INSTITUTO POLITECNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERIA MECANICA Y ELECTRICA
UNIDAD PROFESIONAL "ADOLFO LOPEZ MATEOS"

"IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD VÍA INTERNET"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMUNICACIONES Y ELECTRÓNICA

PRESENTAN:
VERA AURORA CUAQUENTZI CRUZ
EDSON EDUARDO LECHUGA BARRIENTOS
MIGUEL ANGEL NIETO PATLÁN

ASESORES:

ING. HECTOR PIÑA CANALES
M. EN C. ROBERTO GALICIA GALICIA

MEXICO, D.F. 2008

AGRADECIMIENTOS

Doy gracias a Dios por permitirme concluir un ciclo de mi vida satisfactoriamente y haberme permitido tener tantas alegrías hasta el día de hoy.

Esta tesis representa la conclusión de una etapa de mi vida y el comienzo de una nueva. Es por ello que se la dedico con mucho cariño a mis padres Delia y Aarón a los cuales les agradezco su apoyo incondicional, su guía en este camino, la confianza que tuvieron en mi y todo el amor que recibo de ellos y agradezco a ellos por haberme dado una carrera para mi futuro.

A mi hermana Ale a la que quiero mucho y siempre conté con ella para todo y está a mi lado en los buenos y malos momentos.

A Edson porque fue un gran apoyo para mí en los últimos pasos para concluir esta etapa, gracias por estar conmigo, por compartir tantas cosas y cuidarme siempre.

Le doy las gracias a mi director de tesis el Ing. Héctor Piña por su aliento y apoyo para concluir este proyecto, al iniciador de este trabajo el M. en C. Jaime Moreno le agradezco su confianza en nosotros y todo el apoyo que recibimos y al asesor metodológico M. en C. Roberto Galicia por su guía en el proyecto.

Gracias a todos lo que directa e indirectamente me apoyaron y estuvieron conmigo y que no mencioné, se que son parte importante en esta etapa que estoy concluyendo y cada uno de ustedes aportaron un granito con su apoyo, amistad, comprensión y de mas.

Vera Aurora Cuaquentzi Cruz

Gracias:
Primeramente doy gracias a Dios por concederme la enorme dicha de llegar a este momento tan importante para mí, en el cual he concluido una meta más en mi vida y sobre todo gracias por permitirme compartirlo con todos mis seres queridos.

A mis padres Susana y Eduardo por haber confiado en mi y por brindarme la oportunidad de estudiar una carrera, por su cariño, comprensión y apoyo sin condiciones ni medida en todo momento, gracias por sus sabios consejos, por compartir mis alegrías y mis tristezas, por esa palabra de aliento que siempre tuvieron en los momentos más difíciles y por muchas cosas más que no terminaría de mencionar. A mis hermanas Nancy y Yazmín por haberme apoyado siempre que lo necesité, siempre fueron mi inspiración y motivación para seguir adelante a lo largo de este camino.

A Aurora por compartir conmigo estos momentos, por su cariño y apoyo incondicional, eres una parte muy importante en la culminación de esta etapa de mi vida.

A mis asesores el M. en C. Jaime Moreno por la confianza depositada en nosotros para la realización de este proyecto, por su amistad, paciencia, consejos y apoyo, gracias al Ing. Héctor Piña, sus conocimientos y su apoyo fueron fundamentales para la conclusión de esta trabajo y gracias al M. en C. Roberto Galicia por sus consejos durante la realización de esta tesis.

Gracias a todos mis compañeros y amigos por su ayuda y por su apoyo siempre que lo necesité, por compartir tantas experiencias conmigo, pero sobre todo por hacer más placentera esta etapa tan importante de mi vida.

Edson Eduardo Lechuga Barrientos

Gracias:

A mi madre por haber estado siempre pendiente de que no me faltara nada, desde que te levantas hasta que te duermes, gracias mamá por todo tu amor y apoyo que siempre me impulsaron a llegar hasta donde hoy me encuentro.

A mi padre por haberme apoyado tanto económicamente como moralmente, siempre fuiste la palabra exacta cuando tuve algún problema, me diste todo lo que un padre le puede dar a un hijo.

A Erik por también ser ese ejemplo que me impulso y motivo cada día para seguir adelante, por la ayuda que me brindaste y los consejos que me diste.

A Alejandro por brindarme su apoyo y haber estado al pendiente de mi desarrollo en todo éste tiempo.

A Jessica por estar conmigo en la etapa más difícil de mi carrera y no dejarme bajar los brazos, por apoyarme en los momentos en que sentía desfallecer, gracias amor.

A mis profesores por brindarme sus conocimientos y haber formado en mí un profesionista.

A mis amigos y a todas aquellas personas que en algún momento me ayudaron y apoyaron en mi desarrollo profesional y personal.

Pero principalmente a Dios por darme todo lo que tengo en la vida.

Miguel Ángel Nieto Patlán

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

OBJETIVOS

Objetivo General

Diseñar un sistema de video vigilancia para brindar un servicio de seguridad a los laboratorios del área de computación de la ESIME Zacatenco.

Objetivos Particulares.

- Conocer el entorno de los sistemas de video vigilancia en el país así como también dentro del Instituto.
- Analizar la evolución de los sistemas de video seguridad, el Modelo de referencia OSI, protocolos UTP, TCP y USB, los cuales sustenta la parte teórica.
- Resaltar las características de las herramientas que se utilizarán para desarrollar el Sistema propuesto.
- Configurar el sistema operativo Windows Server 2003 además de Windows Media Player versión 9.
- Crear una página WEB para transmitir video a través de Internet.

RESUMEN

El alcance de este proyecto es amplio ya que hoy en día la adquisición de este tipo de sistemas es muy rentable y de gran utilidad para los usuarios ya que en una casa, en una empresa o en cualquier otro lugar es necesario proteger bienes y/o intereses.
La idea de realizar el proyecto surge con el fin de dar una mayor protección a los recursos de la escuela en el área de computación ICE beneficiando con ello a la misma institución y principalmente a los alumnos.

En el capítulo 1 se dan a conocer los sistemas de vídeo vigilancia que existen en la actualidad en México, describiendo las características de dichos sistemas, partiendo de lo general a lo particular, estos es, se describen los sistemas de vídeo vigilancia en distintos lugares públicos y finalmente en el Instituto Politécnico Nacional. Además se hace énfasis al problema de inseguridad que se pretende resolver con este tipo de sistemas.

En el capítulo 2 se explica como han evolucionado los sistemas de vídeo vigilancia, además se hace mención sobre la teoría que sustenta la realización del proyecto, entre los puntos que se describen, está el modelo OSI y los diferentes protocolos de comunicación que permiten que se establezca un intercambio de información entre el servidor y los usuarios, el propósito de éste capítulo es que el usuario comprenda la manera en que funciona el sistema de seguridad.

En el capítulo 3 se describen las características del hardware y software utilizados para la implementación del sistema de vídeo vigilancia. Se explica también el funcionamiento de forma general de las herramientas con las que se llevará a cabo dicho proyecto, entre las cuales se encuentran el sistema operativo Windows Server 2003, los Servicios de Windows Media, el codificador de Windows Media, Dreamweaver y la cámara web.

Dentro del capítulo 4 se explica de manera detallada como funciona cada una de las herramientas empleadas en la configuración del servidor, además se realizan

observaciones muy útiles para el óptimo desempeño del sistema y para la corrección de posibles fallas que se puedan presentar a futuro.

El capítulo 5 contiene la propuesta de implementación del sistema de seguridad, se explica en forma particular como se utilizaron las herramientas, tanto de hardware como de software, en forma conjunta para la implementación del sistema de vídeo vigilancia, también se presenta en un plano la manera en que se propone sean colocadas las cámaras en los laboratorios de computación.

INTRODUCCIÓN

El desarrollo de este proyecto está pensado para resolver los problemas relacionados con la seguridad de cualquier lugar utilizando herramientas tales como las cámaras e Internet. A través de dichas herramientas es posible contar con un sistema de vídeo vigilancia que permita el acceso al mismo utilizando cualquier PC con conexión a Internet. Actualmente es una necesidad contar con este tipo de sistemas que permitan la seguridad, la vigilancia y la monitorización remota.

La vigilancia con cámaras IP o cámaras web permitirán capturar y enviar vídeo en directo a través de una red, como una LAN, intranet o Internet, y admitirá a usuarios autorizados ver y/o gestionar la cámara con un navegador Web a través de un software de captura de vídeo en cualquier equipo local o remoto conectado a una red. Lo cual permitirá a usuarios autorizados que se encuentren en distintas ubicaciones acceder simultáneamente a las imágenes captadas por la misma cámara de red.

Lo que se busca es controlar y disminuir el robo de los equipos en los laboratorios de computación en la ESIME Zacatenco mediante el monitoreo en dichos lugares con cámaras transmitiendo el vídeo en tiempo real a través de una página WEB.

La propuesta de este proyecto surge por la necesidad de implementar un sistema de protección en dicha institución debido a los saqueos continuos de material, componentes de computadoras, proyectores y equipos completos de cómputo que se tiene en las diferentes áreas de la escuela y con el fin de beneficiar a la escuela, a sus alumnos y a todo el personal que labora en ella a demás de que en la ESIME Zacatenco nunca se ha contado con un sistema de monitoreo en su plantel que proporcione seguridad en sus diferentes laboratorios enfocándose el proyecto específicamente a las áreas de los laboratorios de computación de ICE.

La gama de aplicaciones y el alcance de este proyecto son muy amplios debido a que hoy en día la adquisición de este tipo de sistemas es muy rentable y de gran utilidad para los usuarios ya que en una casa, en una empresa o en cualquier otro lugar es necesario proteger bienes y/o intereses.

CAPÍTULO 1

VÍDEO VIGILANCIA EN LA ACTUALIDAD

1.1 SEGURIDAD EN LA SOCIEDAD

La inseguridad se entiende como la consecuencia de todo desorden social y económico: es argumento político, ético, económico, moral, y cultural para justificar la intervención de los poderes gubernamentales, mediáticos y financieros, en la esfera del espacio público y de la vida privada. Se tiene actualmente en la sociedad un monstruo llamado *inseguridad*, que transita entre lo paranoico imaginario y lo fáctico.

La inseguridad no es producida necesariamente por la falta de seguridad. La inseguridad es un problema sistémico e integral más que un problema de falta de vigilancia.

La seguridad en nuestros días recae en gran medida en la vigilancia pública, privada y la tele-vigilancia que se realiza tanto en algunos lugares públicos como en forma externa e interna de muchas empresas. En el caso de la vídeo vigilancia esta puede ser llevada a cabo mediante un circuito cerrado de televisión (CCTV), programas de reconocimiento facial, sensores de proximidad, cámaras infrarrojas, cámaras robots, secuenciadores de vídeo, cámaras de intemperie con radiofrecuencia, cámaras de baja iluminación con cobertura de hasta 120 m. en total obscuridad, de interiores visibles u ocultas, cámaras acuáticas, etcétera.

Este tipo de sistemas de seguridad ha sido implementado en cajeros automáticos, transmisiones telemáticas, en tiendas departamentales, centros comerciales y de entretenimiento, bancos, escuelas, cárceles, instituciones públicas y privadas, calles, plazas, carreteras, tráfico vehicular, seguridad infantil, clima, medio ambiente, hospitales empresas, casas y puede ser implementado en "cualquier espacio que requiera vigilancia".

Debido al aumento de la inseguridad, la sociedad se ha visto en la necesidad de adquirir servicios que les brinden una mayor protección, y uno de los más requeridos es el sistema a través de cámaras de vídeo que se ha ido desarrollando a pasos agigantados comenzando con los circuitos cerrados de televisión hasta las cámaras IP (Protocolo de Internet) en nuestros días.

Los sistemas de vigilancia por vídeo se están volviendo más comunes en los edificios de oficinas, estructuras externas, escuelas e incluso en las calles. La vigilancia se ha convertido en un componente integral de los métodos de control de acceso enriquecidos con sistemas biométricos y sistemas de rastreo.

En la actualidad han surgido y crecido diversas empresas que se especializan en el monitoreo a través de cámaras a las que se puede acceder desde cualquier parte del mundo. Dichas empresas tienen como propósito principal ofrecer seguridad con facilidad de acceso y manejo sin importar la distancia ni el tiempo.

1.2 SISTEMAS DE SEGURIDAD EN LUGARES PÚBLICOS

Una de las prioridades en los lugares públicos es mantener el orden y la seguridad para el beneficio de la población es por ello que se ha comenzado a implementar equipos de vídeo vigilancia en muchos de estos lugares.

1.2.1 Vídeo vigilancia en el metro del D.F.

Hoy en día el Metro es uno de los medios de transporte más utilizados, si no el de mayor demanda entre la población capitalina, así como también un lugar con alto índice de delincuencia en sus diversas estaciones de cada línea. Por tal motivo el gobierno está trabajando en la prevención y control de dicho problema y así proteger a sus usuarios.

En la línea 1, operan 150 cámaras de vigilancia en las estaciones Merced, Candelaria, Pino Suárez, Salto del Agua, Balderas, andenes de Pantitlán y otras funcionando en la línea 1 que va de Pantitlán a Observatorio, Figura 1.1.

Figura 1.1.- Vigilancia en el Sistema de Transporte Colectivo Metro

El Sistema de Transporte Colectivo Metro instalará próximamente la infraestructura para colocar 2500 cámaras que integrarán el sistema de vídeo vigilancia en las estaciones de mayor afluencia. Además se tiene el proyecto para la instalación del sistema de fibra óptica para la colocación de las cámaras en el interior de las instalaciones del transporte subterráneo. Para ello se requiere que en varias de las estaciones del Metro se realice la instalación del cableado de fibra óptica para colocar el equipo y transportar la imagen. Además de las 150 que ya están instaladas y funcionando en la línea 1 que corre de Pantitlán a Observatorio con lo que sumarán un total de 2650 equipos de video vigilancia.

El sistema de vídeo vigilancia del Metro estará conectado al centro de mando “C4” de la Secretaría de Seguridad Pública para atender situaciones de emergencia.

Las aspiraciones que se tienen son que las cámaras cuenten con un micrófono para mantener comunicación directa con los usuarios, e incluso, hacerles señalamientos al presentarse alguna situación de peligro para los usuarios o cuando realicen actividades de graffiti, desórdenes y otros.

1.3 GUARDERÍAS CON VIGILANCIA

El ritmo de vida actual es realmente frenético y no deja tiempo a casi nada. Y es muy difícil para los padres cuidar a los hijos, es por ello que una solución a este problema en la actualidad es poder vigilar a sus hijos pequeños a distancia. Con la tecnología que se ha desarrollado rápidamente en nuestros días los padres pueden ver a sus hijos en las guarderías a través de la vídeo vigilancia en Internet y pueden dejar con más confianza en manos del personal de guarderías y jardines de infancia el cuidado de sus hijos mientras ellos trabajan o están en el hogar y en cualquier momento poder observar a sus hijos desde sus casas o trabajo. La Figura 1.2 muestra el funcionamiento de los sistemas de vigilancia en guarderías.

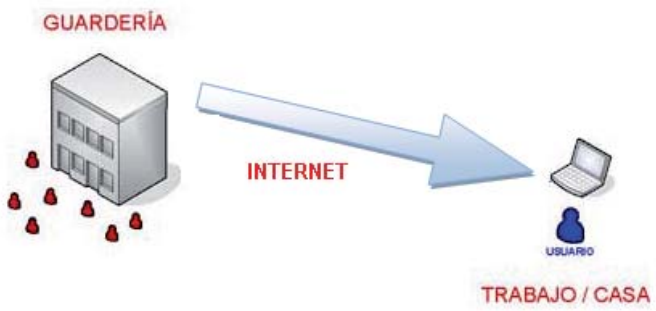

Figura 1.2.- Vigilancia en guarderías

El ISSSTE (Instituto de Seguridad Social al Servicio de los Trabajadores del Estado) actualmente cuenta con catorce guarderías las cuales atienden a niños de dos meses a seis años de edad. Dicho instituto recibirá una inversión para el mantenimiento de las guarderías, y parte de dicha inversión será utilizado para la instalación de un sistema de vídeo vigilancia.

1.3.1 Servicios de E-guarderías

La empresa E-guarderías se dedica a la vídeo vigilancia enfocada a guarderías y jardines de infancia. Con este sistema de tele vigilancia por Internet los padres pueden vigilar y observar a sus hijos de una manera cómoda, sencilla y segura.

Para poder observar a sus hijos por Internet en una guardería que tenga instalada e-guardería, los padres o familiares sólo tienen que disponer de una conexión a Internet y de una cuenta de usuario válida.

Dicha empresa ofrece servicios a los padres tales como:

- Observar las instalaciones de la guardería.
- Observar el comportamiento de su hijo.
- Ver de primera mano la atención que recibe su hijo.
- Ver como interactúa su hijo con los demás niños.

La empresa E-guarderías realiza la instalación de las diferentes cámaras y equipamiento adicional que se utilizará para visualizar diferentes partes del edificio tales como:

- Aulas.
- Entrada.
- Jardín.
- Patio de juegos.

1.4 SISTEMAS DE SEGURIDAD DENTRO DE INSTITUCIONES EDUCATIVAS

1.4.1 Sistema de vídeo vigilancia IP en la construcción del edificio 18 en la U.N.A.M.

Con el fin de que la comunidad de la Universidad Nacional Autónoma de México pueda observar el avance de las obras de la construcción del edificio 18, se puso en operación una página Web comunicada con una cámara robótica de vídeo IP. Esta página Web puede ser consultada desde cualquier computadora de escritorio, PDA o laptop conectada a la red del Instituto a través de la red cableada o la red inalámbrica. Igualmente se puede consultar desde cualquier lugar con servicio de Internet.

La cámara se conecta directamente a la red de datos y utiliza los protocolos de comunicación de Internet (TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet) para transmitir el vídeo a un servidor, que a su vez es consultado a través de una página Web. La cámara también ofrece rutas programadas, paradas predefinidas para realizar acercamiento *(zoom)* hacia algún detalle en particular que se requiera revisar, fotografiar o grabar en vídeo; ofrece visión nocturna y generación de alarmas con la ayuda de sensores, puede girar en su eje vertical y también en el horizontal y maneja diferentes algoritmos de compresión para usar un menor ancho de banda de la red de datos.

Esta solución es muy flexible y económica, a diferencia de los sistemas con cámaras analógicas y cable coaxial, ya que este tipo de cámaras IP pueden ser conectadas en cualquier punto de una red de datos tanto alámbrica como inalámbrica y pueden ser controladas y administradas desde cualquier punto donde exista servicio de Internet. En las Figuras 1.3 y 1.4 muestran los medios por los cuales se tiene acceso a este sistema de vídeo vigilancia, y la Figura 1.5 muestra la cámara IP que esta vigilando.

Figura 1.3.- Laptop conectada a la Red

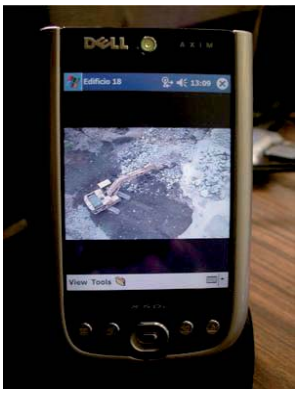

Figura 1.4.- PDA conectada a la red

Figura 1.5.- Cámara IP

1.4.2 Cámaras de vídeo en escuelas del D.F.

El Instituto Politécnico Nacional, la UNAM y diferentes empresas, invertirán recursos para comprar cámaras de vídeo vigilancia que serán instaladas en escuelas públicas del DF, de las cuales se incluyen desde el nivel básico hasta bachillerato. Dicho proyecto consiste en implementar una red de vigilancia con el objetivo de cubrir la vigilancia en las inmediaciones de planteles educativos, verificar los problemas de narcomenudeo, maltrato y abuso contra los estudiantes.

Los planteles educativos, primarias, secundarias, bachillerato, y nivel superior contarán con este sistema de vídeo vigilancia que en el 2008 se iniciará con una nueva etapa de la instalación de esas cámaras de vídeo con el propósito de tener más vigilancia en todas estas áreas.

1.5 SISTEMAS DE SEGURIDAD EN EL IPN

En la mayoría de las escuelas, ya sea del nivel medio superior o del nivel superior y áreas administrativas del Instituto Politécnico Nacional no se cuenta en la actualidad con este tipo de sistemas de vídeo vigilancia que ofrezcan seguridad a la población estudiantil, docente, personal administrativo y de los bienes materiales.

Existen otras áreas del Instituto, tal como el edificio inteligente donde se cuenta con equipo de seguridad conformado por cámaras de vídeo. Sin embargo debido al problema de inseguridad que se tiene, tanto interna como externamente se ha solicitado apoyo a diferentes instituciones gubernamentales para instalar este tipo de equipos en todas sus unidades.

CAPÍTULO 2

MARCO TEÓRICO

2.1 EVOLUCIÓN DE LOS SISTEMAS DE VÍDEO SEGURIDAD

2.1.1 Sistemas circuitos cerrados de televisión análogos de coaxial y fibra óptica

El origen de CCTV (*Circuito Cerrado de Televisión*) se remonta a los años 50's del siglo pasado, con grandes avances en los años 70's, concretamente a través de los sistemas de grabación análoga y cámaras de estado sólido se impulsaron a las tecnologías dedicadas a la seguridad, vigilancia y control. Tal como se muestra en la Figura 2.1, el sistema tradicional usaba cable coaxial de 75 Ohms. Varias cámaras se conectaban por medio de este cableado y se conectaban a multiplexores (MUX) que alimentaban a varias grabadoras de vídeo en un cuarto de control central.

Se podían visualizar las imágenes en tiempo real por medio de un sólo monitor con un interruptor (switch) para cambiar a la cámara deseada, o de monitores capaces de aceptar múltiples fuentes de vídeo en ventanas separadas.

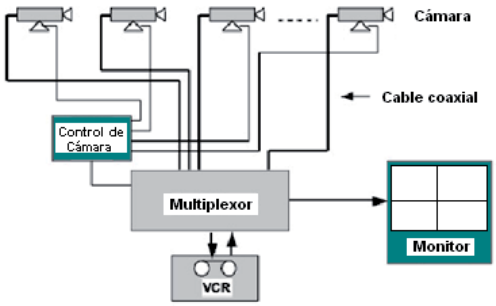

Figura 2.1.- Diagrama del Sistema Análogo CCTV

Una desventaja inherente a este método es el costo de la estación de monitorización de seguridad. Además, el centro de seguridad "centralizado" constituye un punto de crítico dentro de la infraestructura de seguridad. Todas las alimentaciones de vídeo y los cables de control tienen que estar instalados hacia la estación de monitorización. Si una cámara era reubicada, frecuentemente se requería de un nuevo tendido de cable. Por otro lado las videotecas requieren de muchas cintas y, debido a que los medios magnéticos son susceptibles a descargas magnéticas o electroestáticas, estos sistemas no siempre proporcionan la funcionalidad para la cual fueron diseñados. El factor humano también es parte de este sistema, ya que una persona debe cambiar físicamente las cintas, monitorear las sesiones de grabación, etcétera.

En ocasiones, el uso de fibra óptica era necesario en ambientes donde las distancias requerían el uso de repetidores para amplificar la señal o donde la interferencia electromagnética (EMI: *Electro-Magnetic Interference*) representa un problema.

2.1.2 UTP y transmisión análoga CCTV sobre sistemas de cableado estructurado

Con la llegada de cámaras para UTP (*Unshielded Twisted Pair; Par Trenzado no Blindado*), véase la Figura 2.2, nacía un sistema de segunda generación. Las cámaras direccionales IP pueden ser incorporadas actualmente en la infraestructura existente en los edificios. Estos sistemas explotan los beneficios de esta infraestructura a diferencia del cable coaxial.

Este sistema puede requerir de costosas cintotecas y monitores, sin embargo, el costo de una estación de monitoreo central se ha reducido. Los movimientos, adiciones y cambios son más fáciles, ya que las cámaras pueden instalarse dondequiera que exista una salida. El cableado viaja hacia un multiplexor que soporta los populares conectores RJ45. Las cámaras tradicionales con conectores coaxiales pueden reacondicionarse convirtiendo la señal de un cable coaxial (no balanceada) a la del cable de par trenzado (balanceada).

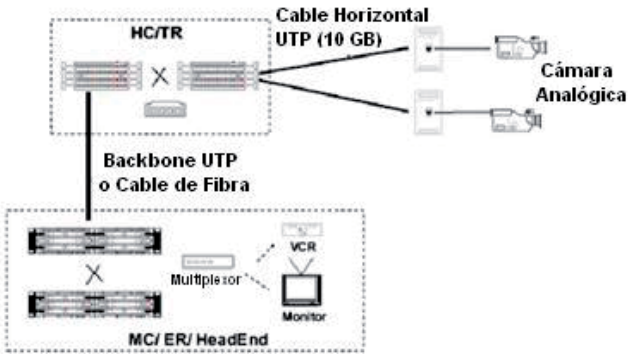

Figura 2.2.- Sistema análogo CCTV basado en UTP y cableado estructurado

2.1.3 El advenimiento de la era digital

Las Grabadoras de Vídeo Digital (*DVRs; Digital Vídeo Recorders*) se introdujeron para resolver muchos de los problemas de las cintotecas de medios magnéticos. Los vídeos digitales se graban en unidades de discos duros de la misma forma en que un archivo se almacena en una computadora. Esto permite obtener redundancia, monitoreo descentralizado, mejor calidad de imagen y mayor longevidad de las grabaciones. Las transmisiones digitales pueden almacenarse sin la necesidad de intervención humana o cambio de cintas. Los tiempos de grabación son mayores, y gracias a algoritmos de compresión de datos dentro de los dispositivos y secuencias de vídeo, estas grabaciones pueden accederse instantáneamente y virtualmente observarse en cualquier lugar donde las políticas de seguridad lo permitan.

Un DVR típico puede multiplexar 16 canales análogos para grabación y reproducción. Esto representa una reducción significativa en costo aunado a un incremento también significativo en funcionalidad en comparación con otros métodos. Las cámaras IP direccionables de estándar abierto son tan fáciles de integrar en una red de seguridad como una PC. Se ha observado una reducción significativa en el precio de almacenamiento de datos con el surgimiento de NAS (*Network Attached Storage, Almacenamiento de Redes Adjuntas*), y SAN (*Storage Area Networks, Almacenamiento de Área de Redes*) trayendo a CCTV una nueva evolución.

2.1.4 Vídeo digital sobre IP

La característica Plug and Play permite a las cámaras IP direccionables 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 vídeos 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 y 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 (*Protocolo de Control de Transmisión/Protocolo de Internet*) 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 y accesibilidad de los recursos de red. Con la habilidad de utilizar la infraestructura existente, un edificio puede volverse totalmente automatizado utilizando un sólo sistema de cableado. Esta automatización puede incluir no sólo CCTV, sino también control de accesos, sistemas de fuego y seguridad, 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 sólo 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 sólo sitio o distribuidos en múltiples ubicaciones.

Un sistema típico CCTV basado en el protocolo IP es completamente diferente de las otras dos soluciones. Las cámaras IP, servidores de vídeo IP y teclados IP pueden colocarse en cualquier punto. Los teclados IP pueden controlar actualmente las funciones PTZ *(Pan, Tilt and Zoom; Vista Panorámica, Inclinación y Ampliación)* 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; Procesamiento de Señales Digitales*), 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; Protocolo de Manejo de Red Simple*) 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 vídeo. Las versiones más recientes vienen equipadas con DVRs internos que pueden incrementarse con un servidor DVR centralizado.

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

2.2 MODELO DE REFERENCIA OSI (INTERCONEXIÓN DE SISTEMA ABIERTO)

2.2.1 Antecedentes del modelo OSI

En 1979, ISO (*Organización Internacional para la Estandarización*) definió su modelo de arquitectura de red OSI (Interconexión de sistemas abiertos). Este modelo fue adoptado en 1980 por el CCITT (*Comité Consultivo Internacional de Telefonía y Telegrafía*) en su recomendación X.200.

La comunicación de datos comprende 2 aspectos principales:

- *El transporte:* involucra todas las funciones relacionadas con la transferencia de datos entre dos usuarios.
- *La manipulación de datos:* los datos deben ser liberados en una forma inteligible. En algunos casos los datos deben ser convertidos.

2.2.2 Capas del modelo OSI

Las redes de computadoras, proveen al usuario de una serie de servicios, e internamente poseen funciones. La cuales son realizadas por las capas o niveles de la arquitectura que posee el tipo de red. Las arquitecturas de las redes tienen una serie de capas superpuestas, una encima de otra, en la que cada una desempeña su función.

Las funciones y características de las capas son las siguientes:

- Permiten fraccionar el desarrollo del protocolo que usa.
- Las capas facilitan el entendimiento del funcionamiento global de un protocolo.
- Facilitan las compatibilidades, tanto de software como de hardware de los distintos sistemas conectados.
- La arquitectura o estructuras de capas son flexibles a la hora de modificarlas.

a) CAPA FÍSICA

Es responsable del transporte de bits. Dependiendo del tipo de enlace físico los bits se representan de una manera en la que puedan ser transportados a través del medio.

Define voltajes, tiempo de duración de los pulsos, el número de patas que tiene el conector de la interface y sus funciones, la forma de establecer la conexión inicial y de interrumpirla, etc.

Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión como ondas o enlaces vía satélite.

b) CAPA DE ENLACE DE DATOS

- Asegura que la información sea transmitida sin errores entre nodos adyacentes de la red sin importar el medio de transmisión utilizado.
- Maneja tramas de datos como unidad de transmisión de datos.
- Crea los límites de la trama.
- Resuelve problemas de daño, pérdida o duplicidad de tramas.
- Participa en la regulación de flujo de tramas entre los nodos.

c) 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 protocolo principal de esta capa es el Protocolo de Internet (IP) aunque también se encuentran a este nivel los protocolos ARP, ICMP e IGMP.

- Se encarga de que los datos sean enviados a su correcto destino, determinando la ruta de transmisión.
- La unidad de transmisión de datos en esta capa es el paquete de datos.
- Participa en el control de congestión de la red.
- Puede llevar la contabilidad del número de paquetes o bits que se enviaron a cada cliente para cuestiones de facturación.
- Puede resolver problemas de interconexión de redes heterogéneas.

d) 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. Además añade la noción de puertos, como se tratará más adelante.

- Acepta los datos de la capa de sesión, los divide, siempre que sea necesario, en unidades más pequeñas (la capa de red generalmente pone un límite en el tamaño de los mensajes que acepta), los pasa a la capa de red y asegura que todos ellos lleguen correctamente a su destino.
- A partir de la capa de red, las 4 capas superiores restantes manejan mensajes como unidad de transmisión de datos.
- Detecta fallas en la red y realiza las acciones correspondientes.
- Solicita el establecimiento de un nuevo enlace, en el caso de que falle un enlace de la red.

d) CAPA DE SESIÓN

- Es un tipo de sistema operativo para la comunicación de datos.
- Permite que los usuarios de diferentes computadoras puedan establecer sesiones entre ellos.
- Realiza el control del diálogo.
- Lleva a cabo la función de sincronización, es decir, inserta puntos de verificación en el flujo de datos, con objeto de que solamente tengan que retransmitirse los datos que se encuentren en seguida del último punto de verificación cuando se reanuda el servicio después de una caída de la red.

e) CAPA DE PRESENTACIÓN

- Permite a dispositivos que intercambian información, entenderse o interpretarse entre ellos independientemente de la codificación que utilicen para los caracteres, por ejemplo, código ASCII (*American Standard Code for Information Interchange; Código Estadounidense Estándar para el Intercambio de Información*) y EBCDIC (*Extended Bynary Coded Decimal Interchange Code;*

Código Extendido de Binario Codificado Decimal).

- Convierte los datos transmitidos a una forma inteligible para el dispositivo terminal.
- Maneja aspectos de representación de la información, por ejemplo: la compresión de datos y la criptografía.

f) CAPA DE APLICACIÓN

Proporciona los distintos servicios de Internet: correo electrónico, páginas Web, FTP, TELNET.

Contiene una variedad de protocolos que hacen posible ofrecer una serie de aplicaciones al usuario final, por ejemplo:

- Correo electrónico.
- Transferencia de archivos.
- Terminal virtual (telnet).
- Directorio electrónico.

2.3 CAPA DE RED

Se explicará detalladamente la capa de red, porque dentro de ésta se tienen las direcciones IP, el protocolo IP y la máscara de subred. Los cuales son importantes para establecer la comunicación entre el servidor y los usuarios.

Por medio de las direcciones IP se hace referencia al punto de publicación que se transmitirá por internet, ésta conexión se basa en el protocolo IP.

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir que se encarga de encontrar un camino manteniendo una tabla de enrutamiento y atravesando los equipos que sean necesarios, para hacer llevar los datos al destino. Los equipos encargados de realizar este encaminamiento se denominan ruteadores.

Adicionalmente la capa de red debe gestionar la congestión en la red, que es el fenómeno que se produce cuando una saturación de un nodo tira la red, es decir, provoca una falla en toda la red.

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.

2.3.1 Direcciones IP

La dirección IP es el identificador de cada host dentro de su red de redes. Cada anfitrión 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 anfitrión. En el caso de Internet, no puede haber dos computadoras con 2 direcciones IP públicas iguales.

Es posible tener dos computadoras con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Las direcciones IP se clasifican en:

- Direcciones IP públicas. Son visibles en todo Internet. Una computadora con una IP pública es accesible (visible) desde cualquier otra computadora conectada a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- Direcciones IP privadas (reservadas). Son visibles únicamente por otros anfitriones de su propia red o de otras redes privadas interconectadas por ruteadores. Se utilizan en las empresas para los puestos de trabajo. Las computadoras con direcciones IP privadas pueden salir a Internet por medio de

un ruteador (o *proxy*) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a computadoras con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- Direcciones IP estáticas (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.
- Direcciones IP dinámicas. Un anfitrión que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. 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 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 IBM es 129.42.18.99.

Las direcciones IP también se pueden representar en:

- hexadecimal, desde la 00.00.00.00 hasta la FF.FF.FF.FF
- binario, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.

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

Decimal	128.10.2.30
Hexadecimal	80.0A.02.1E
Binario	10000000.00001010.00000010.00011110

¿Cuántas direcciones IP existen? Si se calcula 2^{32} se obtiene más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a un anfitrión (host). 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 en 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 anfitrión. Dependiendo del número de anfitriones 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 identifican no a un anfitrión, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar, ya que están reservadas. Tal como lo muestran las Tablas 2.1 y 2.2, donde se especifica para cada clase los bits que son utilizados para la red y los de anfitrión así como los formatos de cada clase.

Tabla 2.1.- Clases de direcciones IP's.

<table>
<tr><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>8</td><td>16</td><td>24</td><td>31</td></tr>
<tr><td>Clase A</td><td>0</td><td colspan="4">red</td><td colspan="4">host</td></tr>
<tr><td colspan="10"></td></tr>
<tr><td>Clase B</td><td>1</td><td>0</td><td colspan="5">red</td><td colspan="3">host</td></tr>
<tr><td colspan="10"></td></tr>
<tr><td>Clase C</td><td>1</td><td>1</td><td>0</td><td colspan="6">red</td><td>host</td></tr>
<tr><td colspan="10"></td></tr>
<tr><td>Clase D</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="5">grupo de multicast (multidifusión)</td></tr>
<tr><td colspan="10"></td></tr>
<tr><td>Clase E</td><td>1</td><td>1</td><td>1</td><td>1</td><td colspan="5">(direcciones reservadas: no se pueden utilizar)</td></tr>
</table>

Tabla 2.2.- Especificaciones de clases de direcciones IP's.

Clase	Formato (r=red, h=host)	Número de redes	Número de hosts por red	Rango de direcciones de redes	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	-

Difusión (broadcast) y multidifusión (multicast).- El término difusión se refiere a todos los anfitriones de una red; multidifusión se refiere a varios anfitriones (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 anfitrión.

2.3.2 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 anfitrión: algunas de ellas tienen significados especiales. Las principales direcciones especiales se resumen en la Tabla 2.3. Su interpretación depende del anfitrión desde el que sean utilizadas.

Tabla 2.3.- Direcciones Especiales

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

Difusión o *broadcast* es el envío de un mensaje a todas las computadoras que se encuentran en una red. La dirección de *loopback* (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestra propia computadora.

Las direcciones de redes 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.

En el caso de tener salida a Internet, el direccionamiento IP permite que los anfitriones con direcciones IP privadas puedan salir a Internet pero impide el acceso a los anfitriones 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.

2.3.3 Máscara de subred

Una máscara de subred es aquella dirección que enmascarando una dirección IP, indica si otra dirección IP pertenece a esa subred o no. La Tabla 2.4 muestra las máscaras de subred correspondientes a cada clase:

Tabla 2.4.- Máscaras de subred de acuerdo a la clase de dirección IP

Clase	Máscara de subred
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Si se expresa la máscara de subred de clase A en notación binaria, se tiene:

11111111.00000000.00000000.00000000

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

Supóngase una subred con máscara 255.255.0.0, en la que se tiene una computadora con dirección 148.120.33.110. Si se expresa esta dirección y la de la máscara de subred en binario, se tiene:

148.120.33.110 10010100.01111000.00100001.01101110 (dirección de una máquina)
255.255.0.0 11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.120.0.0 10010100.01111000.00000000.00000000 (dirección de su subred)
<------RED------> <------HOST----->

Al hacer el producto binario de las dos primeras direcciones (donde hay dos 1's en las mismas posiciones se pone un 1 y en caso contrario, un 0) se obtiene la tercera.

Si hacemos lo mismo con otra computadora, por ejemplo el 148.120.33.89, se obtiene la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

148.120.33.89 10010100.01111000.00100001.01011001 (dirección de una máquina)
255.255.0.0 11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.120.0.0 10010100.01111000.00000000.00000000 (dirección de su subred)

En cambio, si se toma la 148.115.89.3, se observa que no pertenece a la misma subred que las anteriores.

148.115.89.3 10010100.01110011.01011001.00000011 (dirección de una máquina)
255.255.0.0 11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.115.0.0 10010100.01110011.00000000.00000000 (dirección de su subred)

Cálculo de la dirección de difusión.- Ya se ha visto que el producto lógico binario (AND) de una IP y su máscara devuelven su dirección de red. Para calcular su dirección de difusión, hay que hacer la suma lógica en binario (OR) de la IP con el inverso (NOT) de su máscara.

En una red de redes TCP/IP no puede haber anfitriones 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 una computadora sabe si otra computadora 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 anfitriones están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del anfitrión origen.

Este ruteador pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del anfitrión destino y se complete la entrega del mensaje.

Las máscaras 255.0.0.0 (clase A), 255.255.0.0 (clase B) y 255.255.255.0 (clase C) suelen ser suficientes para la mayoría de las redes privadas. Sin embargo, las redes más pequeñas que podemos formar con estas máscaras son de 254 anfitriones y para el caso de direcciones públicas, su contratación tiene un costo muy alto. Por esta razón suele ser habitual dividir las redes públicas de clase C en subredes más pequeñas.

En la tabla 2.5 se muestran las posibles divisiones de una red de clase C. La división de una red en subredes se conoce como subnetting o subneteo.

Tabla 2.5.- Divisiones de una Red clase C

Máscara de subred	Binario	Número de subredes	Núm. de hosts por subred	Ejemplos de subredes (x=a.b.c por ejemplo, 192.168.1)
255.255.255.0	00000000	1	254	x.0
255.255.255.128	10000000	2	126	x.0, x.128
255.255.255.192	11000000	4	62	x.0, x.64, x.128, x.192
255.255.255.224	11100000	8	30	x.0, x.32, x.64, x.96, x.128, ...
255.255.255.240	11110000	16	14	x.0, x.16, x.32, x.48, x.64, ...
255.255.255.248	11111000	32	6	x.0, x.8, x.16, x.24, x.32, x.40, ...
255.255.255.252	11111100	64	2	x.0, x.4, x.8, x.12, x.16, x.20, ...
255.255.255.254	11111110	128	0	ninguna posible
255.255.255.255	11111111	256	0	ninguna posible

2.3.4 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. Se trata de un sistema de entrega de paquetes (llamados 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.

2.3.5 Formato del datagrama IP

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas (recuérdese la trama Ethernet) de las distintas redes que va atravesando. Cada vez que un datagrama tiene que atravesar un ruteador, el datagrama saldrá de la trama física de la red que abandona y se acomodará en el campo de datos de una trama física de la siguiente red.

Este mecanismo permite que un mismo datagrama IP pueda atravesar redes distintas: enlaces punto a punto, redes ATM, redes Ethernet, redes Token Ring, etc. El propio datagrama IP tiene también un campo de datos: será aquí donde viajen los paquetes de las capas superiores. La Figura 2.3 muestra el formato del datagrama IP y la tabla 2.6 muestra los campos del datagrama.

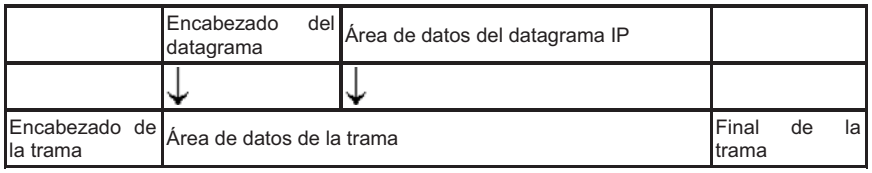

Figura 2.3.- Formato del datagrama IP

Tabla 2.6.- Campos del Datagrama

0										10										20										30
0	1	2	3	4	5	6	7	8	9	0	1	2	3	3	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
VERS				HLEN				Tipo de servicio							Longitud total																
Identificación																				Banderas		Desplazamiento de fragmento									
TTL								Protocolo							CRC cabecera																
Dirección IP origen																															
Dirección IP destino																															
Opciones IP (si las hay)																													Relleno		
Datos																															

Campos del datagrama IP:

a) VERS (4 bits). Indica la versión del protocolo IP que se utilizó para crear el datagrama. Actualmente se utiliza la versión 4 (IPv4) aunque ya se están las especificaciones de la siguiente versión, la 6 (IPv6).

b) HLEN (4 bits). Longitud de la cabecera expresada en múltiplos de 32 bits. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.

c) Tipo de servicio. Los 8 bits de este campo se dividen a su vez en:

- Prioridad (3 bits). Un valor de 0 indica baja prioridad y un valor de 7, prioridad máxima.
- Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los ruteadores que se encuentren a su paso los cuales pueden tenerlas en cuenta o no.
- Bit D *(Delay; Retardo)*. Solicita retardos cortos (enviar rápido).
- Bit T *(Throughput; Completar proceso)*. Solicita un alto rendimiento (enviar mucho en el menor tiempo posible).
- Bit R *(Reliability; Confiabilidad)*. Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien).
- Los siguientes dos bits no tienen uso.

d) Longitud total (16 bits). Indica la longitud total del datagrama expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes.

e) Identificación (16 bits). Número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un datagrama en toda la red. Si se trata de un datagrama fragmentado, llevará la misma identificación que el resto de fragmentos.

f) Banderas o indicadores (3 bits). Sólo 2 bits de los 3 bits disponibles están actualmente utilizados. El bit de Más Fragmentos (MF) indica que no es el último datagrama. Y el bit de No Fragmentar (NF) prohíbe la fragmentación del datagrama. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste no se podrá transmitir y se descartará.

g) Desplazamiento de fragmentación (13 bits). Indica el lugar en el cual se insertará el fragmento actual dentro del datagrama completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud que es múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.

h) Tiempo de vida o TTL (8 bits). Número máximo de segundos que puede estar un datagrama en la red de redes. Cada vez que el datagrama atraviesa un ruteador se resta 1 a este número. Cuando llegue a cero, el datagrama se descarta y se devuelve un mensaje ICMP *(Control Message Protocol; Protocolo de Mensajes de Control de Internet*) de tipo "tiempo excedido" para informar al origen de la incidencia.

i) Protocolo (8 bits). Indica el protocolo utilizado en el campo de datos: 1 para ICMP, 2 para IGMP (*Internet Group Management Protocol; Protocolo de Administración de Grupos de Internet*), 6 para TCP y 17 para UDP.

j) CRC cabecera (16 bits). Contiene la suma de comprobación de errores sólo para la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores.

k) Dirección origen (32 bits). Contiene la dirección IP del origen.

l) Dirección destino (32 bits). Contiene la dirección IP del destino.

m) Opciones IP. Este campo no es obligatorio y especifica las distintas opciones solicitadas por el usuario que envía los datos (generalmente para pruebas de red y depuración).

n) Relleno. Si las opciones IP (en caso de existir) no ocupan un múltiplo de 32 bits, se completa con bits adicionales hasta alcanzar el siguiente múltiplo de 32 bits (recuérdese que la longitud de la cabecera tiene que ser múltiplo de 32 bits).

2. 4 CAPA DE TRANSPORTE

A través de la capa de transporte se asignan puertos a las cámaras que están capturando el vídeo y transmitiéndolo vía Internet, dichos puertos son conocidos como well-known (bien conocidos) los cuales están definidos en la *RFC 1700*. Los puertos que se utilizan en el caso de los navegadores web conectados a dicho servidor son asignados de manera dinámica.

La capa de red transfiere datagramas entre dos computadoras a través de la red utilizando como identificadores las direcciones IP. La capa de transporte añade la noción de puerto para distinguir entre los muchos destinos dentro de un mismo anfitrión. No es suficiente con indicar la dirección IP del destino, además hay que especificar la aplicación que recogerá el mensaje. Cada aplicación que esté esperando un mensaje utiliza un número de puerto distinto; más concretamente, la aplicación está a la espera de un mensaje en un puerto determinado (escuchando un puerto).

Pero no sólo se utilizan los puertos para la recepción de mensajes, también para el envío: todos los mensajes que envíe una computadora debe hacerlo a través de uno de sus puertos.

En la Figura 2.4 se representa una transmisión entre la computadora 194.35.133.5 y la 135.22.8.165. La primera utiliza su puerto 1256 y la segunda, el 80.

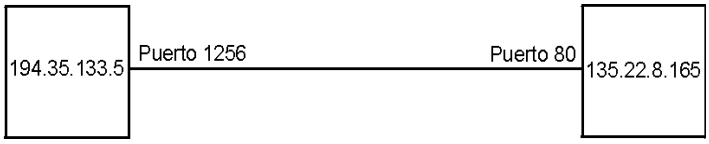

Figura 2.4.- Comunicación entre 2 PC's.

La capa de transporte transmite mensajes entre las aplicaciones de dos computadoras. Por ejemplo, entre un navegador de páginas web y un servidor de páginas web, o entre un programa de correo electrónico y un servidor de correo. La Figura 2.5 muestra algunos protocolos de comunicación en las capas del modelo OSI.

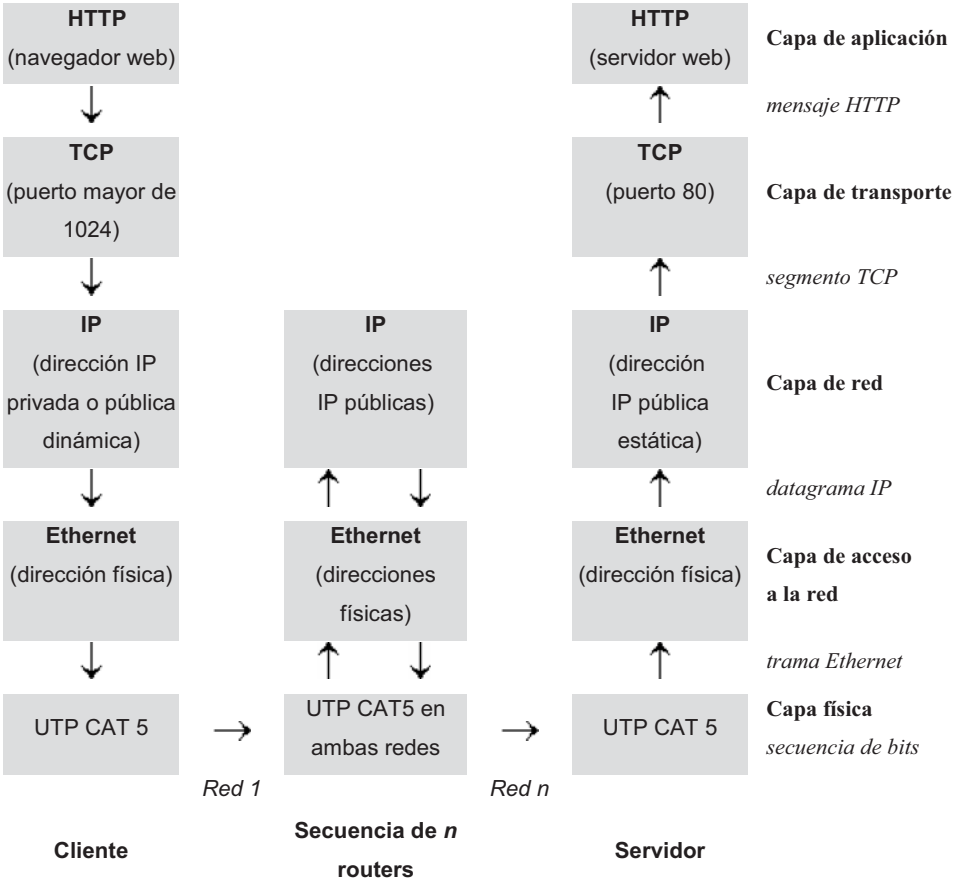

Figura 2.5.- Protocolos de las Capas del Modelo OSI

2.4.1 Puertos

Una computadora puede estar conectada con distintos servidores a la vez; por ejemplo, con un servidor de noticias y un servidor de correo. Para distinguir las distintas conexiones dentro de una misma computadora se utilizan los puertos.

Un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada computadora. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

Los números de puerto de las aplicaciones cliente son asignados dinámicamente y generalmente son superiores al 1024. Cuando una aplicación cliente quiere comunicarse con un servidor, busca un número de puerto libre y lo utiliza.

En cambio, las aplicaciones servidoras utilizan unos números de puerto prefijados: son los llamados puertos well-known (bien conocidos). Estos puertos están definidos en la *RFC 1700*. A continuación se enumeran los puertos well-known más usuales:

Tabla 2.7.- Puertos bien-conocido mas usuales

Palabra clave	Puerto	Descripción
	0/tcp	Reservar
	0/udp	Reservar
tcpmux	1/tcp	TCP Puerto de Servicio Multiplexor
rje	5/tcp	Anotación de Trabajo Remoto
echo	7/tcp/udp	Echo
discard	9/tcp/udp	Descartar
systat	11/tcp/udp	Usuarios Activos
daytime	13/tcp/udp	Fecha
qotd	17/tcp/udp	Cita del Día
chargen	19/tcp/udp	Generador de Calidad
ftp-data	20/tcp	Transferencia de Archivos [Default Data]
ftp	21/tcp	Transferencia de Archivo [Control]
telnet	23/tcp	Telnet
smtp	25/tcp	Transferencia Simple de Correo
time	37/tcp/udp	Tiempo
nameserver	42/tcp/udp	Nombre del Servidor Anfitrión
Palabra clave	**Puerto**	**Descripción**

nicname	43/tcp/udp	Quién es
domain	53/tcp/udp	Servidor de nombres de dominios
bootps	67/udp/udp	Bootstrap Protocol Server
tftp	69/udp	Transferencia Trivial de Ficheros
gopher	70/tcp	Mensajero
finger	79/tcp	Identificador
www-http	80/tcp	Red Mundial HTTP
dcp	93/tcp	Protocolo de Control de Dispositivos
supdup	95/tcp	SUPDUP
hostname	101/tcp	NIC Nombre del Servidor Anfitrión
iso-tsap	102/tcp	ISO-TSAP
gppitnp	103/tcp	Red de Transmisión Punto a Punto Génesis
rtelnet	107/tcp/udp	Servicio Tel Net Remoto
pop2	109/tcp	Protocolo de Oficina Postal - Versión 2
pop3	110/tcp	Protocolo de Oficina Postal - Versión 3
sunrpc	111/tcp/udp	Llamada de Procedimiento remoto SUN
auth	113/tcp	Servicio de Autentificación
sftp	115/tcp/udp	Protocolo Simple de Transferencia de Ficheros
nntp	119/tcp	Protocolo de Transferencia de Datos en la Red
ntp	123/udp	Protocolo de Tiempo de Red
pwdgen	129/tcp	Protocolo Generador de Contraseña
netbios-ns	137/tcp/udp	Servicio de Nombres NETBIOS
netbios-dgm	138/tcp/udp	Servicio de Datagrama NETBIOS
netbios-ssn	139/tcp/udp	Servicio de Sesión NETBIOS
snmp	161/udp	SNMP
snmptrap	162/udp	SNMPTRAP
irc	194/tcp	Internet Relay Chat Protocol

Los puertos tienen una memoria intermedia *(buffer)* situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

Los dos protocolos principales de la capa de transporte son UDP y TCP. El primero ofrece una transferencia de mensajes no fiable y no orientada a conexión y el segundo, una transferencia fiable y orientada a conexión.

2.4.2 Protocolo UDP

El protocolo UDP (*User Datagram Protocol, Protocolo de Datagrama de Usuario*) proporciona una comunicación muy sencilla entre las aplicaciones de dos computadoras. Al igual que el protocolo IP, UDP es:

- No orientado a conexión. No se establece una conexión previa con el otro extremo para transmitir un mensaje UDP. Los mensajes se envían sin más y éstos pueden duplicarse o llegar desordenados al destino.
- No fiable. Los mensajes UDP se pueden perder o llegar dañados.

UDP utiliza el protocolo IP para transportar sus mensajes. Como vemos, en la Figura 2.6, no añade ninguna mejora en la calidad de la transferencia; aunque sí incorpora los puertos origen y destino en su formato de mensaje. Las aplicaciones (y no el protocolo UDP) deberán programarse teniendo en cuenta que la información puede no llegar de forma correcta. La Tabla 2.8 muestra el formato del mensaje UDP.

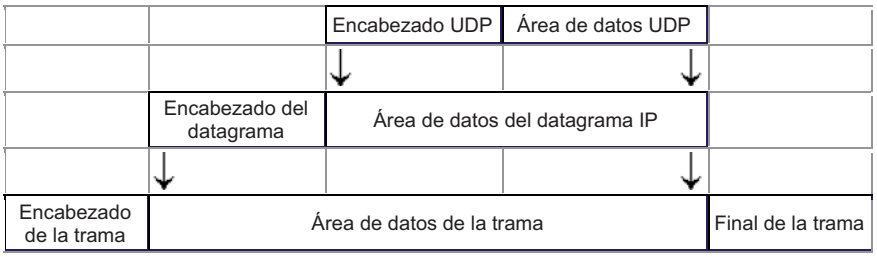

Figura 2.6.- Formato de IP en el Protocolo de Datagrama de Usuario

Tabla 2.8.- Formato del mensaje UDP

0										10										20										30
0	1	2	3	4	5	6	7	8	9	0	1	2	3	3	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Puerto UDP origen																Puerto UDP destino															
Longitud mensaje UDP																Suma verificación UDP															
Datos																															
...																															

- Puerto UDP de origen (16 bits, opcional). Número de puerto de la máquina origen.
- Puerto UDP de destino (16 bits). Número de puerto de la máquina destino.
- Longitud del mensaje UDP (16 bits). Especifica la longitud medida en bytes del mensaje UDP incluyendo la cabecera. La longitud mínima es de 8 bytes.
- Suma de verificación UDP (16 bits, opcional). Suma de comprobación de errores del mensaje. Para su cálculo se utiliza una pseudo-cabecera que también incluye las direcciones IP origen y destino. Para conocer estos datos, el protocolo UDP debe interactuar con el protocolo IP.
- Datos. Aquí viajan los datos que se envían las aplicaciones. Los mismos datos que envía la aplicación origen son recibidos por la aplicación destino después de atravesar toda la red de redes.

2.4.3 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 viajan por un circuito virtual. Es conocido 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 crea la ilusión de que existe un circuito único 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 los 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, la conexión es full-dúplex.

Fiabilidad

¿Cómo es posible enviar información fiable basándose en un protocolo no fiable? Es decir, si los datagramas que transportan los segmentos TCP se pueden perder, ¿cómo pueden llegar los datos de las aplicaciones de forma correcta al destino?

La respuesta a esta pregunta es sencilla: cada vez que llega un mensaje se devuelve una confirmación (*acknowledgement*) para que el emisor sepa que ha llegado correctamente. Si no le llega esta confirmación pasado un cierto tiempo, el emisor reenvía el mensaje.

A continuación se muestra la manera más sencilla (aunque ineficiente) de proporcionar una comunicación fiable. El emisor envía un dato, arranca su temporizador y espera su confirmación (ACK). Si recibe su ACK antes de agotar el temporizador, envía el siguiente dato. Si se agota el temporizador antes de recibir el ACK, reenvía el mensaje. El esquema mostrado en la Figura 2.7 representa este comportamiento:

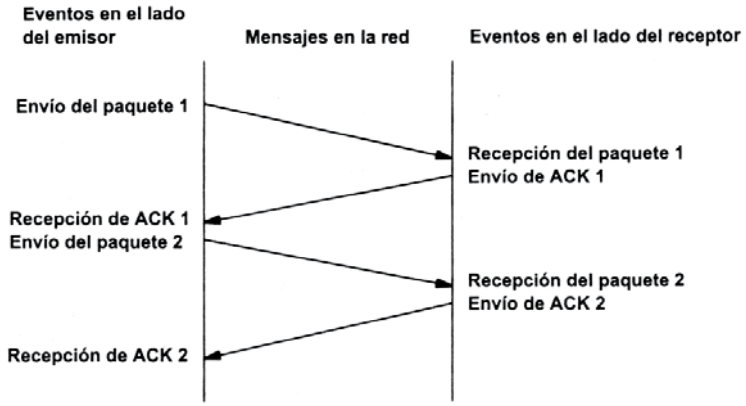

Figura 2.7.- Comunicación fiable del protocolo TCP

Conexiones

Una conexión son dos direcciones IP: puerto. No puede haber dos conexiones iguales en un mismo instante en toda la Red. Aunque bien es posible que una misma computadora tenga dos conexiones distintas y simultáneas utilizando un mismo puerto. El protocolo TCP utiliza el concepto de conexión para identificar las transmisiones.

Para que se pueda crear una conexión, el extremo del servidor debe hacer una *apertura pasiva* del puerto (escuchar su puerto y quedar a la espera de conexiones) y el cliente, una *apertura activa* en el puerto del servidor (conectarse

con el puerto de un determinado servidor).

Formato del segmento TCP

Ya se ha comentado que el flujo de bytes que produce una determinada aplicación se divide en uno o más segmentos TCP para su transmisión. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Para facilitar el control de flujo de la información los bytes de la aplicación se numeran. De esta manera, cada segmento indica en su cabecera el primer byte que transporta. Las confirmaciones o acuses de recibo (ACK) representan el siguiente byte que se espera recibir (y no el número de segmento recibido, ya que éste no existe). El formato de TCP se muestra en la Tabla 2.9.

Tabla 2.9.- Formato del Segmento TCP

<table>
<tr><td colspan="10">0</td><td colspan="10">10</td><td colspan="10">20</td><td colspan="2">30</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>3</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="16">Puerto TCP origen</td><td colspan="16">Puerto TCP destino</td></tr>
<tr><td colspan="32">Número de secuencia</td></tr>
<tr><td colspan="32">Número de acuse de recibo</td></tr>
<tr><td colspan="4">HLEN</td><td colspan="6">Reservado</td><td colspan="6">Bits código</td><td colspan="16">Ventana</td></tr>
<tr><td colspan="16">Suma de verificación</td><td colspan="16">Puntero de urgencia</td></tr>
<tr><td colspan="24">Opciones (si las hay)</td><td colspan="8">Relleno</td></tr>
<tr><td colspan="32">Datos</td></tr>
</table>

- Puerto fuente (16 bits). Puerto de la máquina origen. Al igual que el puerto destino es necesario para identificar la conexión actual.
- Puerto destino (16 bits). Puerto de la máquina destino.
- Número de secuencia (32 bits). Indica el número de secuencia del primer byte que trasporta el segmento.
- Número de acuse de recibo (32 bits). Indica el número de secuencia del siguiente byte que se espera recibir. Con este campo se indica al otro extremo de la conexión que los bytes anteriores se han recibido correctamente.

- HLEN (4 bits). Longitud de la cabecera medida en múltiplos de 32 bits (4 bytes). El valor mínimo de este campo es 5, que corresponde a un segmento sin datos (20 bytes).
- Reservado (6 bits). Bits reservados para un posible uso futuro.
- Bits de código o indicadores (6 bits). Los bits de código determinan el propósito y contenido del segmento. A continuación se explica el significado de cada uno de estos bits (mostrados de izquierda a derecha) si está a 1.
- URG. El campo *Puntero de urgencia* contiene información válida.
- ACK. El campo *Número de acuse de recibo* contiene información válida, es decir, el segmento actual lleva un ACK. Observemos que un mismo segmento puede transportar los datos de un sentido y las confirmaciones del otro sentido de la comunicación.
- PSH. La aplicación ha solicitado una operación *push* (enviar los datos existentes en la memoria temporal sin esperar a completar el segmento).
- RST. Interrupción de la conexión actual.
- SYN. Sincronización de los números de secuencia. Se utiliza al crear una conexión para indicar al otro extremo cual va a ser el primer número de secuencia con el que va a comenzar a transmitir (más adelante se vera que no tiene porqué ser el cero).
- FIN. Indica al otro extremo que la aplicación ya no tiene más datos para enviar. Se utiliza para solicitar el cierre de la conexión actual.
- Ventana (16 bits). Número de bytes que el emisor del segmento está dispuesto a aceptar por parte del destino.
- Suma de verificación (24 bits). Suma de comprobación de errores del segmento actual. Para su cálculo se utiliza una *pseudo-cabecera* que también incluye las direcciones IP origen y destino.
- Puntero de urgencia (8 bits). Se utiliza cuando se están enviando datos urgentes que tienen preferencia sobre todos los demás e indica el siguiente byte del campo *Datos* que sigue a los datos urgentes. Esto le permite al destino identificar donde terminan los datos urgentes. Nótese que un mismo segmento

puede contener tanto datos urgentes (al principio) como normales (después de los urgentes).

- Opciones (variable). Si está presente únicamente se define una opción: el tamaño máximo de segmento que será aceptado.
- Relleno. Se utiliza para que la longitud de la cabecera sea múltiplo de 32 bits.
- Datos. Información que envía la aplicación.

2.5 CAPA DE APLICACIÓN

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.
Entre los protocolos (refiriéndose a protocolos genéricos, no a protocolos de la capa de aplicación de OSI) más conocidos destacan:

- HTTP (*Protocolo de Transferencia de Hipertexto*) el protocolo bajo la www (World Wide Web; Red Mundial).
- FTP (*Protocolo de Transferencia de Archivos*) (FTAM, fuera de TCP/IP) transferencia de ficheros
- SMTP (*Protocolo de Transferencia Simple de Correo*): X.400 fuera de TCP/IP envío y distribución de correo electrónico.
- POP (*Post Office Protocol; Protocolo de Oficina Postal*)/IMAP: reparto de correo al usuario final

- SSH (*Secure Shell; Capa de Seguridad*) principalmente terminal remota, aunque en realidad cifra casi cualquier tipo de transmisión.
- Telnet otra terminal remota, ha caído en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.
- Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:
- SNMP (*Protocolo de Manejo de Red Simple*).
- DNS (*Sistema de Dominio de Nombres*).

2.6 NOMBRES DE DOMINIO

Generalmente no se trabaja con direcciones IP sino con nombres de dominio. Para que esto pueda ser posible es necesario un proceso previo de conversión de nombres de dominio a direcciones IP, ya que el protocolo IP requiere direcciones IP al enviar sus datagramas. Este proceso se conoce como resolución de nombres.

2.6.1 Métodos estándar de resolución de nombres

A continuación se comentan brevemente los distintos métodos de resolución de nombres que utiliza Microsoft Windows para traducir un nombre de dominio a dirección IP, tal como lo muestra la Tabla 2.10. Estos métodos son aplicables a las utilidades TCP/IP que proporciona Windows (Ping, Tracert) y son distintos a los utilizados desde Entorno de Red.

Tabla 2.10.- Métodos de Resolución de Nombres

Método de resolución	Descripción
1. Nombre de host local	Nombre de host configurado para la máquina (Entorno de Red, TCP/IP, configuración DNS)
2. Fichero HOSTS	Fichero de texto situado en el directorio de Windows que contiene una traducción de nombres de dominio en direcciones IP.
3. Servidor DNS	Servidor que mantiene una base de datos de direcciones IP y nombres de dominio
4. Servidor de nombres NetBIOS	Servidor que mantiene una base de datos de direcciones IP y nombres NetBIOS. Los nombres NetBIOS son los que vemos desde Entorno de Red y no tienen porqué coincidir con los nombres de dominio

Método de resolución	Descripción
5. Local Broadcast	Broadcasting a la subred local para la resolución del nombre NetBIOS
6. Fichero LMHOSTS	Fichero de texto situado en el directorio de Windows que contiene una traducción de nombres NetBIOS en direcciones IP

El fichero HOSTS proporciona un ejemplo muy sencillo de resolución de nombres:

127.0.0.1 local host
192.168.0.69 servidor
129.168.0.1 ruteador

2.6.2 Necesidad del DNS

En los orígenes de Internet, cuando sólo había unos cientos de computadoras conectadas, la tabla con los nombres de dominio y direcciones IP se encontraba almacenada en un fichero de una única computadora con el nombre de HOSTS.TXT. El resto de computadoras debían consultarle a ésta cada vez que tenían que resolver un nombre. Este fichero contenía una estructura plana de nombres, tal como se observó en el ejemplo anterior y funcionaba bien ya que la lista sólo se actualizaba una o dos veces por semana.

Sin embargo, a medida que se fueron conectando más computadoras a la red comenzaron los problemas: el fichero HOSTS.TXT comenzó a ser demasiado extenso, el mantenimiento se hizo difícil ya que requería más de una actualización diaria y el tráfico de la red hacia esta computadora llegó a saturarla.

Es por ello que fue necesario diseñar un nuevo sistema de resolución de nombres que distribuyese el trabajo entre distintos servidores. Se ideó un sistema jerárquico de resolución conocido como DNS (*Domain Name System:* Sistema de Dominio de Nombres).

2.6.3 Componentes del DNS

Para su funcionamiento, el DNS utiliza tres componentes principales:

- *Clientes DNS (resolvers)*. Los clientes DNS envían las peticiones de resolución de nombres a un servidor DNS. Las peticiones de nombres son preguntas de la forma: ¿Qué dirección IP le corresponde al nombre: *dominio*?
- *Servidores DNS. Lo*s servidores DNS contestan a las peticiones de los clientes consultando su base de datos. Si no disponen de la dirección solicitada pueden reenviar la petición a otro servidor.
- *Espacio de nombres de dominio.* Se trata de una base de datos distribuida entre distintos servidores.

Espacio de nombres de dominio

El espacio de nombres de dominio es una estructura jerárquica con forma de árbol que clasifica los distintos dominios en niveles.

A continuación se muestra en la Figura 2.8 una pequeña parte del espacio de nombres de dominio de Internet:

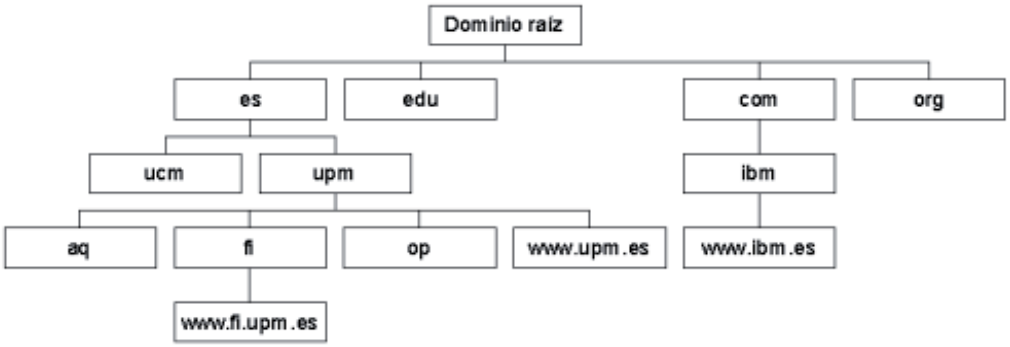

Figura 2.8.- Dominios de Internet

El punto más alto de la jerarquía es el dominio raíz. Los dominios de primer nivel (es, edu, com.) parten del dominio raíz y los dominios de segundo nivel (upm,

ucm, microsoft.), de un dominio de primer nivel; y así sucesivamente. Cada uno de los dominios puede contener tanto anfitriones como más subdominios.

Generalmente cada uno de los dominios es gestionado por un servidor distinto; es decir, se tendrá un servidor para diferentes dominios.

Los dominios de primer nivel *(Top-Level Domains)* han sido clasificados tanto en función de su estructura organizativa como geográficamente.

Ejemplos de dominio de primer nivel se muestran en las Tablas 2.11 y 2.12:

En función de su estructura organizativa:

Tabla 2.11.- Nombres de dominio por su estructura organizativa

Nombre de dominio	Significado
com	organizaciones comerciales
net	redes
org	otras organizaciones
edu	instituciones educativas y universidades
gov	organizaciones gubernamentales
mil	organizaciones militares

Geográficamente:

Tabla 2.12.- Nombres de dominio geográficos

Nombre de dominio	Significado
mx	México
es	España
tw	Taiwán
fr	Francia
tv	Tuvalu

Zonas de autoridad

Una zona de autoridad es la porción del espacio de nombres de dominio de la que es responsable un determinado servidor DNS. La zona de autoridad de estos servidores abarca al menos un dominio y también pueden incluir subdominios;

aunque generalmente los servidores de un dominio delegan sus subdominios en otros servidores.

Tipos de servidores DNS

Dependiendo de la configuración del servidor, éste puede desempeñar distintos papeles:

a) Servidores primarios *(primary name servers)*. Estos servidores almacenan la información de su zona en una base de datos local. Son los responsables de mantener la información actualizada y cualquier cambio debe ser notificado a este servidor.
b) Servidores secundarios *(secundary name servers)*. Son aquellos que obtienen los datos de su zona desde otro servidor que tenga autoridad para esa zona. El proceso de copia de la información se denomina transferencia de zona.
c) Servidores maestros *(master name servers)*. Los servidores maestros son los que transfieren las zonas a los servidores secundarios. Cuando un servidor secundario arranca busca un servidor maestro y realiza la transferencia de zona. Un servidor maestro para una zona puede ser a la vez un servidor primario o secundario de esa zona. Estos servidores extraen la información desde el servidor primario de la zona. Así se evita que los servidores secundarios sobre carguen al servidor primario con transferencias de zonas.
d) Servidores locales *(caching-only servers)*. Los servidores locales no tienen autoridad sobre ningún dominio: se limitan a contactar con otros servidores para resolver las peticiones de los clientes DNS. Estos servidores mantienen una *memoria caché* con las últimas preguntas contestadas. Cada vez que un cliente DNS le formula una pregunta, primero consulta en su memoria caché. Si encuentra la dirección IP solicitada, se la devuelve al cliente; si no, consulta a otros servidores, apunta la respuesta en su memoria caché y le comunica la respuesta al cliente.

Los servidores secundarios son importantes por varios motivos. En primer lugar, *por seguridad* debido a que la información se mantiene de forma redundante en varios servidores a la vez. Si un servidor tiene problemas, la información se podrá recuperar desde otro. Y en segundo lugar, *por velocidad* porque evita la sobrecarga del servidor principal distribuyendo el trabajo entre distintos servidores situados estratégicamente (por zonas geográficas, por ejemplo).

2.6.4 Resolución de nombres de dominio

La resolución de un nombre de dominio es la traducción del nombre a su correspondiente dirección IP. Para este proceso de traducción los *clientes DNS* pueden formular dos tipos de preguntas (recursivas e iterativas).

- Preguntas recursivas. Si un cliente formula una pregunta recursiva a un servidor DNS, éste debe intentar por todos los medios resolverla aunque para ello tenga que preguntar a otros servidores.
- Preguntas iterativas. Si, en cambio, el cliente formula una pregunta iterativa a un servidor DNS, este servidor devolverá o bien la dirección IP si la conoce o si no, la dirección de otro servidor que sea capaz de resolver el nombre.

Por ejemplo: Estamos trabajando con Internet Explorer y escribimos en la barra de dirección: www.ibm.com. En primer lugar, el navegador tiene que resolver el nombre de dominio a una dirección IP. Después podrá comunicarse con la correspondiente dirección IP, abrir una conexión TCP con el servidor y mostrar en pantalla la página principal de IBM. En la Figura 2.9 se muestra el esquema de resolución:

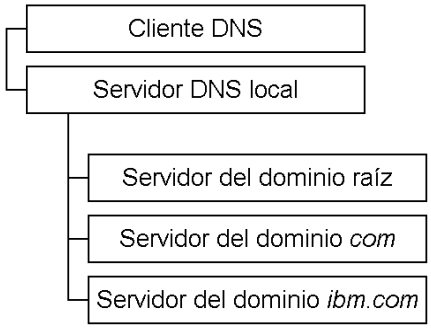

Figura 2.9 Esquema de resolución de Nombres de Dominio

1. Nuestra computadora (cliente DNS) formula una pregunta recursiva a nuestro servidor DNS local (generalmente el proveedor de Internet).
2. El servidor local es el responsable de resolver la pregunta, aunque para ello tenga que reenviar la pregunta a otros servidores. Se supone que no conoce la dirección IP asociada a www.ibm.com; entonces formulará una pregunta iterativa al servidor del dominio raíz.
3. El servidor del dominio raíz no conoce la dirección IP solicitada, pero devuelve la dirección del servidor del dominio *com*.
4. El servidor local reenvía la pregunta iterativa al servidor del dominio *com*.
5. El servidor del dominio .*com* tampoco conoce la dirección IP preguntada, aunque sí conoce la dirección del servidor del dominio *ibm.com,* por lo que devuelve esta dirección.
6. El servidor local vuelve a reenviar la pregunta iterativa al servidor del dominio *ibm.com*.
7. El servidor del dominio *ibm.com* conoce la dirección IP de www.ibm.com y devuelve esta dirección al servidor local.
8. El servidor local por fin ha encontrado la respuesta y se la reenvía a nuestra computadora.

Preguntas inversas

Los clientes DNS también pueden formular preguntas inversas, esto es, conocer el nombre de dominio dada una dirección IP. Para evitar una búsqueda exhaustiva por todo el espacio de nombres de dominio, se ha creado un dominio especial llamado *in-addr.arpa*. Cuando un cliente DNS desea conocer el nombre de dominio asociado a la dirección IP *a.b.c.d*, formula una pregunta inversa a *d.c.b.a.in-addr.arpa*. La inversión de los bytes es necesaria debido a que los nombres de dominio son más genéricos por la derecha, al contrario que ocurre con las direcciones.

CAPÍTULO 3

HERRAMIENTAS PARA LA CONSTRUCCIÓN DEL SISTEMA

3.1 WINDOWS SERVER 2003

Windows Server 2003 es la versión de Windows para servidores lanzada por Microsoft en el año 2003. Está basada en el núcleo de Windows XP, al que se le han añadido una serie de servicios, y se le han bloqueado algunas características (para mejorar el rendimiento, o simplemente porque no serán usadas). En términos generales, Windows Server 2003 es un Windows XP simplificado, no con menos funciones, sino que estas están deshabilitadas por defecto para obtener un mejor rendimiento y para centrar el uso de procesador en las características de servidor. Sin embargo, en internet existen multitud de guías para "transformar" a Windows Server 2003 en Windows XP, para su uso doméstico, por ejemplo, ya que este último trae demasiados "errores" que provocan la lentitud general del sistema.

Funciones del Servidor

Windows Server 2003 es un sistema operativo de propósitos múltiples capaz de manejar una gran gama de funciones de servidor, en base a sus necesidades, tanto de manera centralizada como distribuida. Algunas de estas funciones del servidor son:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN: *Virtual Private Networks*).

- Servicio de directorio, Sistema de dominio (DNS: *Domain Name Server*), y servidor DHCP (*Dynamic Host Configuration Protocol; Protocolo de Configuración de Host Dinámico*).
- Servidor de transmisión de multimedia en tiempo real.
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

3.1.1 Beneficios de Windows Server 2003

Windows Server 2003 cuenta con cuatro beneficios principales que se muestran en la tabla 3.1:

Tabla 3.1.- Beneficios que brinda Windows Server 2003

Beneficio	Descripción
Seguro	Es el sistema operativo de servidor más rápido y más seguro que ha existido. Windows Server 2003 ofrece fiabilidad al: Proporcionar una infraestructura integrada que ayuda a asegurar que su información de negocios estará segura. Proporcionar fiabilidad, disponibilidad, y escalabilidad para que usted pueda ofrecer la infraestructura de red que los usuarios solicitan.
Productivo	Ofrece herramientas que le permiten implementar, administrar y usar su infraestructura de red para obtener una productividad máxima. Windows Server 2003 realiza esto al: Proporcionar herramientas flexibles que ayuden a ajustar su diseño e implementación a sus necesidades organizativas y de red. Ayudarle a administrar su red proactivamente al reforzar las políticas, tareas automatizadas y simplificación de actualizaciones. Ayudar a mantener bajos los gastos generales al permitirles a los usuarios trabajar más por su cuenta.

Beneficio	Descripción
Conectado	Puede ayudarle a crear una infraestructura de soluciones de negocio para mejorar la conectividad con empleados, socios, sistemas y clientes. Windows Server 2003 realiza esto al: Proporcionar un servidor Web integrado y un servidor de transmisión de multimedia en tiempo real para ayudarle a crear más rápido, fácil y seguro una Intranet dinámica y sitios de Internet. Proporcionar un servidor de aplicaciones integrado que le ayude a desarrollar, implementar y administrar servicios Web en XML (eXtensible Markup Language; Lenguaje Marcado Extensible) más fácilmente. Brindar las herramientas que le permitan conectar servicios Web a aplicaciones internas, proveedores y socios.
Mejor economía	Cuando está combinado con productos Microsoft como hardware, software y servicios de los socios de negocios del canal brindan la posibilidad de ayudarle a obtener el rendimiento más alto de sus inversiones de infraestructura. Windows Server 2003 lleva a cabo esto al: Proporcionar una guía preceptiva y de fácil uso para soluciones que permitan poner rápidamente la tecnología a trabajar. Ayudarle a consolidar servidores aprovechando lo último en metodologías, software y hardware para optimizar la implementación de su servidor. Bajar el costo total de propiedad para recuperar rápido la inversión.

3.1.2 Características básicas de Windows Server 2003

Windows Server 2003 contiene tecnologías básicas construidas en base a las fortalezas de Windows 2000 Server para ofrecer un sistema operativo rentable y superior. El aprender sobre diferentes y nuevas tecnologías y características hacen de Windows Server 2003 una plataforma de servidor ideal para organizaciones de cualquier tamaño. El conocer como este sistema operativo de servidor seguro puede hacer que su organización y sus empleados sean más productivos y estén mejor conectados.

Seguro

Windows Server 2003 cuenta con la fiabilidad, disponibilidad, escalabilidad y seguridad que lo hace una plataforma altamente segura. IIS 6.0 (*Internet Information Services; Servicios de Información de Internet)* es un componente

importante de la familia Windows el cual está configurado para una máxima seguridad, sus características avanzadas incluyen: servicios de criptografía selectiva, autenticación de resumen avanzado, y acceso configurable de control de procesos.

Estas son algunas de las muchas características de seguridad en IIS 6.0 que le permiten llevar a cabo negocios con seguridad en la Web.

Disponibilidad

Windows Server 2003 ofrece una disponibilidad mejorada de soporte a *clustering*. Los servicios de clustering han llegado a ser esenciales para las organizaciones en cuanto a implementación de negocios críticos, comercio electrónico y aplicaciones de negocios en línea, porque proporcionan mejoras significativas en disponibilidad, escalabilidad y manejabilidad. La instalación y configuración de clustering es más fácil y más robusta en Windows Server 2003, mientras que algunas características de red mejoradas en el producto ofrecen mejor recuperación de fallos y un tiempo productivo alto del sistema.

La familia de Windows Server 2003 soporta clusters de servidor de hasta 8 nodos. Si uno de los nodos en un cluster no se puede usar debido a un fallo o por mantenimiento, inmediatamente otro nodo empieza a dar servicio, un proceso conocido como recuperación de fallos. Windows Server 2003 también soporta balanceo de carga de red, el cual nivela el tráfico de entrada dentro del Protocolo de Internet, a través de los nodos en un cluster.

Escalabilidad

Windows Server 2003 ofrece escalabilidad a través de "Scale-up", habilitado por SMP (*Symmetrical Multiprocessing; Multiprocesamiento Simétrico*) y "Scale-out", habilitado por clustering. Pruebas internas indican que, comparado con Windows 2000 Server, Windows Server 2003 da hasta un 140 por ciento de mejor desempeño en la administración de archivos y un rendimiento más significativo en varias otras características, incluyendo servicio Microsoft Active Directory

(Directorio Activo de Microsoft), servidor Web y componentes Terminal Server así como servicios de red.

Windows Server 2003 abarca desde soluciones de procesador únicas hasta sistemas de 32 vías. Esto soporta procesadores tanto de 32-bits como de 64 bits.

Fiabilidad

Los negocios han hecho crecer la tradicional red de área local al combinar redes internas, externas y sitios de Internet. Como resultado de esto, el aumento de seguridad en los sistemas es ahora más crítica que antes. Como parte del compromiso de Microsoft de brindar computación segura, la compañía ha revisado intensamente la familia Windows para identificar posibles fallos y debilidades. Windows Server 2003 ofrece muchas mejoras y características nuevas e importantes de seguridad entre las que se incluyen el tiempo de ejecución, esta función del software es un elemento clave de Windows Server 2003 que mejora la fiabilidad y ayuda a asegurar un entorno seguro. Esto reduce el número de fallas y huecos de seguridad causados por errores comunes de programación. Como resultado, hay menor vulnerabilidad de que ocurran ataques. El tiempo de ejecución de lenguaje común también verifica que estas aplicaciones puedan correr sin errores y verifica permisos de seguridad válidos, asegurando que el código realice solamente las operaciones correspondientes.

Productivo

En el corazón de cualquier organización de Tecnologías de la Información (TI), la habilidad que se tenga de administrar eficientemente los recursos de archivo e impresión, es lo que permitirá que estos estén disponibles y seguros para los usuarios. Al aumentar las redes en tamaño con más usuarios localizados en sitios cercanos, en ubicaciones remotas, o en compañías de socios, los administradores de TI enfrentan cada vez más carga pesada. La familia Windows ofrece servicios inteligentes de manejo de archivos e impresión con una funcionalidad y rendimiento elevado, permitiéndole reducir el costo total de propiedad.

Active Directory

En numerosas áreas, Windows Server 2003 tiene capacidades que pueden hacer que su organización y empleados sean más productivos. Servicios de impresión y archivos es un servicio de directorio de la familia de Windows Server 2003, el cual almacena información acerca de objetos en la red y hace que esta información sea fácil de encontrar por los administradores y usuarios proporcionando una organización lógica y jerárquica de información en el directorio. Windows Server 2003 trae muchas mejoras para Active Directory, haciéndolo mas versátil, fiable y económico de usar. En Windows Server 2003, Active Directory ofrece una escalabilidad y rendimiento elevado. Esto también le permite mayor flexibilidad para diseñar, implementar y administrar el directorio de su organización.

Servicios de Administración.

Mientras que la computación se ha proliferado en ordenadores de sobremesa y dispositivos portátiles, el costo real de mantenimiento de una red distribuida de ordenadores personales ha aumentado significativamente. Reducir el mantenimiento día a día a través de la automatización, es la clave para reducir costos de operación. Windows Server 2003 contiene varias herramientas importantes de administración automatizada como Microsoft Software Update Services y asistentes de configuración de servidor para ayudar a automatizar la implementación.

La Administración de Políticas de Grupo se hace más fácil con la nueva Consola para Administración de Políticas de Grupo, permitiendo que más organizaciones utilicen mejor el servicio Active Directory para sacar beneficio de sus poderosas características de administración. En conclusión, las herramientas de líneas de comandos permiten que los administradores realicen la mayoría de las tareas desde la consola de comandos.

Administración de almacenamiento

Windows Server 2003 introduce características nuevas y mejoradas herramientas para la administración del almacenamiento, haciendo que sea más fácil y más

seguro manejar y dar mantenimiento a discos y volúmenes, respaldar y recuperar datos, y conectarse a una red de almacenamiento

Terminal Services (Servicios Terminales)

Es un componente de Microsoft Windows Server 2003, se construye en el modo de servidor de aplicaciones en Windows 2000 Terminal Services, le permite enviar aplicaciones en Windows, virtualmente a cualquier dispositivo, incluyendo aquellos que no pueden correr Windows.

Conectado

Windows Server 2003 incluye características y mejoras nuevas para asegurarse de que su organización y usuarios permanezcan conectados.

Servicios Web XML

Los administradores y desarrolladores de aplicaciones Web demandan una plataforma Web rápida que sea tanto escalable como segura. Las mejoras significativas de arquitectura en IIS abarcan un modelo de procesos nuevo que en gran medida aumenta la fiabilidad, la escalabilidad y el desempeño. IIS está instalado predeterminadamente en estado seguro (Lock down). La seguridad se incrementa debido a que el administrador del sistema habilita y deshabilita funciones del sistema de acuerdo a requerimientos de la aplicación. En conclusión, el apoyo directo de edición de XML mejora la administración.

Comunicaciones y redes

Las comunicaciones y redes nunca han sido tan críticas para las organizaciones que enfrentan el reto de competir en el mercado global. Los empleados necesitan conectarse a la red desde cualquier lugar y cualquier dispositivo. Socios, vendedores y otros fuera de la red necesitan interactuar eficientemente con recursos clave, y la seguridad es más importante que nunca. Las nuevas características y mejoras en redes en la familia de Windows Server 2003 incrementan la versatilidad, manejabilidad y fiabilidad de infraestructura de red.

Servicios empresariales UDDI (Universal Description, Discovery and Integration; Descripción, Descubrimiento e Integración Universal,).

Windows Server 2003 incluye servicios empresariales UDDI, una infraestructura dinámica y flexible para servicios Web XML. Esta solución basada en estándares le permite a las compañías llevar a cabo sus propios servicios internos UDDI para redes de uso interno y externo. Los desarrolladores pueden encontrar y reutilizar fácil y rápidamente los servicios Web disponibles dentro de la organización.

Los administradores TI pueden catalogar y administrar los recursos programables de su red. Con servicios empresariales UDDI, las compañías pueden crear e implementar aplicaciones más inteligentes y seguras.

Servicios de Windows Media

Windows Server 2003 incluye los servicios de medios digitales más poderosos de la industria. Estos servicios son parte de la nueva versión de la plataforma de tecnologías de Microsoft Windows Media que también incluyen un nuevo reproductor de Windows Media, un codificador de Windows Media, códecs de audio y vídeo y un paquete para desarrollo de software de Windows Media.

3.2 SERVICIOS DE WINDOWS MEDIA

Con los Servicios de Windows Media 9 Series de Microsoft en Windows Server 2003, se puede entregar contenido a los usuarios a través de Internet o de una intranet. Los Servicios de Windows Media poseen dos interfaces administrativas que se pueden utilizar para configurar y administrar uno o varios servidores que estén ejecutando dicha aplicación.

3.2.1 Windows Media 9 Series

Windows Media 9 Series es el término que hace referencia a la familia de software multimedia digital desarrollado por Microsoft. Todas las series se han diseñado para funcionar de forma conjunta y proporcionar una experiencia multimedia digital óptima.

Los Servicios de Windows Media son una plataforma que se utiliza para transmitir contenido de audio y vídeo a los clientes a través de Internet o una intranet. Estos clientes pueden ser otros equipos o dispositivos que reproducen el contenido a través de un reproductor, como el Reproductor de Windows Media. Asimismo, pueden ser otros equipos en los que se ejecutan los Servicios de Windows Media (denominados servidores de Windows Media) y que transmiten el contenido a través de *proxy*, lo almacenan en caché o lo redistribuyen.

También pueden ser aplicaciones personalizadas, desarrolladas mediante el kit de desarrollo de software (SDK: *Software Development Kit*) de Windows Media.

El contenido que el servidor de Windows Media transmite a los clientes puede ser una secuencia en directo o material ya existente, como un archivo multimedia digital. Si se desea transmitir contenido en directo, el servidor se debe conectar a software de codificación, como el Codificador de Windows Media, capaz de difundir una secuencia en directo en formato compatible con el servidor.

Asimismo, puede transmitir contenido ya existente codificado con el Codificador de Windows Media, Microsoft Producer for PowerPoint, Windows Movie Maker, el Reproductor de Windows Media u otros programas de codificación de terceros.

3.2.2 Componentes de la plataforma

Los Servicios de Windows Media son ahora un servicio único que se ejecuta en Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition, y Windows Server 2003, Datacenter Edition. Sus componentes esenciales se han desarrollado con el Modelo de objetos componentes (COM: *Component Object Model*) para crear una arquitectura flexible fácilmente personalizable para aplicaciones específicas. Es compatible con una amplia gama de protocolos de control, incluidos el Protocolo de Transmisión en Tiempo Real (RTSP: *Real Time Streaming Protocol*), el protocolo MMS (*Multimedia Messaging Services; Sistema de Mensajería Multimedia)* y el Protocolo de Transferencia de Hipertexto (HTTP: *Hypertext Transfer Protocol*).

Esta plataforma cumple con los siguientes estándares del sector:

a) Instrumentación de la Administración de Windows (WMI: *Windows Management Instrumentation*) para el envío de mensajes y la notificación de sucesos de servidor.

b) SNMP (Protocolo de Manejo de Red Simple) para componentes de red.

c) XML, Modelo de Objetos de Documento (DOM: Document Object Model) y Lenguaje de Integración Multimedia Sincronizada (SMIL: *Synchronized Multimedia Integration Language)* 2.0 para la implementación de listas de reproducción.

d) MPEG (*Moving Picture Experts Group; Grupo de Expertos en Imágenes en Movimiento*) 1 y 2 para formatos de vídeo y audio.

La mayoría de las transmisiones por secuencias pueden realizarse utilizando los componentes básicos instalados con los Servicios de Windows Media. No obstante, es posible que para casos más avanzados sea necesario algún trabajo de programación e integración personalizado. Para programadores e integradores de sistemas, el kit de desarrollo de software (SDK) de los Servicios de Windows Media proporciona acceso a todos los elementos del servidor mediante una combinación de complementos, un modelo de objetos totalmente documentados y un rico conjunto de notificaciones de sucesos externos, todo diseñado para una personalización sencilla.

A medida que se explore el complemento de los Servicios de Windows Media y el Administrador de Servicios de Windows Media para el Web, encontrará una gran variedad de complementos para realizar diferentes tareas. Más de la mitad de las características del servidor se realizan mediante el uso de complementos. Si es necesario, se pueden desarrollar complementos personalizados a fin de integrar el servidor de Windows Media en otros sistemas. Por ejemplo, si dispone de una gran cantidad de contenido de ancho de banda elevado en una base de datos propietaria, se puede desarrollar un complemento de origen de datos para recuperarlo de la misma.

A medida que se evalúe la implementación del servidor de Windows Media, es posible que se decida por una solución personalizada. Todas las características que se pueden configurar en una interfaz administrativa se hallan expuestas en el modelo de objetos del servidor de Windows Media, documentado en el SDK del mismo. Con el modelo de objetos, se puede obtener acceso a la programación de cada uno de los contadores, interfaces, complementos, puntos de publicación y listas de reproducción.

De hecho, las interfaces administrativas se crearon con este modelo de objetos. Para obtener más información sobre la creación de aplicaciones personalizadas, ver el kit SDK de los Servicios de Windows Media, disponible en la página principal de Windows Media en el sitio Web de Microsoft.

Si se desea explorar las posibilidades de automatización de los Servicios de Windows Media, éste proporciona sucesos a través de SNMP y WMI. También son compatibles con las secuencias de comandos de línea de comando. Combinando secuencias de comandos en línea de comando y sucesos, se puede automatizar muchas de las tareas de administración del servidor.

3.2.3 Arquitectura de Complementos

Los Servicios de Windows Media admiten configuraciones del servidor personalizables mediante el uso de complementos. La mayoría de las características de los servicios se pueden implementar habilitando y configurando los complementos que se desean utilizar. Algunos complementos del sistema proporcionan características básicas y se habilitan de forma predeterminada. Se utilizan los complementos para realizar una gran variedad de tareas, incluidas la administración de protocolos, el análisis de datos, la autenticación, la autorización y el almacenamiento en archivos; aplicar un complemento a todo el servidor de Windows Media o a un punto de publicación específico del servidor habilitándolo para el nivel apropiado.

También puede modificar la configuración del complemento para cada uno de los servidores o puntos de publicación que esté administrando.

Los complementos de los Servicios de Windows Media se dividen en categorías según la función que desempeñan (Tabla 3.2). Cada categoría contiene varios tipos de complemento.

Tabla 3.2.- Categorías existentes de los complementos de los Servicios de Windows Media

Categoría de complemento	Descripción
Archivado	Se utiliza para almacenar el contenido que se transmite desde un punto de publicación de difusión en un archivo.
Autenticación	Se utiliza para validar las credenciales de los clientes antes del envío de datos adicionales a los mismos.
Autorización	Se utiliza para permitir o denegar el acceso de los clientes al contenido.
Administración de proxy-caché	Se utiliza para controlar las políticas de proxy y caché del equipo.
Protocolo de control	Se utiliza para controlar los datos enviados entre los clientes y los servidores.
Origen de datos	Se utilizan para recibir datos de un codificador, sistema de archivos u origen de red.
Notificación de sucesos	Se utiliza para controlar y personalizar la forma en que el servidor responde a los sucesos internos.
Registro	Se utiliza para registrar la actividad de clientes y servidores.
Analizador de multimedia	Se utiliza para permitir al servidor la conversión de diferentes tipos de archivos multimedia digitales o secuencias en tiempo real.
Transmisión por secuencias de multidifusión	Se utiliza para controlar la entrega de contenido a través de transmisiones por secuencias de multidifusión. Este complemento debe configurarse para cada punto de publicación con el que se realicen entregas de multidifusión.
Analizador de listas de reproducción	Se utiliza para permitir al servidor la conversión de diferentes tipos de lista de reproducción.
Transformación de lista de reproducción	Se utiliza para cambiar la forma como se transmite el contenido desde una lista de reproducción o directorio.
Transmisión por secuencias de unidifusión	Se utiliza para controlar las entregas de contenido a través de transmisiones por secuencias de unidifusión.

Puede utilizar complementos de terceros y complementos personalizados con los Servicios de Windows Media a fin de implementar soluciones de transmisión personalizadas, como servidores proxy-caché, formatos de transmisión múltiple, aplicaciones de registro personalizadas y almacenamiento especializado de datos.

Puede obtener una lista de complementos de terceros para los Servicios de Windows Media en la página del Centro de asociados de Windows Media de Microsoft del sitio Web de Microsoft. Puede descargar el kit de desarrollo de software (SDK) de los Servicios de Windows Media en la página *Windows Media Technologies Application Development* en el mismo sitio.

Nota: los complementos personalizados o de terceros deben ubicarse en un directorio protegido para evitar alteraciones. El directorio protegido puede ser cualquier directorio configurado para denegar el permiso de escritura a los usuarios no autorizados.

3.2.4 Requisitos del sistema

La instalación predeterminada de los Servicios de Windows Media instala el siguiente software en el disco duro del servidor:

a) Servicio de Servicios de Windows Media. Este dispositivo permite transmitir contenido multimedia digital a los clientes a través de una intranet o de Internet.

b) Complemento de los Servicios de Windows Media. Este complemento permite administrar y configurar los Servicios de Windows Media a través de MMC *(Microsoft Management Console; Consola de Gestión de Microsoft).*

Se debe considerar también la posibilidad de instalar los componentes opcionales siguientes en el servidor y obtener así soporte técnico para utilizar características adicionales:

1. *Administrador de Servicios de Windows Media para la Web.* Este componente ofrece soporte técnico para la administración remota basada en el explorador

del servidor de Windows Media. Al seleccionar este componente, se instala un Servidor de Páginas Activas (ASP) para utilizar con IIS. Una vez instalado, el sitio de administración de los Servicios de Windows Media aparece en la carpeta de sitios Web de IIS. El Administrador de Servicios de Windows Media para el Web también se puede instalar independientemente del servicio de Servicios de Windows Media.

2. *Agente de registro de anuncios y de multidifusión.* Este componente permite registrar estadísticas de reproductores que se conectan al contenido a través de un servidor Web. Al seleccionar este componente, se instala una extensión del servidor de Servicios de Windows Media que recoge la información de registro y la escribe en un archivo de registro en la ubicación que se especifique.

3.2.5 El servicio y complemento de los servicios de Windows Media

La instalación predeterminada de los Servicios de Windows Media incluye el servicio y el complemento del mismo nombre. Este complemento proporciona un control completo del servidor y permite administrar grupos de servidores de Windows Media utilizando MMC.

La Tabla 3.3 muestra los requisitos de sistema necesarios para el equipo que ejecute la asistencia de los Servicios de Windows Media y el complemento de los mismos:

Tabla 3.3.- Requisitos del Sistema para la instalación de los Servicios Windows Media

Componente	Requisito	Recomendación
Sistema operativo	Windows Server 2003, Standard Edition	Windows Server 2003, Enterprise Edition, o Windows Server 2003, Datacenter Edition
Procesador	233 megahercios (MHz)	550 MHz o superior
Memoria	256 megabytes (MB) de RAM	1 gigabyte (GB) de RAM o superior

Componente	Requisito	Recomendación
Tarjeta de interfaz de red	Tarjeta Ethernet y Protocolo de control de transmisión/Protocolo Internet (TCP/IP)	Idéntico
Espacio libre en el disco duro	21 MB (6 MB para archivos del sistema y 15 MB para la instalación); espacio en disco adecuado para el almacenamiento del contenido	21 MB (6 MB para archivos del sistema y 15 MB para la instalación); 500 MB para el almacenamiento del contenido

El complemento de los Servicios de Windows Media se puede agregar a los clientes que reúnan los requisitos mostrados en la tabla 3.4 y posean los derechos administrativos adecuados.

Tabla 3.4.- Requisitos del Sistema para la instalación de los Servicios de Windows Media en los Clientes

Componente	Requisito
Sistema operativo	Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition, Windows Server 2003, Datacenter Edition
Software	Microsoft Management Console

3.2.6 Administrador de servicios de Windows Media para la Web

El Administrador de Servicios de Windows Media para la Web es una interfaz basada en un explorador que utiliza páginas ASP alojadas por IIS. Este conjunto de páginas ASP se ubica en el sitio de administración de Windows Media en IIS.

Para admitir la administración de los Servicios de Windows Media desde equipos remotos, se instala el Administrador de Servicios de Windows Media para el Web en un servidor de red. Éste puede ser un servidor de Windows Media o un equipo que ejecute Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition, o Windows Server 2003, Datacenter Edition, con los IIS de Microsoft instalados.

En la Tabla 3.5 se muestran los requisitos del sistema para el servidor que aloja el Administrador de Servicios de Windows Media para la Web:

Tabla 3.5.- Requisitos del Sistema para la instalación de los Servicios de Windows Media para la Web en el Servidor Administrador

Componente	Requisito	Recomendación
Sistema operativo	Windows Server 2003, Standard Edition	Windows Server 2003, Enterprise Edition, o Windows Server 2003, Datacenter Edition
Procesador	233 megahercios (MHz)	550 MHz o superior
Memoria	256 megabytes (MB) de RAM	1 gigabyte (GB) de RAM o superior
Tarjeta de interfaz de red	Tarjeta Ethernet y Protocolo de control de transporte/Protocolo Internet (TCP/IP)	Igual
Espacio libre en disco	3,4 MB	3,4 MB
Software	Servicios de Internet Information Server (IIS) de Microsoft compatible con el Administrador de Servicios de Windows Media para el Web basado en explorador	Igual
Sistema de archivos	NTFS	Igual

Una vez instalado el Administrador de Servicios de Windows Media para el Web en el servidor, podrán obtener acceso al mismo los clientes que cumplan con los requisitos mostrados en la tabla 3.6 y que dispongan de los permisos administrativos adecuados.

Tabla 3.6.- Requisitos del Sistema para la instalación de los Servicios de Windows Media para la Web en los Clientes

Componente	Requisito
Sistema operativo	Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000, Windows XP o Windows Server 2003
Software	Microsoft Internet Explorer 5.5 o posterior, o Netscape Communicator 6.0 o posterior

Notas:

- Para funcionar correctamente, el sitio de administración de Windows Media debe ser capaz de instalar cookies en el equipo remoto del cliente, por lo que es necesario asegurarse de que la opción de seguridad del explorador del cliente las admite.
- Hay que leer detenidamente la información que se muestra en Protección del sitio de administración de Windows Media para garantizar la seguridad del sitio Web.
- Los documentos ASP no son compatibles con la estructura de archivos FAT32 (*File Allocation Table; Tabla de Asignación de Archivos*). Si se tienen problemas para visualizar el Administrador de Servicios de Windows Media para el Web, comprobar que el sistema de archivos no utiliza la arquitectura FAT32.

3.2.7 Agente de registro de anuncios y de multidifusión

Para registrar las estadísticas de los reproductores que se conectan al servidor Web para recibir transmisiones por secuencias de multidifusión o de contenido publicitario, se instala el Agente de registro de anuncios y de multidifusión en un servidor de la red. Éste puede ser un servidor de Windows Media o cualquier otro equipo con Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition, o Windows Server 2003, Datacenter Edition, que tenga instalado IIS. El Agente de registro de anuncios y de multidifusión es una extensión de la aplicación IIS que utiliza Wmsiislog.dll para recopilar información de los reproductores. Wmsiislog.dll se instala en la carpeta *%unidadsistema%\WMPub\Wmiislog*. En la Tabla 3.7 se detallan los requisitos del sistema que debe cumplir el equipo para poder alojar el Agente de registro de anuncios y de multidifusión:

Tabla 3.7.- Requisitos del Sistema para la instalación del Agente de Registro de Anuncios y de Multidifusión

Componente	Requisito	Recomendación
Sistema operativo	Windows Server 2003, Standard Edition	Windows Server 2003, Enterprise Edition, o Windows Server 2003, Datacenter Edition
Procesador	233 megahercios (MHz)	550 MHz o superior
Memoria	256 megabytes (MB) de RAM	1 gigabyte (GB) de RAM o superior
Tarjeta de interfaz de red	Tarjeta Ethernet y Protocolo de control de transporte/Protocolo Internet (TCP/IP)	Ídem
Software	Servicios de Internet Information Server (IIS) de Microsoft	Ídem

3.2.8 Implementación de los Servicios de Windows Media

Existen bastantes casos en los que se pueden implementar los Servicios de Windows Media. Algunos ejemplos que deben tenerse en cuenta son: demostraciones de productos en directo, programas de televisión y películas interactivas, conferencias de clientes en tiempo real, historias en noticias de última hora, tiendas de vídeo de banda ancha y presentaciones de formación interactivas. Una vez que el contenido está accesible a través de Internet, el número de clientes que puede descubrirlo y solicitarlo es enorme. Al planear la implementación, se debe prever la reacción del servidor en aquellas situaciones en las que se vea inundado de solicitudes de contenido. Hay que tener en cuenta los siguientes requisitos al evaluar la implementación:

1. Escalabilidad. El diseño de los Servicios de Windows Media es escalable para admitir diferentes implementaciones, desde pequeñas emisoras de radio en Internet con cientos de solicitudes de conexión hasta sitios Web de medios de transmisión de gran tamaño que generan millones de solicitudes. Se puede administrar grupos de servidores y puntos de publicación, y servidores únicos y

puntos de publicación.

2. Seguridad. Para asegurar ciertos contenidos del servidor de Windows Media que permitan sólo que algunos clientes concretos se conecten. Los Servicios de Windows Media son compatibles con varios métodos de autenticación y autorización que permiten controlar el acceso al contenido.
3. Calidad de la secuencia. Cuantos más clientes se conecten al servidor, el ancho de banda disponible puede disminuir. Además, la carga del servidor puede sobrepasar la capacidad del procesador para servir el contenido. Si transmite contenido de vídeo, hay que probar una codificación mediante vídeo con múltiples velocidades de bits para que el ancho de banda se pueda acomodar según sea necesario.

3.3 CODIFICADOR DE WINDOWS MEDIA

El Codificador de Windows Media de Microsoft 9 Series es una eficaz herramienta de producción para convertir audio y vídeo en directo o pregrabado en archivos de Windows Media o en secuencias.

La siguiente sección presenta información conceptual acerca del proceso de codificación y proporciona los pasos que deben seguirse para utilizar el Codificador de Windows Media. Se incluye información acerca de cómo configurar una sesión de codificación mediante unos sencillos pasos que permitan utilizar los inicios rápidos o el Asistente para nueva sesión. También se incluye información acerca de las novedades de esta versión del Codificador de Windows Media, las características requeridas y los requisitos de hardware y software. Por último, se describen los diversos páneles que conforman la interfaz del Codificador.

3.3.1 Características requeridas

La Tabla 3.8 proporciona información acerca de las características del Codificador de Windows Media que presentan requisitos específicos de códec, sistema operativo o Reproductor de Windows Media de Microsoft.

Tabla 3.8.- Características del Codificador de Windows Media

Característica	Reproductor de Windows Media			Sistemas operativos	Códecs
	6.4	7.1/Windows XP	9 Series		
Vídeo de salida entrelazado			X	Microsoft Windows XP	Windows Media Vídeo 9
Salida de píxeles no cuadrados			X		
Contenido MBR de múltiple resolución			X		
MBR audio			X		
Compatibilidad con DRM	X	X	X		
Audio de varios canales			X	Microsoft Windows XP	Windows Media Audio 9 Professional o Windows Media Audio 9 Lossless
Audio de alta resolución (24 bits, 96 kHz)[1]			X	Microsoft Windows XP	Windows Media Audio 9 Professional
Control de intervalo dinámico			X	Microsoft Windows XP	Windows Media Audio 9 Professional
codificación CBR (1 ó 2 pasadas)	X	X	X		Ver tabla 3.9
VBR basada en la calidad		X	X		Ver tabla 3.9
VBR basada en la velocidad de bits		X	X		Ver tabla 3.9
VBR basada en la velocidad máxima de bits		X	X		Ver tabla 3.9

Los Reproductores o sistemas operativos anteriores procesarán contenido a 16 bits y 48 kHz. Se debe tomar en cuenta que el contenido codificado con los códecs Windows Media Audio y Vídeo 9 Series (excepto en el caso del códec Windows Media Audio 9) no es compatible con el Reproductor de Windows Media versión 6.4. En el caso del Reproductor de Windows Media 7.1 y el de Windows Media

para Windows XP, el contenido codificado con cualquiera de los códecs requiere que los usuarios descarguen el códec antes de la reproducción. El contenido codificado, utilizando la codificación VBR con el códec Windows Media Audio 9, puede dar problemas o provocar silencio durante la reproducción en el Reproductor de Windows Media versión 6.4. En el caso del Reproductor de Windows Media versión 7.1 y el de Windows Media para Windows XP, el contenido codificado con el códec Windows Media Audio 9 no requiere que un usuario descargue el códec.

Tabla 3.9.- Métodos de Codificación Admitidos para los Códecs que se incluyen en el Codificador de Windows Media

Códec	CBR de 1 pasada	CBR de 2 pasadas	VBR basada en la calidad	VBR basada en la velocidad de bits	VBR basada en la velocidad máxima de bits
Windows Media Audio 9 Professional	Sí	Sí	Sí	Sí	Sí
Windows Media Audio 9 Lossless	No	No	Sí	No	No
Windows Media Audio 9	Sí	Sí	Sí[1]	Sí[1]	Sí[1]
Windows Media Audio 9 Voice	Sí	No	No	No	No
Windows Media Vídeo 9	Sí	Sí	Sí	Sí	Sí
Windows Media Vídeo 8.1	Sí	Sí	Sí	Sí	Sí
Windows Media Vídeo 7	Sí	Sí	Sí	Sí	Sí
Windows Media Vídeo 9 Screen	Sí	No	Sí	No	No

3.3.2 Vistas del Codificador

La ventana principal del Codificador de Windows Media tiene varios páneles que proporcionan información acerca de la sesión en curso. Los páneles que aparecen cuando se codifica dependen del tipo de contenido codificado, el número de orígenes configurados para la sesión y las preferencias personales. Pueden visualizarse los páneles adicionales o bien ocultar los que se muestran. Los cambios que realizados en la ventana se guardarán de una sesión a otra.

- Pánel de propiedades. Incluye propiedades para ajustar la configuración de la sesión en curso o para configurar una sesión personalizada.
- Pánel Vídeo. Muestra el contenido que se está configurando. Según el tipo de contenido, se puede personalizar la ventana para mostrar el contenido previo a la codificación, el contenido codificado o ambos. En algunos casos, el contenido del origen o la salida codificada no se muestran durante la codificación.
- Pánel Orígenes. Muestra una lista de todos los orígenes de la sesión en curso. Mientras codifica se puede pasar de un origen a otro haciendo clic en el botón del origen que se desee.
- Pánel Audio. Contiene controles que permiten supervisar y ajustar el volumen de la secuencia de audio que se está codificando.
- Pánel Dispositivo. Aparece cuando se tiene un dispositivo conectado al equipo a través de un puerto IEEE (Institute of Electrical and Electronics Engineers; Instituto de Ingenieros Eléctricos y Electrónicos) 1394 o un puerto COM que utilice un grabador de cintas de vídeo (VTR, Vídeo Tape Recorder; Grabadora de Cintas de Vídeo) compatible con el protocolo Sony RS422. Se pueden controlar las funciones de reproducción, pausa, detención, avance rápido, rebobinado y expulsión del dispositivo mostrado en el pánel. También se pueden crear una EDL (Edit Decision List; Lista de Decisiones de Edición) para que codifique automáticamente segmentos de tiempo específicos del contenido en una o varias cintas de vídeo.

- Pánel Monitor. Contiene información acerca del estado de la sesión.
- Pánel Secuencia de comandos. Aparece si se ha habilitado secuencias de comandos como tipo de origen al configurar la sesión en curso. Desde este pánel, se puede insertar una secuencia de comandos en la secuencia durante la codificación.

3.3.3 Utilidades del Codificador.

En el Codificador de Windows Media se incluyen cuatro utilidades:

- Editor de perfiles de Windows Media. Se utiliza para crear perfiles personalizados para utilizarlos en sesiones de codificación.
- Editor de archivos de Windows Media. Esta herramienta, denominada anteriormente Indizador de formato ASF (*Advanced Streaming Format; Formato de Difusión Avanzada*) de Windows Media, se utiliza para editar un archivo de Windows Media. Por ejemplo, recortar los puntos inicial y final del archivo, agregar marcadores y secuencias de comandos, controlar el intervalo dinámico del contenido de audio y, en el caso de los archivos de audio de varios canales, controlar cómo se reducen para la reproducción en estéreo.
- Editor de secuencia de Windows Media. Se utiliza esta herramienta para dividir o combinar secuencias de archivos de Windows Media existentes y crear un archivo a partir de las mismas. Por ejemplo, dividir un archivo MBR en varios archivos de velocidad de bits única. Otra opción es crear varios archivos, cada uno con la misma secuencia de vídeo, pero una secuencia de audio diferente (por ejemplo, para crear un único archivo en varios idiomas).
- Secuencia de comandos de codificación de Windows Media. Esta utilidad de línea de comandos (Wmcmd.vbs), denominada anteriormente Windows Media Encoding Utility, se utiliza para codificar y difundir contenido. La utilidad se instala en la misma ubicación que el Codificador, C:\Archivos de programa\Componentes de Windows Media\Codificador.

3.3.4 Códecs y Sesiones

En esta sección se proporciona información general acerca del trabajo con el Codificador de Windows Media 9 Series. El contenido de audio y vídeo sin comprimir puede consumir mucho ancho de banda cuando se transfieren o crean archivos de gran tamaño. Al comprimir el contenido, puede difundirse por anchos de banda de Internet comunes o guardarse en un archivo de Windows Media de un tamaño razonable. Para comprimir el contenido, se aplican algoritmos de compresión a los datos, teniendo en cuenta la calidad de salida deseada y el ancho de banda disponible. Antes de reproducirse el contenido, se descomprime utilizando algoritmos de descompresión. Estos algoritmos de compresión y descompresión se llaman códecs. La tabla 3.10 proporciona información más detallada sobre los códecs disponibles en el Codificador de Windows Media.

Tabla 3.10.- Códecs disponibles en el Codificador de Windows Media

Códec	Descripción
Windows Media Audio 9 Professional	Proporciona una experiencia de sonido envolvente completo y un control de intervalo dinámico. Reduce de forma inteligente el audio de varios canales a dos (estéreo) o 1 (mono), según la configuración del altavoz del dispositivo reproductor. velocidades de datos de 128 a 768 Kbps.
Windows Media Audio 9 Lossless	Proporciona codificación sin pérdidas del contenido de audio. Admite codificación de audio de varios canales y control dinámico de intervalos.
Windows Media Audio 9	Proporciona una mejora del 20 por ciento en la compresión con relación al códec Windows Media Audio 8. Admite la codificación de audio VBR.
Windows Media Audio 9 Voice	Ofrece calidad superior para el contenido de audio con énfasis en la voz. Proporciona codificación en modo mezclado de voz y música. Velocidades de datos inferiores a 20 Kbps.
Windows Media Vídeo 9	Crea vídeos de alta calidad para su transmisión, descarga y reproducción y entrega con formato físico. Proporciona de un 15 a un 50 por ciento de mejora en la compresión con relación al códec Windows Media Vídeo 8.1, Reproduce contenido entrelazado en televisiones y descodificadores.

Códec	Descripción
Windows Media Vídeo 8.1	Admite una amplia variedad de anchos de banda de red. Elimina el entrelazado del contenido antes de la codificación.
Windows Media Vídeo 7	Permite a los usuario del códec Windows Media 7 ver contenido de vídeo codificado sin necesidad de descargar primero los códecs más actualizados. Se trata de la mejor elección cuando el equipo de codificación no cumple los requisitos de rendimiento de los códecs de vídeo de Windows Media más recientes.
Windows Media Vídeo 9 Screen	Proporciona un control mejorado de imágenes sombreadas, movimiento de pantalla y desplazamiento para capturas de pantalla. Admite la codificación VBR y CBR de 1 pasada sin descartar cuadros. Este códec está completamente optimizado tanto para escenarios de transmisión por secuencias como de descarga y reproducción.

Para poder codificar, es preciso configurar una sesión de codificación. Entre las tareas de configuración se incluyen:

- Especificar el origen del contenido de audio o vídeo. El origen puede estar en dispositivos, archivos o ambos. También puede capturar pantallas directamente desde el escritorio.
- Elegir la opción de salida. Seleccionar entre difundir el contenido o codificarlo en un archivo. Si difunde el contenido, se puede insertar la secuencia en un servidor de Windows Media y habilitar los servidores y Reproductores de Windows Media para que extraigan la secuencia del Codificador. También se puede elegir archivar una copia de la difusión para utilizarla posteriormente.

Asimismo, hay que comprobar la configuración de la calidad y la compresión antes de realizar la codificación. Se aplicará la configuración predeterminada, aunque puede ser preciso ajustarla para que se adapte a las necesidades. Por ejemplo, si se piensa distribuir el contenido para que se descargue y reproduzca en un equipo, se debe utilizar la codificación VBR basada en la velocidad de bits y establecer el nivel de calidad de audio y vídeo en una tasa de bits más elevada.

Después de identificar el origen del contenido y especificar la salida, se disponen de varias opciones para personalizar la sesión. Por ejemplo, optimizar el audio o el vídeo para mejorar la calidad del contenido codificado.

Cuando se ha acabado de configurar la sesión para adaptarla a las necesidades, se puede empezar la codificación. Si se desea volver a ejecutar la sesión, se puede guardar en un archivo de sesión, antes o después de efectuar la codificación.

3.3.5 Codificación CBR o VBR

El Codificador de Windows Media permite codificar contenido de audio y vídeo a una velocidad de bits constante (CBR) o variable (VBR).

Codificación CBR

La codificación CBR ofrece mejores resultados al trabajar con la transmisión por secuencias. En ella, la velocidad de bits se mantiene bastante constante y similar a la velocidad de bits final durante toda la secuencia, dentro de un período reducido determinado por el tamaño del búfer. La desventaja es que la calidad del contenido codificado no es constante. Dado que algunos fragmentos del contenido son más difíciles de comprimir que otros, algunas partes de una secuencia CBR son de menor calidad. Además, la codificación CBR proporciona una calidad desigual de una secuencia a otra. En general, las variaciones en la calidad son más pronunciadas al utilizar velocidades de bits inferiores.

Codificación VBR

La codificación VBR es más ventajosa cuando se codifica contenido que es una mezcla de datos simples y complejos, por ejemplo, un vídeo que cambia entre cámara lenta y cámara rápida. Con la codificación VBR, se asignan automáticamente menos bits a partes menos complejas del contenido, dejando bits suficientes disponibles para producir una buena calidad para partes más complicadas. Esto significa que el contenido que tiene una complejidad consistente (por ejemplo, una noticia del telediario) no se beneficiaría de la

codificación VBR. Cuando se utiliza con contenido mezclado, la codificación VBR produce un resultado codificado mejor, tratándose del mismo tamaño de archivo al compararlo con la codificación CBR. En algunos casos, se puede terminar obteniendo un archivo codificado mediante VBR que tenga la misma calidad que un archivo codificado mediante CBR con la mitad de tamaño de archivo.

3.4 DREAMWEAVER

Macromedia Dreamweaver MX 2004 es un editor HTML (*HyperText Markup Language; Lenguaje de Marcado de Hipertextos*) profesional para diseñar, codificar y desarrollar sitios, páginas y aplicaciones Web. Tanto si se desea controlar manualmente el código HTML como trabajar en un entorno de edición visual, Dreamweaver proporciona útiles herramientas que mejoran la experiencia de creación Web.

Las funciones de edición visual de Dreamweaver permiten crear páginas de forma rápida, sin escribir una sola línea de código. Se pueden ver todos los elementos activos del sitio y arrastrarlos desde un pánel fácil de usar directamente hasta un documento, agilizar el flujo de trabajo de desarrollo mediante la creación y edición de imágenes en Macromedia Fireworks o en otra aplicación de gráficos y su posterior importación directa a Dreamweaver, o bien añadir objetos Macromedia Flash.

Dreamweaver también ofrece un entorno de codificación con todas las funciones, que incluye herramientas para la edición de código (tales como coloreado de código y terminación automática de etiquetas) y material de referencia sobre HTML, CSS (*Cascading Style Sheets*), JavaScript, CFML (ColdFusion Markup Language), ASP y JSP (JavaServer Pages). La tecnología Roundtrip HTML de Macromedia importa los documentos con código manual HTML sin modificar el formato del código. Posteriormente, si se desea se puede formatear el código con el estilo que preferido.

Dreamweaver permite crear aplicaciones Web dinámicas basadas en bases de datos empleando tecnologías de servidor como CFML, ASP.NET, ASP, JSP y PHP.

3.4.1 Diseño del Espacio de Trabajo de Dreamweaver

En el espacio de trabajo de Dreamweaver todas las ventanas y páneles están incluidos en una única ventana de la aplicación de mayor tamaño, permite ver las propiedades de los documentos y los objetos. Además, coloca muchas de las operaciones más frecuentes en barras de herramientas para realizar cambios en los documentos rápidamente (Figura 3.1).

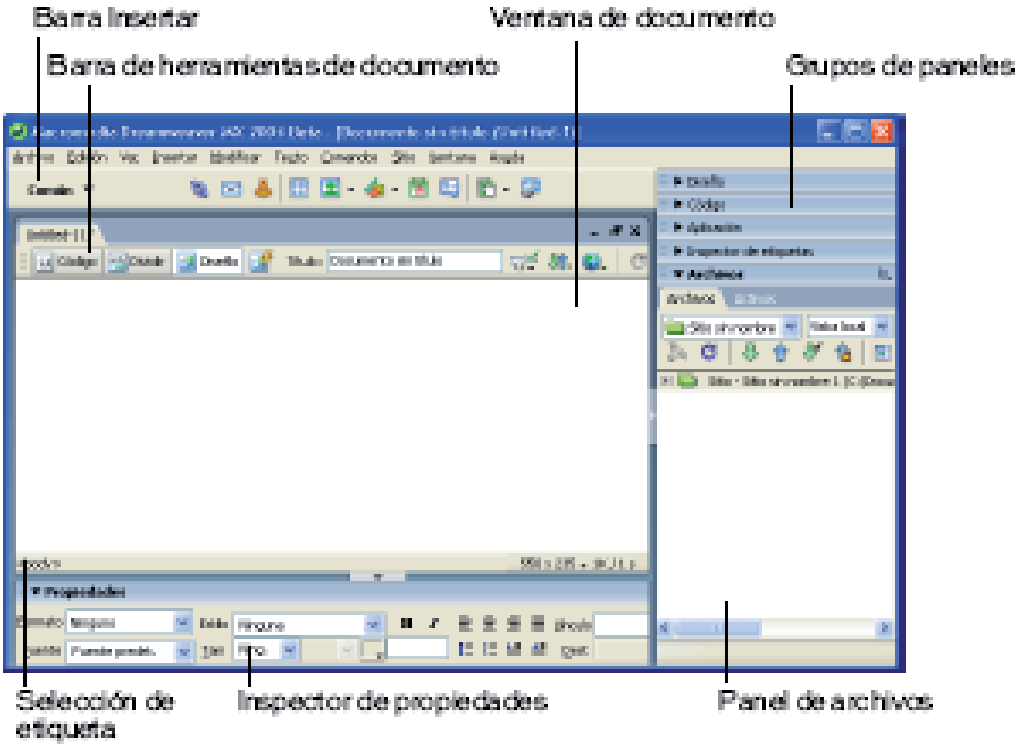

Figura 3.1.- Espacio de trabajo de Dreamweaver

3.4.2 Elementos del Espacio de Trabajo de Dreamweaver

La página de inicio permite abrir un documento reciente o crear un documento nuevo. La barra Insertar contiene botones para la inserción de diversos tipos de "objetos", como imágenes, tablas y capas, en un documento. Cada objeto es un fragmento de código HTML que permite establecer diversos atributos al insertarlo. Por ejemplo, poder insertar una tabla haciendo clic en el botón Tabla de la barra Insertar o insertar objetos utilizando el menú Insertar en lugar de la barra Insertar.

La barra de herramientas de documento contiene botones que proporcionan opciones para diferentes vistas de la ventana de documento (como la vista Diseño y la vista Código), diversas opciones de visualización y algunas operaciones comunes como la obtención de una vista previa en un navegador.
La barra de herramientas Estándar (que no aparece en el diseño de espacio de trabajo predeterminado) contiene botones para las operaciones más habituales de los menús Archivo y Edición: Nuevo, Abrir, Guardar, Guardar todo, Cortar, Copiar, Pegar, Deshacer y Rehacer. Para mostrar la barra de herramientas Estándar, seleccione Ver > Barras de herramientas > Estándar.

La ventana de documento muestra el documento actual mientras lo está creando y editando.

El inspector de propiedades permite ver y cambiar las propiedades del objeto o texto seleccionado. Cada tipo de objeto tiene diferentes propiedades. El inspector de propiedades no está ampliado de forma predeterminada en el diseño del espacio de trabajo del codificador.

El selector de etiquetas, que aparece en la barra de estado en la parte inferior de la ventana de documento, muestra la jerarquía de etiquetas que rodean a la selección actual. Haga clic en cualquier etiqueta de la jerarquía para seleccionar la etiqueta y todo su contenido.

Los grupos de páneles son conjuntos de páneles relacionados apilados bajo un encabezado común. Para ampliar un grupo de páneles, hacer clic en la flecha de

ampliación situada a la izquierda del nombre del grupo; para desacoplar un grupo de páneles, arrastrar el punto de sujeción situado en el borde izquierdo de la barra de título del grupo.

El pánel de archivos permite gestionar los archivos y las carpetas, tanto si forman parte de un sitio de Dreamweaver como si se encuentran en un servidor remoto. El pánel de archivos también proporciona una vista de todos los archivos del disco local, como ocurre en el Explorador de Windows.

La vista Diseño es un entorno para el diseño visual de la página, la edición visual y el desarrollo rápido de aplicaciones. En esta vista, Dreamweaver muestra una representación visual del documento completamente editable, similar a la que aparecería en un navegador. Se puede configurar la vista de diseño para que muestre el contenido dinámico mientras se trabaja en el documento.

La vista Código es un entorno de codificación manual para escribir y editar código HTML, JavaScript o código de lenguaje de servidor, como por ejemplo PHP o CFML y otros tipos de código. Es posible ver el mismo documento en las dos vistas, Código y Diseño, en una sola ventana de documento. Cuando la ventana de documento tiene una barra de título, ésta muestra el título de la página y entre paréntesis el nombre y la ruta del archivo. Si se han realizado cambios que aún no se han guardado, después del nombre del archivo Dreamweaver incluye un asterisco. Cuando se maximiza la ventana de documento en el diseño integrado de espacio de trabajo no aparece la barra de título; en este caso, el título de la página y el nombre y la ruta del archivo aparecen en la barra de título de la ventana principal del espacio de trabajo. Cuando una ventana de documento está maximizada, aparecen fichas en la parte superior de la misma con los nombres de archivo de todos los documentos abiertos. Para cambiar a un documento, hacer clic en su ficha.

La barra de herramientas Documento (Figura 3.2) contiene botones que permiten alternar entre diferentes vistas del documento rápidamente: vista Código, vista Diseño y una vista dividida que muestra las vistas Código y Diseño, también

cuenta con algunos comandos y opciones relativas a la visualización del documento y a su transferencia entre los sitios local y remoto.

Figura 3.2.- Barra de herramientas documento de Dreamweaver

En la barra de herramientas Documento, aparecen las siguientes opciones:

- Mostrar vista de código: sólo muestra la vista Código en la ventana de documento.
- Mostrar vistas de código y diseño: muestra la vista Código en una parte de la ventana de documento y la vista Diseño en la otra parte. Cuando se seleccione esta vista combinada, se encontrará disponible la opción Vista de diseño encima del menú Ver. Esta opción especifica qué vista debe aparecer en la parte superior de la ventana de documento.
- Mostrar vista de diseño sólo muestra la vista Diseño en la ventana de documento.

La Depuración del servidor: muestra un informe que ayuda a depurar la página de ColdFusion actual. El informe contiene los errores de la página, si los hay.

Título: permite introducir un título para el documento, que aparecerá en la barra de título del navegador. Si el documento ya tiene título, éste aparecerá en dicho campo.

No hay errores de comprobación de navegador: permite comprobar la compatibilidad con distintos navegadores.

Administración de archivos: muestra el menú emergente Administración de archivos.

Vista previa/Depurar en explorador: permite ver una vista previa del documento o depurarlo en un navegador. Seleccionar un navegador en el menú emergente.

Actualizar vista de diseño: actualiza la vista Diseño tras realizar cambios en la vista Código. Los cambios realizados en la vista Código no aparecerán de forma automática en la vista Diseño hasta que se efectúen acciones determinadas, como guardar el archivo o hacer clic en este botón.

Ver opciones: permite definir las opciones de las vistas Código y Diseño, y establecer qué vista va a aparecer en la parte superior de la ventana. Las opciones del menú corresponden a la vista actual: la vista Diseño, la vista Código o ambas.

La barra de herramientas Estándar contiene botones para las operaciones más habituales de los menús Archivo y Edición: Nuevo, Abrir, Guardar, Guardar todo, Cortar, Copiar, Pegar, Deshacer y Rehacer. Estos botones se utilizan del mismo modo que los comandos de menú equivalentes.

La barra de estado (Figura 3.3), situada en la parte inferior de la ventana de documento, proporciona información adicional sobre el documento que está creando.

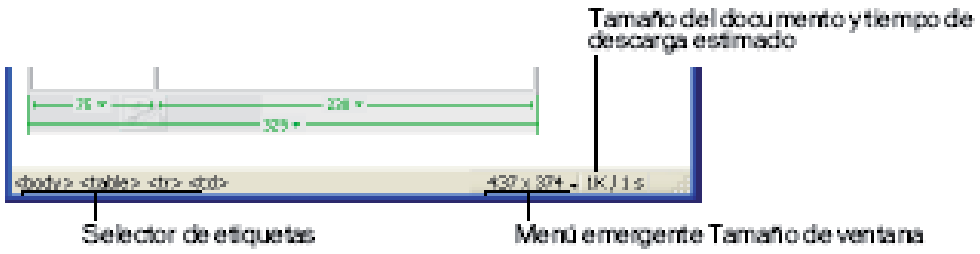

Figura 3.3 Barra de estado de Dreamweaver

El selector de etiquetas muestra la jerarquía de etiquetas que rodea a la selección actual. Se da clic en cualquier etiqueta de la jerarquía para seleccionar la etiqueta y todo su contenido. Haga clic en <body> para seleccionar todo el cuerpo del documento. Para definir los atributos class o ID para una etiqueta en el selector de etiquetas, se da clic con el botón de derecho del ratón y elija una clase o un ID del menú contextual.

El menú emergente Tamaño de ventana (que sólo aparece en la vista Diseño) permite cambiar el tamaño de la ventana de documento para que adopte dimensiones predeterminadas o personalizadas.

A la derecha del menú emergente Tamaño de ventana aparecen la estimación del tamaño del documento y del tiempo de descarga de la página, incluidos todos los archivos dependientes, como imágenes y otros archivos multimedia.
La barra Insertar (Figura 3.4) contiene botones para la creación e inserción de diversos tipos de objetos, como tablas, capas e imágenes. Al pasar el apuntador sobre un botón, aparece una descripción de la herramienta con el nombre del botón.

Los botones están organizados en categorías, que se pueden cambiar en la parte izquierda de la barra Insertar. Si el documento actual contiene código de servidor, como los documentos ASP o CFML, aparecen también otras categorías. Cuando se inicia Dreamweaver, se abre la última categoría con la que ha trabajado.

Figura 3.4.- Barra Insertar de Dreamweaver

Algunas categorías tienen botones con menús emergentes. Al seleccionar una opción de un menú emergente, dicha opción se convierte en la acción predeterminada del botón. Por ejemplo, al seleccionar Marcador de posición de imagen en el menú emergente del botón Imagen, la siguiente vez que se de clic en

el botón Imagen, Dreamweaver insertará un marcador de posición de imagen. Siempre que se seleccione una nueva opción del menú emergente cambiará la acción predeterminada del botón.

La barra Insertar está organizada en las categorías siguientes:

- La categoría Común permite crear e insertar los objetos que se utilizan con más frecuencia, como las imágenes y las tablas.
- La categoría Diseño permite insertar tablas, etiquetas div, capas y marcos. También se puede elegir entre las tres vistas de las tablas: Estándar (valor predeterminado), Tablas expandidas y Diseño. Si se selecciona el modo de diseño, se pueden utilizar las herramientas de diseño de Dreamweaver: Dibujar celda de diseño y Dibujar tabla de diseño.
- La categoría Formularios contiene botones que permiten crear formularios e insertar elementos de formulario.
- La categoría Texto permite insertar diversas etiquetas de formato de texto y listas, como b, em, p, h1 y ul.
- La categoría HTML permite insertar etiquetas HTML para las reglas horizontales, el contenido de la sección head, las tablas, los marcos y los scripts.
- Las categorías de código de servidor sólo están disponibles para las páginas que emplean un lenguaje de servidor determinado, como ASP, ASP.NET, CFML Basic, CFML Flow, CFML Advanced, JSP y PHP. Cada una de estas categorías contiene objetos de código de servidor que pueden insertarse en la vista Código.
- La categoría Aplicación permite insertar elementos dinámicos como juegos de registros, regiones repetidas y grabar formularios de inserción y actualización.
- La categoría Elementos Flash permite insertar elementos Flash.
- La categoría Favoritos permite agrupar y organizar los botones de la barra Insertar que se utilizan con más frecuencia en un lugar común.

3.4.3 Creación de un Sitio Web con Dreamweaver

Un sitio Web es un conjunto de documentos y archivos vinculados con atributos compartidos, como temas relacionados, un diseño similar o un objetivo común. Un sitio de Dreamweaver permite organizar todos los documentos asociados con un sitio Web. La organización de los archivos en un sitio permite utilizar Dreamweaver para cargar el sitio en el servidor Web, controlar y mantener los vínculos de forma automática, administrar y compartir archivos.

Un sitio de Dreamweaver consta de un máximo de tres partes o carpetas, según el entorno de desarrollo y el tipo de sitio Web que se desarrolle: La carpeta local es el directorio de trabajo. En Dreamweaver esta carpeta se conoce como “sitio local”. Esta carpeta puede colocarse en el equipo local o en un servidor de red. En ella se almacenan los archivos con los que se está trabajando en un sitio de Dreamweaver.

Para definir un sitio de Dreamweaver, tan sólo hay que configurar una carpeta local. Para transferir archivos a un servidor Web o desarrollar aplicaciones Web, también se necesita añadir datos para un sitio remoto y un servidor de prueba. En la carpeta remota se almacenan los archivos, según el entorno de desarrollo, para fines de prueba, producción, colaboración, etcétera. En Dreamweaver ésta carpeta se conoce como “sitio remoto” en el pánel Archivos. En general, la carpeta remota suele colocarse en el equipo donde se ejecuta el servidor Web. Las carpetas de datos locales y remotos permiten transferir archivos entre el disco local y el servidor Web, lo cual facilita la administración de los archivos en los sitios de Dreamweaver.

3.5 CÁMARAS WEB

Una cámara Web o Webcam es una pequeña cámara digital conectada a una computadora, la cual puede capturar imágenes y transmitirlas a través de Internet en directo, ya sea a una página web o incluso a otra u otras computadoras de forma privada.

Las Webcams necesitan una computadora para transmitir las imágenes. Sin embargo, existen otras cámaras autónomas que tan sólo necesitan un punto de acceso a la red informática, ya sea Ethernet o inalámbrico. Para diferenciarlas de la webcam o cámaras de web se les denomina Netcam o cámaras de red.

Software

La instalación básica de una Webcam consiste en una cámara digital conectada a una computadora, normalmente a través del puerto USB. Lo que hay que tener en cuenta es que dicha cámara no tiene nada de especial, es como el resto de cámaras digitales, y que lo que realmente le da el nombre de webcam es el software que la acompaña.

El software de la webcam toma un frame de la cámara cada cierto tiempo (puede ser una imagen estática cada medio segundo) y la envía a otro punto para ser visualizada. Si lo que se pretende es utilizar esas imágenes para construir un vídeo, de calidad sin saltos de imagen, comúnmente éstas cámaras tienen una tasa de unos 15 - 30 frames por segundo.

Para los vídeos que tengan como objetivo ser colgados en internet o ser enviados a dispositivos móviles, es mejor una tasa de 14 frames por segundo. De esta manera se consigue ahorrar espacio y aún así seguir teniendo calidad, si bien se apreciaran ligeros saltos en el movimiento.

Si lo que se desea es que esas imágenes sean accesibles a través de internet, el software se encargará de transformar cada frame en una imagen en formato jpg y enviarlo a un servidor web utilizando el protocolo FTP.

Tecnología

Las Webcams normalmente están formadas por una lente, un sensor de imagen y la circuitería necesaria para manejarlos. Existen distintos tipos de lentes, siendo las lentes plásticas las más comunes. Los sensores de imagen pueden ser CCD (*Charge Coupled Device; Dispositivo de Cargas Interconectadas*) o CMOS *(Complementary Metal Oxide Semiconductor; Semiconductor de Óxido Metálico*

Complementario), este último suele ser el habitual en cámaras de bajo costo, aunque eso no signifique necesariamente que cualquier cámara CCD sea mejor que cualquiera CMOS.

Las webcams para usuarios medios suelen ofrecer una resolución VGA (*Vídeo Graphics Array; Matriz Gráfica de Video*) de 640x480 Pixeles con una tasa de unos 30 *frames* por segundo, en la actualidad están ofreciendo resoluciones medias de 1 a 1.3 Mega Pixeles.

La circuitería es la encargada de leer la imagen del sensor y transmitirla a la computadora. Algunas cámaras usan un sensor CMOS integrado con la circuitería en un único chip de silicio para ahorrar espacio y costos. El modo en que funciona el sensor es equivalente al de una cámara digital normal.

3.6 PUERTO USB

USB (*Bus Serial Universal; Canal Serie Universal*) es una interface Plug and Play entre la PC y ciertos dispositivos tales como teclados, ratones, escáner, impresoras, módems, placas de sonido, cámaras, etc.

Algunas cámaras Web están instaladas a grandes distancias de las PC que se encargan del proceso. La única diferencia en este caso es que la imagen no podrá enviarse por cable.

Es necesario un equipo transmisor junto a la cámara para convertir la imagen en señal de radio y un equipo receptor junto a la PC, que reconvierte la señal de radio en imagen, tal como normalmente llega un programa desde exteriores a un canal de televisión.

Antecedentes:

- Diseñado como una extensión en la arquitectura estándar del PC y orientado principalmente en la integración de periféricos, que aparecen como un solo puerto en lo que se refiere a utilización de recursos.

- Intel y otros líderes de la industria diseñaron el Bus Universal Serie.
- Dotación a la PC de un bus de alta velocidad.
- CTI (Computer Telephony Integrations; Integración de dispositivos telefónicos en los computadores).

Características del puerto USB:

- El canal de USB soporta intercambio simultáneo de datos entre una computadora y un amplio conjunto de periféricos.
- Todos los periféricos conectados comparten el ancho de banda del canal por medio de un protocolo de arbitraje basado en testigos ("Tokens").
- Permite conexión y desconexión dinámica (requieren un tratamiento especial para su desconexión).
- Es posible conectar hasta 127 dispositivos a una computadora.
- Consume pocos recursos.
- Gran ancho de banda, fácil de usar y configurar.
- Es un canal en serie bidireccional y de bajo costo.

Las especificaciones, del puerto USB se muestran en la Figura 3.5.

Figura a. Conector de USB

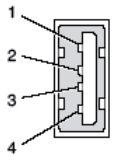

Tabla a. Señal del conector de USB

Pin	Señal	Descripción
1	VCC	+5 VDC
2	D–	Dato -
3	D+	Dato +
4	GND	Tierra

Figura 3.5.- Diagrama de especificaciones del USB.

Funcionamiento

El canal en serie USB es síncrono. Utiliza el algoritmo de codificación NRZI (Non Return to Zero Inverted; No Retorno a Cero Invertido). En éste sistema existen dos voltajes opuestos; una tensión de referencia corresponde a un "1", pero no hay retorno a cero entre bits, de forma que una serie de unos corresponde a un voltaje uniforme; en cambio los ceros se marcan como cambios del nivel de tensión, de modo que una sucesión de ceros produce cambios sucesivos de tensión entre los conductores de señal.

A partir de las salidas proporcionadas por los concentradores raíz (generalmente conectores del tipo "A") y utilizando concentradores adicionales, pueden conectarse más dispositivos hasta el límite señalado.

La información es enviada en paquetes; cada paquete contiene una cabecera que indica el periférico a que va dirigido.

Existen cuatro tipos de paquetes distintos: Token, Datos, Handshake, y Especial; el máximo de datos por paquete es de 8; 16; 32 y 64 Bytes respectivamente.

Se utiliza un sistema de detección y corrección de errores bastante robusto tipo CRC (Cyclical Redundancy Check; Chequeo de Redundancia Cíclica).
El funcionamiento está centrado en el anfitrión, todas las transacciones se originan en él. Es el controlador anfitrión el que decide todas las acciones, incluyendo el número asignado a cada dispositivo (esta asignación es realizada automáticamente por el controlador "anfitrión" cada vez que se inicia el sistema o se añade, o elimina, un nuevo dispositivo en el canal), su ancho de banda, etc. Cuando se detecta un nuevo dispositivo es el anfitrión el encargado de cargar los controladores oportunos sin necesidad de intervención por el usuario.

Ventajas:

- Es totalmente Plug and Play.
- Es reconocido e instalado de manera inmediata.
- Posee una alta velocidad.

- Permite alimentar dispositivos externos a través de él (5 volts).
- Ya casi toda máquina posee este puerto.
- Conexión más sencilla.
- Conexión en Caliente (Conectar y desconectar sin apagar la máquina).
- Son económicos por lo que un producto no aumenta mucho por el puerto.

Desventajas:

- El ancho de banda debe repartirse entre los dispositivos.
- Necesita de una PC que coordine su actividad a través de un controlador.
- No funcionan en MS-DOS.
- No funciona en versiones antiguas de Windows.
- No funciona en Linux con núcleos viejos.

3.7 SISTEMA DE ENERGÍA ININTERRUMPIDA UPS

Un Sistema de Energía Ininterrumpida es un equipo cuya función principal es evitar una interrupción de energía en la carga a proteger.

Son varios los nombres que recibe este tipo de equipos, a continuación se enumeran los más comunes:

- UPS: (*Uninterruptible Power System; Sistema de Energía Ininterrumpida*).
- No Break: Que significa sin interrupción.
- SFI: Por Sistema de Fuerza Ininterrumpida.
- SAI: Por Sistema de Alimentación Ininterrumpida.

Un UPS / NO BREAK es una unidad de almacenamiento de energía, la cual permite proteger diferentes equipos, como computadoras, contra bajas y altas de luz, así como también interrupciones de energía, éste no break puede almacenar energía para trabajar hasta durante varios minutos u horas, tiempo suficiente para almacenar la información y apagar el equipo con tranquilidad y esperar a que se restablezca la energía.

En el diagrama a bloques de la Figura 3.7, se observa el voltaje de alimentación del UPS y la batería, ambas son las dos fuentes de energía para la salida del UPS. El UPS tomará energía de la Batería, en caso de que haya ausencia del voltaje de entrada y de esta manera se podrá seguir dando voltaje a la carga.

La carga esta constituida por los aparatos a ser alimentados por el voltaje de salida de UPS y de los cuales no se desea interrumpir la energía.

Un UPS se compone de 4 partes:

1. Un rectificador que rectifica la corriente alterna de entrada, proveyendo corriente continua para cargar a una batería. Desde ésta se alimenta a un inversor que la convierte nuevamente en alterna. Luego de haberse descargado la batería, ésta se recarga generalmente en un tiempo de 8 a 10 horas, por lo cuál la capacidad del cargador debe ser proporcional al tamaño de la batería necesaria.
2. Una batería cuya capacidad (en Amperes hora) depende del tiempo (autonomía) durante el cual debe entregar energía cuando se corta la entrada del equipo UPS.
3. Un Inversor que convierte la corriente continúa de la batería en corriente alterna, adecuada para alimentar a los equipos conectados a la salida del UPS. Su capacidad de potencia depende del consumo total de los equipos a alimentar.
4. Un conmutador (By-Pass) de 2 posiciones que permite conectar la salida con la entrada del UPS (By Pass) o con la salida del inversor.

La Figura 3.6 muestra un diagrama del funcionamiento del UPS, donde se observan las etapas de un UPS.

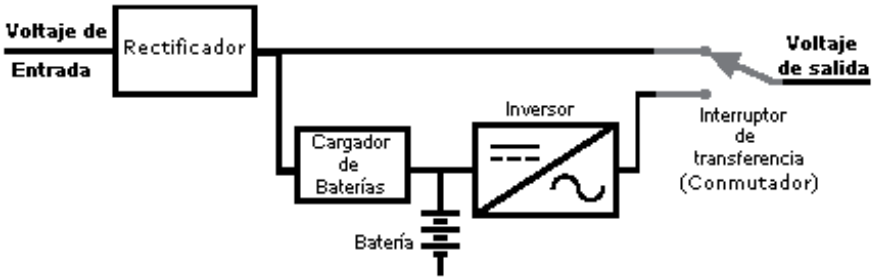

Figura 3.6.- Funcionamiento por etapas de un UPS.

3.7.1 Topologías de UPS: Funcionamiento

A continuación se mencionan algunas de sus topologías de manera general:

Tecnologías de UPS

- Off-Line (Fuera de Línea)
- On Line (En Línea)

I.- Fuera de Línea *(Off Line) ó* en Espera *(Stand-By).* Se le llama Fuera de Línea porque el Inversor se encuentra fuera del camino principal de la corriente, y se le llama en Espera porque el Inversor se encuentra apagado de que sea requerido encenderse.

El UPS Fuera de Línea es el tipo de UPS más económico ya que integra muy pocos componentes, el nivel de protección obtenido con este tipo de equipos también es muy limitado pero en general es muy adecuado para protección de la computadora ya que la inversión es muy baja y aún así se tiene protegido al equipo.

En la Figura 3.7 se muestra un diagrama a bloques del funcionamiento del UPS Fuera de Línea.

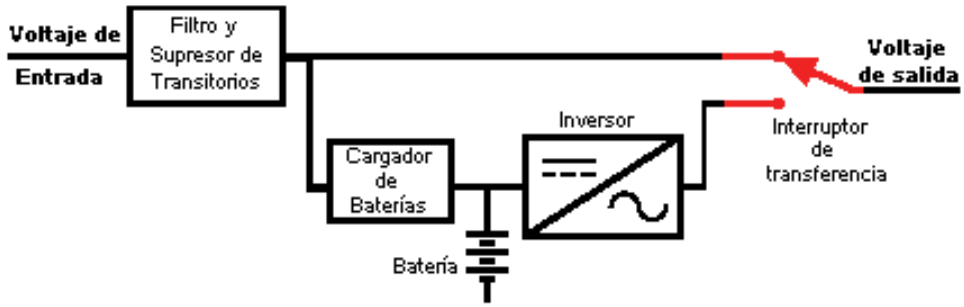

Figura 3.7.- UPS Fuera de Línea.

II.- En Línea *(On Line).* Este tipo de equipos es llamado en línea debido a que el Inversor se encuentra dentro de la línea principal de energía ya que siempre se encuentra operando. Ver la Figura 3.8.

En el sistema on line, sea con baterías internas o externas, el rectificador y el inversor están diseñados para entregar permanentemente la potencia nominal. La única diferencia entre ambos es con respecto al funcionamiento del rectificador en su función de cargador de baterías.

Esta tecnología es la más cara de todas pero es la que ofrece el mayor nivel de protección.

El voltaje de entrada pasa por medio del Interruptor INT1 al primer bloque que es el rectificador.

Rectificador.- El Rectificador del UPS On Line consiste de la etapa de rectificación con SCR generalmente con el objeto de poder variar el ángulo de disparo de los SCR y de esta manera poder regular el voltaje de CD a obtener a la salida, obviamente después de ser rectificado el voltaje de Entrada se filtra con Capacitores para obtener un voltaje continuo y regulado. El voltaje regulado de corriente directa obtenido en el Rectificador, tiene dos objetivos:

- El primero es mantener las baterías en flotación e incluso recargarlas después de un corte de energía.
- El segundo es alimentar al Inversor para que este a su vez convierta la corriente directa del rectificador en corriente alterna.

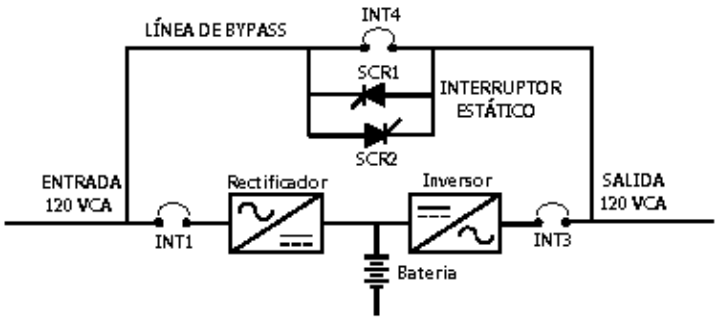

Figura 3.8.- UPS en Línea.

CAPÍTULO 4

CONFIGURACIÓN DE UN SERVIDOR DE WINDOWS MEDIA

4.1 IMPLEMENTACIÓN DE UN SERVIDOR DE SERVICIOS WINDOWS MEDIA 9 SERIES

En esta sección se describe la aplicación práctica e implementación de los Servicios de Windows Media. Debido a que Servicios de Windows Media es una tecnología extremadamente versátil y configurable, se puede utilizar para lograr una solución de medios de transmisión adecuada. La siguiente información puede ayudar durante el proceso de implementación y permite utilizar los conocimientos acerca del hardware local, y las condiciones de la red para configurar una solución de transmisión adecuada a las necesidades específicas del usuario.

Cualquier proyecto de medios de transmisión tiene tres etapas principales: planeación del proyecto, montaje y administración del contenido y coordinación de la distribución del contenido. Además de estas tres etapas, existen bastantes precauciones iniciales y pasos complementarios para mejorar el proceso de medios de transmisión.

Un sistema de medios de transmisión basado en Tecnologías de Windows Media se muestra en la Figura 4.1, consta normalmente de un equipo que ejecuta un codificador, como el Codificador de Windows Media, un servidor que ejecuta los Servicios de Windows Media y un número de equipos cliente que ejecutan un reproductor, como el Reproductor de Windows Media.

El Codificador convierte el contenido de audio y vídeo en directo y pregrabados en el Formato de Windows Media.

El servidor de Windows Media distribuye el contenido a través de una red o de Internet. El reproductor recibe entonces el contenido.

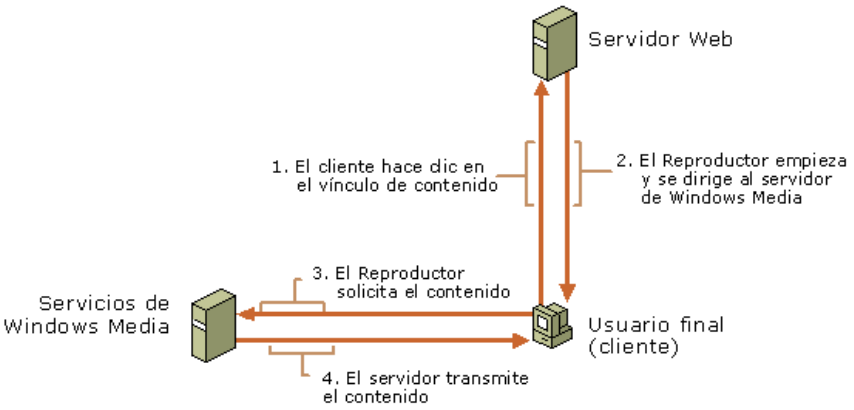

Figura 4.1.- Distribución del Contenido.

El caso de un usuario típico se muestra en la Figura 4.2, éste hace clic en un vínculo de una página Web para solicitar el contenido. El servidor Web redirige entonces la solicitud al servidor de Windows Media e inicia el reproductor en el equipo del usuario. En este momento, el servidor Web ya no forma parte del proceso de medios de transmisión, ya que el servidor de Windows Media establece una conexión directa con el reproductor y comienza la transmisión del contenido directamente al usuario.

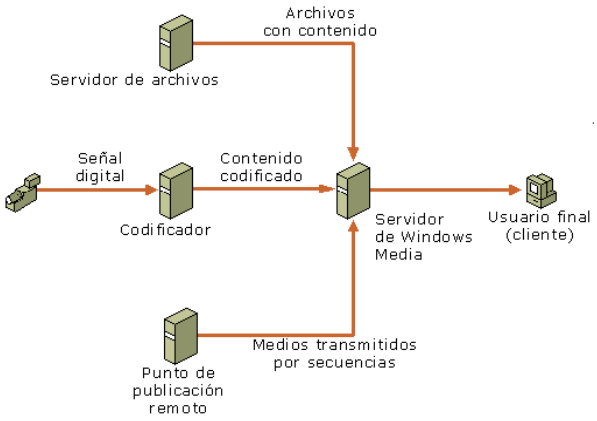

Figura 4.2.- Origen del contenido de transmisión.

El servidor de Windows Media puede recibir el contenido desde varios orígenes diferentes. Los acontecimientos en directo se pueden capturar mediante un dispositivo de grabación digital y procesarse con un Codificador antes de enviarlos al servidor de Windows Media para su difusión. Los Servicios de Windows Media pueden además volver a difundir el contenido transmitido desde un punto de publicación en un servidor remoto de Windows Media.

Una implementación efectiva de los medios de transmisión requiere la administración correcta de tres factores principales: el ancho de banda disponible para la audiencia, las capacidades de la conexión de red o de Internet y los requisitos de transmisión del contenido. El factor más importante, es la audiencia. La cantidad de ancho de banda disponible para la audiencia tiene una misión clave al determinar el tipo y la calidad del contenido proporcionado. Una secuencia de vídeo grande con alta definición y sonido estéreo requiere más ancho de banda del que hay disponible para los clientes que utilizan una conexión estándar de módem de acceso telefónico. También debe conocer el tamaño de la audiencia. Incluso un pequeño número de secuencias de alta velocidad pueden afectar el rendimiento de una red comercial o una puerta de conexión a Internet normales.

La evaluación de la capacidad de la red es el segundo factor. Una red de equipos como una red de área local puede transferir una cantidad limitada de datos en un momento dado. Cada una de las conexiones individuales de la red utiliza una parte de su capacidad. Cuando la cantidad total de datos transferidos se aproxima al límite de la red, las conexiones de datos individuales se vuelven más lentas. Al planear la implementación de los medios de transmisión, se asegura de que la capacidad de la red es muy superior a los requisitos de ancho de banda del contenido.

El contenido es el factor más flexible y diverso. Con audio y vídeo, cuanto mejor sea la calidad de los contenidos, mayores serán los requisitos de ancho de banda. La utilización de métodos de mejora de calidad, como la codificación con velocidades múltiples de bits o la codificación con velocidad de bits variable, puede crear grandes diferencias en el ancho de banda necesario. Antes de que se

pueda transmitir a la audiencia, el contenido en directo y pregrabado pasa por el proceso de codificación. Las selecciones realizadas durante este proceso tienen un impacto significativo en la cantidad de audiencia a la que se puede llegar, y en la cantidad de ancho de banda necesaria.

4.2 CONSIDERACIONES DE LA IMPLEMENTACIÓN

En todos los casos de implementación, existen algunas elecciones básicas que se deben realizar. Éstas dependerán del tipo de contenido multimedia digital (vídeo, audio o ambos) que se desee distribuir, la naturaleza de la audiencia y del equipo que se desee utilizar para entregar el contenido. Para la implementación del sistema de seguridad el contenido multimedia que se distribuirá será vídeo.

4.2.1 Transmisión de contenido en directo o pregrabado

Los Servicios de Windows Media pueden utilizarse para transmitir contenido en directo o pregrabado. Sin embargo, existen algunas diferencias en la forma de desarrollar una solución de transmisión que depende de si el contenido es en directo o pregrabado.

Contenido en directo

Se puede obtener contenido en directo de varias formas distintas. Se puede conectar un dispositivo de captura en directo, como un micrófono o una videocámara digital, a un equipo que ejecute un codificador, como el Codificador de Windows Media, y tenga una conexión de red con el servidor de Windows Media. También se pueden conectar otros dispositivos de reproducción de contenido multimedia digital, como reproductores de vídeo o CD al equipo de codificación de la misma forma para crear una difusión en directo de material grabado. Normalmente, se transmitirá contenido en directo como una difusión en lugar de una secuencia a petición, porque el usuario no puede controlar la reproducción de contenido en directo. Además, las conexiones de red entre el codificador y el servidor deben tener asignada una cantidad de ancho de banda que no puede interrumpir el resto del tráfico de red.

Además, el sistema tiene menos capacidad de recuperación ante errores de transmisión durante una difusión en directo, porque el contenido sólo está en la memoria de buffer del servidor durante un corto periodo de tiempo. Se puede utilizar la corrección de errores progresiva durante la reproducción, sin forzar que el reproductor solicite información de corrección de errores al servidor. Si se desea que el contenido esté disponible para los usuarios una vez finalizada la difusión, se debe considerar la posibilidad de archivar la difusión para que pueda volver a difundir el contenido o proporcionarlo a petición.

Contenido pregrabado

El contenido pregrabado es el tipo de contenido más fácil de administrar y configurar. Generalmente, asume la forma de archivos de audio o vídeo precodificados, que pueden procesarse utilizando un reproductor, como el Reproductor de Windows Media. Se puede transmitir un solo archivo o varios, o bien crear un archivo de lista de reproducción que organice el contenido para convertirlo, en una experiencia consistente para los usuarios. Si el contenido pregrabado está almacenado en un origen de red en lugar del servidor local, se debe comprobar que el servidor pueda tener acceso a la red y pueda recuperar el contenido de forma oportuna. Generalmente, esto no es un problema porque el servidor puede recuperar contenido pregrabado a una velocidad de datos muy alta ya que el servidor no tiene que procesar el contenido.

Al transmitir contenido pregrabado, se debe decidir qué tipo de experiencia desea crear para los usuarios. El contenido pregrabado puede transmitirse utilizando tanto puntos de publicación a petición como de difusión.

4.2.2 Selección de transmisión por secuencias de unidifusión o multidifusión

Unidifusión y multidifusión son dos formas distintas de distribución de medios de transmisión. Ambos tienen sus ventajas e inconvenientes en función de la naturaleza de la audiencia y el tipo de contenido.

Unidifusión

En las transmisiones por secuencias de unidifusión se envía una sola transmisión a cada Reproductor. La transmisión por secuencias de unidifusión tiene las ventajas de la interactividad entre Reproductor y servidor, configuración sencilla y capacidad de transmisión de múltiples velocidades de bits. Sin embargo, el número de usuarios que pueden recibir transmisiones por secuencias de unidifusión está limitado por la velocidad de bits del contenido y la velocidad de red del servidor.

Si la audiencia de unidifusión es muy amplia, la red o el servidor pueden saturarse rápidamente. Se recomienda utilizar la transmisión por secuencias de unidifusión si:

- Se desea aprovechar las ventajas de la codificación de múltiples velocidades de bits y de una transmisión por secuencias inteligente.
- La audiencia prevista y la velocidad de bits del contenido son compatibles con las capacidades de la red y del servidor.
- Se necesita un registro detallado de clientes.
- La red no está habilitada para transmisiones por secuencias de multidifusión.

Multidifusión

Las transmisiones por secuencias de multidifusión crean una relación entre un servidor y varios clientes. El servidor emite una sola transmisión y los usuarios pueden tener acceso a la transmisión en curso. Los usuarios no pueden controlar la reproducción del contenido. Las transmisiones por secuencias de multidifusión suponen una carga menor para el servidor y la red, pero pueden requerir una modificación de esta última para que pueda coexistir la transmisión por secuencias de multidifusión y el tráfico normal de la red. Se recomienda el uso de transmisiones por secuencias de multidifusión si:

- Se transmite contenido a un gran número de usuarios y la capacidad de ancho de banda de la red y el servidor es limitada.
- La red está habilitada para multidifusión.

4.2.3 Puntos de Publicación

- Los Servicios de Windows Media utilizan puntos de publicación para traducir las solicitudes de contenido de los clientes en rutas de acceso físicas en el servidor en el que éste se aloja. Una vez que el cliente se conecta correctamente al punto de publicación, el servidor de Windows Media administra la conexión y transmite el contenido.

Tipos de puntos de publicación

- Los clientes tienen acceso a las secuencias de contenido de su servidor conectándose a un punto de publicación. Servicios de Windows Media incluye dos tipos de puntos de publicación: de difusión y a petición. Cada tipo se puede configurar para enviar una secuencia desde uno o más tipos de orígenes, como una secuencia activa de un codificador, un archivo o una lista de reproducción. Un servidor de Windows Media se puede configurar para que ejecute varios puntos de publicación y aloje una combinación de contenido de difusiones y a petición.
- Estos dos tipos de puntos de publicación son similares en muchos aspectos, pero presentan algunas diferencias importantes. En general, el punto de publicación a petición se utiliza para que el cliente pueda controlar la reproducción, mientras que el punto de publicación de difusión sirve para controlar la reproducción desde el servidor.

Puntos de publicación a petición

- La transmisión de contenido desde un punto de publicación a petición se adapta mejor a las situaciones en las que desea que los usuarios puedan controlar la reproducción del contenido que se transmite. Este tipo de punto de publicación se utiliza normalmente para alojar contenido procedente de archivos, listas de reproducción o directorios. Cuando un cliente se conecta al punto de publicación, el contenido empieza al principio y el usuario final puede utilizar los controles de reproducción del Reproductor para realizar pausas, avanzar, rebobinar, saltar partes de una lista de reproducción o parar.

- Un punto de publicación a petición sólo transmite contenidos si hay algún cliente conectado para recibir la secuencia. El contenido transmitido desde un punto de publicación a petición siempre se envía como secuencia de unidifusión, lo que significa que el servidor mantiene una conexión diferente con cada cliente.
- También se puede utilizar un punto de publicación a petición para enviar una secuencia de difusión desde un codificador, un servidor remoto u otro punto de publicación. Cualquiera de éstos se puede seleccionar como origen único del contenido o se puede incluir como parte de una lista de reproducción de contenido. Cuando el contenido se crea a partir de un origen diferente del servidor de Windows Media, el usuario no puede utilizar los controles de reproducción del Reproductor para realizar pausas, avanzar, rebobinar, saltar partes de una lista de reproducción o parar.

Puntos de publicación de difusión

- La transmisión de contenidos desde un punto de publicación de difusión es especialmente adecuada para situaciones en las que desee crear una experiencia similar a la de ver un programa de televisión; el contenido se controla y transmite desde el punto de origen o el servidor. Este tipo de punto de publicación se utiliza frecuentemente para enviar secuencias activas desde codificadores, servidores remotos u otros puntos de publicación de difusión. Cuando un cliente se conecta a un punto de publicación de difusión, se une a una difusión que ya está en curso. Un cliente puede iniciar y parar la secuencia, pero no puede realizar una pausa, ni avanzar rápidamente, rebobinar o saltar.
- También puede transmitir archivos y listas de reproducción de archivos en un punto de publicación de difusión. Cuando procede de un punto de publicación de difusión, el servidor envía el archivo o la lista de reproducción como secuencia de difusión y el dispositivo no puede controlar la reproducción como sucede con las secuencias a petición. La experiencia del usuario es como la de recibir una difusión de una secuencia activa codificada; el cliente empieza a reproducir la secuencia en progreso.

- Normalmente, un punto de publicación de difusión se transmite desde que se inicia y continúa hasta que se detiene o hasta que finaliza el contenido. Sin embargo, es posible configurar un punto de publicación de difusión para que empiece y se ejecute, sólo si hay uno o más clientes conectados. Con esto, se guardan los recursos de red y servidor cuando no hay clientes conectados.
- Puede enviar contenido de un punto de publicación de difusión como secuencia de unidifusión o multidifusión. Es posible grabar la secuencia de un punto de publicación de difusiones como archivo de almacenamiento y ofrecerla a usuarios finales como reproducción a petición de la difusión original.

4.3 ADMINISTRACIÓN Y PRODUCCIÓN DE CONTENIDO

Los métodos y prioridades de la administración de contenido diferirán de un proyecto a otro según varios factores, como la demografía de la audiencia, el tipo de contenido y el equipo disponible. En esta sección se trata el problema de la administración del contenido en directo o pregrabado. Dado que el contenido publicitario puede presentarse de muchas formas distintas, se tratará independientemente de los demás tipos de contenido. Al igual que en cualquier proyecto complejo, la planeación es prioritaria.

Dado que los proyectos de medios de transmisión deben funcionar sin errores y pueden implementarse de tantas formas distintas, nunca está de más destacar la importancia de una planeación eficaz.

4.3.1 Contenido pregrabado

El contenido pregrabado está formado por archivos multimedia digitales. Es importante que éstos tengan el formato correcto para su transmisión y reproducción. Se puede configurar el servidor que ejecute los Servicios de Windows Media para transmitir un solo archivo o varios archivos, según sea necesario. Se puede utilizar una lista de reproducción para administrar la distribución del contenido pregrabado mediante un solo archivo de lista de reproducción para establecer la cantidad y el tipo de archivos multimedia digitales.

Después de crear las listas de reproducción, puede emplearlas para configurar el contenido a transmitir de la forma deseada. Existe una gran variedad de formatos de archivos multimedia digitales, pero no todos ellos pueden transmitirse con los Servicios de Windows Media. En algunos casos, debe convertir los archivos multimedia digitales a un formato compatible antes de poder ser transmitidos.

Compatibilidad con diferentes tipos de archivos

De forma predeterminada, se pueden utilizar los siguientes tipos de archivos con los Servicios de Windows Media. La extensión de los archivos se ofrece entre paréntesis:

- *Archivos de formato avanzado de sistemas (.asf)*. Archivos de Windows Media que contienen varios elementos, como vídeo, audio, secuencias de comandos, HTML y metadatos, que se pueden codificar utilizando cualquier tipo de códec.
- *Archivos de audio de Windows Media (.wma)*. Archivos multimedia digitales a los que se da el formato avanzado de sistemas y se codifican utilizando el códec Windows Media Audio. Son generalmente archivos de audio, aunque también pueden contener secuencias de comandos, imágenes y metadatos.
- *Archivos de vídeo de Windows Media (.wmv).* Archivos multimedia digitales a los que se da el formato avanzado de sistemas y se codifican utilizando el códec Windows Media Vídeo o Pinnacle Studio 9.0. Son generalmente archivos de vídeo, aunque también pueden contener secuencias de comandos y otras instrucciones.
- *Archivos MP3 (.mp3).* Archivos multimedia digitales que utilizan el formato de audio de Grupo de Expertos en Imágenes en Movimiento (MPEG).
- *Archivos JPEG (.jpeg o .jpg***)**. Archivos de imagen que utilizan el formato estándar de Grupo Conjunto de Fotógrafos Expertos.
- *Archivos de información de multidifusión (.nsc)*. Metarchivos de Windows Media que dirigen a los clientes a una difusión de multidifusión. Se utilizan para definir las propiedades de una secuencia de multidifusión a un reproductor, como el Reproductor de Windows Media.
- *Archivos de lista de reproducción del cliente (.asx, .wax y .wvx)*. Metarchivos de Windows Media que el servidor utiliza como listas de reproducción del cliente y

como redirectores de clientes. Contienen instrucciones y referencias para el reproductor, como el Reproductor de Windows Media.

- *Archivos de lista de reproducción del servidor (.wsx).* Metarchivos de Windows Media que se utilizan como listas de reproducción del servidor. Contienen combinaciones de archivos de audio, vídeo e imágenes.

4.3.2 Planeación de contenido pregrabado

El proceso de planeación para el contenido pregrabado difiere significativamente de la planeación que debe realizarse para el contenido en directo.

Por ejemplo, si la velocidad de bits de la transmisión de archivos de audio es demasiado alta para el ancho de banda de los usuarios, la secuencia experimentará varias pausas durante la reproducción para que el reproductor tenga tiempo de almacenar el contenido en buffer. Si la velocidad de bits es demasiado baja, la calidad del sonido puede verse afectada. Con pequeños ajustes en el proceso de codificación, como pasar de sonido estereofónico a monoaural, se puede reducir la velocidad de bits necesaria para la transmisión a aproximadamente la mitad sin mermar la calidad del sonido.

También pueden darse situaciones en las que se transmita un contenido a un amplio número de usuarios con perfiles de ancho de banda distintos: algunos a través de una red de área local, otros suscritos a una línea digital (DSL) y otros conectados a través de módems de acceso telefónico. Una preparación minuciosa permite transmitir contenido simultáneamente a todo tipo de usuario a la vez que se proporciona a cada uno la mejor calidad posible. Con los Servicios de Windows Media se puede transmitir contenido de audio en los formatos Audio de Windows Media Audio (WMA), ASF y MP3. Se debe preparar su contenido de audio convirtiéndolo o codificándolo en uno de estos formatos de archivo. El ancho de banda es problemático cuando se quiere transmitir contenido de audio. Las transmisiones en estéreo de alta calidad pueden saturar fácilmente la capacidad de un módem estándar de acceso telefónico. En una grabación de audio existen varios componentes configurables que se pueden ajustar durante el proceso de

codificación a fin de ayudar a alcanzar el equilibrio adecuado entre la velocidad de transmisión de datos y la calidad de audio. Siempre es una buena idea experimentar con el proceso de codificación a fin de encontrar la combinación óptima de parámetros. Si el contenido de audio procede de varios orígenes, es posible que la calidad sea incoherente. Debe intentar que el paso de un archivo de contenido al siguiente sea suave, continuo y de calidad.

La velocidad de bits del contenido multimedia digital es un factor aún más importante cuando se desea transmitir contenido de vídeo. Para evitar retrasos prolongados, interrupciones y distorsiones durante la reproducción, la velocidad de bits de la transmisión de vídeo debe adecuarse al ancho de banda del equipo de la audiencia, que suele ser limitado.

El contenido de vídeo no es más que la visualización rápida de una serie de imágenes fijas llamadas fotogramas. Cada uno de los fotogramas debe visualizarse con un cierto grado de detalle, o resolución, para que la reproducción sea exacta. Cuanto mejor sea la resolución de los fotogramas, con mayor detalle se verá el contenido. El número de fotogramas mostrados por segundo se llama velocidad de fotogramas. A medida que la velocidad de fotogramas aumenta, el movimiento del vídeo se hace más fluido.

La velocidad de bits de la transmisión está determinada por la combinación de la velocidad de fotogramas y la resolución del vídeo. Ambos parámetros pueden modificarse durante el proceso de codificación a fin de obtener la velocidad de bits ideal para el usuario.

El contenido de vídeo de alta resolución se transmite con fluidez a través de las conexiones de Internet de alta velocidad o de las LAN. Las redes extremadamente rápidas pueden procesar contenido de vídeo y audio capaz de rivalizar en calidad con un DVD. No obstante, a través de una conexión telefónica normal la transmisión de vídeo de alta calidad es imposible, sin tiempos de almacenamiento en buffer prohibitivamente largos. Existen técnicas que se pueden utilizar durante

la producción y los procesos de codificación del vídeo para mejorar la experiencia del usuario independientemente de la conexión utilizada:

- *Mantener el movimiento al mínimo.* En lugar de enviar toda la imagen de cada fotograma del vídeo, las transmisiones multimedia digitales sólo muestran con detalle las diferencias entre un fotograma y el siguiente. Si las diferencias se mantienen al mínimo, la velocidad de bits se mantiene también en un nivel bajo. Mientras se crea contenido de vídeo, se debe minimizar el movimiento de las personas, la cámara y el fondo para reducir la cantidad de información que se transmitirá por secuencias posteriormente.

- *Mantener un diseño de producción sencillo.* A menudo se puede disminuir el número de bits necesarios para reproducir un fotograma de vídeo reduciendo la complejidad de las escenas. Al grabar a una persona contra un fondo monocromo se requiere una transferencia de datos inferior que al hacerlo con un fondo multicolor o irregular. También se puede sacrificar parte de la calidad del sonido a cambio de obtener una calidad de vídeo mejorada durante el proceso de codificación, siempre que la calidad de vídeo sea más importante que la calidad de audio.

- *Hacer un uso inteligente de las posibilidades de transmisión por secuencias de los Servicios de Windows Media*. Se puede configurar el Codificador para que codifique el contenido multimedia digital con velocidades de bits distintas. De esta forma, independientemente del tipo de conexión del usuario, el servidor de Windows Media será capaz de enviar secuencias optimizadas para cada velocidad de bits.

4.3.3 Contenido en directo

La transmisión de contenido en directo puede tener varias ventajas sobre la transmisión de contenido pregrabado. La información de entretenimiento y noticias generalmente es más impactante al difundirla en directo y algunas informaciones

de actualidad pueden perder todo su valor para el usuario si se graban y se difunden posteriormente.

La producción de contenido en directo para su difusión no tiene por qué ser complicada ni costosa. Es posible transmitir vídeo en directo de forma relativamente sencilla si se dispone del equipo adecuado. Además, una secuencia en directo puede ser tan simple como conectar el Codificador a una fuente de contenido en directo de una señal de televisión o radio.

En cualquier caso, es muy importante notificar a la audiencia de la hora correcta y la dirección URL del suceso de transmisión en directo. Igual que en cualquier proyecto complejo, la programación es la principal prioridad. Dado que a menudo las transmisiones multimedia digitales no pueden revisarse ni ajustarse una vez iniciadas, se debe planear la difusión con antelación al suceso.

4.3.4 Preparación de contenido en directo

Para garantizar el éxito de la difusión en directo, es muy importante dedicar tiempo a la planeación y organización al inicio del proyecto. Los tres pasos principales en este proceso son: preparación de sucesos, preparación de los medios de entrada y preparación del Codificador.

Preparación de sucesos

Sea cual sea el tipo de suceso de difusión en directo, se debe establecer una hora de inicio y fin predeterminadas. Si establece una hora de inicio, puede dar a conocer a la audiencia cuándo tendrá lugar la difusión. La colocación del equipo de difusión es también un factor importante en el proceso de planeación. El movimiento del dispositivo de captura de multimedia digital está restringido por el cable que lo conecta con el equipo de codificación. El equipo de codificación, a su vez, debe estar conectado en red con el equipo que ejecuta los Servicios de Windows Media que, obviamente, debe tener acceso a una red o a Internet para que la audiencia pueda recibir la secuencia.

Preparación de los medios de entrada

Los medios de entrada pueden consistir en un dispositivo de captura, como una cámara de vídeo digital o un micrófono, o un suministro de datos de un origen de medio. Se debe asegurar de que el dispositivo de captura tenga una señal de salida digital y que se disponga del equipo adecuado para generar una salida digital. Muchas cámaras de vídeo y reproductores de casete no son compatibles con los requisitos de entrada digital de un codificador, como el Codificador de Windows Media. Se debe conocer cómo funciona el equipo. Se debe practicar el suceso con antelación para evitar contratiempos durante la difusión en directo. Además, se debe asegurar de que todas las baterías estén suficientemente cargadas y de que se haya realizado el mantenimiento necesario en los equipos.

Preparación del codificador

La velocidad de bits es el tema principal al transmitir contenido multimedia digital de cualquier tipo. La velocidad de bits afecta tanto al intervalo como al número de personas que podrán recibir la difusión. En términos generales, una velocidad de bits variable permitirá llegar a una mayor audiencia y permitirá el número máximo de conexiones individuales, si bien la calidad se verá perjudicada. Cuanto mejor sea la calidad, mayor deberá ser la velocidad de bits, con lo que se limitará el número de conexiones individuales.

Se debe recordar que la codificación de contenido de audio y vídeo en directo se produce en tiempo real y no hay oportunidad de cambiar la configuración una vez iniciada. Por ello, se debe practicar con antelación para determinar cuál es la configuración correcta para el Codificador.

4.4 PLANEACIÓN DE LA CAPACIDAD

El objetivo de la planeación de la capacidad es garantizar que el contenido llegará a todos los usuarios sin demoras ni interrupciones. Una red de medios de transmisión que se haya programado y configurado adecuadamente mejorará el

tiempo de respuesta, el rendimiento y la disponibilidad del contenido, al tiempo que reducirá la frecuencia de error de datos.

La planeación de la capacidad se basa en tres variables: volumen de audiencia, tipo y tamaño del contenido y número y velocidad de los servidores. En la mayoría de los casos, la planeación de la capacidad se utiliza para determinar los requisitos de servidor, necesarios para proporcionar una cantidad de contenido concreta a una audiencia seleccionada, aunque también se puede programar cualquiera de las variables en ciertas circunstancias.
Se puede calcular la capacidad de red que necesita mediante la siguiente ecuación:

Capacidad de red necesaria	=	Velocidad de bits del contenido	x	Número estimado de clientes

4.4.1 Evaluación del contenido de transmisión

A medida que crece la resolución y el tamaño de pantalla de su contenido, también lo hacen las demandas al servidor. Hay que Determinar cómo se desea utilizar el contenido y en qué contexto. ¿Se va a distribuir el contenido a una gran audiencia? En tal caso, se debería intentar mantener el tamaño mínimo de archivo posible. ¿Va a utilizar la audiencia varias velocidades de conexión para tener acceso al contenido? En tal caso, se deba considerar la posibilidad de utilizar una codificación de velocidades múltiples de bits para el contenido. Para determinar una estimación aproximada del requisito de ancho de banda de cada usuario, se divide el tamaño de archivo por el tiempo de reproducción en segundos. Por ejemplo, un archivo multimedia digital de 2 megabytes (MB) representa unos 16.000.000 bits. Si el contenido tiene una duración de 1 1/2 minutos, tendrá una velocidad media de bits de 180 kilobits por segundo (Kbps). La mayoría de los módems de marcado no pueden transferir información a más de 56 Kbps, lo que significa que un cliente que tenga acceso a la secuencia mediante una línea telefónica tendrá que esperar a que el reproductor almacene el archivo en caché

antes de empezar a reproducirlo o bien recibirá el vídeo o audio de forma intermitente.

4.4.2 Estimación del volumen de la audiencia

Aunque no se espere que todos los usuarios soliciten contenido al mismo tiempo, es importante prever puntos máximos de utilización. Asimismo, se debe tener en cuenta las velocidades de conexión de los usuarios, ya que pueden variar enormemente. Para estimar el volumen de su audiencia, se debe averiguar el número mayor de usuarios simultáneos durante un suceso de transmisión.
Por ejemplo, una empresa tiene previsto ofrecer formación en línea a todos sus 10.000 empleados mediante su red de área local. El aprovechamiento anterior de la formación indica que, como máximo, es probable que un cinco por ciento de los empleados tenga acceso a la formación en un determinado momento. Por tanto, la red debe tener capacidad para suministrar de forma confiable el contenido a 500 usuarios simultáneos.

4.4.3 Cálculo de la capacidad necesaria del servidor

Se utiliza el requisito de ancho de banda y el volumen de audiencia estimados para determinar la capacidad que deben poseer la red y el servidor para ajustarse a la demanda. Para calcular la capacidad total necesaria del servidor, se multiplica la velocidad de bits necesaria por usuario por el volumen de audiencia estimado. La capacidad real de un servidor determinado varía de un equipo a otro.

Por regla general, un equipo con un único procesador (233 megahertz) con 256 MB de memoria RAM que ejecute los Servicios de Windows Media puede dar servicio a un total de 1.000 secuencias de unidifusión a 28,8 Kbps.

La tabla 4.1 muestra la necesidad de aumentar la capacidad de servidor a medida que se incrementa el número de usuarios y la velocidad de bits del contenido.

Tabla 4.1.- Capacidad de usuarios simultáneos

Velocidad de bits de la secuencia (Kbps)	Tipo de conexión de red	Número de usuarios simultáneos por servidor
28,8 (20 real)	Módem telefónico	1.200
56,6 (33 real)	Módem telefónico	600
100	ISDN (RDSI)	300
300	DSL/cable/LAN	100

Por ejemplo, si se envía contenido de formación en línea a una velocidad de 300 Kbps a 100 usuarios simultáneos, el servidor y la red deben ser capaces de tratar 30 megabits por segundo. Como regla general un servidor de Windows Media tiene la capacidad de dar servicio de 30 Megabits por segundo.

4.4.4 Evaluación del potencial de crecimiento

Con el tiempo, las audiencias tienden a crecer y el contenido a multiplicarse. Se deberán evaluar los planes de medios de transmisión a largo plazo y ajustar los cálculos de capacidad requerida según corresponda. Otros de los aspectos que pueden influir en el crecimiento de la audiencia son las características de seguridad y los servicios adicionales, como la réplica automática de contenido y el software de equilibrio de la carga. A medida que aumenta el número de personas que utiliza el servidor, aumentará probablemente el número de conexiones simultáneas. Se deberán tener en cuenta los límites máximos del sistema y considerar qué tipo de respuesta es adecuada para su implementación. Por ejemplo, se deberá considerar si se desea estar preparado para hacer frente a un potencial de crecimiento del 50 por ciento o si se desea que la capacidad del sistema sea un límite de entorno para la implementación.

4.4.5 Ensamblaje de la capacidad requerida

Una vez que se ha estimado el ancho de banda que requiere el contenido, el volumen de audiencia y la capacidad de servidor deseada, y determinada la tasa de crecimiento proyectado, se puede proceder a crear el sistema de servidor y

realizar los cambios necesarios en la red actual con el fin de adaptarla a la capacidad del servidor.

En la siguiente lista se describen brevemente algunas de las técnicas más efectivas para actualizar la capacidad del servidor y de la red:

- Actualización de un servidor de una sola CPU a un servidor con varias CPU's.
- Instalación de tarjetas de red adicionales o actualización de la tarjeta de red del servidor para que admita una conexión de red de mayor ancho de banda.
- Adición de servidores que ejecuten los Servicios de Windows Media e implementación de un programa de equilibrio de carga para crear un servidor lógico de mayor tamaño para llevar a cabo la transmisión por secuencias a través de la red.
- Distribución de servidores de proxy-caché a través de la red e implementación de un programa de duplicación de contenido, para distribuir el contenido de forma más próxima a los clientes y liberar de parte de la demanda a los servidores que generan el contenido.
- Definición de conmutadores de red para procesar las solicitudes de los medios de transmisión y definición de las transmisiones en modo dúplex completo, para mantener un flujo de información sin interrupciones.

4.4.6 Prueba de la capacidad

Antes de implementar la solución de medios de transmisión, se debe realizar una prueba de carga para asegurar que el sistema de servidor ensamblado, admite el contenido y audiencia requeridos y se comporta del modo esperado. Se puede ejecutar el Simulador de procesos de Windows Media 9 Series en uno o más equipos cliente para simular cualquier número de conexiones de cliente. También se puede configurar el simulador de procesos para recrear una serie de comportamientos de cliente, incluida la reproducción continua de contenido, la transmisión de contenido a múltiples velocidades de bits, la exploración y búsqueda de contenido a petición y las conexiones con autenticación. Según la velocidad de la máquina, cada simulador de procesos puede probar los límites

máximos de la red y el servidor, cargando al servidor con más de 1.000 conexiones simultáneas.

4.5 CONSIDERACIONES DE SEGUIMIENTO

4.5.1 Realización de equilibrio de carga y clústeres

Los clústeres garantizan la disponibilidad de los servicios vitales utilizando un grupo de equipos, o clúster, en lugar de un único equipo, la Figura 4.3 muestra los clústeres. Cada equipo de un clúster se denomina nodo. Los clústeres aumentan la tolerancia a errores y la escalabilidad del sistema, lo que permite suprimir uno o varios nodos del servicio sin obstaculizar el funcionamiento del sistema. Los clústeres generalmente forman parte de un proceso de equilibrio de carga en el que las solicitudes de contenido se distribuyen entre los nodos para repartir la carga de forma uniforme.

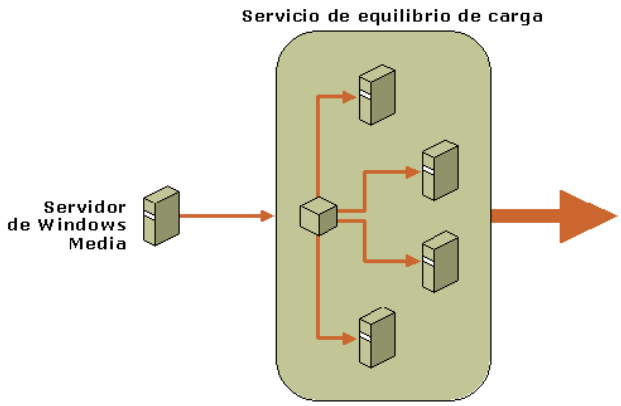

Figura 4.3.- Clústeres

Clústeres

Cada nodo de un clúster proporciona un conjunto específico de recursos al grupo. Los Servicios de Windows Media pueden ser tan sólo uno de los distintos recursos disponibles en un nodo concreto, y es posible que no todos los nodos de un clúster determinado tengan instalados los Servicios de Windows Media. Si un

nodo falla o se apaga, el software de clúster reasigna la solicitud del servidor a otros miembros del clúster que tengan disponibles los recursos necesarios. Este proceso se denomina conmutación por error. Existen dos modos comunes de conmutación por error:

- *Conmutación por error en cascada.* Los recursos del nodo que falla se distribuyen uniformemente a otros nodos de todo el clúster. Este modo asume que todos los otros nodos del clúster tienen alguna capacidad adicional.
- *Conmutación por error N+1.* Los recursos del nodo que falla se redireccionan a un nodo en suspensión que se mantiene como reserva. Este modo asume que la mayoría o toda la capacidad sobrante del clúster se asigna a un nodo.

Cuando se recupera un nodo con fallos o desconectado, el software de clústeres puede mover automáticamente alguno o todos los recursos redistribuidos de nuevo a su ubicación original. Además de controlar la conmutación por error, el software de clústeres permite a los administradores controlar y administrar los nodos como un mismo sistema en lugar de como equipos individuales. Con el fin de proporcionar una protección eficaz de conmutación por error, cada nodo del clúster debe tener una conexión directa con el origen de contenido. El origen de contenido puede ser un codificador, un punto de publicación o un servidor de archivos.

Los clústeres de Equilibrio de la carga en la red es un método de clúster de servidor que se ofrece en Windows Server 2003. Cada clúster puede admitir un máximo de 32 equipos con un mismo nombre lógico de Internet. El clúster detecta automáticamente el fallo o cambio de estado del servidor y redirecciona las solicitudes al resto de servidores al tiempo que mantiene una apariencia completamente operativa para el usuario.

Equilibrio de carga

El software de equilibrio de carga habitualmente trabaja con el software de clúster para administrar la carga del servidor dentro del clúster, para que se distribuya de forma uniforme entre los nodos. Supervisa el funcionamiento de cada nodo y

divide la carga de los medios de transmisión, siguiendo una fórmula o algoritmo predeterminado. También garantiza que, aunque la secuencia pueda originarse de un nodo cualquiera de los distintos que existen, el contenido está representado por una única dirección IP.

Existen dos estrategias principales para el equilibrio de la carga:

- *Equilibrio de carga basado en hardware*. También conocido como proxy inverso, este método emplea un servidor proxy situado en la red entre el clúster del servidor y los clientes. El servidor proxy inverso recibe solicitudes de transmisión del cliente y redirecciona el cliente al servidor correspondiente o bien delega el contenido de dicho servidor al cliente. Para evitar crear un punto de error único, puede utilizar dos o más máquinas de proxy inverso en paralelo.
- *Equilibrio de carga basado en software*. Los productos de equilibrio de carga basados en software asignan un porcentaje de la carga total del servidor a cada nodo del clúster. El software de equilibrio de carga se ejecuta en cada nodo del clúster y calcula qué nodo será el siguiente que aceptará una solicitud basándose en el porcentaje de la carga de trabajo total de cada servidor. Algunas de las ventajas de este método de equilibrio de carga son la velocidad, capacidad de configuración y confiabilidad, además de su precio reducido. Figura 4.4

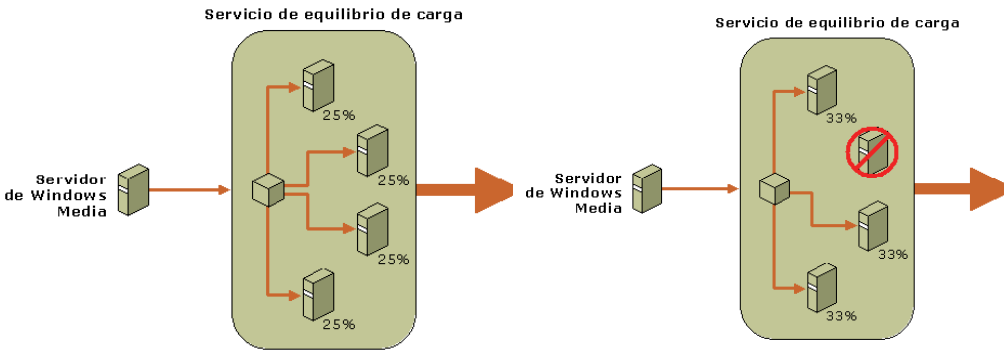

Figura 4.4.- Equilibrio de carga basado en software

Equilibrio de carga en red se ofrece con Microsoft Windows Server 2003 y utiliza un algoritmo de filtrado completamente distribuido. Cada segundo, cada nodo del clúster emite una señal de "latido" que contiene información sobre su estado. El software equilibrio de la carga en la red supervisa estas señales para ver si se han producido cambios en el estado del clúster, y cambia la distribución de solicitudes del servicio según corresponda.

4.5.2 Supervisión del rendimiento del servidor

La capacidad de supervisar el rendimiento del sistema de servidores es vital para una administración eficaz. Con la supervisión del rendimiento, se puede:

- Conseguir el mejor rendimiento posible del servidor.
- Evaluar el valor del contenido para la audiencia.
- Evaluar patrones y tendencias entre la audiencia.

Utilización de supervisión de rendimiento

Los Servicios de Windows Media incluyen un supervisor gráfico del rendimiento en tiempo real para observar el comportamiento de los servidores y los puntos de publicación. Esta herramienta muestra la elección de datos de rendimiento a lo largo de un período. Además de la visualización gráfica, la supervisión de rendimiento de Windows Media dispone de varios contadores de rendimiento configurables.

Utilización del complemento controlador de eventos WMI de WMS

Este complemento permite supervisar aspectos específicos del funcionamiento del servidor. Después de habilitar y configurar el complemento Controlador de eventos WMI de WMS, se podrán recibir notificaciones locales o remotas de los sucesos del servidor. Con este complemento se pueden supervisar las siguientes funciones del servidor:

- *Servidor.* Informa sobre el estado del servidor y de los cambios realizados en las propiedades.

- *Cliente.* Informa sobre los sucesos del cliente del Reproductor de Windows Media.
- *Límites.* Informa sobre los límites del servidor en el momento en que se modifican o se alcanzan.
- *Lista de reproducción.* Informa sobre los sucesos relacionados con la lista de reproducción.
- *Caché*. Informa sobre los sucesos relacionados con la actividad de la caché.
- *Punto de publicación*. Informa sobre los cambios en el estado o las propiedades de los puntos de publicación.
- *Complemento.* Informa sobre la actividad del complemento del servidor y de los puntos de publicación.

4.6 TOLERANCIA A ERRORES

En la transmisión de contenido multimedia digital, por tolerancia a errores se entiende la capacidad de un sistema de medios de transmisión de mantener o, como mínimo, recuperar, el servicio después de un error del sistema. La posibilidad de que un error del sistema ocasione un fallo, es también una forma de medir la tolerancia a errores del sistema. La tolerancia a errores puede medirse también en términos de disponibilidad del sistema o del porcentaje de tiempo de actividad del sistema. Un sistema de medios de transmisión no es más que una cadena de componentes, que van desde el origen del contenido hasta el consumidor como muestra la Figura 4.6. Al igual que una cadena, cada componente debe realizar de forma correcta su tarea asignada o fallará todo el sistema. Los errores pueden producirse en cualquier punto del sistema de medios de transmisión. Los errores directos, en relación con los Servicios de Windows Media, son los que tienen que ver con el origen del contenido, como el codificador o la biblioteca multimedia digital. Los errores indirectos son los que tienen que ver con la distribución del contenido al cliente, como los errores en los servidores de distribución o los servidores de proxy-caché.

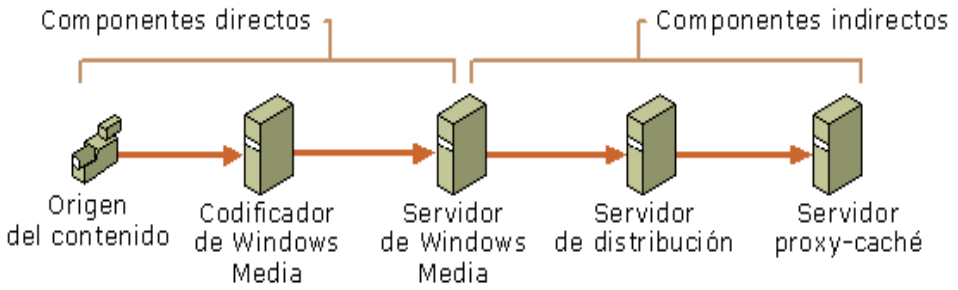

Figura 4.5.- Tolerancia de errores

La clave de la tolerancia a errores en un sistema de medios de transmisión es la redundancia. Un sistema que depende en cada etapa del proceso de distribución de un único componente es un sistema vulnerable a los fallos.

4.6.1 Errores directos

Un fallo de entrada en los Servicios de Windows Media, ya sea de un codificador, un punto de publicación remoto o un servidor de archivos, es especialmente peligroso porque es posible que el administrador del sistema no se dé cuenta de que hay un problema. Cuando un origen de contenido directo falla o se desconecta, se escribe un error en la ficha Solución de problemas y en el registro de sesión, si bien no hay una indicación explícita de que exista un problema en los Servicios de Windows Media. Puede minimizar el riesgo de un error directo utilizando varios orígenes de contenido para el punto de publicación. Éstos pueden consistir en codificadores redundantes o archivos de contenido alternativo que el punto de publicación puede utilizar si el origen de contenido principal no está disponible. Figura 4.6

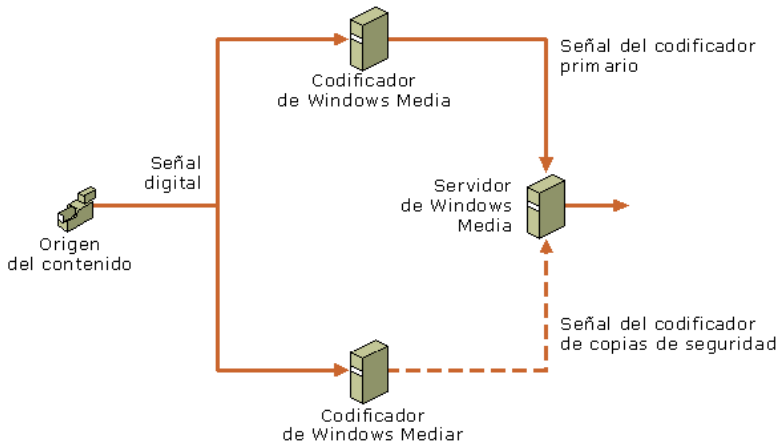

Figura 4.6.- Errores Directos

4.6.2 Errores indirectos

El fallo del servidor de Windows Media o uno de sus componentes indirectos, como un servidor de distribución, puede impedir que los clientes reciban el contenido que han solicitado. Si se utilizan varios servidores de Windows Media para transmitir el mismo contenido, por medio de *clústeres*, se reduce el riesgo de interrupción del servicio. El uso de clústeres es una valiosa técnica de tolerancia a errores porque la capacidad reducida o el fallo de alguno de los servidores, es difícil que interrumpa todo el sistema. Si un servidor deja de responder, la carga de trabajo del servidor con problemas puede transferirse de forma inmediata y uniforme a los otros servidores. Figura 4.7

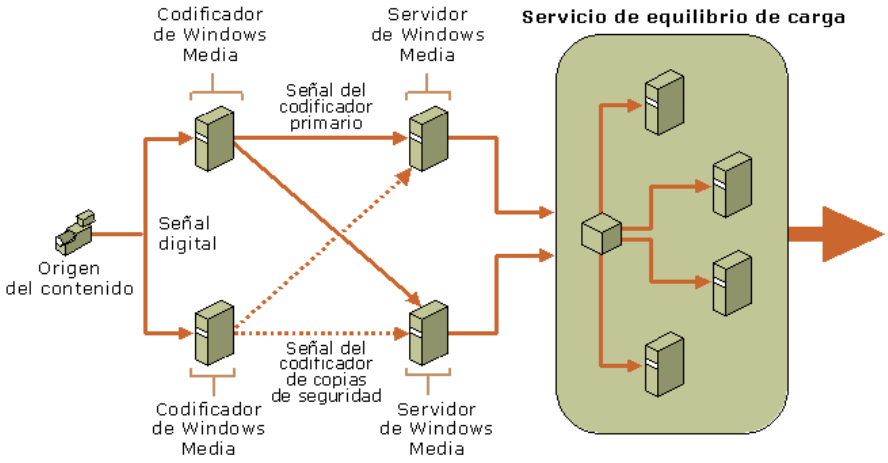

Figura 4.7.- Errores indirectos

4.7 ESCALABILIDAD

La escalabilidad se describe como la facilidad con que se pueden agregar o quitar componentes de un sistema, al tiempo que se mantiene la confiabilidad del mismo. A medida que el número de usuarios crece, tal vez se deban agregar servidores, a fin de que el aumento de la demanda no sobrecargue el sistema. Asimismo, también existe la posibilidad de dividir un sistema de servidor de grandes dimensiones en varios más pequeños y especializados. En ambos casos, se deberá plantear la escalabilidad del software y el hardware como temas independientes.

4.7.1 Escalabilidad del software

Los Servicios de Windows Media están diseñados para admitir una amplia gama de implementaciones, desde pequeñas emisoras de radio por Internet con algunos cientos de solicitudes de conexión, hasta sitios Web de transmisión a gran escala de medios que generan millones de solicitudes. El complemento Servicios de Windows Media le permite administrar tantos grupos de servidores y puntos de publicación como servidores y puntos de publicación aislados.

4.7.2 Escalabilidad del hardware

En el contexto de los Servicios de Windows Media, la escalabilidad se refiere principalmente a las operaciones de agregar y quitar servidores de un sistema. Agregar servidores en un sistema que se encuentra saturado por un aumento de las conexiones o del contenido, puede contribuir a una mejora espectacular del rendimiento. El número de servidores necesarios en un sistema se determina a partir de la velocidad de bits del contenido, el tipo de contenido y el número de conexiones simultáneas por parte de los clientes.

Al utilizar varios servidores, es importante que se utilice alguna forma de equilibrio de carga para evitar la sobrecarga de alguno. Los servidores deben presentar un rendimiento y una capacidad similares, para garantizar que el método de equilibrio de carga sea lo más eficaz posible. El número de servidores que se pueden combinar en un sistema de Servicios de Windows Media es ilimitado.

CAPÍTULO 5

PROPUESTA PARA LA IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD

5.1 DESCRIPCIÓN DEL SISTEMA DE SEGURIDAD

A continuación se describirán las características que presenta el sistema de seguridad que se propone llevar a cabo, el propósito de dichas características es satisfacer las necesidades del usuario, resolviendo así el problema planteado anteriormente; que es brindar seguridad en el área de cómputo en la ESIME Zacatenco.

El diseño del sistema de vídeo vigilancia se muestra en la Figura 5.1.

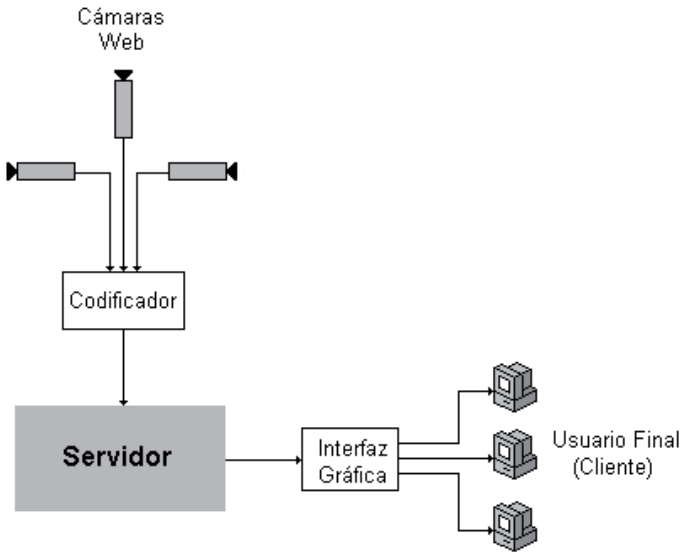

Figura 5.1.- Sistema de Vídeo Vigilancia

Se trata de un sistema de seguridad que posibilita la emisión del vídeo de vigilancia por Internet desde un equipo remoto equipado con una cámara web. Se utiliza para ello un servidor de Windows Media y el codificador.

Desde una computadora conectada a Internet, se envía una señal de vídeo al servidor. Para ello se instala un software en la PC. Este software lo que hace es recoger la señal de vídeo entrante a la PC, codificarla y enviar esa señal codificada al servidor.

Los usuarios de este sistema de seguridad son usuarios exclusivos que se conectan al servidor para vigilar el lugar. El vídeo en tiempo real es observado por los usuarios por medio de una interfaz gráfica, es decir, una página web por medio de la cual los usuarios pueden observar las diferentes imágenes de las cámaras conectadas al servidor.

El sistema usa cable de extensión USB para la conexión entre las cámaras y la computadora que emite el vídeo codificado al servidor, con el objetivo de que se tenga un mayor alcance para la correcta colocación de las cámaras.

5.2 HARDWARE DEL SISTEMA

5.2.1 Características del Servidor

Para que el servidor que se pretende utilizar tenga un buen funcionamiento, se proponen las siguientes características:

- Procesador Intel Pentium 4 a 2.8 GHZ, 1MB Cache L2.
- Memoria RAM de 1 GB, DDR2, SDRAM, 533MHZ.
- Disco Duro 240 GB SATA, 7200 RPM.
- Drive óptico combo DVD/CD-RW.
- Tarjeta de red integrada 10/100/1000 Mbps.
- Tarjeta de vídeo y tarjeta de sonido.
- Puerto USB.

El costo estimado de este tipo servidor es aproximadamente de $8,000.00, las características mencionadas anteriormente son sólo una propuesta para que el servidor trabaje bien, sin embargo puede optarse por adquirir uno de mayor o menor desempeño aunque este cambio tendrá un impacto directo en el costo del mismo.

Características del equipo para codificar el vídeo

Es importante considerar que se requiere de un equipo para la codificación del vídeo de las cámaras web, debido al uso que se le dará a esta computadora, no se requieren características iguales a las del servidor, el equipo que se propone presenta las siguientes características.

- Procesador Intel Pentium 4 a 1.8 GHZ, 512MB Cache L2.
- Memoria RAM de 512 MB, DDR2, SDRAM, 533MHZ.
- Disco Duro 80 GB IDE.
- Drive óptico combo DVD/CD-RW.
- Tarjeta de red integrada 10/100/1000 Mbps.
- Tarjeta de vídeo y tarjeta de sonido.
- Puerto USB (mínimo 5).

5.2.2 Elección y colocación de las cámaras

La elección de las cámaras web, en lugar de las cámaras IP fue debido a que las primeras tienen un costo menor que las segundas, su mantenimiento y reparación no requiere de conocimientos muy especializados y se encuentran a la venta en cualquier lugar que venda equipos de computación, por otro lado, se debe tomar en cuenta que todas las cámaras presentan un retardo en el momento de transmitir el vídeo, cabe mencionar que dicho retardo es mayor en las cámaras web que en las cámaras IP, gracias a la tecnología de compresión de vídeo MPEG4 (*Moving Picture Experts Group; Grupo de Imágenes Expertas en Movimiento)* con la cuenta este tipo de cámaras, pero en términos generales, el funcionamiento de las cámaras web, como ya se describió en capítulos anteriores, se ajusta a las necesidades requeridas por el proyecto.

Se recomienda también utilizar cámaras con visión nocturna, que permitan tener visibilidad del lugar, aún cuando esté obscuro, así como UPS (Sistema de Energía Ininterrumpida) que permitan tener el sistema encendido durante un periodo largo de tiempo, en caso de una falla en la energía eléctrica.

Cámaras utilizadas

En la Figura 5.2 se observa la cámara web empleada en el sistema de seguridad, a continuación se describirán sus características y especificaciones, mismas que fueron de gran importancia para elegirlas en el proyecto.

Figura 5.2.- Cámara Web

Descripción

La cámara web que se utiliza es marca Genius y tiene un costo de 399 pesos.

Esta cámara cuenta con tecnología infrarroja, lo que permite capturar el vídeo en condiciones de poca luz y en tiempo real. Esta excelente cámara tiene resolución de 320K píxeles rojo-infrarrojos automáticos se interpola hasta 1.3 Mega píxeles para tomar magníficas fotos fijas.

La VídeoCam Trek 310 posee un diseño especial que la hace ligera y fácil de llevar a cualquier lado. Cuenta con clip para sujetarla a computadoras portátiles o pantallas planas. Se pueden convertir archivos de formato AVI a MPEG1 para reducir el tamaño de los archivos. También tiene un botón en la parte superior para tomar fotos fijas con facilidad y rapidez.

La VídeoCam Trek310 puede funcionar como una cámara de seguridad que puede grabar automáticamente cualquier movimiento que ocurra enfrente del

monitor. Si no hay movimiento, se apaga automáticamente después de cuatro segundos. Es un excelente sistema de monitoreo de seguridad que permite configurar el software para que funcione cuando el usuario no esté presente.

Programa de sistema de seguridad

- Sistema de circuito cerrado por un bajo costo.
- Gran ángulo de visión de 52 grados.
- Comienza a filmar cuando detecta cualquier movimiento.
- Sistema con Zoom para acercamientos a detalle.
- La base ajustable gira 360 grados.

Especificaciones técnicas

En la Tabla 5.1 se muestran las especificaciones técnicas de la cámara web y la Tabla 5.2 muestra los requisitos que debe cumplir la computadora a la que se va a conectar dicha cámara.

Tabla 5.1.- Especificaciones técnicas de la cámara web

Especificaciones Técnicas	
Sensor de imagen	CMOS VGA (640x480)
Lente	Enfoque manual
Interfaz	USB 1.1/1.0. Compatible con USB 2.0
Resolución máxima	Imagen fija: 1280x960 (1.3MP) Captura AVI: 640x480
Velocidad de fotogramas	Hasta 30fps.
TWAIN	Compatible
Dimensiones	4.5 x 4.5 x 6 cm
Peso	76g.

Tabla 5.2.- Requerimientos de la computadora

Requerimientos del Sistema
• Pentium III 800MHz compatible con MMX • 64MB de RAM CD-ROM • Puerto USB • 160MB de espacio en disco duro • Para LINUX: versión Kernel 2.4.22/2.4.25/2.4.26/2.6.9

5.2.3 Plano de ubicación de las cámaras

Un aspecto muy importante en el diseño del sistema de seguridad es la ubicación de las cámaras, las cuales deben ser colocadas en puntos estratégicos con el objetivo de obtener la mayor visibilidad posible, que a su vez proporcione una mayor protección del lugar que se está vigilando.

La Figura 5.3 muestra la forma en que se colocarán las cámaras.

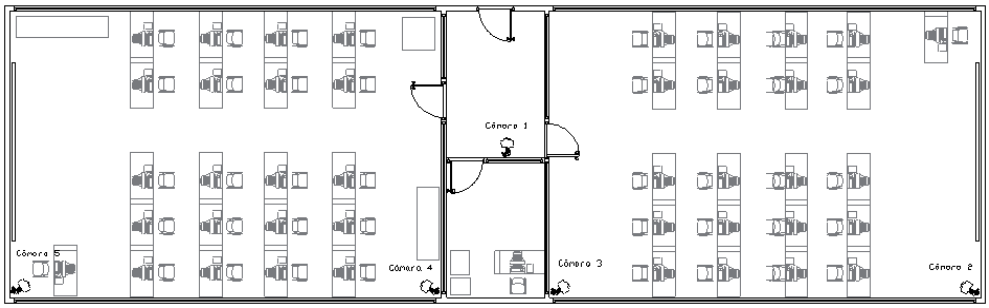

Figura 5.3.- Plano de laboratorios 1 y 2

La cámara 1 se coloca en esa posición con el objetivo de tener un control en el tráfico de las personas que entran y salen de los laboratorios. La ubicación de las cámaras en el laboratorio se realizó en las esquinas del lugar, es decir, la colocación fue en una misma pared en sus esquinas superiores, de manera que se pudiera cubrir una mayor área del laboratorio. La ubicación de las cámaras permite cubrir el laboratorio en diferentes ángulos y por lo tanto tener una mejor vigilancia de los laboratorios. Ya que si se colocan en esquinas opuestas no se cubre toda el área del laboratorio, teniendo el inconveniente de tener el mismo panorama en diferentes ángulos.

5.2.4 Conexión

El cableado del sistema de vídeo vigilancia se observa en la Figura 5.4, dicho cableado se realiza con una extensión de USB, con el objetivo de que las cámaras tengan un mayor alcance y se puedan conectar a la computadora donde se esté

codificando el vídeo.

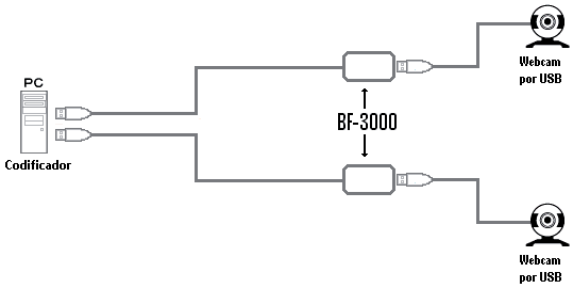

Figura 5.4.- Conexión de las cámaras web

En la Figura 5.5 se muestra la extensión del cable USB 2.0.

Figura 5.5.- Cable de extensión USB 2.0

CABLE DE EXTENSIÓN USB 2.0 (ACTIVO)

Funcionalidades

El cable activo para extender las conexiones USB asegura la calidad de señal para satisfacer plenamente los requerimientos electrónicos y la velocidad de transmisión de la conexión cumpliendo la especificación USB 2.0 (480 Mbps).

Permite, conectar hasta cinco de ellos en serie, extender hasta 25 metros (80 pies) para la conexión de la cámara web a la computadora.

Es compatible con HUBs USB 2.0 y con cualquier dispositivo USB 1.1

Tiene un costo de $200.00.

Las especificaciones de la extensión USB modelo BF-3000 se muestran en las Tablas 5.3 y 5.4.

Tabla 5.3.- Especificaciones técnicas del cable de extensión USB BF-3000

Especificaciones Técnicas	
Longitud del cable:	5 metros
Conectores:	Tipo A macho y hembra, este último con sistema de retención, que evita su desconexión.
Software:	No requiere controladores ni software.
Otras	N o requiere alimentación externa

Tabla 5.4.- Requerimientos del sistema para el uso de la extensión USB BF-3000

Requerimientos del Sistema para su uso
• PC compatible 266 MHz o superior. • Puerto USB 2.0 (480 mbps) o USB 1.1 (12mbps) disponible. • Windows® 98SE, Windows® ME, Windows® 2000 or Windows® XP.

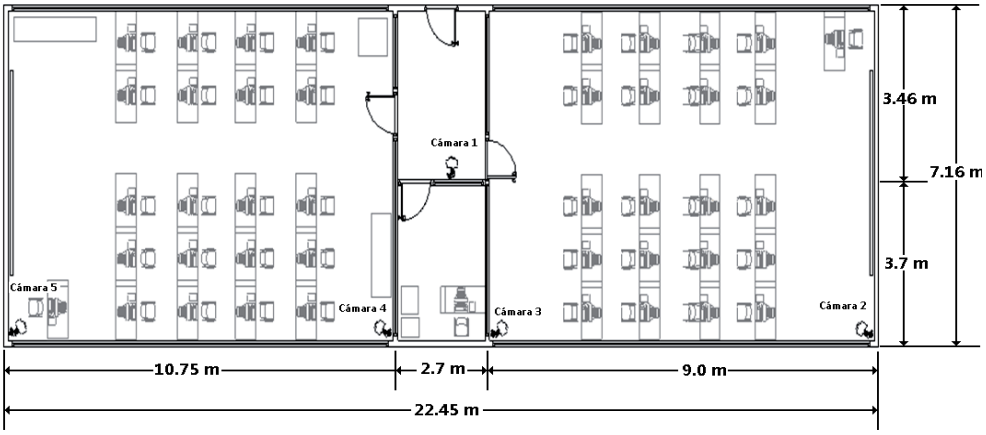

Figura 5.6.- Plano de laboratorios 1 y 2 con sus respectivas medidas

La Figura 5.6 muestra las mediciones del los laboratorios, las cuales permiten determinar el numero de extensiones de USB se requieren para la conexión del sistema.

5.3 CODIFICACIÓN DE VÍDEO

El codificador de Windows Media permitirá convertir el vídeo captado en directo por la cámara en secuencias, o bien en un archivo de Windows Media, para su transmisión mediante el Servidor de Windows Media. Para la codificación de un

suceso en vivo se configura el codificador, con ciertas características que permiten la transmisión del vídeo en tiempo real. La Figura 5.7 muestra la configuración que se realiza para la codificación.

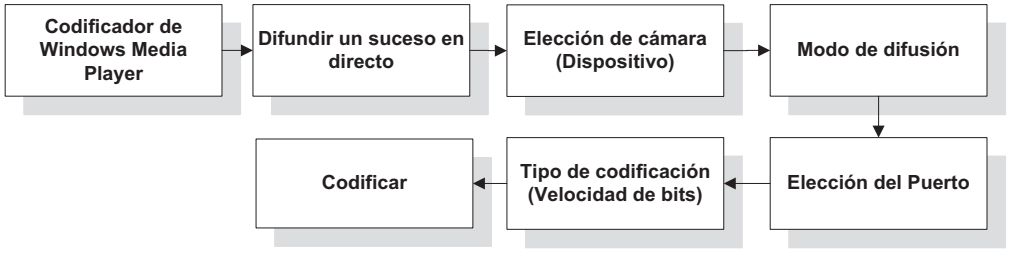

Figura 5.7 Configuración del Codificador de Windows Media

La codificación es para la difusión de un acontecimiento en directo, el codificador captura el vídeo desde la cámara web que se encuentra conectada en una PC y difunde el contenido en directo, insertando la secuencia en el servidor.

El codificador de Windows Media tiene compatibilidad con las características de Plug and Play, y esto permite que el codificador detecte automáticamente los dispositivos, tal como la cámara Web, que es el dispositivo utilizado para la captura del vídeo. Pero es necesario indicarle al codificador, cuál es el dispositivo del que se desea capturar el vídeo.

El contenido ya codificado para su difusión es necesario extraerlo del codificador de Windows Media, de manera que el servidor es quien inicia la conexión, transmitiendo y distribuyendo la secuencia como una secuencia de multidifusión hacia los usuarios conectados a internet.

Es importante asignar el puerto, ya que a través de éste, el servidor y el reproductor de Windows Media pueden tener acceso a la secuencia. Así que el puerto es el que permite la comunicación entre el codificador y el servidor. El número del puerto utilizado es un puerto predeterminado, dicho puerto pertenece a los conocidos como puerto well-known, mencionados anteriormente. El puerto más usual es el puerto 8080, ya que es un puerto de Red Mundial. Y es el más

recomendable, pero no necesariamente es el único puerto que se puede utilizar, y es por ello que está la opción de buscar un puerto libre, el cual pueda ser utilizado para poder tener acceso a la secuencia del codificador.

La dirección URL para la conexión es la dirección del servidor, esta dirección es una IP estática, es decir, es una dirección fija, la cual es contratada, en este caso es una dirección de la red del Instituto Politécnico Nacional, y pertenece a una de sus subredes, la de la ESIME Zacatenco, esta dirección IP estática permite al codificador la conexión con el servidor de Windows Media.

Es necesario indicar desde el codificador cuál es la velocidad de bits, la velocidad de cuadros y el tamaño del buffer para la codificación del vídeo.

La velocidad de bits se realiza mediante CBR (Constant Bit Rate; Tasa de Bits Constante), la cual ofrece mejores resultados para trabajar con la transmisión por secuencias, con CBR la velocidad de bits se mantiene constante durante la secuencia dentro de un periodo reducido que está determinado por el buffer. Pero como en todo, tiene una desventaja, la calidad del contenido no se mantiene constante, esto debido a que en ciertos fragmentos del contenido es más difícil la compresión de éste. Para el uso del sistema de vídeo vigilancia, esta reducción de calidad en la transmisión es insignificante.

5.4 CONFIGURACIÓN DE UN PUNTO DE PUBLICACIÓN

Un punto de publicación es el portal a través del cual un cliente se conecta para recibir una secuencia. El origen es la ubicación del contenido que un cliente puede recibir desde un punto de publicación. Puede asignar el tipo de origen que desee de entre varios tipos a un punto de publicación, como un archivo, un directorio de archivos, una lista de reproducción de contenido o una secuencia en directo de un codificador. Para la realización del sistema de vídeo vigilancia, su utiliza la transmisión por secuencias en directo desde un codificador, ya que los usuarios necesitan observar el vídeo en tiempo real para saber que está sucediendo en los distintos laboratorios. En la Figura 5.8 se observa el procedimiento que se debe

seguir para configurar un punto de publicación.

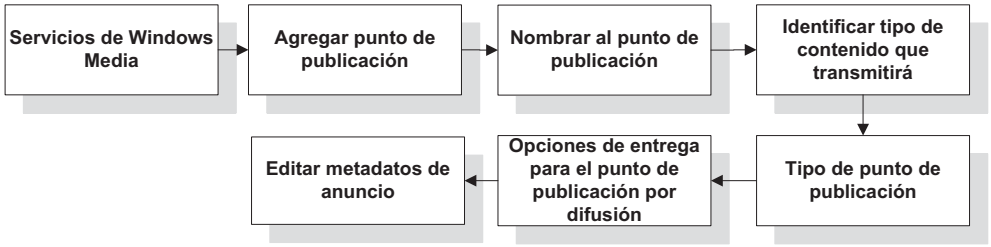

Figura 5.8.- Configuración del punto de publicación

El punto de publicación debe ser de difusión, ya que el usuario no podrá controlar la reproducción del contenido que se transmita del servidor, cuando inicia un punto de publicación de difusión manualmente, el contenido empieza a transmitirse independientemente de si algún cliente se encuentra conectado. Un cliente que se conecte al punto de publicación de difusión empezará a reproducir la secuencia de transmisión en progreso. También puede parar un punto de publicación de difusión. Si lo hace, todos los clientes dejarán de recibir la secuencia.

A medida que los clientes conectados dejan de recibir la secuencia, el número de conexiones disminuye gradualmente.

Si desea desconectar a todos los clientes inmediatamente, puede seleccionar el comando *Desconectar todos los clientes*. Si ha denegado las conexiones a su punto de publicación y desea empezar a proporcionar acceso a los clientes, puede seleccionar la opción *Permitir nuevas conexiones de unidifusión*. Además se deben tomar en cuenta los siguientes puntos:

- Si envía el contenido como secuencia de unidifusión y multidifusión, la denegación de nuevas conexiones sólo afectará a los clientes que reciban el contenido como secuencia de unidifusión.
- Si para el punto de publicación de difusión, también se detendrán las transmisiones por secuencias de multidifusión.

- Si envía el contenido como secuencia de multidifusión, no puede utilizar la propiedad de inicio automático porque los clientes de multidifusión no se conectan directamente al servidor. Puede seleccionar la opción de iniciar automáticamente el punto de publicación cuando finalice el Asistente para anuncios de multidifusión o iniciar manualmente el punto de publicación.
- Al iniciar un punto de publicación de difusión, se omite la propiedad *Iniciar punto de publicación cuando el primer cliente se conecte*. Si desea que el punto de publicación de difusión empiece y pare automáticamente en base a las conexiones de los clientes, no inicie manualmente el punto de publicación.

Otro aspecto importante al momento de configurar el punto de publicación, es indicar la URL del codificador, es decir, la dirección IP y el puerto desde donde se está codificando el vídeo.

La Figura 5.9 muestra el ejemplo de un punto de publicación.

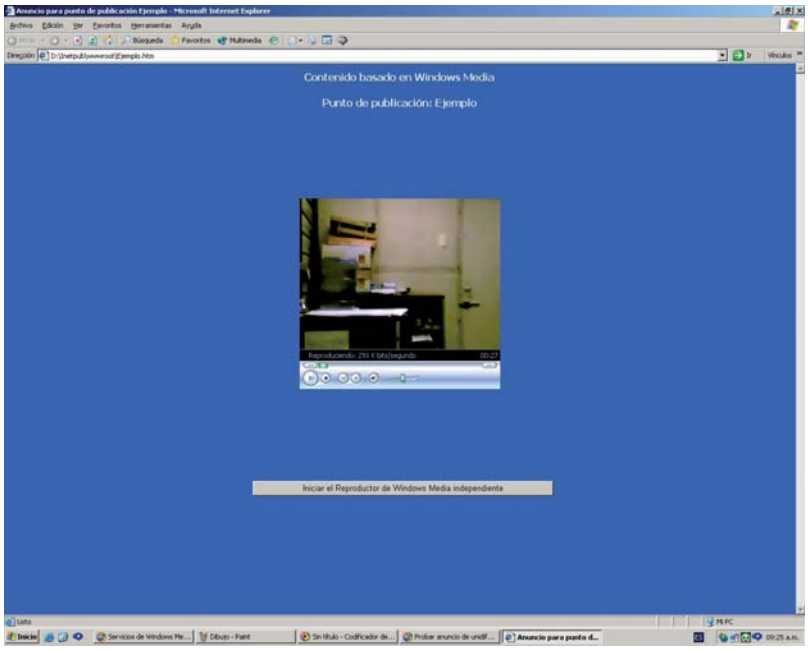

Figura 5.9.- Ejemplo de un punto de publicación

5.5 DISEÑO DE LA PÁGINA WEB

A continuación se describirá el procedimiento que se siguió para la elaboración de la página web, la cual es la interfaz gráfica para el usuario y mediante la cual podrá visualizar el vídeo en tiempo real desde el lugar en donde se encuentre.

5.5.1 Creación de sitios con el asistente de definición del sitio de Dreamweaver.

El asistente de Definición del sitio de Dreamweaver MXs una guía durante el proceso de configuración de un sitio. Esto significa dar nombre al sitio, especificar la tecnología de servidor, especificar un lugar para los archivos en el equipo e introducir la información para publicar y cargar los archivos en un servidor. El procedimiento es el siguiente:

1. Seleccionar Sitio > Nuevo sitio en la barra de menú principal para ejecutar el asistente de Definición del sitio.

2. Escribir el nombre del sitio y hacer clic en *Siguiente* para proceder, (Figura 5.10).

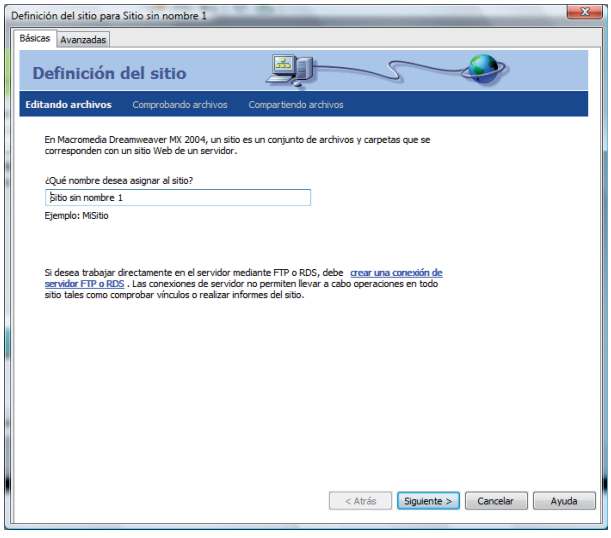

Figura 5.10.- Elección del nombre del sitio en el asistente de Definición del sitio de Dreamweaver

3. Seleccionar “No, no deseo utilizar una tecnología de servidor”, esto es para trabajar solamente en el servidor local.

4. Hacer clic en Siguiente.

5. Seleccionar “Editar copias locales en mi equipo y luego cargarlas al servidor cuando estén listas”. Para llenar el campo titulado “¿En qué lugar del equipo desea almacenar los archivos?”, buscar el directorio donde se desean colocar los archivos del sitio (Figura 5.11).

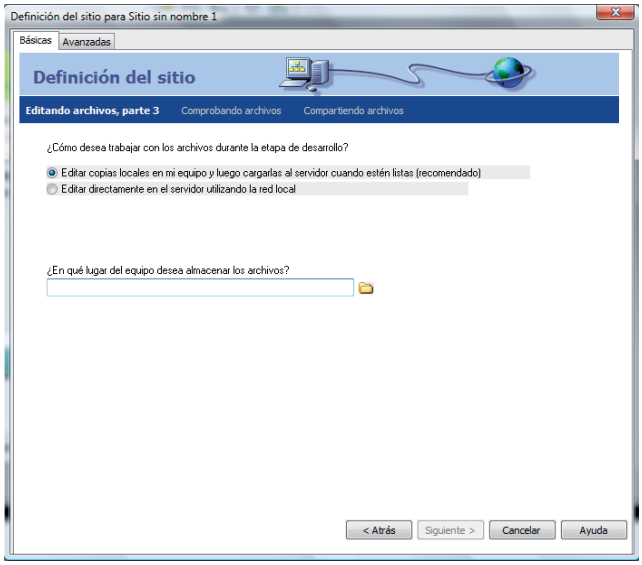

Figura 5.11.- Selección de la carpeta local

Nota: Si se ha creado anteriormente un sitio en Dreamweaver MX, este campo se llena con la ubicación del último sitio creado. No se debe usar la misma carpeta raíz local para dos sitios diferentes. Si trata de usar la misma carpeta raíz local para más de un sitio, Dreamweaver le pedirá que elija una carpeta distinta para el nuevo sitio. Una vez definido el directorio, hacer clic en *Siguiente*.

6. Seleccionar “Ninguno” en el menú emergente “¿Cómo conecta con su servidor remoto?”. Como éste es un sitio estático, no es necesario especificar un servidor remoto.

7. Hacer clic en *Siguiente.*

8. Como se muestra en la Figura 5.12, la pantalla final del asistente de Configuración del sitio muestra un resumen de preferencias. Revisar la información y utilizar el botón Atrás para regresar y hacer cualquier corrección que fuera necesaria. O bien, hacer clic en Listo si toda la información es correcta.

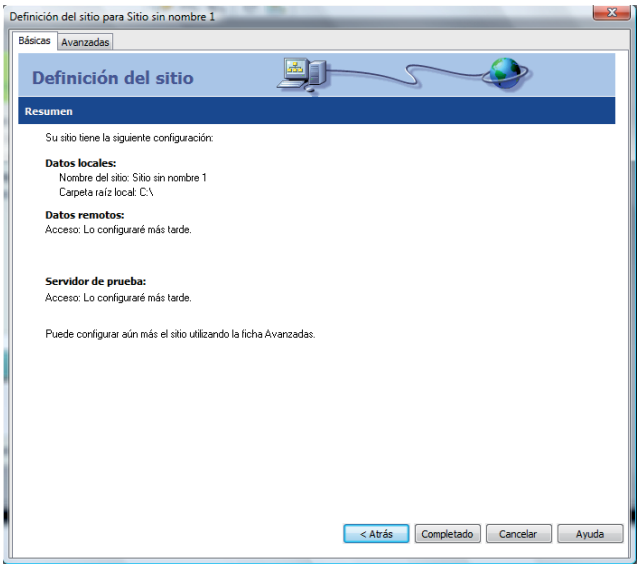

Figura 5.12.- Pantalla final del asistente de Configuración del Sitio de Dreamweaver

5.5.2 Adición y edición de un documento web en el sitio creado

Para agregar documentos web al sitio creado previamente a partir de un archivo de diseño de Dreamweaver:

- Seleccionar Archivo>Nuevo. Aparecerá el cuadro de diálogo Nuevo documento (Figura 5.13). La ficha General ya aparece seleccionada.
- En la lista Categoría, seleccionar Hojas de estilos CSS, Diseños basados en tablas, Diseños de páginas (CSS), Diseños de páginas o Diseños de páginas

(accesibles), dependiendo de las necesidades del sitio, a continuación, seleccionar un archivo de diseño de la lista de la derecha. Puede obtener una vista previa de un archivo de diseño y leer una descripción breve de los elementos de diseño de un documento. Para más información sobre las opciones de este cuadro de diálogo, hacer clic en el botón Ayuda del mismo.

- Hacer clic en el botón Crear. El documento nuevo se abrirá en la ventana del documento. Si se seleccionó una hoja de estilos CSS, el documento CSS aparecerá en la ventana del documento y la hoja de estilos CSS se abrirá en la vista Código.
- Guardar el documento. Si el archivo contiene vínculos a archivos activos, aparecerá el cuadro de diálogo Copiar archivos dependientes para que pueda guardar una copia de los archivos dependientes.
- Si aparece el cuadro de diálogo Copiar archivos dependientes, defina las opciones y haga clic en Copiar para copiar los archivos en la carpeta seleccionada. Es posible elegir una ubicación propia para los archivos dependientes o utilizar la ubicación predeterminada de carpeta que genera Dreamweaver (basada en el nombre original del archivo de diseño).

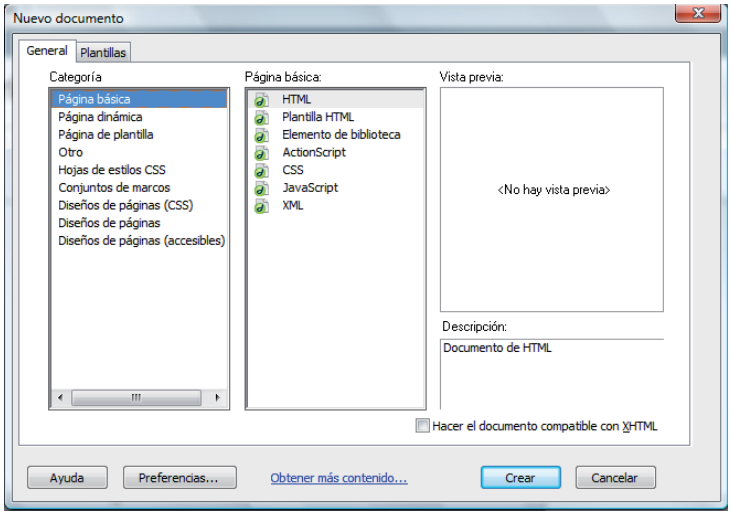

Figura 5.13.- Selección del tipo de página.

Una vez agregado el documento se procede a su edición debido a que al agregarla al sitio, ésta se encuentra en blanco o con el diseño de una plantilla u hoja de estilo, si se eligió alguna de éstas.

5.5.3 Página web del sistema de monitoreo

Para el caso específico del sistema de seguridad, se seleccionaron hojas de estilo y se modificaron de manera que se tenga acceso a las diferentes áreas a monitorear mediante una página principal (Figura 5.14), y una vez seleccionada alguna se ingresa para poder visualizar lo que está capturando una cámara y poder cambiar de vista entre una y otra en el mismo recinto o tener las dos vistas en una sola página (Figura 5.15), en el lado derecho se encuentran los enlaces para cambiar de una cámara a otra, y debajo los enlaces a sitios externos, como la página de internet del IPN, la ESIME Zacatenco y la Academia de Computación de ésta escuela.

Figura 5.14.- Página principal del sistema de monitoreo

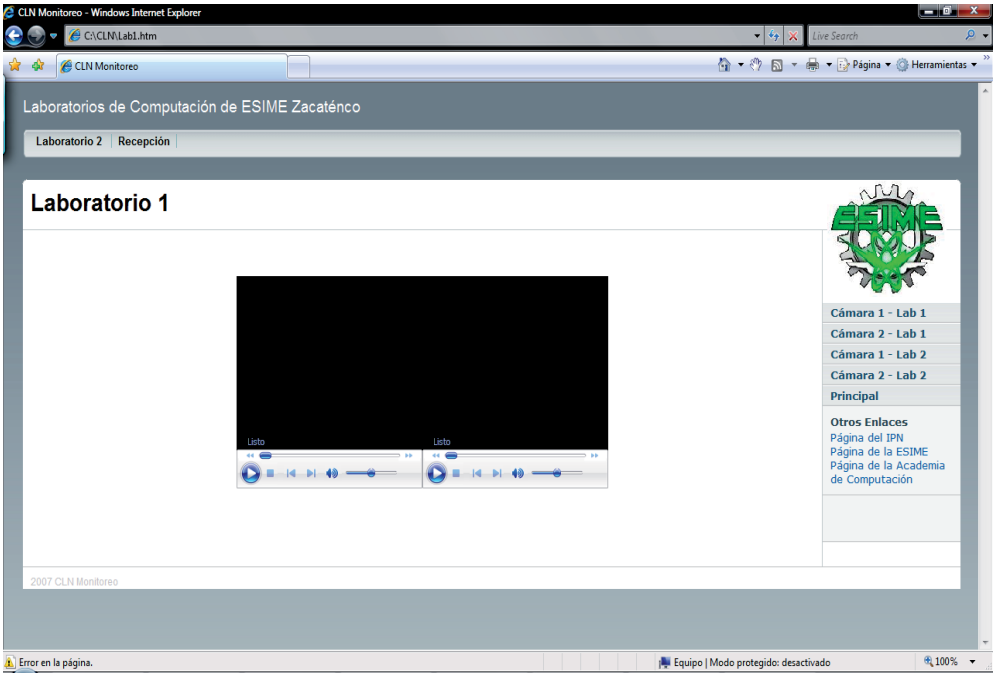

Figura 5.15.- Visualización de las 2 cámaras en una sola página

5.6 PROTECCIÓN DEL SISTEMA DE VÍDEO VIGILANCIA

El sistema requiere de un elemento que ofrezca protección en situaciones que no se cuente con energía eléctrica, la cual es indispensable para mantener funcionando dicho sistema. Para ello se considera necesaria la utilización de un UPS (Uninterruptible Power System; Sistema de Energía Ininterrumpida). El UPS cuenta con elementos que permiten evitar daños en el equipo, a continuación se describen las características y el funcionamiento del UPS empleado para el proyecto.

La Figura 5.16, muestra el UPS que se empleará en el sistema.

Figura 5.16.- UPS / No break.

El UPS es de la marca APC, esta unidad respalda entre 20 minutos y 60 minutos, esto depende de la potencia que se esté utilizando.

Ante cualquier baja de luz, es capaz de responder con energía acumulada, para que el sistema no deje de trabajar, y también protege al equipo en caso de sobrecarga, cuenta con un regulador de intensidad y no permite que pase hasta el equipo, ya que éste se dañaría.

Funciones principales del UPS

- Permite guardar los documentos antes de apagar su computadora.
- Calendariza apagado del sistema cuando usted lo requiere.
- Monitorea el sistema y suministro eléctrico gráficamente.
- Notifica de fallas del sistema o suministro vía correo electrónico.
- Su Interfaz es gráfica y muy sencilla de usar.
- Mejora la calidad de vida de su equipo de cómputo.
- Evita que se descompongan componentes internos de la PC (fuente de energía, módem, etcétera).
- Conexiones: 4 de respaldo y 4 supresores de pico.
- Protección de línea telefónica, fax y módem.
- Interface USB, DC con software y manual del usuario.

Características del UPS

- *Batería de Respaldo de emergencia.* Protege su computadora de caídas repentinas de energía, el respaldo de batería proveerá suficiente tiempo para guardar los documentos y apagar correctamente la PC.
- *Reguladores Automáticos.* El regulador automático de voltaje protege la PC contra cortes particulares de energía, alzas y bajas de voltaje y otras irregularidades.
- *Protección Internet / Fax / Modem* .El sistema de energía ininterrumpida protege la línea telefónica contra irregularidades electrónicas que puedan dañar la PC.
- *Protección contra poderosas descargas eléctricas (rayos), picos de voltaje, ruido de altas frecuencias.* El sistema de energía ininterrumpida cuenta con filtros que protege la PC de rayos, cambios súbitos de energía, picos y ruidos.
- *Económico.* Tiene un costo de $500.00.

Cabe mencionar que dicho regulador, deberá ser colocado dentro de una protección especial, la cual puede ser una caja de metal con un candado, a la que sólo tenga acceso el encargado o encargados del sistema de vídeo vigilancia, con la finalidad de que no sea apagado o desconectado quedando las computadoras sin protección alguna, y por lo tanto vulnerables a cualquier daño.

5.7 ANÁLISIS DE LOS COSTOS

La evaluación desde el punto de vista económico de este proyecto analiza la factibilidad y rentabilidad para instalar este sistema de vídeo vigilancia.

El propósito de realizar un análisis de los costos del proyecto es que el usuario tenga conocimiento de la inversión que se requiere para implementar este sistema de seguridad.

A continuación se mencionarán los costos que se requieren cubrir para llevar a cabo el sistema de seguridad en un área, la cual consta de dos laboratorios y un cubículo.

La Tabla 5.5 presenta el análisis económico del hardware para la implementación del proyecto:

Tabla 5.5.- Costos del Hardware del sistema

Objeto	Cantidad	Costo Unitario	Costo Total
Cámara Web	5	$400.00	$2,000.00
Extensión de USB	7	$200.00	$1,400.00
UPS	2	$500.00	$1,000.00
Servidor	1	$8,000.00	$8,000.00
Codificador	1	$4,500.00	$4,500.00
		Total	**$16,900.00**

La Tabla 5.6 muestra el análisis de costos totales del software que requiere el sistema de vídeo vigilancia.

Tabla 5.6.- Costos del Software del sistema

Objeto	Cantidad	Costo Unitario	Costo Total
Windows Server 2003	1	$15,000.00	$15,000.00
Codificador de Windows Media	1	Gratuito	Gratuito
		Total	**$15,000.00**

En la Tabla 5.7 se observa el costo total del sistema de vídeo vigilancia para una área.

Tabla 5.7.- Costo total del sistema

Objeto	Cantidad	Costo Total
Hardware	1	$16,900.00
Software	1	$15,000.00
	Total	**$31,900.00**

Para realizar la instalación en los otros laboratorios de computación, ya no es necesario invertir en el servidor y tampoco en la licencia de Windows Server 2003, ya que este equipo soportaría la conexión de las cámaras previstas de acuerdo al número de áreas en las sea necesario implementar el sistema de seguridad.

Sólo se requiere adquirir las cámaras, los cables de extensión USB, el equipo de protección (UPS) y la computadora que codifique el vídeo.

La instalación del cableado y colocación de cámaras en este sistema no es muy compleja, por lo que no requiere de personal especializado ni de mucho tiempo, por lo tanto el costo se estima que no sea mayor de $500.00.

5.8 VIGILANCIA CON CÁMARAS IP

Las cámaras IP son otra opción para implementar este tipo de sistemas, cabe mencionar que este tipo de cámaras cuenta con características que permiten una conexión más fácil a internet, pero debido a esto el costo de estas es elevado.

Los sistemas de seguridad basados en cámaras IP son sistemas de vigilancia remota digital. Este tipo de cámaras cuentan con 3 características:

1.- Es una cámara de vídeo de gran calidad.

2.- Contienen un chip de compresión que prepara las imágenes para ser transmitidas por internet.

3.- Cuentan con un ordenas que se conecta por sí mismo a internet.

Como anteriormente se menciona las cámaras IP comprimen la imagen digital en una imagen que contiene menos datos que permiten una transferencia más eficiente a través de la red.

La resolución de las imágenes digitales se mide en píxeles. La imagen más detallada es la que tiene más datos y por tanto mayor número de píxeles. Las imágenes con más detalles ocupan más espacio en los discos duros y precisan mayor ancho de banda para su transmisión. Para almacenar y transmitir imágenes a través de una red los datos deben estar comprimidos o consumirán mucho espacio en disco o mucho ancho de banda. Si el ancho de banda está limitado la cantidad de información que se envía debe ser reducida rebajando el número de frames (imágenes) por segundo o aceptando un nivel de calidad

inferior. Existen múltiples estándares de compresión. El estándar utilizado por las cámaras IP es MPEG4 este tipo de compresión permite que las imágenes transmitidas a través de la red utilicen menos ancho de banda.

Una cámara de red tiene su propia dirección IP y características propias de una computadora para gestionar la comunicación en la red. Todo lo que se precisa para la visualización de las imágenes a través de la red se encuentra dentro de la misma unidad. Una cámara de red puede describirse como una cámara y una computadora combinadas. Se conecta directamente a la red como cualquier otro dispositivo de red y cuenta con software propio para servidor Web, servidor FTP, cliente FTP.

Existen actualmente una gama infinita de modelos de cámaras IP y diferentes costos y de de acuerdo a las necesidades requeridas para la implementación de este sistema se sugiere un modelo del cual se describen sus características y se puede observar la cámara en la Figura 5.17.

Figura 5.17.- Cámara IP Vivotek CIC 901 Wireles

PRINCIPALES CARACTERISTICAS

- Flexible en la detección de movimientos y funciones de grabación de imágenes.
- Notificación de correo electrónico para la detección de movimiento.
- Subir imágenes de movimiento detectado a un determinado servidor FTP
- Detectable de visión nocturna con 8 LED IR.
- 2 entradas digitales y una salida digital con notificación de alertas.
- Apoyo IP estático, DHCP, PPPoE, DDNS, NTP.
- 2 niveles de gestión de usuario administrador/usuario.
- WEP 64/128 bits para Wi-Fi seguridad.

En la Tabla 5.8 Se pueden observar las especificaciones de ésta cámara.

Tabla 5.8.- Especificaciones del la Cámara IP Vivotek

MODELO:	**CIC-901W**
CPU:	• MIPS / JPEG codificar chip (VGA)
LENS:	• Sensor CMOS VGA con 307.200 píxeles
FORMATO DE IMAGEN:	• 640x480 (VGA),) • 320x240 (QVGA) • 160x120 (QQVGA)
FPS:	• Hasta 25fps @ QVGA, VGA @ 15fps
COMPRESIÓN DE VIDEO :	• M-JPEG
COMPRESIÓN DE AUDIO:	• PCM 64 kbit
LED:	• Potencia • LAN • WLAN
IR LED:	• 8 (Auto / Manual)
GPIO:	• Sensor en x 2

	• Alarma-out x 1
BOTÓN DE RESET:	• Sí
INTERFAZ DE RED:	• RJ-45 • 10/100 Fast Ethernet
PODER:	• 5V DC 2A
TEMPERATURA:	• 0°F a 50 °F
HUMEDAD:	• 20% a 80% sin condensación
DIMENSIÓN:	• 17 * 8.5 * 6.5 (cm)
PESO:	• 254.5g

La conexión de del sistema utilizando este tipo de cámaras se puede observar en la Figura 5.18.

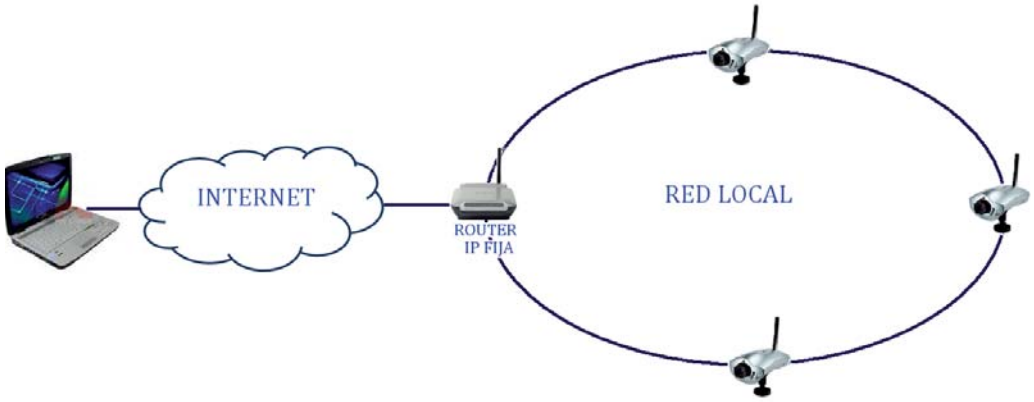

Figura 5.18.- Conexión del sistema con Cámaras IP

La Tabla 5.9 presenta el análisis económico del hardware necesario utilizando cámaras IP:

Tabla 5.9.- Costos del Hardware del sistema con cámaras IP

Objeto	Cantidad	Costo Unitario	Costo Total
Cámara IP	5	$3250.00	$16,250.00
UPS	2	$500.00	$1,000.00
Servidor	1	$8,000.00	$8,000.00
Ruteador	1	$600.00	$600.00
		Total	**$25,850.00**

La Tabla 5.10 muestra el análisis de costos totales del software que requiere el sistema de vídeo vigilancia.

Tabla 5.10.- Costos del Software del sistema con cámaras IP

Objeto	Cantidad	Costo Unitario	Costo Total
Windows Server 2003	1	$15,000.00	$15,000.00
Codificador de Windows Media	1	Gratuito	Gratuito
		Total	**$15,000.00**

En la Tabla 5.11 se observa el costo total del sistema de vídeo vigilancia para una área.

Tabla 5.11.- Costo total del sistema

Objeto	Cantidad	Costo Total
Hardware	1	$25,850.00
Software	1	$15,000.00
	Total	**$40,850.00**

CONCLUSIONES

Ante la inseguridad que se vive actualmente, la sociedad se ha visto obligada a buscar formas que ofrezcan una mayor seguridad en la protección tanto de vidas humanas, así como de los bienes que se tienen. De esta manera, muchos organismos públicos y privados, lo mismo que de forma individual, han empezado a implementar diversos modos que permitan mantener una vigilancia de los lugares en donde ocurren o puedan ocurrir eventos que dañen a las personas, ya sea físicamente o en sus propiedades. Uno de estos mecanismos de vigilancia es el uso de cámaras de vídeo.

La implementación del sistema de vídeo vigilancia pretende disminuir el problema de inseguridad que ha crecido dentro de la ESIME Zacatenco, la realización de este sistema cumple con los objetivos planteados al inicio, dichos objetivos fueron la configuración de un servidor, la codificación del vídeo y el diseño de una página web, que al trabajar de manera conjunta, forman un sistema efectivo de seguridad.

De acuerdo con las necesidades del proyecto, se propuso un sistema basado en un servidor, un codificador, una cámara web y una página de internet como interfaz gráfica para el usuario. Para la mejor comprensión del funcionamiento del sistema de monitoreo, se planteó un panorama general sobre el desempeño de los sistemas de vídeo vigilancia, en la actualidad en diferentes lugares del Distrito Federal, incluido el Instituto Politécnico Nacional.

Se explicó la teoría en la que está basado dicho sistema, la cual es de gran importancia y utilidad, por medio de ésta, el usuario puede familiarizarse con el tema, para posteriormente entender fácilmente como es que se establece la comunicación vía internet desde el servidor hacia los clientes.

Para la implementación del sistema de seguridad se detalló el funcionamiento de cada elemento utilizado, primero individualmente, tanto el hardware como el

software, y después se describió como funcionan de manera conjunta todos los elementos.

Para llevar a cabo este proyecto, primero se configuró un servidor bajo la plataforma Windows Server 2003, el cual es encargado de transmitir el vídeo obtenido de la cámara web mediante un codificador, y es observado por los usuarios a través de una página web realizada en Dreamweaver.

RECOMENDACIONES

En este trabajo se hizo la propuesta para instalar este sistema, dicha propuesta contiene los puntos necesarios para la vídeo vigilancia en cualquier lugar, en este caso en los laboratorios de computación de la ESIME, pero es importante hacer mención sobre otras tareas que se puedan realizar para la mejora del funcionamiento de este equipo de seguridad, entre las cuales está la utilización de dispositivos especiales de grabación para almacenar el vídeo por períodos de 7 días o más, software que permita la captura de fotogramas al detectar movimiento o en un intervalo de tiempo establecido por el usuario y poder almacenar dichos fotogramas de la manera que el cliente desee, ya sea en una computadora o en otros medios de almacenamiento. Otro aspecto que se debe tener en cuenta es la seguridad del sistema, esto es, permitir el acceso únicamente a las personas autorizadas para evitar daños al servidor, y por consecuente, daños al sistema de vídeo vigilancia. También es de gran utilidad, contar con otro equipo servidor de respaldo, para que en caso de una falla en el servidor que no se pueda corregir fácilmente, el sistema continúe monitoreando el lugar. Por el solo hecho de que la tecnología avanza constantemente, este sistema de seguridad puede utilizar tanto hardware como software más sofisticado que mejore el rendimiento y resuelva las necesidades del usuario y son estas necesidades las que determinarán que dispositivos puede utilizar para obtener el funcionamiento más óptimo y a un precio accesible.

APÉNDICE

CÓDIGO DE LA PÁGINA PRINCIPAL

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>:: CLN ::</title>
<link rel="stylesheet" href="2col_leftNav.css" type="text/css" />
<style type="text/css">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>:: CLN ::</title>
<link rel="stylesheet" href="2col_leftNav.css" type="text/css" />
<style type="text/css">
<!--
.Estilo1 {font-family: Verdana, Arial, Helvetica, sans-serif}
.Estilo5 {font-family: Georgia, "Times New Roman", Times, serif}
.Estilo6 {color: #000000}
.Estilo7 {color: #000000; font-family: Verdana, Arial, Helvetica, sans-serif; }
-->
</style>
</head>

<BODY BACKGROUND="liquido.jpg" style="background-repeat: no-repeat;
background-attachment: fixed; background-position: center center;" >
<!-- The structure of this file is exactly the same as 2col_rightNav.html;
     the only difference between the two is the stylesheet they use -->
<body>
<div id="masthead">
  <div align="center">
    <h1><span class="Estilo1"><img src="ipn.jpg" alt="" width="137" height="186"
align=left /></span></h1>
    <h1><span class="Estilo5"><img src="esime.jpg" alt="" width="197"
height="166" align="right" /></span></h1>
    <h2 class="Estilo5">Instituto Polit&eacute;cnico Nacional </h2>
    <h2 class="Estilo5">Escuela Superior de Ingenier&iacute;a Mec&aacute;nica y
El&eacute;ctrica </h2>
    <h2 class="Estilo5">Ingenier&iacute;a en Comunicaciones y
Electr&oacute;nica</h2>
    <h3 class="Estilo5">Academia de Computaci&oacute;n </h3>
    <p class="Estilo5"> </p>
    <h2 class="Estilo5">Monitoreo de los Laboratorios de Computaci&oacute;n
</h2>
    <h1> </h1>
  </div>
```

```
  <div id="globalNav">
    <h2 align="center"><a href="Lab1.htm">Laboratorio 1 </a> | <a
href="Lab2.htm">Laboratorio 2 </a> | <a href="Rec.htm">Recepci&oacute;n</a>
</h2>
  </div>
</div>
<!-- end masthead -->
<div id="content">
  <div id="breadCrumb"></div>
  <center><div class="feature"><center>
  </center>
    </div>
    <h2 id="pageName"> </h2>
  </center>
  <div class="feature">
  <center>
    <p>   </p>
          </center>
    <p> </p>
    <h3> </h3>
  </div>
</div>
<div id="navBar"><div id="sectionLinks"></div>
  <div class="relatedLinks"></div>
</div>
<!--end navbar -->
<div id="siteInfo">  <div align="center">CLN 2007 </div>
</div>
<br />
</body>
</html>
.Estilo1 {font-family: Verdana, Arial, Helvetica, sans-serif}
.Estilo5 {font-family: Georgia, "Times New Roman", Times, serif}
.Estilo6 {color: #000000}
.Estilo7 {color: #000000; font-family: Verdana, Arial, Helvetica, sans-serif; }
-->
</style>
</head>
<BODY BACKGROUND="liquido.jpg" style="background-repeat: no-repeat;
background-attachment: fixed; background-position: center center;" >
<!-- The structure of this file is exactly the same as 2col_rightNav.html;
     the only difference between the two is the stylesheet they use -->
<body>
<div id="masthead">
  <div align="center">
    <h1><span class="Estilo1"><img src="ipn.jpg" alt="" width="137" height="186"
align=left /></span></h1>
```

```
   <h1><span class="Estilo5"><img src="esime.jpg" alt="" width="197"
height="166" align="right" /></span></h1>
   <h2 class="Estilo5">Instituto Polit&eacute;cnico Nacional </h2>
   <h2 class="Estilo5">Escuela Superior de Ingenier&iacute;a Mec&aacute;nica y
El&eacute;ctrica </h2>
   <h2 class="Estilo5">Ingenier&iacute;a en Comunicaciones y
Electr&oacute;nica</h2>
   <h3 class="Estilo5">Academia de Computaci&oacute;n </h3>
   <p class="Estilo5"> </p>
   <h2 class="Estilo5">Monitoreo de los Laboratorios de Computaci&oacute;n
</h2>
   <h1> </h1>
  </div>
  <div id="globalNav">

<!---Inicio del código de los enlaces a las distintas áreas a monitorear-->

<h2 align="center"><a href="Lab1.htm">Laboratorio 1 </a> | <a
href="Lab2.htm">Laboratorio 2 </a> | <a href="Rec.htm">Recepci&oacute;n</a>
</h2>

<!---Fin del código de los enlaces a las distintas áreas a monitorear-->

  </div>
</div>
<!-- end masthead -->
<div id="content">
  <div id="breadCrumb"></div>
  <center><div class="feature"><center>
  </center>
    </div>
    <h2 id="pageName"> </h2>
  </center>
  <div class="feature">
  <center>
    <p>   </p>
          </center>
    <p> </p>
    <h3> </h3>
  </div>
</div>
<div id="navBar"><div id="sectionLinks"></div>
  <div class="relatedLinks"></div>
</div>
<!--end navbar -->
<div id="siteInfo">  <div align="center">CLN 2007 </div>
</div>
```

```
<br />
</body>
</html>
```

CÓDIGO DE LA PÁGINA QUE MONITOREA A UN LUGAR ESPECÍFICO

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>CLN Monitoreo</title>
<link rel="stylesheet" href="emx_nav_right.css" type="text/css" />
<script type="text/javascript">
<!--
var time = 3000;
var numofitems = 7;

function menu(allitems,thisitem,startstate){
  callname= "gl"+thisitem;
  divname="subglobal"+thisitem;
        this.numberofmenuitems = 7;
        this.caller = document.getElementById(callname);
        this.thediv = document.getElementById(divname);
        this.thediv.style.visibility = startstate;
}

function ehandler(event,theobj){
  for (var i=1; i<= theobj.numberofmenuitems; i++){
          var shutdiv =eval( "menuitem"+i+".thediv");
    shutdiv.style.visibility="hidden";
        }
        theobj.thediv.style.visibility="visible";
}

function closesubnav(event){
  if ((event.clientY <26)||(event.clientY > 85)){
    for (var i=1; i<= numofitems; i++){
      var shutdiv =eval('menuitem'+i+'.thediv');
                        shutdiv.style.visibility='hidden';
                }
        }
}
</script>
<style type="text/css">
<!--
.Estilo1 {color: #005FA9}
-->
```

```
</style>
</head>
<body onmousemove="closesubnav(event);">
<div id="row1">
  <div id="siteName">
    <h1>        Laboratorios de Computaci&oacute;n de ESIME
Zacat&eacute;nco</h1>
  </div>

<!-- Inicio del Código de la Barra Superior de la Página -->


  <div id="globalNav">
    <img alt="" src="gblnav_left.gif" height="32" width="4" id="gnl" /> <img alt=""
src="glbnav_right.gif" height="32" width="4" id="gnr" />
    <div id="globalLink">    <a href="Lab2.htm" id="gl2" class="glink"
onmouseover="ehandler(event,menuitem2);">Laboratorio 2 </a><a href="Rec.htm"
id="gl3" class="glink"
onmouseover="ehandler(event,menuitem3);">Recepci&oacute;n</a></div>
  </div>

<!-- -Fin del Código de la Barra Superior de la Página -->


  <div id="subglobal2" class="subglobalNav">
    <a href="#">subglobal2 link</a> | <a href="#">subglobal2 link</a> | <a
href="#">subglobal2
    link</a> | <a href="#">subglobal2 link</a> | <a href="#">subglobal2 link</a> | <a
href="#">subglobal2
    link</a> | <a href="#">subglobal2 link</a>
  </div>
  <div id="subglobal3" class="subglobalNav">
    <a href="#">subglobal3 link</a> | <a href="#">subglobal3 link</a> | <a
href="#">subglobal3
    link</a> | <a href="#">subglobal3 link</a> | <a href="#">subglobal3 link</a> | <a
href="#">subglobal3
    link</a> | <a href="#">subglobal3 link</a>
  </div>
  <div id="subglobal4" class="subglobalNav">
    <a href="#">subglobal4 link</a> | <a href="#">subglobal4 link</a> | <a
href="#">subglobal4
    link</a> | <a href="#">subglobal4 link</a> | <a href="#">subglobal4 link</a> | <a
href="#">subglobal4
    link</a> | <a href="#">subglobal4 link</a>
  </div>
  <div id="subglobal5" class="subglobalNav">
    <a href="#">subglobal5 link</a> | <a href="#">subglobal5 link</a> | <a
href="#">subglobal5
```

```
   link</a> | <a href="#">subglobal5 link</a> | <a href="#">subglobal5 link</a> | <a
href="#">subglobal5
   link</a> | <a href="#">subglobal5 link</a>
  </div>
  <div id="subglobal6" class="subglobalNav">
   <a href="#">subglobal6 link</a> | <a href="#">subglobal6 link</a> | <a
href="#">subglobal6
   link</a> | <a href="#">subglobal6 link</a> | <a href="#">subglobal6 link</a> | <a
href="#">subglobal6
   link</a> | <a href="#">subglobal6 link</a>
  </div>
  <div id="subglobal7" class="subglobalNav">
   <a href="#">subglobal7 link</a> | <a href="#">subglobal7 link</a> | <a
href="#">subglobal7
   link</a> | <a href="#">subglobal7 link</a> | <a href="#">subglobal7 link</a> | <a
href="#">subglobal7
   link</a> | <a href="#">subglobal7 link</a>
  </div>
  <div id="subglobal8" class="subglobalNav">
   <a href="#">subglobal8 link</a> | <a href="#">subglobal8 link</a> | <a
href="#">subglobal8
   link</a> | <a href="#">subglobal8 link</a> | <a href="#">subglobal8 link</a> | <a
href="#">subglobal8
   link</a> | <a href="#">subglobal8 link</a>
  </div>
</div>
<!-- end row1 -->
<div id="pagecell1">
  <!--pagecell1-->
  <img alt="" src="tl_curve_white.gif" height="6" width="6" id="tl" /> <img alt=""
src="tr_curve_white.gif" height="6" width="6" id="tr" />
  <div id="breadCrumb">
  </div>
  <div id="pageName">
   <h2>          Laboratorio  1 <img src="esime2.jpg" alt="" name="esime_imag"
width="160" height="140" id="esime_imag" /></h2>
  </div>
  <div id="col2">
   <div class="feature">

<!-- -Inicio del Código del Reproductor de Video de la Página -->

        <table border="0" width="100%" height="80%">
                <tr>
                        <td width="100%">
                        <p align="center">
                        <script language="Javascript">
```

```
                        if( g_bNetscape )
                        {
                                document.writeln( "<APPLET mayscript
code=WMPNS.WMP name=WMP1 width=450 height=350 MAYSCRIPT >" );
                        }
                    </script>
                    <OBJECT CLASSID="clsid:6BF52A52-394A-11D3-B153-
00C04F79FAA6" ID="WMP">
                    <PARAM NAME="Name" VALUE="WMP1">
                    <PARAM NAME="URL"
VALUE="mms://148.204.219.120/Camara">
                    </OBJECT>

                    <OBJECT CLASSID="clsid:6BF52A52-394A-11D3-B153-
00C04F79FAA6" ID="WMP">
                    <PARAM NAME="Name" VALUE="WMP2">
                    <PARAM NAME="URL"
VALUE="mms://148.204.219.120\Camara3">
                    </OBJECT></td>
                </tr>
                <tr>
                        <td width="100%"><p align="center"> 
            <script language="Javascript">
                        if( !g_bNetscape )
                        {
                                document.writeln( "<input type=\"button\"
id=\"cmdStandAlone\" value=\"" + L_LAUNCHSAP_TEXT + "\">" );
                        }
                    </script>
                </tr>
        </table>

<!-- -Fin del Código del Reproductor de Video de la Página -->

   </div>
  </div>

<!-- -Inicio del Código de la Barra Lateral de la Página -->

  <div id="pageNav" align="left">
    <div id="sectionLinks">      <a href="C1L1.htm">C&aacute;mara 1 - Lab 1 </a>
<a href="C2L1.htm">C&aacute;mara 2 - Lab 1 </a><a
href="C1L2.htm">C&aacute;mara 1 - Lab 2 </a>  <a
href="C2L2.htm">C&aacute;mara 2 - Lab 2 </a>  <a
href="Index.htm">Principal</a>
    </div>
    <div class="relatedLinks">
      <h3>Otros Enlaces </h3>
```

```
    <a href="http://www.ipn.mx">P&aacute;gina del IPN</a><a
href="http://www.esimez.ipn.mx">P&aacute;gina de la ESIME</a> <a
href="http//azul2.bnct.ipn.mx/~computacion">P&aacute;gina de la Academia de
Computaci&oacute;n </a></div>
  </div>

<!-- -Fin del Código de la Barra Lateral de la Página -->

  <!--end col1 div -->
  <div id="siteInfo">    2007
    CLN Monitoreo </div>
</div>
<!--end pagecell1-->
<br />
<script type="text/javascript">
    <!--
      var menuitem1 = new menu(7,1,"hidden");
                          var menuitem2 = new menu(7,2,"hidden");
                          var menuitem3 = new menu(7,3,"hidden");
                          var menuitem4 = new menu(7,4,"hidden");
                          var menuitem5 = new menu(7,5,"hidden");
                          var menuitem6 = new menu(7,6,"hidden");
                          var menuitem7 = new menu(7,7,"hidden");
    // -->
    </script>
</body>
</html>
```

GLOSARIO TÉCNICO

Clustering.- Es la agrupación que realizan los buscadores para no mostrar más de un cierto número de páginas de una web para una determinada búsqueda.

Códec.- Es una abreviatura de Codificador-Decodificador. Describe una especificación desarrollada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos o una señal.

Extranet.- 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.

Internet.- La mayor red pública de redes TCP/IP.

Intranet.- Es una red de computadoras dentro de una red de área local (LAN) privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no.

Loopback.- El dispositivo de red loopback es un interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado. El valor en IPv4 es 127.0.0.1. y ::1 para el caso de IPv6. Se utiliza en tareas de diagnóstico de conectividad y validez del protocolo de comunicación, así como para indicar que el destino del puntero o URL es el mismo host.

GLOSARIO DE SIGLAS

ARP (Protocolo de Resolución de Direcciones)

ASCII (Código Estadounidense Estándar para el Intercambio de Información)

ASF (Formato de Difusión Avanzada)

ASP (Servidor de Páginas Activas)

CBR (Tasa de Bits Constante)

CCD (Dispositivo de Cargas Interconectadas)

CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía)

CCTP (Circuito Cerrado Par Trenzado)

CCTV (Circuito Cerrado de Televisión)

CFML (Lenguaje de Marcado de ColdFusion)

CMOS (Semiconductor de Óxido Metálico Complementario)

COM (Modelo de Objeto Componente)

CRC (Chequeo de Redundancia Cíclica)

CSS (Hojas de Estilos en Cascada)

CTI (Integración de dispositivos telefónicos en los computadores).

DHCP (Protocolo de Configuración de Anfitrión Dinámico)

DNS (Sistema de Dominio de Nombres)

DOM (Modelo de Objetos de Documento)

DSP (Procesamiento de Señales Digitales)

DVRs (Grabadoras de Video Digital)

EBCDIC (Código Extendido de Binario Codificado Decimal)

EDL (Lista de Decisiones de Edición)

EMI (Interferencia Electromagnética)

FAT (Tabla de Asignación de Archivos)

FTP (Protocolo de Transmisión de Archivos)

HTML (Lenguaje de Marcado de Hipertextos)

HTTP (Protocolo de Transmisión Hipertexto)

ICMP (Protocolo de Mensajes de Control de Internet)

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)

IGMP (Protocolo de Administración de Grupos de Internet)

IIS (Servidor de Información de Internet)

IP (Protocolo de Internet)

JSP (Páginas de Servidor Java)

LAN (Red de Área Local)

MMC (Consola de Gestión de Microsoft)

MMS (Sistema de Mensajería Multimedia)

MPEG (Grupo de Expertos en Imágenes en Movimiento)

NAS (Almacenamiento de Redes Adjuntas)

OSI (Interconexión de sistemas abiertos)

PHP (Procesador de Hipertexto)

POP (Protocolo de Oficina Postal)

PTZ (Vista Panorámica, Inclinación y Ampliación)

SAN (Almacenamiento de Área de Redes)

SDK (Kit de Desarrollo de Software)

SMIL (Lenguaje de Integración Multimedia Sincronizada)

SMP (Multiproceso Simétrico)

SMTP (Protocolo de Transferencia Simple de Correo)

SNMP (Protocolo de Manejo de Red Simple)

RTSP (Protocolo de Flujo de Datos en Tiempo Real)

SSH (Capa de Seguridad)

TCP (Protocolo de Control de Transmisión)

TI (Tecnologías de la Información)

UDDI (Descripción, Descubrimiento e Integración Universal)

UDP (Protocolo de Datagrama de Usuario)

UPS (Sistema de Energía Ininterrumpida)

UTP (Par Trenzado no Blindado)

VBR (Tasa de Bits Variable)

VGA (Matriz Gráfica de Video)

VPN (Red Privada Virtual)

VTR (Grabadora de Video Cintas)

WMI (Instrumentación Administrativa de Windows)

XML (Lenguaje de Marcas Extensible)

REFERENCIAS

BARAJA, Saulo ***Curso de Protocolos de TCP/IP*** http://www.saulo.net/pub/tcpip

BARBERÁN, Manuel ***Cómo funciona una webcam,*** Roberto Solans. Áreas net. http://www.ctv.es/areas/comofunciona/multimedia/3.htm

BLACK, Uyless ***Redes de Computadores Protocolos, normas e interfaces*** Editorial Alfaomega.

CCTV Cámaras de Seguridad CCTV Radiocomunicación, http://www.cctv-seguridad.com.mx

CCTV y Vigilancia por Video sobre 10G IP. The Siemon Company, www.siemon.com

EL ECONOMISTA S.A. de C.V. ***Instalarán sistema de vídeo vigilancia en el Metro***. Copyright © 1994-2000, http://www.economista.com.mx/sinprivilegios/articulos/2007-05-09-35931.

MICROSOFT Corporation. ***Codificador de Windows Media 9 Series***. http://www.microsoft.com/windows/windowsmedia/es/9series/encoder/default.aspx

Servidor Guardián por Internet. Serviguard, http://www.serviguard.com.mx

STALLINGS, William ***Comunicaciones y Redes de Computadores*** Madrid, 2000. Editorial Prentice Hall.

TALENS, Oliag Sergio**, HERNÁNDEZ,** Orallo José ***INTERNET Redes de computadores y sistemas de información*** Segunda edición, 1998. Editorial Paraninfo.

UNAM, Instituto de Ingeniería ***Sistema de Video Vigilancia IP*** México.1995 - 2007, http://www.ii.unam.mx.

Video Vigilancia en guarderías a través de Internet. DATACYL, Valladolid, http://www.e-guarderias.com