%
Pared 5 cm espesor	5-8	50%
Pared 10 cm espesor	10	30%
Pared +10 cm espesor	15-20	15%
Hormigón	20-25	10%
Techo/suelo	15-20	15%
Techo/suelo (amplio)	20-25	10%

5.1.4 Ubicación del MDF

Para el diseño de una red mixta, como es el caso, es necesario el diseño de la parte cableada de la red. Para ello es necesario el diseño de los armarios de cableado MDF e IDF.

Topología de red

El tipo de topología escogida para la LAN cableada es tipo estrella ya que todas las computadoras convergen a un punto central correspondiente a un switch, escogido por su funcionalidad, número de puertos y características que presenta. La topología estrella en una red LAN cableada permite mantener a los demás usuarios en red si uno de ellos pierde la conexión, y permite añadir de manera sencilla un nuevo usuario.

Requerimientos de tráfico de la red

- Administración

Está ubicada en el edificio principal de las instalaciones, consta de las siguientes dependencias: Vicerrectorado, Sala de reuniones, Rectorado, Secretaría General, Archivo, Sala de espera, Recepción, Administración, Contabilidad, Oficina de servicios, Sala de Profesores y personal, Sistemas, Charlas con Padres de Familia, y Aula de Computación.

En estas dependencias tenemos la mayor concentración de demanda de servicio ya que 39 de los 50 usuarios se encuentran es este edificio, con alto tráfico de red, consultas frecuentes al servidor y accesos frecuentes a Internet con valores picos de 0.80 Mbps.

- Primaria

Está ubicada en una edificación del mismo nombre, consta de las siguientes dependencias: 6 aulas con capacidad para estudiantes, Sala de video, 2 Oficina de Profesores, 2 Dependencias de Psicología.

En estas dependencias no existe mayor demanda de servicio ya que 3de los 50 usuarios se encuentran es este edificio, con bajo tráfico de red, consultas medias al servidor y accesos frecuentes a Internet con valores picos de 0.25 Mbps.

- Secundaria

Está ubicada en una edificación del mismo nombre, consta de las siguientes dependencias: Vicerrectorado, 12 aulas con capacidad para 20 estudiantes, 2 aulas con capacidad para 9 personas, Departamento médico, Sala de Video, Sala de inglés, Sala de Profesores, Departamento de Inspección.

En estas dependencias no existe mayor demanda de servicio ya que 7 de los 50 usuarios se encuentran es este edificio, con bajo tráfico de red, consultas medias al servidor y accesos frecuentes a Internet con valores picos de 0.35 Mbps.

- Preescolar

Está ubicada en una edificación del mismo nombre, consta de las siguientes dependencias: Oficina, Guardería, 2 Aulas Primer Grado, Aula Kinder, Expresión Corporal.

En estas dependencias no existe casi demanda de servicio ya que 1 de los 50 usuarios se encuentran es este edificio, con escaso tráfico de red, consultas esporádicas al servidor y accesos esporádicos a Internet.

Requerimientos de seguridad en la red

La Institución Educativa desea que se establezcan reglas de seguridad particularmente en el departamento de Administración. También se desea establecer políticas de seguridad en los accesos a la red pública (Internet), en cuanto a la red cableada se refiere.

De esta manera resultaría óptimo establecer un firewall en el servidor que permita realizar este control, es decir examinar todo el trafico de entrada y salida de la red permitiendo solamente el paso del tráfico autorizado.

Diseño lógico de la red

El edificio principal del Liceo del Valle corresponde a las instalaciones de administración, las demás dependencias que son: primaria, secundaria, preescolar y aula de uso múltiple están alejadas relativamente de administración y entre sí.

Teniendo en cuenta esta disposición física de las distintas dependencias y los requerimientos de tráfico y seguridad vistos anteriormente se decidió desarrollar cableada la parte de administración para asegurar el servicio a los usuarios y para dirigir los servicios al resto de la red, se colocará access points, de manera que nuestra red será mixta:

cableada en administración e inalámbrica en primaria, secundaria, preescolar y aula de uso múltiple.

Colocación del MDF

De acuerdo con este criterio es necesaria la colocación de una unidad de distribución principal (MDF), donde se aloje el núcleo o backbone de la red.

El MDF es la instalación principal de distribución principal, se puede decir que es el recinto de comunicación primaria de un edificio, el punto central de una topología de networking en estrella, donde están ubicados los paneles de conexión, y en este caso el switch.

Se decidió colocar dicho MDF en el edificio de administración, ya que luego del análisis previamente realizado la mayor cantidad de tráfico de la red se encuentra en esta dependencia y corresponde a la parte cableada de la red.

5.1.5 Herramientas de diseño:

5.1.5.1 Software WirelessMon

WirelessMon es un programa que permite a los usuarios monitorear el status de uno o varios adaptadores WiFi y obtener información acerca de puntos de acceso y hot spots cercanos en tiempo real. También se puede almacenar la información recopilada en un archivo, el cual provee imágenes con el nivel de las señales además de estadísticas 802.11 WiFi.

También, posee muestra gráfica de resultados, que recoge el uso on line de los distintos canales de radio. Se usa para elegir uno que no esté saturado. Se puede crear mapas de puntos de acceso, vía GPS o de forma manual.

Por último, gracias esta herramienta se puede consultar gran cantidad de información relacionada con la conexión, desde el tráfico de datos, hasta la direcciones MAC de los distintos puntos de acceso, etcétera.

Cualquier adaptador Wireless que cumpla con el estándar NDIS_802.11 podrá reportar información a WirelessMon. El programa ha sido diseñado para Windows 2000 (Service pack 4 en adelante), XP y 2003.

Pantallas capturadas por Wirelesmon

Figura. 5.3 AP-Administración, Señal más óptima

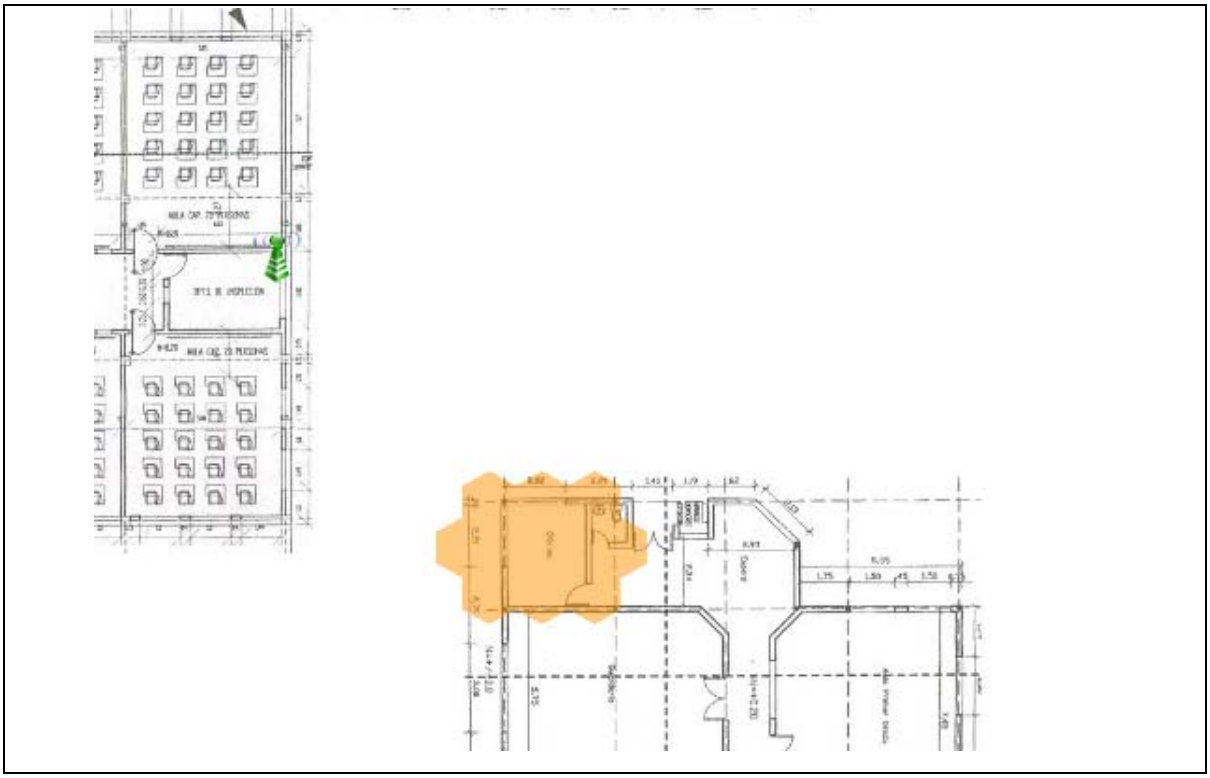


Figura. 5.4. AP-Preescolar, señal más óptima

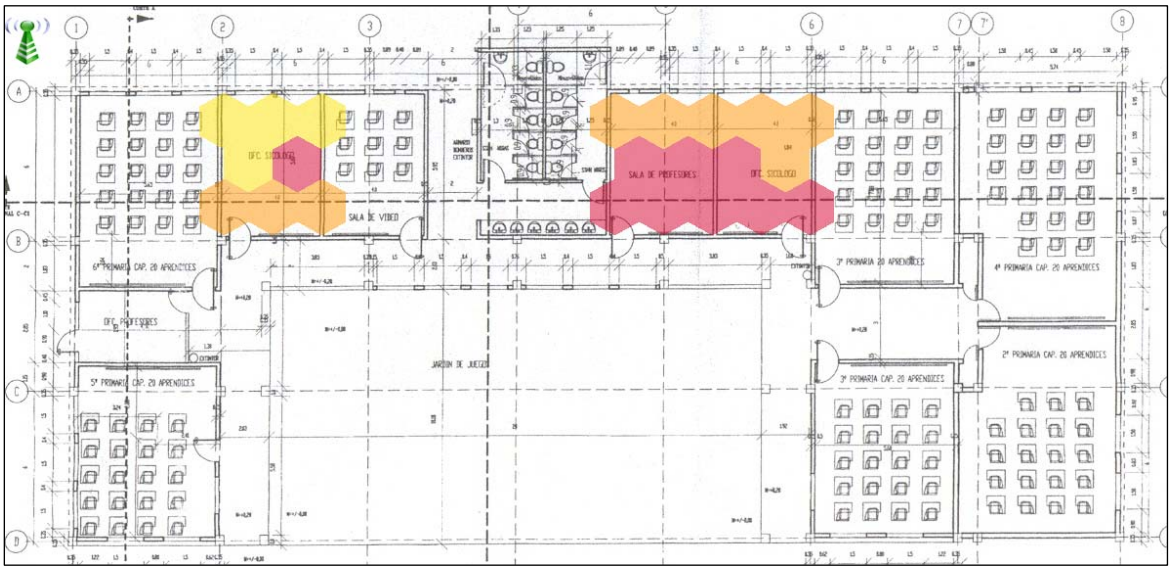


Figura. 5.5. AP-Administración, señal más óptima con cobertura en primaria.

Figura. 5.6. AP-Primaria, señal más óptima

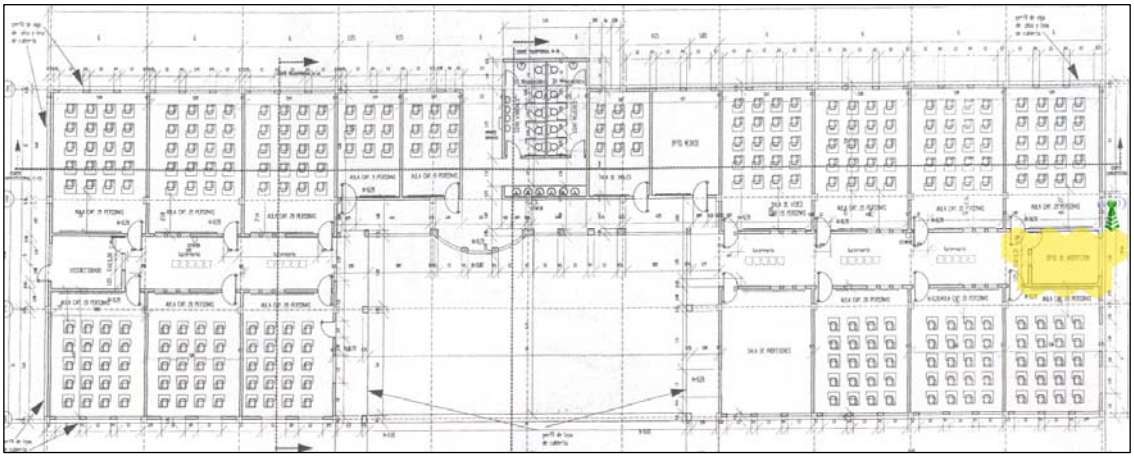


Figura. 5.7. AP-Secundaria, señal más óptima con cobertura en inspección

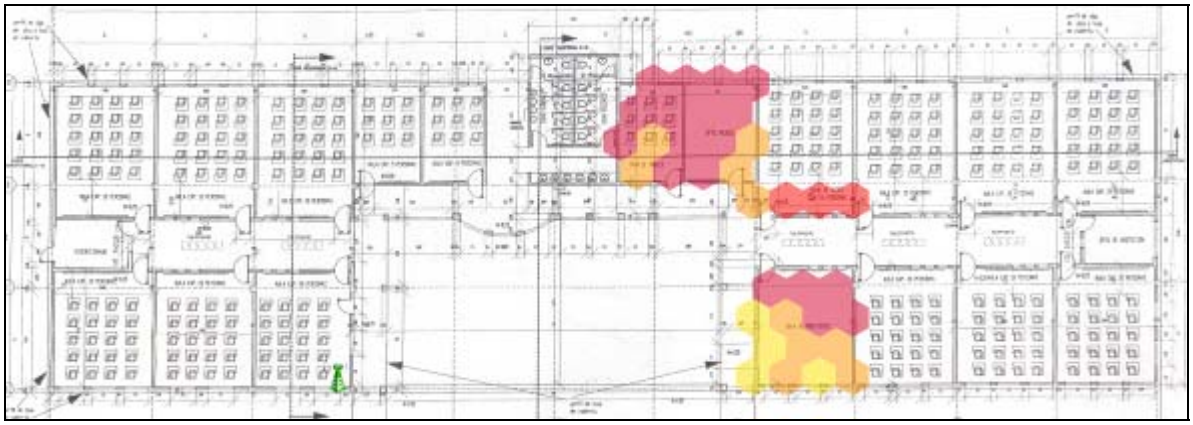


Figura. 5.8. AP-Secundaria, señal más óptima con cobertura en sala de profesores

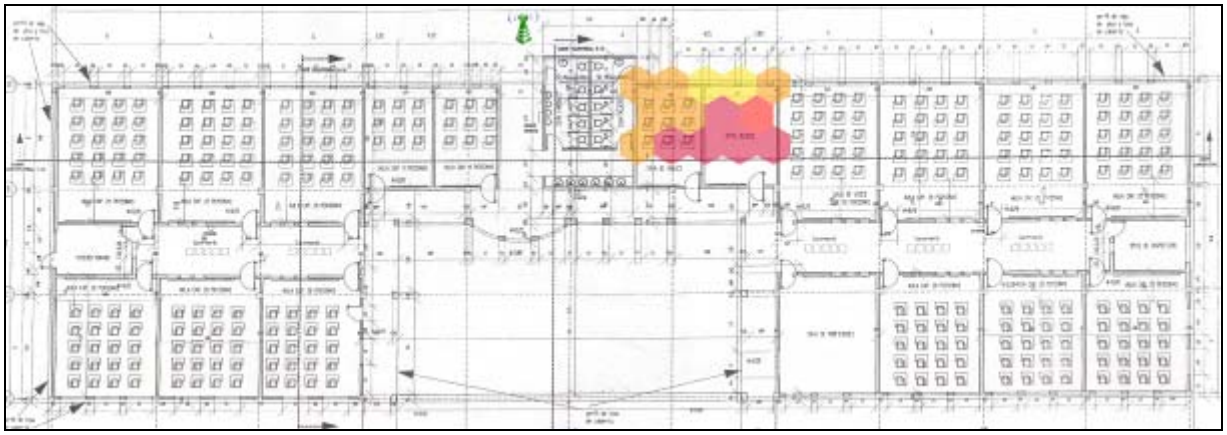


Figura. 5.9. AP-Secundaria, señal más óptima con cobertura en sala de profesores

5.1.5.2 Software NetStumbler

Además del software WirelessMon, indicado anteriormente, se usó el software Netstumbler con el fin de verificar una buena calidad de cobertura de los access point dentro de la red y el área a dar el servicio.

Netstumbler es un programa para Windows que permite detectar WLANs usando tarjetas wireless 802.11a, 802.11b y 802.11g. Tiene varios usos, como:

1.- Verificar que la red está bien configurada.
2.- Estudiar la cobertura o señal que se tiene en diferentes puntos de domicilio de la red.
3.- Detectar otras redes que pueden causar interferencias a la que es objeto de análisis.
4.- Es muy útil para orientar antenas direccionales cuando se quiere hacer enlaces de larga distancia, o simplemente para colocar la antena o tarjeta en el punto con mejor calidad de la señal.
5.- Sirve para detectar puntos de acceso no autorizados (Rogue AP's).
6.- Por último, también sirve para WarDriving, es decir, detectar todos los APs que están alrededor.

Y si se cuenta con GPS, permite no solo detectar sino también localizar los APs.

Esta herramienta sirve para controlar y administrar redes Wifi, por lo que no servirá para abrir redes que estén protegidas. NetStumbler muestra si la red está bien configurada comprobando la cobertura de la señal en diferentes emplazamientos.

A continuación se muestran las pantallas capturadas correspondientes a los AP en la red del Liceo del Valle, acorde a la ubicación correspondiente.

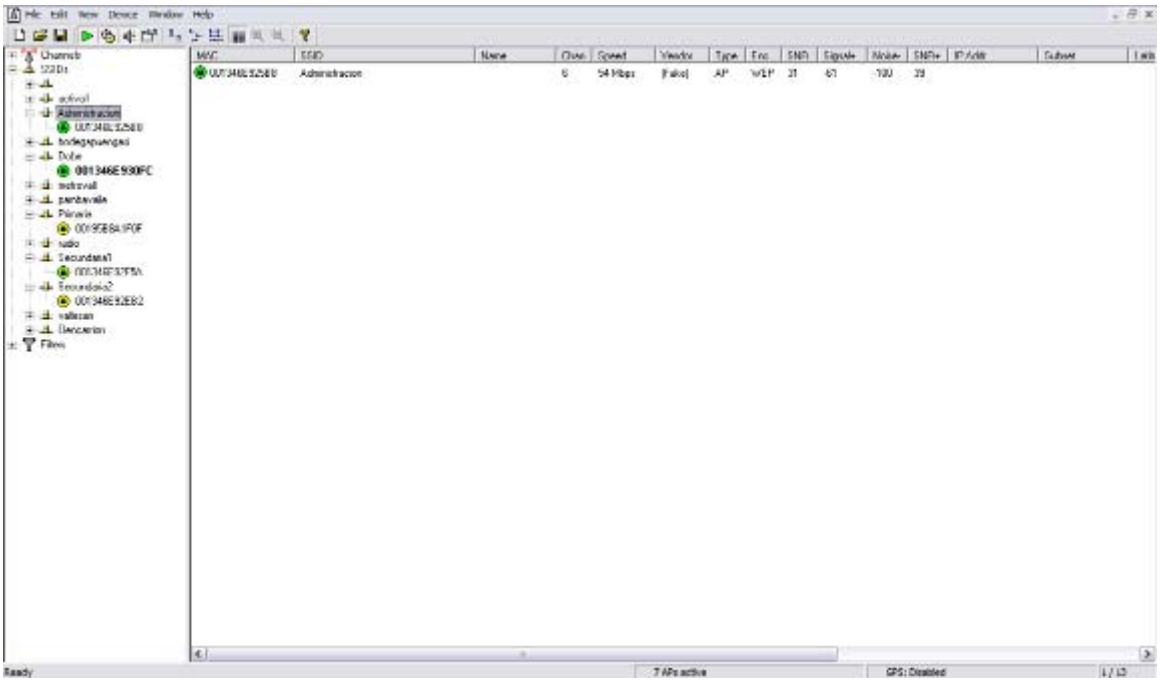


Figura. 5.10. Análisis AP-Administración en Software Netstumbler

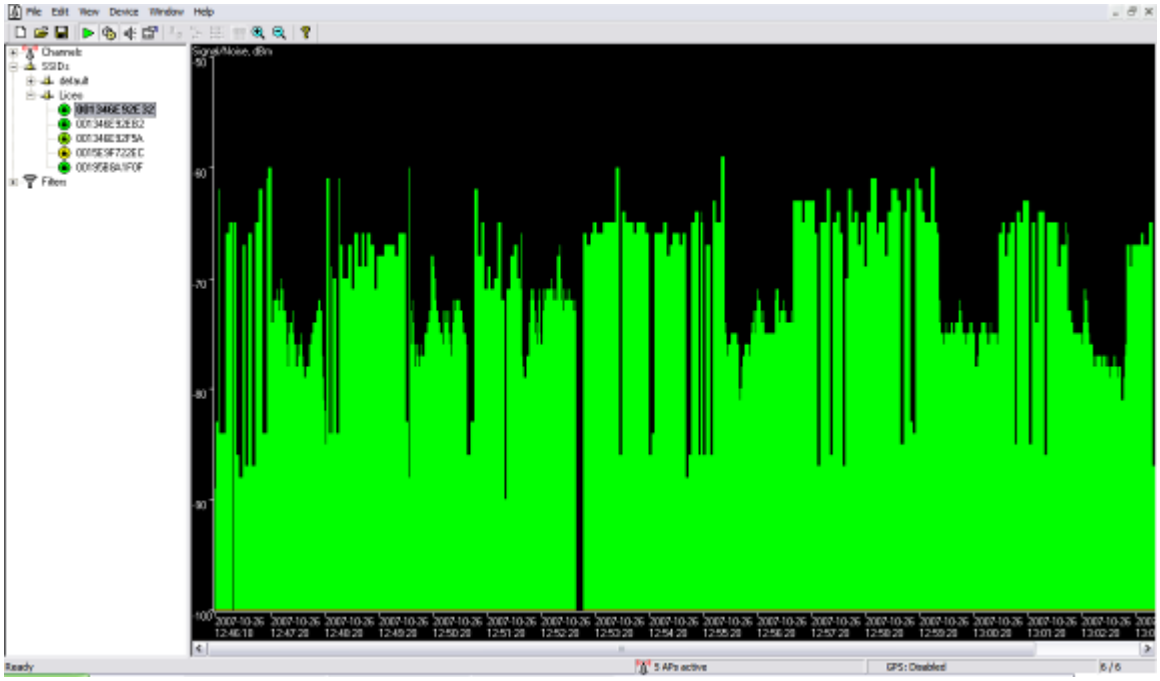


Figura. 5.11. Relación señal-ruido, AP-Netstumbler

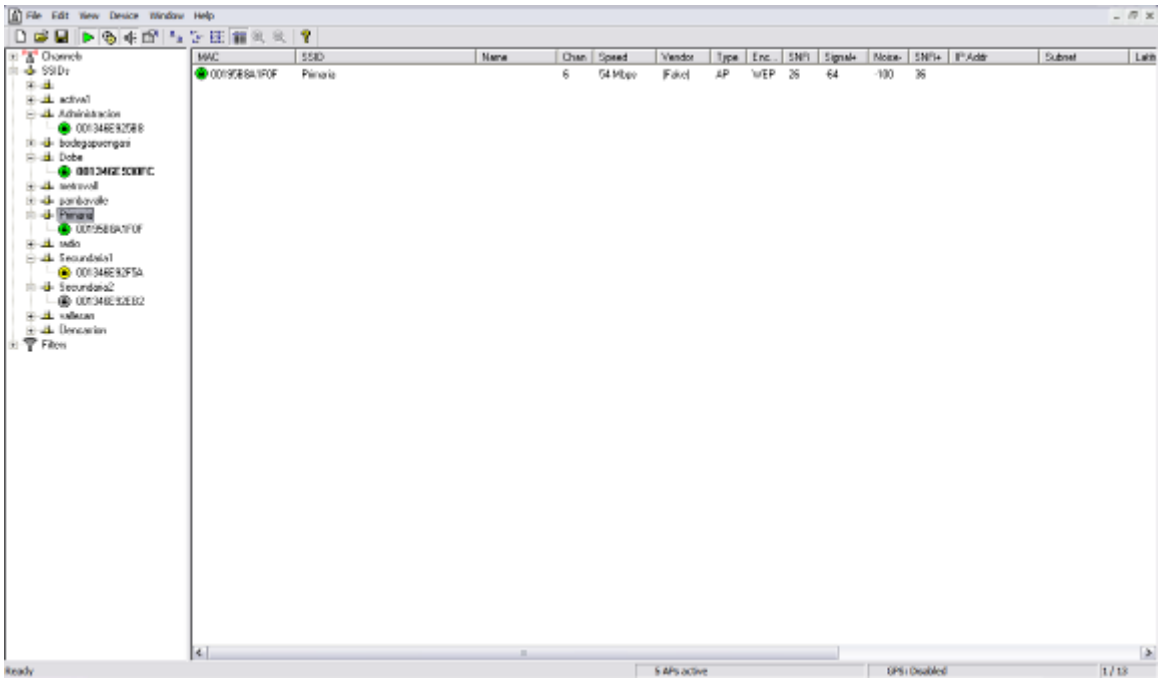


Figura. 5.12. Análisis AP-Primaria en Software Netstumbler

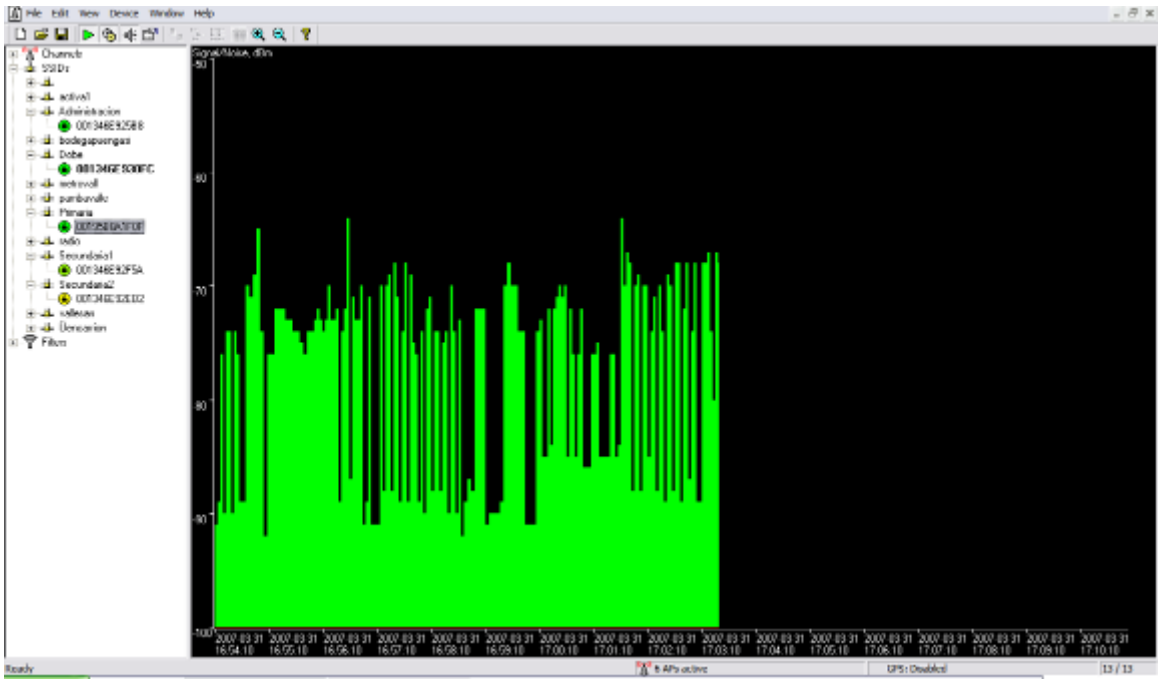


Figura. 5.13. Relación señal-ruido, AP-Primaria

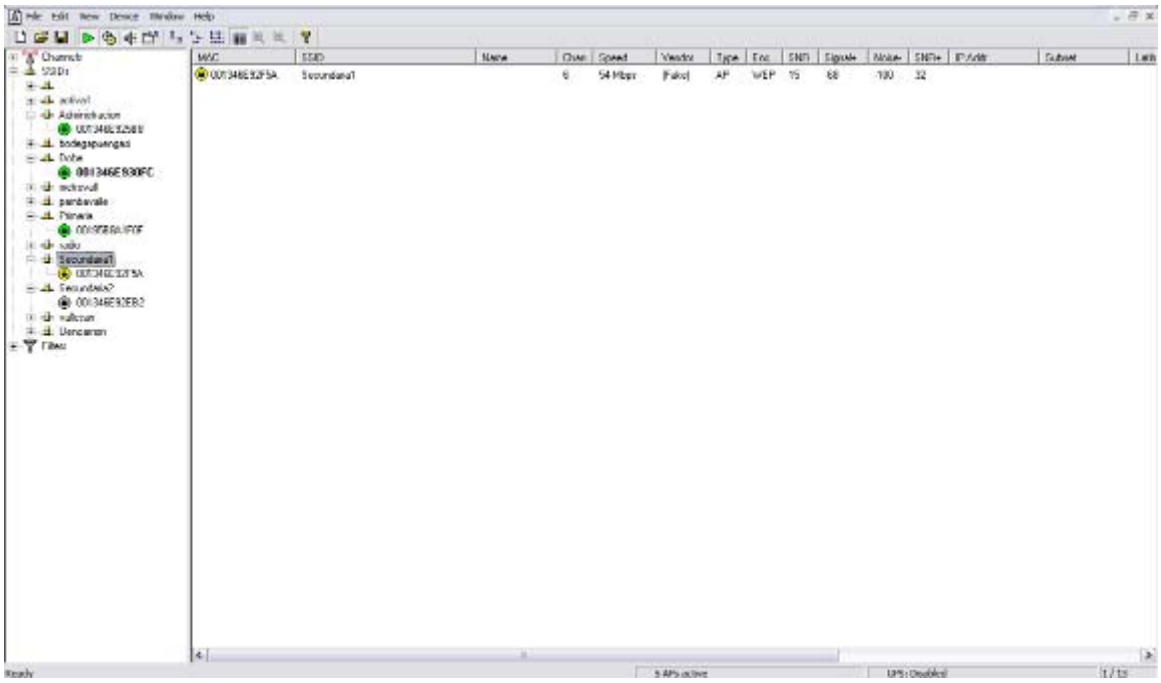


Figura. 5.14. Análisis AP-Secundaria 1 en Software Netstumbler

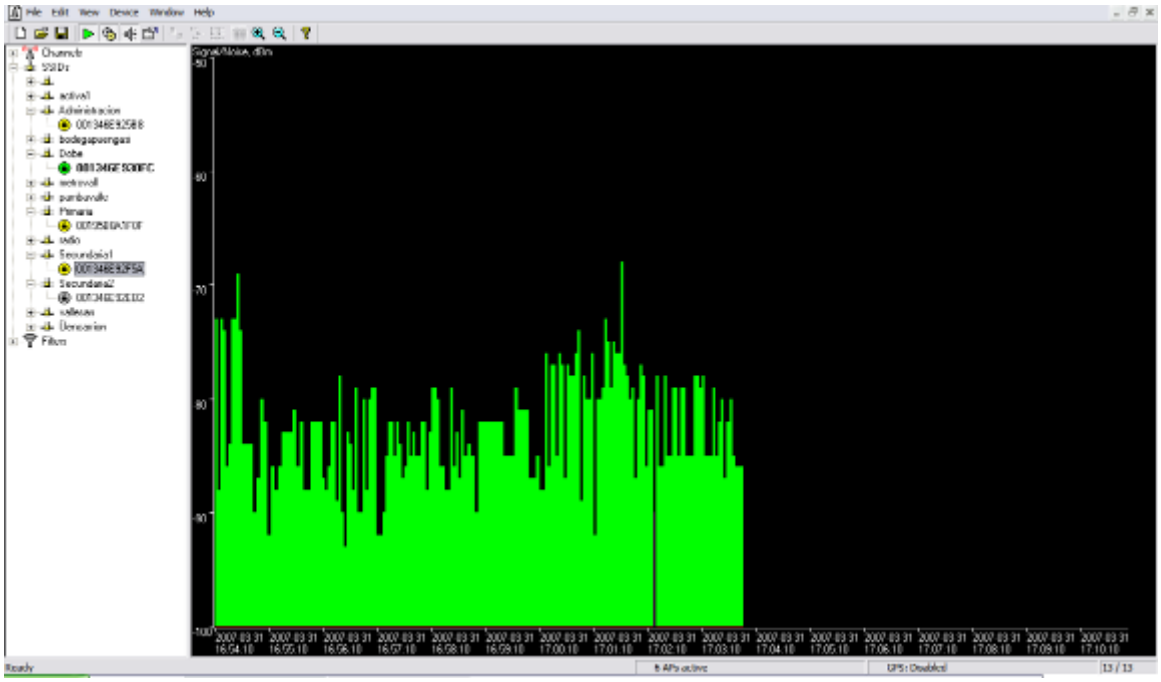


Figura. 5.15. Relación señal-ruido, AP-Secundaria 1

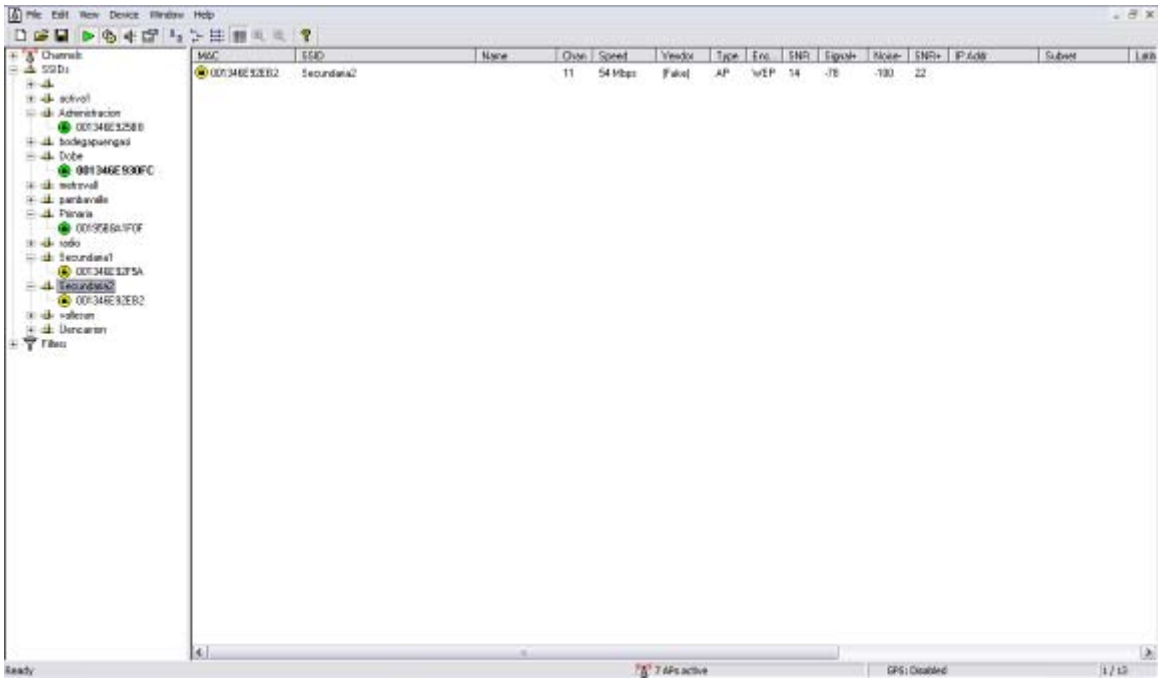


Figura. 5.16. Análisis AP-Secundaria 2 en Software Netstumbler

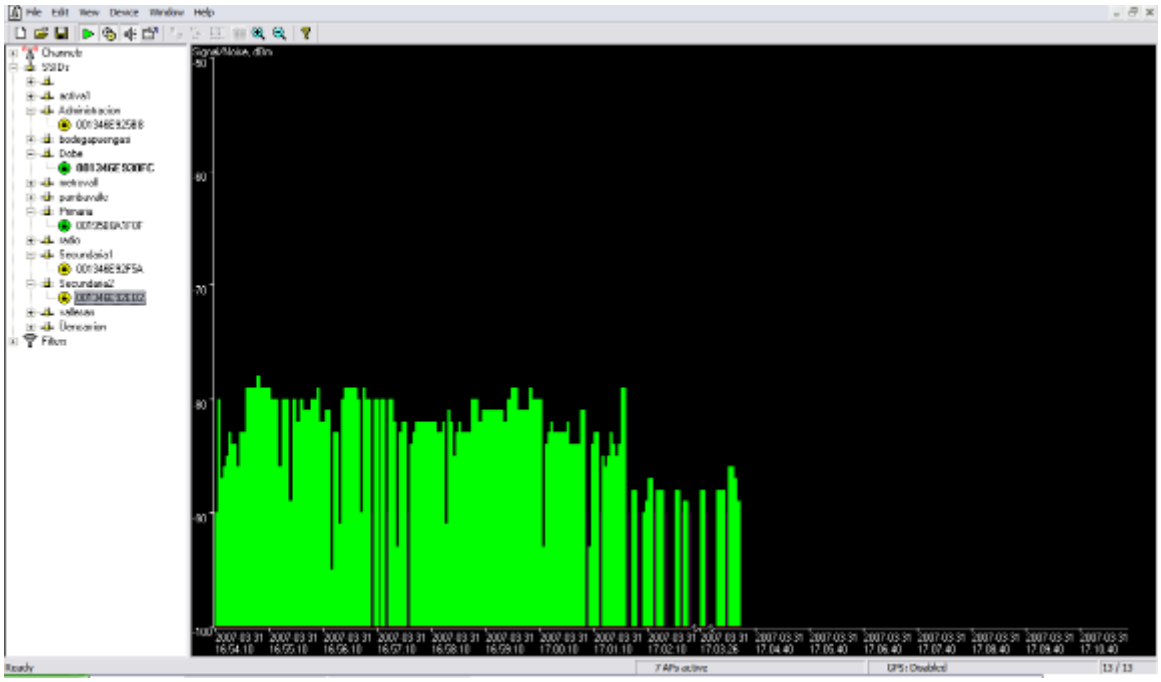


Figura. 5.17. Relación señal-ruido, AP-Secundaria 2

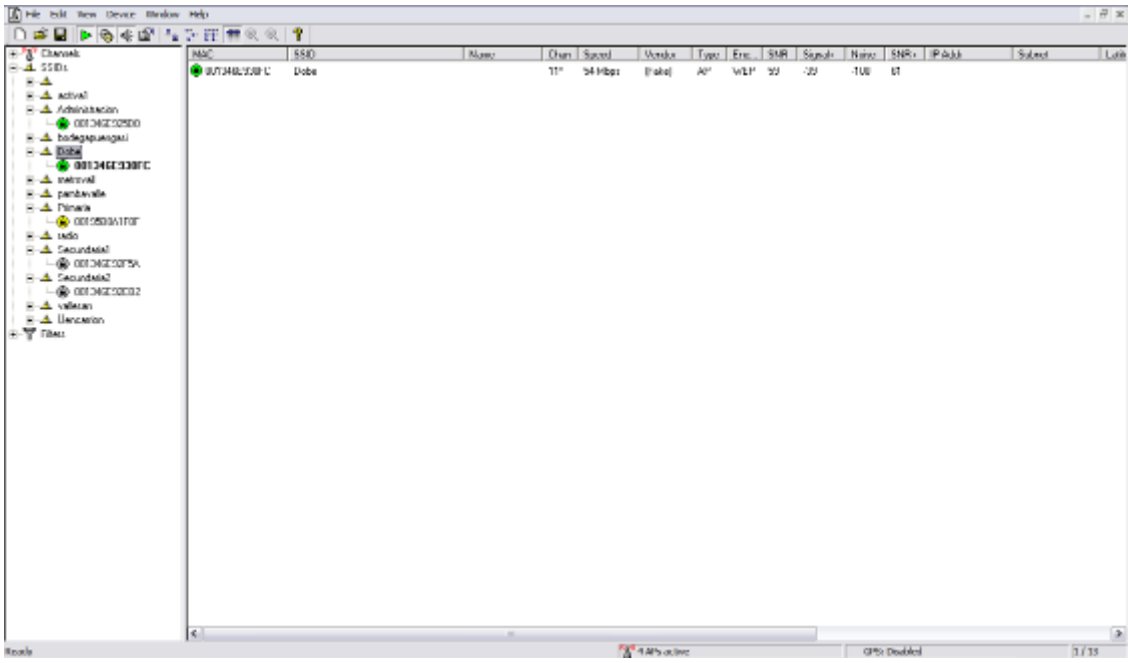


Figura. 5.18. Análisis AP-Preescolar en Software Netstumbler

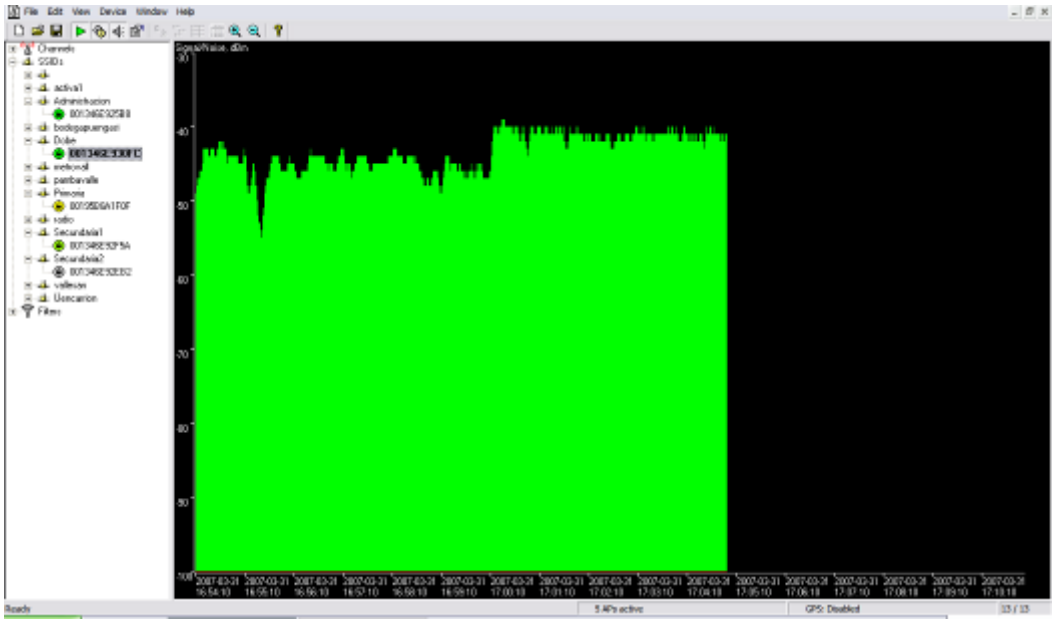


Figura. 5.19. Relación señal-ruido, AP-Preescolar

5.1.6 Dimensionamiento de dispositivos WLAN: - número de usuarios

Dentro del dimensionamiento de una red hay varios parámetros importantes a ser considerados para brindar un buen servicio, calidad y cobertura a los usuarios.

Uno de estos factores corresponde al número de usuarios al cual se va a brindar el servicio, para considerar como distribuir los AP en las diferentes secciones de cobertura.

En el capítulo 1 se realizó un censo dentro de la institución educativa correspondiente al número de computadores existentes, que van a hacer uso de los servicios a ser implementados. De dicho censo se concluyó que aproximadamente va a existir un número de usuarios correspondiente a 50, sin embargo se debe considerar establecer un rango de futuro crecimiento en la red de un 15% por lo que se va a dimensionar los servicios para 65 máquinas.

Sectorizando los usuarios acorde a las facilidades físicas de la infraestructura del colegio, se ha ubicado de la siguiente manera:

Tabla. 5.3. Sectorización de usuarios

1	Administración	Windows XP	Laptop	Gerencia
2	Administración	Windows XP	Laptop	Vicerrectorado
3	Administración	Windows XP	Laptop	Sistemas
4	Administración	Windows XP	PC escritorio	Rectorado
5	Administración	Windows XP	PC escritorio	Vicerrectorado
6	Administración	Windows XP	PC escritorio	Tesorería
7	Administración	Windows XP	PC escritorio	Contabilidad
8	Administración	Windows XP	PC escritorio	Información
9	Administración	Windows XP	PC escritorio	Secretaría Secundaria
10	Administración	Windows XP	PC escritorio	Sistemas
11	Administración	Windows XP	PC escritorio	Sistemas
12	Administración	Windows XP	PC escritorio	Biblioteca
13	Administración	Windows XP	PC escritorio	Almacén
14	Administración	Windows XP	PC escritorio	Biblioteca

- Distancias

Para decidir las distancias que van a determinar el funcionamiento de la red inalámbrica se va a tomar como referencia los planos analizados en el punto 5.1.2 del capítulo, una vez analizadas las instalaciones del campus del colegio mediante los softwares usados como herramientas de diseño, es necesario determinar las distancias a ser

cubiertas para el servicio de los usuarios, el access point escogido para fines de diseño e implementación es el DWL-2100AP, por las características mostradas a continuación:

ESTÁNDARES
IEEE 802.11g
IEEE 802.11b
IEEE 802.3
IEEE 802.3u

SISTEMAS DE FUNCIONAMIENTO WIRELESS
Ap client
Bridge
Bridge+Ap
Repeater

SEGURIDAD
64,128, 152 bits WEP
WPA (WiFi Protected Access)
Mac Address Access Control

CONTROL DE ACCESO AL MEDIO
CSMA/CA con ACK

RANGO DE FRECUENCIA WIRELESS
2.4GHz

RANGO DE OPERACIÓN WIRELESS
Interiores 100m
Exteriores 400m

*Las condiciones adversas del entorno pueden afectar el rango de la señal inalámbrica.

POTENCIA DE TRANSMISIÓN WIRELESS

15dBm (32mW ±2dBm)

CANALES DE TRANSMISIÓN

11 canales

TIPO DE ANTENA EXTERNA

Antena Dipolo de 1 dB.

DIMENSIONES

Largo = 142 mm

Ancho =109 mm

Altura = 31mm

SENSIBILIDAD DEL RECEPTOR

Sensibilidad -66dBm para conexión a 54 Mbps

Sensibilidad -89dBm para conexión a 2 Mbps

Acorde al software empleado como herramienta de diseño, y tomando pruebas con access point de las características mencionadas, se ha decidido realizar el montaje de 5 AP, distribuidos de la siguiente manera:

-1 AP DWL-2100 en el edificio de administración

-1 AP DWL-2100 para cobertura del área de Primaria

- 2 AP DWL-2100 para cobertura del área de Secundaria.

- 1 AP DWL-2100 para cobertura de Preescolar.

Es necesario además considerar el dimensionamiento de las antenas a ser usadas con los APs, debido a la implementación de enlaces tipo bridge. En la red del Liceo se van a llevar a cabo 2 enlaces :

- Primer enlace: desde el edificio de administración hacia primaria con una distancia aproximada de 40m, con línea de vista.

- Segundo enlace: desde el edificio de primaria hacia secundaria con una distancia aproximada de 40m, con línea de vista.

Para lograr enlaces confiables y adicionalmente brindar conectividad wireless a los equipos de los usuarios, se ha considerado colocar antenas onminidireccionales de 8dBi, las cuales tienen las características que se detallan a continuación:

- obstáculos

En el apartado 5.1.3 de este capítulo se realizó un estudio de los diferentes materiales que afectan la transmisión de datos de la red inalámbrica, tomando en cuenta los existentes en el campus del Liceo, los principales obstáculos considerados son:

- Ventana (metal), pérdida 5-8dB
- Pared 10 cm espesor, pérdida 10 dB
- Hormigón, pérdida 20-25 dB

Para evitar interferencia o superposición de las señales, se ha decidido acorde a los softwares de diseño, la mejor ubicación de los equipos AP y antenas que permitan disminuir a menor grado los efectos contrarios de los obstáculos en la red.

5.1.7 Ubicación de los equipos AP

Después de las diferentes herramientas de diseño empleadas anteriormente se ha decidido colocar los 5 AP, en la siguiente distribución:

5.2 REQUERIMIENTOS TÉCNICOS

5.2.1 Definición de Ancho de banda e Interconexión con el proveedor

En cuanto a los factores que participan en el diseño de una red inalámbrica uno de los más relevantes es la elección del Ancho de Banda y el proveedor de servicios que va a brindarlo.

El primer paso para este fin es averiguar con que posibilidades de elección se cuenta a los alrededores de la instalación, para el caso El Liceo del Valle, que tiene una ubicación

alejada de la ciudad se torna un poco complicado hallar proveedores de Internet a sus alrededores que funcionen con una tecnología que garantice la confiabilidad y calidad del servicio.

Con todos estos parámetros como criterio de selección, se contrata 1 Mbps simétrico al proveedor *Tambillo Net* el cual es un carrier de andinanet y brinda servicios al Liceo y las viviendas de sus alrededores, su medio de comunicación es la fibra.

Con esa velocidad de transmisión y ancho de banda es posible implementar todos los servicios planteados para la red y priorizar entrega de paquetes acorde a la aplicación.

Es importante además indicar el tipo de cliente que va a contratar el servicio ya que acorde al número de usuarios, aplicaciones dentro de la red y presupuesto se puede tomar una decisión.

5.2.2 Hardware del servidor de aplicaciones

En el capítulo 2, luego de analizar las diferentes distribuciones Linux del mercado, se decidió implementar el servidor de aplicaciones en plataforma Centos 4.3, el cual para su instalación tiene como requerimientos mínimos:

- Memoria RAM: 256 MB (Mínimo).
- Espacio en Disco Duro: 2 GB (Minimo) - 10 GB (Recomendado).
- Procesador: Intel Pentium III/IV/Celeron, AMD II/III, AMD Duron, AMD Athlon/XP/MP.

Tomando en cuenta estos parámetros, se ha decidido adquirir un computador de las siguientes características:

- Memoria Ram 512MB
- Disco duro 80 GB
- Procesador Pentium IV 2.8GHz
- Tipo clon
- Unidad de CD-RW
- Floppy 3 ½

- Monitor 15 pulgadas
- Teclado, mouse

Dicho servidor proveerá servicios de dhcp, Proxy, firewall, mail, entre otros a aproximadamente 50 computadores.

Dichos servicios no serán provistos de manera simultánea a la cantidad de usuarios antes indicada, sino que será dependiendo de la demanda y el tipo de servicio.

A pesar de que se diera el caso de que todos los usuarios ingresen a todos los servicios simultáneamente, el servidor instalado será suficiente para satisfacer todos los requerimientos.

Tomando en cuenta, los análisis de demanda de servicios y de la cantidad de usuarios se ha decidido las características de hardware para el servidor de aplicaciones y además se ha decidido implementar el servidor en CentOS ya que dicha distribución corresponde a un servicio a nivel empresarial y además es de distribución gratuita y cumple con las características requeridas para la implementación de los diferentes servicios como fue analizado en el capítulo 2, al compararla junto con otras distribuciones Linux.

5.2.3 Red WLAN – Cobertura

Dentro de los parámetros más importantes dentro del diseño de una red inalámbrica, está la cobertura de su servicio y la disponibilidad de sus clientes para poder desplazarse, ya que la movilidad es uno de los principales objetivos de una WLAN.

Si bien es cierto que la mayoría de los puntos de acceso y otros componentes de la infraestructura inalámbrica disponibles actualmente en el mercado funcionan casi como aplicaciones plug and play y que operan correctamente desde el primer momento en entornos muy sencillos y sin interferencias de radiofrecuencia, también es cierto que en el mundo actual existen ya pocos entornos libres de interferencias de radiofrecuencia

La cobertura de una red inalámbrica está determinada por varios factores, detallados a continuación:

Potencia de los equipos de comunicación tanto de transmisión como de recepción.

En el numeral 5.1.6 del presente capítulo se dio a conocer las características de los equipos wireless, al escoger Access Point DWL-2100AP se tiene una potencia de los equipos de 32mW, cada uno de estos equipos viene con una antena de 1dBm, que acorde al software empleado como herramientas de diseño, se concluyó que se requieren 5 APs, para garantizar total cobertura para todas las áreas demandadas para la utilización del servicio inalámbrico.

Figura. 5.20. Access Point DWL-2100AP

Se debe también tomar en cuenta que con la ganancia de las antenas que vienen por defecto con los APs no es suficiente para abastecer de una buena señal y tampoco son las más adecuadas para ser montadas en exteriores. Del numeral 5.1.5 se deriva la ubicación de los APs y se determinó que las antenas corresponden a una potencia de 8dBi.

Ganancia de las antenas a emplearse en los equipos.

Para mayor compatibilidad con el AP seleccionado para la implementación se colocarán antenas Dlink ANT24-0800 antena exterior omni dBi.

Figura. 5.21. Antena D-Link 24-0800

La antena D-Link modelo ANT24-0800, con sus 8 dBi de ganancia, permite extender la señal de cobertura de una red local basada en la tecnología inalámbrica IEEE 802.11b a 11Mbps. Esta antena permite la conexión a cualquier punto de acceso capaz de soportar antenas externas.

El conector presente en la antena es de tipo N hembra, y el material con el que ha sido hecha es capaz de resistir las peores condiciones atmosféricas en instalaciones exteriores.

El kit de montaje permite posicionar la antena de forma que se pueda aprovechar al máximo las características omnidireccionales de la misma. Dentro del paquete se encuentra una protección para la antena contra las descargas electroestáticas y un cable de 50 cm.

A continuación se listan sus especificaciones técnicas

- Frecuencia : 2.4 ~ 2.5 GHz
- Ganancia : 8 dBi
- Polarización : Lineal vertical
- HPBW: horizontal 360?, vertical 15?
- Impedancia : 50 Ohm nominales
- Conector estándar : N hembra
- Resistencia al viento : 180 km/h máx.
- Temperatura de funcionamiento: -40 ^{o}C ~ +70 ^{o}C
- Humedad : 100% a 25 ^{o}C
- Protección : respecto a masa
- Color : Blanco
- Kit de montaje incluido
- Peso : 0.3 kg
- Longitud : 65 cm
- Garantía : 1 año

La calidad de señal en una zona de cobertura wireless viene determinada por la relación entre la potencia de la señal recibida y el nivel de ruido existente, incluyendo

posibles señales interferentes. A dicha diferencia de potencias se le conoce como la relación señal-ruido, o SNR. Se ha considerado que por encima de 15db de señal SNR la calidad de la señal recibida es aceptable. Así pues dicho umbral de señal SNR al movernos alrededor de un punto de acceso determinará un área de cobertura determinada.

Hay también que recordar que para disponer de roaming entre celdas wireless ,estas deberán solaparse parcialmente. De ahí la ubicación estratégica de cada uno de los APs.

En cuanto a las tarjetas de red inalámbricas que trabajan como receptor en cada usuario, corresponden a las tarjetas DLINK DWL-G520 o DWL-G120, que acorde a la disponibilidad de los equipos puede ser de tipo usb para portátiles o tipo PCMCIA para desktops.

Tarjeta PCMCIA Dlink

Figura. 5.22. Tarjetas usb Dlink

Configuración óptima de los puntos de acceso

El objetivo es proporcionar la cobertura de radiofrecuencia (RF) necesaria en las zonas necesarias de sus instalaciones.

Una vez determinadas las necesidades de cobertura, los APs serán configurados como AP + bridge, los factores más sobresalientes de configuración es el canal de transmisión y las MACs del AP anterior y próximo. Se debe además analizar que las redes colindantes con la nuestra para evitar altos factores de interferencia en la señal.

Seguridad

Dentro de las opciones de la red existen varios equipos que pueden aportar a brindar seguridad por si solos y en conjunto fortalecer este parámetro.

Para diseñar un esquema de seguridad dentro de una red inalámbrica existen varios parámetros y factores a ser tomados en cuenta, dentro de las soluciones se plantea lo siguiente:

El servidor de comunicaciones de la red es el core de la misma, ya que es el dispositivo de salida y entrada para usuarios, información, paquetes y filtraje de funciones a nivel de aplicaciones. Dentro del servidor se implementó un firewall y un antivirus general y de correo que permite filtrar contenidos, destinos e información, ya sea por servicios, por puertos o por aplicaciones. Dicho procedimiento fue explicado a detalle en el numeral 2.5 del capítulo II.

Otra implementación de seguridad es el protocolo o esquema de protección a ser usado en los equipos. Acorde a las características hasta aquí definidas para los equipos y lo analizado en el capítulo III numeral 3.2.6, existen 2 tipos de cifrado en la red:

WEP

Significa privacidad equivalente a conectado con red cableada. WEP le permite al administrador definir un conjunto de claves para la WLAN. Estas claves son compartidas entre los clientes y puntos de acceso y son usados para cifrar datos antes de transmitirse. Si un cliente no tiene la clave WEP correcta, no puede descifrar los paquetes recibidos o enviar datos a otros clientes. Lo cual evita el acceso no autorizado de la red y escuchas furtivas. El WEP es un sistema de cifrado estático y sin nacionalidad, lo que significa que una vez que ingreso la clave correcta en el diálogo Claves WEP/WPA, CommView for WiFi será capaz inmediatamente de descifrar paquetes.

WPA

WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

Para el uso personal doméstico: El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

Para el uso en empresarial/de negocios: El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor RADIUS.

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA. La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP (ver arriba). AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 será compatible tanto con la versión para la empresa como con la doméstica.

Al analizar ambos tipos de encriptaciones, y acorde a las capacidades de los DWL-2100AP, se colocará la opción OpenSystem para comunicar la clave a través de la red, es el método de autenticación por defecto del estándar 802.11, el tipo de clave es de 128 bits y ASCII, la clave válida es la primera clave de activación. Con ello se obtendrá el servicio de roaming entre los APs de la red para tener movilidad y continuidad en el servicio y seguridad con la solicitud de clave.

Escalabilidad

La escalabilidad es la capacidad de un sistema informático de cambiar su tamaño o configuración para adaptarse a circunstancias inestables. La escalabilidad juega aquí un importante papel en el diseño porque los elementos activos de red manejan datos a tiempo real de todo un entorno, como lo son los paquetes de VoIP y videovigilancia que tienen alta demanda de accesibilidad de los usuarios.

Las WLANs pueden ser configuradas en una gran variedad de formas para encontrar las necesidades específicas de ciertas aplicaciones e instalaciones: para el modelo DWL-2100AP escogido para la implementación de la red del Liceo del Valle, las configuraciones son fácilmente cambiadas, y la gama de redes punto a punto adecuadas para un pequeño número de usuarios hasta redes tipo infraestructura para integrar cientos o miles de usuarios, dependen del número de dispositivos inalámbricos desplegados.

El DWL-2100AP es compatible , en modo por defecto, con los siguientes productos wireless:

D-Link *Air*Plus Xtreme G DWL-G650

Adaptadores wireless usados con laptops

D-Link *Air*Plus Xtreme G DWL-G520

Tarjetas PCI wireless usadas con desktops

El DWL-2100AP es también interoperable con otros 802.11g y 802.11b compatible con los estándares de dispositivos.

Calidad de Servicio

En cuanto a la implementación de calidad de servicio, en el capítulo II, numeral 2.4.2, se indica que dicha aplicación será implementada en el servidor Linux, para dar propiedad a los paquetes se VoIP y videovigilancia dentro del tráfico de la red diseñada y los parámetros a seguir para este fin.

En cuanto a los equipos activos de red el objetivo constituye en esencia clasificar los paquetes para optimizar el consumo de ancho de banda así como priorizar por tipo de tráfico. La idea, en esencia es permitir descargas masivas, como http (isos, fuentes, etc...), emule, bittorrent, ftp, etc... sin mermar el tráfico interactivo, como vozip, videoconferencias, navegación, etc. De forma que todo pueda coexistir sin necesidad de saturar la red por diferente tipo de tráfico. De forma que entre los usuarios puede haber (incluso hacia Internet) transferencias de ISOs (http, ftp, samba) descomunales sin necesidad de que los juegos en línea o las videoconferencias se vean mermadas.

Existen scripts de QoS tanto en los bridges como en los AP's repetidores, tanto para priorizar el tipo de tráfico como para establecer los parámetros de subida y bajada de cada cliente. De esta forma se consigue una gran eficiencia en el uso del ancho de banda y una gran interactividad en las comunicaciones de los usuarios.

5.2.4 Equipos VoIP

Para diseñar la aplicación de VoIP, se hará referencia al capítulo 4 donde se analizan características de funcionamiento y especificaciones técnicas de los equipos que permitieron establecer un criterio adecuado para la elección de los dispositivos de VoIP a ser implementados, en el numeral 5.1.1 se analiza acorde al número de usuarios la demanda de los diferentes servicios por parte de los usuarios.

Continuando con la línea DLink implementada en la parte inalámbrica, se ha escogido el modelo DVX-1000 correspondiente a una IP-PBX con servidor de conferencia.

Esta central es una IP-PBX basada en protocolo SIP que incorpora todas las características necesarias de un sistema telefónico del cual puede depender una compañía.

Ofrece características como: desvío de llamadas, llamadas en espera, buscador y buzón de mensajes. Permite utilizar teléfonos comunes a través de una salida externa vía gateway o servicios costo/efectivos a través de teléfonos IP.

Figura. 5.23. SIP IP-PBX DVX-1000

Soporta 25 extensiones, las cuales pueden ser ubicadas en cualquier parte donde exista acceso a internet. Además es una opción escalable ya que permite incorporar a través de licencias hasta 100 extensiones. Si se desea pueden ser usadas más DVX-1000 para incrementar el número de extensiones o unir una empresa que tenga más sucursales a través de un único sistema PBX, como información general ya que para la aplicación del Liceo del Valle es suficiente con la instalación de un solo DVX-1000.

Es configurable a nivel usuario a través de las herramientas de configuración web. Permite asignar un perfil de telefonía a cada extensión, para un mejor cruce de asignación de funciones de trabajo para usuarios. Cada usuario puede afinar su asignación de perfil vía web para sincronizar su agenda de trabajo diaria.

Posee un puente de conferencia telefónica, que agrega un mayor valor sin incorporar mayores costos. Los usuarios están habilitados para agendar e invitar a reuniones de conferencia vía configuración web. Utiliza características avanzadas de seguridad, frente a accesos no autorizados. Para prevenir hackers, la IPPBX DVX-1000 utiliza un software de autentificación-encriptación MD5 SIP. También incorpora de manera integrada un firewall para detección de intrusos y protección contra ataques DoS (denial of service).

Se lo puede montar en paredes y es stackeable con otros switches o gateways existentes.

Por todas las características mencionadas anteriormente se ha escogido esta central para implementarla en la red, a continuación se detalla las características del gateway que se ajusta al diseño de la red.

Gateway Dlink Dvg-7022s

Con la finalidad de enrutar las llamadas provenientes de teléfonos analógicos, conectando la red empresarial de VoIP a la PSTN se requieren de un equipo que permita integrar diversas funcionalidades de comunicación de VoIP considerando tanto la conexión hacia líneas telefónicas como la transformación de infraestructura tradicional de telefonía hacia VoIP.

El equipo requerido para esta función, incursionando dentro de la línea DLink es el DVG-7022S que combina puertos FXS y FXO.

Figura. 5.24. Dvg-7022s

El DVG-7022S posee una excelente calidad de voz y comunicación confiable a través de la implementación de patrones internacionales para redes de voz y datos. Soporta también funciones de QoS para garantizar que los paquetes de voz que se transfieran a través de Internet tengan un normal curso. En relación a los datos, esta característica le da preferencia a la voz. Permite utilizar líneas telefónicas estándar ya que cuenta con 2 puertos FXO que permiten integrar 2 líneas telefónicas PSTN con la IP PBX. También este gateway IP cuenta con dos puertos FXS que permiten la conexión directa de dos teléfonos análogos al mundo IP. Adicionalmente, cuenta con 4 puertos LAN 10/100Mbps que permiten la conexión de 4 teléfonos IP y otros dispositivos como PCs, Access Points Wireless, Switch Smart que permitan potenciar el valor de convergencia en esta red propuesta. Incluye también un puerto WAN que permite la conexión de la red a Internet de

banda ancha y de esta forma permitir que los dispositivos de la red compartan la conexión a Internet.

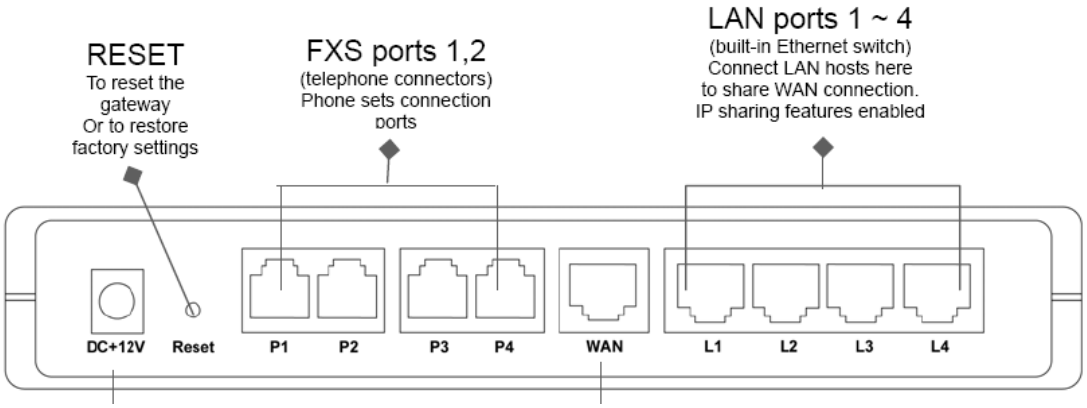


Figura. 5.25. DVG 7022S Vista posterior

Para la solución dada por Dlink la central DVX-1000 y el gateway DVG 7720S trabajan como paquete para solución de telefonía IP. Es una solución escalable y pensada para el crecimiento, una solución ideal para actualizarse desde una PBX tradicional hacia una solución IP PBX. Ambos dispositivos son admnistrables via web.

5.2.5 Cámaras IP

Para el servicio de videovigilancia es necesario dimensionar los requerimientos del equipo acorde a las demandas del servicio e infraestructura del Liceo del Valle.

Una cámara de seguridad inalámbrica está diseñada como un sistema de seguridad y monitoreo autónomo, que permite observar remotamente, desde el hogar u oficina, un lugar determinado a monitorear.

Se ha escogido para la aplicación requerida la cámara DCS-2100G de la línea Dlink que cuenta con las siguientes características:

- Soporte para conexión vía Wireless 802.11g o Ethernet
- Sistema de monitoreo autónomo gracias a su Servidor Web Integrado,
- Monitoreo Remoto vía Web
- Monitoreo de múltiples cámaras vía Software Windows, hasta 16 en forma simultanea,
- Activación de grabado de video, ante detección de movimiento, y

- Fácil y rápida implementación de sistema de video vigilancia,
- Zoom digital de 4x
- Soporte de UPnP & DNS
- Captura de vídeo bajo circunstancias de poca luz
- E-mails de alerta

Figura. 5.26. Cámara DCS-2100G

Con todas las facilidades, la cámara DCS-2100G puede ser conectada a cualquier red Wireless o Ethernet en una Oficina o Campus, además de Internet de Banda Ancha, vía un wireless router por ejemplo. La cámara provee una alta calidad de video, además tiene incorporado un Servidor Web y detecta movimiento para grabar. Adicionalmente incorpora gratuitamente un poderoso software para monitoreo y administración de múltiples cámaras.

Tabla. 5.4. Descripción General de Cámara DCS-2100G

Interfaces	1 Porta RJ-45 auto-sensing Fast Ethernet 10/100Mbps 802.11g Wireless LAN
Especificaciones de la Camara	- Incorpora un sensor CMOS color de 1/4" - Control automático de ganancia (AGC): 24 dB - Exposición Automática (AE) support - Control automático de blancos (AWB) - Disparador automático: 1/60 to 1/1500 sec. - Iluminación mínima: 1.0 Lux @ f2.0 - Lente fijo - Focal fijo (4mm, f2.0) con afinación de precición
Resolución	- 30 fps @ 320 x 240 and 160 x 120 - 10 fps @ 640 x 480
Formatos	- MPEG4 Modo de compresión corta para video - JPEG Compresor de imágenes - Radio de compresión: 5 niveles - Max. Velocidad de imágen: 30 fps

	- Ajuste de tamaño imagen, calidad y velocidad binaria - Estampado de fecha/hora y posicionamiento de texto sobre la imagen. - Tamaño video: QQVGA, QVGA, VGA (seleccionable por el usuario)
Zoom-In	- Zoom digital hasta 4x
Entrada de audio	- Incorpora micrófono omni-direccional con un rango dinámico de 60 dB
Protocolos y Aplicaciones	- Soporte de los servidores mas utilizados de DDNS - Soporte UPnP - NTP Cliente - SMTP Cliente - FTP Cliente - ServidorFTP - Soporta modo pasivo de FTP - Servidor HTTP: Max. 10 usuarios viendo a la vez - Puerto server ajustable - Autenticación SMTP
Detección de movimiento	- 3 ventanas para detección de movimiento - 2 Parámetros de ajuste: sensibilidad y porcentaje
Administración	- Via navegador.
Características Wireless	- Wireless LAN Standards: 802.11g/b - **Velocidad de datos:** 802.11g: up to 54 Mbps (6/9/12/18/24/36/48/54 Mbps) 802.11b: up to 11 Mbps (1/2/5.5/11 Mbps) - **Rango de frecuencias:** 2.4 to 2.4835 GHz ISM band - **Canales de Operación:** 1 to 11 channels (FCC), 1 to 13 channels (ETSI) - **Antena:** Externa de 2 dBi de ganancia dipole antena (reverse SMA connector) - **Sensibilidad de recepción (para 802.11b)** (Typically @PER < 8% packet size 1024 @ 25 C +/- 5 C) - 11Mbps (CCK): - 80 dBm - 5.5Mbps (CCK): - 83 dBm - 2Mbps (QPSK): - 84 dBm - 1Mbps (BPSK): - 87 dBm **Sensibilidad de recepción (para 802.11g)** o o (Typically @PER < 8% packet size 1024 @ 25 C +/- 5 C) - 54Mbps (OFDM): -65 dBm - 48Mbps (OFDM): -66 dBm - 36Mbps (OFDM): -70 dBm

	- 24Mbps (OFDM): -72 dBm - 18Mbps (OFDM): -77 dBm - 12Mbps (OFDM): -79 dBm - 9Mbps (OFDM): -81 dBm - 6Mbps (OFDM): -82 dBm **Rango de Operación *** - Indoors: Up to 100 meters - Outdoors: Up to 300 meters • Factores medioambientales podrían alterar el rango de cobertura **Seguridad** Encriptación de datos WEP 64/128-bit (user-selectable)
Características Físicas	- Alimentación: 5V DC, 2.0A - Power Supply: Fuente externa AC Auto-Switching - Consumo: 4.3 watts - Dimensiones: 26.8 (L) x 72.8 (W) x 115.2 (H) mm - Peso: 215 grams - Temperatura de operación: 0º to 50º C - Emision (EMI): FCC Clase B, CE Clase B

CAPÍTULO 6

ANÁLISIS ECONÓMICO

6.1 ELECCIÓN DE EQUIPOS DE RED, SERVIDOR Y PROVEEDORES ISP Y VOIP

Durante el desarrollo de esta tesis, en capítulos anteriores, se han establecido las especificaciones técnicas de los equipos a ser utilizados, tanto de los componentes principales como de cada dispositivo de la red.

En el mercado existe variedad de marcas para los equipos que se utilizarán en esta tesis, pero se debe evaluar a cada una de estas, tanto el cumplimiento de las características técnicas, cuanto el aspecto económico, para poder elegir el más adecuado según el análisis costo-beneficio que se realizará previo a la adquisición de estos.

Criterios de selección.

Por cada marca preseleccionada, se evaluará el costo unitario de cada equipo, así como el monto total. Si una misma marca no tiene los mejores precios, se analizará el monto en otras marcas con precios más competitivos, así como sus características técnicas. En caso de que la diferencia no sea sustancial, por condiciones de garantía y compatibilidad entre equipos, se preferirá a una sola marca.

La empresa proveedora de los equipos, deberá dar como mínimo, un año de garantía en estos, tiempo en el cual deberá brindar de manera inmediata, repuestos, mantenimiento y asesoría técnica.

La marca seleccionada de equipos, deberá cumplir en su totalidad con las características técnicas previstas para el buen funcionamiento de la implementación de esta tesis.

Cuadros comparativos, pre-selección

Con los criterios para selección de equipos, se procede a realizar cuadros comparativos de las marcas precalificadas.

Tabla. 6.1. Cuadro comparativo de Access Point

MARCA	**CISCO**	**3COM**	**D-LINK**	**LINKSYS**
MODELO	**Aironet 1100**	**Enterprise 7250**	**DWL 2100**	**WAP 54G**
Cumple especificaciones técnicas	Si	Si	Si	No
Garantía	1 año	1 año	1 año	1 año
Representación en el País	Si	Si	Si	Si
Costo unitario	234	190	98	44

Tabla. 6.2. Cuadro comparativo de Adaptadores de Red PCI

MARCA	**CISCO**	**3COM**	**D-LINK**	**LINKSYS**
MODELO	**Aironet PCI-G**	**Office Connect 802.11g PCI**	**DWL G-520**	**WMP 54GS**
Cumple especificaciones técnicas	Si	Si	Si	No
Garantía	1 año	1 año	1 año	1 año
Representación en el País	Si	Si	Si	Si
Costo unitario	185	51	46	50

Tabla. 6.3. Cuadro comparativo de cámara IP inalámbrica

MARCA	**CISCO**	**3COM**	**D-LINK**	**LINKSYS**
MODELO	**54G**	**X**	**DCS-2100G**	**WV-C54GC**
Cumple especificaciones técnicas	Si		Si	No
Garantía	1 año		1 año	1 año
Representación en el País	Si		Si	Si
Costo unitario	230		199	138

Tabla. 6.4. Cuadro comparativo de switch 24P

MARCA	**CISCO**	**3COM**	**D-LINK**	**LINKSYS**
MODELO	**Catalyst 2950**	**3870**	**DES- 1024D/A**	**SR-224G**
Cumple especificaciones técnicas	Si	Si	Si	No
Garantía	1 año	1 año	1 año	1 año
Representación en el País	Si	Si	Si	Si
Costo unitario	661,7	190	93,92	145

Tabla. 6.5. Cuadro comparativo de central telefónica IP

MARCA	**CISCO**	**3COM**	**D-LINK**	**LINKSYS**
MODELO	**ICS-7750**	**NBX-V300**	**DVX-1000**	**SPA-9000**
Cumple especificaciones técnicas	Si	Si	Si	No
Garantía	1 año	1 año	1 año	1 año
Representación en el País	Si	Si	Si	Si
Costo unitario	4000	2000	1013	800

En los cuadros indicados, se ha contrastado tanto el carácter técnico como económico de los equipos a ser utilizados, en cuatro de las marcas más reconocidas en el mercado.

Como resultado del análisis realizado, se pudo determinar que la marca Linksys no cumple con las especificaciones técnicas necesarias para la selección de los equipos, motivo por el cual se toman en cuenta las tres marcas restantes.

De las tres marcas que cumplen con las características técnicas, se evaluó el aspecto económico, seleccionando de esta manera a la marca D-Link, como la más viable para la adquisición de los equipos a ser implementados.

6.2 COSTOS DE EQUIPOS

Con los resultados del análisis costo-beneficio efectuado en el numeral anterior, se procede a realizar la adquisición de los equipos principales, en las marcas indicadas.

En la tabla 6.5, se puede apreciar estos equipos, así como las cantidades a implementarse.

Tabla. 6.6. Equipos principales

ÍTEM	CÓDIGO	DESCRIPCIÓN	CANT.	UDM	PRECIO UNITARIO	PRECIO TOTAL
01	(DLK-ANT24-0800)	ANTENA OMNIDIRECCIONAL 2.4GHz,8dBi PARA EXTERIORES.	5	uni	144	720
02	(DLK-DCS-2100G	CAMARA IP INALAMBRICA IEEE 802.11g, 2.4GHZ, 54Mbps CON AUDIO.	8	uni	199	1592
03	(DLK-DES-1005D)	SWITCH L2, 5 P 10/100BASE-T PARA ESCRITORIO.	1	uni	30	30
04	(DLK-DES-1024D/A)	SWITCH L2, 24 P 10/100BASE-T PARA ESCRITORIO + KIT PARA RACK	2	uni	93,92	187,84
05	(DLK-DFE-520TX)	TARJETA PCI 10/100BASE-TX 32 BITS.	1	uni	5,27	5,27
06	(DLK-DWL-2100AP)	ACCESS POINT INALAMBRICO IEEE 802.11G, 54/108MBS, BRIDGE.	6	uni	98	588
07	(DWL-G520)	TARJETA INALÁMBRICA DE RED	9	uni	46,1	414,9
08	(DLK-Dvx-1000)	CENTRAL TELEFÓNICA SIP IP-PBX, CONFERENCING SERVER	1	uni	1013	1013
09	(DLK-DVG-7022S)	ROUTER IP CON MULTIPUERTOS, VoIP, GATEWAY, 4P 10/100, 2P FXO	1	uni	800	800
10	(DLK-)	TELÉFONO IP	2	uni		0
11	(DLK-)	TELÉFONO ANALÓGICOS	2	uni		0
12	CYS-SRVCOM-ADV	SERVIDOR DE COMUNICACIONES AVANZADO.	1	uni	744,73	744,73
					TOTAL	**$ 6.095,74**

Los valores mostrados en la tabla 6.5 no contempla el valor del IVA.

Así también se tiene un listado de los elementos secundarios para la instalación, estos se detallan en la tabla 6.6.

Tabla. 6.7. Elementos secundarios

ÍTEM	COD.	DESCRIPCIÓN	CANT.	UDM	PRECIO UNITARIO	PRECIO TOTAL
01	(BEA-I-0301)	GABINETE LIVIANO 20X20	5	uni	18	90,00
02	(BEA-I-1034)	SOPORTE DE PARED 19plg 6UR.	1	uni	29	29,00
03	(BEA-I-1043)	RACK ABIERTO DE PISO 48plg 24UR.	1	uni	110,7	110,7
04	(BEA-I-1101)	BANDEJA ESTANDAR 19plg 2UR.	1	uni	14,85	14,85
05	(BEA-I-1135	MULTITOMA HORIZONTAL 19plg 4 TOMAS DOBLES.	1	uni	36,36	36,36
06	(BEA-I-1143	ORGANIZADOR HORIZONTAL 2 UR 60x80.	3	uni	10,85	32,55
07	(DEX-P-1000)	CAJA SOBREPUESTA PARA INTERRUPTOR O TOMACORRIENTE 40 mm	41	uni	1,38	56,58
08	(DEX-P-1003)	CANALETA PLASTICA 32X12 LISA MARFIL.	51	uni	1,56	79,56
09	(DEX-P-1006)	CANALETA PLASTICA 40X25 LISA MARFIL.	26	uni	3,8	98,8
10	(DEX-P-1007)	CANALETA PLASTICA 60X40 LISA MARFIL.	20	uni	5,6	112
11	(DEX-P-1012)	CANALETA PLASTICA 100x45 LISA MARFIL.	13	uni	11,14	144,82
12	(DEX-P-1031)	ANGULO EXTERNO PARA CANALETA 32X12 MARFIL.	17	uni	0,55	9,35
13	(DEX-P-1032)	ANGULO PLANO PARA CANALETA 32X12 MARFIL.	13	uni	0,55	7,15
14	(DEX-P-1034)	UNION PARA CANALETA 32X12 MARFIL.	11	uni	0,52	5,72
15	(DEX-P-1035)	TAPA FINAL PARA CANALETA 32X12 MARFIL.	16	uni	0,52	8,32
16	(DEX-P-1040)	ANGULO INTERNO PARA CANALETA 40X25 MARFIL.	4	uni	0,7	2,8
17	(DEX-P-1041)	ANGULO EXTERNO PARA CANALETA 40X25 MARFIL.	5	uni	0,7	3,5
18	(DEX-P-1042	ANGULO PLANO PARA CANALETA 40X25 MARFIL.	1	uni	0,7	0,7
19	(DEX-P-1044)	UNION PARA CANALETA 40X25 MARFIL.	10	uni	0,58	5,8
20	(DEX-P-1045)	TAPA FINAL PARA CANALETA 40X25 MARFIL.	3	uni	0,58	1,74
21	(DEX-P-1050)	ANGULO INTERNO PARA CANALETA 60X40 MARFIL.	9	uni	1,9	17,1
22	(DEX-P-1051)	ANGULO EXTERNO PARA CANALETA 60X40 MARFIL.	10	uni	1,9	19
23	(DEX-P-1054)	UNION PARA CANALETA 60X40 MARFIL.	2	uni	1,54	3,08
24	(DEX-P-1055)	TAPA FINAL PARA CANALETA 60X40 MARFIL.	1	uni	1,54	1,54
25	(DEX-P-1070)	ANGULO INTERNO PARA CANALETA 100X45 MARFIL.	4	uni	4,8	19,2
26	(DEX-P-1071)	ANGULO EXTERNO PARA CANALETA 100X45 MARFIL.	2	uni	4,8	9,6
27	(DEX-P-1072)	ANGULO PLANO PARA CANALETA 100X45 MARFIL.	3	uni	4,8	14,4
28	(DEX-P-1074)	UNION PARA CANALETA 100X45 MARFIL.	8	uni	4,8	38,4
29	(DEX-P-1075	TAPA FINAL PARA CANALETA 100X45 MARFIL.	1	uni	4,8	4,8
30	(GEN-ETIQ)	ETIQUETAS.	1	uni	30	30
31	(NXS-32510)	CABLE UTP 4 PARES CAT 5E.	2135	m	0,34	725,9
32	PR-ANTIVIRUS	ANTIVIRUS.	50	uni	12,21	610,5
33	QST-NFP-2028	FACE PLATE 2 P. BLANCO.	42	uni	0,89	37,38
34	(QST-NIN-1108)	BLANK PARA FACE PLATE BLANCO.	20	uni	0,25	5
35	(QST-NKJ-5103)	CONECTOR RJ45 JACK CAT. 5E ROJO.	48	uni	2,24	107,52
36	(QST-NPC-1303)	PATCH CORD COBRE DE 3 PIES CAT. 5E ROJO.	48	uni	0,91	43,68
37	(QST-NPC-1307)	PATCH CORD COBRE DE 7 PIES CAT. 5E ROJO.	49	uni	1,35	66,15
38	(QST-NPP-1024)	PATCH PANEL RJ45 DE 24 P. CAT. 5E SOLIDO.	3	uni	80	240
					TOTAL	**$ 2.843,55**

Los valores mostrados en la tabla 6.6 no contempla el valor del IVA.

Las dos tablas indicadas anteriormente, muestran los costos directos de los equipos tanto primarios, como secundarios a ser utilizados.

6.3 COSTOS DE MANTENIMIENTO

Para el correcto funcionamiento de los servicios generales implementados dentro del liceo del valle, se ha decido llevar un mantenimiento trimestral, el mismo que conlleva las actividades listadas en la tabla 6.7

Tabla. 6.8. Mantenimiento trimestral

ÍTEM	DESCRIPCIÓN	CANT.	UDM	PRECIO UNITARIO	PRECIO TOTAL
01	CHEQUEO GENERAL DE FUNCIONAMIENTO DE SERVICIOS	1	global	20	20
02	ACTUALIZACIÓN DE SOFTWARE DE SERVIDOR DE COMUNICACIONES	1	global	10	10
03	ACTUALIZACIÓN DE FIRMWARES DE ELEMENTOS IP ACTIVOS	1	global	10	10
04	DEPURACIÓN DE INFORMACIÓN EN SERVIDOR DE COMUNICACIONES	1	global	10	10
				TOTAL	**$ 50,00**

Las actividades descritas en la tabla mostrada, se realizarán cada 3 meses con el costo indicado en la misma.

6.4 COSTOS DE MANO DE OBRA

Para realizar los trabajos en el liceo del valle, se contará con dos clases de mano de obra, estos son: técnico-especializada y general.

Mano de obra técnico-especializada.-

La parte técnica a desarrollarse, será realizada directamente por el personal especializado, el mismo que certificará el buen funcionamiento y configuración de los equipos.

En la tabla 6.8, se puede observar el detalle del costo de la mano de obra técnico-especializada.

Tabla. 6.9. Mano de obra técnico-especializada

ÍTEM	DESCRIPCIÓN	CANT.	UDM	PRECIO UNITARIO	PRECIO TOTAL
01	SERVICIO DE INSTALACION Y CONFIGURACION DE FIREWALL.	6	uni	30	180
02	SERVICIO DE AFINAMIENTO/TUNNING/CONFIGURACION DE EQUIPOS PC.	1	uni	294	294
03	CONFIGURACIÓN DE SERVIDOR DE COMUNICACIONES	1	uni	800	800
				TOTAL	**$ 1.274,00**

Mano de obra general.-

La mano de obra general, contempla el montaje de los equipos, instalación de puntos eléctricos, así como de datos, tendido de cable, canaletas y demás accesorios mínimos.

Este rubro se lo puede observar en la tabla 6.9

Tabla. 6.10. Mano de obra técnico-especializada

ÍTEM	DESCRIPCIÓN	CANT.	UDM	PRECIO UNITARIO	PRECIO TOTAL
01	MANO DE OBRA	8	global	122,8125	982,5
				TOTAL	**$ 982,50**

6.5 ANÁLISIS DE SENSIBILIDAD

Luego de haber obtenido los valores que constituyen el monto total de la implementación del sistema en el liceo del valle, se tiene como resultado lo que en la tabla 6.10 se detalla.

Tabla. 6.11. Resumen, monto total de proyecto

ÍTEM	DESCRIPCIÓN	CANT.	UDM	PRECIO UNITARIO	PRECIO TOTAL
01	EQUIPOS PRINCIPALES	1	global	6095,74	6095,74
02	ELEMENTOS SECUNDARIOS	1	global	2843,55	2843,55
03	MANTENIMIENTO TRIMESTRAL	1	global	50	50
04	MANO DE OBRA TÉCNICO-ESPECIALIZAD	1	global	1274	1274
04	MANO DE OBRA GENERAL	1	global	982,5	982,5
				TOTAL	**$ 11.245,79**

Otra referencia importante para llevar a cabo el análisis financiero correspondiente del proyecto, constituye el registro de ingresos del liceo del valle, con énfasis en el monto destinado para solventar y recuperar gastos generados por la implementación del sistema.

Tomando como base el año lectivo, se ha considerado conveniente cobrar un valor adicional en la matrícula de inicio de año, correspondiente al valor de internet inalámbrico, como servicio principal para los alumnos de la institución.

Dicho monto ha sido fijado en un valor de 15 USD por cada alumno, tomando como referencia el rubro correspondiente a la inversión total inicial. Al realizar un estudio de los servicios implementados, se desprende que se fijará porcentajes diferentes de costos, entre las secciones de preescolar, primaria y secundaria ya que no es de igual magnitud la ocupación de los servicios. Para las secciones de preescolar y primaria, se les cargará un porcentaje del 20% del valor a pagar es decir 8 USD anuales

Cálculo de TIR, VAN y Período de recuperación.

La inversión total generada por la implementación del sistema en el liceo del valle, asciende a un valor de 11.245,79 USD, para el cual se calculará el TIR, así como el VAN, con una tasa de interés del 10%.

Tabla. 6.12. Análisis económico

Período	Flujo de Fondos
2008	-$ 11.245,79
2009	$ 4.140,00
2010	$ 4.140,00
2011	$ 4.140,00
2012	$ 4.140,00

TIR: 18%
VAN: $ 1.877,45

El flujo de fondos que se obtendrá anualmente durante los años de recuperación, es de 4140 USD, el mismo que ha sido calculado a partir de los valores que serán cobrados a los estudiantes como un adicional al valor de la matrícula, como se lo explicó en el numeral 6.5.

Como se puede observar en la tabla 6.11, el período de recuperación de la inversión es de 4 años, con una tasa interna de retorno (TIR) de 18% y un Valor Actual Neto (VAN) de 1.877,45 dólares, con lo cual, la inversión del proyecto de tesis será recuperada hasta el 2012.

CAPÍTULO 7

IMPLEMENTACIÓN

7.1 CONFIGURACIÓN DE EQUIPOS

7.1.1 Servidor y servicios

Para empezar a implementar la red objeto de este proyecto, se detallará a continuación la configuración del servidor, cuyas características tanto de hardware como software fueron dimensionadas en capítulos anteriores.

Se escogió la distribución Centos 4.6, después de evaluar el tipo de servicio que se requiere y sus respectivas funcionalidades como paquete destinado a aplicaciones de servidor empresarial.

Los pasos a seguir detalladamente desde donde conseguir el software de distribución libre, como descargarlo y el procedimiento de instalación se encuentran detallados en el capítulo 2, sección 2.2, se muestran pantallas ilustrativas que indican paso a paso las opciones a escoger.

Acorde a criterios de diseño analizados en el capítulo 5, se concluyó las características del equipo a ser usado como servidor en el apartado 5.2.2.

Con ambos criterios definidos, respecto al hardware y software Centos 4.6, se procede a la configuración de servicios, proceso detallado en el capítulo 2 apartado 2.3, mostrando paso a paso con pantallas, la configuración y levantamiento de servicios requeridos.

Para la conexión del servidor dentro de la red se procedió a la instalación del cableado estructurado de los sectores donde se requiere el servicio cableado.

Figura. 7.1. Rack y patch panel de los nodos cableados.

Se empleo un switch Dlink DES1024D para el rack, desde este punto se conecta el servidor de aplicaciones que ya fue previamente configurado.

Figura. 7.2. Conexión del servidor de comunicaciones al patch panel de la red cableada

7.1.2 Red WLAN

Los equipos de red correspondientes a ser instalados, contemplan los Access Point, en el capítulo 5 apartado 5.2.5, se ha elegido el tipo de AP a ser empleado, un D-Link DWL-2100AP.

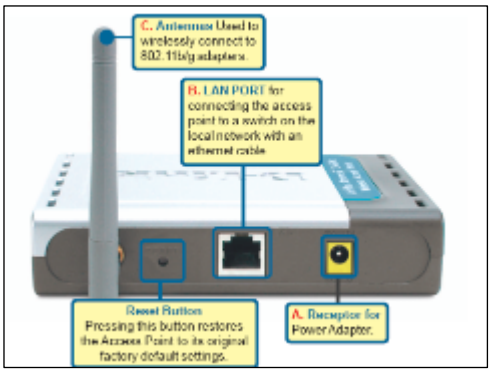


Figura. 7.3. Vista posterior DWL-2100AP

Antes de montar los equipos es necesario configurarlos y hacer pruebas locales para garantizar su correcto funcionamiento, se requiere de un computador con tarjeta de red, un browser y un cable UTP directo.

Se conecta la PC, mediante el cable UTP al Access Point.

En la PC, se ingresa Panel de Control y luego a Conexiones de Red.

En Conexiones de Red, se debe asegurar que todas las redes estén desactivadas, con excepción de la Red cableada (Conexión de Área Local).

En Conexión de Área Local dar clic derecho y se muestra la siguiente pantalla.

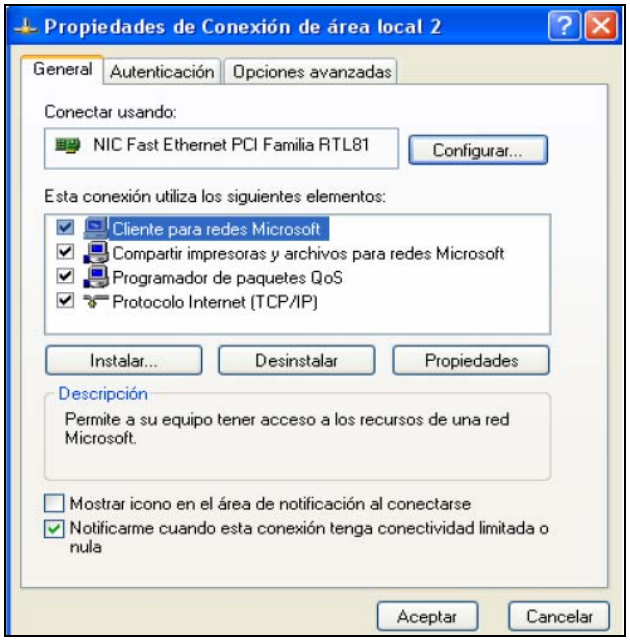


Figura. 7.4. Configuración de IP

Clic en el botón propiedades y colocamos como dirección IP de la PC cualquier dirección que se encuentre en el rango de la red 192.168.0.0 /24 ya que la dirección por defecto del access point corresponde a 192.168.0.50/24:

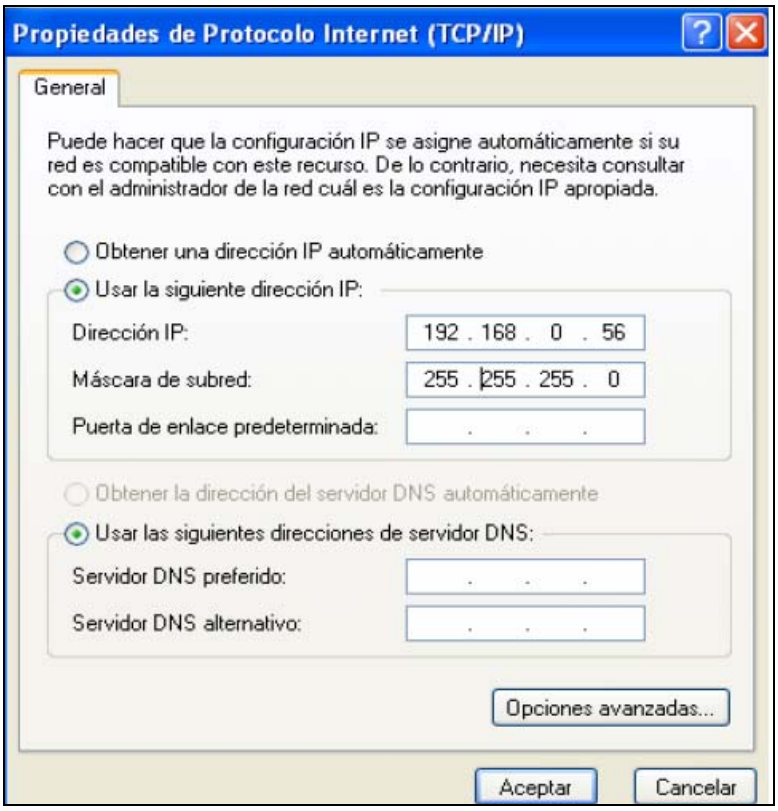


Figura 7.5. Vista posterior DWL-2100AP

Una vez que ambos dispositivos estén en la misma red, se puede acceder desde cualquier browser a configurar el Access Point.

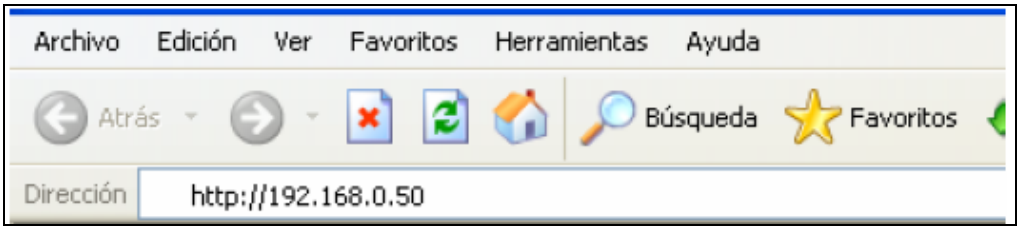


Figura. 7.6. Dirección IP por defecto del DWL-2100AP

Una vez que se ingresa al Access Point se visualiza la siguiente pantalla:

Figura. 7.7. Datos de usuario y contraseña

El usuario viene dado por defecto al igual que la dirección IP, es admin, y la contraseña no esta definida, así que basta con dar Enter para acceder a la administración

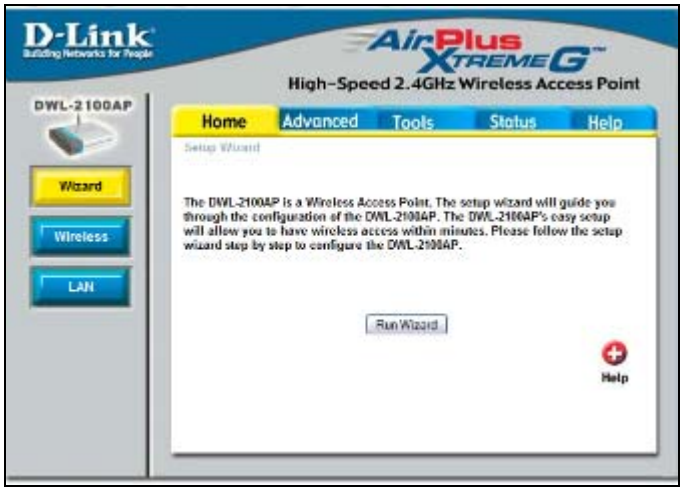


Figura. 7.8. Primera pantalla de configuración de AP

Luego de ingresar al menú de configuración, se puede cambiar la dirección IP por una dirección que esté dentro del segmento de la red local en la cual va a trabajar el AP. El cambio de Dirección se realiza en la opción LAN, para este access point que corresponde a

Administración, la dirección IP es la 192.168.100.10/24, dentro de los campos indicados en la figura 7.7.

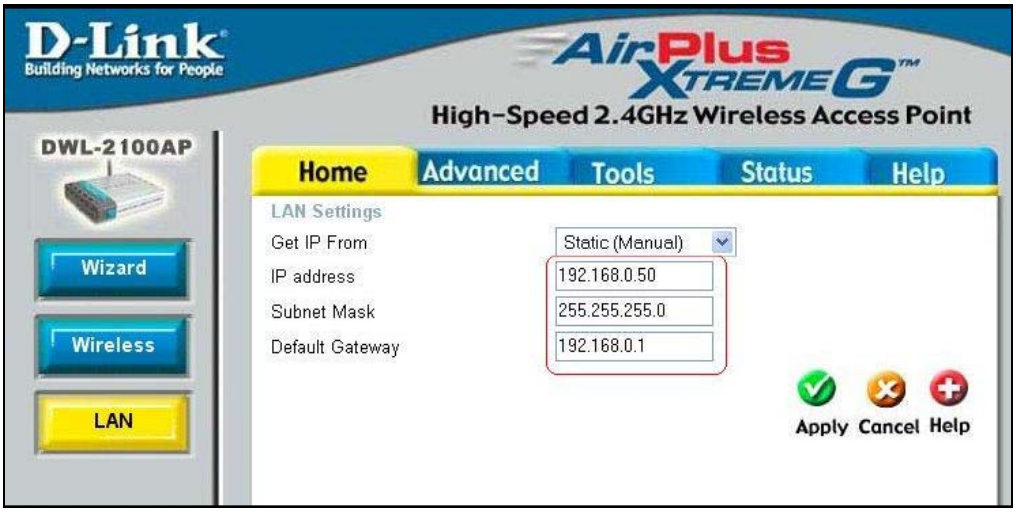


Figura. 7.9. Configuración de parámetros LAN

Posteriormente se procede a reiniciar el equipo y a integrarlo a la red para administrarlo con un PC inalámbricamente, se recuerda que dentro de la PC destinada para configurar el AP, es necesario setear parámetros de IP para que se encuentren en la misma red.

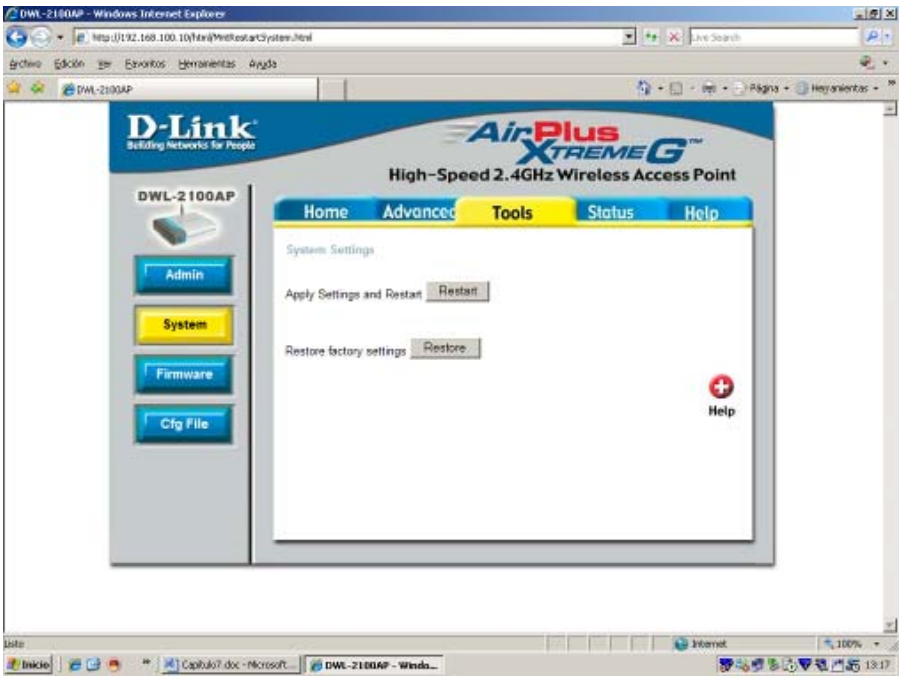


Figura. 7.10. Reinicio del equipo para aplicación de cambios.

Entre algunas funciones del DWL-2100 AP existe la actualización de versión del firmware cargando el archivo desde una ubicación específica dentro de la red a la que pertenece

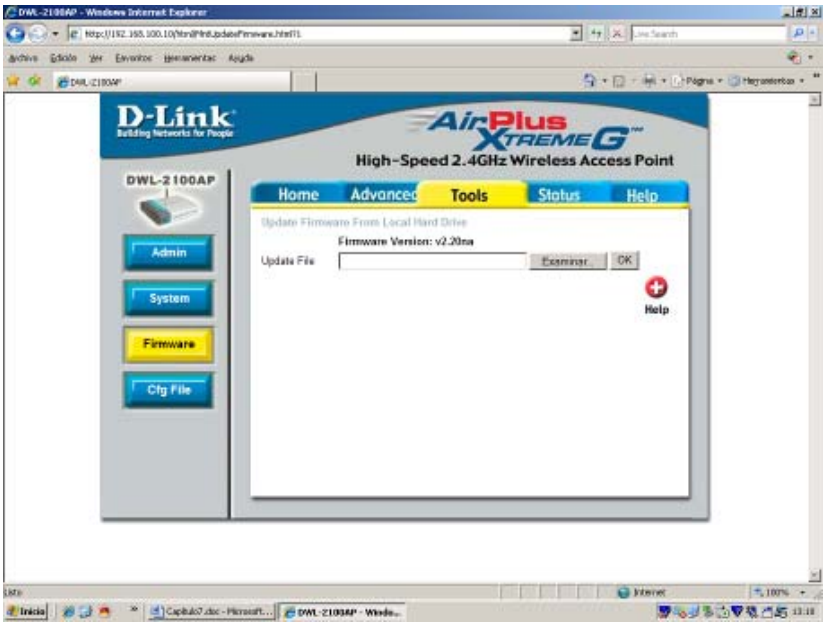


Figura. 7.11. Actualización del firmware del AP

Es posible además realizar un respaldo del archivo de configuración, en caso de que se requiera resetear el equipo y volver a cargar dicha información o se requiera colocar el respaldo en otro AP como referencia.

Figura. 7.12. Respaldo del archivo de configuración.

Dentro de la pestaña STATUS se puede observar un resumen de información del equipo con datos generales de configuración LAN y WLAN.

Figura. 7.13. Información LAN y WLAN del AP.

En la opción STATS se visualiza estadísticas de tráfico de red soportado por el Access Point.

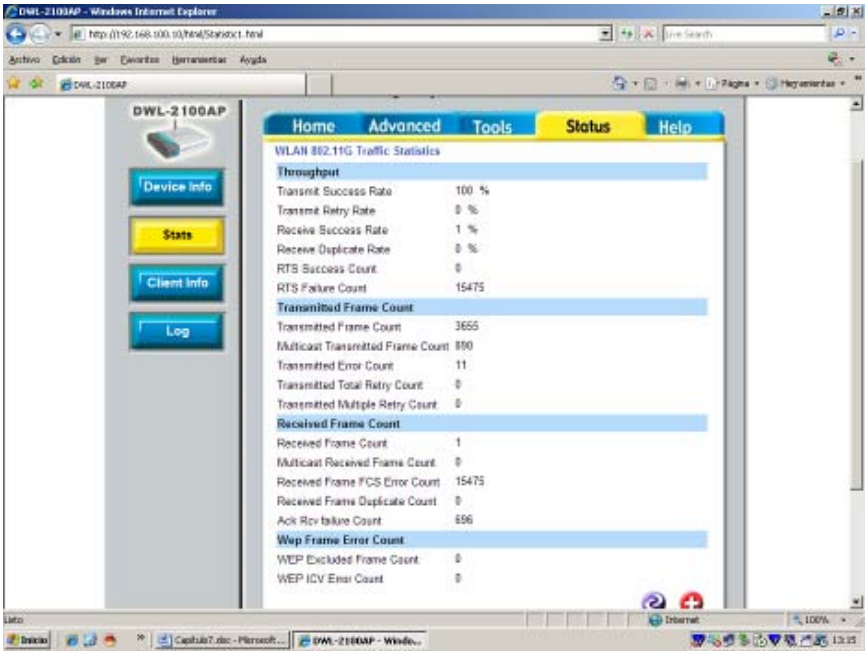


Figura. 7.14. Estadísticas de tráfico de red.

En la pestaña de Client Info se puede visualizar los usuarios de la red conectado en el momento al AP, con información de direcciones MAC, SSID, Autenticación entre otros.

Figura. 7.15. Visualización de clientes conectados al AP

En la pestaña Log se indica un historial de los sucesos acontecidos en el AP y el tipo de acceso si es por parte del cliente o desde el servidor, un ligero mensaje de la actividad y la fecha.

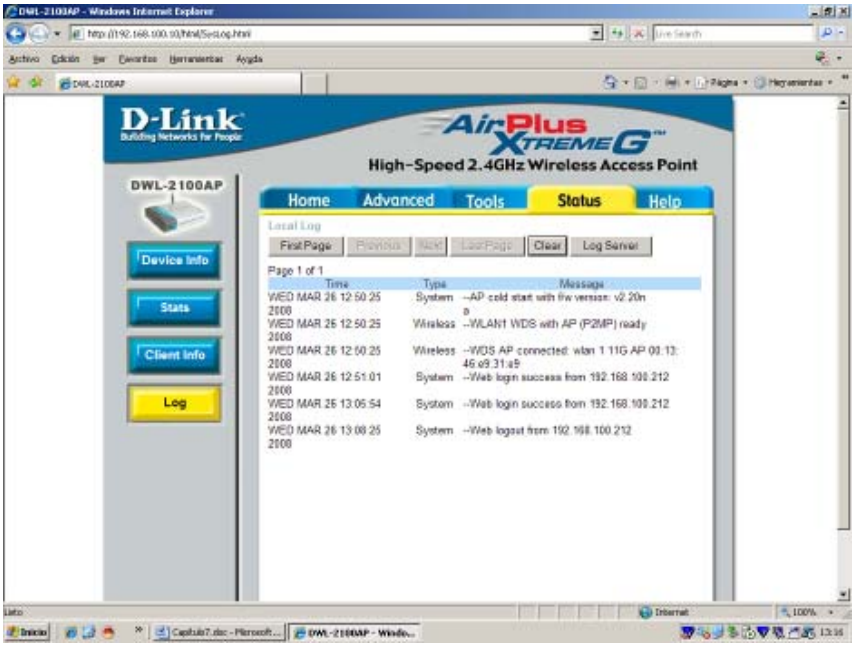


Figura. 7.16. Histórico de los eventos del AP

Configuración Wireless

El objeto más importante de configuración corresponde al servicio de red inalámbrica, dentro de la opción Wireless del AP. Existen 5 pestañas correspondientes a la sección inalámbrica del AP.

En la primera pestaña HOME, se encuentran opciones como:

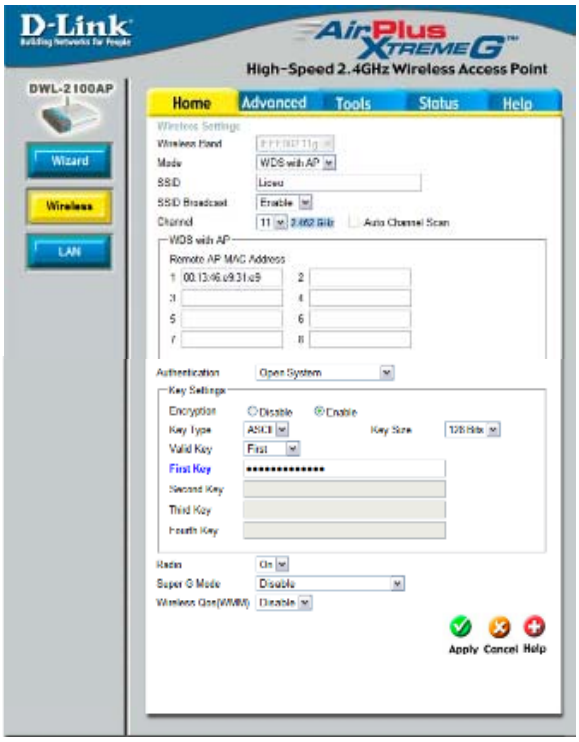


Figura. 7.17. Parámetros de configuración Wireless

El modelo DWL-2100 AP puede ser configurado para trabajar en 5 diferentes modos:

- Access Point Wireless
- Cliente Wireless
- Bridge Wireless
- Bridge Punto-Multipunto
- Repetidor

Se ingresa al Menú de configuración y en la opción Wireless se selecciona WDS with AP.

Esta modalidad de configuración se utiliza cuando se requiere hacer un puente inalámbrico o bridge con una red ubicada en un punto remoto, en la red remota se necesita un equipo similar que soporte esta modalidad, además en este modo los Access

Point no pierden la cualidad de Access Point. Dicha función fue escogida para establecer comunicación entre los 5 APs colocados, para que se comuniquen entre ellos y a la vez los usuarios wireless también puedan acceder al mismo.

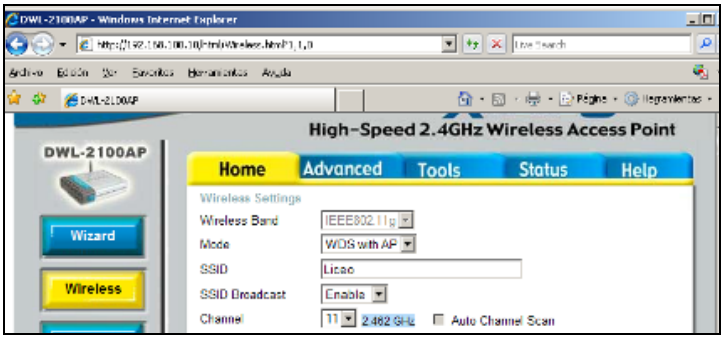


Figura. 7.18. Modo de funcionamiento del AP

Es necesario saber la dirección mac address del equipo remoto y configurarla en la opción 1, Remote mac address.

En el equipo remoto es necesario hacer el mismo proceso pero digitando la dirección mac address del access point local. Ambos equipos deben estar configurados en el mismo channel, en este caso 11.

Figura. 7.19. Configuración de bridge con otro AP entre MACs

Configuración avanzada, rendimiento:

Wireless Band : Permite seleccionar entre 802.11 g o 802.11g y b.

Frequency: la frecuencia permanece en 2.437GHz.

*Channe*l: Selección de canales entre 1 y 11. Para el caso el canal de trabajo escogido *para los AP es 11.*

Data Rate: Las tasas de datos varían entre valores de: Auto, 1Mbps, 2Mbps, 5.5Mbps,

6Mbps, 9Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps.

Beacon Interval : Beacons son paquetes enviados por una access point para conectarse a la red. Especificar un valor de intervalo de beacon. El valor por defecto 100 es recomendado.

DTIM : 3 es el valor usado por defecto, es una cuenta regresiva informando a los clientes de la próxima ventana para escuchar mensajes de broadcast y multicast.

Fragment Length: Especificada en bytes, determina que paquetes serán defragmentados. Paquetes que excedan el 2346 byte seteado, será fragmentado antes de la transmisión.2346 es el valor por default.

RTS Length El valor de este campo por defecto está seteado en 2,346, si son encontradas inconsistencias en el flujo de datos, solo menores modificaciones al valor del rango entre 256 y 2,346 son recomendados.

Transmit power Permite escoger la potencia, media potencia (-3dB) o cuarto de potencia (-6dB) u octavo de potencia (-9bB).

Figura. 7.20. Parámetros de configuración WLAN

Los siguientes parámetros también deben ser configurados

SSID: Nombre de la red inalámbrica, para el caso es Liceo.

SSID Broadcast: Con esta opción configurada en Enable es posible detectar el nombre de la red configurada en SSID.

Channel: Seleccionar un canal que no esté utilizado por otro AP, para este access point que es el de Administración es 11.

Dentro de la opción *Tools* se setea el password para el administrador cada vez que ingrese al equipo vía browser.

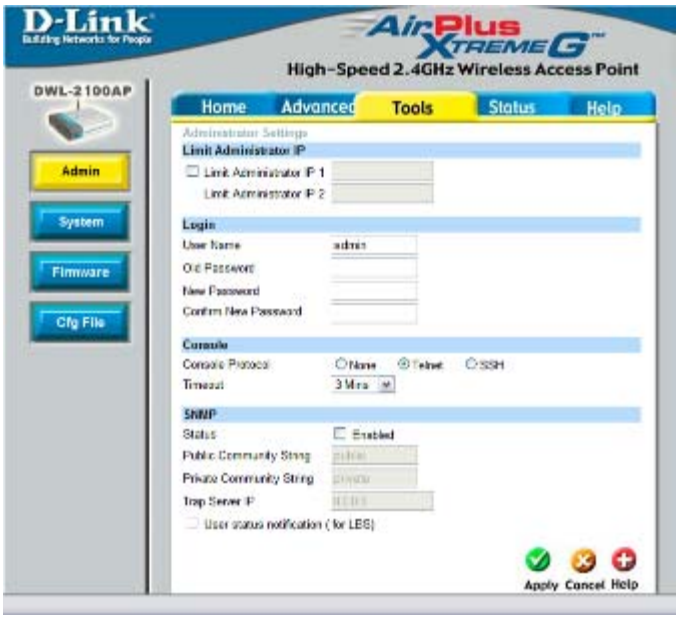


Figura. 7.21. Parámetros de configuración de password administrador

Dentro de la pestaña *Status* se despliega un cuadro de información general del equipo, es decir todos los parámetros configurados anteriormente para su conexión ethernet y la parte de wireless, además de la dirección MAC del equipo y la versión del firmware actual.

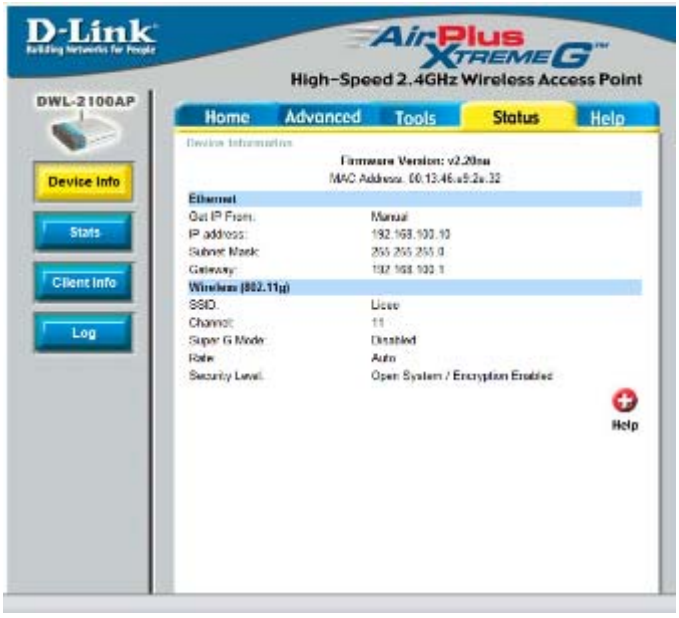


Figura. 7.22. Resumen de los parámetros configurados en el AP

Por último está la pestaña *Help* donde se lista todas las pantalla de ayuda a las que se puede acceder.

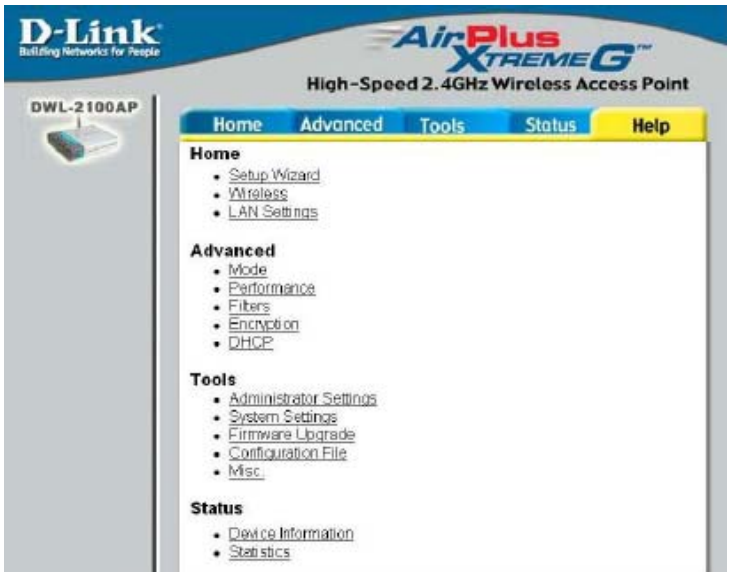


Figura. 7.23. Lista de link de ayuda del equipo

Existe la posibilidad de emplear el software AP Manager que es una herramienta conveniente para administrar de la red desde una computadora central. Con el AP Manager no hay necesidad de configurar los equipos cada uno por separado. Este programa es para conocimiento general ya que para el caso de la implementación en el Liceo del Valle se configuraron uno a uno los equipos con la finalidad de realizar pruebas entre los puentes establecidos en los APs.

7.2 INSTALACIÓN DE EQUIPOS DE RED WLAN

Una vez configurados los equipos de procede a su instalación, los equipos a instalarse son los siguientes:

-5 cajas Beaucoup para intemperie

-5 antenas D-link de 8dBi

-5 fuentes de poder

-5 soportes de antenas

-Tornillos

Figura. 7.24. Cajas para intemperie montadas con antenas para AP

Cada caja tiene una ubicación estratégica en la azotea de las diferentes secciones del colegio, 1 AP va en el balcón de administración, 1 AP va en la azotea de la sección primara, en configuración bridge con el AP de administración y 3 AP en la azotea de la sección secundaria, 1 al lado izquierdo, otro al lado derecho y uno en el centro, también en configuración bridge con el AP de la sección primaria, para obtener mayor cobertura.

Cada AP va en el interior de la caja con el cable de poder y el pigtail para la antena.

Figura. 7.25. Cajas para intemperie con su respectivo AP

Una vez montados los Access Points, es necesario verificar por las luces de los leds frontales si el equipos está correctamente instalado, posteriormente se realizarán pruebas de funcionamiento de la red.

7.3 CONFIGURACIÓN DE LOS EQUIPOS DE USUARIO

7.3.1 Tarjetas de red inalámbricas

Una vez instalados los Access Point, el siguiente paso para la red inalámbrica es instalar y configurar los equipos de recepción en las computadoras de los usuarios, para ello se ha escogido tarjetas inalámbricas Dlink, anteriormente analizadas y explicadas en el capítulo 5 numeral 5.2.3. Dependiendo del equipo de cada usuario pueden ser tarjetas PCI para desktops o USB para laptops.

Por lo general en una laptop se encuentran ya instaladas las tarjetas de red inalámbricas, y para el caso del liceo los principales usuarios de este servicio son desktops ubicadas en la zona posterior del colegio.

Para instalar las tarjetas de red hay que apagar el computador, abrir el case y tener acceso al interior del CPU, en la placa bse , donde están las tarjetas de expansión , hay varias ranuras , donde se va a insertar la tarjeta , buscando una que este vacía, colocarla con cuidado, y asegurarse de que quede insertada correctamente. Poner el tornillo y cerrar la caja. La instalación es bastante sencilla. Cuando se encienda el PC detectará un nuevo dispositivo de red y se creará la correspondiente conexión de red (Windows XP) que es el sistema operativo de todas las PCs del Liceo del Valle.

Figura. 7.26. Tarjetas inalámbricas para desktop

Las tarjetas empleadas son las PCI, para instalarlas hay que retirar el case del CPU y colocarlas en los slots PCI destinados para el fin, estas tarjetas deben ser las DLINK DWL-G520

Figura. 7.27. Tarjetas inalámbricas para desktop

7.3.2 Equipos para VoIP

En esta sección se va a configurar los equipos para VoIP que son la central telefónica DVX1000, el gateway DVG 7022S y los teléfonos IP.

Central telefónica

La central telefónica se configura vía browser, se accede mediante la IP que es la 192.168.100.60, una vez que podemos acceder es posible configurar parámetros de IP para setear una IP que pertenezca a la red. La primera pantalla en aparecer es la de *Home*

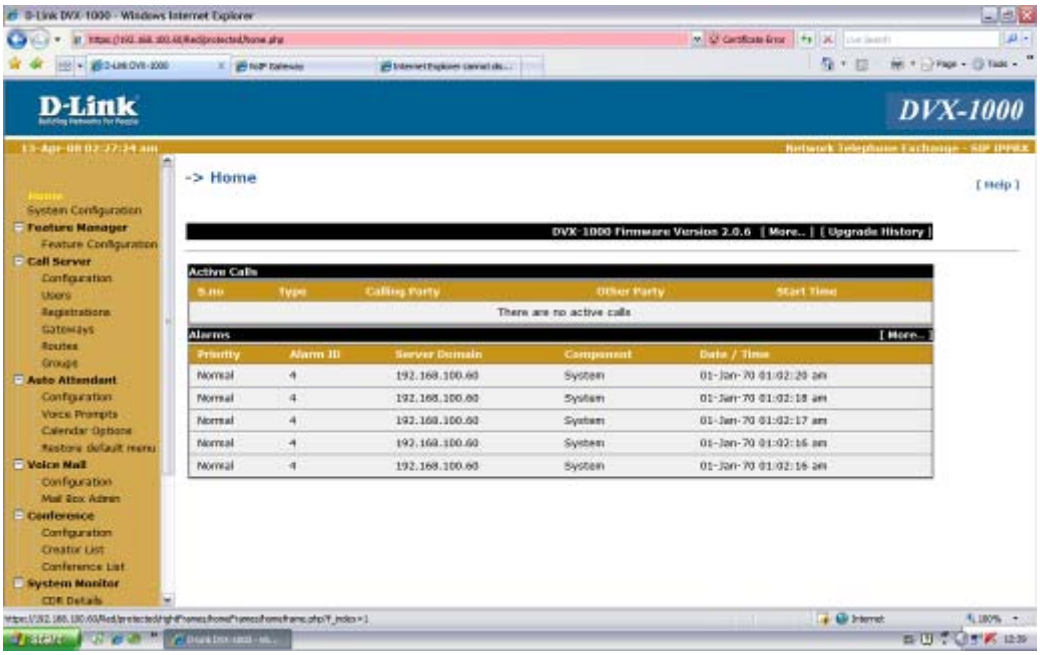


Figura. 7.28. Página de inicio de DVX-1000

Se despliega un menú al lado izquierdo de la pantalla que corresponde a las opciones para configurar el equipo, se analizará los ítems necesarios para el funcionamiento de la central.

System Configuration

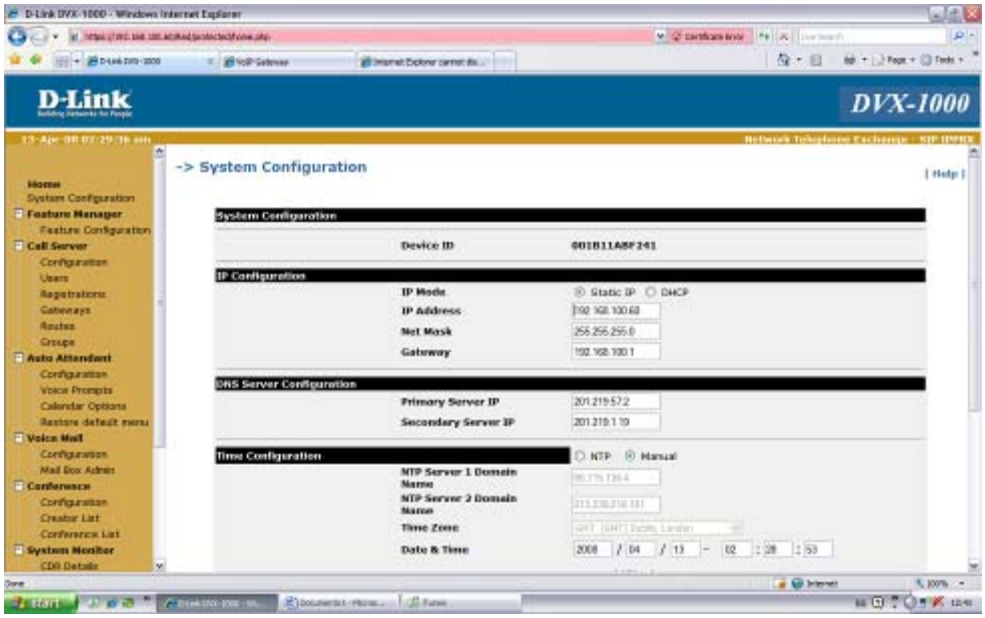


Figura. 7.29. Configuración del sistema de DVX-1000

En esta opción se encuentran los parámetros de configuración IP del equipo, si va a ser una dirección estática o asignada por DHCP, la máscara de red y la puerta de enlace.

Otra opción es la configuración de DNS con la opción de servidor primario y secundario.

La opción de *time configuration* indica si es asignado por servidor NTP o manualmente, los factores automáticos vienen dados por defecto.

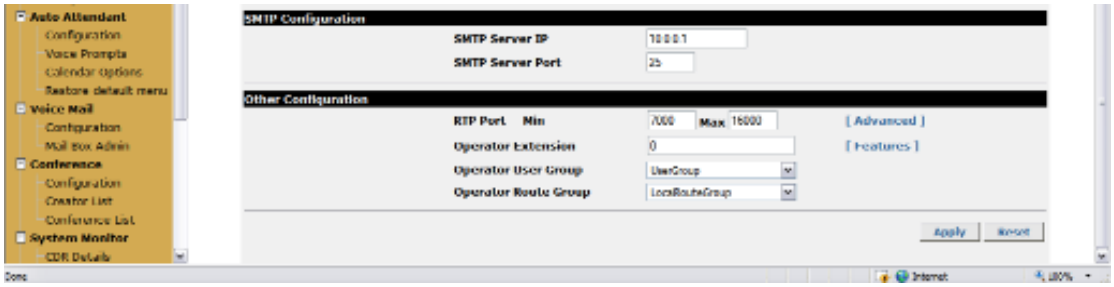


Figura. 7.30. Configuración del sistema de DVX-1000

La opción SMTP permite el ingreso de la IP y el puerto por el cual se va a acomunicar la central.

En otras configuraciones hay parámetros que no son susceptibles de configuración para este caso.

Feature Manager-Feature Configuration

Indica los parámetros de configuración de las características de la central como desvío de llamadas, envío al correo de voz, retorno de llamadas, etc

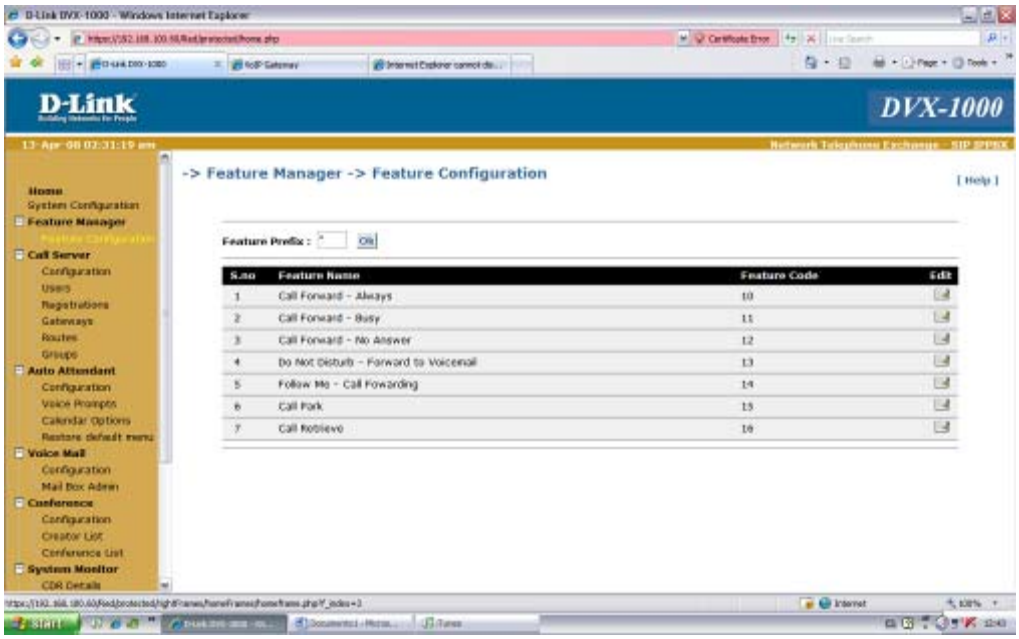


Figura. 7.31. Administrador de características de DVX-1000

Call Server Configuration

Al visualizar la pantalla del servidor de llamadas se exhibe información ya configurada en la central en las opciones anteriores, para el caso este parámetro no requiere configuración extra.

Figura. 7.32. Administrador de características de DVX-1000

Call Server –Users

Dentro de este parámetro se crean y configuran los usuarios de cada extensión de la central y los privilegios de cada de ellas, si son llamadas internas, locales, regionales, celulares o internacionales, y se va anidando entre ellas para llegar a un nivel de un usuario con todos los permisos del caso.

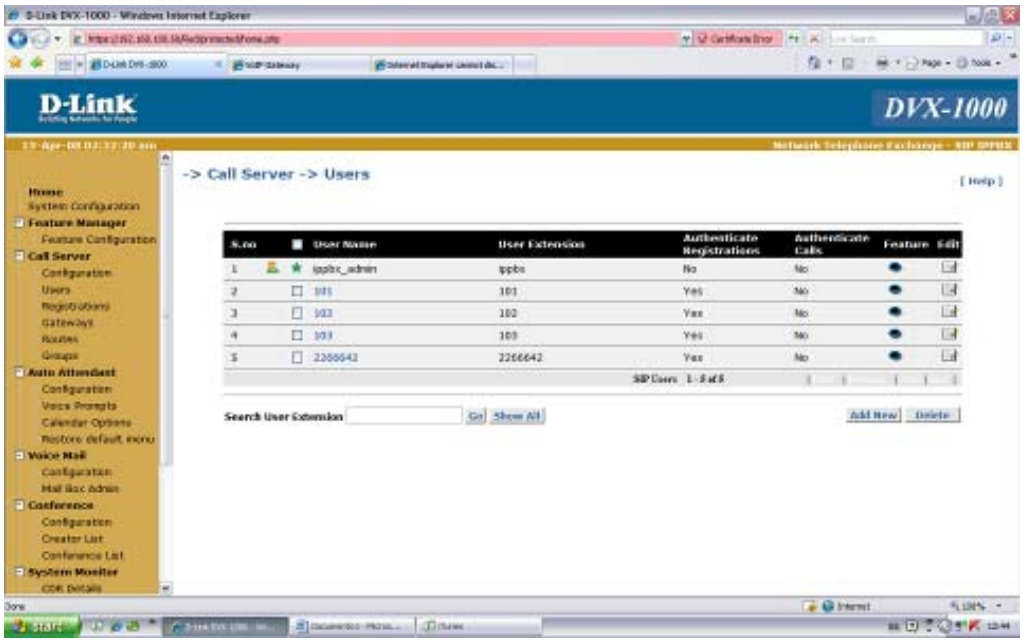


Figura. 7.33. Configuración de usuarios de DVX-1000

Para editar los parámetros de cada usuario basta con dar clic en la opción editar correspondiente de cada usuario, se visualizará la siguiente pantalla:

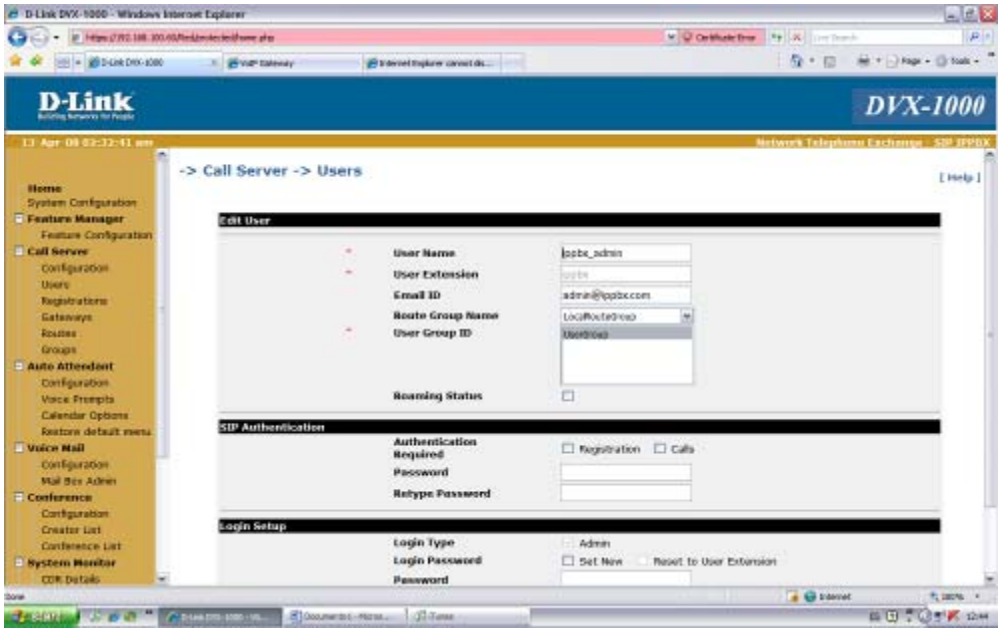


Figura. 7.34. Configuración de usuarios de DVX-1000

Se puede setear parámetros como nombre de usuario, asignarle número de extensión, identificar a que grupo de privilegios establecidos pertenece y contraseñas en general.

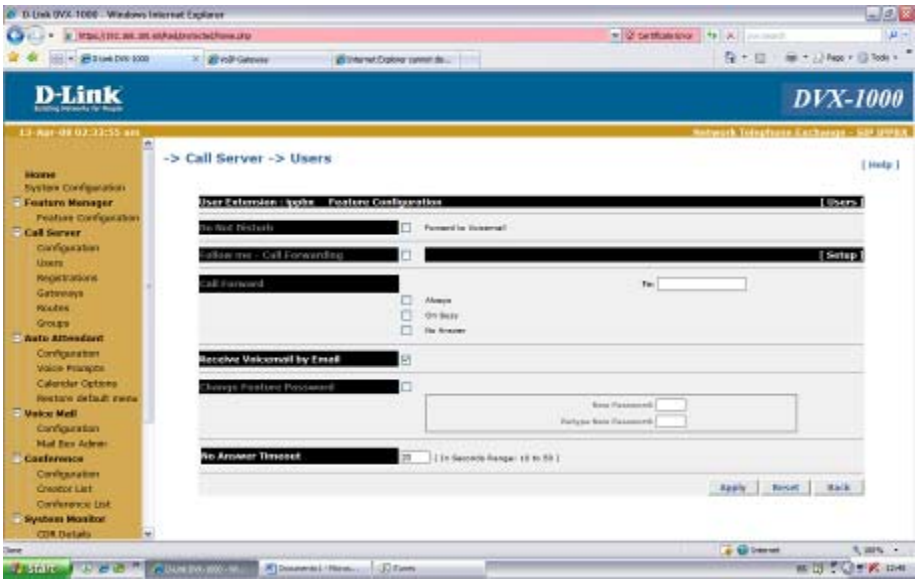


Figura. 7.35. Configuración de usuarios de DVX-1000

Registrations

En esta opción de la central se registran las extensiones para su autenticación y el tiempo en el que caduca esta registración.

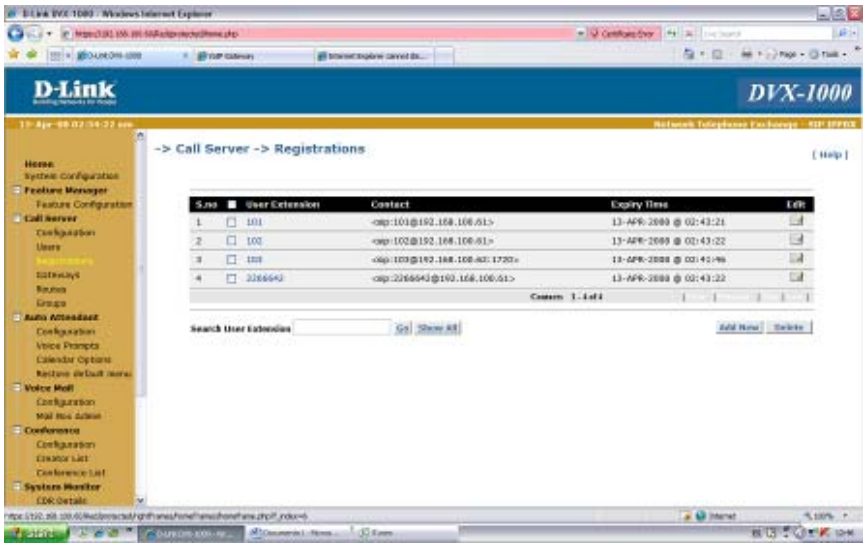


Figura. 7.36. Registro de usuarios en la central DVX-1000.

Gateway

En esta parte de la configuración se indica las puertas de enlace de la central telefónica, que para nuestro caso son 2, por una parte se comunica con la intranet y los teléfonos análogos a través del ruteador gateway DVG-7022S y con el exterior con un proveedor de servicios VoIP el cual indica el dominio el cual debemos conectarnos y el ID que le corresponde para el protocolo SIP.

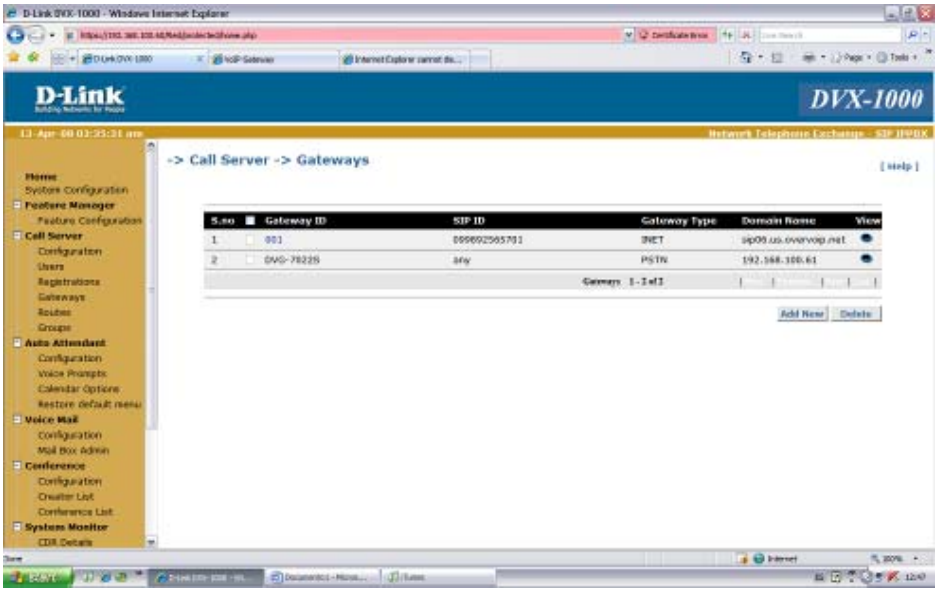


Figura. 7.37. Gateways usados por la central telefónica.

En la pantalla de inicio, en el botón de Add New, podemos ingresar cuantos gateways sean necesarios para el funcionamiento de la central IP, los parámetros que son requeridos para configurar un gateway a continuación

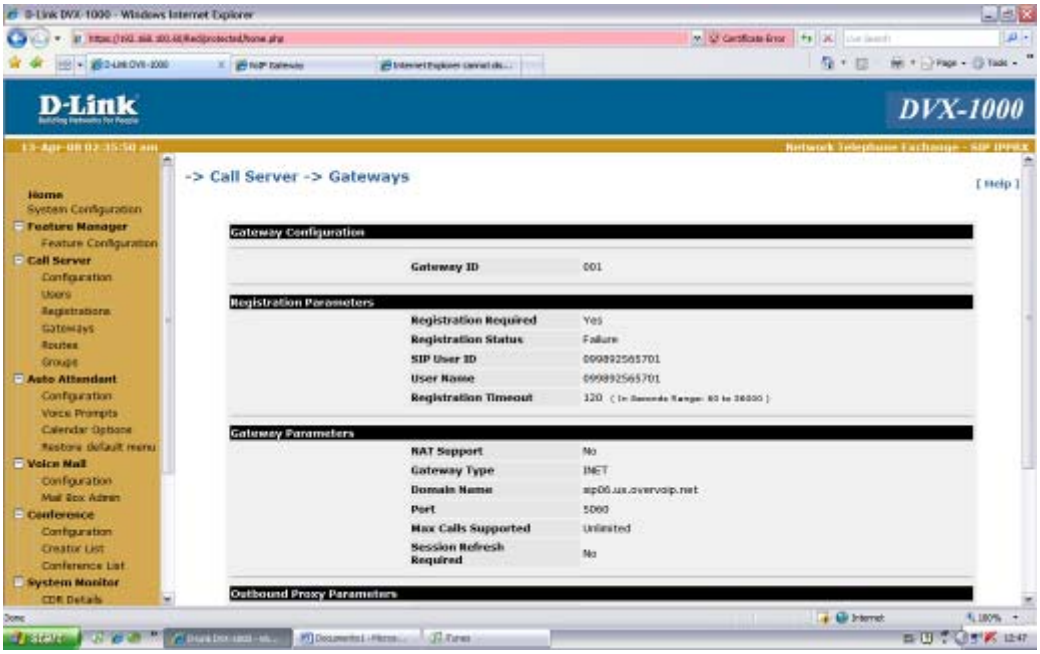


Figura. 7.38. Gateways usados por la central telefónica.

Para la configuración de una gateway se requiere un ID, registrarlo para que se autentique en la central y los datos entregados por el proveedor con el SIP ID y el user name, de que tipo es el gateway y soporta NAT el dominio, en este caso del proveedor de servicios y el puerto 5060 que por lo general es el puerto de VoIP, los demás parámetros no es necesario su configuración

Routes

En este item se configura las rutas que van a tomar los paquetes de VoIP dependiendo de las condiciones en las que sean seteadas y los permisos que se les otorgue.

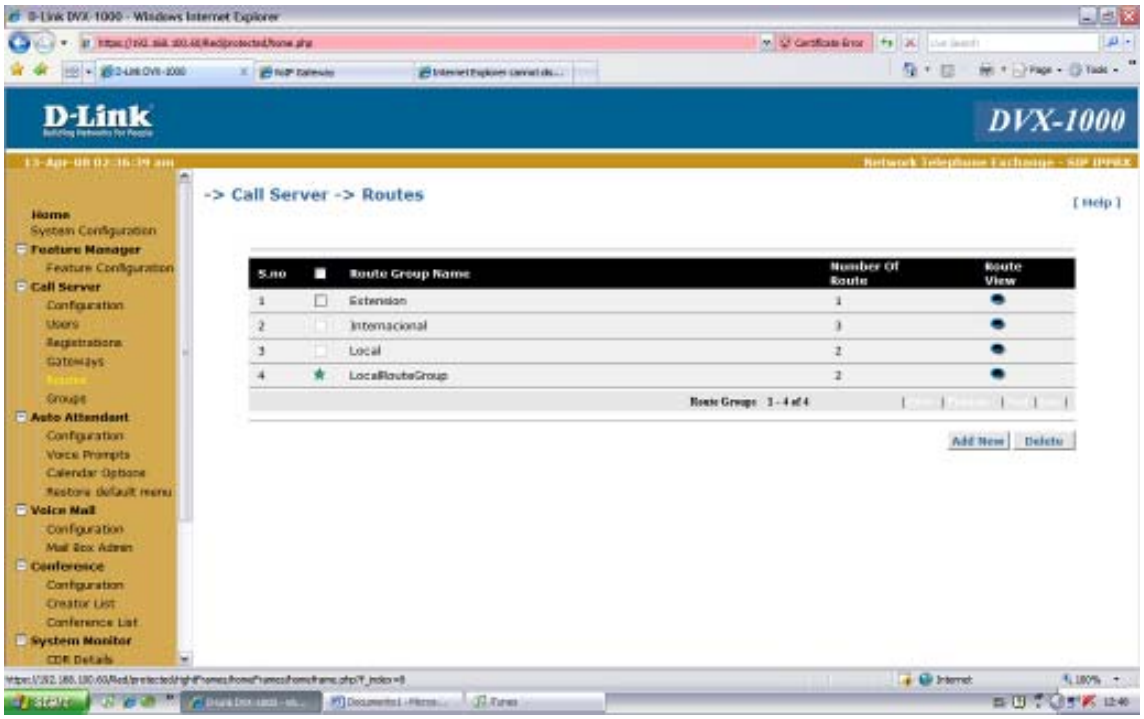


Figura. 7.39. Rutas usadas por la central telefónica.

Para configurar las rutas de los paquetes que van a salir por el proveedor de servicios de VoIP es necesario introducir ciertos valores en los parámetros de las rutas como la prioridad , el número mínimo y máximo de dígitos , en este caso no se requiere dígitos de enmascaramiento porque no se desea salir a la red PSTN.

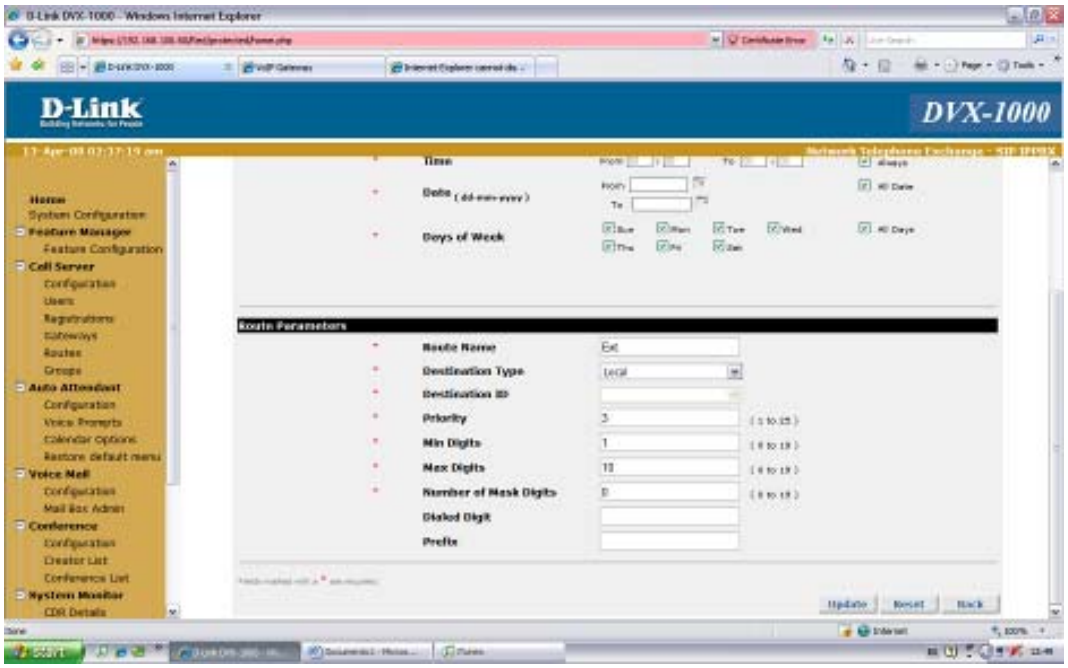


Figura. 7.40. Rutas usadas por la central telefónica.

Para el caso de las rutas que van a salir por la PSTN, en el botón de Add New se pueden editar los parámetros de cada ruta, e identificar a que grupo van a pertenecer, parámetro de tiempo de duración de la ruta, y la prioridad de la ruta, así como también el número mínimo y máximo de dígitos y los dígitos de enmascaramiento, es decir con que número se sale desde las extensiones para poder tener tono y realizar una llamada.

Por ejemplo, para una llamada a un convencional, al levantar el auricular marcamos el numero 9 y nos da tono, quiere decir que se marco 9240317, pero al momento de conmutar la llamada a la operadora local, esta no va a entender el número si lleva el 9 al inicio, entonces se debe enmascarar o eliminar el primer dígito para poder realizar la llamada y que la operadora local comprenda el número que se desea marcar.

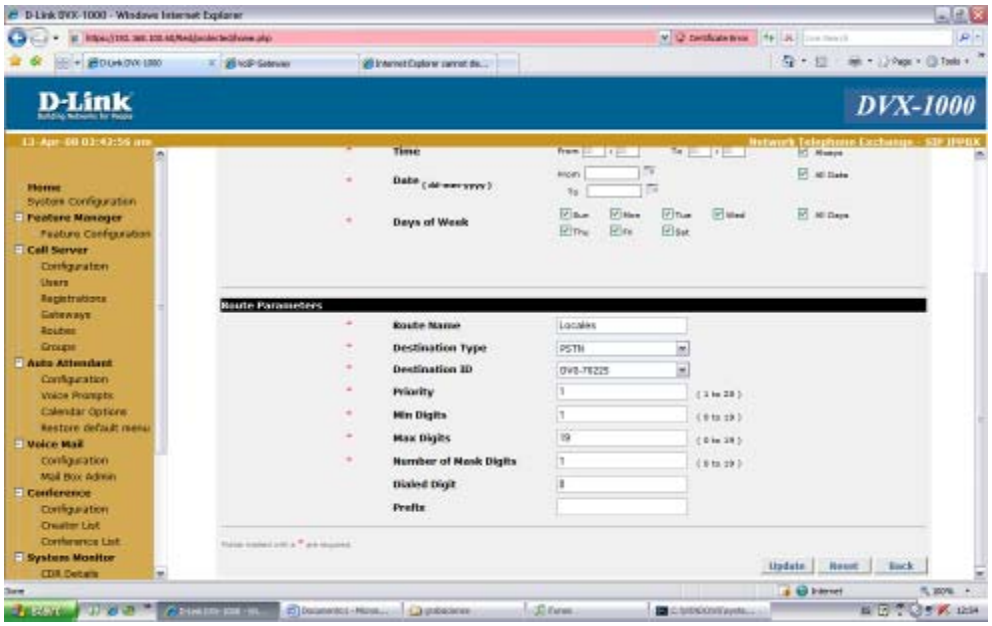


Figura. 7.41. Parámetros de configuración de una ruta en la central IP

Después de configurar las rutas de la central IP se visualiza la siguiente pantalla con información general de las rutas configuradas.

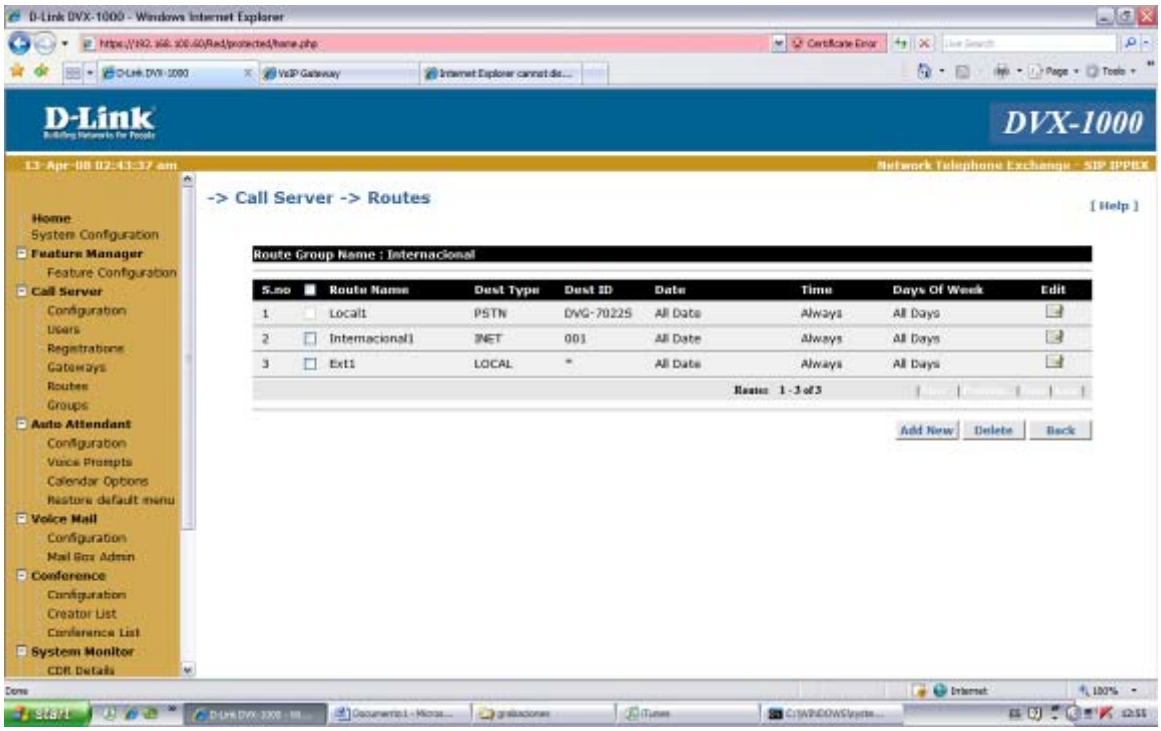


Figura. 7.42. Rutas configuradas en la central IP

Grupos

Los grupos pueden ser de 2 tipos:

- UserGroup

-HuntGroup

La opción User Group es específicamente usada para determinar los privilegios de las llamadas durante su recepción. Un usuario puede contestar una llamada desde otra extensión que pertenezca a su grupo. Se puede aumentar otro grupo en con el botón Add New. Para el HuntGroup se lo puede configurar en 4 modos: (First Only /Sequential /Parallel/Distributed). Cada grupo puede soportar un máximo de 20 usuarios y un usuario puede pertenecer máximo a 5 grupos.

Autoattendant

En este parámetro se puede configurar el número que corresponderá a la contestadora de la central IP, para este caso el 7000y además se pueden cargar archivos para les mensajes de saludo, de transferencia, de error de llamada, etc.

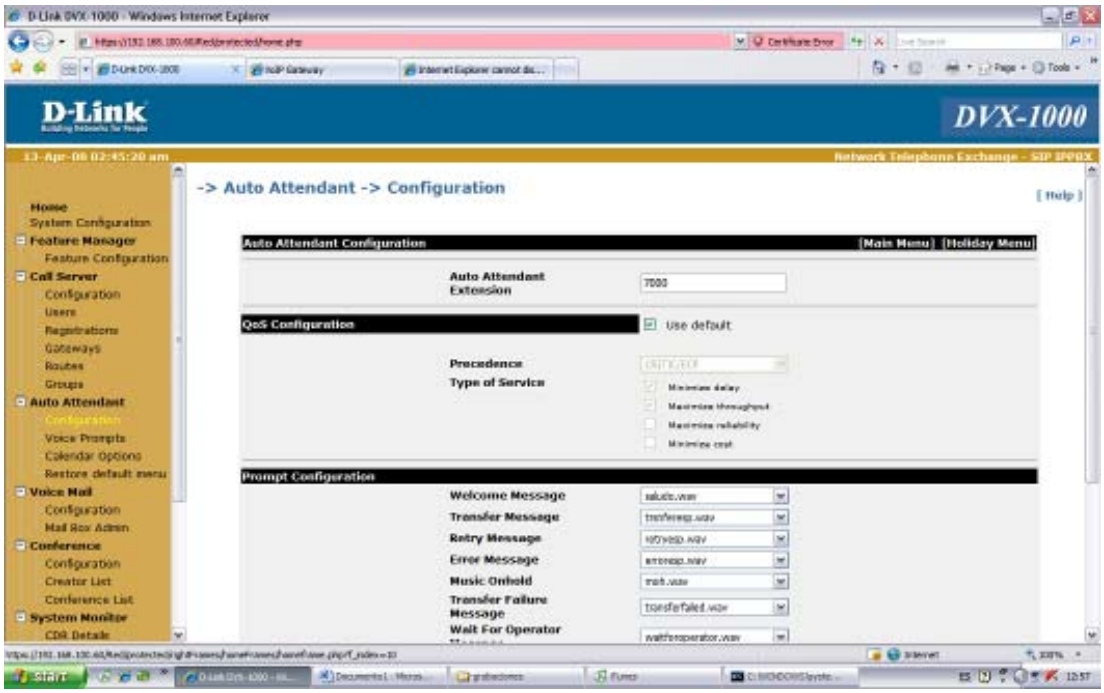


Figura. 7.43. Parámetros de configuración autoattendant

Para cargar estos nuevos archivos de voz, dentro de la central es necesario que los archivos sean guardados con el siguiente formato:

wav (8kHz, 8bit, mono, muLaw)

Max file size: 200 Kb

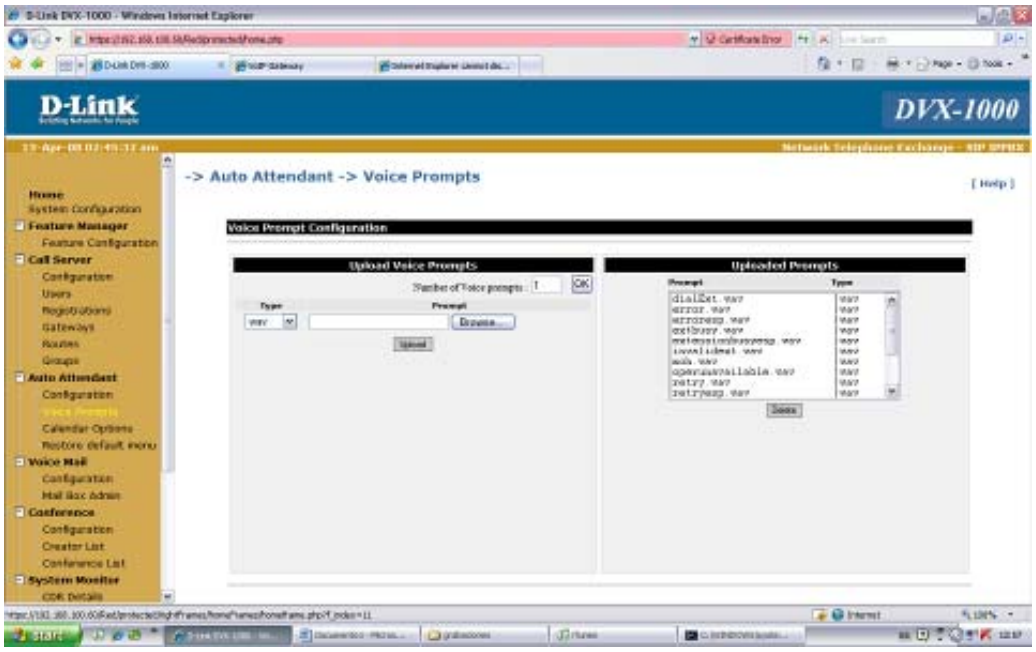


Figura. 7.44. Cargar archivos de voz en el autoattendant

Voice Mail

Aquí se va a configurar el número al que se llama para escuchar los mensajes dejados en el buzón de entrada y el espacio físico en KB del espacio que se le asignará a cada usuario para su buzón.

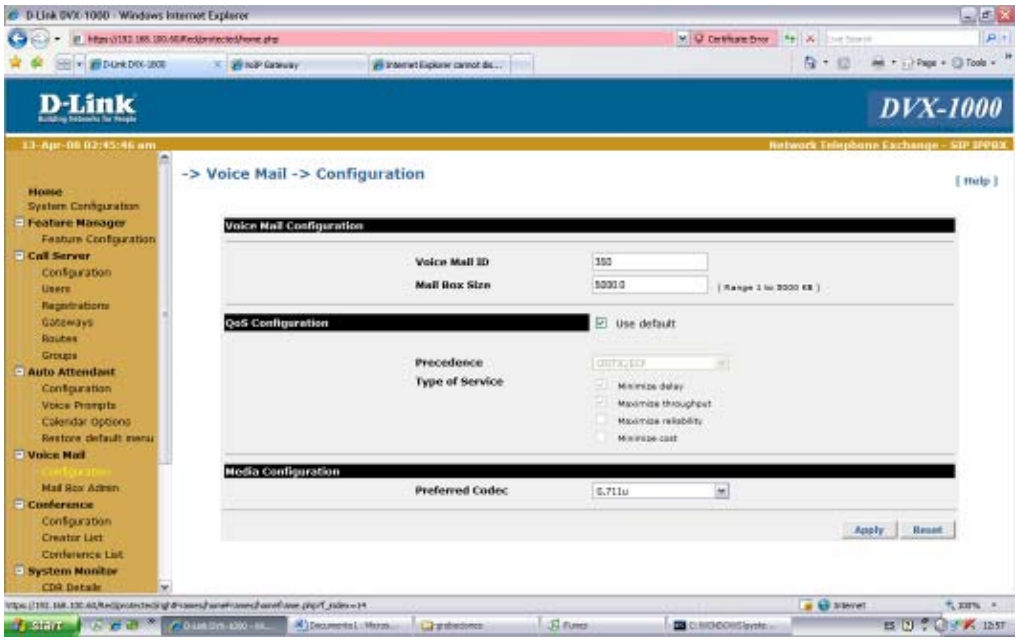


Figura. 7.45. Pantalla de configuración de Voice Mail

También es posible escoger si el campo de acción de esta configuración va dirigido a todos los usuarios, o se aplicará solamente a un grupo de usuarios.

Figura. 7.46. Pantalla de configuración de usuarios de Voice Mail

Los demás parámetros no son susceptibles de configuración para nuestra aplicación.

CONFIGURACION GATEWAY DVG 7022S

Para configurar el gateway Ruteador es necesario conectarlo por un puerto ethernet RJ45 a la central telefónica IP, en el puerto WAN se le asigna la IP siguiente a la central telefónica. Es decir la 192.168.1000.61 y a la central dentro de la configuración se le incluye como n puerto FXO.

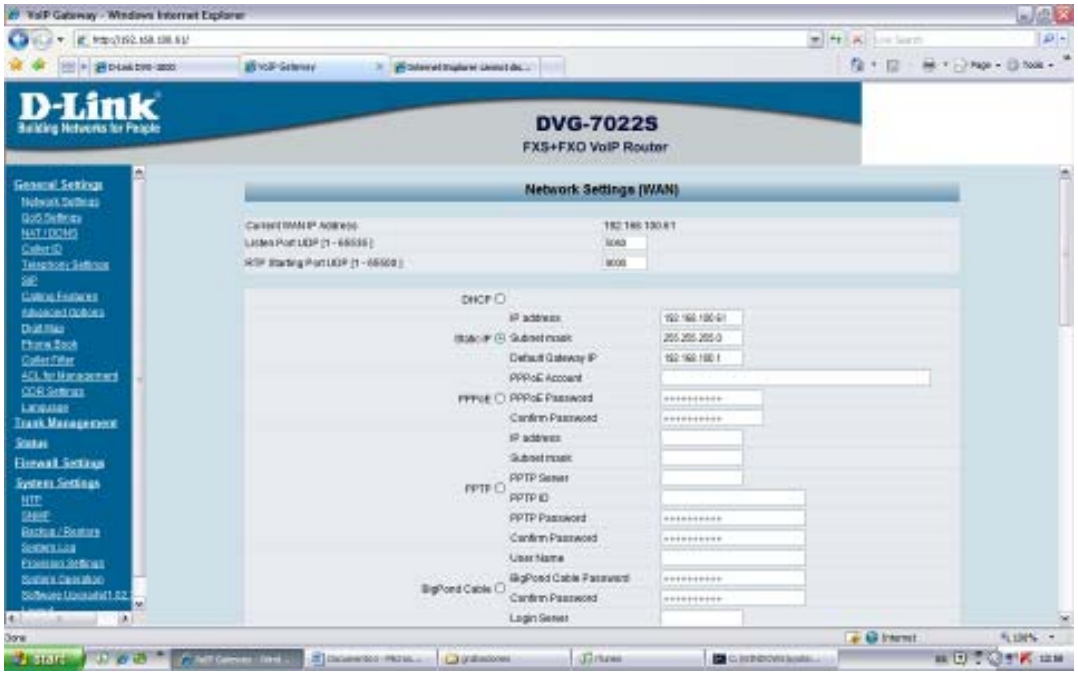


Figura. 7.47. Pantalla de configuración de red del DVG-7022S

Los parámetros siguientes de red como servidores DNS son los mismos de toda la red ya que el gateway general es el servidor Linux para salir a Internet, el 192.168.100.1.

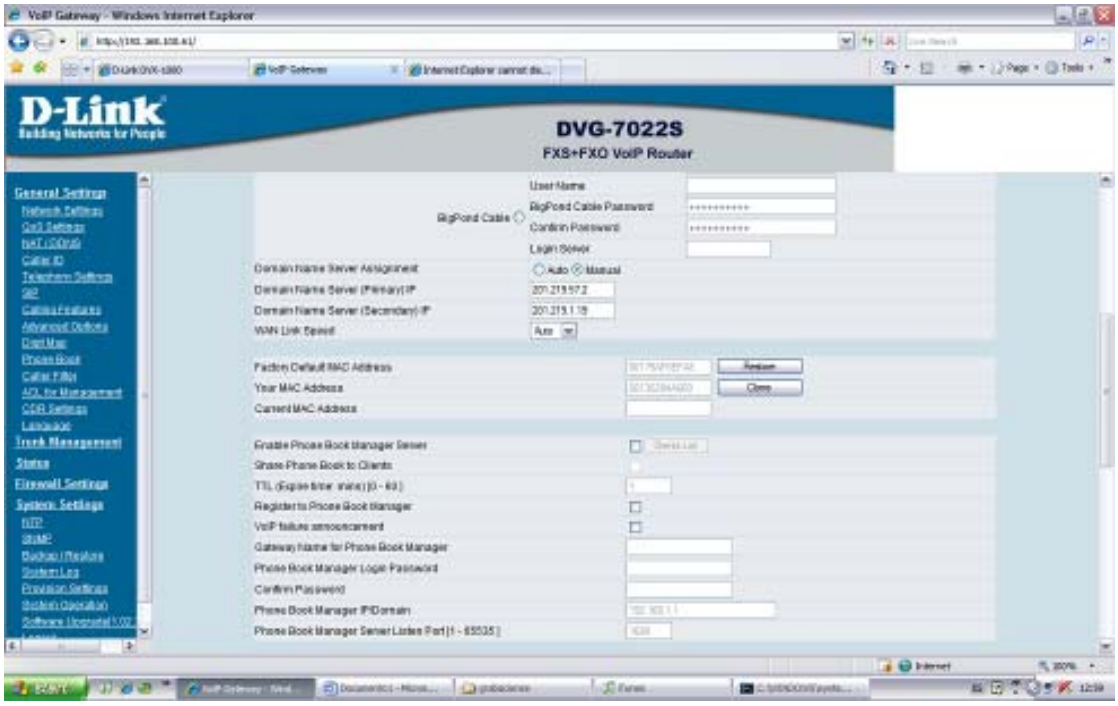


Figura. 7.48. Pantalla de configuración de red del DVG-7022S

Los parámetros de LAN se setean como en cualquier equipo de red, la dirección IP y su máscara de red, se v a configurar el equipo tipo bridge.

Figura. 7.49. Pantalla de configuración de red LAN del DVG-7022S

En la parte de QoS se setean los campos de la siguiente manera

Figura. 7.50. Parámetros de QoS del gateway

Para la opción de Caller ID, se configura de la siguiente manera.

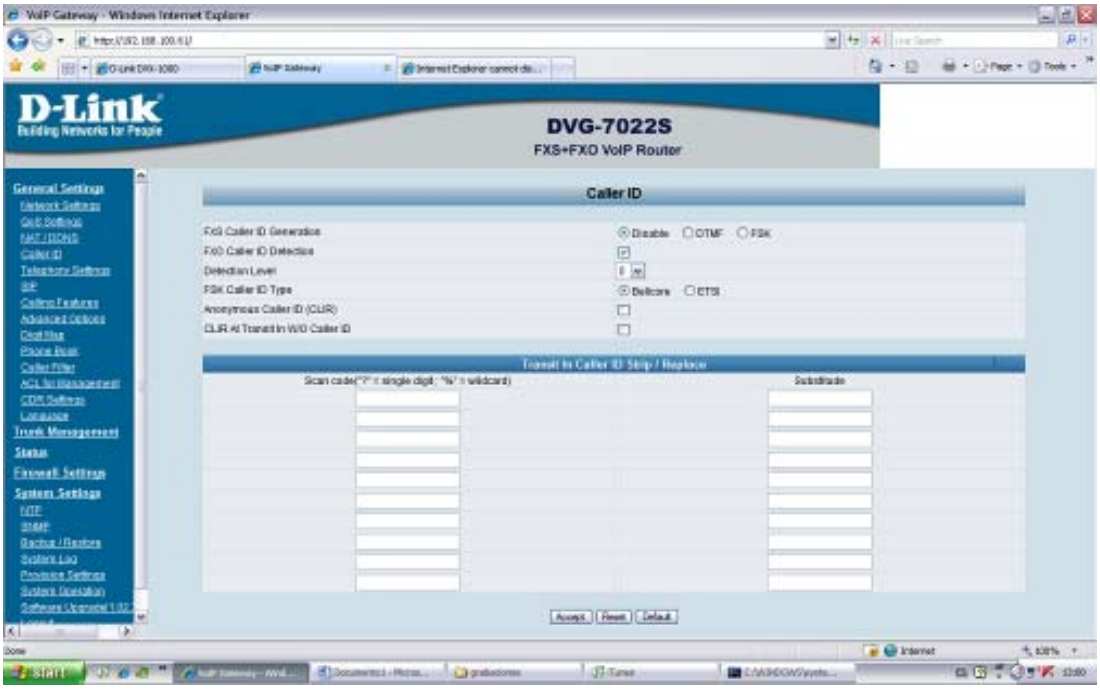


Figura. 7.51. Parámetros de QoS del gateway

En la pestaña de Telephony settings, se desplegará la siguiente pantalla y se requiere de los siguientes parámetros.

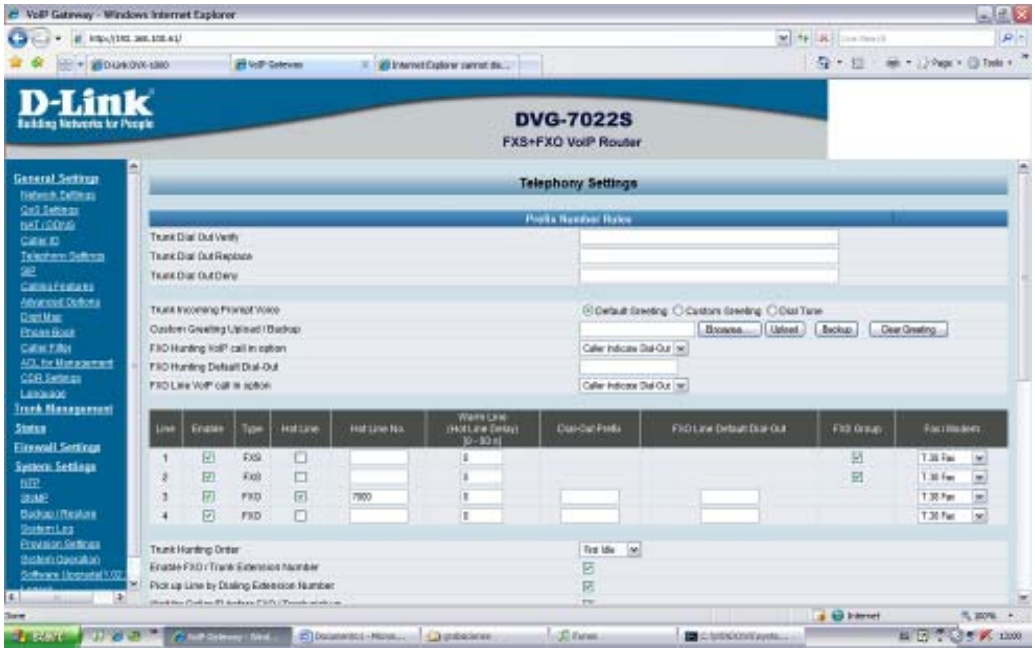


Figura. 7.52. Parámetros de Telephoy Settings

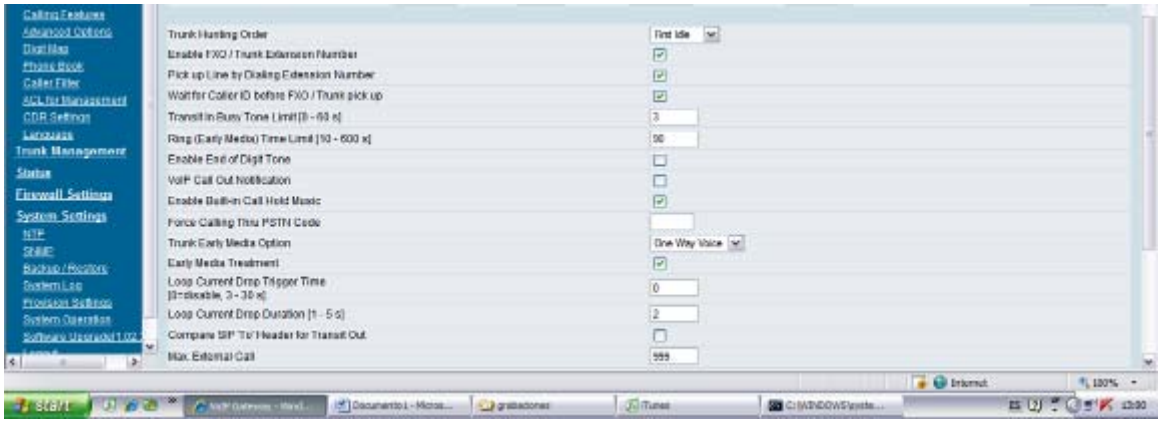


Figura. 7.53. Parámetros de Telephoy Settings

Figura. 7.54. Parámetros de Telephoy Settings

En la parte de opciones avanzadas, se puede configurar las passwords de administración del equipo, el tipo de dial de FXO y es importante habilitar la opción de RFC 2833, para objeto de compatibilidad con la central IP.

Figura. 7.55. Opciones Avanzadas

Finalmente es necesario resetear el equipo para que todos los cambios sean guardadosy tomen efecto.

Figura. 7.56. Opcion System Operation de reinicio de equipo

Como se indicó al inicio, solamente se indican los parámetros que son susceptibles de configuración, los demás ítems se dejan tal cual vienen seteados de fábrica ya que no afectan el funcionamiento del servicio.

7.3.3 Cámaras IP

Para la implementación de las cámaras IP, se ha decidido instalar las DLink DCS2100G, que acorde a las características técnicas analizadas en el capítulo 5, numeral 5.2.5 cumple con las especificaciones requeridas por el cliente y las necesidades de la red.

Para el caso del Liceo del Valle, se asignaron las siguientes IPs a las cámaras de videovigilancia:

- 192.168.100.74/8084 Laboratorio 1
- 192.168.100.72/8082 Laboratorio 2
- 192.168.100.71/8081 Primaria
- 192.168.100.73/8083 Recepción
- 192.168.100.75/8085 Secundaria 1
- 192.168.100.76/8086 Secundaria 2
- 192.168.100.77/8087 Repuesta

A continuación se muestra el proceso para configuración de una cámara IP.

Una vez instalada la cámara, se puede acceder vía web a la ip propia de la cámara (la suele indicar el fabricante en el manual, o suele llevar un programa de detección de IP). La dirección IP para el caso es 192.168.100.72

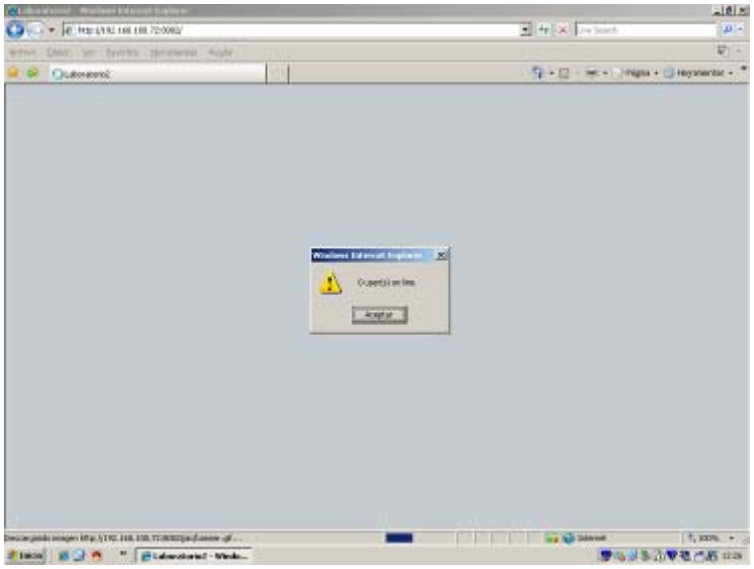


Figura. 7.57. Pantalla de ingreso web a cámara.

Se indica el número de usuarios en ese momento, antes de visualizar en la pantalla de lo que esta grabando la cámara en ese momento.

Figura. 7.58. Imagen de la cámara 192.168.100.72

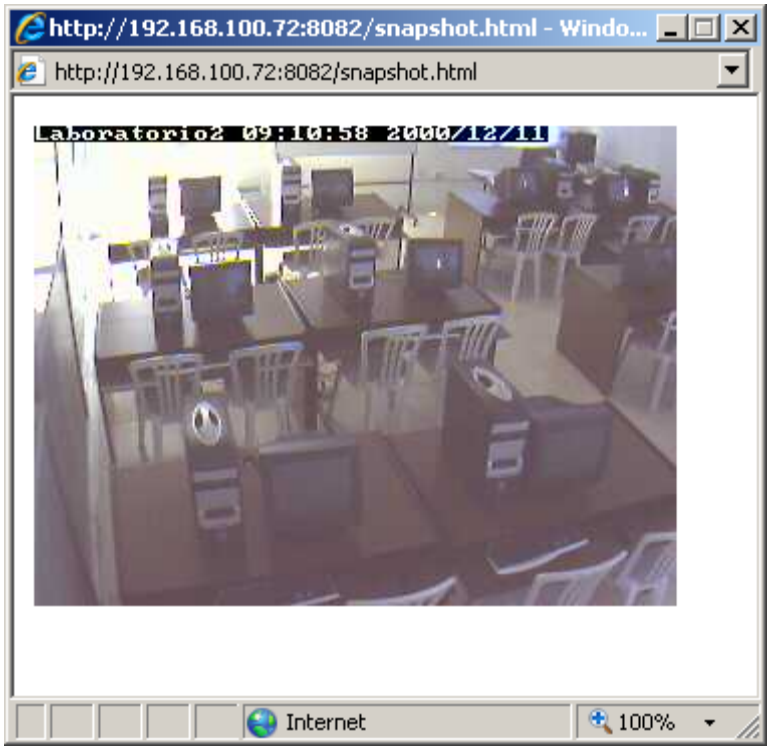


Figura. 7.59. Imagen ampliada

En la pestaña de conexión se despliega la opción de deshabilitar el audio y escoger el protocolo para transmisión de la imagen.

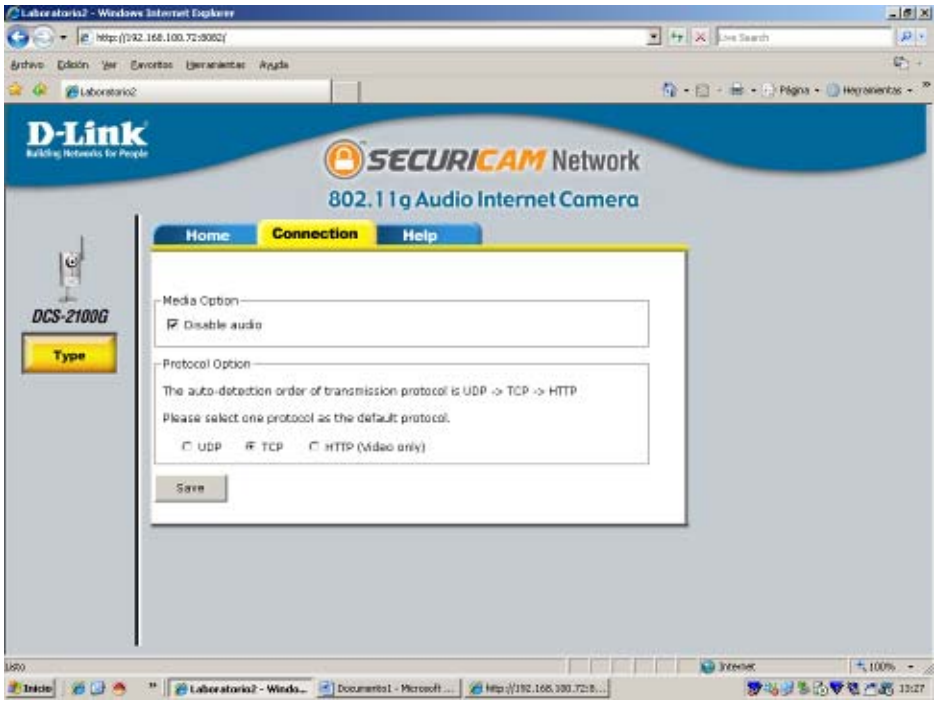


Figura. 7.60. Opción Conexión

En la opción Avanzado, se configura parámetros de IP, dirección, máscara de red , default router o puerta de enlace en este caso, y DNSs, primario y secundario. En el puerto http se configura la opción de acceder desde cualquier browser en cualquier parte del mundo a la imagen de la cámara, siempre y cuando se asignen los permisos necesarios de acceso en el servidor.

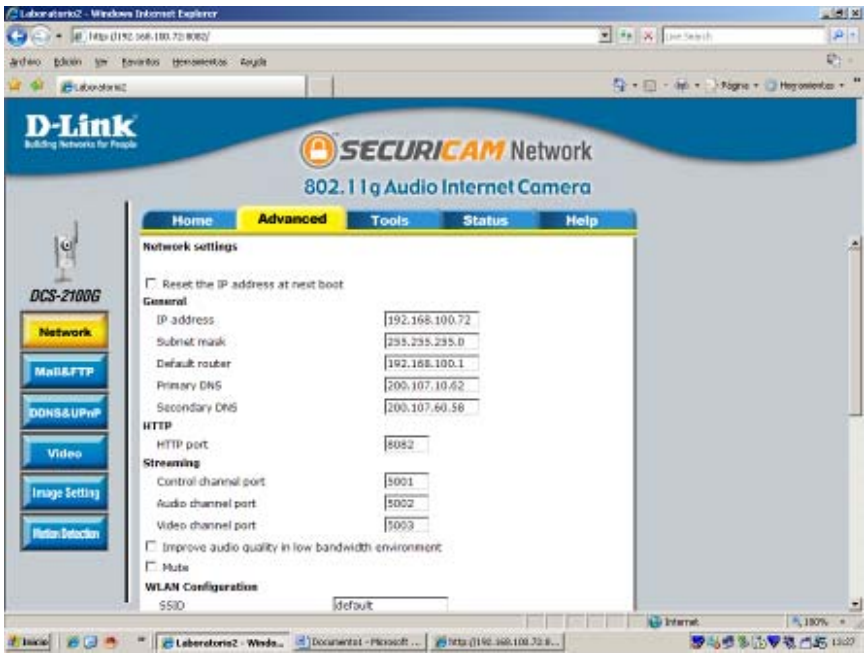


Figura. 7.61. Configuración de parámetros de red

Para los parámetros de configuración WLAN no se requiere configuración ya que la cámara saldrá al Internet por medio del servidor.

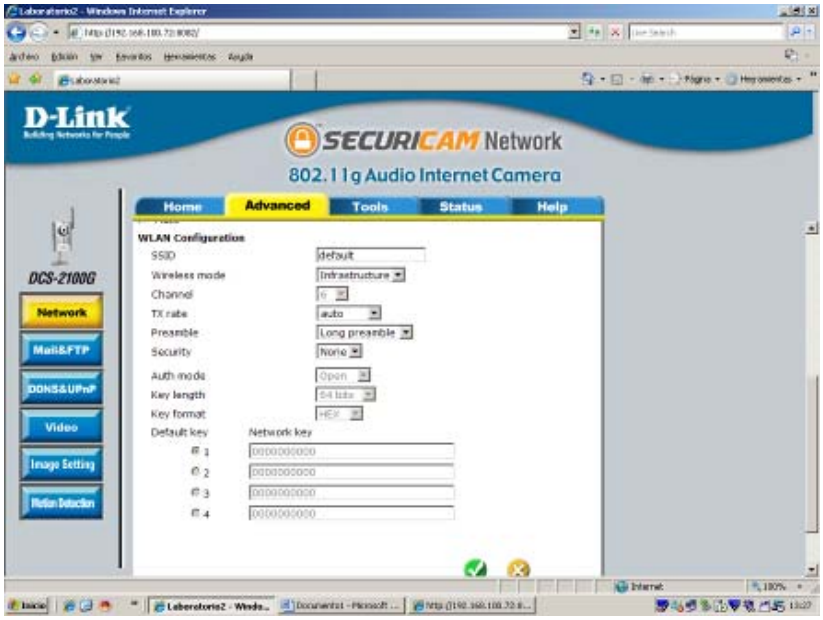


Figura. 7.62. Configuración de parámetros de red WLAN

Para las opciones de Mail &FTP no se requiere cambios en la configuración por defecto.

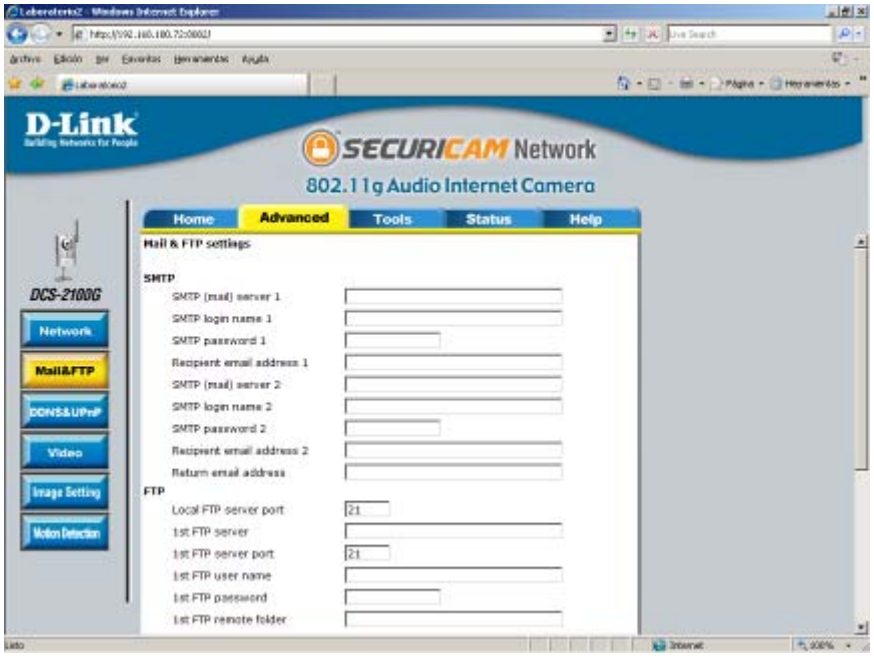


Figura. 7.63. Mail & FTP

En la opción de DDNS&UPnP tampoco se requiere cambios en la aplicación para los fines de la red que se implementa.

Figura. 7.64. DDNS&UPnP

En la opción video se ajusta parámetros como color, tamaño, frecuencia de la línea de alimentación de las luminarias del lugar donde se encuentra instalada la cámara, calidad, etc.

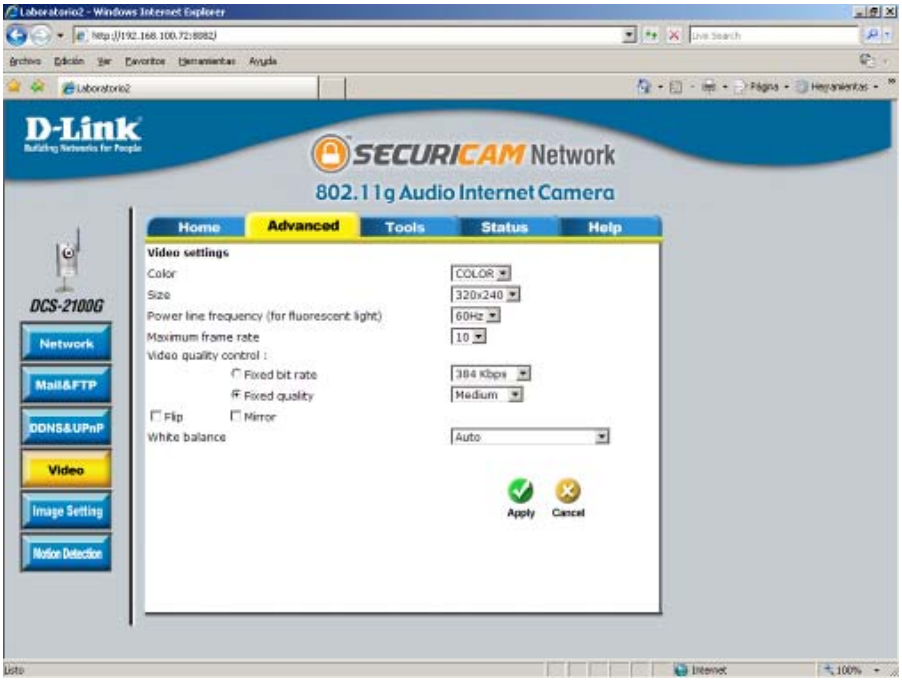


Figura. 7.65. Video

En la opción de *Image Setting* se puede variar parámetros de imagen como brillo, contraste, saturación y tono de la imagen mostrada por la cámara.

Figura. 7.66. Filtros de video

La opción de *Motion Detection* permite acceder a los parámetros que afectan como la DCS-2100G puede servir como un dispositivo de seguridad grabando solamente cuando se detecta movimiento. Se puede habilitar la opción poniendo visto en *Enable motion detection* y ajustar la sensibilidad del movimiento y el porcentaje de movimiento permitido antes de iniciar una alerta de movimiento detectado.

Figura. 7.67. Detección de movimiento

En la pestaña de Herramientas dentro de la opción Admin se puede setear el password para restringir el ingreso de otras personas a la cámara,y se puede crear cuentas para usuarios que no precisamente tengan privilegios de administrador.

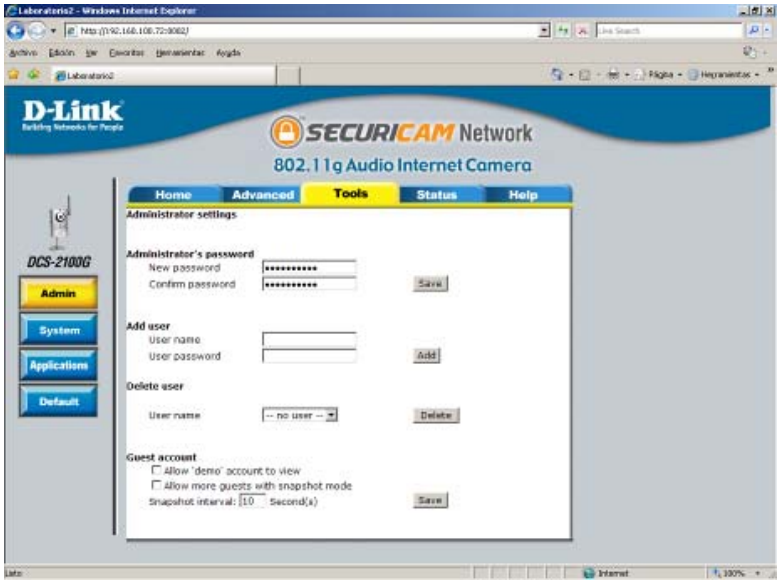


Figura. 7.68. Ingreso de password

En la opción de *Systems* se ingresa el nombre de la cámara que aparecerá como texto dentro del sistema operativo Windows. Este nombre también se mostrará en la pantalla de log in.

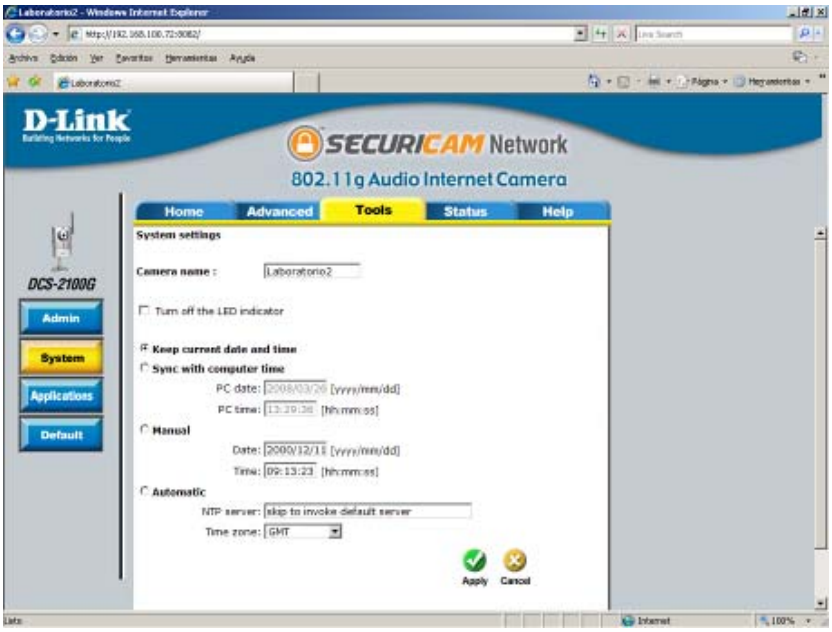


Figura. 7.69. Nombre de cámara

En la opción de *Applications* se puede programar las operaciones de la cámara dentro de un horario determinado.

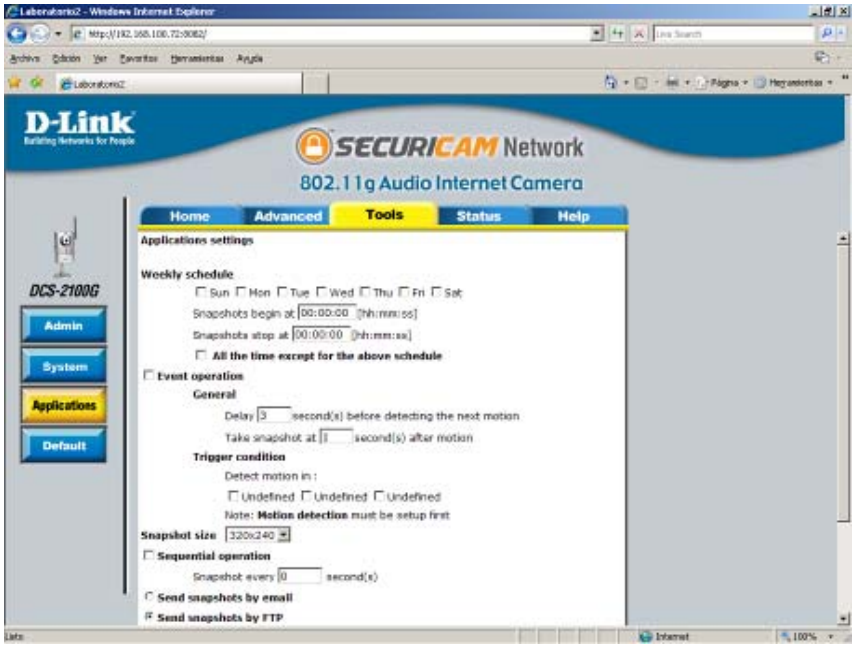


Figura. 7.70. Programación de eventos acorde a horarios

En la opción Default dando clic en la opción *apply* se puede restaurar los valores de fábrica que vienen por defecto en la cámara.

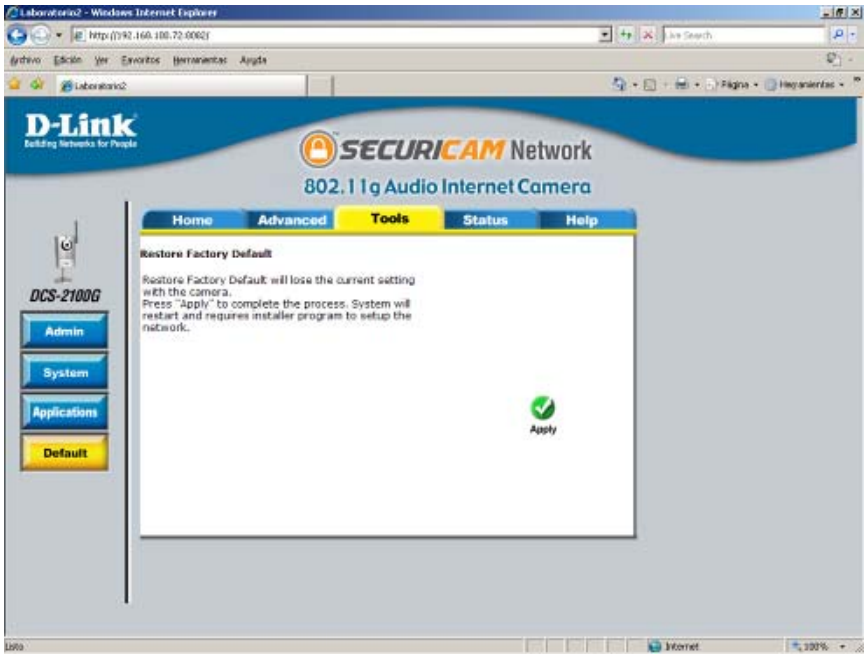


Figura. 7.71. Tools- Default regresar a parámetros de fábrica

En la pestaña Status muestra información general del equipo, con todos los parámetros configurados en pasos anteriores.

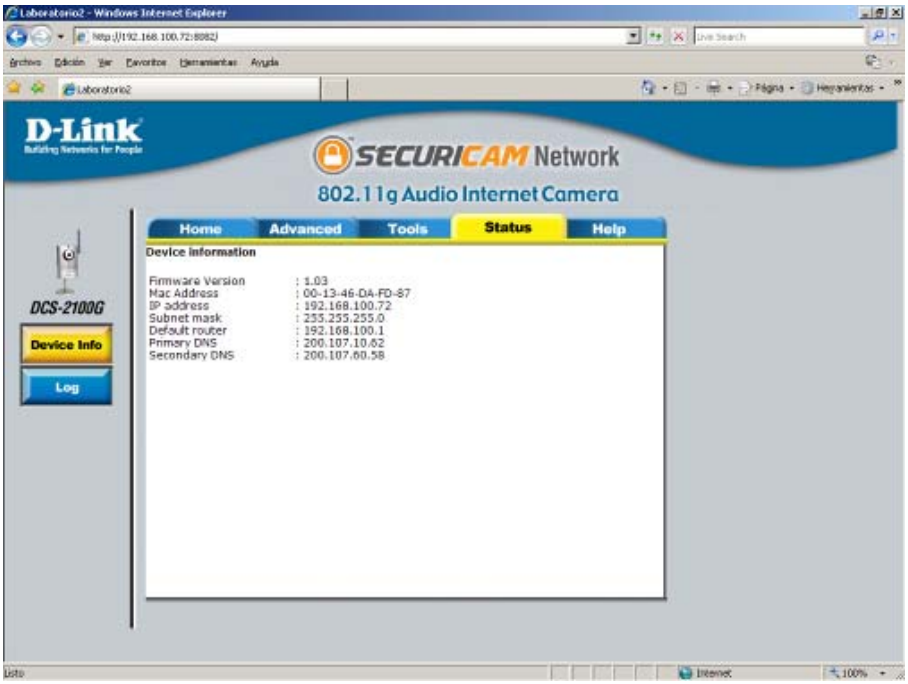


Figura. 7.72. Status-Información general de configuración del equipo

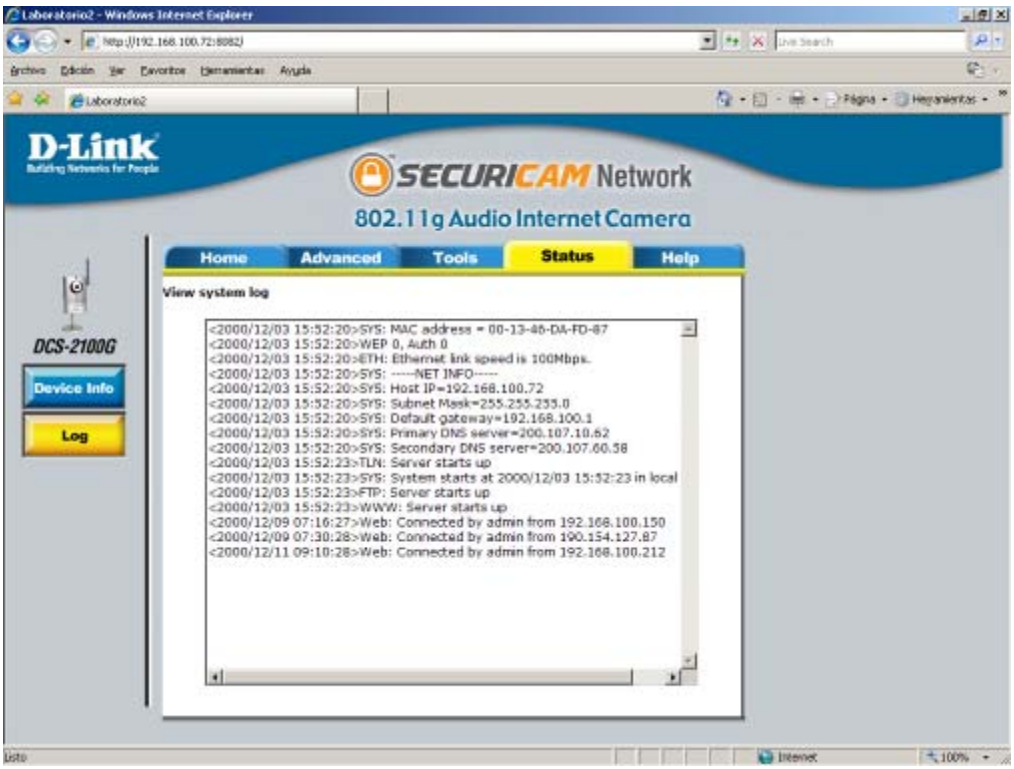


Figura. 7.73. Status-Información general de configuración del equipo

Por último en la pestaña de ayuda se lista temas de ayuda acerca del equipo y su configuración.

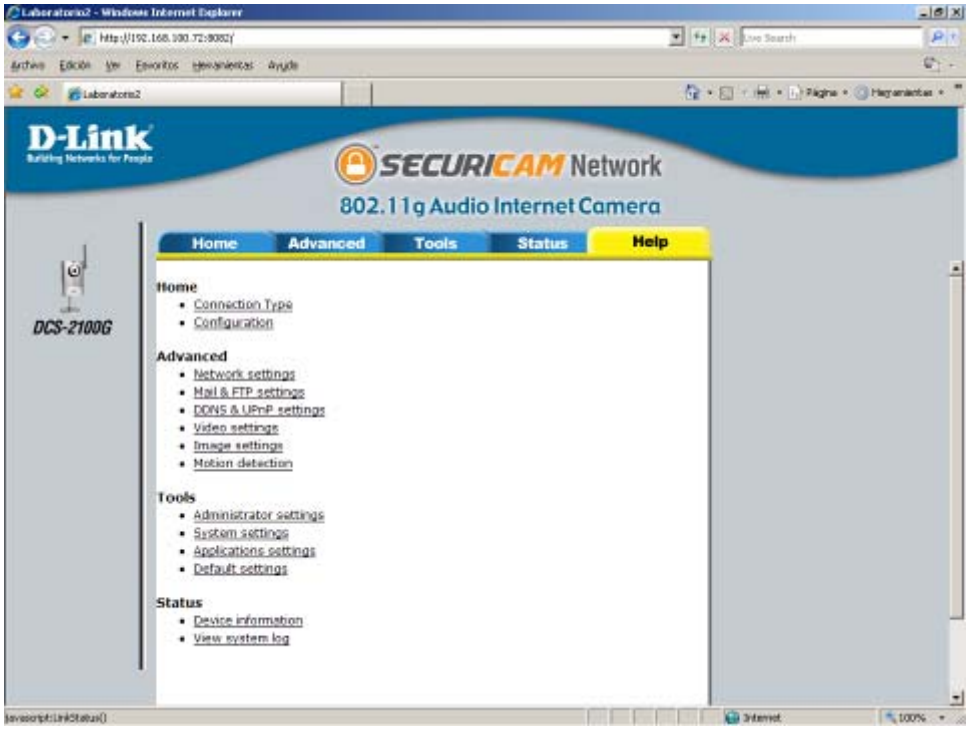


Figura. 7.74. Menú de ayuda de cámara DCS-2100G

Una vez configurados los equipos, se puede proceder a montarlos en los lugares requeridos con su respectivo soporte.

Figura. 7.75. Cámara DCS-2100G instalada

7.4 PRUEBAS

Para comprobar el correcto funcionamiento de la red, es necesario realizar algunas pruebas que garanticen que los equipos estén on line, comunicados entre sí, y configurados acorde a sus funciones dentro de la red, para ello se lleva a cabo las siguientes evaluaciones.

7.4.1 Conectividad

Aunque hay muchas asombrosas herramientas de alta tecnología dando vueltas para ayudar en la correcta implementación de una red, no hay que olvidar lo básico. Hay que estar muy familiarizados con estas herramientas ya que están presentes en la mayoría de los sistemas operativos Pueden ser muy útiles, a la hora de verificar problemas desde las capas más básica del modelo OSI, física y de enlace de datos.

Estos simples comandos verifican niveles básicos de configuración y comunicación entre equipos. Con el comando PING se verifica que el equipo al que se hace la solicitud esté correctamente conectado y configurado en la red.

Ping al servidor

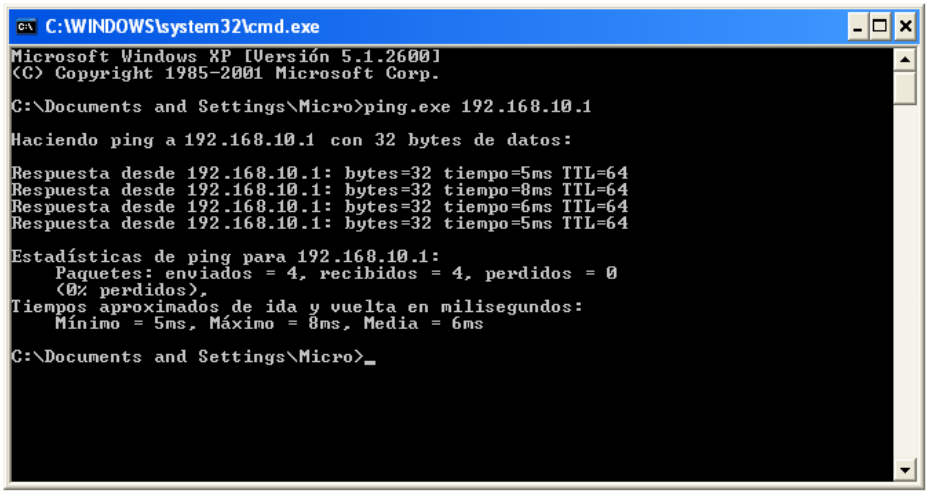


Figura. 7.76. Pruebas de conectividad a servidor

Ping a cámara IP

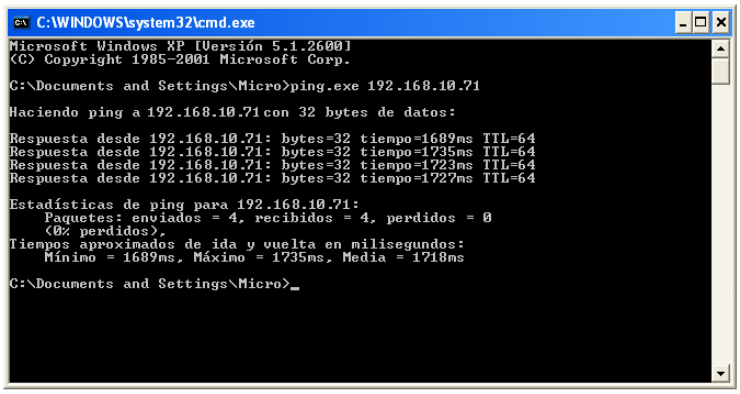


Figura. 7.77. Pruebas de conectividad a cámara IP

Ping a usuario de la wireless

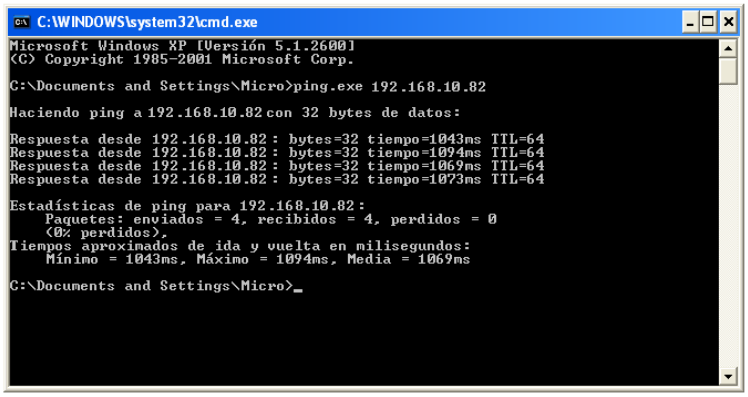


Figura. 7.78. Pruebas de conectividad a usuario wireless

Ping a central IP

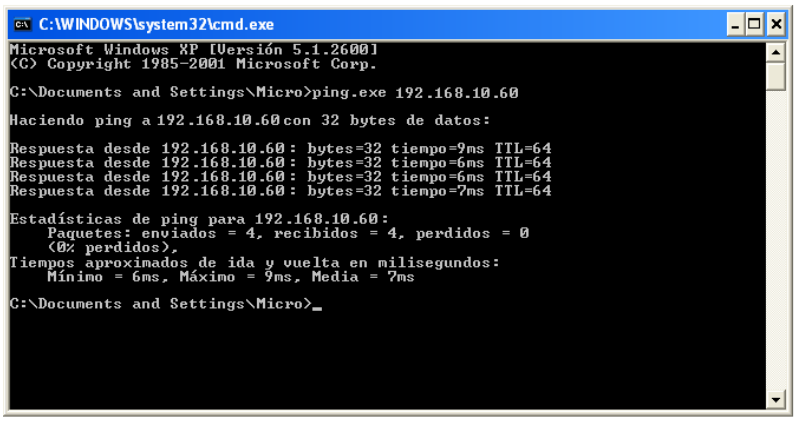


Figura. 7.79. Pruebas de conectividad a central IP

Ping a gateway IP

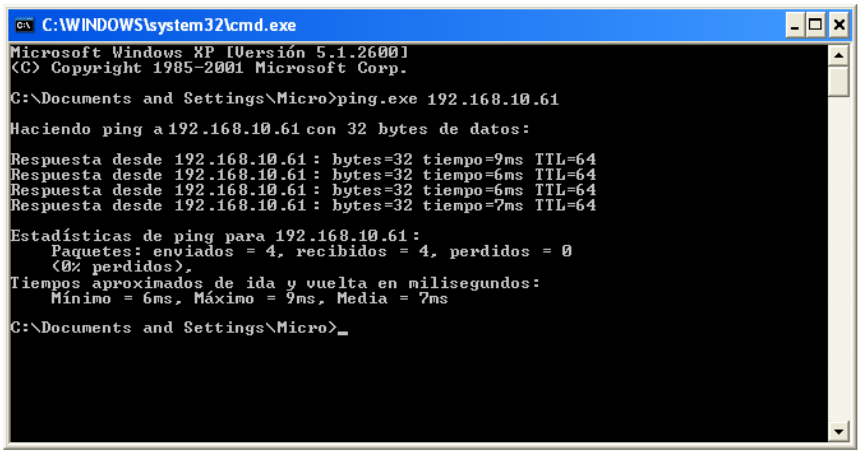


Figura. 7.80. Pruebas de conectividad a gateway IP

7.4.2 Funcionamiento

Para verificar el funcionamiento de los servicios, se realizaron pruebas de la corrida de cada aplicación y su respectivo uso. Para el funcionamiento del servidor se verifica que desde cualquier punto de la red se pueda ingresar remotamente con el software putty y administrar el servidor de aplicaciones.

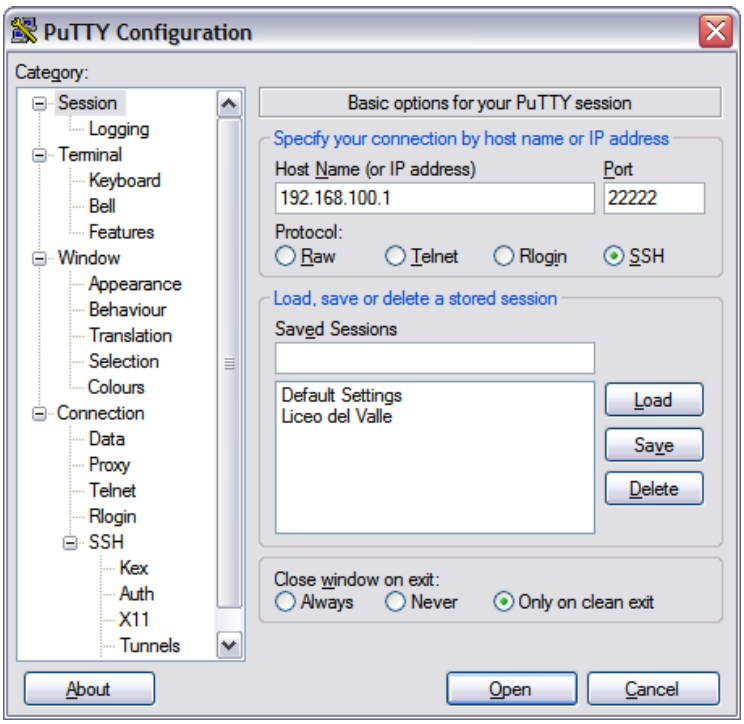


Figura. 7.81. Acceso local vía SSH al servidor

Con este programa se comprueba que el servidor esta levantado funcionando y con los servicios instalados, al poder establecer cohesión remota al servidor

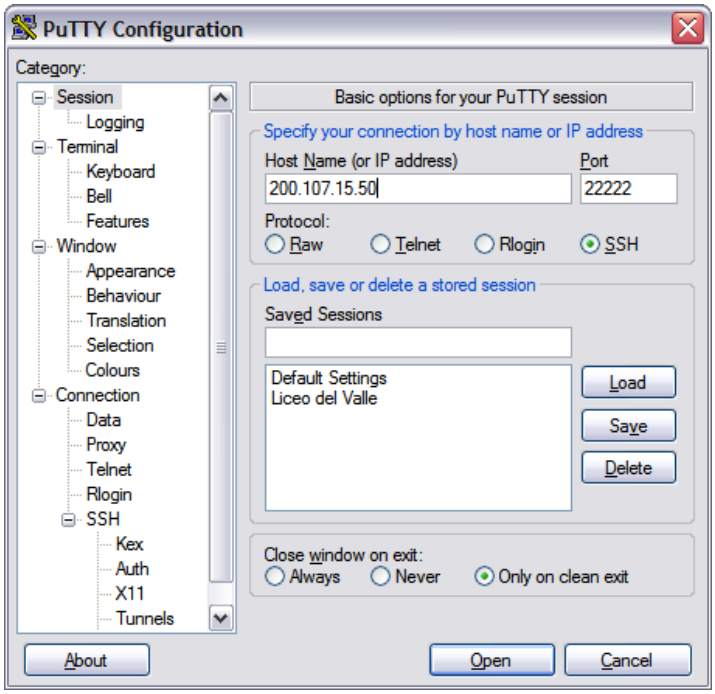


Figura. 7.82. Acceso remoto vía SSH al servidor

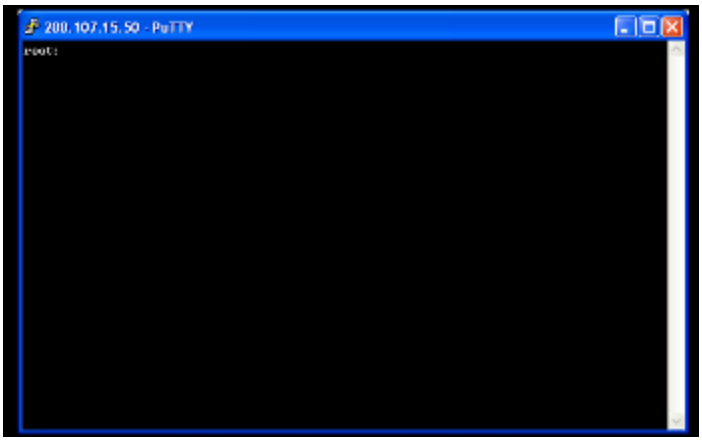


Figura. 7.83. Acceso remoto aprobado

Además de que se cuenta con servicio de navegación, con Proxy transparente.

Figura. 7.84. Navegación en Internet

7.4.3 Servicios

Correo

Para comprobar el servicio de correo se debe configurar una cuenta de Outlook con el dominio de usuario@liceodelvalle.edu.ec y hacer envíos y recepciones.

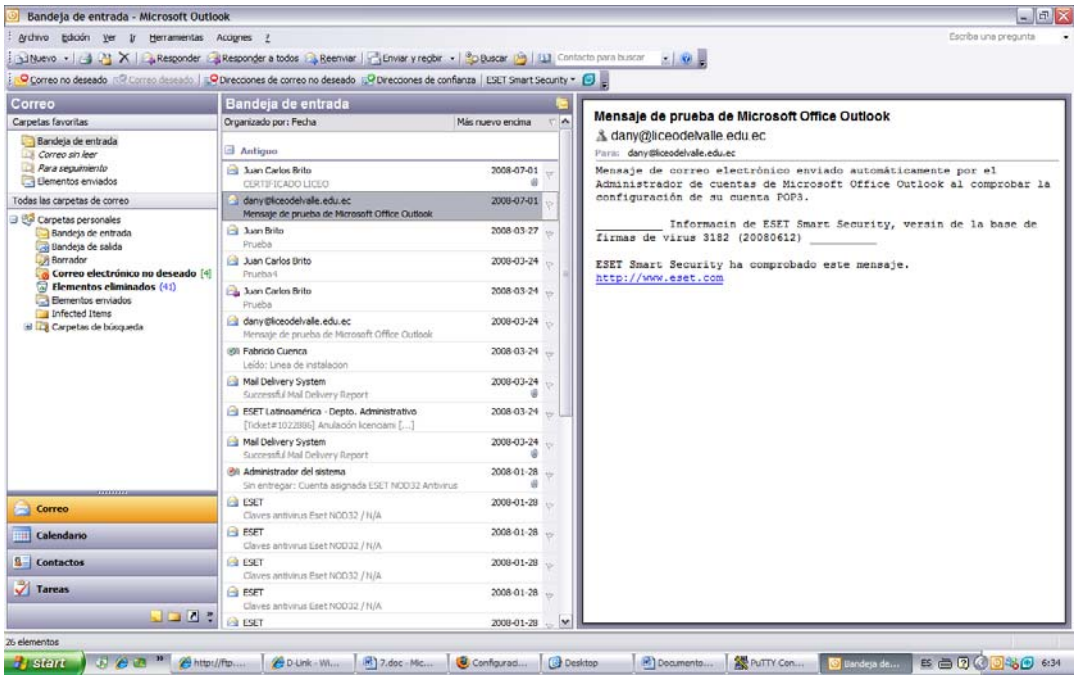


Figura. 7.85. Prueba de envío correo electrónico

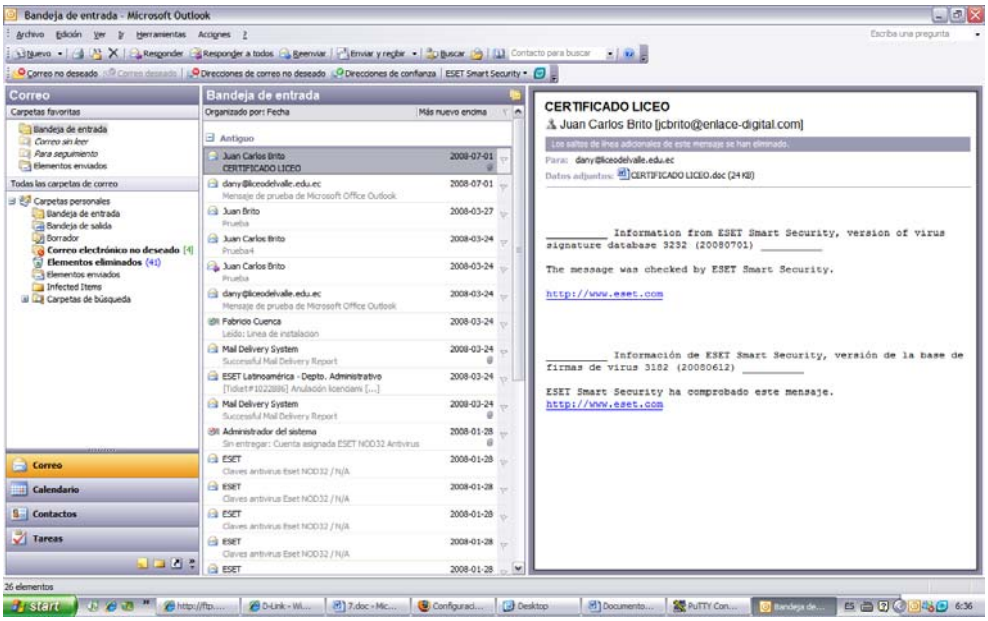


Figura. 7.86. Prueba de recepción correo electrónico

7.4.4 Calidad de servicio

Para la parte de la implementación de calidad de servicio es necesario verificar que los anchos de banda asignados para cada aplicación se estén cumpliendo, y no colapse la red ni se demore la entrega de paquetes de VoIP y videovigilancia que son prioritarios dentro de la gestión de la red.

Como ejemplo bajamos un archivo sin los servicios de VoIP y Videovigilancia y la tasa de descarga es:

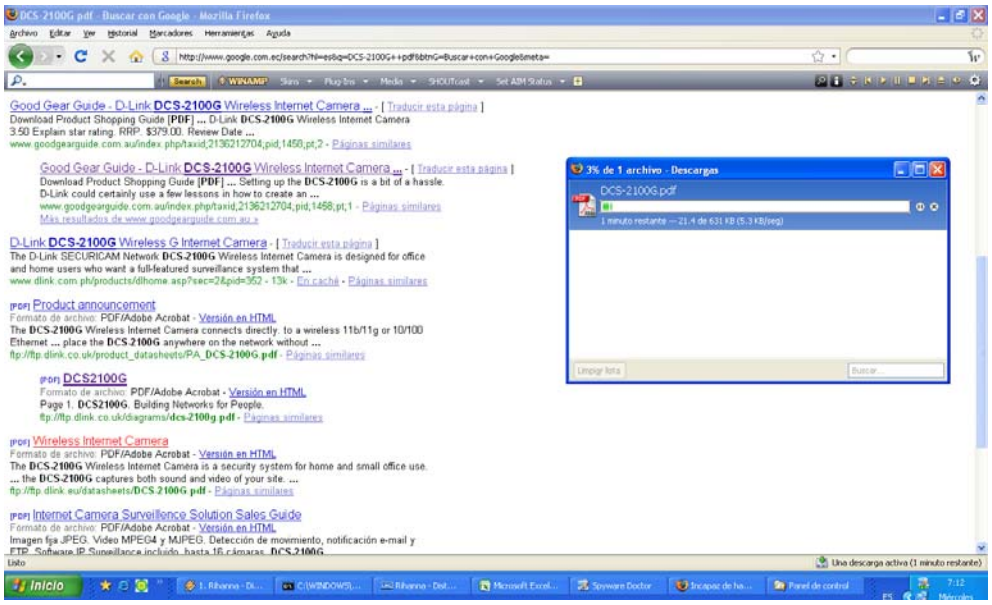


Figura. 7.87. Tasa de transferencia sin prioridad de servicio

Ahora notemos la diferencia de descarga con una llamada en la red IP al bajar un archivo:

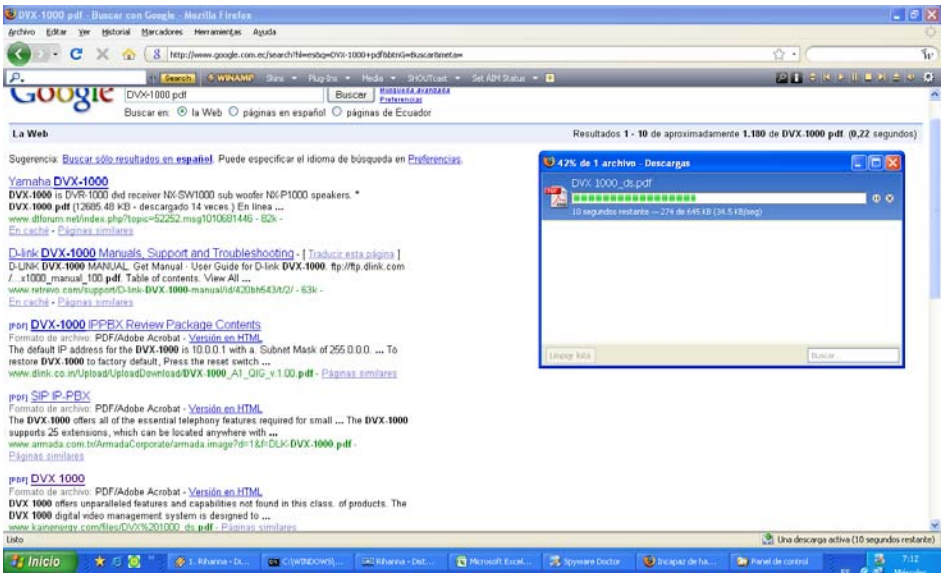


Figura. 7.88. Tasa de transferencia con prioridad de servicio

CAPÍTULO 8

CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

- Al término de la presente tesis, se ha cumplido de una manera satisfactoria el objetivo principal, es decir, se logró Diseñar e implementar una red wireless con servicios de Internet, VoIP y video-vigilancia basada sobre plataforma Linux, donde la solución integral implantada es ciento por ciento al diseño de planificación realizados en este documento. El producto resultante se encuentra funcionando y cumpliendo a su cabalidad las expectativas previas que el Liceo del Valle tenía del proyecto. El correcto funcionamiento y operación de la red implementada y sus servicios demuestran que el diseño y planificación desarrollados para el fin ha cumplido a cabalidad avalizando los procedimientos y criterios técnicos aplicados en el proyecto en general.

- Realizar un análisis costo-beneficio de los equipos a ser implementados en el proyecto, fue de suma importancia, ya que basándose en ello, se pudo realizar la correcta elección, tanto para el proveedor de servicios de internet, así como para la compra de equipos e insumos, además de brindar un buen servicio en el Liceo del Valle, comprende un factor importante la optimización de los recursos económicos que permitan tener calidad, confiabilidad y servicio sin descuidar tecnología y garantía ininterrumpida de servicio.

- Un adecuado diseño de la red wireless, determina el lugar más conveniente para la ubicación de los Access Point, y para este estudio es necesario considerar varias herramientas que nos permitan ampliar los criterios técnicos en cuanto a parámetro de cobertura, eficiencia, potencia y en general aspectos técnicos de los equipos a ser escogidos, además se requieren llevar a cabo una serie de pruebas de campo con registros

de variaciones y resultados que permitan observar el comportamiento de los equipos en los diferentes casos que puedan suscitarse durante el uso del servicio por parte de los usuarios.

- Mediante el uso del software NetStumbler, se puede comprobar de manera eficaz la calidad de la señal transmitida por los equipos wireless, entre las funciones utilizadas para este proyecto se encuentran: verificación de configuración de la red, estudio de la cobertura o señal que tenemos en diferentes puntos de acceso a la red, detectar otras redes que pueden causar interferencias a la nuestra, es muy útil para orientar antenas direccionales cuando queremos hacer enlaces de larga distancia, o simplemente para colocar la antena o tarjeta en el punto con mejor calidad de la señal, sirve para detectar puntos de acceso no autorizados (Rogue AP's). Por último, también nos sirve para detectar todos los APs que están a nuestro alrededor. Además brinda Y con GPS nos permite no solo detectar sino también localizar los APs.

- Mediante el uso del software WirelessMon se determina el lugar más adecuado para la ubicación de los Access point , es una herramienta muy útil para diseñar la ubicación estratégica de los APs, realiza análisis de interferencias acorde a los obstáculos y materiales de los mismos. Brinda versatilidad para ingresar planos del lugar donde se va a implementar los access points y tener localidades específicas de cobertura para colocación de los equipos.

- Existe una amplia gama de equipos de networking para implementación de una red, en lo que se refiere a routing, switching, seguridades y VoIP. Para el diseño de una red completamente nueva es necesario considerar equipos que no queden obsoletos al pasar de los años y que posean garantía para seguridad de los clientes.

- Otro factor importante para el diseño de una red nueva, es como primer paso, realizar un censo tecnológico para saber las demandas de los usuarios y prever el número de equipos a los que hay que prestar los servicios, dejando un margen de crecimiento, que oscile entre el 10 y 15% dependiendo de las aplicaciones y campos de acción de los usuarios.

- Para la implementación de una WLAN es necesario tomar en cuenta llevar a cabo un estudio radioeléctrico de la zona de servicio ya que las condiciones climatológicas del

lugar también afectan la calidad e intensidad de transmisión de información y determinan la potencia de las antenas de transmisión y recepción a ser instaladas.

- Dentro de una red empresarial es indispensable contar con un servidor de comunicaciones que administre y brinde ciertas aplicaciones para los usuarios de la red, dentro del Liceo del Valle fue implementado un servidor de comunicaciones en Centos 4.0, una distribución de Linux que presenta varias ventajas para aplicaciones empresariales, analizadas en el capítulo 2 de este proyecto, frente a otras distribuciones del mismo sistema operativo, es necesarios llevar a cabo un mantenimiento continuo en lo que se refiere a actualizaciones de software del servidor Linux, en general la configuración se puede realizar por comandos en texto plano, pero también existen ambientes gráficos que facilitan la implementación y puesta en marcha de los servicios.

- Para una red mixta con componentes cableados e inalámbricos es importante considerar puntos estratégicos de la red donde es necesario brindar un medio cableado para no provocar latencia en la señal y optimizar recursos muy valiosos como el ancho de banda con que cuenta la red.

- Dentro de la red del Liceo del Valle fue necesario implementar servicios agregados para optimización y monitoreo del ancho de banda y priorización de envío de paquetes QoS en el servidor Linux, para aplicaciones en tiempo real como la telefonía IP y la videovigilancia, ya que si no se aplica este criterio en la VoIP, esta sufre retrasos de transmisión o se escucha distorsionado.

- Para tener un criterio amplio de decisión acerca de la marca de equipos a ser instalados se desarrolló un análisis financiero para conocer acerca de inversión, rentabilidad, tiempo de recuperación de la inversión, costos operativos y de mantenimiento, características y especificaciones técnicas en general que permitan comparar entre diferentes marcas y bondades de los equipos.

- Los equipos Dlink instalados en la red del Liceo del Valle, brindan confiabilidad, escalabilidad, y calidad de señal en las diferentes aplicaciones usadas, la marca ofrece varios equipos, que sin necesidad de ser extremadamente costosos, garantía y asistencia técnica con sus distribuidores, además son fáciles de configurar y presentan un entorno amigable para el administrador.

- El estándar IEEE 802.11g es el más usado en estos días para implementar redes tipo WLAN, con tecnología WiFi. Ha desplazado al conocido 802.11b aunque los dispositivos de red vienen con compatibilidad para ambos tipos de tecnología. Cada vez las empresas buscan mayor rendimiento y velocidad en sus redes corporativas, el estándar IEEE 802.11n está introduciéndose en el mercado con velocidades de hasta 218 Mbps, con tecnologías Wi Max, a diferencia de las otras versiones de Wi-Fi, 802.11n puede trabajar en dos bandas de frecuencias: 2,4 GHz (la que emplean 802.11b y 802.11g) y 5 GHz (la que usa 802.11h). Gracias a ello, 802.11n es compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi. Además, es útil que trabaje en la banda de 5 GHz, ya que está menos congestionada y en 802.11n permite alcanzar un mayor rendimiento.

8.2 RECOMENDACIONES

- Es recomendable empezar desde cero en el servidor de comunicaciones, es decir formateado, para poder realizar una partición en el disco duro e instalar en cada una de ellas un sistema operativo, Linux y en este caso Windows XP, ya que con este procedimiento, permite recuperar mas fácilmente la información en el caso de requerirlo.

- Para el uso de tarjetas wireless es recomendable instalar tarjetas usb en portátiles y PCI en desktops, ya que la usb se puede retirar y colocar cuando se desee y es más transportable para los propósitos.

- Para las computadoras y terminales en general que pertenecen a la intranet, se recomienda mantenerlos actualizados en cuanto se refiere a las versiones de sus sistema operativo. Generalmente todos los equipos de los usuarios usan Windows y es recomendable que tengan instalado SP2 (Service Pack 2). En este paquete de servicios se incorporan las herramientas necesarias para el reconocimiento de la encriptación para las seguridades de la red y el estándar de sesee seguridad 802.x. Con todos los usuarios de la red usando Windows SP2, será posible activar un mayor nivel de seguridad en la WLAN. Los Access Point y los adaptadores de acceso inalámbrico a la red con que ya cuenta el Liceo del Valle brinda altos niveles de seguridad.

- Constituye un factor de suma importancia dentro de una red establecer seguridades a nivel de usuario, entre estas opciones se encuentra la instalación de un antivirus que ofrezca protección además de contra virus, contra otros eminentes peligros como malware,

pishing, spyware, ya que cada usuario es una fuente importante de ingreso de este tipo de programas maliciosos a la red y contamina al resto de usuarios, poniendo en peligro el buen funcionamiento de toda la red.

- Para la utilización de todos los servicios implementados en el Liceo del Valle, es necesario dar una adecuada capacitación a los usuarios que les permita utilizar y sacar el mayor provecho de todos los servicios que se encuentran a su disposición, especialmente del servicio de VoIP y el manejo de la central, grabación de mensajes, transferencia de llamadas, entre otros.

- Es importante colocar un sistema de protecciones atmosféricas dentro de la institución para evitar futuras sobrecargas eléctricas atmosféricas causadas por las lluvias constantes en el sector, lo que potencialmente puede causar importantes daños en los equipos instalados a la intemperie desde daño de puertos hasta pérdida total de los equipos.

- Para el servicio de videovigilancia se recomienda instalar el software de monitoreo en las computadoras del administrador de la red y del personal de seguridad, así como también de las autoridades del colegio, para aprovechar al máximo las funciones del servicio, que van desde captura de imágenes a mono de fotografías, hasta grabación continua durante el día de las actividades registradas por las cámaras. Para el segundo caso, se recomienda tener un histórico de las grabaciones registradas y llevar a cabo una depuración de las mismas cada cierto tiempo para evitar saturaciones en el espacio del disco donde se almacena esta información.

- En cuanto al servicio de correo se recomienda instruir a los usuarios de la opción de revisión de su correo a través de la web, ya que este servicio es de mucha ayuda para cuando se encuentren fuera de las oficinas, además se recomienda depurar cada cierto tiempo la base de datos de los correos para evitar la saturación del disco donde se almacena esta información y configurar en el Outlook de cada usuario la opción de guardar los datos del buzón de entrada y permitir que sean borrados después de algún tiempo, por si el usuario necesita recuperar o revisar información de su correo.

ANEXOS

A1. WIRELESS INTERNET CAMARA

Wireless Internet Camera

D-Link
Building Networks for People

DCS-2120

KEY FEATURES

- Image/Sound Surveillance Through Internet & 802.11g Wireless LAN
- View Live Video Streams From 3G Mobile Phone/PDA
- Light-Sensitive Lens & Digital Zoom *
- Intruder Detection With Still Image Capture & E-Mail Notification
- Easy Deployment With UPnP/DDNS Support

Wireless Internet Camera For Home & Small Office

The DCS-2120 wireless Internet camera is a powerful surveillance system that features 802.11g wireless connection and the ability to view live video streams from a 3G mobile phone or PDA.

Features and Benefits:

Stand-alone System With Integrated Web Server:

Designed as a standalone system complete with CPU and web server, advanced features such as a light sensitive lens, digital zoom capability and powerful video/sound surveillance and remote monitoring utility, and this camera presents a low-cost solution for demanding home/office security needs.

Watch and Listen Remotely:

Snapshot enables users to save images directly from a web browser to a computer's hard drive without installing any additional software. With 0.5 lux light sensitivity, this camera is capable of capturing video in rooms with minimal lighting. Images can be zoomed using the 4x digital zoom feature. This camera allows users to monitor video and audio using an Internet browser from any where in the world. Simple installation procedures, along with the built-in web-based interface, offer easy integration to any network environments.

View live video streams:

Users have the ability to view live video streams from a compatible 3G cell phone. The live camera feed of the camera can be pulled from the 3G cellular network by using a compatible cell phone or PDA with a 3G video player. From anywhere within the 3GPP service area, users are offered a flexible and convenient way to remotely monitor a home or office in real time.

Motion Detected Recording:

Instead of recording 24 hours a day, 7 days a week, images can be recorded to a computer hard drive only when motions are detected. This saves disk space and eliminates the time wasted to view unnecessary images. Playback consumes little time with triggered event browsing and fast database searching.

Multi-Camera Monitoring:

Software is included to let users view up to 16 cameras on a single computer screen at one central location. Images can be recorded manually or according to a pre-set schedule. Users can set up automated e-mail alerts for sending through the Internet to be alarmed instantly of all unusual happenings.

Built-in wireless network interface:

For effective surveillance in and around a building, this camera comes with a built-in high-speed 802.11g wireless network interface, allowing images to be transmitted at up to 54Mbps wireless speed. In addition, a 10/100BASE-TX Ethernet port is also provided for convenient connection to an Ethernet network or to a broadband Internet via a gateway router.

Easy Deployment:

The camera adheres to the Universal Plug-n-Play specification, which allows computers running Windows XP/ME to automatically recognize the camera and add it to the network. It can be accessed and viewed from any network place as a device on the network. By signing up with one of the many free Dynamic DNS services available on the web, users can assign an easy-toremember name and domain to the camera (e.g. Www.mycamera.myddns.com). This allows them to remotely access the camera without having to remember the IP address, even if their Internet Service Provider has changed it.

WIRELESS

* 4x digital zoom enlarges an image by magnifying the pixels in a selected portion of the image by 4 times.

TECHNICAL SPECIFICATIONS DCS-2120

General

- Network Protocol Support
  - TCP/IP, RTSP, RTP, RTCP, HTTP, SMTP, FTP, NTP, DNS, DHCP, UPnP, DDNS
- Connectivity
  - 802.11g wireless LAN
  - 802.3 10/100Mbps 10/100BAS-TX Ethernet supporting NWay auto negotiation

Video Algorithm Support
- JPEG for still image
- Enhanced video compression using MPEG4 Simple Profile

Video Resolution
- Up to 30fps at 160x120
- Up to 30fps at 176x144
- Up to 30fps at 320x240
- Up to 30fps at 640x480

Video Features
- Adjustable image size and quality
- Time stamp and text overlays
- 3 configurable motion detection windows
- Flip & mirror

Video Bit Rate
- 1 20K to 4M

Camera Specifications
- 1/4-inch CMOS sensor
- 0.5 Lux @ f1.4
- AGC/AWB/AES
- Electronic shutter: 1/60 to 1/15000 secretary.
- Standard fixed mount type lens 4mm, f2.0
- 62 field of view

Security
- Administrator and user group protected
- Password authentication
- Wireless LAN security: 64/128-bit WEP and WPA-PSK data encryption

Surveillance Software Functions
- Remote management/control of up to 16 DCS-2120 cameras
- Viewing of up to 16 cameras on one screen
- Supports all management functions provided in web interface
- Scheduled motion triggered, or manual recording options

Microphone
- Directivity: omni-directional
- Frequency: 50 to 16000Hz
- S/N ratio: more than 60dB

Wireless Transmit Output Power
- 16dBm (typical)

Wireless Receive Sensitivity
- For 802.11b: (Typically @PER < 8% packet size 1024 @ 25 C +/- 5 C)
  11Mbps (CCK): -80 dBm
  5.5Mbps (CCK): -83 dBm
  2Mbps (QPSK): -84 dBm
  1Mbps (BPSK): -87 dBm
- For 802.11g: (Typically @PER < 8% packet size 1024 @ 25 C +/- 5 C)
  54Mbps (OFDM): -65 dBm
  48Mbps (OFDM): -66 dBm
  36Mbps (OFDM): -70 dBm
  24Mbps (OFDM): -72 dBm
  18Mbps (OFDM): -77 dBm
  12Mbps (OFDM): -79 dBm
  9Mbps (OFDM): -81 dBm
  6Mbps (OFDM): -82 dBm

Wireless Operating Range [1]
- Indoors: 100 meters
- Outdoors: 300 meters

Viewing System Requirements
- Operating System: Microsoft Windows XP, 2000, ME
- Browser: Internet Explorer v.5.0 or above

Remote Management
- Configuration accessible via web browser
- Take snapshots and save to local hard drive via web browser

Surveillance (Motion detection weekly schedule)
- Upload snapshot via email
- Upload snapshot via FTP

Supported PDA, Mobile Phones & Software
- Handsets with 3GPP player
- Packet Video Player 3.0
- QuickTime 6.5
- Real Player 10.5
- Windows ME, 2000, XP

LEDs
- 2-color LED

Physical & Environmental

- Power Input
  - Through 5V DC 2.0A external power adapter
- Power Consumption: 3.5 watts
- Dimensions
  - 26.8 (L) x 72.8 (W) x 115.2 (H) mm (camera only, excluding antenna)
- Weight
  - 185 grams (camera, including antenna)
- Operating Temperature: - 0° to 50° C
- Storage Temperature: -30° to 75° C
- Operaing Humidity
  - 5% to 95% non-condensing
- Emission (EMI)
  - FCC
  - IC
  - CE
  - C-Tick
- Radio: EN 300 328-2 (07-2000)
- Safety: EN60950
- Package Includes
  - DCS-2120 camera
  - External power adapter
  - Cat. 5 Ethernet cable
  - Quick Installation Guide
  - Master CD
  - Dipole antenna
  - Camera stand

Ordering Information:

DCS-2120

Wireless Internet Camera

K1-202-0-1.2-0703

[1] Environmental factors may adversely affect range.

©2007 D-Link India Ltd. All rights reserved.
Users' agree to indemnify, defend and hold D-Link harmless from and against all losses, expenses, damages, including reasonable costs and fees, aris ing out of or relating to any misuse by the Users of the Product or of the information or content provided in this document.

Call us at: 1-800-222-002, 91-22-2844 7600
E-mail: sales@dlink.co.in
www.dlink.co.in

D-Link
Building Networks for People

A2. GUIA RAPIDA DE INSTALACIÓN

D-Link

Quick Installation Guide

This product can be set up using Internet Explorer or Netscape Navigator, 6.x or above, with Javascript enabled

DVG-7022S

FXS+FXO VoIP Router

Before You Begin

You must have at least the following:

- A subscription with bundled service provider included in this package
- A Computer with a CD-ROM drive and an Ethernet port running a Windows
- Ethernet based broadband modem

Check Your Package Contents

These are the items included with your purchase:
If any of the below items are missing, please contact your reseller.

DVG-7022S FXS+FXO VoIP Router

Phone Cord

CAT5 Ethernet Cable

CD-ROM

12V DC Power Adapter

⚠ Using a power supply with a different voltage rating will damage this product and void the warranty

©2005 D-Link Systems, Inc. All rights reserved. Trademarks or registered trademarks are the property of their respective holders. Software and specifications subject to change without notice. DVG-7022S FXS+FXO VoIP Router

1 Hardware Overview

Front Panel

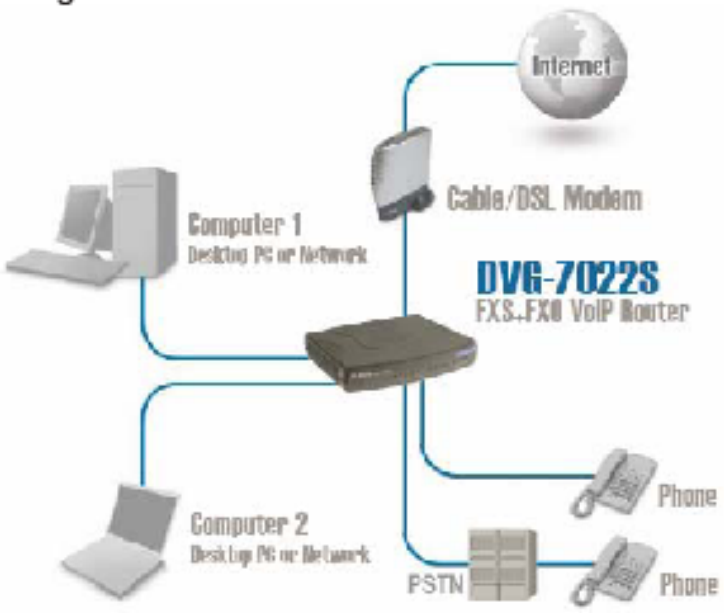
Power LED	Indicates the unit is powered on.
Run	The Run LED will flash when performing a self-test/booting up and light solid green if the self-test or bootup fails.
Alarm	The Alarm LED will light solid red if the self-test or bootup fails. The Alarm will flash red when the system is registering with the service provider or register fails.
WAN LED	When a connection is established the 10 or 100 LED will light up solid. The LED will blink to indicate activity. If the 10 or 100 LED does not light up when a cable is connected, verify the cable connections and make sure your devices are powered on.
LAN LEDs	When a connection is established the 10 or 100 LED will light up solid on the appropriate port. The LEDs will blink to indicate activity. If the 10 or 100 LED does not light up when a cable is connected, verify the cable connections and make sure your devices are powered on.
Phone LEDs	This LED displays the VoIP status and Hook activity on the phone port that is used to connect your normal telephone(s). If a phone connected to a phone port is off hook or in use, this LED will light solid. When a phone is ringing, the indicator will blink.
Line LEDs	Light on means the line is in use (off-hook), and vice versa.

Rear Panel

Phone Ports	Connect to your phones using standard phone cabling.
Line Ports	Connect to your original telephone line on the wall jack with RJ-11 cable.
LAN Port	Connect to your Ethernet enabled computers using Ethernet cabling.
WAN Port	Connects to your broadband modem using an Ethernet cable.
Reset	This is used to reset the unit to the factory default settings.
DC 12V	The power adapter attaches here. ⚠ Using a power supply with a different voltage rating will damage this product.

2 Connecting the DVG-7022S directly to a Modem and Computer

If your computer connects directly to a DSL or Cable modem and does not connect to a router, follow the steps below to install your DVG-7022S. For any other configuration, please refer to the user manual located on the CD-ROM. After the steps are completed, your setup should look similar to the diagram below.



a. Turn off your Computer.

b. Disconnect the power to your Cable/DSL Modem (Unplug or turn off the power switch).

c. Unplug the existing Ethernet cable that is connected to your Cable/DSL Modem's LAN or Ethernet port. Leave the other end of this cable attached to your PC.

d. Plug the Ethernet cable connector that you just removed from the modem into one of the four LAN ports on the back of the DVG-7022S. The other end remains attached to the PC.

2 Connecting the DVG-7022S directly to a Modem and Computer (continued)

e. Attach one end of the Ethernet Cable provided in this package to the LAN or Ethernet Port on the Cable/DSL Modem.

f. Attach the other end of the provided Ethernet Cable to the WAN Port of the DVG-7022S.

g. Connect a standard analog telephone and the phone port on the rear panel of the DVG-7022S by the provided phone cable.

h. Connect your original telephone line on the wall jack and the line port on the rear panel of the DVG-7022S by the provided phone cable.

i. Reconnect the power to the Cable/DSL Modem (Plug in or turn on the power switch).

j. Connect the Power Adapter to the Power Connecter on the DVG-7022S.

k. Connect the other end of the Power Adapter to an available electrical outlet (Wall Socket or Surge Protector).

l. Restart your PC.

- If your ISP registers your computer's MAC address, see the section labeled *MAC Cloning* for Connections in the user manual on the CD-ROM.
- **PPPoE Users**, please continue to the next page for additional configuration steps.

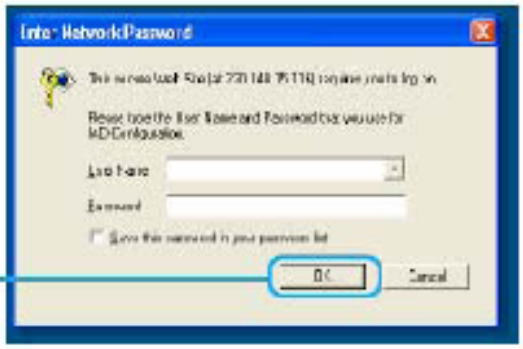
Hardware configuration is complete! If your VoIP service is already activated, you can make phone calls now.

3 PPPoE Configuration

Some Internet Service providers use PPPoE as their method of connecting clients. If you have a PPPoE connection, you must follow the steps below to complete the configuration of your hardware. If you are unsure of your connection type or do not know your username and password, please check with your Internet Service Provider.

Open your Web browser and type http://192.168.8.254 into the URL address box. Press the Enter or Return Key

Click OK to enter Web Site.



Click Network Settings.

Click PPPoE.

Enter PPPoE Account, Password and Confirm Password.

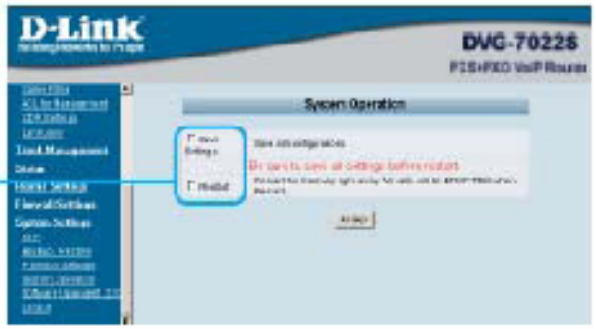
3 PPPoE Configuration (continued)

Click Accept at the bottom of this page.

Click System Operation at left menu.

Select Save Settings and Restart.

Click Accept.



Once the unit reboots you will see the message. Check to see if the status LED light goes from blinking green to solid green on the front panel of the DVG-7022S.

The information found on the Device Information page is necessary for VoIP service registration

A3. DVX-1000

D-Link
Building Networks for People

DVX-1000

FEATURES

Key Features:

- Includes 25 User Extensions
- Supports 25 Simultaneous Inbound/Outbound Calls
- Supports Multiple Users Across Multiple Sites
- Add External Analog Trunk Gateways to Use Standard Phones
- Save Money by using Internet Phone Service (VoIP)

Networking Features

- SIP (RFC 3261) Compliant
- 10/100Mb IEEE 802.3 Compliant
- Integrated DoS/IDS Firewall

Telephony Features

- Caller ID
- Call Transfer
- Call Forward
- Call Park/Hold
- Voicemail
- IVR/Auto Attendant
- Hold Music
- Customizable Greetings

Integrated Conference Bridge

- Dial In/Dial Out
- Access Control
- Conference Recording
- E-Mail Notifications

Product Data Sheet

XSTACK™

IP Telephony

SIP IP-PBX with Conferencing Server

D-Link, an industry leader in networking, introduces the DVX-1000, a SIP-based IP-PBX for up to 25 extensions.

Internet IP telephony, also called Voice over IP (VoIP), is defined as the transport of telephone calls over the Internet as standard Internet data packets. Internet telephone calls can originate from traditional phone handsets via phone line-to-Internet (Analog Trunk) gateways, by PCs using software, or embedded devices (IP Phones). Most of the interest in Internet telephony is motivated by cost savings and ease of developing and integrating new services. Internet telephony integrates a variety of services provided by the current Internet and the Public Switched Telephone Network (PSTN) infrastructure.

The DVX-1000 offers all of the essential telephony features required for small businesses. Features such as call forwarding, call hold, find me-follow me, and voicemail. Incoming calls are directed by the integrated auto-attendant and hunt groups to assist callers to their destinations. It can utilize standard phone lines via an external phone line gateway or cost effective Internet Telephony services.

One unit can support up to 25 extensions, which can be located anywhere with Internet access. Multiple units can be used to increase number of extensions or unite a company that has many locations under a single PBX system.

The PBX phone features are user adjustable via the DVX-1000's web configuration tool. The administrator assigns each extension a profile of telephony features, which allows the best match for a user's job function. Each user can fine-tune their assigned profile via the web to match their daily business schedule.

Phone conferencing is typically expensive external hardware or service. The DVX-1000 includes a phone conferencing bridge, which makes it unsurpassed for value and features. Users are able to schedule and invite parties to conferences via the web configuration. Conference Notifications are sent out by e-mail, which includes the phone number and access codes.

The DVX-1000 uses advanced security features to protect your voice network from unauthorized access. To prevent hackers from breaching the system, the DVX-1000 uses MD5 SIP authentication encryption encoder software. The DVX-1000 also includes an integrated firewall for intrusion detection and protection against denial of service attacks.

The DVX-1000 features a fanless solid-state design offering years of non-stop operation. The compact housing can be easily fastened to the wall of your distribution closet or stacked with your existing Ethernet switches or PSTN Gateways. The DVX-1000 is designed with dual processors for supporting up to 25 simultaneous calls. Its class leading performance allows a 1-to-1 extension to phone line mapping, allowing it to scale with your business.

Utilizing our 19+ years of networking design technology and manufacturing, D-Link created the new xStack IP Telephony family. The DVX-1000 was designed to include all the necessary features of a phone system a company can depend upon.

XSTACK™

DVX-1000

SIP IP-PBX with Conferencing Server

Specifications

Management Features
- Includes 25 User Extensions
- Supports 25 simultaneous Inbound/Outbound calls
- Single IP PBX support multiple users across multiple sites
- Add external Analog Trunk Gateways to use standard phone-lines
- Save Money by using Internet Phone service (VoIP)
- User-Friendly Administration Interface
- Web-base Monitoring and Administration
- Call Statistics and Calling Detail Records

Basic Calling Features
- Basic Business Calling Features
- Caller ID, Call Transfer, Call History, Call Hold, Do Not Disturb, Call Forwarding (Always/on Busy/on No Answer/Follow me)

IVR/Auto-Attendant Features
- Music on Hold
- Attendant Override (Barge-In)
- Customizable Greetings
- Configurable IVR Menu
- Holiday List Configuration

Voicemail
- Mailbox Access Control (PIN)
- Configurable Mailbox Size
- Customizable Greetings
- Message Priority
- Notification Via E-mail

Security Features
- Built-in Firewall
- MD5 Authentication for SIP
- Secure Web Administrative and User Access for Configuration

Conference Server
- Dial In/Dial Out Conferences
- Access Control (PIN)
- Conference Recording

Protocol Standards
- SIP (RFC 3261)
- SDP (RFC 2327)
- RTP (RFC 1889)
- RTCP (RFC 1889)
- Out-Of-Band DTMF (RFC 2833)
- RTSP (RFC 2326)

Configuration
- Secure Web Based Management
- Configuration Backup/Restore
- Software Upgrade
- D-Link Endpoint Provisioning
- License Control for Advanced Features

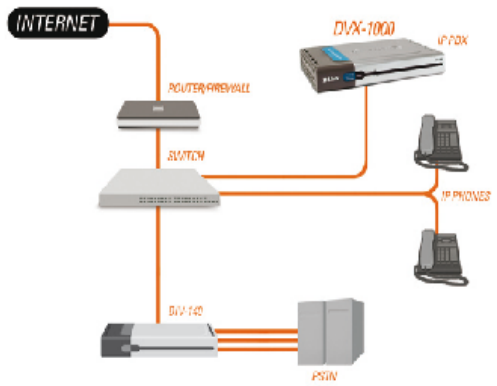
Hardware
- Dual Intel IXP-425 533 MHz StrongARM Processors
- 64 MB SDRAM (Expandable to 256 MB)
- 1 GB of storage (VM, Announcements)
- 10/100Mb Ethernet Port (RJ-45)

Physical
- Power LED
- LAN Link/Act
- Dimensions: 9.25" x 6.49" x 1.3"
- Power Input: 5V DC, 3A
- Power Adapter: 90~265V AC
- Power Consumption: 15 Watt Max
- Operating: 32° to 122° F
- Humidity: 5% to 95% (Non-condensing)

Warranty
1-Year Limited Warranty

Related products
- DIV-140: 4-Port Analog Trunk Gateway
- DVG-2001S: 1-Port Analog Terminal Adapter (ATA)
- DVG-1402S: Wired Router with 2-Port ATA
- DVG-G1402S: Wired/Wireless Router with 2-Port ATA
- DPH-140S: Wired Ethernet IP Phone

YOUR NETWORK SETUP
(INTEGRATE BOTH VoIP AND PSTN CALLS)



D-Link Systems, Inc. 17595 Mt Herrmann, Fountain Valley CA, 92708-4160 www.dlink.com ©2005 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link, the D-Link logo and XStack are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States and other countries. Other trademarks are the property of their respective owners. All references to speed are for comparison purposes only. Product specifications, size and shape are subject to change without notice, and actual product appearance may differ from that depicted herein. Visit www.dlink.com for more details.

D-Link®
Building Networks for People

A4. DWL-2100AP

D-Link®
Building Networks for People

108Mbps[1] Wireless Networking

DWL-2100AP

Up to 15x Faster

- Up to 108Mbps[1] with D-Link 108G Products
- Improved Wireless Security with WPA and 802.1X Authentication
- SNMP Management Software Included
- More Mobility with WDS and Five Operational Modes

2.4 GHz

ENHANCED SECURITY

SNMP MANAGEMENT SUPPORT

D-Link 108G

FREE 24/7 TECH SUPPORT

AirPlus XTREME G®

802.11g/2.4GHz Wireless

108Mbps[1] Access Point

D-Link, the industry pioneer in wireless networking, introduces a performance breakthrough in wireless connectivity – D-Link Air Plus Xtreme G™ series of high-speed devices now capable of delivering transfer rates up to 15x faster than the standard 802.11b with the new D-Link 108G. With the new Air Plus Xtreme G DWL-2100AP Wireless Access Point, D-Link sets a new standard for wireless access points.

With the D-Link 108G enhancement, the DWL-2100AP can achieve wireless speeds up to 15x in a pure D-Link 108G environment through the use of new wireless technologies such as Packet Bursting Fast Frame, Compression & Encryption, and Turbomode. These technologies enable a throughput high enough to handle video/audio streaming and future bandwidth-intense applications. The DWL-2100AP also supports SNMP v.3 for better network management with the provided Wireless AP Manager software that manages network configuration and firmware upgrades. For Enterprise networks, the DWL-2100AP supports network administration and real-time network traffic monitoring via D-Link's D-View Network Management software.

The DWL-2100AP features WDS (Wireless Distribution System) that can be configured to perform in any one of five modes: a Wireless Access Point, a Point-to-Point (PtP) bridge with another DWL-2100AP, a Point-to-Multipoint (PtMP) bridge, a Repeater for range extension, or as a Wireless Client. The WDS feature makes the DWL-2100AP an ideal solution for quickly creating and extending a wireless local area network (WLAN) in offices or other workplaces, or even at hotspots.

Wireless security is addressed as the DWL-2100AP uses WPA (Wi-Fi Protected Access) and 802.1X authentication to provide a higher level of security for data communication amongst wireless clients. The DWL-2100AP is also fully compatible with the IEEE 802.11b and 802.11g standards. With great manageability, versatile operation modes, solid security enhancement, the cost-effective D-Link Air Plus Xtreme G DWL-2100AP Wireless Access Point provides the ultra-fast wireless signal rates and everything else a network professional dreams of.

AirPlusXtremeG®

DWL-2100AP

802.11g/2.4GHz Wireless

108Mbps[1] Access Point

SPECIFICATIONS

Standards
- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.11
- IEEE 802.3
- IEEE 802.3u

Device Management
- Web-Based – Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java- enabled browsers.
- SNMP v.3

Wireless Distribution System
- AP Client
- PtP Bridge
- PtMP Bridge
- Repeater

Security
- 64-, 128 152-bit WEP
- 802.1X (EAP-MD5, EAP-TLS, EAP-TTLS and EAP-PEAP)
- WPA —Wi-Fi Protected Access
- MAC Address Access Control (WPA-TKIP and WPA-AES)

Media Access Control
CSMA/CA with ACK

Wireless Frequency Range
2.4GHz to 2.4835GHz

Wireless Operating Range [2]
Indoors: Up to 328 ft (100 meters)
Outdoors: Up to 1312 ft (400 meters)

Modulation Technology
- Orthogonal Frequency Division Multiplexing (OFDM)
- Complementary Code Keying (CCK)
- DQPSK
- DBPSK

Wireless Transmit Power
15dBm (32mW) ± 2dB
(Control TX power level from full, 50%, 25%, 125% and min.)

Receiver Sensitivity
- 54Mbps OFDM, 10% PER, -66dBm)
- 48Mbps OFDM, 10% PER, -71dBm)
- 36Mbps OFDM, 10% PER, -76dBm)
- 24Mbps OFDM, 10% PER, -80dBm)
- 18Mbps OFDM, 10% PER, -83dBm)
- 12Mbps OFDM, 10% PER, -85dBm)
- 11Mbps CCK, 8% PER, -83dBm)
- 9Mbps OFDM, 10% PER, -86dBm)
- 6Mbps OFDM, 10% PER, -87dBm)
- 2Mbps QPSK, 8% PER, -89dBm)

External Antenna Type
1.0dB Dipole with reverse SMA connector

LEDs
- Power
- LAN (10/100)
- WLAN (Wireless Connection)

Temperature
- Operating: 32°F to 140°F (0°C to 40°C)
- Storing: 4°F to 149°F (-20°C to 65°C)

Humidity
95% maximum (non-condensing)

Power Input
Ext. Power Supply DC 5V, 2.0A

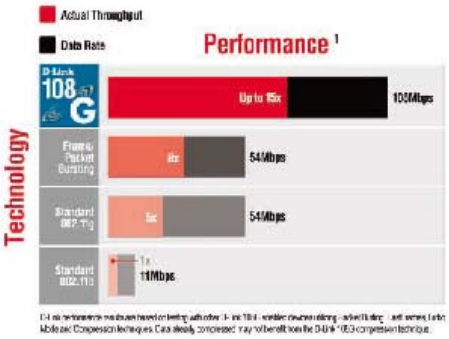
Safety & Emissions
- FCC • UL • VCCI • CSA • EN

Dimensions
- L = 5.6 inches (142mm)
- W = 4.3 inches (109mm)
- H = 1.2 inches (31mm)

Weight
0.44 lbs (200g)

Warranty
3 Year

[1] Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.
[2] Environmental conditions may adversely affect wireless signal range.



D-Link Systems, Inc. 17595 Mt. Herrmann Street Fountain Valley CA 92708 www.dlink.com
©2004 D-Link Corporation/D-Link Systems, Inc. All rights reserved. D-Link, the D-Link logo and AirPlus Xtreme G are registered trademarks of D-Link Corporation or its subsidiaries in the United States and other countries. Other trademarks are the property of their respective owners. All references to speed are for comparison purposes only. Product specifications, size and shape are subject to change without notice, and actual product appearance may differ from that depicted herein.
Visit www.dlink.com for more details.

D-Link®
Building Networks for People

REFERENCIAS BIBLIOGRÁFICAS

LIBROS:

- PCM WIRELESS SOLUTIONS
  (John Wiley & Sons LTD)

- WIRELESS: LOS MEJORES TRUCOS (2º ED)
  Flickenger, Rob y Weeks,Roger
  Nº Edición**:**2ª
  Año de edición:2006
  Plaza edición: Madrid

- EMERGING WIRELESS MULTIMEDIA SERVICES AND TECHNOLOGIES
  Salkintzis, Apostolis (Wiley John + Sons)

- CAMARAS IP: COMO VIGILAR TU CASA Y TU NEGOCIO POR INTERNET O DESD E EL MOVIL DESDE CUALQUIER LUGAR DEL MUNDO
  Lopez Gomez, Javier
  Nº Edición**:**1ª
  Año de edición:2007
  Plaza edición: Madrid

- COMUNICACIONES EN REDES WLAN
  Huidobro Moya, Jose Manuel
  Nº Edición**:**1ª
  Año de edición:2005
  Plaza edición: Las Rozas

- ADMINISTRACION DE SISTEMAS LINUX (ANAYA MULTIMEDIA/O REILLY)
  Adelstein, Tom y Lubanovic, Bill

Nº Edición**:**1ª

Año de edición:2007

Plaza edición: Madrid

PÁGINAS WEB:

- *Equipos DLINK*

http://www.dlink.com/products/?pid=450

http://www.dlinkla.com/home/productos/servicios_05.jsp

http://www.redaragon.com/informatica/wireless/redwireless.asp

http://www.zero13wireless.net/foro/showthread.php?t=1813

http://www.forosdelweb.com/f20/configuracion-dcs-2120-a-486003/

- *Servidores Linux*

http://www.xserver.cl/configuraciondeservidores.php

http://www.xserver.cl/configuraciondeservidores.php

http://www.sorgonet.com/collaborations/servidor-ies/

http://es.tldp.org/COMO-INSFLUG/COMOs/Servidor-Intranet-Como/Servidor-Intranet-Como-4.html

- *Redes WLAN*

http://www.radioptica.com/Radio/estandares_WLAN.asp

http://www.redaragon.com/informatica/wireless/redwireless.asp

- *VoIP*

http://www.recursosvoip.com/

http://www.eurocomm-group.eu/soluciones/soluciones_masinfo.php?t=2&id=59

HOJA DE LEGALIZACIÓN

Juan Carlos Brito Vallejo **Luisa Daniela Macas Pallo**

AUTORES

Ing. Carlos Romero

DIRECTOR CARRERA REDES Y COMUNICACIÓN DE DATOS

Sangolquí, 06 de octubre del 2008

HOJA DE LEGALIZACIÓN

Juan Carlos Brito Vallejo	**Luisa Daniela Macas Pallo**

AUTORES

Ing. Gonzalo Olmedo

DIRECTOR CARRERA TELECOMUNICACIONES

Sangolquí, 06 de octubre del 2008