PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

DISERTACIÓN DE GRADO

TEMA:

"IMPLEMENTACIÓN DE TECNOLOGÍA IP PARA TRANSMISIÓN DE IMÁGENES EN LA PUCESA EN EL PERÍODO 2006-2007"

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
BIBLIOTECA

ESCUELA:

INGENIERÍA DE SISTEMAS

PROPONENTE:

VERÓNICA DE LOS ÁNGELES VALDEZ SIERRA

SECRETARIA GENERAL
PROCURADURIA

AMBATO, 2006

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

ESCUELA DE INGENIERÍA DE SISTEMAS

DISERTACIÓN DE GRADO PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERÍA DE SISTEMAS

"IMPLEMENTACIÓN DE TECNOLOGÍA IP PARA TRANSMISIÓN DE IMÁGENES EN LA PUCESA EN EL PERÍODO 2006-2007"

DIRECTOR:

Ing. Janio Jadán MSc. MBA.

PROPONENTE:

VERÓNICA DE LOS ÁNGELES VALDEZ SIERRA

DEDICATORIA

Les dedico este trabajo a todas las personas que creyeron en mi sin dudar, que me apoyaron y ayudaron incondicionalmente de una u otra forma a terminar este proyecto, y con esto culminar felizmente una etapa de mi vida.

También a todas esas personas que utilizarán este trabajo para de el aprender algo nuevo, asi tendré la satisfacción de que todo el esfuerzo entregado al mismo habrá sido útil para ayudar a alguien mas.

AGRADECIMIENTO

Agradezco a mis padres por haber confiado en mi siempre, por apoyarme y ayudarme no solamente a terminar este proyecto sino en toda las etapas de mi vida, por brindarme amor y muchos momentos felices.

A mis hermanos por sus consejos sabios y palabras de aliento, por estar a mi lado en todo momento, por pensar siempre en mi bienestar.

A mi esposo, por todo su amor y ayuda incondicional, por enseñarme que con esfuerzo y perseverancia no existen imposibles, y que juntos con amor podemos vencer cualquier obstáculo, aprender de el y asi ser mejores cada dia.

A mi hijito, que con su sonrisa me da las energias que necesito para salir adelante y me recuerda agradecerle a Dios por estar viva cada dia y por todas las bendiciones que me regala.

No podria olvidarme de mis maestros que con paciencia supieron enseñarme los conocimientos para desenvolverme eficazmente en el mundo del trabajo a si ser una persona productiva para la sociedad.

A todas estas personas muchas gracias y que Dios les colme de Bendiciones siempre...

INDICE DE CONTENIDOS

PORTADA ____ i

CONTRAPORTADA ____ ii

DEDICATORIA ____ iii

AGRADECIMIENTO ____ iv

INDICE DE CONTENIDOS ____ v

INDICE DE FIGURAS ____ ix

INDICE DE TABLAS ____ xi

CAPITULO I ____ 1

1. PROYECTO DE INVESTIGACIÓN ____ 1

1.1. INTRODUCCIÓN ____ 1

1.2. PLANTEAMIENTO DEL PROBLEMA ____ 2

1.2.1. Problema ____ 2

1.2.2. Problematización ____ 2

1.3. DELIMITACIÓN ____ 2

1.4. IMPORTANCIA Y JUSTIFICACIÓN ____ 3

1.4.1. Importancia ____ 3

1.4.2. Justificación ____ 4

1.5. OBJETIVOS ____ 4

1.5.1. Objetivo General ____ 4

1.5.2. Objetivos Específicos ____ 4

1.6. HIPÓTESIS ____ 5

1.7. ASPECTOS METODOLÓGICOS ____ 5

1.7.1. Fundamentos Teóricos ____ 5

1.7.2. Métodos de Investigación ____ 6

1.7.3. Tipo de investigación ____ 6

1.7.4. Nivel de investigación ____ 6

CAPITULO II ____ 8

2. MARCO TEÓRICO ____ 8

2.1. FUNDAMENTOS DE LA ARQUITECTURA TCP/IP 8
2.1.1. Generalidades 8
2.1.1.1. Capa Física 8
2.1.1.2. Capa de Acceso a la Red 9
2.1.1.3. Capa de Red 9
2.1.1.4. Capa de Transporte 9
2.1.1.5. Capa de Aplicación 9
2.1.2. Protocolos TCP/IP 10
2.1.2.1. Protocolo IP 11
2.1.2.2. Direcciones IP 14
2.1.2.2.1. Clasificación de la Direcciones IP 14
2.1.2.2.2. Estructura de las Direcciones IP 15
2.1.2.2.3. Clases de Direcciones IP 16
2.1.2.2.4. Difusión (broadcast) y multidifusión (multicast) 16
2.1.2.2.5. Direcciones IP Especiales y Reservadas 18
2.1.2.3. Máscara de subred 19
2.1.2.4. Encaminamiento (Enrutamiento) 21
2.1.2.5. Protocolo TCP 22
2.1.3. Intranet 23
2.1.4. Extranet 23
2.1.5. Internet 23
2.1.6. Banda Ancha 24
2.2. VOZ Y VIDEO SOBRE IP 26
2.2.1. Voz sobre IP 26
2.2.2. Protocolos de Voz sobre IP 27
2.2.2.1. H.323 28
2.2.2.2. Session Initiation Protocol (SIP) 28
2.2.2.3. Voz sobre IP en aplicaciones 28
2.2.3. Video sobre IP 29
2.2.3.1. Video Broadcast sobre IP 29
2.2.3.2. Video on Demand (VOD) sobre IP 30
2.2.3.3. Videoconferencia sobre IP 30
2.2.3.4. Video Digital sobre IP 31
2.2.3.5. Normas de Compresión de Video 33

2.2.3.6. Normas para Vídeo sobre IP 35
2.2.3.7. Bits y Bytes de Ancho de Banda 35
2.2.3.8. Cuellos de Botella y Obstáculos 36
2.3. Cámaras IP 37
2.3.1. Qué es una cámara IP? 38
2.3.2. Funcionamiento de una cámara IP 39
2.3.3. Ventajas de una Cámara IP 42
2.3.4. Aplicaciones de las Cámaras IP 43
2.3.5. Tipos de cámaras IP 44
2.4. MONITOREO Y VIGILANCIA DE CENTROS EDUCATIVOS 45
2.4.1. Firewall 46
2.4.2. Proxy 47
2.4.3. Autenticación 48
2.5. ACCESO REMOTO 49

CAPITULO III 50
3.1. ANALISIS DE LA RED DE LA PUCESA 50
3.2. SELECCIÓN DE LA CÁMARA IP 50
3.3. Cámara IP D-Link CS-5300 51
3.3.1. Características Principales 52
3.3.2. Ficha Técnica 52
3.4. Análisis de la Instalación de una Cámara IP 54
3.4.1. Configuración básica para una sola cámara 57
3.4.2. Configuración básica para varias cámaras con un router doméstico 58
3.4.3. Direcciones IP estáticas o dinámicas 59
3.4.4. Nombre de dominio para las cámaras 59
3.4.5. Acceso y publicación 60
3.4.6. Instalación de la Cámara IP D-Link CS-5300 en la PUCESA 60
3.4.6.1. Instalación del hardware 60
3.4.6.2. Instalación del software y configuración básica 63
3.4.7. Manejo y uso de la cámara 68
3.4.7.1. Tipo de conexión 71
3.4.7.2. Administración de usuarios 72
3.4.7.3. Configuración de red 74

3.4.7.4. Configuración de audio y video 76
3.4.7.5. Ajustes de la imagen 78
3.4.7.6. Control de la cámara 78
3.4.7.7. Detección de movimiento 80
3.4.7.8. Configuración del sistema 81
3.4.8. Instalación de la cámara a través de un router 82
3.4.8.1. Asignar una dirección IP local a la cámara 83
3.4.8.2. Conectarse a la cámara a través del Internet Explorer 83
3.4.8.3. Configuración en el router 84
3.4.8.4. Abrir el servidor de puertos virtuales del router 85
3.4.9. Desarrollo de la Aplicación 86
3.4.9.1. Diseño de la Base de Datos 86
3.4.9.2. Diseño del Sitio Web 87
3.4.9.3. Utilización del Sitio Web 93

CAPITULO IV 102
4. VALIDACIÓN Y VERIFICACIÓN DE RESULTADOS 102
4.1. Conclusiones 102
4.2. Recomendaciones 103

BIBLIOGRAFÍA 105
GLOSARIO 106

INDICE DE FIGURAS

Figura 1: Ejemplo de conexión de tres redes con diferentes IP 11
Figura 2: Cabecera de un paquete IP 12
Figura 3: Ejemplo de aplicación de máscaras en una red 21
Figura 4: Banda Ancha con ADSL 25
Figura 5: Configuración básica de un sistema de Voz sobre IP 27
Figura 6: Esquema de una red con Video sobre IP 33
Figura 7: Esquema de conexión de una cámara IP 38
Figura 8: Estructura básica de una cámara IP 39
Figura 9: Estructura ampliada de una cámara IP 39
Figura 10: Utilización de firewall en una red con cámara IP 47
Figura 11: Vista externa y partes principales de la cámara D-Link CS-5300 51
Figura 12: Conexión de una cámara IP a una LAN 54
Figura 13: Conexión de una cámara IP a través de un Router 55
Figura 14: Conexión de una cámara IP a través de un Módem 55
Figura 15: Conexión de una cámara IP a un computador 55
Figura 16: Conexión del cable UTP a la cámara 61
Figura 17: Conexión del cable de poder a la cámara 61
Figura 18: Conexión del cable de Audio/Video a la cámara 62
Figura 19: Conexión del cable de Video al Televisor 62
Figura 20: Conexión del cable de Audio al Televisor 63
Figura 21: Pantalla de Bienvenida y Menú Principal para instalación de la cámara 63
Figura 22: Software buscando cámaras conectadas 64
Figura 23: Orificio para reset 64
Figura 24: Datos de la(s) cámara(s) detectada(s) 65
Figura 25: Configuración básica 66
Figura 26: Configuración de parámetros de red 67
Figura 27: Guardando cambios 67
Figura 28: Pantalla principal de visualización y manejo 68
Figura 29: Controles de manejo 69
Figura 30: Controles de posición 69
Figura 31: Esquema del mando a distancia 70
Figura 32: Opciones de zoom digital 70

PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
SEDE AMBATO
BIBLIOTECA

Figura 33: Imagen capturada con Snapshot 71
Figura 34: Tipos de protocolos 72
Figura 35: Administración de usuarios 73
Figura 36: Parámetros de red, servidor de correo y servidor FTP 74
Figura 37: Configuración de Audio y Video 77
Figura 38: Ajustes de la imagen 78
Figura 39: Control de la cámara 79
Figura 40: Configuración de detección de movimiento 80
Figura 41: Configuración de hora y fecha 81
Figura 42: Dirección IP de la cámara 83
Figura 43: Configuración de puertos 84
Figura 44: Esquema de navegación del sitio Web 87
Figura 45: Diseño página principal 88
Figura 46: Diseño página "cámaras" 89
Figura 47: Diseño página "ingreso de cámaras" 90
Figura 48: Diseño página "ingreso de usuarios" 91
Figura 49: Página principal del sitio 93
Figura 50: Listado de cámaras 93
Figura 51: Ingreso de usuario y contraseña 94
Figura 52: Página de conexión a la cámara 95
Figura 53: Ingreso a administración del sitio 96
Figura 54: Menú principal de administración 97
Figura 55: Ingreso de cámaras 98
Figura 56: Eliminación de cámaras 99
Figura 57: Ingreso de usuarios 100
Figura 58: Eliminación de usuarios 101
Figura 59: Cierre de sesión 101

INDICE DE TABLAS

Tabla 1: Modelo de referencia TCP/IP 8
Tabla 2: Enrutamiento para la interconexión de tres redes 11
Tabla 3: Resumen de las clases de direcciones IP 16
Tabla 4: Direcciones IP especiales y reservadas 18
Tabla 5: Rango de direcciones reservadas 18
Tabla 6: Máscaras de subred de cada clase 19
Tabla 7: Direcciones y máscara en binario 19
Tabla 8: Parámetros de red para las cámaras IP 56
Tabla 9: Direcciones IP y puertos de la cámara 59
Tabla 10: Estructura de la tabla "camaras" 86
Tabla 11: Estructura de la tabla "users" 87

CAPITULO I

1. PROYECTO DE INVESTIGACIÓN

1.1. INTRODUCCIÓN

Desde hace varias décadas el país se ha visto envuelto en problemas delincuenciales, y en países del tercer mundo como el Ecuador ha sido imposible erradicar en su totalidad este tipo de atropellos a la privacía de las personas e instituiciones, es así que la seguridad pública no basta, y la sociedad apoyada de herramientas tecnológicas podría prevenir hechos futuros que tengan como causal el quebrantamiento de las seguridades. En países desarrollados que poseen la tecnología necesaria, ya se están aplicando medios que permitan establecer controles y vigilancia desde cualquier lugar del mundo. En el Ecuador existe un caso en particular en donde ya se ha comenzado a utilizar un sistema de vigilancia por medio de cámaras de video, éste es el Sistema Ojos de Aguila instalado en la capital de la república.

Dentro de la ciudad de Ambato se ha podido observar que entidades bancarias o financieras utilizan circuitos cerrados de televisión para monitorear actos delictivos. Muchos de éstos equipos y programas son importados y costosos, de ahí el interés de la presente disertación para construir un sistema de monitoreo remoto por medio de cámaras a través del Internet utilizando recursos disponibles en nuestro medio.

La Pontificia Universidad Católica del Ecuador Sede Ambato, ha sido testigo tiempo atrás de algunos incidentes de inseguridad y de actividades no acordes al propósito de brindar una educación de excelencia a sus educandos. En este sentido se ha podido palpar una mayor afluencia de personas que creen en la garantía de la PUCESA, y de ahí que sus autoridades necesitan ejercer un control y vigilancia de las instalaciones desde cualquier lugar del mundo gracias a las nuevas tecnologías.

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Problema

No existe en la PUCESA un sistema de vigilancia remoto con tecnologia IP que muestre video real a través de Internet y que permita mantener la seguridad y control de los accesos a las edificaciones de la Universidad, durante el periodo 2006 - 2007.

1.2.2. Problematización

- La falta de un sistema de control de las actividades que se realicen en zonas críticas de la PUCESA en horas no laborables o cuando el personal administrativo no se encuentre en la Universidad.

- No existen nuevas tecnologías que ayuden a complementar el cuidado de los bienes de la Universidad.

- La carencia de un sistema que aproveche la tecnología IP que actualmente posee la PUCESA con fines de seguridad y vigilancia.

1.3. DELIMITACIÓN

La solución al problema planteado se lo realizará dentro del Campus Universitario de la Pontificia Universidad Católica del Ecuador, Sede Ambato, ubicada en la Provincia de Tungurahua, cantón Ambato, sector El Tropezón, durante el periodo 2006-2007.

Para posibilitar la implementación de un sistema de control y vigilancia de los accesos críticos a las dependencias de la Universidad por medio de cámaras IP, es necesario utilizar su plataforma tecnológica que ya posee, es decir su acceso a Internet por banda ancha, su red IP tanto cableada como inalámbrica.

El Hardware necesario para la implementación es una cámara IP conectada a uno de los concentradores de la red de la Universidad. Para una posible expansión de los sitios de

cobertura bastaría con conectar a otro punto del concentrador. Para lograr mayor definición se utilizará una cámara IP con conexión por cable y no inalámbrica.

Para el acceso mediante Internet se desarrollará una página Web que permita autenticar a personas autorizadas, así como la lista de cámaras disponibles, en dónde se pueda seleccionar una y de ésta forma se muestre el video en tiempo real.

Previo el proceso de desarrollo e implantación se investigará la mejor alternativa de configuración en cuanto se refiere a configuración de Proxy, IP pública y la compatibilidad con el sistema Linux instalado en el servidor Solaris que permite la conexión a Internet.

El tiempo aproximado para la culminación del presente trabajo es de seis meses contados a partir de la fecha de elaboración del plan de tesis.

1.4. IMPORTANCIA Y JUSTIFICACIÓN

1.4.1. Importancia

A nivel local la PUCESA podría mejorar el control de accesos a las dependencias y por ende accesos a documentos y bienes de propiedad de la universidad ya que lo que capta la cámara se puede ver desde cualquier computador local o desde cualquier parte del mundo con el nivel de seguridad respectivo.

Al mismo tiempo se puede verificar que: empleados, docentes, y estudiantes sigan los procedimientos y políticas establecidas, a fin de que todas las labores se lleven a cabalidad.

A nivel provincial la Universidad Católica sería una de las pocas, por no decir la única entidad educativa que posea éste tipo de tecnologías. Además de funcionar como sistema de vigilancia, la universidad podría en el futuro utilizarlo como medio de promoción ya que también se puede usar para transmitir eventos en vivo por Internet.

A nivel Nacional será de gran importancia porque se lograría sentar un precedente que pueda ser imitado por otras sedes y de ésta manera lograr tener acceso visual de ellas para apoyar a las metas del Sistema Nacional de Universidades Católicas del Ecuador.

1.4.2. Justificación

Desde el punto de vista Tecnológico se justifica la implementación de un Sistema de vigilancia remoto de los predios de la PUCESA, al existir una plataforma tecnológica de acceso a Internet por medio de banda ancha, y al existir una red IP cableada e inalámbrica. Así como la posibilidad de adquirir en nuestro medio una cámara IP para su posterior configuración e implementación.

En cuanto a lo Económico, las nuevas tecnologías son cada vez menos costosas, y el único hardware indispensable que no se lo fabrica en el ámbito nacional sería la cámara IP, que complementado con el ingenio y formación académica se logrará desarrollar el nivel de configuración y software adicional, por lo que se está en capacidad de desarrollar este proyecto.

1.5. OBJETIVOS

1.5.1. Objetivo General

Implementar un sistema de vigilancia remoto con tecnología IP a través de una cámara que permita acceso de video a la universidad por medio del Internet, para así mantener la seguridad y control de los accesos a las edificaciones de la PUCESA.

1.5.2. Objetivos Específicos

- Investigar la mejor alternativa de configuración de una Cámara IP y su integración con la plataforma existente en la Pontificia Universidad Católica del Ecuador, Sede Ambato.

- Integrar a la Universidad nuevas tecnologías que permitan la vigilancia de los accesos a las edificaciones y el cuidado de los bienes existentes, a cualquier hora y desde cualquier lugar del mundo a través del Internet.

- Implementar un sistema de seguridad y control de las actividades que se realicen en la Universidad por medio de una CÁMARA IP ubicada estratégicamente en los predios de la PUCESA.

1.6. HIPÓTESIS

Mediante la Implementación de un sistema de vigilancia remoto con tecnología IP, la PUCESA dispondrá de mayor seguridad y control de los accesos a las edificaciones a cualquier hora y desde cualquier lugar del mundo por parte de personal autorizado.

1.7. ASPECTOS METODOLÓGICOS

1.7.1. Fundamentos Teóricos

En este proyecto de disertación se utilizarán tres paradigmas descritos a continuación:

- **Empirista:** Porque toda actividad se llevará a cabo en base a la práctica y a los conocimientos adquiridos durante el desarrollo del proyecto.

- **Racionalista:** Porque el proyecto tiene preconcebida la implementación de hardware y configuración de software que integren todo un sistema.

- **Pragmatista:** Puesto que como resultado final se logrará la implementación y funcionamiento del Sistema de vigilancia remoto con tecnología IP, independientemente de los medios que se utilicen para llegar a éste propósito.

1.7.2. Métodos de Investigación

Durante el proceso de investigación del presente proyecto de disertación, se utilizarán conjuntamente:

- **El Método Científico**: Para plantear los fundamentos teóricos de la investigación.

- **Investigación Experimental**: En la medida en que se ejecutará experimentación en la realización de la página Web que permitirá acceso al sistema y en la búsqueda del hardware adecuado que permita la culminación del proyecto

1.7.3. Tipo de investigación

Para la realización de este proyecto de disertación se aplicarán tres tipos de investigación:

- **Investigación de Tipo Inductiva**: Puesto que se realizará primeramente un estudio concreto de las especificaciones de los componentes de hardware que se van a utilizar.

- **Investigación de Tipo Deductiva**: Ya que se analizará como realizar la estructura de acceso al Sistema en forma general, para aplicarlo en el desarrollo de este proyecto.

- **Investigación de Tipo Bibliográfica**: Puesto que se realizará primeramente un estudio de las especificaciones de los componentes de hardware y su compatibilidad con la tecnología IP existente en la Universidad.

1.7.4. Nivel de investigación

El nivel de investigación se resumirá en los tres puntos más importantes:

- Investigar la configuración actual de la red IP y los cambios necesarios para lograr la salida de video al Internet.

- Integrar una Cámara IP a la red de la Universidad

- Desarrollar páginas Web de acceso con niveles de seguridad.

En conclusión, el proyecto de investigación será de tipo aplicado, porque se realizarán estudios y trabajos directos con la configuración del hardware y el desarrollo de páginas Web que permitan el acceso al video que muestra la Cámara IP.

CAPITULO II

2. MARCO TEÓRICO

2.1. FUNDAMENTOS DE LA ARQUITECTURA TCP/IP

2.1.1. Generalidades

La familia de protocolos que se eligieron para permitir que Internet sea una "*Red de redes*" es TCP/IP, decimos familia de protocolos ya que son muchos los protocolos que la integran, aunque para simplificar hablamos sencillamente del protocolo TCP/IP (Transport Control Protocol / Internet Protocol).

El protocolo TCP/IP tiene que estar a un nivel superior del tipo de red empleado y funcionar de forma transparente en cualquier tipo de red; y a un nivel inferior de los programas de aplicación particulares (páginas WEB, correo electrónico, entre otros) de cada sistema operativo. Todo esto nos sugiere el siguiente modelo de referencia:

Capa de aplicación (HTTP, SMTP, FTP, TELNET, entre otros)

Capa de transporte (UDP, TCP)

Capa de red (IP)

Capa de acceso a la red (Ethernet, Token Ring, entre otros)

Capa física (cable coaxial, par trenzado, banda ancha, entre otros)

Tabla 1: Modelo de referencia TCP/IP

2.1.1.1. Capa Física

El nivel más bajo es la capa física, aquí nos referimos al medio físico por el cual se transmite la información. Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión como fibra óptica, microondas o enlaces vía satélite.

2.1.1.2. Capa de Acceso a la Red

La capa de acceso a la red determina la manera en que las estaciones (computadores) envían y reciben la información a través del soporte físico proporcionado por la capa anterior. Es decir, una vez que tenemos un cable, ¿Cómo se transmite la información por ese cable? ¿Cuándo puede una estación transmitir? ¿Tiene que esperar algún turno o transmite sin más? ¿Cómo sabe una estación que un mensaje es para ella? Pues bien, son todas estas cuestiones las que resuelve esta capa.

2.1.1.3. Capa de Red

La capa física y la capa de acceso a la red quedan a un nivel inferior del protocolo TCP/IP, es decir, no forman parte de este protocolo. La capa de red define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino.

El principal protocolo de esta capa es el IP aunque también se encuentran a este nivel los protocolos ARP, ICMP e IGMP. Esta capa proporciona el direccionamiento IP y determina la ruta óptima a través de los ruteadores (*routers*) que debe seguir un paquete desde el origen al destino. Un router (enrutador o router) es un dispositivo hardware o software de interconexión de redes de computadores que opera en la capa de red. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red. Un router puede también ser un computador con varias direcciones IP, una para cada red, que permita el tráfico de paquetes entre sus redes.

2.1.1.4. Capa de Transporte

La capa de transporte (protocolos TCP y UDP) ya no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza.

2.1.1.5. Capa de Aplicación

Una vez que tenemos establecida la comunicación desde el origen al destino nos queda lo más importante, ¿qué podemos transmitir? La capa de aplicación nos proporciona los distintos servicios de Internet: correo electrónico, páginas Web, FTP, TELNET.

2.1.2. Protocolos TCP/IP

La familia de protocolos TCP/IP fue diseñada para permitir la interconexión entre distintas redes. El mejor ejemplo de interconexión de redes es Internet: se trata de una verdadera red de redes a nivel mundial.

Se pueden construir redes privadas que funcionen siguiendo el mismo esquema de Internet. En una red TCP/IP es posible tener, por ejemplo, servidores Web y servidores de correo para uso interno. Obsérvese que todos los servicios de Internet se pueden configurar en pequeñas redes internas TCP/IP, denominadas "Intranets".

A continuación se muestra un ejemplo de interconexión de tres redes, cada nodo o *host* (computador) tiene una dirección física que viene determinada por su adaptador de red. Estas direcciones se corresponden con la capa de acceso al medio y se utilizan para comunicar dos computadores que pertenecen a la misma red. Para identificar globalmente un computador dentro de un conjunto de redes TCP/IP se utilizan las direcciones IP (capa de red). Observando una dirección IP sabremos si pertenece a nuestra propia red o a una distinta (todas las direcciones IP de la misma red comienzan con los mismos números, según veremos más adelante).

Host	Dirección física	Dirección IP	Red
A	00-60-52-0B-B7-7D	192.168.0.10	Red 1
R1	00-E0-4C-AB-9A-FF	192.168.0.1	
	A3-BB-05-17-29-D0	10.10.0.1	Red 2
B	00-E0-4C-33-79-AF	10.10.0.7	
R2	B2-42-52-12-37-BE	10.10.0.2	
	00-E0-89-AB-12-92	200.3.107.1	Red 3
C	A3-BB-08-10-DA-DB	200.3.107.73	
D	B2-AB-31-07-12-93	200.3.107.200	

Tabla 2: Enrutamiento para la interconexión de tres redes

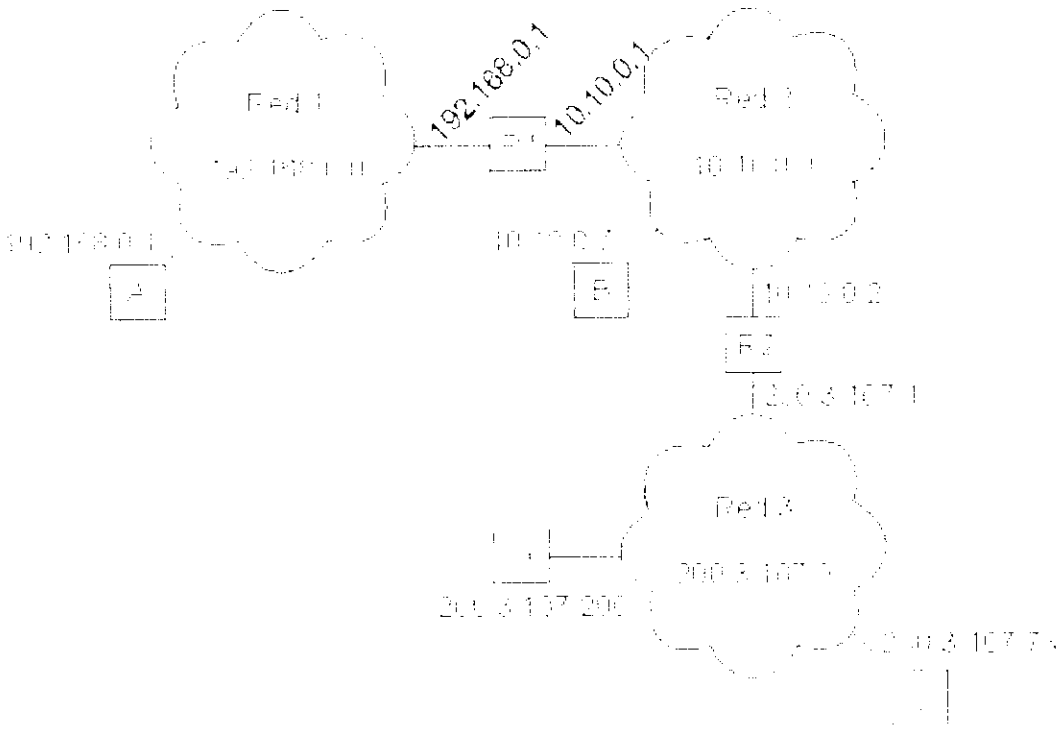


Figura 1: Ejemplo de conexión de tres redes con diferentes IP

2.1.2.1. Protocolo IP

IP es el principal protocolo de la capa de red. Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes. Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Es un sistema de entrega de paquetes (*datagramas IP*) que tiene las siguientes características:

- Es no orientado a conexión debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.

- Es no fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

El concepto de red está relacionado con las direcciones IP que se configuren en cada computador, no con el cableado. Es decir, si tenemos varias redes dentro del mismo

cableado solamente los computadores que pertenezcan a una misma red podrán comunicarse entre sí. Para que los computadores de una red puedan comunicarse con los de otra red es necesario que existan routers que interconecten las redes.

La capa de red se encarga de fragmentar cada mensaje en paquetes de datos llamados Datagramas IP y de enviarlos de forma independiente a través de la red de redes. Cada datagrama IP incluye un campo con la dirección IP de destino. Esta información se utiliza para enrutar los datagramas a través de las redes necesarias que los hagan llegar hasta su destino.

Un datagrama IP consiste en una parte de cabecera y en una parte de datos cuyo tamaño es variable.

Cabecera

En la cabecera hay una parte fija de 20 bytes y una parte opcional de longitud variable. En la Figura 2 se puede observar el formato de la cabecera IP:

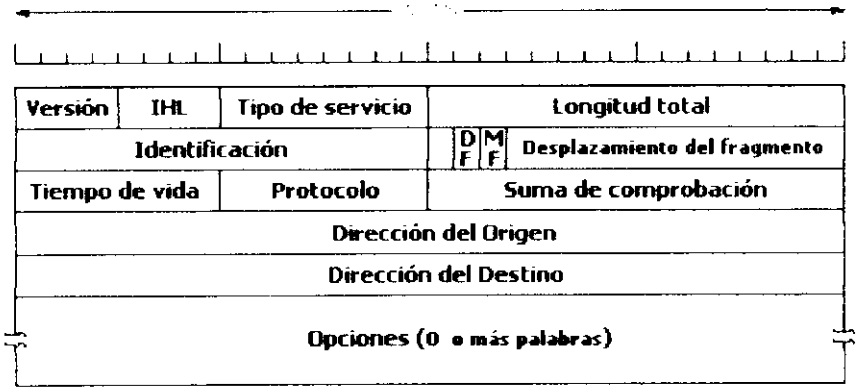


Figura 2: Cabecera de un paquete IP

Versión (4 bits): Número de versión del protocolo al que pertenece el datagrama.

IHL (Internet Header length) (4 bits): Longitud de la cabecera en palabras de 32 bits (4 bytes).

Tipo de servicio (8 bits): Permite que el host especifique que tipo de servicio quiere, pudiéndose combinar confiabilidad y velocidad. Para el video digitalizado es más importante realizar la entrega de forma rápida que precisa, mientras que para

la transferencia de archivos no importa a que velocidad se realiza la transferencia pero si que esté libre de errores.

Longitud total (16 bits): Longitud total en bytes que tendrá todo el datagrama, considerando tanto la cabecera como los datos.

Identificador (16 bits): Es un número de secuencia que junto a la dirección origen, la dirección destino y el protocolo de usuario, sirven para que la máquina destino determine a qué datagrama pertenece el fragmento que ha recibido.

Indicadores (3 bits): El primer bit no se utiliza actualmente. El indicador de más fragmentos (MF) cuando vale 1 indica que este datagrama tiene más fragmentos y toma el valor 0 en el último fragmento. El indicador de no fragmentar (DF) prohíbe la fragmentación cuando vale 1. Es una orden que se le da a los routers de que no fragmenten el datagrama cuando el destino es incapaz de reensamblarlo. Si este bit vale 1, el datagrama se descartará si se excede el tamaño máximo en una subred de la ruta.

Desplazamiento del fragmento (13 bits): Indica en qué posición del datagrama original, medido en unidades de 8 bytes (64 bits), va el fragmento actual.

Tiempo de vida (8 bits): Es un contador que sirve para limitar la vida de un paquete. Aunque lo lógico sería pensar que cuenta el tiempo en segundos, en realidad lo que cuenta es el número de saltos de dispositivo de encaminamiento que realiza.

Protocolo (8 bits): Se utiliza por la capa de red para saber a qué protocolo de la capa de transporte le tiene que enviar el datagrama una vez que lo ha reensamblado. Existen diferentes protocolos de transporte, entre ellos TCP y UDP. En el RFC 1700 ("Request For Comments") se definen todos estos protocolos, el RFC es la pila donde se encuentra la lista de protocolos de Internet.

Suma de comprobación (16 bits): Sirve para verificar el contenido de la cabecera y es útil para la detección de errores generados durante la transmisión del datagrama.

Dirección origen (32 bits): Indica el número de red y el número del computador que envía el datagrama.

Dirección destino (32 bits): Indica el número de red y el número del computador al que se envía el datagrama.

Opciones (variable): Contiene las opciones solicitadas por el usuario que envía los datos y se diseñó para que las versiones posteriores del protocolo pudieran incluir información no considerada originalmente.

Relleno (variable): El campo de opciones se rellena para que su tamaño sea múltiplo de 32 bits (4 bytes).

2.1.2.2. Direcciones IP

La dirección IP es el identificador de cada host dentro de su red. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos computadores con dos direcciones IP iguales. Pero sí podríamos tener dos computadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

2.1.2.2.1. Clasificación de la Direcciones IP

Hay diferentes formas de catalogar direcciones IP; por tipo de acceso se dividen en:

- **Direcciones IP públicas**. Son visibles en todo Internet. Un computador con una IP pública es accesible (visible) desde cualquier otro computador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

- **Direcciones IP privadas.** Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los computadores con direcciones IP privadas pueden salir a Internet por medio de un router (o Proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a computadores con direcciones IP privadas.

A su vez, las direcciones IP pueden clasificarse por el tipo de asignación en:

- **Direcciones IP estáticas**. Un host que se conecte a la red con dirección IP estática siempre lo hará con la misma, es decir, no cambia. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios. Estas direcciones hay que contratarlas.

- **Direcciones IP dinámicas**. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta, es decir, se renueva en cada conexión. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Las direcciones IP de distintos tipos se pueden combinar de la siguiente forma: pública fija, pública dinámica, privada fija, privada dinámica.

2.1.2.2.2. Estructura de las Direcciones IP

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma A.B.C.D donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP del servidor de la Universidad Católica del Ecuador Sede Ambato (www.pucesa.edu.ec) es 200.107.37.166.

Las direcciones IP también se pueden representar en hexadecimal, desde la 0.00.00.00 hasta la FF.FF.FF.FF o en binario, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.

Las tres direcciones siguientes representan a la misma máquina (podemos utilizar una calculadora científica para realizar las conversiones).

Decimal	128.10.2.30
Hexadecimal	80.0A.02.1E
Binario	10000000.00001010.00000010.00011110

2.1.2.2.3. Clases de Direcciones IP

Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan por que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: el *identificador de red* y el *identificador de host*.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las **clases primarias A, B** y **C**. La **clase D** está formada por direcciones que no identifican a un host, sino a un grupo de ellos. Las direcciones de **clase E** no se pueden utilizar, ya que la Fuerza de Tareas de Ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación.

Clase	Formato (r=red, h=host)	Redes	Hosts por red	Rango de direcciones	Máscara de subred
A	r.h.h.h	128	16.777.214	0.0.0.0 - 127.0.0.0	255.0.0.0
B	r r h h	16.384	65 534	128 0 0 0 - 191.255.0.0	255 255 0 0
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	Grupo	-	-	224.0.0.0 - 239.255.255.255	-
E	No válidas	-	-	240.0.0.0 - 255.255.255.255	-

Tabla 3: Resumen de las clases de direcciones IP

2.1.2.2.4. Difusión (broadcast) y multidifusión (multicast)

El término difusión (broadcast) se refiere a todos los hosts de una red, es el envío de un mensaje a todos los computadores que se encuentran en una red; multidifusión (multicast) se refiere a varios hosts (aquellos que se hayan suscrito dentro de un mismo

grupo). Siguiendo esta misma terminología, en ocasiones se utiliza el término unidifusión para referirse a un único host.

2.1.2.2.5. Direcciones IP Especiales y Reservadas

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host, algunas de ellas tienen significados especiales. Las principales direcciones especiales se resumen en la siguiente tabla. Su interpretación depende del host desde el que se utilicen.

Bits de red	Bits de host	Significado	Ejemplo
todos 0		Mi propio host	0.0.0.0
todos 0	host	Host indicado dentro de mi red	0.0.0.10
Red	todos 0	Red indicada	192.168.1.0
todos 1		Difusión a mi red	255.255.255.255
Red	todos 1	Difusión a la red indicada	192.168.1.255
127	cualquier valor válido de host	Loopback (mi propio host)	127.0.0.1

Tabla 4: Direcciones IP especiales y reservadas

La dirección de *loopback* (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio computador, no garantiza que la tarjeta de red funcione correctamente.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (intranets). Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

Clase	Rango de direcciones reservadas de redes
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
C	192.168.0.0 - 192.168.255.0

Tabla 5: Rango de direcciones reservadas

2.1.2.3. Máscara de subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Tabla 6: Máscaras de subred de cada clase

Si expresamos la máscara de subred de clase A en notación binaria, tenemos:

11111111.00000000.00000000.00000000

Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.

Supongamos una subred con máscara 255.255.0.0, en la que tenemos un computador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

148.120.33.110	10010100.01111000.00100001.01101110	(DIRECCIÓN DEL PC)
255.255.0.0	11111111.11111111.00000000.00000000	(Su máscara de subred)
148.120.0.0	10010100.01111000.00000000.00000000	(Dirección de su subred)

Tabla 7: Direcciones y máscara en binario

Al hacer el producto binario de las dos primeras direcciones (donde hay dos 1 en las mismas posiciones ponemos un 1 y en caso contrario, un 0) obtenemos la tercera.

En una red de redes TCP/IP no puede haber hosts aislados, todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara un computador sabe si otro computador se encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente; en cambio, si los hosts están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del host origen. Este router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del host destino y se complete la entrega del mensaje.

Por ejemplo, como muestra la Figura 3, los proveedores de Internet habitualmente disponen de una o más redes públicas para dar acceso a los usuarios que se conectan por módem. El proveedor va cediendo estas direcciones públicas a sus clientes a medida que se conectan y liberándolas según se van desconectando (direcciones dinámicas). Supongamos que cierto ISP (proveedor de servicios de Internet) dispone de la red 63.81.0.0 con máscara 255.255.0.0. Para uso interno utiliza las direcciones que comienzan por 63.81.0 y para ofrecer acceso a Internet a sus usuarios, las direcciones comprendidas entre la 63.81.1.0 hasta la 63.81.255.254 (las direcciones 63.81.0.0 y 63.81.255.255 están reservadas). Si un usuario conectado a la red de este ISP tiene la dirección 63.81.1.1 y quiere transferir un archivo al usuario con IP 63.81.1.2, el primero advertirá que el destinatario se encuentra en su misma subred y el mensaje no saldrá de la red del proveedor (no atravesará el router).

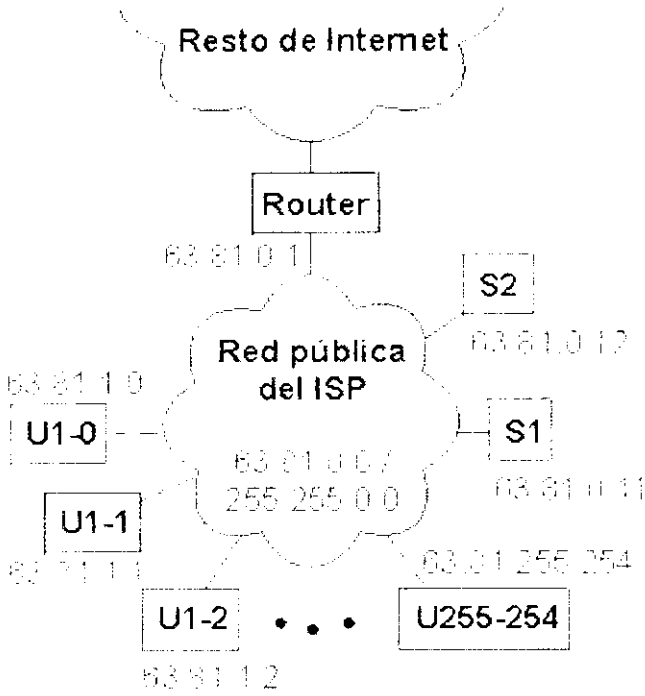


Figura 3: Ejemplo de aplicación de máscaras en una red

2.1.2.4. Encaminamiento (Enrutamiento)

Una *red de redes* está formada por redes interconectadas mediante encaminadores o routers. Cuando enviamos datos desde un computador hasta otro, éste tiene que ser capaz de encontrar la ruta más adecuada para llegar a su destino. Esto es lo que se conoce como *encaminamiento*.

Los *routers* (routers) son los encargados de elegir las mejores rutas, estas máquinas pueden ser computadores con varias direcciones IP o bien, aparatos específicos. Los routers deben conocer, al menos parcialmente, la estructura de la red que les permita encaminar de forma correcta cada mensaje hacia su destino. Esta información se almacena en las llamadas *tablas de encaminamiento*, observemos que debido al sistema de direccionamiento IP esta misión no es tan complicada, lo único que necesitamos almacenar en las tablas son los prefijos de las direcciones (que nos indican la red). Por ejemplo, si el destino es la máquina 149.33.19.4 con máscara 255.255.0.0, nos basta con conocer el encaminamiento de la red 149.33.0.0 ya que todas las que empiecen por 149.33 se enviarán hacia el mismo sitio.

2.1.2.5. Protocolo TCP

El protocolo TCP (*Transmission Control Protocol*, protocolo de control de transmisión) está basado en IP que es no fiable y no orientado a conexión, y sin embargo es:

- Orientado a conexión. Es necesario establecer una conexión previa entre las dos máquinas antes de poder transmitir ningún dato. A través de esta conexión los datos llegarán siempre a la aplicación destino de forma ordenada y sin duplicados. Finalmente, es necesario cerrar la conexión.

- Fiable. La información que envía el emisor llega de forma correcta al destino.

El protocolo TCP permite una comunicación fiable entre dos aplicaciones, de esta forma, las aplicaciones que lo utilicen no tienen que preocuparse de la integridad de la información: dan por hecho que todo lo que reciben es correcto.

El flujo de datos entre una aplicación y otra viaja por un *circuito virtual*, sabemos que los datagramas IP pueden seguir rutas distintas, dependiendo del estado de los routers intermedios, para llegar a un mismo sitio. Esto significa que los datagramas IP que transportan los mensajes siguen rutas diferentes aunque el protocolo TCP logre la ilusión de que existe un único circuito por el que viajan todos los bytes uno detrás de otro (algo así como una tubería entre el origen y el destino). Para que esta comunicación pueda ser posible es necesario abrir previamente una conexión. Esta conexión garantiza que todos los datos lleguen correctamente de forma ordenada y sin duplicados. La unidad de datos del protocolo es el *byte*, de tal forma que la aplicación origen envía bytes y la aplicación destino recibe estos bytes.

Sin embargo, cada byte no se envía inmediatamente después de ser generado por la aplicación, sino que se espera a que haya una cierta cantidad de bytes, se agrupan en un *segmento* y se envía el segmento completo. Para ello son necesarias unas *memorias intermedias* o *buffers*. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Si el segmento es muy grande será necesario fragmentar el datagrama, con la consiguiente pérdida de rendimiento; y si es muy pequeño, se estarán enviando más

cabeceras que datos. Por consiguiente, es importante elegir el mayor tamaño de segmento posible que no provoque fragmentación.

El protocolo TCP envía un *flujo de información no estructurado*. Esto significa que los datos no tienen ningún formato, son únicamente los bytes que una aplicación envía a otra. Ambas aplicaciones deberán ponerse de acuerdo para comprender la información que se están enviando.

Cada vez que se abre una conexión, se crea un canal de comunicación bidireccional en el que ambas aplicaciones pueden enviar y recibir información, es decir, una conexión es *full-dúplex*.

2.1.3. Intranet

Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (Web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como "internets" en miniatura o lo que es lo mismo, Internet es una intranet pública gigantesca.

2.1.4. Extranet

Es la unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, punto a punto, etc.) o a través de Internet.

2.1.5. Internet

La mayor red pública de redes TCP/IP. Es una red global de equipos informáticos que se comunican mediante este protocolo. Es similar al sistema de teléfonos internacional: nadie posee ni controla todo el conjunto, pero está conectado de forma que funcione como una gran red. Hoy en día, entre treinta y cuarenta millones de personas tienen acceso a Internet.

2.1.6. Banda Ancha

Consiste en transmitir señales en forma digital modulando la señal sobre ondas portadoras que pueden compartir el ancho de banda del medio de transmisión mediante multiplexación por división de frecuencia, es decir, actúa como si en lugar de un único medio se estuvieran utilizando líneas distintas lo que permite una mayor velocidad en la transmisión efectiva de datos, audio y vídeo. Este método hace imprescindible la utilización de un módem para la modulación y demodulación de las señales analógicas que transmiten.

Los medios de transmisión que se pueden utilizar son: el cable coaxial de banda ancha y el cable de fibra óptica.

En un sentido general, Banda Ancha se refiere a la transmisión de datos en el cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva. En ingeniería de redes este término se utiliza también para los métodos en donde dos o más señales comparten un medio de transmisión.

Algunas de las variantes de los servicios de Línea de Abonado Digital Asimétrica (del inglés Asymmetric Digital Subscriber Line, ADSL) son de banda ancha en el sentido en que la información se envía sobre un canal y la voz por otro canal, pero compartiendo el mismo par de cables. Los módems analógicos que operan con velocidades mayores a 600 bps también son técnicamente banda ancha, pues obtienen velocidades de transmisión efectiva mayores usando muchos canales en donde la velocidad de cada canal se limita a 600 baudios. Por ejemplo, un módem de 2400 bps usa cuatro canales de 600 baudios. Este método de transmisión contrasta con la transmisión en banda base, en donde un tipo de señal usa todo el ancho de banda del medio de transmisión, como por ejemplo Ethernet 100BASE-T.

Algunas tecnologías que utilizan banda ancha son:

- Cable módem

- DSL (Digital Subscriber Line)
- ADSL (Asymmetric Digital Subscriber Line)
- Internet por satélite
- LMDS para zonas rurales y su derivación portátil para ciudad: WiMAX
- Power Line Communication (PLC)
- WiFi

En los últimos años en nuestro país la tecnología de banda ancha para Internet ha mejorado considerablemente, no solo por las exigencias de los usuarios sino también por la competencia que día a día han ido fomentando las empresas proveedoras de este servicio; las mismas que brindan los servicios de "Dial Up" y de ADSL para banda ancha. Éstas son las tecnologías para conexión a Internet más conocidas y más utilizadas tanto a nivel personal como a nivel empresarial. La ciudad de Ambato no se queda exenta de este servicio, contando con los dos tipos de conexión mencionados, de los cuales la PUCESA hace uso de ADSL para el servicio de Internet en sus instalaciones, motivo por el cual se realiza una explicación un poco más detallada del funcionamiento de esta tecnología de banda ancha.

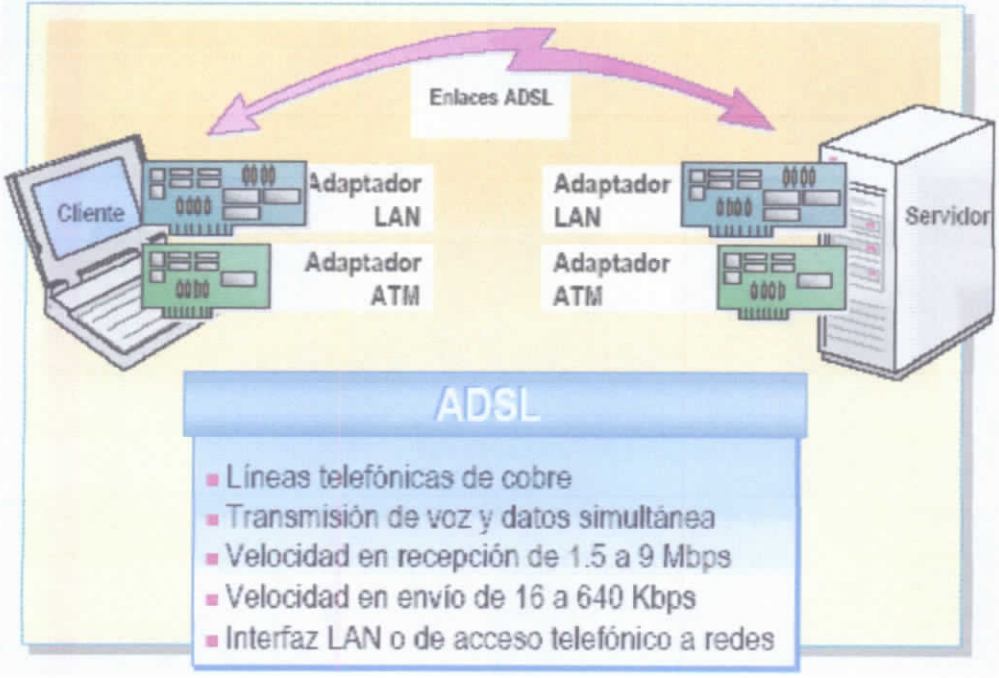


Figura 4: Banda Ancha con ADSL

La línea de subscriptor digital asimétrica (ADSL) es una tecnología que permite enviar mayor cantidad de datos sobre líneas telefónicas de cobre existentes. ADSL lo consigue utilizando la porción del ancho de banda de la línea telefónica no utilizado por la voz, permitiendo la transmisión simultánea de voz y datos.

Los usuarios de acceso remoto telefónico a redes reciben mucha más información que envían. La naturaleza asimétrica de la conexión ADSL encaja bien con la mayoría de usos de negocio remoto e Internet. En la recepción de datos, ADSL soporta velocidades de transferencia desde 1,5 a 9 Mbps.

En el envío de datos, ADSL soporta velocidad de transferencia de 16 a 640 Kbps. Aunque ADSL proporciona mayores velocidades de transmisión de datos que las conexiones PSTN y RDSI, el equipo cliente puede recibir datos a una mayor velocidad que enviar datos.

El equipo ADSL puede aparecer a Windows 2000 tanto como un interfaz LAN como un interfaz de acceso telefónico a redes. Cuando un adaptador ADSL aparece como un interfaz LAN, la conexión ADSL opera del mismo modo que una conexión LAN a Internet.

Cuando un adaptador ADSL aparece como un interfaz de acceso telefónico a redes, ADSL proporciona una conexión física y los paquetes individuales se envían utilizando el modo de transferencia asíncrona (ATM). Se instala un adaptador ATM con un puerto ADSL tanto en el cliente como en el servidor de acceso remoto.

2.2. VOZ Y VIDEO SOBRE IP

2.2.1. Voz sobre IP

La voz sobre IP es la tecnología que permite la transmisión de fragmentos auditivos a través de Internet.

Mientras la transmisión de datos e información ha sido hasta hoy en día la aplicación más prevaleciente en sistemas de información, el traslado de Voz sobre esta

misma infraestructura ha generado grandes expectativas por el ahorro de recursos que ésta representa.

La tecnología telefónica utilizada en muchas regiones llamada Circuit-Switched implica la apertura de un canal digital permanente de punta-a-punta para establecerse la comunicación, mismo mecanismo que se traduce en un alto consumo de recursos, ya que una conversación no es llevada simultáneamente por ambas partes además de poseer una serie de silencios, ante estas deficiencias, nace la Voz sobre IP que tiene como su base la tecnología denominada Packet-Switched en la que típicamente eran encapsulados datos para ser distribuidos a lo largo de un medio compartido.



Figura 5: Configuración básica de un sistema de Voz sobre IP

2.2.2. Protocolos de Voz sobre IP

Hoy en día, existen dos protocolos para transmitir voz sobre IP, ambos definen la manera en que dispositivos de este tipo deben establecer comunicación entre sí, además de incluir especificaciones para codecs de audio -- *cod*ificador-*deco*dificador -- para convertir una señal auditiva a una digitalizada compresa y viceversa.

2.2.2.1. H.323

H.323 es el estándar creado por la Unión Internacional de Telecomunicaciones (ITU) que se compone por un protocolo sumamente complejo y extenso, el cual además de incluir la voz sobre IP, ofrece especificaciones para vídeo-conferencias y aplicaciones en tiempo real, entre otras variantes.

2.2.2.2. Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) fue desarrollado por la IETF (Internet Engineering Task Force) específicamente para telefonía IP, que a su vez toma ventaja de otros protocolos existentes para manejar parte del proceso de conversión, situación que no se aplica en H.323 ya que define sus propios protocolos bases.

2.2.2.3. Voz sobre IP en aplicaciones

El potencial ahorro de recursos, al poder reutilizar infraestructura existente para datos que es el Internet en sí y transmitir voz sobre ella, ha producido una serie de aplicaciones y productos diseñados para tomar ventaja de esta tecnología.

En forma de equipos especializados para actuar como PBX ("Private Branch Exchange") o conmutadores, software para instalarse en servidores de datos, o en aplicaciones tipo "Messenger" para uso personal en PC, el uso de Voz sobre IP es amplio. Algunos desarrollos basados en Voz sobre IP son los siguientes:

- Asterisk: Es un software libre de Voz sobre IP para PBX ("Private Branco Exchange") o conmutadores.
- Skipe: Una aplicación estilo "Messenger" para PC que emplea voz sobre IP.
- Vonage: Es un proveedor de servicios para telefonía basado exclusivamente en voz sobre IP.

2.2.3. Video sobre IP

Las presentaciones de video pueden agruparse en tres categorías: Video Broadcasting, Video on Demand, y Videoconferencia. De las tres, solo la videoconferencia es full duplex, las otras son esencialmente transmisiones unidireccionales. Estas transmisiones de vídeo sobre IP son escalables, costo eficientes y muy flexibles. Estas nuevas herramientas de negocio integran oficinas distintas en una sola empresa y se están expandiendo rápidamente. De acuerdo con Gartner Group, las aplicaciones de vídeo IP se utilizarán en el 80% de las compañías Fortune 2000 para el año 2006. Estas aplicaciones están rápidamente reemplazando las aplicaciones tradicionales de videoconferencia sobre ISDN. De acuerdo con In-Stat/MDR (marzo del 2003), la venta de puntos de videoconferencia se espera que alcance $875 millones de dólares en el 2007, y la venta total de servicios de videoconferencia se espera que alcance $5.5 billones de dólares en el mismo año.

2.2.3.1. Video Broadcast sobre IP

Video broadcast sobre IP es una transmisión unidireccional de red de un archivo con contenido de vídeo. Los puntos terminales son meramente visualizadores pasivos sin control sobre la sesión. Video broadcast puede ser Unicast o Multicast desde el servidor. En una configuración Unicast, el servidor hace un replica de la transmisión para cada visualizador terminal. En una configuración Multicast, la misma señal es enviada sobre la red como una sola transmisión, pero hacia varios puntos terminales o, simplemente, hacia un grupo de usuarios.

Esta tecnología está siendo implementada en ambientes corporativos como un medio de distribuir capacitación, presentaciones, minutas de reuniones y discursos; también está siendo utilizada por universidades, centros de educación técnica o educación continua, emisoras, proveedores de webcast, solo por nombrar algunos. Hay tres factores para determinar cuánto ancho de banda requerirá esta tecnología: el número de usuarios, su ancho de banda al servidor, y la longitud de la presentación o vídeo. Video broadcast se considera típicamente como una "tubería abierta".

2.2.3.2. Video on Demand (VOD) sobre IP

Generalmente, VOD permite a un usuario pedir una determinada secuencia de vídeo almacenada en un servidor. Esta tecnología difiere de Vídeo broadcast en que el usuario tiene las opciones de parar, iniciar, adelantar o regresar el vídeo ya que el servicio es interactivo. VOD tiene también otra característica en la que generalmente se acompaña del uso de datos para la visualización y la tarifación de los servicios o tiempo de vídeo. Aunque VOD se puede usar para visualización en tiempo real, generalmente se utiliza para archivos almacenados de vídeo. Esta tecnología se usa para e- learning, capacitación, mercadeo, entretenimiento, broadcasting, y otras áreas donde el usuario final requiere visualizar los archivos con base en su propio itinerario y no en el horario del proveedor de vídeos.

Una aplicación típica de VOD sobre una red IP, contiene los siguientes elementos:

- El Servidor de Vídeo (puede ser un servidor de archivos o un cluster de servidores).
- El Servidor Controlador de Aplicaciones el cual inicia la transmisión (puede estar incluido en un servidor de archivos).
- Un punto terminal con un convertidor para responder a la petición de visualización y control de reproducción.
- Software de Administración y/o software de tarifación.
- PC o Dispositivo de Red para registrar/convertir los archivos de vídeo.

2.2.3.3. Videoconferencia sobre IP

Videoconferencia (VC) es una combinación de transmisiones full duplex de audio y vídeo los cuales permiten a usuarios ubicados en distintos lugares verse y oírse el uno al otro tal como si estuvieran en una conversación cara a cara. Se utiliza una cámara en cada uno de los puntos terminales para capturar y enviar las señales de vídeo. Se usan micrófonos en cada punto terminal para capturar y transmitir la voz la cual es luego

reproducida en altoparlantes. Las comunicaciones son en tiempo real y generalmente no se almacenan.

La primera tecnología de videoconferencia fue introducida en el Mercado por AT&T en 1964. La norma tradicional para comunicaciones es ITU H.320. Esta norma tiene restricciones en los costos de utilización y los usuarios tienen que mantener el equipo dedicado en una sola ubicación. Las nuevas normas liberadas en 1996 (H323) permiten VC basado en IP. Los servicios basados en IP son mucho mejores ya que la conferencia puede iniciarse desde cualquier PC en una red apropiadamente equipada, y las señales viajan sobre la infraestructura y equipo regular de la red, eliminando la necesidad de líneas dedicadas y cargos de utilización.

Estos servicios pueden usarse para diversas aplicaciones incluyendo comunicaciones corporativas, telemedicina, telehealth, capacitación, e-learning, tele-conmutación y servicio a usuarios. La videoconferencia puede ser punto a punto (un usuario a un usuario), o multipunto (varios usuarios participando en la misma sesión). Los usuarios pueden posteriormente ser visualizados en ventanas separadas. La videoconferencia ha introducido también un nuevo concepto en comunicaciones por medio de la colaboración. Un tablero electrónico puede ser incluido en la conferencia permitiendo a los usuarios escribir notas en el mismo tablero y/o visualizar las presentaciones y notas de los otros mientras se conversa.

Un MCU (Multipoint Conference Unit) se mantiene generalmente en una ubicación central. Esta unidad permite que varias alimentaciones de video sean visualizadas simultáneamente. Una caja llamada Gatekeeper se incluye normalmente para conferencias multipunto. Esta caja controla el ancho de banda, direccionamiento, identificación y medidas de seguridad para las conferencias. Aunque el Gatekeeper es generalmente una aplicación de software que reside en una PC separada, los modelos de equipo más reciente tienen esta funcionalidad integrada.

2.2.3.4. Video Digital sobre IP

La característica "*plug and play*" permite a las cámaras direccionables IP ser colocadas en cualquier lugar dentro de la infraestructura. Los equipos electrónicos que

manejan actualmente tráfico IP se han vuelto parte integral de los sistemas de vigilancia. Ya que los videos se almacenan en formato digital, pueden ser vistos en cualquier lugar de la red con nuevas capacidades de seguridad para los archivos administrados como parte de las políticas de seguridad de la red. Además, éstos pueden ser vistos simultáneamente desde varios puntos de la red. No sólo es fácil de implementar, sino también es extremadamente versátil. Las redes no son sobrecargadas con otro protocolo. Las transmisiones son "nativas" en la infraestructura actual, eliminando la necesidad de sistemas de cableado separados.

TCP/IP se ha convertido en el estándar de facto para las redes. Su arquitectura abierta permite que varios sistemas puedan compartir el espacio de red, y aprovechar estas nuevas tecnologías para aumentar su capacidad, confiabilidad, escalabilidad u accesibilidad de los recursos de red. Con la habilidad de utilizar la infraestructura existente, un edificio puede volverse totalmente automatizado utilizando un solo sistema de cableado. Esta automatización puede incluir no sólo CCTV (Circuito Cerrado de Televisión), sino también control de accesos, sistemas de fuego y seguridad (de la vida), sistemas de automatización de edificios, voz y, por supuesto, tráfico de red. Los administradores y los usuarios de la red no estarán más encadenados a un solo puesto ya que el control y/o administración de estos sistemas puede realizarse desde cualquier estación de trabajo con acceso a la red. Esto mismo aplica para el personal de seguridad. Ellos pueden ubicarse en cualquier lugar. La cámara digital se vuelve ahora el punto de falla, no el centro de control, ya que es extremadamente fácil hacer redundantes los servidores digitales ya sea en un solo sitio o distribuidos en múltiples ubicaciones.

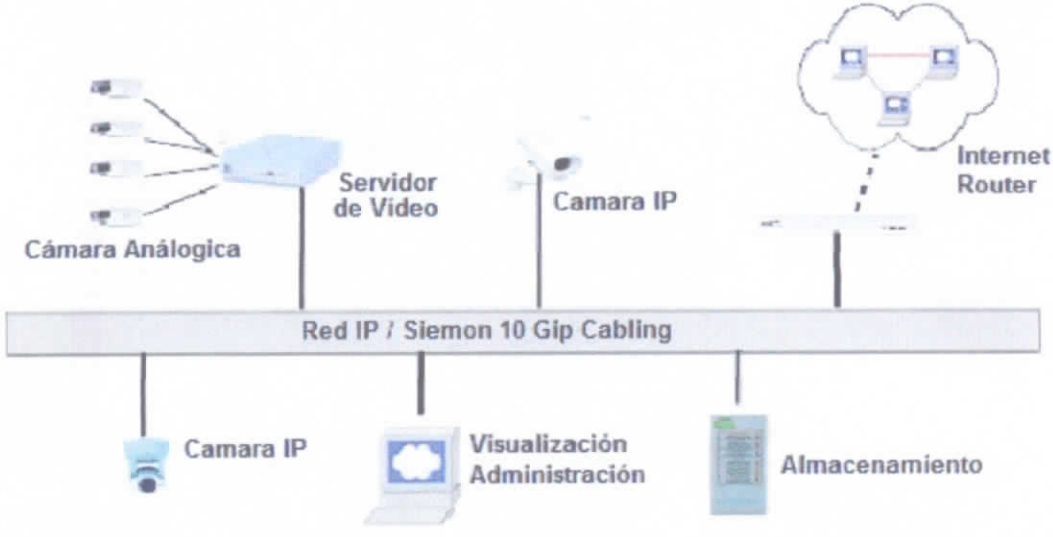


Figura 6: Esquema de una red con Video sobre IP

Un sistema típico CCTV basado en IP se muestra en la Figura 6. Como se puede observar, es completamente diferente de las otras dos soluciones presentadas. Las cámaras IP, servidores de video IP y teclados IP pueden colocarse en cualquier punto. Los teclados IP pueden controlar actualmente las funciones PTZ (Pan, Tilt and Zoom) de cualquier videocámara con base en su dirección IP. Como cualquier protocolo IP, las funciones de administración son incorporadas en la transmisión. Esto incluye DSP (Digital Signal Processing), manejo de alarmas, grabación, capacidades de búsqueda y/o archivo, calendarización y automatización. Estas funciones de administración y control utilizan SNMP (Simple Network Management Protocol) y otros cuadros de control, todas ellas parte del estándar IP.

Estas cámaras pueden equiparse con características avanzadas tales como sensores de movimiento, PTZ automatizado y, si se desea, salidas análogas de video. Las versiones más recientes vienen equipadas con DVRs internos que pueden replicarse con un servidor DVR centralizado. Investigaciones realizadas por J.P. Freeman y Frost & Sullivan estiman que las ventas para estas cámaras en el mercado de los Estados Unidos alcanzarán varios millones para el año 2007.

Otro sistema basado en IP, CCTP (Closed Circuit Twisted Pair), fue introducido por una compañía llamada Anixter. Este sistema permite que las señales de video, control y alimentación eléctrica sean transmitidas en un solo cable de par trenzado. Este sistema tipo chasis puede acomodar 40 cámaras fijas y 16 cámaras PTZ (pan-tilt-zoom) en un sólo chasis. La añadidura de alimentación eléctrica a la infraestructura provee un beneficio adicional al sistema al facilitar los movimientos y cambios así como instalaciones iniciales, ya que no se requiere instalar un cable eléctrico en paralelo con el sistema de cableado.

2.2.3.5. Normas de Compresión de Video

Las imágenes digitales de alta resolución necesitan mayor ancho de banda para transmisión y más espacio en disco para almacenamiento. El almacenaje y la transmisión de estas imágenes son muy problemáticos en las tecnologías e infraestructuras tanto en la

intranet como en el Internet. Se han desarrollado algoritmos de compresión para ayudar a asegurar transmisiones de alta calidad sobre mecanismos de menor ancho de banda. Existe un conflicto entre la tasa de transferencia de paquetes y la calidad de la imagen. JPEG, JPEG2000, MPEG-1, 2, 4, Wavelet y H.261/H.263 son todos ellos métodos de compresión que tratan con estas transmisiones.

JPEG (Joint Photographic Experts Group) y MPEG (Motion Pictures Expert Group) son normas ISO/IEC que permiten transmisiones de video de alta calidad. JPEG es la norma para imágenes fijas mientras que MPEG lo es para imágenes en movimiento. La última norma internacional de audio-video, video en movimiento, es MPEG4 (ISO/IEC 14496). Wavelet-Like Motion-JPEG es el proceso de combinar fotos fijas dentro del video en movimiento. Las normas H.261 y H.263 fueron desarrolladas para videoconferencia y *no* ofrecen imágenes claras para objetos en movimiento rápido.

Al discutir acerca de CCTV y de todas las demás necesidades de red, hay un mensaje dominante. La utilización de ancho de banda sigue aumentando. El asunto de la compresión no es ya un gran problema como lo era antes, en gran parte debido a que existe mayor ancho de banda disponible. Videoconferencia, CCTV y todas las demás aplicaciones convergentes tienen un impacto especialmente si la infraestructura de uno está fuera de especificaciones o desactualizada. Hace apenas dos años nadie se imaginaba que se podía enfocar con una cámara un niño en una clase o mirar Video on Demand sobre las redes. Pero la realidad es que estas tecnologías ya están aquí. Habrá nuevas tecnologías mañana que hoy son sólo sueños.

Las soluciones Siemon 10G IP™ son 10G 6™, fibra XGLO™ y TERA™. En combinación o por separado, estas representan la solución de cableado para TI de mayor desempeño disponible para las realidades actuales y las posibilidades del mañana. Su sistema CCTV puede transportar video de alta calidad, alta resolución, y tiempo real en un ambiente de convergencia. 10G IP™ ha sido diseñado con el usuario final en mente y con el hecho de que las compañías esperan que sus infraestructuras duren al menos 10 años. Este sistema, instalado hoy, se integrará en forma transparente con MAN/WAN 10G sin la necesidad de actualizar su infraestructura con futuras generaciones de equipo activo. Esto asegura la protección de la inversión en la infraestructura de red. Una simple tendencia

actual se está expandiendo a cada industria, esto es, las compañías quieren proteger no sólo sus datos, sino todos los bienes y gente que ellas emplean.

Los sistemas basados en IP incluyendo servidores, electrónicos, CCTV, y la miriada de otras soluciones se juzgan con base en su confiabilidad, escalabilidad y longevidad de equipo. Este sistema de cableado se ha diseñado con base en estos principios para ofrecer un retorno de inversión sólido. Siemon participa en todas las organizaciones de normas apropiadas para asegurar que nuestros sistemas proporcionen la durabilidad y un cableado state-of-the-art para asegurar que su inversión en electrónicos a su máxima capacidad hoy y mañana.

2.2.3.6. Normas para Vídeo sobre IP

Los requisitos de sistemas abiertos especifican que las comunicaciones deben ocurrir dentro de una estructura predefinida de paquetes IP y que cualquier equipo interactúe con cualquier otro sin importar la marca y de una manera no propietaria. Los dos principales protocolos de componentes son H.323 y SIP (Session Initiation Protocol). Los cuatro principales componentes - terminales, gateways, gatekeepers, y unidades de control multipunto - están definidos en la norma H.323 y sus adendas. SIP fue desarrollado por la IETF (Internet Engineering Task Force) a mediados de los 90's y es un protocolo de señalización para conferencias en Internet, telefonía, presencia, notificación de eventos y mensajería instantánea. SIP se desarrolló dentro del grupo de trabajo IETF MMUSIC (Multiparty Multimedia Session Control), con trabajos posteriores desde septiembre del 1999 en el grupo de trabajo IETF SIP. Las aplicaciones de vídeo actuales utilizan compresión de vídeo y tecnología de codificación de vídeo para transportar la porción de vídeo con un consumo reducido de ancho de banda atribuible al esquema de compresión. MPEG (Motion Picture Experts Group) es el desarrollador predominante de las normas de compresión para alimentaciones de vídeo, con MPEG-4 como la última tecnología.

2.2.3.7. Bits y Bytes de Ancho de Banda

Cuando una señal análoga se convierte a una señal digital (como en el caso de transmisiones de vídeo o voz), el proceso se completa por lo que se conoce como muestreo. El muestreo, tal como su nombre lo indica, se refiere a la toma de muestras de la

señal varias veces por segundo (la tasa de muestreo) con una profundidad de muestreo (bits por muestra). A mayor tasa de muestreo, mayor tamaño del archivo. El número de valores es igual al número de valores de muestra (on u off) elevado a la potencia del número de bits muestreados. En términos más simples, un CD de música se hace un muestreo a una tasa de 44,000 muestras por segundo o generalmente 5 MB de muestras (datos) por minuto de música.

La misma técnica se usa para vídeo, aunque de manera algo más compleja. La diferencia consiste en que lo que está siendo ahora transmitido es una imagen construida en elementos pictográficos conocidos como pixels. La norma MPEG utiliza lo que se conoce como compresión "lossy", que significa que mucho de la imagen se pierde pero no lo suficiente como para disminuir la comprensión del ojo humano ya que el cerebro humano tiende a llenar los vacios. El vídeo se muestrea en segmentos del vídeo. El primer cuadro (el cuadro índice) se transmite entero y los cuadros restantes transmiten cambios con respecto al cuadro índice inicial. A mayor compresión, mayor pérdida de cuadros. En una red congestionada, las muestras pueden recibirse fuera de secuencia y ocurre un fenómeno conocido como pixelación. La pixelación es cuando los pixels parecen fuera de lugar al compararlos con el cuadro índice original y la imagen se sesga.

Una alimentación en bruto de vídeo (no comprimida) totalmente muestreada requiere 165 Mbps para una calidad D1. La resolución D1 es una pantalla completa de 720 x 480 de TV para NTSC (National Television System Committee) y 720 x 576 para PAL (Phase Alternating Line). Existen dos formas de comprimir la alimentación: una es bajando la resolución y la otra es a través de la tasa de muestreo. Ya comprimida, la alimentación consumirá obviamente menos recursos pero a cambio se perderá calidad de vídeo.

2.2.3.8. Cuellos de Botella y Obstáculos

Con el fin de implementar vídeo en tiempo real en la red, dicha red debe estar en excelentes condiciones de funcionamiento. Moldeadores de tráfico pueden contribuir con la prioritización de tráfico de vídeo y tráfico de voz utilizando el bit de Calidad de Servicio. Todos los encabezados IP tienen una sección denominada TOS o byte de Tipo de Servicio. Este fue introducido dentro del protocolo varios años atrás. Calidad de Servicio es un término que se refiere a un conjunto de parámetros tanto para transmisiones en modo

de aseguramiento de conexión (TCP) y sin aseguramiento de conexión (UDP), los cuales proporcionan el desempeño en términos de calidad de transmisión y de disponibilidad de servicio. Éste abarca demora máxima, rendimiento y prioridad de paquetes transmitidos. Los primeros bits del byte ToS se reconfiguran con la información QoS. El tráfico prioritizado de la red coloca los paquetes sensibles al tiempo al principio de la transmisión de paquetes de datos. Este mismo método se usa en redes de VoIP (Voz sobre IP).

Tal como ocurre con el e-mail, las compañías comenzarán a depender enormemente de estos servicios en un futuro cercano. Cada administrador está consciente de los desastres que resultan cuando los sistemas críticos se "caen".

Las compañías están luchando para alcanzar, al igual que los proveedores de servicios, un porcentaje de disponibilidad de la red del 99.999%. Las caídas de red son muy costosas. La disponibilidad de la red se vuelve muy difícil de alcanzar en la medida en que las redes transportan cargas adicionales de alta sensibilidad y mayor calidad de servicio. Hay un solo denominador común para todas las aplicaciones: la infraestructura.

Una infraestructura robusta con amplio margen adicional, ancho de banda y capacidad será el más importante factor en cualquier instalación de servicios de convergencia IP. 10G *IP*™ se ha desarrollado para solucionar esta necesidad. ¿Por qué? La tecnología no se queda quieta. La habilidad alimenta la ingenuidad. Cada día se desarrollan nuevas normas para soportar nuevas aplicaciones. Hace cinco años, nadie pensaba que se daría la necesidad de transmisiones 10G. La realidad es que actualmente 10G existe y está siendo utilizada. Tiene mucho sentido dotar a su infraestructura con el margen necesario para crecimiento. 10G *IP*™ puede hacerlo ya al ser la mejor tecnología de cableado disponible en la actualidad y soportará sus aplicaciones del mañana.

2.3. Cámaras IP

Una cámara Web permite transmitir imágenes o vídeo en tiempo real a través de Internet. Éstas tienen múltiples aplicaciones y usos, desde la videoconferencia hasta la televigilancia, pasando por la monitorización de guarderías y otras instalaciones.

A diferencia de las anteriores, tenemos las cámaras IP, las cuales se conectan directamente a una conexión LAN (RJ45) de una instalación de Internet o red doméstica y llevan incorporado un servidor Web. Son totalmente autónomas del computador, se les asigna una dirección IP interna, y tan sencillo como teclear esa dirección IP desde cualquier navegador para acceder a la cámara y disponer de los menús que permiten todo tipo de funciones; visionar, realizar grabaciones, escuchar, alarmas, etc. Se puede controlar el hogar, la oficina o negocio desde cualquier lugar que disponga de Internet.



Figura 7: Esquema de conexión de una cámara IP

También existe otra opción más "limpia". Son las cámaras IP wireless, que le permite realizar una instalación sin apenas cableado.

Los dispositivos externos de vigilancia permiten conectar hasta 4 cámaras/fuentes de vídeo para el seguimiento de las mismas de forma simultánea, secuencial o manual. Esto es, el dispositivo dispone de 4 entradas de vídeo compuesto, y salidas de vídeo compuesto, S-SVHS y VGA. La salida VGA sirve para conectar directamente a un monitor de computador y utilizar este monitor como visualizador de las imágenes. Al disponer de salida de video-compuesto y S-VHS el usuario puede grabar las imágenes en un vídeo doméstico o similar. La operativa es sencilla, ya que una vez se han efectuado las conexiones, basta con seleccionar el modo de visualización. Este puede ser QUAD, es decir que cada imagen ocupa 1/4 del tamaño de la pantalla.

2.3.1. Qué es una cámara IP?

Una cámara IP o cámara de red puede ser descrita como una cámara y un computador en una unidad inteligente. Captura y transmite imágenes digitales en vivo

directamente a través de cualquier red IP (por ejemplo: LAN / intranet / Internet), permitiendo a los usuarios ver y/o manejar la cámara de forma remota a través de un servidor Web en cualquier lugar y en cualquier momento.

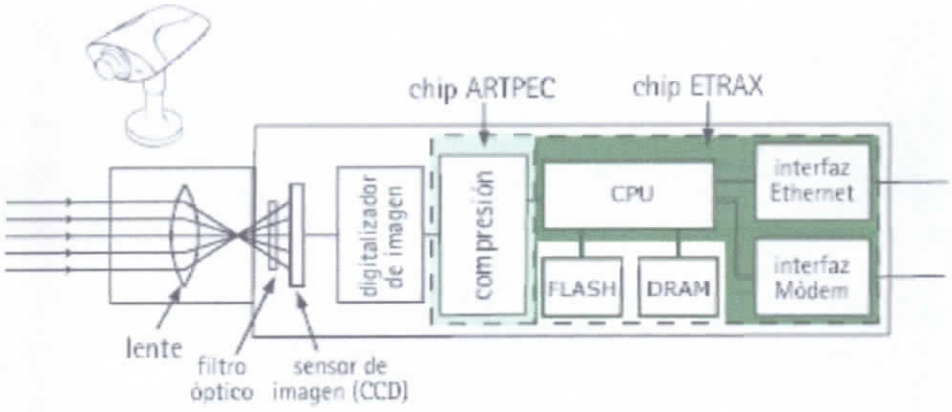


Figura 8: Estructura básica de una cámara IP

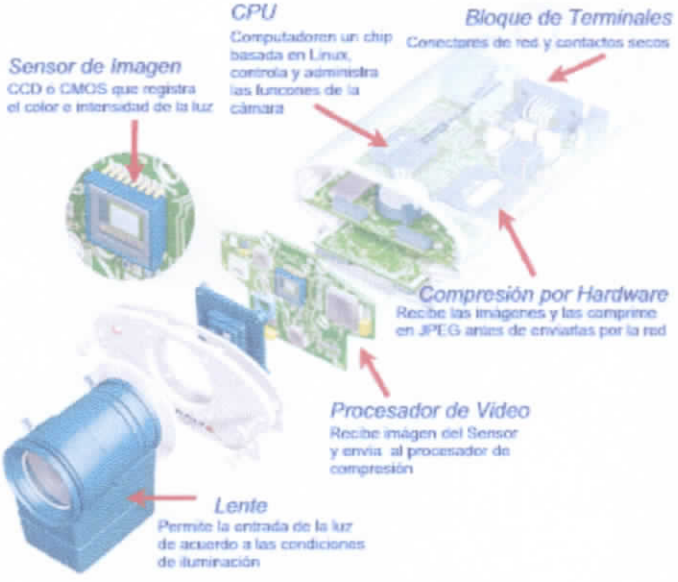


Figura 9: Estructura ampliada de una cámara IP

2.3.2. Funcionamiento de una cámara IP

Una cámara de red posee su propia dirección IP y funciones de servidor independiente integradas. Todo lo necesario para ver las imágenes a través de la red está incluido dentro de la cámara. La cámara se conecta directamente a la red como cualquier otro dispositivo de red, tiene su propio software integrado, servidor FTP, cliente FTP y cliente e-mail (FTP).

Incluye también entradas de alarma y salidas para relé. Según el modelo de cámara podrá ir equipada con muchas otras funciones como son la detección de movimiento o la salida de vídeo analógico.

Los componentes de cámara de las cámaras de red capturan la imagen, que se puede describir como luces con diferentes longitudes de onda y la transforman en señales eléctricas. Estas señales son convertidas entonces del formato analógico al digital y se transfieren al componente computador de la cámara donde la imagen es comprimida y enviada a través de la red.

La lente de la cámara enfoca la imagen en el sensor de imágenes (CCD). Antes de llegar al sensor la imagen pasa a través del filtro óptico, que elimina cualquier luz infrarroja para que los colores mostrados sean "correctos". El sensor de imagen convierte la imagen, compuesta por información lumínica, en señales eléctricas. Estas señales eléctricas digitales están ya en un formato que puede comprimirse y enviarse a través de la red.

El chip ARTPEC (Axis Real Time Picture EnCoder), desarrollado por Axis, es el que realiza las funciones de control de la cámara como son la gestión de la exposición, el balance de blancos (ajusta los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen. El chip ARTPEC también incluye un componente de compresión de vídeo que comprime la imagen digital a una imagen con la información reducida para su eficiente envío a través de la red.

La conexión Ethernet de la cámara se consigue gracias al chip ETRAX, una solución de sistema en un chip que permite conectar periféricos a la red. El ETRAX incluye una CPU de 32 bit, conectividad 10/100 Mb Ethernet, funcionalidad DMA (Direct Memory Access) avanzada y un amplio rango de interfaces de Entrada/Salida.

La CPU, memoria Flash y la memoria DRAM representan el "cerebro" o funciones de computador de la cámara y están diseñadas específicamente para aplicaciones de red. Juntas, gestionan la comunicación con la red y el servidor Web.

A saber, si se desea tener archivado lo que sucede en un sitio específico, las Cámaras IP son capaces de grabar la información permanentemente en el disco duro de la computadora a la que están conectadas; pueden ser programadas para hacer fotografías con intervalos específicos, de escasos segundos si es necesario; y pueden reaccionar a comandos enviados por mail, como por ejemplo, movimientos, enfoques más cercanos, en fin cualquier ángulo, en cualquier momento, desde cualquier computador. Y claro, esto es posible, porque cualquier cámara de vídeo se puede conectar a la red.

Claro está que las cámaras más sofisticadas -con capacidad de movimiento, enfoque, lente con zoom óptico, etc.- son más costosas, y por supuesto, está la conexión a Internet, indispensable, condición sin la cual no podremos verla desde cualquier lugar y para que la información esté publicada todo el tiempo. Es posible, sin embargo, activar una cámara telefónicamente para que las imágenes que la cámara capta sean publicadas en ese momento en la red.

Las alternativas son múltiples y dependen de las necesidades en cuestión, y sin embargo el truco puede ser mucho menos costoso que el ya mentado sistema cerrado de televisión, pues instalar las cámaras y acceder a las imágenes no requiere un sistema de cableado adicional, se utiliza la misma infraestructura que conecta a todos los computadores de la oficina, no se necesita monitores especiales, y los guardias de seguridad que pasean día y noche frente a las puertas pueden pasar a actividades más productivas para la empresa.

Y en cuanto a las imágenes y su accesibilidad: en un mismo sitio Web se pueden publicar varias cámaras y cada una de ellas puede ser vista mediante una clave que únicamente la conoce quien debe, o por el contrario, todas las cámaras pueden ser vistas para quien conozca el sitio Web en donde las imágenes se publican.

Evidentemente, la seguridad y el seguimiento a distancia de un escenario son las utilidades más difundidas de este tipo de tecnología. Y sin embargo, pueden además tener

otras diversas aplicaciones como por ejemplo el monitoreo del clima, del tráfico, de los daños causados por los desastres, la visibilidad de sitios inaccesibles, etc.; y ya que están conectadas a la Internet, tres, dos o apenas una misma cámara pueden servir para la municipalidad, la prensa, los ciudadanos o empresas específicas a un costo cada vez menor a medida que crecen los usuarios.

Los avances tecnológicos en los sistemas de videovigilancia de tercera generación junto con la convergencia de los mercados de informática y de seguridad abren nuevas oportunidades que van a permitir maximizar el aprovechamiento de la infraestructura de red y aportar innovadoras soluciones ante los nuevos retos planteados en el hito de la seguridad.

2.3.3. Ventajas de una Cámara IP

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 primer lugar podemos mencionar que una cámara de red es una unidad independiente y no requiere de ningún otro dispositivo ó computadora para la captura y transmisión de imágenes ya 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. Además podemos mencionar 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.

2.3.4. Aplicaciones de las Cámaras IP

Las cámaras de red proporcionan un enorme abanico de posibilidades de costo efectivo para el monitoreo y vigilancia remota de personas, propiedades, lugares, activos, maquinaria y equipo, zonas turísticas, aseguramiento de bienes y personas con ayuda de información de alarmas y detección de movimiento. Prácticamente las posibilidades son ilimitadas y tienen la ventaja de que el video al ser 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, fábricas 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.

2.3.5. Tipos de cámaras IP

En el mercado, básicamente podemos encontrar varios tipos de cámaras IP en base a distintas clasificaciones, las principales son:

- Por el tipo de conexión a la red:
  - Cableadas
  - WIFI (Wireless Fidelity)
- Por su movimiento
  - Fijas
  - PT
  - PTZ

Cámaras IP Cableadas

Son aquellas cámaras que se conectan a la red a través de un cable de red, ya sea directamente a un computador, a un switch, a un router, etc.

Cámaras IP WIFI

En este grupo están consideradas las cámaras "inalámbricas", es decir, aquellas que se conectan a la red sin cables o medios físicos, sino a través de ondas.

Cámaras IP Fijas

Son las que mantienen una posición constante y fija en el lugar donde han sido instaladas. Para su cambio de posición se requiere la intervención directa de la mano del hombre para su modificación.

Cámaras IP PT

A diferencia de las anteriores, estas cámaras presentan movimiento tanto horizontal como vertical, el mismo que es controlado a través del software propio de la cámara o de Internet. Algunas cámaras de éste tipo, presentan únicamente movimientos horizontales o verticales.

Cámaras IP PTZ

Son similares a las del tipo PT, pero éstas además de los movimientos, presentan la posibilidad de hacer "zoom", es decir acercar o alejar la imagen. El tipo de zoom varía de acuerdo a la marca y al modelo de la cámara, y es controlado también desde su propio software o desde Internet.

2.4. MONITOREO Y VIGILANCIA DE CENTROS EDUCATIVOS

El monitoreo y la vigilancia son medidas que se las ha venido tomando cada día con más intensidad en nuestro medio, debido a los altos índices de inseguridad en los que cada día desenvolvemos nuestras actividades diarias. Tal es el caso que la mayoría de empresas, organizaciones, instituciones e incluso hogares, han adoptado estas medidas como prioritarias para su buen desempeño y correcto desarrollo. Las instituciones educativas no están exentas de estas medidas en vista que han sido también víctimas de la inseguridad de la sociedad actual.

Hoy por hoy, es importante vigilar sus equipos, oficinas, instalaciones e incluso a las personas que asisten diariamente ya sea en calidad de empleados, docentes, estudiantes o simplemente visitantes. Esto como una medida más de seguridad que garantice la estabilidad de los centros de educación tanto primarios, secundarios como universitarios.

En este contexto la PUCESA no podía quedarse atrás ya que no es suficiente el contar con personal de seguridad para garantizar que todo el campus y sus instalaciones se encuentren libres de cualquier posibilidad de hurto o robo.

En base a esta investigación, es fácil darse cuenta que una de las maneras más fiables de realizar el monitoreo y la vigilancia en cualquier organización y especialmente en instituciones educativas es a través de las cámaras IP. Al analizar su capacidad y versatilidad podemos concluir que son herramientas muy útiles, fácilmente aplicables y de fácil (pero seguro) acceso no solo para el personal de vigilancia sino también para el resto de personal interesado en la seguridad.

Por otro lado debemos mencionar que al permitir las cámaras el acceso a éstas desde Internet, debemos tomar en cuenta las seguridades que toda conexión a la red de

redes debe tener, especialmente cuando se trata de empresas u organizaciones. Dentro de estas seguridades se encuentran el *"cortafuego o firewall"* y el *"proxy"*, de los cuales vamos a hablar a continuación.

2.4.1. Firewall

Un **Cortafuego** o **Firewall** es un elemento (de hardware o software) utilizado en una red de computadoras para prevenir algunos tipos de comunicaciones prohibidos según las políticas de la red que se hayan definido en función de las necesidades de la organización y de la persona administradora de la red.

La idea principal de un firewall es crear un punto de control de la entrada y salida de tráfico de una red. Un firewall apropiadamente configurado es un sistema adecuado para añadir protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. El firewall permite o niega las transmisiones de una red a otra, por lo que su uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

El firewall actúa como un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el Web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de Web, correo y FTP, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la Web. Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Si hablamos de una cámara IP que no solamente vaya a ser configurada para la red local, sino que es necesario que sea vista desde la Web, deberemos tomar en cuenta si en nuestra red existe un firewall de protección, ya que éste podría impedir la salida de la cámara hacia Internet. Para esto debemos revisar si existe o no un cortafuegos instalado y de ser así, configurarlo adecuadamente para que permita tanto la salida de las imágenes de la cámara hacia la Web, como el ingreso desde Internet hacia nuestra red local dirigiéndole únicamente a la dirección IP y al puerto de la cámara.

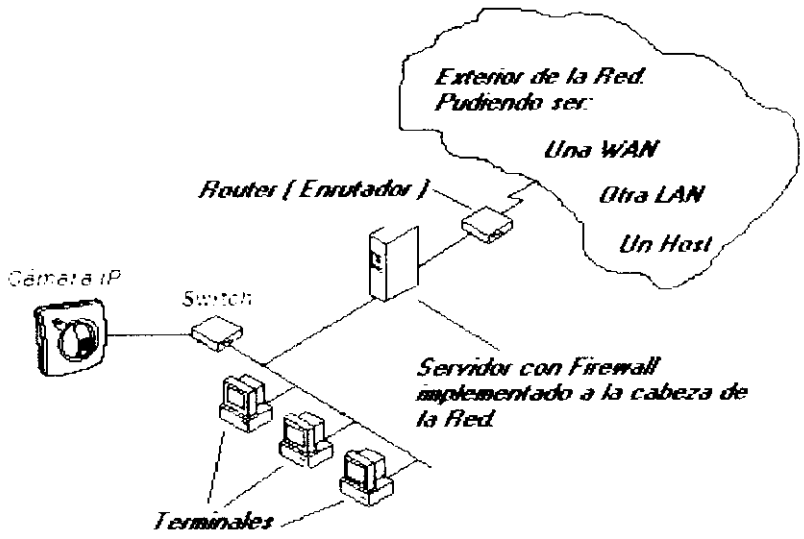


Figura 10: Utilización de firewall en una red con cámara IP

2.4.2. Proxy

Un Proxy es un sistema de software que permite la conexión de una LAN entera al exterior con sólo una dirección IP de salida, es decir, si montamos en el servidor principal de la red un módem, tarjeta de Red, adaptador RDSI, etc., e instalamos un Proxy (configurando también las aplicaciones cliente en los terminales), tendremos acceso al exterior de todos y cada uno de los terminales con una sola cuenta de acceso a Internet.

El fundamento para esta conexión es el siguiente: un terminal tiene, por ejemplo un navegador de Internet abierto, y el usuario le introduce *http: www.pucesa.edu.ec* en la barra de dirección, ahora el cliente del Proxy le pide esta dirección al Proxy, y éste es el que realmente se encarga de pedir la dirección pero con la IP propia del Proxy más no con la del terminal.

En caso de que la red en la cual se va a instalar una cámara IP tenga salida a Internet a través de un Proxy, la cámara no podrá ser visible desde la Web ya que éstas únicamente pueden salir a Internet a través de un router el cual encaminará la IP de la cámara hacia la red externa, en este caso Internet.

En el caso de la PUCESA, en la que existe un servidor Proxy para compartir la conexión a Internet, la cámara a instalarse será únicamente visible desde la red interior, a menos que sea instalada utilizando un router para su salida a Internet o se le asigne una IP pública propia para la cámara.

2.4.3. Autenticación

Una de las líneas de defensa más utilizadas es la protección de las contraseñas. Varias técnicas de seguridad, incluyendo la encriptación, ayudan a asegurarse de que las contraseñas se mantienen a salvo. También es necesario exigir que las contraseñas se cambien frecuentemente, que no sean adivinadas fácilmente o palabras comunes del diccionario, y que no se revelen simplemente. La autenticación es el paso adicional para verificar que la persona que ofrece la contraseña es la persona autorizada para hacerlo.

El servidor cifra la contraseña que recibe del usuario, utilizando la misma técnica de encriptación empleada para cifrar la tabla de contraseñas del servidor. Compara la contraseña cifrada del usuario con la contraseña cifrada en la tabla. Si los resultados encajan, el usuario tiene permiso para entrar en el sistema. Si los resultados no encajan, el usuario no tiene permiso.

Las contraseñas de la gente y los nombres de usuario se almacenan dentro de una base de datos que se encuentra en un servidor que verifica las contraseñas. Dependiendo de la técnica de autenticación de contraseñas que se use, el archivo puede estar cifrado o no.

Para el caso de las cámaras IP, éstas cuentan con un sistema de protección de contraseñas, dependiendo del tipo de usuario que requiera el acceso. Por ejemplo, se podrían tener usuarios con perfiles administrativos los cuales tendrán acceso total a la cámara no solo para visualización sino también para configuración y creación de usuarios.

Se podría tener usuarios con perfiles de acceso únicamente a la visualización y a la manipulación de la cámara, más no a la configuración de la misma. Y finalmente podemos tener usuarios que únicamente puedan ver la transmisión de la cámara pero no puedan manipularla ni cambiar su configuración.

Estos usuarios podrían ser creados por el administrador de la red o del sistema de vigilancia, ya que en la mayoría de las cámaras, esta información se guarda localmente en cada una de ellas, pudiendo con esto además permitir el acceso de ciertos usuarios a ciertas cámaras nada más. Es decir, no necesariamente un usuario puede tener acceso a todas las cámaras de un sistema de vigilancia en red.

2.5. ACCESO REMOTO

El acceso remoto es la capacidad de lograr acceder a un equipo informático o a una red desde un lugar alejado o simplemente remoto. En muchas ocasiones, dentro de una corporación, los empleados que trabajan en sus sucursales, los trabajadores a distancia y los empleados que se encuentran en viaje de negocios necesitan acceder a la red de la organización. La capacidad de acceso remoto también es necesaria para acceder a los servicios de aplicaciones centrales tales como Terminal Server de Microsoft, que proporcionan acceso para múltiples usuarios a ciertas aplicaciones.

El acceso remoto puede darse de varias maneras, las más conocidas son mediante una llamada telefónica y a través de Internet por su puesto. Para el caso de las cámaras IP, hablamos de acceso remoto a ellas utilizando Internet, ya que al ser ésta una red de gran tamaño, decimos que podemos acceder a nuestra cámara literalmente desde cualquier lugar del mundo por más alejados que nos encontremos. Existen además ciertos tipos de cámaras que permiten el acceso a éstas a través de una llamada telefónica, el inconveniente es que para visualizar el video, debemos realizar la llamada desde un video teléfono, lo cual no siempre está al alcance de nuestras manos ni es soportado por todos los tipos de cámaras.

CAPITULO III

3.1. ANALISIS DE LA RED DE LA PUCESA

La red interna de la PUCESA está integrada básicamente por dos segmentos de red formados por las direcciones IP privadas 192.168.1.xxx y 192.168.2.xxx respectivamente. Se cuenta además con un servidor *Solaris* con sistema operativo *Unix*, el cual sirve también de enlace entre la red interna y la red WAN de acceso a Internet. Para esto el servidor cuenta con dos tarjetas de interface, la una para la red interna con la IP 192.168.1.200 y la otra para la red pública con la IP 200.107.37.166, a través de la cual también se puede acceder al sitio Web de la PUCESA.

La conexión interna a Internet, se realiza a través de un servidor Proxy, el cual está en la dirección 192.168.1.200 utilizando el puerto 3128.

Cabe anotar además que parte de uno de los segmentos de la red está formado por componentes de red wireless (inalámbricos), los cuales permiten el acceso remoto a la red y a Internet a través del proxy.

3.2. SELECCIÓN DE LA CÁMARA IP

En el mercado se pueden encontrar varias marcas y tipos de cámaras IP con variaciones en la conectividad, calidad de video, soporte para audio, capacidad de zoom (óptico o digital), capacidad de rotación (PAN y TILT), y desde luego distintos precios dependiendo de la marca y características.

La elección de la cámara adecuada, debe estar dirigida básicamente por las necesidades de uso y aplicación; es decir, cuál es el uso que vamos a darle a la cámara y que beneficio obtendremos del mismo.

En base al análisis realizado de la red de la PUCESA, la plataforma existente y de acuerdo al presupuesto del presente proyecto se seleccionó la Cámara D-Link CS-5300 por ser una de las más versátiles y tener muchas funcionalidades útiles para nuestra aplicación, además de ser totalmente garantizada y a un costo medio. Es la solución de video

vigilancia con la mejor relación costo/efectividad del mercado, ideal y conveniente para organizaciones pequeñas y medianas.

3.3. Cámara IP D-Link CS-5300

Está diseñada como un excelente sistema de seguridad para monitorear remotamente un lugar. Con todas las facilidades esperadas en éste tipo de cámara, puede ser conectada a cualquier red Ethernet, de una Oficina, Banco, Super Mercado o Campus, y vigilar dichos lugares desde la propia red LAN o desde Internet vía banda ancha, permitiendo observar en línea el sitio elegido, entregando además una alta calidad de video, dependiendo del ancho de banda disponible.

Entre sus ventajas estándar incorpora un Servidor Web, detección de movimiento, que puede ser habilitado para grabar cuando exista movimiento, y grabación hacia dispositivo de almacenamiento masivo en línea. Pero además incorpora entre sus ventajas avanzadas movimientos horizontal y vertical (PAN/TILT), que pueden ser controlados a través del software de gestión (IP View) o directamente vía interfaz Web, o si lo prefiere vía control remoto. A las principales ventajas descritas cabe añadirle también su costo, que en nuestro medio es de $400,00.

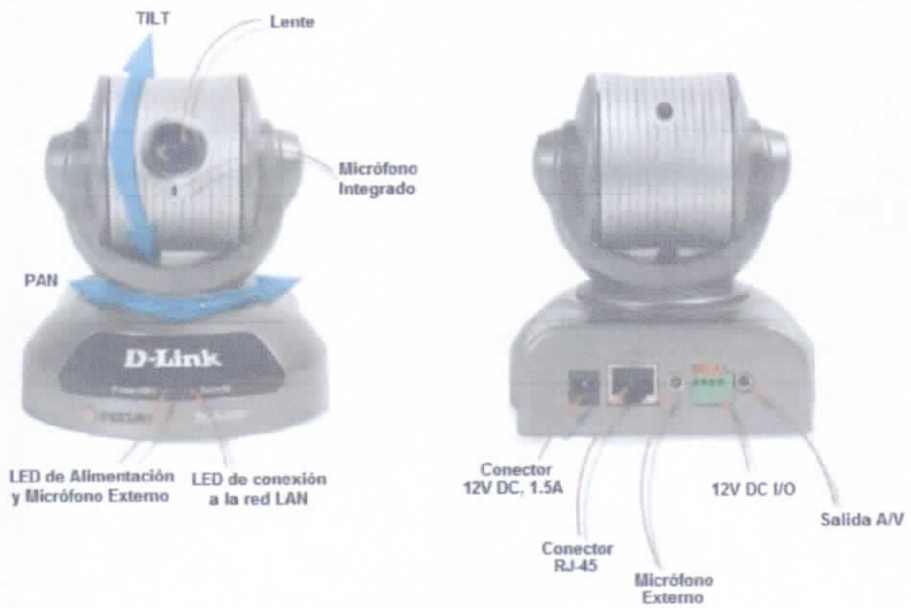


Figura 11: Vista externa y partes principales de la cámara D-Link CS-5300

3.3.1. Características Principales

- Soporte PAN/TILT.
- 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 simultánea.
- Activación de grabado de video, ante detección de movimiento.
- Control remoto, para direccionar la cámara hacia el objetivo deseado.
- Puerto de I/O para comunicación hacia dispositivo externo.
- Audio incorporado.
- Zoom digital (10x).
- Detección de movimiento y notificación vía e-mail.
- Salida de audio y video, para conexión hacia televisor.
- Fácil y rápida implementación de sistema de video vigilancia.

3.3.2. Ficha Técnica

Interfaces	1 Puerta RJ-45 auto-sensing Fast Ethernet 10/100Mbps
Especificaciones de la Cámara	▪ 24-bit RGB, 320x 240 resolución ▪ 1/4"color CCD sensor, interlace scan mode ▪ PAN rango,+/- 135° ▪ TILT rango –45° - +90° ▪ Soporte de Control Automático de Ganancia (AGC) ▪ Soporte de Exposición Automática (AE) ▪ Soporte de Balance Automático del blanco ▪ Disparador Electrónico 1/60 – 1/15000 seg. ▪ Relación Señal/Ruido: 56dB ▪ Mínima iluminación : 2.5 lux @ 1.4 ▪ Montaje del Lente: Estándar CS, 6.0mm, f 1.8
Imagen (configuración de video)	▪ Modo compresión MPEG4, short header ▪ Tasa de Compresión: 5 niveles ▪ Tamaño de imagen ajustable, quality y bit-rate ▪ Time stamp y text overlay
Acceso Usuarios	Vía Web.
Protocolos Soportados	HTTP, FTP, SMTP, DHCP, Telnet, NTP, DNS, DDNS, UPnP, PPPoE

Seguridad	• Administrador y UGP (user group protection) • Password de autenticación de 15-dígitos
Administración y Upgrade	• Configuration y System Log Access via Web browser • Firmware upgrade via TCP/IP
Software de Administración	• Software Windows. Hasta 16 cámaras puede ser monitoreadas • Administración Remota y control de hasta 16 DCS-5300 Internet Cameras • Soporte de todas las funcionalidades Web • Opción de grabación programada o manual
Audio	8Kbps
Alarmas e I/O	• Detección de movimiento • Transferencia periódica de imágenes vía e-mail y descarga a servidor vía FTP • 1 Sensor de entrada (12VDC a 48VDC /50mA) • 1 Relay de salida (max. 24VDC, 125VAC/0,5ª)
Esquemas de Playback	• Fecha, • Intervalo de tiempo y • Eventos activados (triggered), con preview para cada cámara
Modos de Control del Playback	• Play • Stop • Pause • Fast forward • Slow forward • Pull bar • Zoom in, y • Zoom out

Características Físicas

Alimentación Eléctrica	12 VDC 1.5A. External universal power adapter (100 to 240 VAC, 50/60Hz)
Consumo	18 watts
Peso	343grs. Aprox.
Dimensiones	110.5 x 103.5 x 103.0 mm. Aprox.
Temperatura Operación	5° C a 55° C
Temperatura Almacenaje	10° C a 60° C
Humedad	20% a 90% No Condensado
Emisión (EMI)	• FCC Class B • CE Class B • LVD (EN60950)

3.4. Análisis de la Instalación de una Cámara IP

Según el tipo, las cámaras IP disponen de una conexión directa de un puerto ethernet RJ45 o una antena wireless, lo que nos permite monitorizar lugares que necesitemos controlar, con la ventaja de utilizar las redes actuales como Internet transmitiendo hasta 25 fps (fotogramas por segundo) o más según la cámara.

Dependiendo del tipo de conexión que vayamos a realizar, se la puede conectar directamente a un PC, a un puerto ethernet libre de un Router o Switch; e incluso se la puede instalar únicamente en nuestra LAN local o directamente a Internet a través de una IP pública.

Con una simple configuración seremos capaces de ver las imágenes en nuestra red interna y un paso más y podremos verlas desde cualquier parte del mundo.

Monitorizar las imágenes es simple, solo con un navegador de Internet le indicaremos la dirección IP donde se encuentre el sistema y podremos vigilar todo lo que deseemos. Si la aplicación que acompaña al producto no es suficiente, algunas marcas y modelos de cámaras disponen de controles ActiveX para desarrollar aplicaciones a medida.

En base a lo mencionado anteriormente, tenemos cuatro tipos de configuración de una cámara IP. Los parámetros de red difieren según el tipo de configuración de la cámara:

Tipo 1. Conexión LAN/Intranet con un Concentrador de conmutación Ethernet.

La cámara IP se puede instalar en la LAN/Intranet.

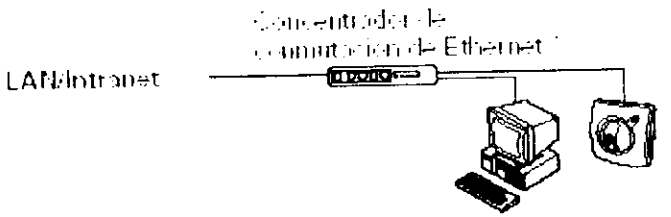


Figura 12: Conexión de una cámara IP a una LAN

Tipo 2. Conexión a Internet con un Router de banda ancha.

Se puede acceder a la cámara desde Internet.

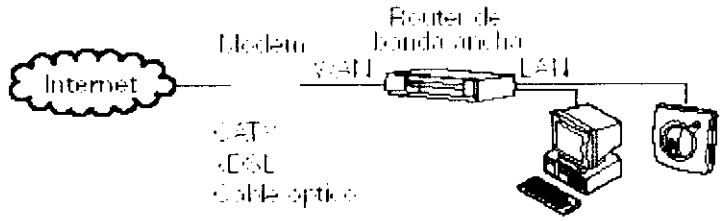


Figura 13: Conexión de una cámara IP a través de un Router

Tipo 3. Conexión directa a Internet con un módem

La cámara IP se puede instalar independientemente sin PC en la red Internet. Cuando instale la cámara IP según el Tipo 3, conéctela temporalmente según el Tipo 1, el Tipo 2 o el Tipo 4.

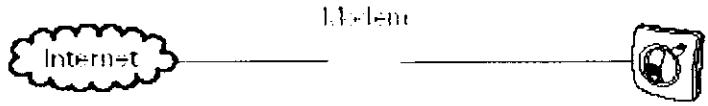


Figura 14: Conexión de una cámara IP a través de un Módem

Tipo 4. Conexión directa con un PC

La cámara IP se puede instalar directamente al PC.

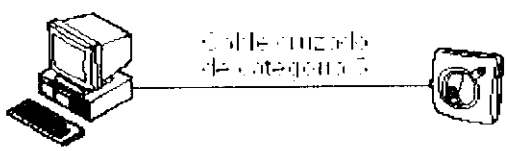


Figura 15: Conexión de una cámara IP a un computador

<table>
<tr><th rowspan="2">Parámetros</th><th colspan="4">Tipo de configuración de la cámara IP</th></tr>
<tr><th>Tipo 1</th><th>Tipo 2</th><th>Tipo 3</th><th>Tipo 4</th></tr>
<tr><td>Puerto [1]</td><td>80 (por defecto)</td><td colspan="2">80 (por defecto) [2]</td><td>80 (por defecto)</td></tr>
<tr><td>Dirección IP</td><td>Estática</td><td>Estática [3]</td><td>Estática [4]</td><td>Estática por defecto</td></tr>
<tr><td>Máscara de Subred</td><td colspan="3">Máscara de subred de la LAN</td><td>Máscara por defecto</td></tr>
<tr><td>Puerta de Enlace</td><td>Puerta de enlace de la LAN</td><td>IP privada del Router de Banda Ancha</td><td>Puerta de enlace de la LAN</td><td rowspan="2">No es necesario</td></tr>
<tr><td>DNS</td><td colspan="2">Dirección del Servidor DNS</td><td>Dirección del Servidor DNS [4]</td></tr>
<tr><td>Uso del Ancho de Banda</td><td colspan="4">Puede restringir el ancho de la banda de transmisión [5]</td></tr>
</table>

Tabla 8: Parámetros de red para las cámaras IP

Antes de proceder con la instalación de una cámara IP, se deben tomar en cuenta las necesidades y que tipo de conexión existe en la red para salir a Internet. Como se vio existen cuatro tipos de conexión básica en función de la utilidad que se va a dar a la cámara y de la manera en que ésta tendrá acceso a Internet. Para el caso de la red de la PUCESA, se escogió en tipo de conexión 1, puesto que como se habló anteriormente la red interna tiene acceso a Internet a través de un servidor Proxy, y la cámara seleccionada no puede trabajar de esta manera, sino únicamente a través de un router o directamente con una dirección IP asignada por el ISP. De esta manera la cámara fue configurada con una dirección IP privada 192.168.1.66 y conectada a uno de los switch's para su utilización en intranet únicamente.

[1] Cuando utilice más de una cámara IP con un Router de banda ancha, cada cámara IP precisa de su propio número de puerto. El número de puerto por defecto puede variar según la marca y el modelo de la cámara.
[2] Muchos ISPs bloquean intencionadamente el Puerto N° 80 para protegerse de ciertos virus de red. Si su ISP bloquea el puerto N° 80, sustituya otro N° de puerto no utilizado.
[3] Consulte el manual del Router de banda ancha acerca de la función de Desvío de puerto.
[4] Cuando utilice la cámara IP en la función DHCP, seleccione [DHCP] e introduzca el nombre de host si el ISP lo requiere. Si obtiene automáticamente la dirección de la puerta de enlace por defecto y del servidor DNS desde el servidor DHCP, no es necesario que lo instale.
[5] Esta alternativa es opcional y puede variar según la marca y el modelo de la cámara.

3.4.1. Configuración básica para una sola cámara

Primero, se debe configurar adecuadamente el router doméstico. Normalmente el ISP le asignará una dirección IP de Internet utilizando DHCP, a la cual nos referiremos en adelante como la IP WAN. Esto es prácticamente transparente para el usuario, pero es necesario para poder acceder a las cámaras de red desde el exterior.

En la LAN, el router tendrá una dirección local. Normalmente es 192.168.0.1. El router doméstico actuará entonces como un servidor DHCP, asignando direcciones IP en la LAN. Lo común es que estas direcciones se asignen desde la 192.168.0.100 hacia arriba. Esto deja espacio para direcciones IP estáticas, que es lo que necesitan la mayoría de las cámaras IP. Por lo tanto es una buena idea usar IPs a partir de la 192.168.0.50 en un ambiente como este. Estas direcciones necesitan ser configuradas manualmente, y es recomendado que esto se realice después de instalar el router doméstico.

Una vez que la cámara tiene su dirección IP asignada, las imágenes deben ser visibles en la red local utilizando un navegador Web. Deshabilite cualquier configuración Proxy en el navegador (esto normalmente viene deshabilitado por defecto) y escriba la dirección IP de la cámara en el campo de dirección del navegador (ej. 192.168.0.50). La imagen ahora debe ser visible.

Para hacer que la cámara esté disponible desde el exterior, use la función de transporte de direcciones (port forwarding) del router doméstico. Esta caracteristica esta disponible en la mayoría de los routers. Especifique que el puerto 80 de la IP WAN apuntará al puerto 80 de la dirección IP local. Esto hará que ahora la cámara sea accesible desde la Internet, dado que la dirección IP WAN es conocida. Puede encontrarla en la página de status dentro de la configuración del router doméstico. La cámara de red está ahora en vivo en Internet.

Recuerde que, cuando la cámara está disponible desde el exterior, cualquier persona que esté en Internet puede monitorearla. Si requiere privacidad, se recomienda cambiar la contraseña por defecto de la cámara o utilizar una aplicación a su medida en la que pueda validar usuarios y contraseñas para el acceso a la cámara.

3.4.2. Configuración básica para varias cámaras con un router doméstico

Para la presente explicación, nos basaremos en un ejemplo supuesto, ya que esta configuración no puede ser aplicada en la red de la PUCESA al no contar con más cámaras ni con un router de enlace.

El primer paso sería ajustar las cámaras de acuerdo con la configuración básica anterior. En este ejemplo asumiremos que habrá 5 cámaras con IPs en el rango de 192.168.0.50 - 192.168.0.54.

Como existe sólo una IP WAN disponible, se necesitarán utilizar diferentes puertos en el router. Como ejemplo, el protocolo HTTP usa por defecto el número de puerto 80. La mayoría de los números de puerto por debajo del 1024 están estandarizados, pero se pueden utilizar de ser necesario. Sin embargo, es muy recomendado no usar los números de puerto inferiores al 80, ya que algunos servicios comunes dependen de ellos. En este ejemplo se utilizarán los puertos 81 y superiores.

A fin de configurar las diferentes cámaras, los puertos de la IP WAN necesitan ser mapeados individualmente a las direcciones internas de las cámaras. Asumiendo que hay 5 cámaras, necesitan ser mapeadas de acuerdo a la tabla de abajo. Este ejemplo supone que el router doméstico puede mapear un número de puerto a una dirección IP con número de puerto diferente (ej. tener el puerto 80 de todas las cámaras mapeados a diferentes puertos en la WAN). En este caso el usuario debe configurar las cámaras para que utilicen de manera local el mismo número de puerto que el que usaran de manera externa.

Esto lo puede hacer en el menú de configuración de las cámaras. Una vez cambiado, no es posible acceder a las cámaras utilizando el puerto HTTP por defecto y el usuario deberá siempre usar el nuevo número de puerto como se indica en la tabla siguiente:

IP WAN	Puerto	IP Local	URL local sin mapeo de puertos cruzados
x.y.z.q	80	192.168.0.50	192.168.0.50

x.y.z.q:81	81	192.168.0.51	192.168.0.51:81
x.y.z.q:82	82	192.168.0.52	192.168.0.52:82
x.y.z.q:83	83	192.168.0.53	192.168.0.53:83
x.y.z.q:84	84	192.168.0.54	192.168.0.54:84

Tabla 9: Direcciones IP y puertos de la cámara

En este momento las cámaras pueden ser vistas desde Internet. Recuerde la seguridad.

3.4.3. Direcciones IP estáticas o dinámicas

La mayoría de los ISPs proveerá al suscriptor de una dirección IP dinámica que, en teoría, puede cambiar cada hora. Sin embargo, es una práctica común mantener la misma dirección IP todo el tiempo que dure activa la conexión. Así que mientras haya actividad la IP se mantendrá igual, y cuando la conexión se restablezca después de un periodo de inactividad, se asignará una nueva dirección IP. El mejor escenario es, por supuesto, que el ISP pueda asignar un IP estática, lo que garantiza que la dirección nunca cambiará.

La dirección IP WAN se puede encontrar en la página de status del router doméstico. Anótela y pruebe las cámaras.

Es probable que el ISP no informe al usuario si sus direcciones IP dinámicas realmente cambien o no (aunque es recomendado preguntar). La única manera segura de averiguarlo es mediante prueba y error. Utilice el router doméstico por un par de semanas, y anote que dirección IP WAN tiene. Si cambia será más difícil tener las cámaras accesibles desde Internet. Es posible, pero requiere cierta programación.

3.4.4. Nombre de dominio para las cámaras

Debido a que es tedioso y difícil recordar la dirección IP de un sitio Web, es preferible tener un nombre de dominio personal (ej. www.camarabodega.com).

Existen dos maneras básicas y recomendables de obtener un nombre de dominio:

a. Registrar un dominio utilizando alguno de los populares sitios DNS dinámicos. El servicio DYN DNS (http://www.dyndns.org/) ofrece un servicio básico gratuito.
b. Registrar un dominio real con alguna empresa especializada (ej. http://www.register.com/).

3.4.5. Acceso y publicación

Dependiendo la aplicación y utilidad que se vaya a dar a las cámaras IP, se puede establecer el acceso y la publicación de las imágenes transmitidas, para que éstas sean públicas o privadas. El software que viene con la mayoría de las cámaras nos permite establecer estas características, pero es altamente recomendable en el caso que sea necesario restringir el acceso, la creación de una aplicación o sitio Web que permita las conexiones únicamente a aquellos usuarios autorizados, a través de nombres de usuario y contraseñas que sean validadas por un servidor. Para esto ciertos modelos de cámaras vienen con controles ActiveX para que cada usuario pueda crear su propio sitio Web o aplicación a medida de sus necesidades y fijando el nivel de seguridad adecuado para el caso.

3.4.6. Instalación de la Cámara IP D–Link CS-5300 en la PUCESA

Los requisitos mínimos para instalar la cámara, según las necesidades planteadas y la plataforma en la cual va a funcionar, sin descuidar el óptimo rendimiento de la misma serían:

- Procesador Pentium III, 800MHz o superior.
- Memoria 128 MB (recomendado 256 MB)
- Tarjeta VGA a 800x600 o superior
- Microsoft Internet Explorer 5.x o superior (Otros navegadores no soportan todas las opciones de la cámara).

3.4.6.1. Instalación del hardware

Primeramente debemos conectar un extremo del cable Ethernet que viene incluido con la cámara, en el conector Ethernet situado en la parte trasera de la misma y el otro

extremo a la red a través de un hub, switch o router. Si se va a conectar directamente la cámara a un computador, se debe utilizar un cable Ethernet CrossOver (cruzado).



Figura 16: Conexión del cable UTP a la cámara

Luego unimos el extremo del cable de alimentación al conector de alimentación DC situado en la parte posterior de la cámara (etiquetado como DC 12V) y el otro extremo a una toma de corriente AC de 110V. Tanto el LED rojo como el verde parpadearán alternativamente, y únicamente el LED rojo permanecerá encendido indicando la correcta alimentación eléctrica de la cámara. El LED verde no se iluminará hasta que se haya configurado la cámara.



Figura 17: Conexión del cable de poder a la cámara

Opcionalmente se puede conectar la cámara a un televisor para ver directamente el video a través de este. Para esto conectamos el cable A/V (Audio/Video) incluido con la cámara, en el conector de salida A/V ubicado en el panel posterior.

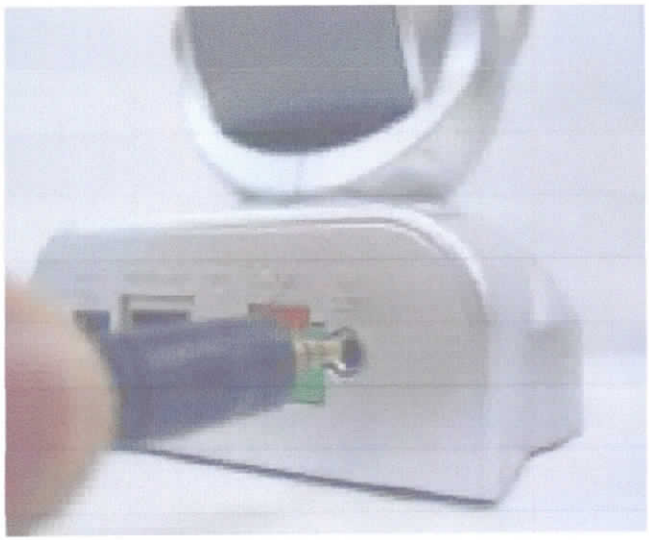


Figura 18: Conexión del cable de Audio/Video a la cámara

Introducimos el conector RCA rojo del otro extremo del cable en el conector de vídeo del televisor.



Figura 19: Conexión del cable de Video al Televisor

Introducimos el conector RCA negro en el conector de audio del televisor.

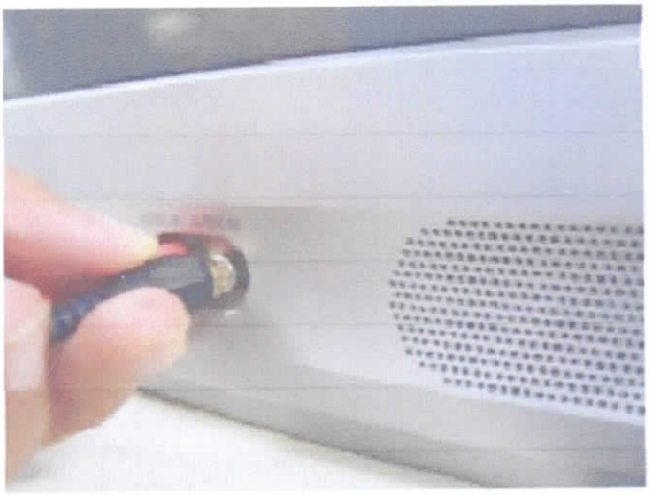


Figura 20: Conexión del cable de Audio al Televisor

De esta manera queda instalado el hardware de la cámara, a continuación procedemos a la instalación de software y configuración de la misma.

3.4.6.2. Instalación del software y configuración básica

Introducimos el CD **DCS – 5300** en la unidad CD-ROM. Esta es la primera pantalla que aparecerá.

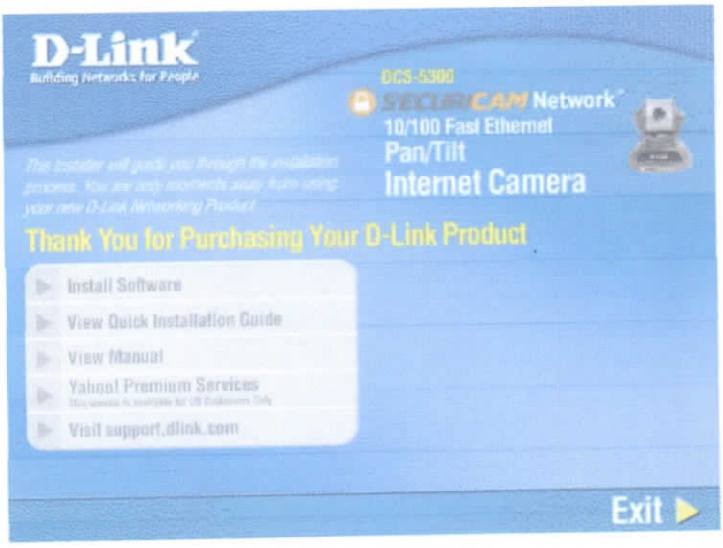


Figura 21: Pantalla de Bienvenida y Menú Principal para instalación de la cámara

Hacer clic en ***Install Software***, y luego en ***Instalation Wizard***. A continuación aparecerá una pantalla indicándonos la instalación del software guía para la configuración

de la cámara. Procedemos con la instalación hasta finalizar el proceso y podemos cerrar la ventana anterior.

Hacemos clic en el icono creado en el escritorio 

para abrir el programa de configuración. Esta es la primera pantalla que aparecerá, la cual nos indicará que el programa está buscando cámaras conectadas a la red.

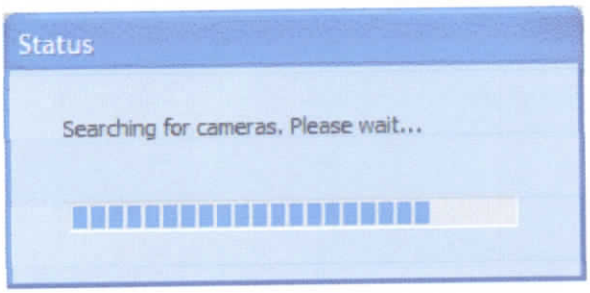


Figura 22: Software buscando cámaras conectadas

Si el software no detecta ninguna cámara, se deberá presionar en el agujero de ***reset***, usando algún instrumento lo suficientemente pequeño, de forma que se realice la conmutación de dos ciclos (los LED rojo y verde parpadearán sin interrupción y se detendrán dos veces). Se podrá retirar el instrumento cuando el LED rojo parpadee por segunda vez.



Figura 23: Orificio para reset

Seguidamente se nos presenta una ventana con opciones de configuración y con datos de las cámaras detectadas en la red.

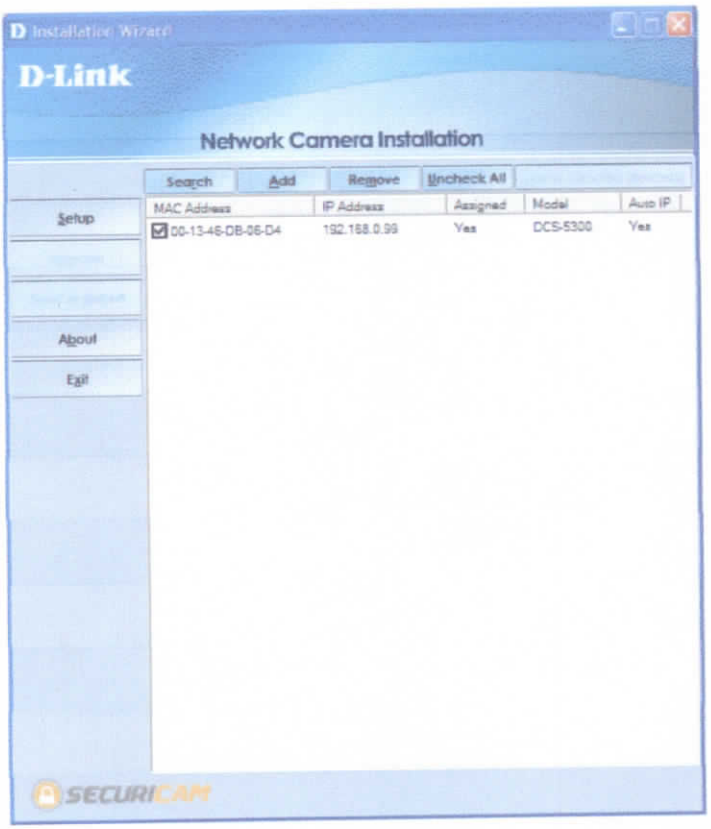


Figura 24: Datos de la(s) cámara(s) detectada(s)

La pantalla nos presentará una dirección MAC de la cámara y una dirección IP (que podrá ser correcta o no en función de a qué se haya conectado la cámara). Si hay un servidor DHCP (Dynamic Host Configuration Protocol) en la red, la dirección IP será válida. Si en la columna ***Assigned*** se muestra la palabra ***Yes***, esto indicará que la dirección IP ha sido asignada a la cámara.

Hacemos clic en ***Setup***, para abrir la ventana de configuración básica de la cámara. Es recomendable en esta parte, crear una contraseña de ***Administrador*** para seguridad del acceso y configuración de la cámara.

En esta pantalla podemos además fijar la fecha y la hora de la cámara haciendo que ésta:

- Mantenga la hora y fecha que conserva actualmente.
- Sincronice la fecha y la hora con la del computador que está ejecutando la configuración.

- Acepte la fecha y la hora ingresadas manualmente.
- Obtenga la fecha y la hora de manera automática desde un servidor NTP.

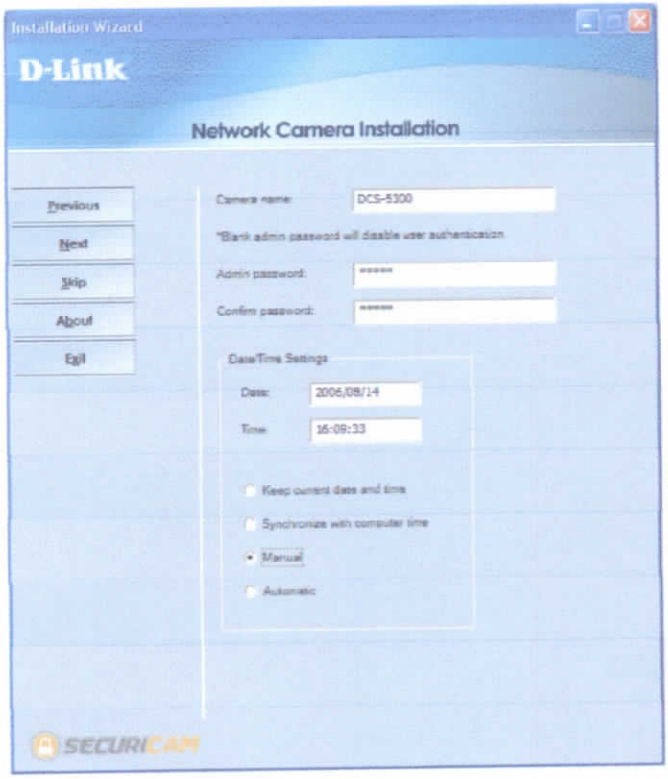


Figura 25: Configuración básica

Hacemos clic en ***Next*** para continuar con la configuración y poder establecer una dirección IP estática en caso de no tener un servidor DHCP instalado en la red. En nuestro caso ingresamos la dirección IP privada 192.168.1.66, asignada por el jefe del centro de Cómputo de la PUCESA, ingresamos además la máscara de subred 255.255.255.0. La puerta de enlace predeterminada y las direcciones de los servidores DNS (Domain Name Server) pueden ser ingresadas en caso de ser necesario.

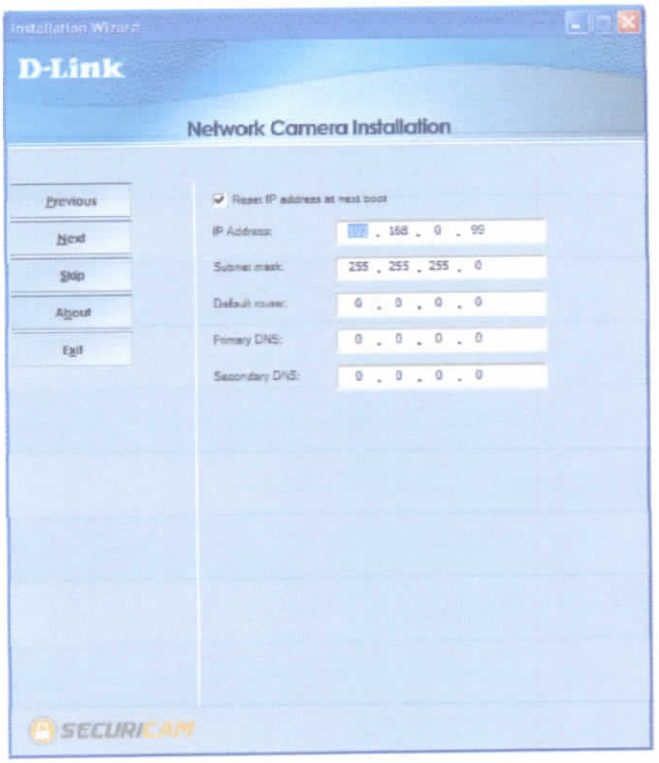


Figura 26: Configuración de parámetros de red

Hacemos clic en ***Next*** para continuar con la configuración y finalmente aplicar los cambios realizados en la cámara, para esto hacemos clic en ***Apply***, y nos aparecerá una ventana indicándonos el progreso de la actualización.

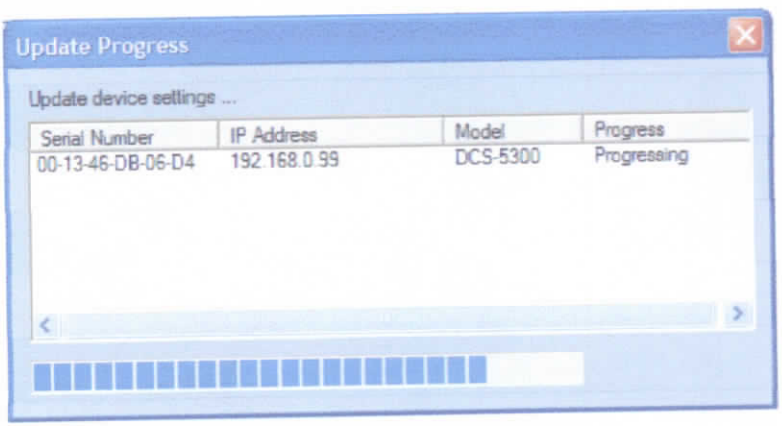


Figura 27: Guardando cambios

Finalmente podemos hacer clic en ***Link to selected device(s)*** y se abrirá automáticamente el Internet Explorer en la dirección IP guardada en la cámara que para el caso es ***http://192.168.1.66***. Se nos pedirá ingresar un nombre de usuario y contraseña para

acceder a la página, entonces ingresaremos la contraseña de administrador guardada anteriormente.

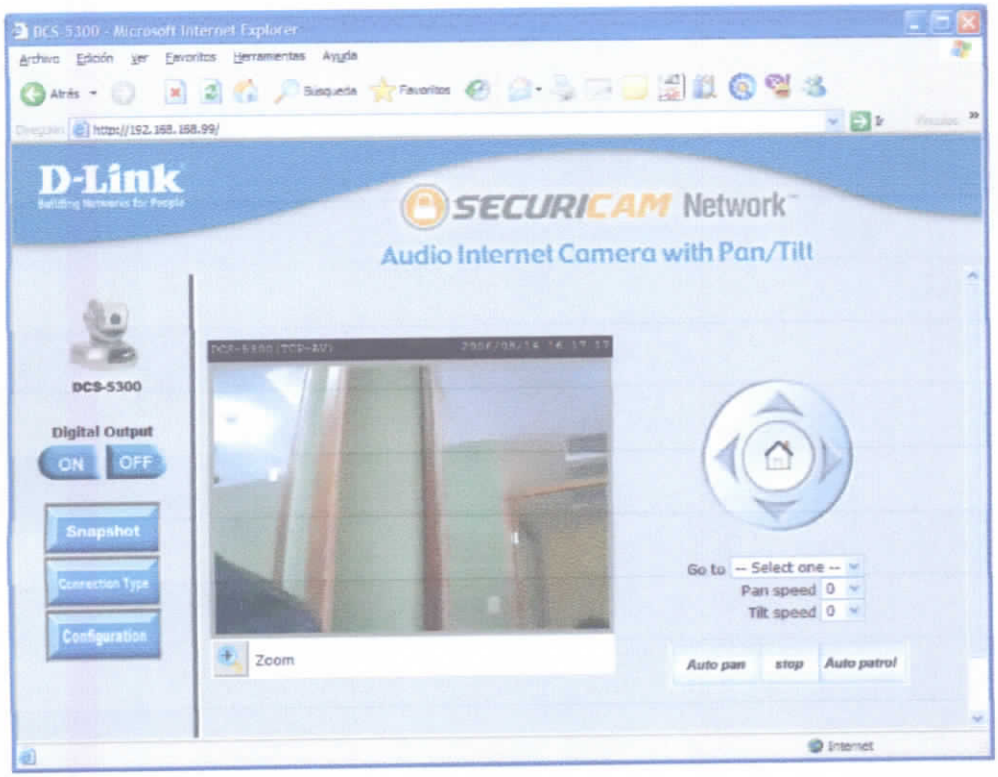


Figura 28: Pantalla principal de visualización y manejo

Se deberá entonces visualizar la imagen captada por la cámara en ese instante. Si es así, se ha finalizado con éxito la conexión y configuración de la cámara IP. Se podrá acceder a la cámara ejecutando el Internet Explorer con la dirección IP asignada a la cámara desde cualquier computador perteneciente a la red.

3.4.7. Manejo y uso de la cámara

En la pantalla principal disponemos de varios controles, los mismos que pueden ser utilizados para la manipulación y otros tipos de configuraciones. Para la rotación de la cámara, podemos utilizar los botones en forma de flecha haciendo clic sobre cualquiera de estos. El botón con el icono de una casa, puede ser utilizado para regresar al lente de la cámara a su posición original en la que se fija luego del encendido.



Figura 29: Controles de manejo

En la parte inferior de los botones descritos tenemos otras opciones para el movimiento de la cámara:

- Go to: Lista las posiciones predeterminadas de la cámara que han sido guardadas con anterioridad. Al seleccionar una, la cámara girará hasta ésa posición.
- Pan speed: Se puede seleccionar una de las 11 velocidades de Pan, desde -5 hasta 5, según la preferencia del usuario.
- Tilt speed: Se puede seleccionar una de las 11 velocidades de Tilt, desde -5 hasta 5, según la preferencia del usuario.
- Auto pan: La cámara inicia con un movimiento horizontal automático.
- Stop: Detiene el movimiento de la cámara iniciado con *Auto pan*.
- Auto patrol: Realiza un movimiento desde la posición actual hasta una de las posiciones predefinidas en la opción *Patrol selection*.

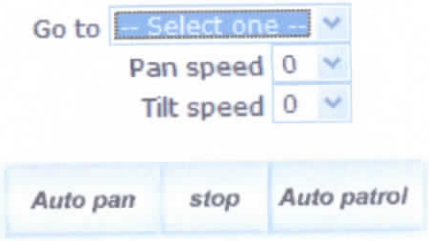


Figura 30: Controles de posición

Los movimientos y controles descritos pueden ser también realizados desde el mando a distancia incluido con la cámara.

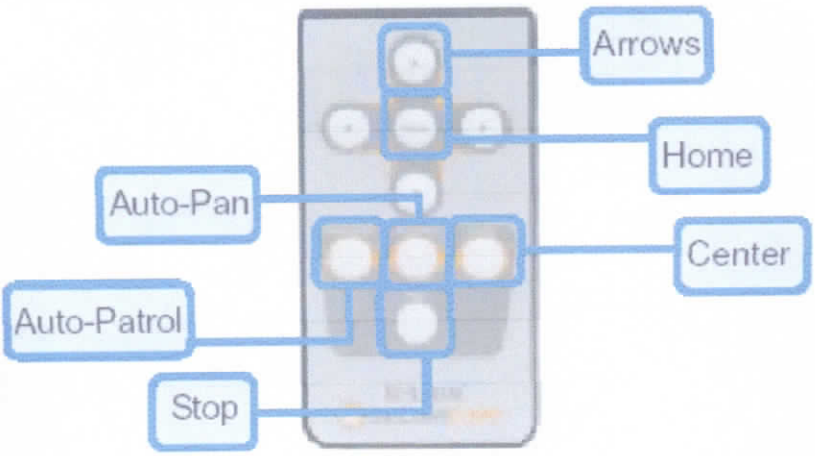


Figura 31: Esquema del mando a distancia

Para realizar zoom, hacemos clic en el botón  ubicado en la parte inferior de la imagen, y luego deslizamos el control manual hasta llegar a la amplitud deseada, finalmente escogemos el botón *Hide* para regresar a la imagen ampliada. El zoom puede ser seleccionado desde el 100% hasta el 400%.

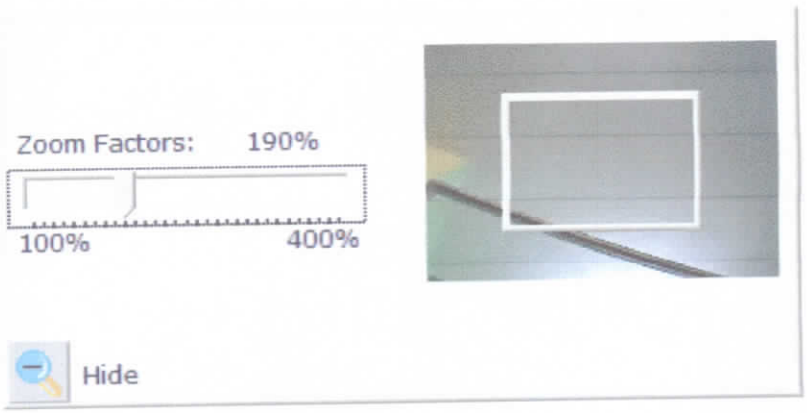


Figura 32: Opciones de zoom digital

La cámara nos permite también capturar imágenes fijas, para esto sencillamente hacemos clic en el botón ***Snapshot*** ubicado en la parte izquierda, e inmediatamente nos aparece una nueva ventana con la imagen capturada, ésta puede ser guardada a un dispositivo de almacenamiento o ser reemplazada por otra imagen con un nuevo clic en el botón mencionado.



Figura 33: Imagen capturada con Snapshot

3.4.7.1. Tipo de conexión

La cámara D-LINK DCS-5300, soporta tres protocolos para la transmisión de audio y video: UDP, TCP, HTTP (video únicamente). Al conectarse exitosamente, ésta detecta de manera automática y selecciona el mejor protocolo para la transmisión, el cual queda guardado en ***Protocol Option***. Si se desea cambiar el protocolo por defecto, basta seleccionarlo de la lista y pulsar el botón ***Save***.

En caso de seleccionar el protocolo HTTP, podemos deshabilitar la opción de transmisión de audio, a través de la casilla de verificación ***Disable audio***.

Todas estas opciones son visibles haciendo clic en el botón ***Connection Type***, y se puede regresar a la ventana de visualización en cualquier momento a través de la etiqueta ***Home***, así como también podemos invocar a la página de ayuda con le etiqueta ***Help***.

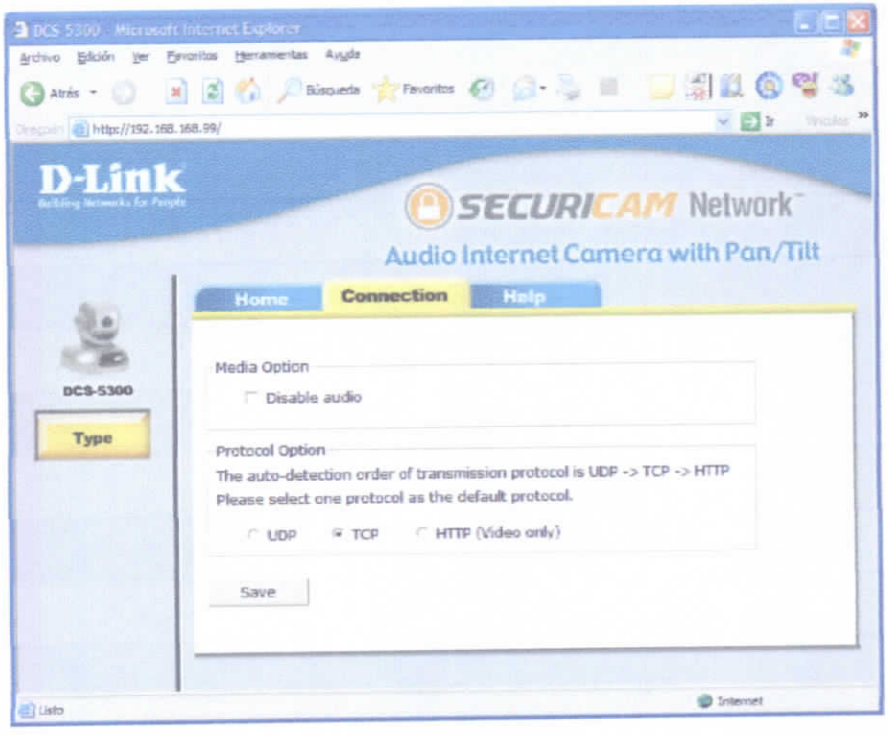


Figura 34: Tipos de protocolos

3.4.7.2. Administración de usuarios

Además del usuario *Administrador*, podemos crear y gestionar hasta 20 usuarios diferentes para acceder a la cámara. Dichos usuarios pueden ser creados con ciertas restricciones de visualización y configuración. Para la administración de usuarios, tenemos que haber ingresado como *Administrador*, y escoger la opción ***Configuration*** y luego la etiqueta ***Tools***.

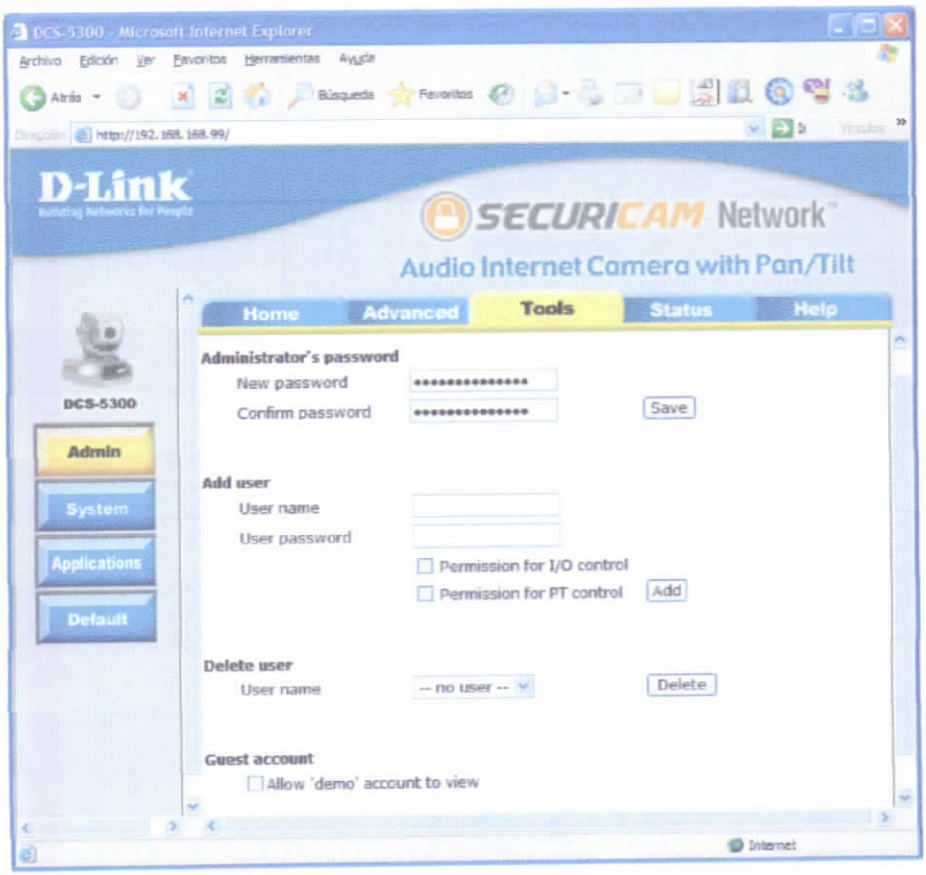


Figura 35: Administración de usuarios

Tenemos las opciones siguientes:

- **Administrator's password**, cambiar la contraseña de administrador. El botón ***Save*** guarda la nueva contraseña.
- **Add user**, añade nuevos usuarios a la cámara. Se ingresa el nombre de usuario y la contraseña. Se pueden otorgar permisos de entrada/salida y de manejo de la cámara a través de las opciones ***I/O control*** y ***PT control***. El botón ***Add*** almacena el usuario ingresado.
- **Delete user**, elimina un usuario registrado, seleccionándolo de la lista desplegable y haciendo clic en el botón ***Delete***.
- **Guest account**, habilita la cuenta de invitado. Este usuario ingresa únicamente a visualizar las imágenes de la cámara con restricción total de su uso y configuración.

Cabe señalar que el único usuario que tiene acceso total a la cámara es el *Administrador*, lo descrito en las siguientes secciones podrá ser utilizado únicamente por este usuario.

3.4.7.3. Configuración de red

Los parámetros de red pueden ser cambiados en cualquier momento según las necesidades del usuario y utilidades que se vayan a dar a la cámara. Se lo puede hacer ingresando a ***Configuration,*** etiqueta ***Advanced*** y botón ***Network***. La cámara y el software se reiniciarán automáticamente en 20 segundos luego de aplicar cualquier cambio realizado en esta sección.

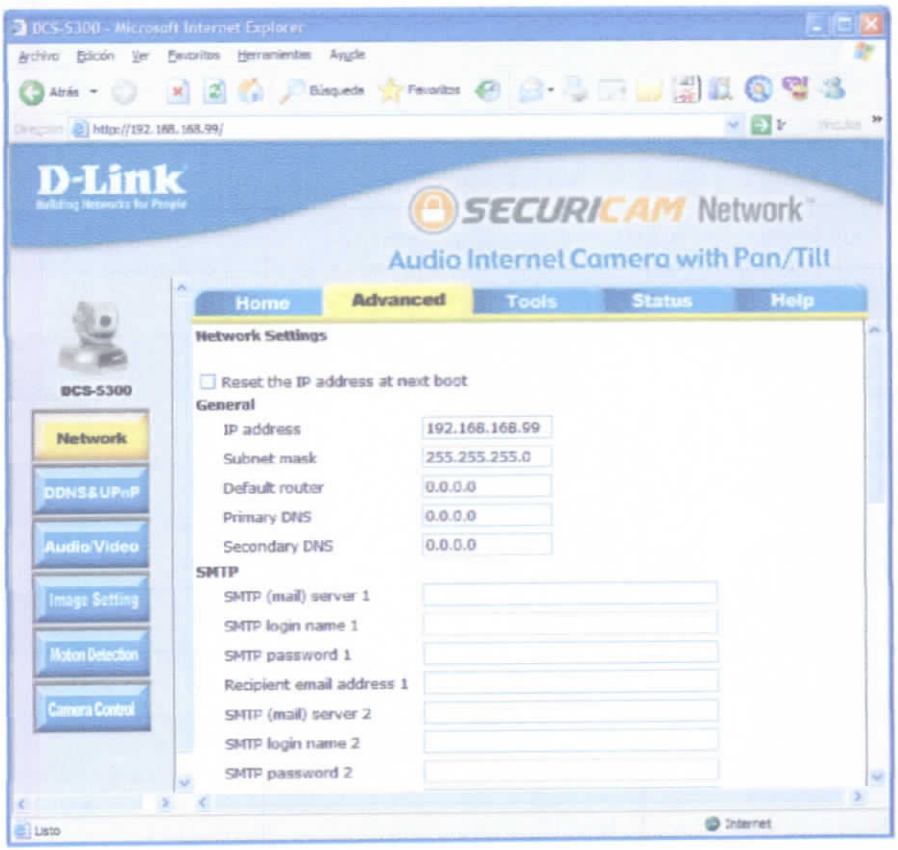


Figura 36: Parámetros de red, servidor de correo y servidor FTP

El software nos permite modificar los parámetros siguientes:

- **Reset de IP address at next boot**, opción deshabilitada por defecto. Sirve para que la cámara mantenga almacenada la dirección IP actual o que vuelva a la dirección por defecto la próxima vez que se reinicie.
- **General**
  - **IP address**, dirección IP de la cámara, la cual le identifica en la red.

- **Subnet mask**, la máscara de subred de la cámara, dependiendo de la configuración de la red. Por defecto será *255.255.255.0*.
- **Default router**, la dirección IP de la puerta de enlace predeterminada.
- **Primary DNS**, la dirección IP del servidor DNS primario.
- **Secondary DNS**, la dirección IP del servidor DNS secundario.

➢ **SMTP**

- **SMTP (mail) Server 1**, el nombre de dominio o dirección IP del servidor de correo electrónico. Es utilizado para enviar correos al detectar movimiento.
- **SMTP login name 1**, el nombre de usuario.
- **SMTP password 1**, la contraseña, si existe.
- **Recipient email address 1**, la dirección que recibirá los correos enviados por la cámara. Si se escriben varias direcciones deben ser separadas con punto y coma (;).
- **SMTP (mail) Server 2, SMTP login name 2, SMTP password 2, Recipient email address 2**, son parámetros opcionales en caso de tener otro servidor de correo electrónico.
- **Return email address**, dirección de correo alternativa a la cual se notificará en caso de haberse producido un error al enviar a las direcciones anteriores.

➢ **FTP**

- **Local FTP server port**, por defecto es el 21. Si es cambiado, el cliente externo también debería hacerlo para una correcta comunicación.
- **1st FTP server**, nombre de dominio o dirección IP de un servidor FTP al cual se vayan a enviar los *snapshots* (imágenes capturadas).
- **1st FTP server port**, Puerto del servidor FTP.
- **1st FTP user name**, nombre de usuario para acceder al servidor FTP externo.
- **1st FTP password**, contraseña para acceder al servidor FTP externo.
- **1st FTP remote folder**, especifica la carpeta de destino en el servidor FTP externo.

- **Primary FTP pasive mode**, permite el acceso de la cámara al servidor FTP externo, si ésta se encuentra atrás de un router protegido por un firewall.
- **2nd FTP server, 2nd FTP server port, 2nd FTP user name, 2nd FTP password, 2nd FTP remote folder, Secondary FTP pasive mode**, parámetros opcionales en caso de existir un segundo servidor FTP externo.

➢ **HTTP**

- **HTTP port**, el valor por defecto es 80. En caso de ser cambiado, los usuarios deberán especificar en el navegador la dirección IP de la cámara, seguido del nuevo número de puerto. Ej. http://192.168.0.99:8080.

➢ **Streaming**

- **Control channel port**, el valor por defecto es 5001, se corresponde con el puerto abierto por el firewall.
- **Audio channel port**, el valor por defecto es 5002, se corresponde con el puerto abierto por el firewall.
- **Video channel port**, el valor por defecto es 5003, se corresponde con el puerto abierto por el firewall.

3.4.7.4. Configuración de audio y video

La configuración de audio y video de la cámara, puede ser cambiada ingresando a ***Configuration,*** etiqueta ***Advanced*** y botón ***Audio/Video***.

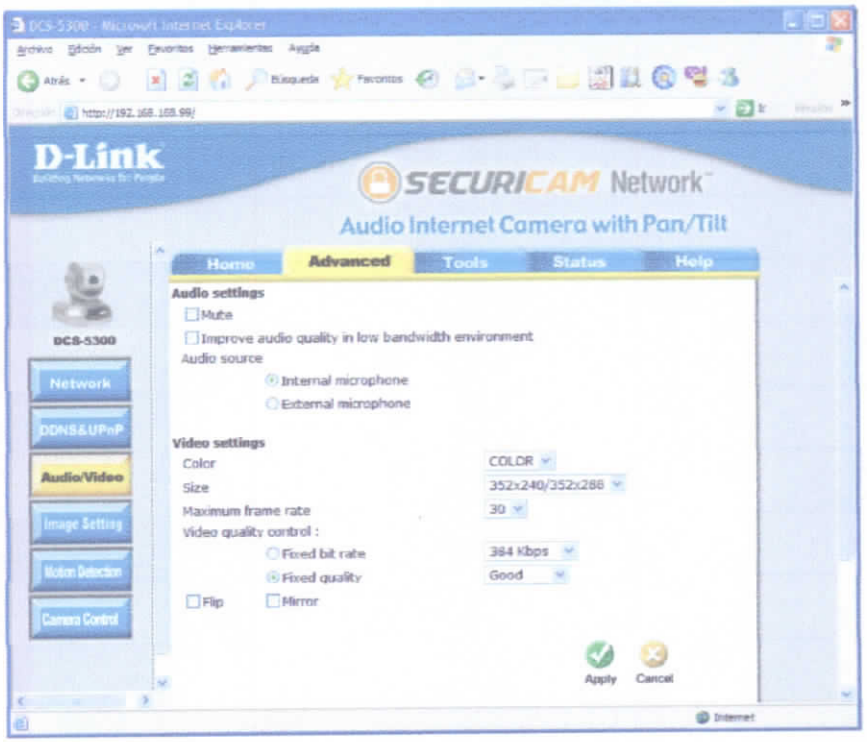


Figura 37: Configuración de Audio y Video

Las opciones se encuentran divididas en dos secciones: audio y video; cada una de las cuales puede ser configurada por separado. Las opciones que nos presentan para la configuración son:

- **Audio Settings**
  - **Mute**, quita el sonido captado por la cámara.
  - **Improve audio quality in low bandwidth environment**, mejora la calidad de audio, disminuyendo el video en tiempo real, en ambientes con bajo ancho de banda.
  - **Audio source**, permite seleccionar el micrófono interno o un micrófono externo conectado a la cámara.
- **Video Settings**
  - **Color**, permite seleccionar entre video a color o en blanco y negro.
  - **Size**, existen tres tamaños de video disponibles para seleccionar.
  - **Maximum frame rate**, selecciona la frecuencia a la cual la señal de video es refrescada. Depende del ancho de banda de la red.
  - **Video quality control**, utilizado para optimizar el comportamiento de la cámara en dependencia del ancho de banda disponible. *Fixed*

by rate, permite fijar la calidad del video en base al número de kilobits por segundo (kbps) a ser transmitidos. *Fixed quality*, permite fijar la imagen en base a parámetros de calidad preestablecidos.

- **Flip**, rota la imagen de manera vertical.
- **Mirror**, rota la imagen de manera horizontal.

3.4.7.5. Ajustes de la imagen

Permite al usuario modificar ciertas características de la imagen, como brillo, contraste, saturación y matiz. Para cada uno de ellos se puede seleccionar un valor entre -5 y +5. Tenemos además los botones *Preview*, para realizar una vista previa del cambio; *Restore*, para regresar la imagen a su estado normal luego de un cambio realizado y *Save*, para hacer permanentes los cambios efectuados. Las opciones se encuentran en ***Configuration,*** etiqueta ***Advanced*** y botón ***Image Setting***.

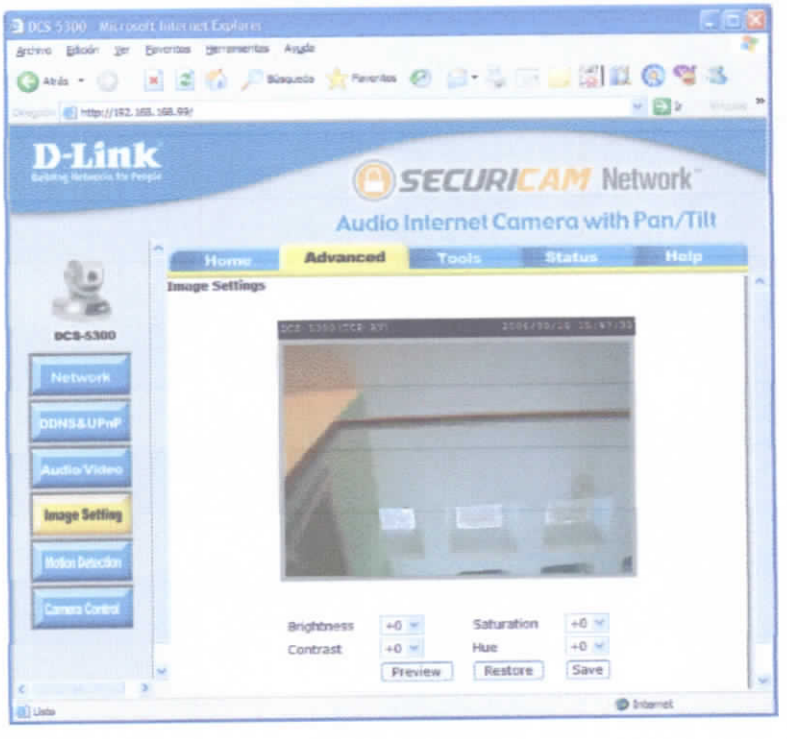


Figura 38: Ajustes de la imagen

3.4.7.6. Control de la cámara

Permite configurar la velocidad de rotación de la cámara, crear y establecer posiciones predeterminadas, entre otros aspectos. Ingresamos a ***Configuration,*** etiqueta ***Advanced*** y botón ***Camera Control.***

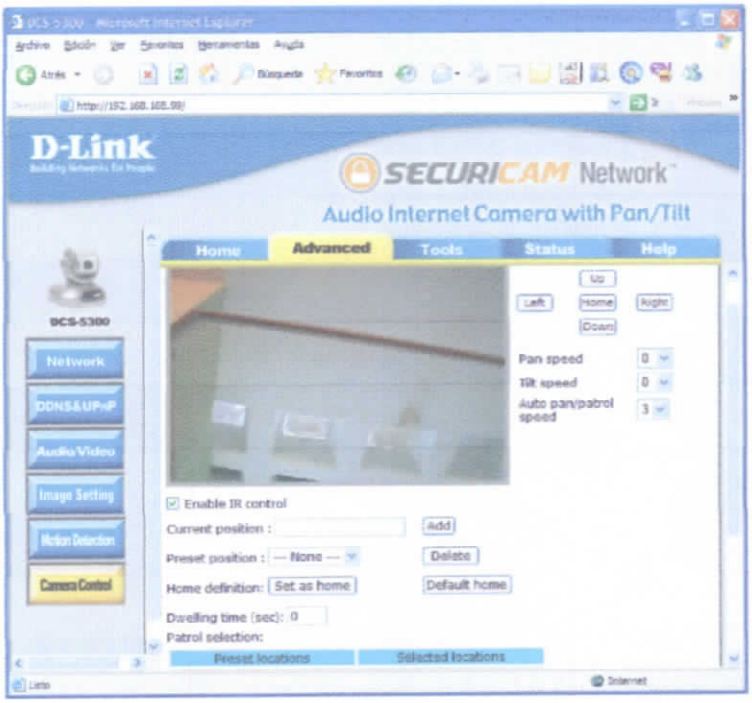


Figura 39: Control de la cámara

Los botones *Up, Down, Left, Right* y *Home*, pueden ser utilizados para el movimiento de la cámara al igual que los botones de la página principal o del control remoto. Las opciones de control de la cámara son:

- **Pan speed**, establece la velocidad del movimiento horizontal en valores desde -5 hasta +5.
- **Tilt speed**, establece la velocidad del movimiento vertical en valores desde -5 hasta +5.
- **Auto pan / patrol speed**, establece la velocidad del movimiento automático horizontal o del patrullaje automático, en valores del 1 al 5.
- **Enable IR control**, esta habilitado por defecto y sirve para habilitar el manejo de la cámara a través del control remoto.
- **Current position**, permite guardar posiciones predeterminadas de la cámara, para lo que se debe mover la cámara hasta una posición deseada, digitar un nombre en el cuadro de texto y hacer clic en *Save*.

- **Preset position**, muestra todas las posiciones almacenadas previamente.
- **Home definition**, fija una posición almacenada como la posición por defecto de la cámara cuando ésta es encendida, o retorna a la posición predeterminada de fábrica.
- **Dwelling time**, establece el tiempo que la cámara se detendrá en cada una de las posiciones predeterminadas.
- **Patrol selection**, permite añadir una posición almacenada. Esto determina a que posiciones se moverá y detendrá la cámara al seleccionar la opción *Auto patrol* de la página principal.

3.4.7.7. Detección de movimiento

La cámara tiene la opción de habilitar la detección de movimiento para realizar diferentes acciones en base a la configuración establecida. Accedemos a estas opciones a través de ***Configuration,*** etiqueta ***Advanced*** y botón ***Motion Detection.***

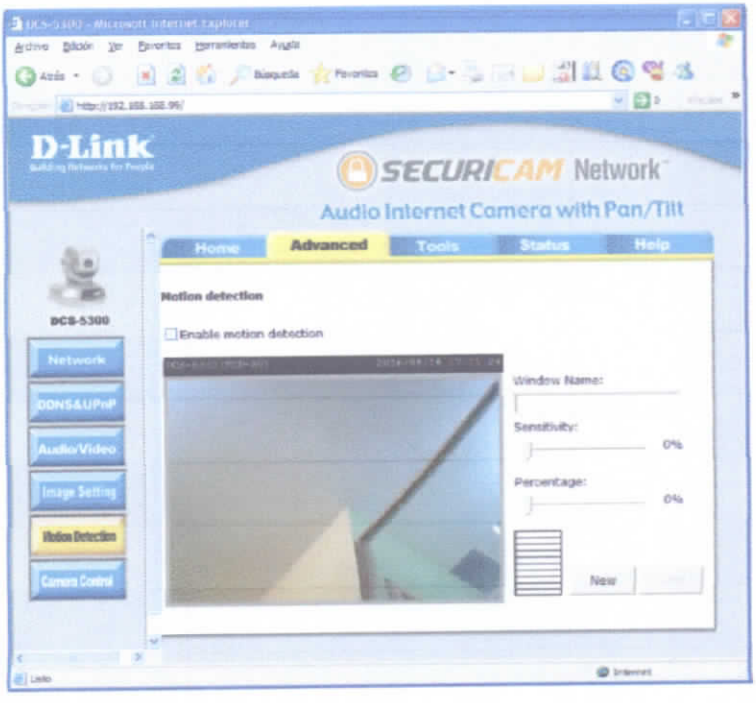


Figura 40: Configuración de detección de movimiento

Las opciones de detección de movimiento son:

- **Enabled motion detection**, habilita la detección de movimiento.

- **New**, añade una nueva ventana para monitorear un área específica. Pueden ser creadas hasta 3 ventanas.
- **Save**, guarda la configuración de la nueva ventana.
- **Window name**, permite escribir un nombre para la ventana creada.
- **Sensitivity**, establece la sensitividad para la detección de movimiento.
- **Percentage**, es recomendable establecer en un nivel bajo. Una alta sensitividad y un porcentaje bajo son recomendables para una óptima detección de movimiento. Un bajo porcentaje significa que el movimiento no debe cubrir toda la ventana para ser detectado, un mínimo movimiento dentro del área de la ventana es fácilmente captado por el sensor.

3.4.7.8. Configuración del sistema

Permite al usuario establecer parámetros como el nombre de la cámara, los indicadores LED y la hora que ésta almacena en su firmware. Se puede acceder a estas opciones a través de ***Configuration,*** etiqueta ***Tools*** y botón ***System.***

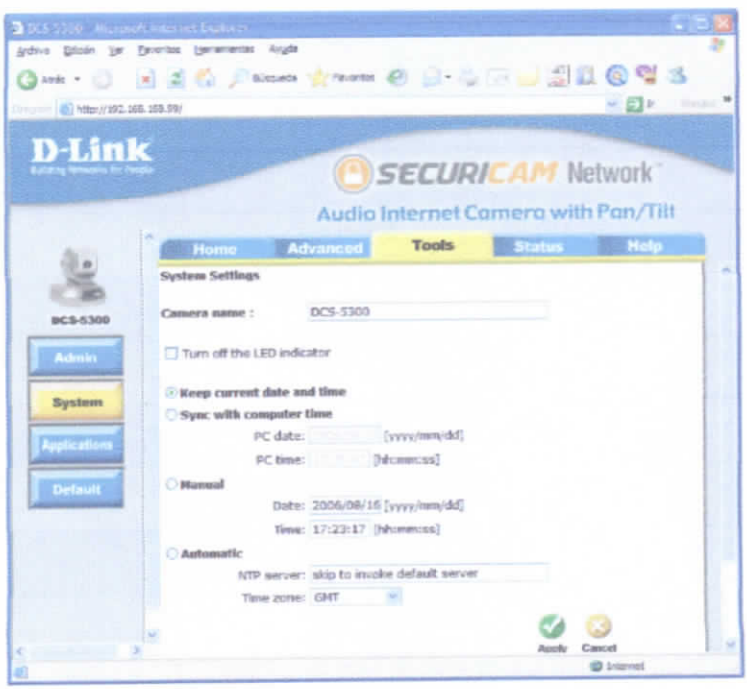


Figura 41: Configuración de hora y fecha

Las opciones que encontramos en detección de movimiento son:

- **Camera name**, almacena el nombre con el cual se va a identificar a la cámara.
- **Turn off the LED indicador**, deshabilita los indicadores LED del frente de la cámara. Es recomendable marcar esta opción para que nadie sepa cuando la cámara está en actividad o no.
- **Keep current date and time**, mantiene la hora y la fecha almacenadas en la cámara. Un reloj interno guarda esta información cuando la cámara se encuentra apagada.
- **Sync with computer time**, sincroniza la fecha y la hora de la cámara con las del computador que está realizando la configuración.
- **Manual**, ajusta la fecha y la hora de la cámara, con los valores ingresados.
- **Automatic**, sincroniza la fecha y la hora con un servidor NTP cuando la cámara es encendida. Si la cámara no encuentra un servidor disponible no se aplica ninguna configuración de tiempo.
- **NTP server**, la dirección IP o nombre de dominio del servidor de tiempo al cual se desea tener acceso.
- **Time zone**, la zona horaria correspondiente al tiempo local.

3.4.8. Instalación de la cámara a través de un router

La instalación detallada anteriormente, nos indica la forma de configurar la cámara dentro de una LAN. Pero ésta puede ser configurada para que perteneciendo a una red LAN, pueda ser vista desde cualquier parte del mundo a través de Internet, lo que se logra accediendo a la cámara mediante un router cableado o inalámbrico.

La instalación se ha dividido en cuatro pasos básicos y fundamentales:

- Asignar una dirección IP local a la cámara.
- Conectarse a la cámara a través del Internet Explorer (recomendado).
- Acceder al router a través del Internet Explorer.
- Abrir el servidor de puertos virtuales del router (habilitar el acceso remoto).

3.4.8.1. Asignar una dirección IP local a la cámara

Se procede con la instalación de la cámara como se describe en pasos anteriores, conectándole a la red local. La cámara tendrá una dirección IP local, para que ésta sea reconocida por el router. Esto ya que se está usando el router para compartir la conexión a Internet entre uno o más computadores. Con lo que se logrará ver la cámara de manera local hasta finalizar la configuración para que sea asequible a través de Internet.

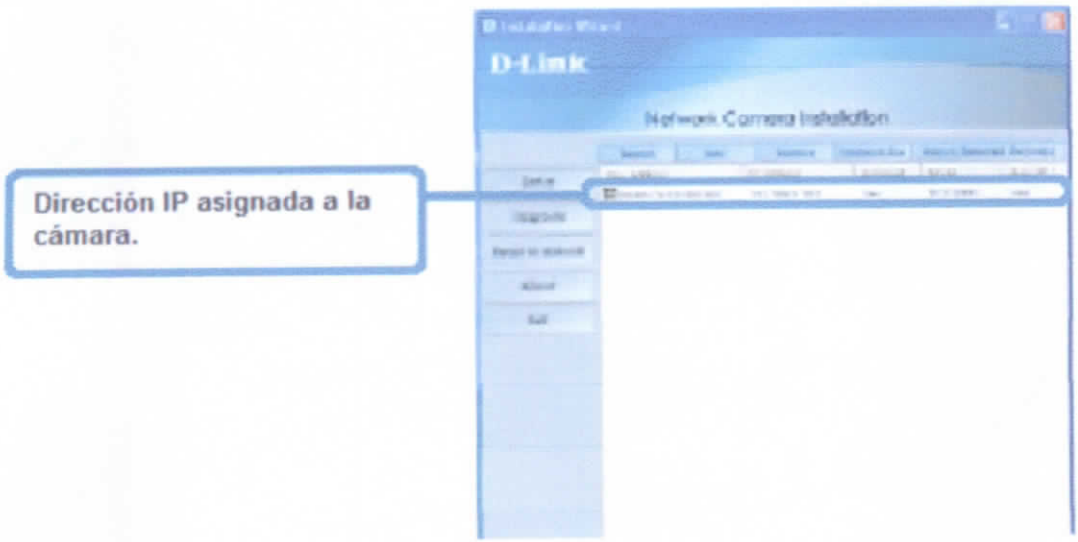


Figura 42: Dirección IP de la cámara

3.4.8.2. Conectarse a la cámara a través del Internet Explorer

Desde el Internet Explorer accedemos a la cámara digitando la dirección IP de ésta (*http://192.168.0.99*), aparecerá la página de inicio visualizando video en vivo transmitido desde la cámara. Se puede ver esta página desde cualquier computador conectado a la red local.

Hacemos clic en el botón ***Configuration***, y bajamos hasta que queden desplegados los puertos de HTTP y del streaming de audio y video. De ser necesario éstos pueden ser cambiados en caso que ya se encuentren en uso por otro dispositivo.

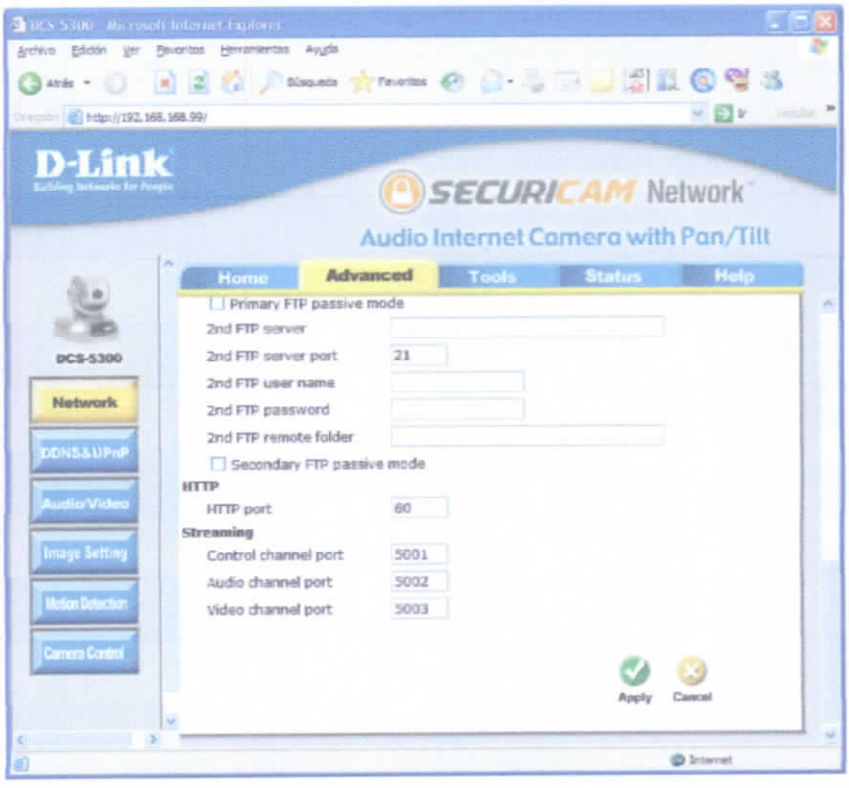


Figura 43: Configuración de puertos

3.4.8.3. Configuración en el router

Si se cuenta con un servicio de Internet DSL o ADSL, se puede tener una dirección IP pública estática o dinámica; en cualquiera de los dos casos, el proceso de configuración es el mismo. La dirección IP pública identifica al router en la red WAN y permite el acceso a Internet.

Es necesario conocer ésta dirección IP, ya sea a través de nuestro proveedor de servicios o accediendo a la página de información de nuestro router a través de un browser; ya que ésta dirección es la que deberá ser escrita en la barra de direcciones del Internet Explorer para visualizar las imágenes de la cámara de manera remota.

Debemos asegurarnos de quitar la marca en la casilla ***Reset IP address at next boot***, antes de digitar la dirección IP; caso contrario la próxima vez que se encienda la cámara, ésta dirección será reemplazada por la IP por defecto de la cámara.

3.4.8.4. Abrir el servidor de puertos virtuales del router

Un router normalmente se conecta a Internet a través de un conjunto de puertos numerados, pero en la mayoría de los casos, éstos se encuentran bloqueados por la misma seguridad del router o por un firewall que éste traiga integrado. Lo necesario es hacer que estos puertos sean accesibles desde Internet.

Para esto debemos configurar el router para que permita que la cámara utilice los puertos para transmitir a través de Internet, algunos routers traen un servidor "virtual" de puertos para realizar estas configuraciones.

Dependiendo el router, se puede acceder a esta configuración de diferente manera, lo importante es establecer los siguientes parámetros:

- Habilitar los protocolos TCP y UDP.
- Ingresar la dirección IP local de la cámara.
- Ingresar el puerto 80 de la cámara en las secciones de puerto público y privado. Si se cambió el número de puerto, se debe ingresar el nuevo valor.
- Repetir el paso anterior para los puertos 5001, 5002 y 5003 para el audio y video de la cámara.

Algunos proveedores de Internet utilizan el puerto 80 para realizar algunos trabajos, por lo que es recomendable averiguar al proveedor si se utiliza este puerto, de ser así debemos cambiar el número de puerto por otro. Además deberemos referirnos al manual de nuestro router para saber la manera correcta de habilitar los puertos y realizar la configuración anteriormente descrita.

Luego de realizar las configuraciones necesarias, se podrá acceder a la cámara tanto desde la red local como desde el Internet. Para esto debemos escribir la dirección IP pública del router, seguida de dos puntos y el número de puerto de la cámara (*http: 200.106.25.2:8080*). Si el puerto de la cámara es el 80, se lo puede omitir de la dirección anterior (*http: 200.106.25.2*).

3.4.9. Desarrollo de la Aplicación

La aplicación realizada es un Sitio Web, el cual permite el acceso hacia la o las cámaras instaladas en la universidad, así como también la administración de las mismas; es decir, la incorporación de nuevas cámaras instaladas para que sean accesibles desde el sitio Web, como la eliminación de aquellas que han sido retiradas o cambiadas de lugar.

Se optó por realizar el sitio de esta manera, ya que al ser uno de los objetivos de la presente disertación la instalación de una cámara IP para vigilancia de las instalaciones y el desarrollo de un sitio Web que permita visualizar la cámara, es necesario que éste cuente con la flexibilidad necesaria para manejar y administrar las cámaras que pueden ser instaladas en el futuro.

Además se cuenta con la facilidad de acceder a las cámaras a través de vínculos en lugar de tener que digitar la dirección IP de la cámara seguida del número de puerto, lo que facilita al acceso al no tener que recordar los números sino simplemente guiarse por la descripción de cada cámara que se presenta en la página correspondiente.

Este sitio fue diseñado utilizando HTML como lenguaje de codificado de páginas Web y PHP como lenguaje de administración de datos, ya que la información tanto de las cámaras como de los usuarios se encuentra almacenada en una base de datos MySQL.

3.4.9.1. Diseño de la Base de Datos

La base de datos del sitio Web denominada "camarabd", está formada por dos tablas: "camaras" y "users", cuya estructura se presenta a continuación:

Tabla "camaras"		
Campo	**Tipo de dato**	**Descripción**
dir_ip	var char(15)	Dirección IP de la cámara
puerto	var char (4)	Puerto HTTP de la cámara
descripción	var char (50)	Información adicional de la cámara, situación, lugar, acceso, etc.

Tabla 10: Estructura de la tabla "camaras"

Tabla "users"		
Campo	**Tipo de dato**	**Descripción**
username	var char(20)	Nombre de usuario para ingresar a la sección de administración.
password	var char (20)	Contraseña correspondiente al nombre de usuario.
nombres	var char (50)	Nombres completos del usuario registrado.

Tabla 11: Estructura de la tabla "users"

Por ser la información totalmente independiente, las tablas no tienen ningún tipo de relación y manejan la información suficiente para el correcto funcionamiento del sitio Web en mención.

3.4.9.2. Diseño del Sitio Web

Para iniciar con el desarrollo del sitio Web, se partió de un esquema de navegación entre páginas, el cual se ilustra a continuación:

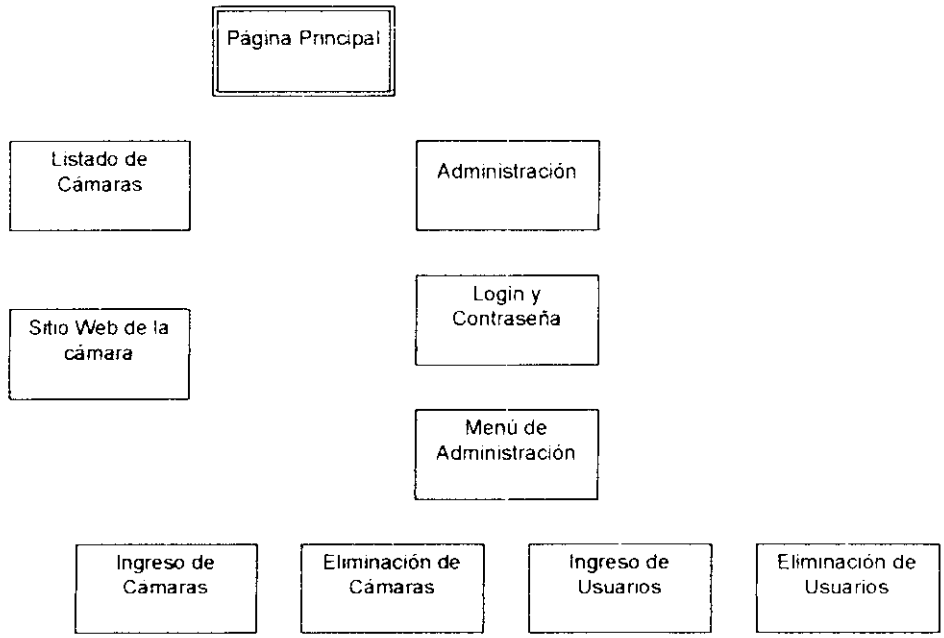


Figura 44: Esquema de navegación del sitio Web

Se utilizó Macromedia Dreamweaver 8, para el diseño y la codificación del sitio tanto en HTML como en PHP, se empezó diseñando la página principal, haciéndola de fácil uso y agradable a la vista del usuario.

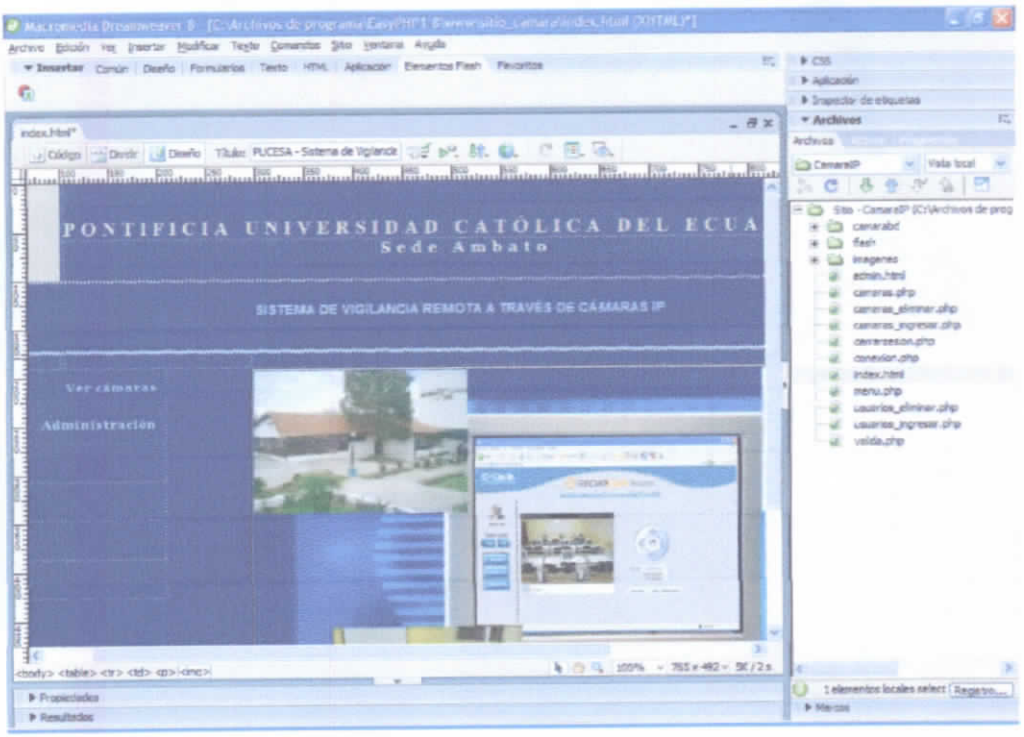


Figura 45: Diseño página principal

Se utilizó una función en PHP para la conexión a la base de datos, la cual es llamada desde cada una de las páginas que necesitan el acceso a los datos, dicha función presenta el siguiente código:

```
<?php
        function conexion()
        {
                if(!($link=mysql_connect("localhost", "root","")))
                {
                        echo "Error conectando a la Base de Datos";
                        exit();
                }
                if(!mysql_select_db("camarabd",$link))
                {
                        echo "Error seleccionando la Base de Datos";
                        exit();
                }
                return $link;
        }
        conexion();
?>
```

Para el desarrollo de la página que presenta el listado de cámaras disponibles, se realiza una consulta a la base de datos, tabla "camaras", y se despliegan en pantalla las cámaras existentes junto a su dirección IP y su puerto correspondiente. Además se crea un hipervínculo directo a cada una de las cámaras.

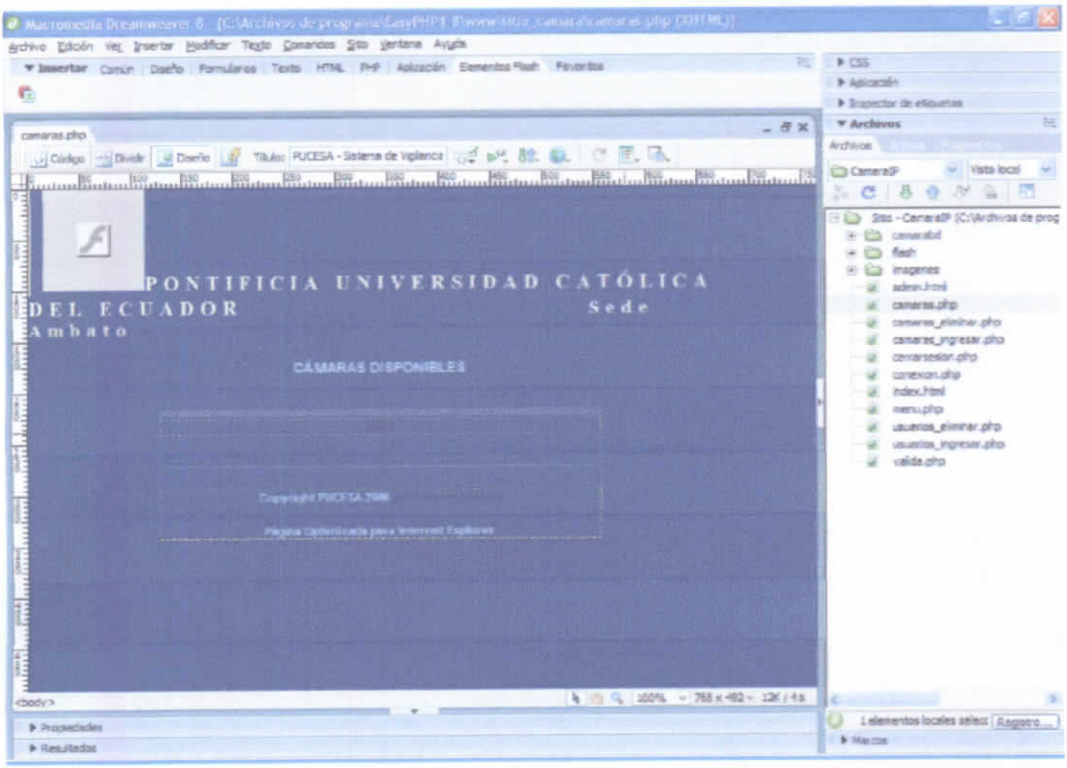


Figura 46: Diseño página "cámaras"

El código de la consulta se presenta a continuación:

```
<?php
        include("conexion.php");
        echo "<form name=form1 method=post action='camaras.php'>";
       $link=conexion();
       $sqlcantidad="SELECT COUNT(*) FROM camaras";
       $rescantidad=mysql_query($sqlcantidad,$link);
       $filacantidad=mysql_fetch_array($rescantidad);
       $cantidad=$filacantidad[0];
       if ($cantidad==0)
       {
         echo "No existe ninguna cámara";
       }
       else
       {
            $sql="SELECT * FROM camaras order by descripcion";
            $result=mysql_query($sql,$link);
            $cont=1;
            while($fila=mysql_fetch_array($result))
       {

            php echo "[$cont]"
            php echo "$fila[2]<br>";
            <a href=" <? echo "http://$fila[0]:$fila[1]" ?> " target="_blank">
            echo "IP:$fila[0]<br>";?> <? echo "<br>Puerto: $fila[1]";
            <a href=" <? echo "http://$fila[0]:$fila[1]" ?> " target="_blank">
            <img src="imagenes/camara.jpg" border="0" align = "center"> </a>
            echo "$fila[2]";
            $cont=$cont+1;
       }
```

```
        echo "</table>";
    } ?>
```

En la parte de administración, se diseño la página con un menú que permita seleccionar ingreso o eliminación de cámaras o usuarios. Para el ingreso de nuevas cámaras o nuevos usuarios de diseñaron sendos formularios para el ingreso de datos, los cuales luego de ser validados, son enviados para ser guardados permanentemente en la base de datos.

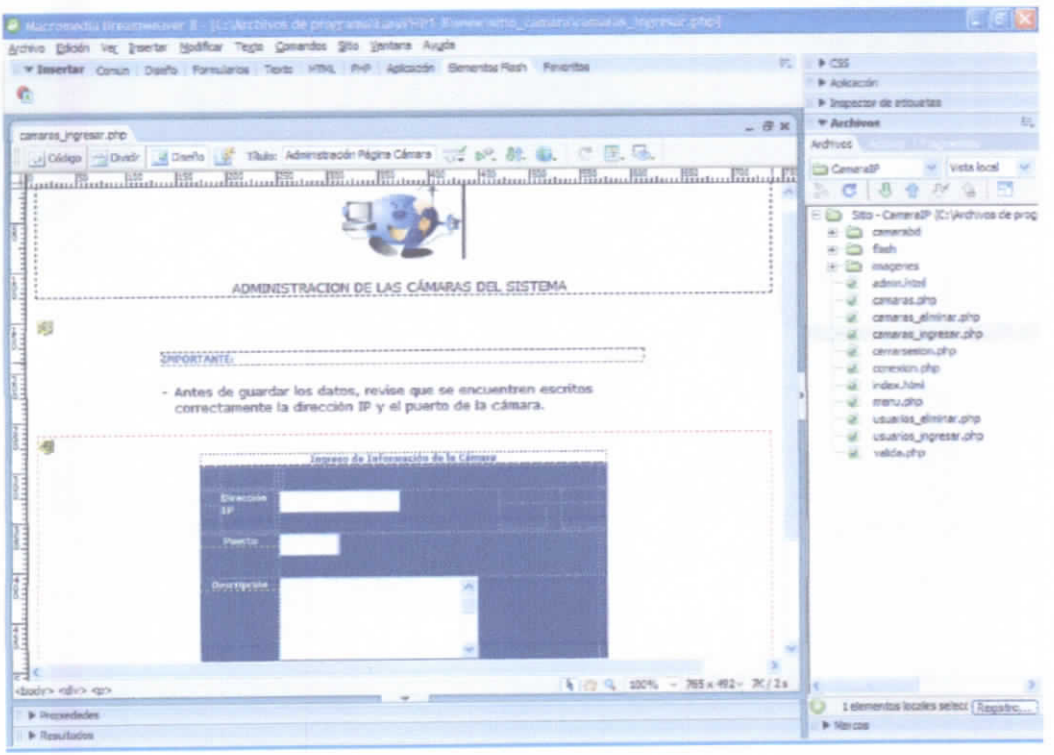


Figura 47: Diseño página "ingreso de cámaras"

```
<?php
if ($activo == 1)
{
        include("conexion.php");
        $link=conexion();
        $sql="INSERT INTO camaras VALUES ('$dir_ip','$puerto','$descripcion')";
        $resultado=mysql_query($sql);
         if ($resultado)
                {
                echo "<script>alert('Información subida correctamente');</script>";
                }
        else
                {
               echo "<script>alert('Error en el ingreso de la información');</script>";
                }
       echo "<script>";
echo self.location='camaras_ingresar.php?dir_ip=0&puerto=0&descripcion=0&activo=0;
      echo "</script>";
```

```
}
?>
```

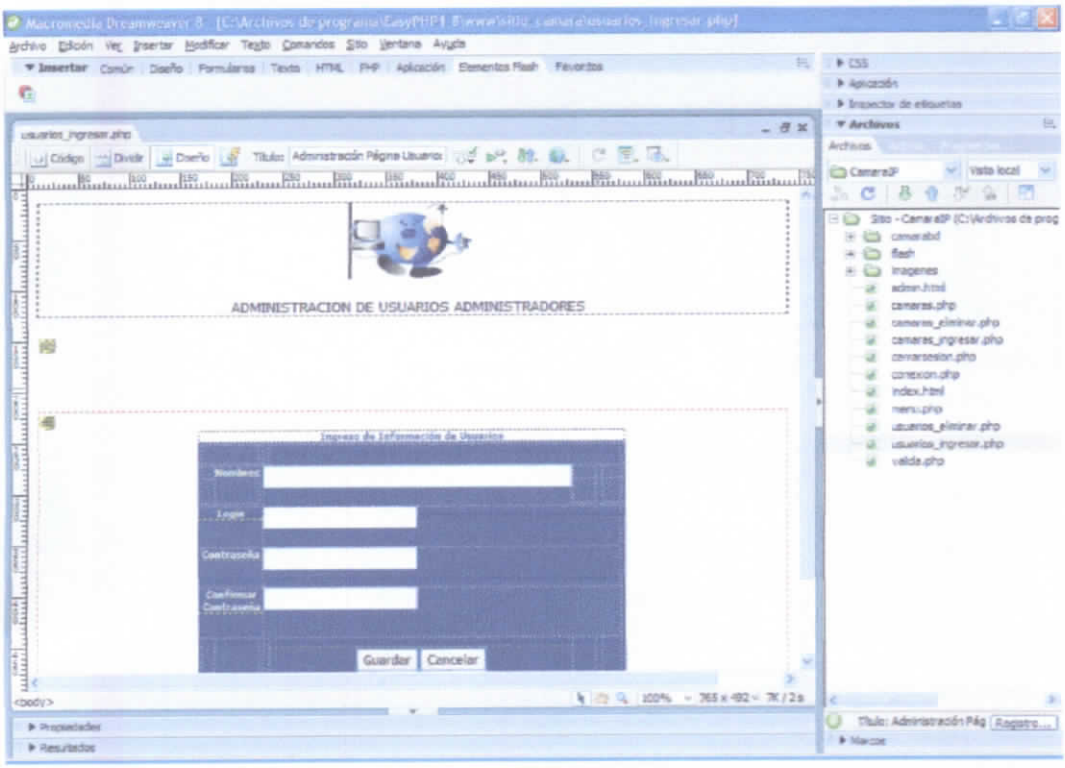


Figura 48: Diseño página "ingreso de usuarios"

```
<?php
if ($activo == 1)
{
    include("conexion.php");
    $link=conexion();
     if ($clave == $clave1)
     {
    $sql="INSERT INTO users VALUES ('$login','$clave','$nombres')";
    $resultado=mysql_query($sql);
    }
     else
    {
    $control=0;
    }
    if ($resultado)
        {
        echo "<script>alert('Información subida correctamente');</script>";
        }
        else
        if ($control == 0)
                {
                echo "<script>alert('Las contraseñas no coinciden');</script>";
                }
        else
                {
        echo "<script>alert('Error en el ingreso de la información');</script>";
        }
       echo "<script>";
```

```
        echo
        self.location='usuarios_ingresar.php?nombres=0&login=0&clave=0&clave1=0&acti
        vo=0"
       echo "</script>"; } ?>
```

Por otra parte para la eliminación de las cámaras o usuarios se diseñaron sendos formularios los cuales presentan un listado de las cámaras o usuarios existentes con una casilla de verificación para que sean seleccionados aquellos que se desean eliminar.

```
<?php
 include("conexion.php");
 echo "<form name=form1 method=post action='camaras_eliminar.php?activo=2'>";
if ($activo == 2) {
   $link=conexion();
  if (isset($_POST['borrar'])) {
       $delArr = $_POST['borrareg'];
       for ($k=0; $k < count($delArr); $k++)
       {
        $sql2 = "select dir_ip from camaras WHERE dir_ip = '" . $delArr[$k] . "'";
        $res2=mysql_query($sql2,$link);
        $fila=mysql_fetch_array($res2);
         $sql = "DELETE FROM camaras WHERE dir_ip = '" . $delArr[$k] . "'";
         $res=mysql_query($sql,$link);
       }
 }
                    echo "<script>";
                    echo "self.location='camaras_eliminar.php?activo=0';";
                    echo "</script>";
}
$link=conexion();
$sqlcantidad="SELECT COUNT(*) FROM camaras";
$rescantidad=mysql_query($sqlcantidad,$link);
$filacantidad=mysql_fetch_array($rescantidad);
$cantidad=$filacantidad[0];
if ($cantidad==0)
{
  echo "No existe ninguna cámara";
}
else
{
       $sql="SELECT * FROM camaras ";
       $result=mysql_query($sql,$link);
       $cont=1;
?>
```

3.4.9.3. Utilización del Sitio Web



Figura 49: Página principal del sitio

La pantalla principal del sitio, nos presenta dos opciones al costado izquierdo de la misma: "Ver cámaras" y "Administración".

La opción "Ver cámaras", nos presenta un listado de las cámaras IP instaladas y disponibles para ser visualizadas en la universidad.

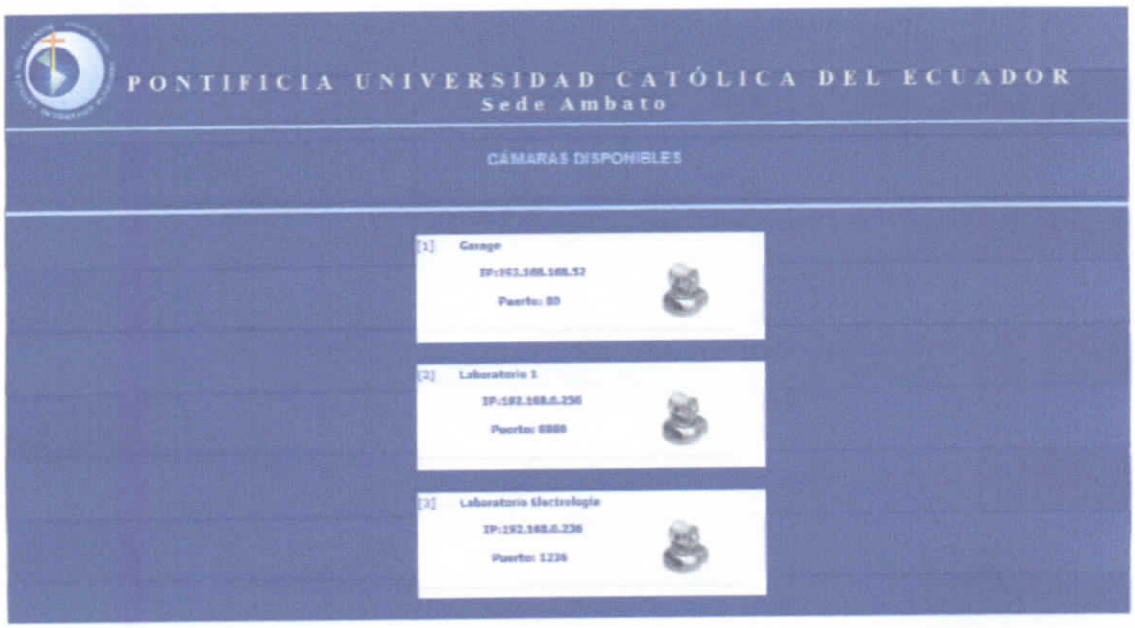


Figura 50: Listado de cámaras

Para acceder a una de ellas, basta con hacer clic en la dirección IP de la misma o en la imagen del costado derecho de cada una. Al hacer esto se nos pedirá introducir el nombre de usuario y la contraseña para el acceso a la cámara, las cuales se encuentran almacenadas en el servidor Web incluido en la propia cámara.

Estos usuarios y contraseñas deberán ser creados por la persona encargada de la administración de las cámaras en la universidad, y deberán ser entregados únicamente a la persona a quien se autorice la visualización.

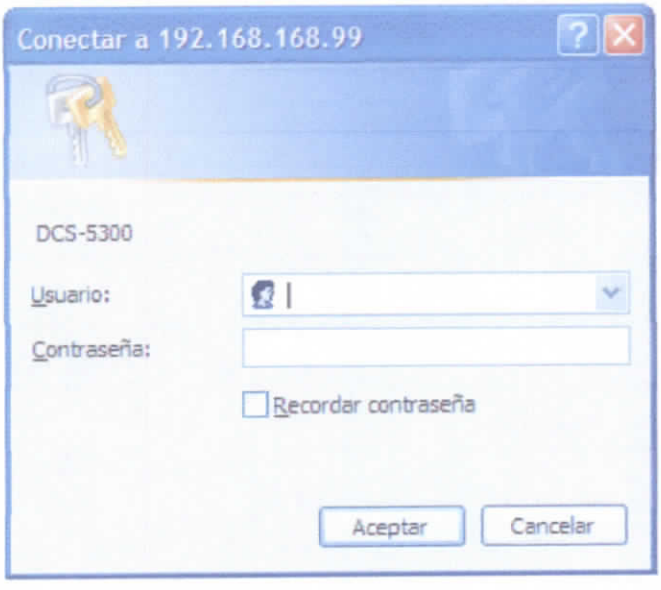


Figura 51: Ingreso de usuario y contraseña

Al introducirlos correctamente, se abrirá una ventana con la dirección IP de la cámara y el número de puerto HTTP de la misma, accediendo de ésta manera a la transmisión que esté realizando en ese momento. Las opciones de manejo y utilización de la cámara van a depender de la marca y modelo de ésta. Para nuestro caso las instrucciones de utilización de la cámara instalada fueron descritas anteriormente.

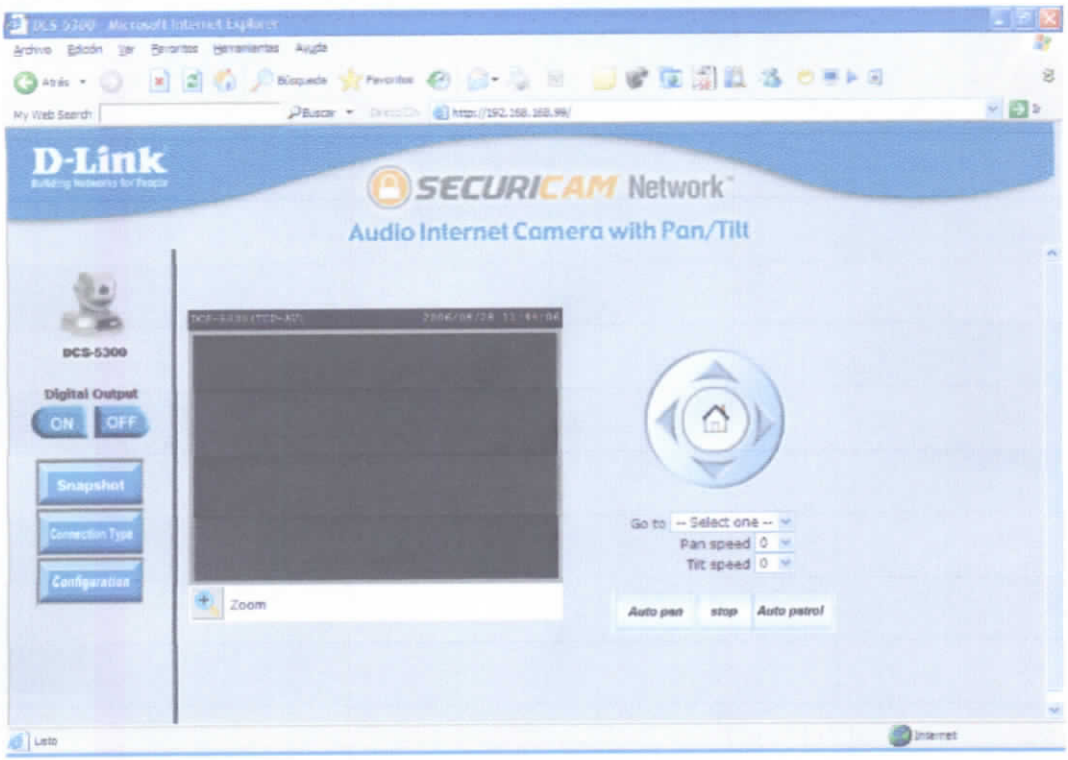


Figura 52: Página de conexión a la cámara

La opción "Administración", nos lleva a una sección en la cual podemos realizar el ingreso y eliminación tanto de cámaras como de usuarios de administración del sitio. Para esto deberemos introducir nuestro nombre de usuario y contraseña de administrador del sitio.



PANEL DE CONTROL

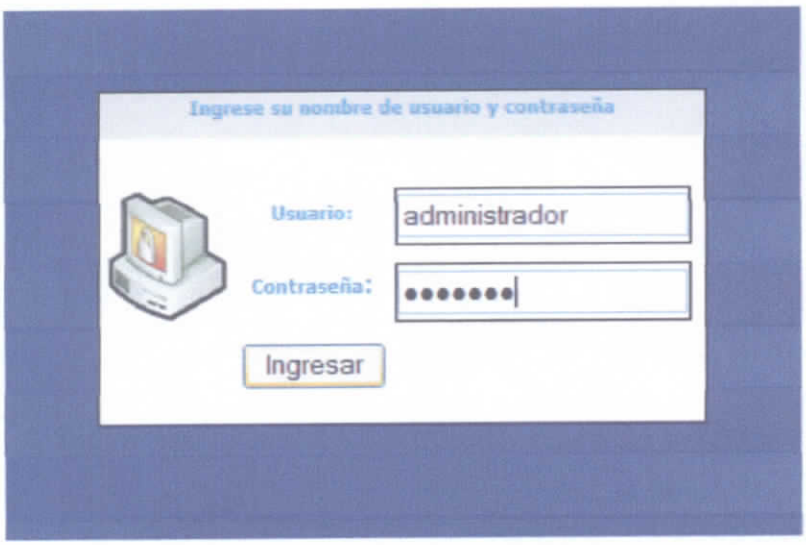


Figura 53: Ingreso a administración del sitio

Una vez ingresados y si son correctos, ingresaremos al menú de opciones de cámaras y de administradores.



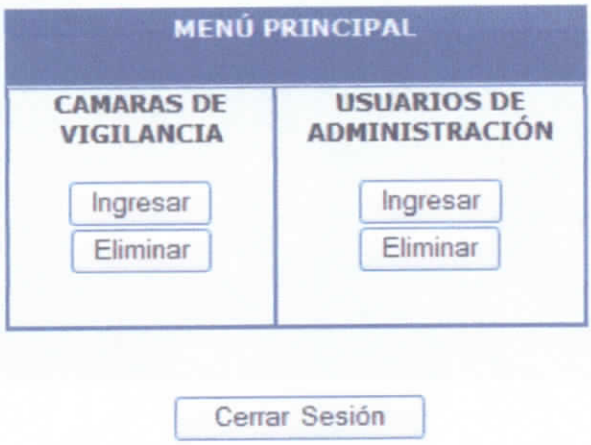


Figura 54: Menú principal de administración

La opción ingresar cámaras, permite al usuario el ingreso de una nueva cámara IP al sitio para que ésta pueda ser vista a través del mismo. Deberemos ingresar la dirección IP de la cámara, su puerto HTTP (que por defecto será el 80 a menos que se haya cambiado) y una descripción que indique básicamente el lugar en el que se encuentra instalada la cámara. Si los datos son correctos procedemos a guardar la información y el sitio nos indicará si ésta fue guardada satisfactoriamente. Se debe tener cuidado al ingresar la dirección IP y el puerto, ya que si éstos son incorrectos, no se tendrá acceso a la cámara. Si la página nos presenta un mensaje de error al guardar la información, esto se debe a que ya existe la dirección IP digitada en la base de datos o que faltó llenar algún campo.



ADMINISTRACION DE LAS CÁMARAS DEL SISTEMA

IMPORTANTE:

- Antes de guardar los datos, revise que se encuentren escritos correctamente la deirección IP y el puerto de la cámara.

Ingreso de Información de la Cámara

Dirección IP: 200.136.256.25

Puerto: 8080

Descripción: Puerta principal de acceso a la universidad

Guardar | Cancelar

Menú | Eliminar

Figura 55: Ingreso de cámaras

La opción eliminar cámaras, permite la eliminación de una o varias cámaras que consten en la base de datos. Para esto seleccionamos la o las cámaras del listado presentado, marcando la casilla de verificación de cada una para luego proceder a eliminar las cámaras marcadas. Cabe anotar que esta acción no se puede deshacer, por lo que si se elimina una cámara accidentalmente, ésta tendrá que ser ingresada nuevamente a través de la opción anterior.



Figura 56: Eliminación de cámaras

Ingresar usuarios, nos permite el ingreso de un nuevo usuario administrador para el sitio Web. Deberemos ingresar los nombres completos del usuario, su nombre de usuario o login, su contraseña de acceso y por seguridad repetir la contraseña. Si los datos son correctos procedemos a guardar la información y el sitio nos indicará si ésta fue guardada satisfactoriamente. Si la página nos presenta un mensaje de error al guardar la información, esto se debe a que ya existe un usuario con el mismo login o que faltó llenar algún campo.



ADMINISTRACION DE USUARIOS ADMINISTRADORES

Ingreso de Información de Usuarios

Nombres: Verónica Valdez Sierra

Login: vvaldez

Contraseña: ●●●●●●●

Confirmar Contraseña: ●●●●●●●

Guardar | Cancelar

Menú | Eliminar

Figura 57: Ingreso de usuarios

Eliminar usuarios, permite la supresión de uno o varios usuarios registrados en la base de datos. Para esto seleccionamos el o los usuarios de la lista desplegada, marcando la casilla de verificación de cada uno para luego proceder a eliminar los usuarios marcados. Esta acción al igual que en el caso anterior no se puede deshacer.

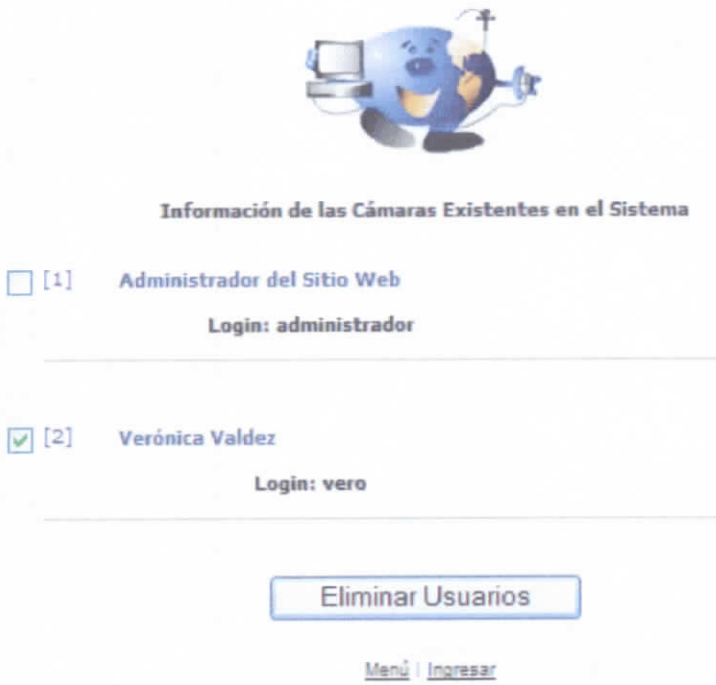


Figura 58: Eliminación de usuarios

Para salir de la sección de administración se debe regresar al menú principal y seleccionar la opción "Cerrar Sesión", con lo cual lo hará de una manera segura. Seguidamente se nos presentará un mensaje indicándonos que la sesión se ha cerrado correctamente para luego salir a la página principal del sitio.

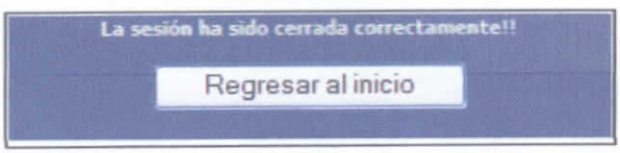


Figura 59: Cierre de sesión

CAPITULO IV

4. VALIDACIÓN Y VERIFICACIÓN DE RESULTADOS

4.1. Conclusiones

- El audio y el video sobre IP son tecnologías a nuestro alcance que tienen muchas aplicaciones prácticas, lamentablemente en nuestro medio son aún desconocidas y su aplicación es casi nula.

- Las cámaras IP brindan un nivel alto y confiable de vigilancia y seguridad gracias a su versatilidad, buena calidad en audio y video, y la transmisión de datos en tiempo real.

- Un mayor ancho de banda permite una mejor transmisión tanto del video como del audio de una cámara IP, logrando que sea casi en tiempo real, con un tiempo mínimo de retraso, especialmente cuando se requiere monitorear varias cámaras a la vez.

- La Pontificia Universidad Católica del Ecuador Sede Ambato, mejorara su sistema de seguridad a través de las cámaras IP, ya que al ser estas monitoreadas desde Internet, se puede contar con una vigilancia total las 24 horas del día, realizada por cualquier persona con acceso permitido y desde cualquier lugar del mundo.

- El valor de un sistema de seguridad IP se encuentra en el software de gestión, así que es una principal característica para valorar un sistema. Sin embargo, dicho software depende en última instancia del rendimiento del sensor de imagen y la calidad de compresión. Hoy en día las cámaras IP todavía tienen una reputación bastante mala para las aplicaciones de seguridad, pero están empezando a aparecer las primeras cámaras IP de calidad profesional.

- La cámara IP instalada en la PUCESA, fue probada en Internet conectándola directamente a la IP pública de la universidad asignada por el ISP, pero al no

ser posible dejarla funcionando de esa manera y al no contar con un router para la salida a Internet, la cámara está funcionando en la red de manera local.

4.2. Recomendaciones

- El centro de cómputo de la universidad, debe asignar un ancho de banda considerable para la transmisión de las imágenes captadas por la cámara IP instalada, para lograr una vigilancia óptima en tiempo real.

- Si las necesidades exigen la grabación del video captado por la cámara instalada, se recomienda utilizar el software "*IP Surveillance*" incluido con la misma, puesto que este permite el monitoreo de hasta 16 cámaras al mismo tiempo, teniendo la opción de captura de imágenes fijas o de video.

- En caso de utilizar el software mencionado anteriormente, se recomienda tomar en cuenta el número de cámaras a monitorear, ya que de este dependen las características del computador que va a ejecutar el software. Los requisitos mínimos para monitorear una cámara, serían:
    - Procesador Intel Pentium III 800MHz o equivalente
    - 128 MB de memoria RAM
    - 10GB de espacio libre en disco
    - Tarjeta de video con aceleración por hardware de al menos 32MB de memoria.

- Se recomienda a la Pontificia Universidad Católica del Ecuador Sede Ambato, instale otras cámaras IP en lugares estratégicos de su campus, para aumentar el nivel de seguridad y mantener vigilados todos sus equipos, oficinas e instalaciones.

- Se recomienda además la adquisición de una IP o de un POOL de 4 IP's públicas para de esta manera poder conectar la cámara permitiendo su salida hacia Internet. En el caso de adquirir el pool, queda abierta la posibilidad de conectar más cámaras en las instalaciones de la universidad.

- La persona encargada de la administración de las cámaras IP, debe crear los usuarios y contraseñas de acceso a las mismas, ya que en la mayoría de cámaras, esta información se almacena en la misma y no en una base de datos externa.

BIBLIOGRAFÍA

LIBROS:

- **LEON,** *"Redes de Comunicación"*, Editorial McGraw Hill, Primera Edición, 2001.
- **McMahon, Richard A.**, *"Introducción a las Redes"*, Editorial Anaya, Primera Edición, 2003.
- **Gutiérrez, Juan Diego**, *"Desarrollo Web con PHP 5 y MySQL"*, Editorial Anaya, Primera Edición, 2005.
- **Roldán, David; Huidobro, José Manuel**, *"Integración de voz y datos: callcenters tecnología y aplicaciones"*, Editorial McGraw Hill, Primera Edición, 2003.
- **Comer, Douglas E.,** *"Internetworking with TCP IP: Principles, Protocols and Architectures"*, Editorial Prentice Hall, Cuarta Edición, 2000.
- **Jonathan Davidson, James Peters, "***Fundamentos de voz sobre IP"*, Editorial Prentice Hall, Primera Edición, 2001.

INTERNET:

- http://www.axis.com/es/documentacion/index.htm
- http://www.mobotix.com/esl_ES/region/index/esl_ES/?URL=technology/how_network_cameras_operate
- www.lsb.es/imagenes/introduccion_aplicacioneswebip.pdf
- www.indigovision.com/files/international/IP-Cameras%20-%20Apr06-Spanish-Revised.pdf
- http://www.domodesk.com/content.asp
- www.siemon.com/la/white_papers/03-08-26-VideoOverIP.asp
- www.i2cat.net/i2cat/servlet/I2CAT.MainServlet?seccio=23_3_2 - 30k
- encuentro.internet2.reuna.cl/programa/tutoriales/video_ip_piquer_arenas.htm
- www.eumed.net/cursecon/ecoinet/seguridad/

GLOSARIO

- **ActiveX**: Nombre asignado a la tecnología OLE 2.0 (Object Linking and Embedding), que es un sistema de objeto distribuido y un protocolo desarrollado por Microsoft.
- **ADSL**: Asymmetric Digital Subscriber Line, consiste en una línea digital de alta velocidad, para acceso a Internet de banda ancha, lo que implica capacidad para transmitir más datos, lo que, a su vez, se traduce en mayor velocidad.
- **ANSI**: American National Standards Institute.
- **Banda Ancha**: Se refiere a la transmisión de datos en el cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión efectiva. En ingeniería de redes este término se utiliza también para los métodos en donde dos o más señales comparten un medio de transmisión.
- **Buffer**: Ubicación de la memoria en una computadora o en un instrumento digital reservada para el almacenamiento temporal de información digital, mientras que está esperando ser procesada.
- **Codec**: Es una abreviatura de *Codificador-Decodificador*. Es una especificación implementada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos o una señal. Estos pueden codificar el flujo o la señal y recuperarlo del mismo modo para la reproducción o la manipulación en un formato más apropiado para estas operaciones.
- **Demodular**: Opuesto a modulación. Consiste en recuperar la información transportada por una onda portadora, que en el extremo transmisor había sido modulada con dicha información.
- **DHCP**: Dinamic Host Configuration Protocol o Protocolo de Configuración Dinámica de Servidores. Protocolo en el que un servidor asigna dinámicamente los parámetros de configuración y conexión a las estaciones de una red.
- **DSL**: Digital Subscriber Line, es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital sobre línea de abonado de la red telefónica local como: ADSL, ADSL2, ADSL2+, etc.
- **Ethernet**: Nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos que define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos.

- **FTP**: File Transfer Protocol.
- **Gateway**: Un gateway es una puerta de enlace; es decir, un nodo en una red informática que sirve de punto de acceso a otra red.
- **Host**: Se refiere a un computador conectado en una red, el cual está identificado por un nombre único.
- **HTTP**: HyperText Transfer Protocol.
- **IP**: Internet Protocol.
- **IRC**: Internet Relay Chat, es un protocolo de comunicación en tiempo real basado en texto, que permite debates en grupo o entre dos personas y que está clasificado dentro de la mensajería instantánea. Las conversaciones se desarrollan en los llamados canales de IRC, designados por nombres que habitualmente comienzan con el caracter # o &. IRC es un sistema de charlas ampliamente utilizado por personas de todo el mundo.
- **ISP**: Internet Service Provider o Proveedor de Servicios de Internet.
- **Kbps**: Kilobit por segundo, utilizada para medir la velocidad de transmisión en un medio.
- **Modular**: Utilizar técnicas para transportar información sobre una onda portadora, típicamente una onda senoidal. Básicamente, consiste en hacer que un parámetro de la onda portadora cambie de valor de acuerdo con las variaciones de la señal moduladora, que es la información que queremos transmitir.
- **Mbps**: Megabit por segundo, utilizada para medir la velocidad de transmisión en un medio.
- **Multiplexación**: Término que indica que un dispositivo puede recibir varias entradas y transmitirlas por un medio de transmisión compartido. Para ello lo que hace es dividir el medio de transmisión en múltiples canales, para que varios nodos puedan comunicarse al mismo tiempo.
- **PAN**: Movimiento horizontal realizado por una video cámara.
- **Plug and play**: Es una tecnología que permite a un dispositivo informático ser conectado a un computador sin tener que configurar jumpers ni proporcionar parámetros a sus controladores. Para que eso sea posible, el sistema operativo con el que funciona el computador debe tener soporte para dicho dispositivo.
- **Relé**: Término utilizado para un interruptor automático controlado por corriente eléctrica. Básicamente consta de una bobina a través de la cual circula corriente

eléctrica, la misma que genera un campo magnético el cual atrae o separa pequeños contactos que actúan como interruptor de otro dispositivo eléctrico o electrónico.

- **SMTP**: Simple Mail Transfer Protocol.
- **Snapshot**: Imagen fija capturada de una cámara de video.
- **TCP**: Transfer Control Protocol.
- **TILT**: Movimiento vertical realizado por una video cámara.
- **UDP**: User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.
- **VGA**: Video Graphics Array, es una norma de visualización de gráficos para computadores creada en 1987 por IBM. Luego se vinieron creando mejoras del estándar VGA denominadas SVGA (Super VGA).
- **Wireless**: Término inglés utilizado para indicar que algún dispositivo es inalámbrico.

