UNIVERSIDAD CATOLICA DE SANTIAGO DE GUAYAQUIL

Facultad de Educación Técnica para el Desarrollo
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

Tesis de Grado

Previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

Mención en Gestión Empresarial

Tema

"ESTUDIO, DISEÑO E IMPLEMENTACION DE UN SISTEMA DE VIDEO VIGILANCIA REMOTO CON RESPALDO DE SERVIDOR PARA LAS AULAS DE LA FACULTAD TECNICA PARA EL DESARROLLO"

Realizado por

Eduardo Enrique Ojeda Mancero

Blanca Esmeralda Cruz Sánchez

Huber Gustavo Espinoza Ramírez

Santiago Joel Escobar Toapanta

Director de Tesis

Ing. Orlando Philco Asqui

Guayaquil – Ecuador

2010

TESIS DE GRADO

Título

“ESTUDIO, DISEÑO E IMPLEMENTACION DE UN SISTEMA DE VIDEO VIGILANCIA REMOTO CON RESPALDO DE SERVIDOR PARA LAS AULAS DE LA FACULTAD TECNICA PARA EL DESARROLLO”

Presentada a la Facultad de Educación Técnica para el Desarrollo, Carrera de Ingeniería en Telecomunicaciones de la Universidad Católica de Santiago de Guayaquil.

Por:

Eduardo Enrique Ojeda Mancero

Blanca Esmeralda Cruz Sánchez

Huber Gustavo Espinoza Ramírez

Santiago Joel Escobar Toapanta

Para dar cumplimiento con uno de los requisitos para optar por el Título de:

INGENIERO EN TELECOMUNICACIONES

Mención en Gestión Empresarial

Miembros del Tribunal

_____

Ing. Héctor Cedeño A.
Decano de la Facultad

_____ _____

Ing. Pedro Tutiven López — Ing**.** Orlando Philco Asqui

Director de Carrera — **Director de Tesis**

_____ _____

Dr. Kléber López Parrales — Ing. Víctor del Valle Ramos

Coordinador Administrativo — **Coordinador Académico**

AGRADECIMIENTO

Nuestra inmensa gratitud a nuestros padres, madres, hermanos, y demás familiares que siempre estuvieron demostrando el aliento y apoyo necesario para luchar por conseguir nuestra objetivo, cual es la de ser profesionales en Ingeniería en Telecomunicaciones.

A nuestros profesores, quienes dedicaron su esfuerzo y dedicación para transmitirnos sus enseñanzas, a las autoridades y personal administrativo de la Facultad Técnica y en especial a nuestro Director de Tesis, Ing. Orlando Philco por su valiosa colaboración en el desarrollo de la tesis.

DEDICATORIA

Esta tesis está dedicada a nuestros/as compañeros/as de la Facultad Técnica y a todos los estudiantes de todas las facultades que tengan como carrera las Telecomunicaciones; esta obra es el producto de un arduo trabajo de diseño e implementación y lo queremos dejar como evidencia para que sirva de consulta o apoyo pedagógico y referencia a los futuros profesionales, de todo lo que se ha planteado, investigado e implementado.

A todos nuestros familiares, profesores y autoridades por su paciencia, apoyo incondicional y consejos, a todos ellos, está dedicada esta tesis.

RESUMEN

El presente trabajo de estudio y diseño es para la supervisión de los bienes activos de la Facultad Técnica para el Desarrollo. Es así que en el primer capítulo se trata de justificar porque monitorear remotamente mediante un sistema de video vigilancia, el capitulo 2, se enmarca en la metodología a utilizar y esta es el marco teórico de sistemas de video vigilancia, el capitulo 3 trata de la selección de equipos y dispositivos de los sistema de video vigilancia. El 4º capitulo se basa en los criterios del diseño, es decir el paso técnico necesario para la futura implementación.

El capitulo 5 nos indica de qué forma se pueden acceder remotamente al sistema, se detalla las pruebas del sistema.

Se investiga textos especializados sobre redes IP y páginas de los fabricantes de las cámaras de video. La propuesta de la tesis es un sistema hibrido de cámaras analógicas que por medio de un equipo llamado DVR (Grabador de Video Digital) se puede llevar a paquetes la información y de esta forma puede ser monitoreada desde cualquier lugar que tenga acceso a internet.

INDICE

CAPITULO III

CAPITULO IV

CAPITULO V

CAPITULO 1

INTRODUCCION

La presente tesis, desarrolla el estudio y diseño de un sistema de video vigilancia con respaldo de servidor para supervisar los pasillos de la Facultad Técnica para el Desarrollo de la Universidad Católica. Hoy en día, la video vigilancia es parte normal de las operaciones en un entorno donde se debe supervisar y cuidar los activos y bienes de una empresa, institución y hasta en el hogar. Los sistemas de video monitoreo análogo ya quedaron en el pasado la tecnología de hoy, esta digitalizando las imágenes y estas pueden ser convertidas a paquetes las cuales logran viajar a través de la red.

Diseñar e implementar un sistema de video vigilancia para la Facultad Técnica es una aplicación de los conocimientos adquiridos a lo largo de la carrera en ingeniería de telecomunicaciones, la tesis presenta desde el primer capítulo la estructura del planteamiento del problema, la justificación y objetivos que se desarrollarán.

El capitulo dos, abarca los fundamentos y componentes de un sistema de voz y video sobre IP. El capitulo tres describe los sistemas de video vigilancia desde los que se llaman circuito cerrado de televisión hasta los que son basados en protocolo IP. El capitulo cuatro, enfoca la elección de los equipos del sistema a implementar. El capitulo cinco es acerca de la implementación del sistema en la Facultad Técnica para el Desarrollo.

1.1 PLANTEAMIENTO DEL PROBLEMA

Supervisar de manera remota y semi presencial las instalaciones de las Facultad Técnica cuidar y proteger sus bienes ante la eventualidad de robos, existe 32 aulas en la Facultad las cuales poseen computadoras modernas y que son propenso a su robo parcial o total. No se puede tener un guardia para cada aula, y tampoco un profesor permanente en el aula, la mayoría de los estudiantes se distraen y pueden acercarse personas inescrupulosas que se roben accesorios o toda la computadora de cualquier aula.

1.2 JUSTIFICACION

Con el uso de este recursos como es la video vigilancia vía IP (Protocolo de Internet), se tendrá con seguridad el monitoreo de la maquina en el aula ya que una cámara apuntando a la computadora, es un medio que detiene o persuade en la acción a la persona que desea llevarse o dañar los activos de la Facultad y de la Universidad en general.

El sistema posee un software de vigilancia que funciona con cámaras y codificadores de vídeo y proporciona funciones de supervisión de vídeo, grabación y gestión de eventos. La persona encargada de administrar el sistema puede realizar una grabación de vídeo continua, programada, activada por alarma y/o por detección de movimiento. El software dispone de múltiples funciones de búsqueda de eventos grabados con esto

es justificado la seguridad contra robo o perdida de accesorios dentro las aulas de la Facultad Técnica.

1.3 HIPOTESIS

El sistema de control y vigilancia propuesto en la tesis, es la mejor opción tecnológica que logra prevenir o evitar robos en cada una de las 32 aulas de la Facultad Técnica. Se puede monitorear los pasillos, el ingreso a las aulas y laboratorios si el encargado de supervisar no está ese momento observando las imágenes que transmite las cámaras, esta información tendrá su respaldo en un servidor de 1 Tera Bytes con lo cual se garantiza tener el grabado o almacenado el monitoreo de aulas las 24 horas del día, los 365 días del año.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Desarrollar el estudio, diseño e implementación de un sistema de video vigilancia con respaldo de servidor para todas las aulas de la Facultad Técnica para el Desarrollo.

1.4.2 OBJETIVOS ESPECIFICOS

1. Conocer el uso y manejo la transmisión de paquetes en redes.
2. Aplicar la selección adecuada en equipos de cámaras robóticas, accesorios y servidores conectados en red.

3. Desarrollar el diseño de cableado estructurado en los edificios de la Facultad.
4. Implementar un sistema de control y vigilancia con respaldo en servidor para todas las aulas de la Facultad Técnica.

CAPITULO 2

VOZ Y VIDEO BASADO EN PROTOCOLO IP

2.1 INTRODUCCION

Los últimos avances han hecho posible conectar cámaras directamente a una red de datos basada en el protocolo IP (Protocol internet). La tecnología de las cámaras IP permite al usuario tener una cámara en un sitio y ver el vídeo en tiempo real desde otro lugar a través de la red interna LAN, WAN o Internet. El desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización o señalización de tráfico, protocolos de transmisión en tiempo real, así como la aparición de nuevos estándares que permitan la calidad de servicio QoS (Quality of Service). Nos comprueban que las redes de próxima generación serán totalmente basadas en protocolo de internet. Se define a continuación sistemas basados en protocolo de internet.

2.1.1 VOZ SOBRE IP (VoIP)

La voz sobre IP es un grupo de recursos que hacen posible que la señal de voz viaje a través de internet empleando un protocolo IP (Internet Protocol). Esto quiere decir que transmite la información o señal de voz en forma digitalizada (paquetes) en lugar de enviarla conmutada (analógica) esto se lo hace a través de circuitos utilizables solo para la telefonía como una empresa telefónica convencional, se puede poner como ejemplo la Corporación Nacional de Telecomunicaciones CNT.

La voz sobre IP aprovecha la comunicación entre las computadoras, el protocolo IP que ha sido posible gracias a la evolución de las tecnologías que lo soportan, las

infraestructuras de telecomunicaciones y especialmente el acceso a la banda ancha. Este aprovechamiento logra que usemos un mismo un canal para transmitir voz y hasta video etc.

2.1.2 FUNCIONALIDAD

La voz sobre IP puede facilitar tareas que sería más difíciles de realizar usando las redes telefónicas rurales, se tiene las siguientes ventajas:

- Las llamadas telefónicas locales pueden ser automáticamente enrutadas a un teléfono VoIP, sin importar donde se esté conectando a la red, uno podría llevar consigo un teléfono VoIP en un viaje, y en cualquier sitio conectado a internet se podría recibir llamadas.
- Existen números gratuitos para usar con VoIP, claro que solo están disponibles en Estados Unidos, Inglaterra, Italia etc. y otros países de organizaciones como usuario VoIP.
- Los agentes de Call Center usando teléfonos VoIP pueden trabajar en cualquier lugar con conexión a internet lo suficientemente rápida.

2.1.3 PROTOCOLOS DE VOIP

El objetivo de VoIP es dividir en paquetes los flujos de voz para transportarlas sobre redes basados en IP. Los protocolos de las redes IP originalmente no fueron diseñados para el fluido el tiempo real de voz o cualquier otro tipo de medio de comunicación.

La PSTN (Public Switched Telephone Network o comúnmente llamada, Red pública Conmutada) está diseñada para la transmisión de voz, sin embargo tiene sus limitaciones tecnológicas.

Es por lo anterior que se crean los protocolos para VoIP, cuyo mecanismo de conexión abarca una serie de transacciones de señalización entre terminales que cargan fluidos flujos de voz para cada dirección de la conversación. Algunos de los protocolos VoIP más importantes son Asterisk PBX.

2.1.4 ASTERISK

Asterisk es una aplicación de lo que se denomina software libre (bajo licencia GPL, General Public License) que proporciona funcionalidades de una central telefónica (PBX, Private Branch eXchange). Como cualquier PBX, se puede conectar un número determinado de terminales telefónicos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP o bien a una red digital (RDSI, Red Digital de Servicios Integrados) tanto básicos como primarios.

Asterisk incluye muchas características y funcionalidades sus usuarios pueden crear nuevas funcionalidades escribiendo un dialplan o plan de marcación en el lenguaje de script de Asterisk o añadiendo módulos escritos en lenguaje C o en cualquier otro lenguaje de programación soportado por Linux.

Asterisk soporta muchos protocolos VoIP como pueden ser SIP, H.323, IAX y MGCP. Asterisk puede interoperar con terminales de voz IP actuando como un registrador y

como Gateway entre ambos. Asterisk no necesita ningún hardware adicional para el VoIP.

2.2 PROTOCOLO SIP

SIP (Session Initiation Protocol) es un protocolo de control y señalización usado mayoritariamente en los sistemas telefónicos basados en IP, que fue desarrollado por el IETF (Internet Engineering Task Force, Fuerza de Trabajo en Ingeniería de Internet) (RFC 3261). Dicho protocolo permite crear, modificar y finalizar sesiones multimedia con uno o más participantes y sus mayores ventajas recaen en su simplicidad y consistencia.

Hasta la fecha, existían múltiples protocolos de señalización tales como el H.323 de la ITU (Unión Internacional de Telecomunicaciones), el SCCP (Skinny Client Control Protocol) que es un protocolo propietario de control de terminal de Cisco, o el MGCP (Media Gateway Control Protocol) que es un protocolo de control de dispositivos, donde un Gateway esclavo (MG, Media Gateway) es controlado por un maestro (MGC, Media Gateway Controller), también llamado “call agent”.

Pero SIP está ganando la batalla del estándar, Cisco está progresivamente adoptando SIP como protocolo en sus sistemas de telefonía IP en lugar de H.323 y SCCP, Microsoft ha elegido SIP como protocolo para su nuevo OCS (Office Communication Server), y los operadores (de móvil y fijo) también están implantando SIP dentro de su estrategia de

convergencia, aprovechando de este modo la escalabilidad y interoperabilidad que nos proporciona el protocolo SIP.

2.2.1 FUNCIONES SIP

El protocolo SIP actúa de forma transparente, permitiendo el mapeo de nombres y la redirección de servicios ofreciendo así la implementación de la IN (Intelligent Network) red inteligente de la PSTN o red pública conmutada.

Para conseguir los servicios de la IN el protocolo SIP dispone de distintas funciones. A continuación se enumeran las más importantes:

- Localización de usuarios (SIP proporciona soporte para la movilidad).
- Capacidades de usuario (SIP permite la negociación de parámetros).
- Disponibilidad del usuario
- Establecimiento y mantenimiento de una sesión.

En definitiva, el protocolo SIP permite la interacción entre dispositivos, cosa que se consigue con distintos tipos de mensajes propios del protocolo que abarca esta sección. Dichos mensajes proporcionan capacidades para registrar y/o invitar un usuario a una sesión, negociar los parámetros de una sesión, establecer una comunicación entre dos a más dispositivos y, por último, finalizar sesiones.

2.2.2 OTROS PROTOCOLOS VoIP

En la actualidad, los protocolos más usados en VoIP son tres: SIP, H.323 y IAX2.

1. H.323 es un estándar de la ITU que provee especificaciones para ordenadores, sistemas y servicios multimedia por redes que no proveen QoS (calidad de servicio). Como principales características de H.323 tenemos:

- Implementa QoS de forma interna.
- Control de conferencias

2. IAX2 (Inter Asterisk eXchange) es un protocolo creado y estandarizado por Asterisk. Unas de sus principales características son: Media y señalización viajan en el mismo flujo de datos.

- Trunking
- Cifrado de datos

Una de las ventajas de este protocolo es que al enviar el "streaming" y la señalización por el mismo flujo de datos, se evitan problemas derivados del NAT (Network Address Translation, en español Traducción de Dirección de Red), se dice que una NAT es un mecanismo utilizado por routeadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente incompatibles direcciones. Entonces consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. Así pues, no es

necesario abrir rangos de puertos para el tráfico RTP (Real-time Transport Protocol, Protocolo de Transporte de Tiempo Real). Por último, IAX2 nos permite hacer trunking de forma que podemos enviar varias conversaciones por el mismo flujo, lo cual supone un importante ahorro de ancho de banda.

Finalmente, veamos qué hace de SIP un protocolo cada día más sólido. Aspectos importantes referentes a dicho protocolo se enumeran como sigue:

- El control de llamadas es stateless o sin estado, y proporciona escalabilidad entre los dispositivos telefónicos y los servidores.
- SIP necesita menos ciclos de CPU para generar mensajes de señalización de forma que un servidor podrá manejar más transacciones.
- Una llamada SIP es independiente de la existencia de una conexión en la capa de transporte.
- SIP soporta autentificación de llamante y llamado mediante mecanismos HTTP.
- Autenticación, criptografía y encriptación son soportados salto a salto por SSL/TSL pero SIP puede usar cualquier capa de transporte o cualquier mecanismo de seguridad de HTTP, como SSH o S-HTTP.
- Un proxy SIP puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultáneamente.

En definitiva, SIP es un protocolo con una gran escalabilidad, modular y muy eficiente. Obsérvese los cambios de las redes en la figura 2.1 y figura 2.2. Gracias a los protocolos basados totalmente en Ip se puede reducir infraestructura en las redes, disminución de costos, confiabilidad y hasta seguridad.

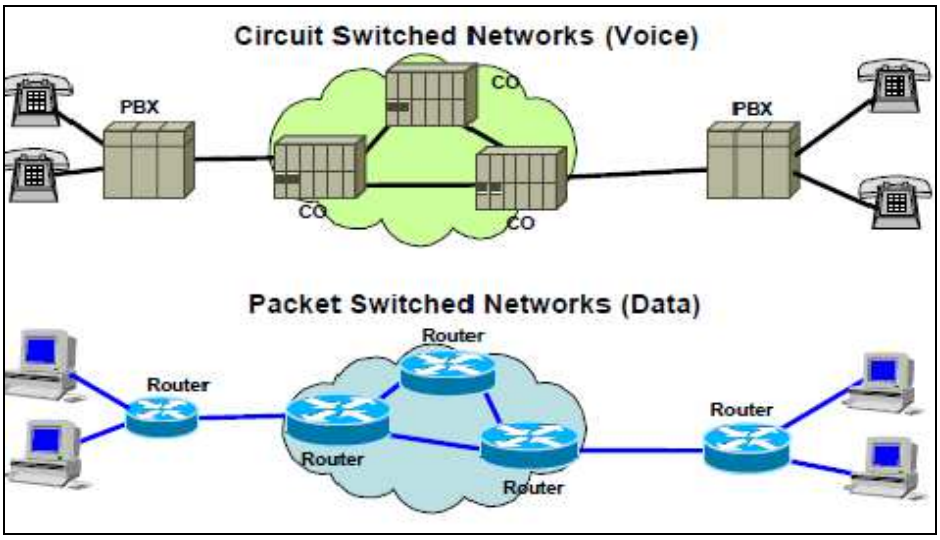

Figura 2.1 Las redes de voz y datos son separadas y así sus servicios

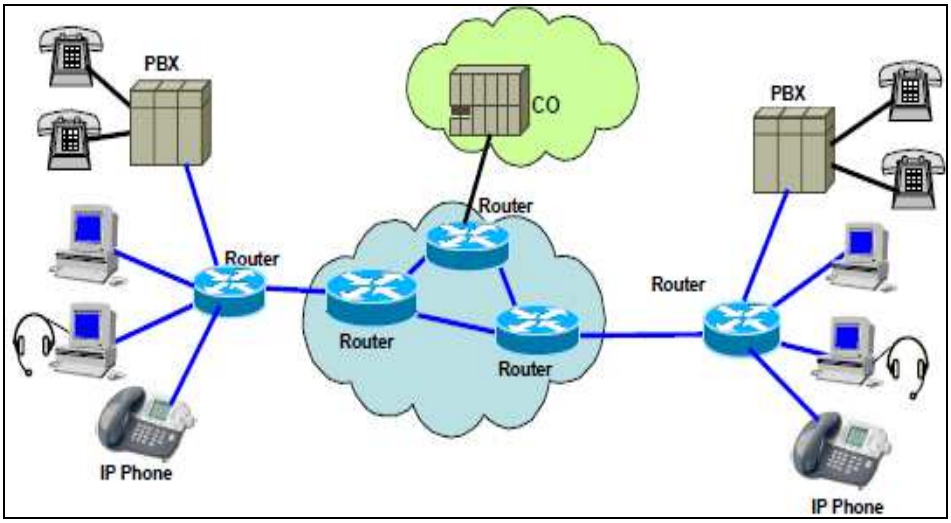

Figura 2.2 Actualmente las redes y sus servicios convergen en una red

2.2.3 ARQUITECTURA SIP

El estándar define varios componentes SIP y hay varias formas de implementarlos en un sistema de control de llamadas.

- Servidores User Agent,
- Proxies
- Registrars,
- Redirect
- Location.

A menudo, estos elementos son entidades lógicas que se ubican todas juntas para conseguir una mayor velocidad de procesamiento que dependerá a su vez de una buena configuración.

Normalmente los UA, user agent en español agente usuarios, son una aplicación en el ordenador del usuario, aunque a veces los UA también pueden ser teléfonos móviles, PSTN (red conmutada), Gateways, una PDA (Personal Digital Assistant o Ayudante Personal Digital) etc. Obsérvese la figura 2.3 que detalla una infraestructura básica usando protocolo SIP, la comunicación de voz es mayormente IP pero es compatible con la red conmutada por medio de Gateway, proxies que entienden la señalización y por ello se mantiene fiable la comunicación de voz.

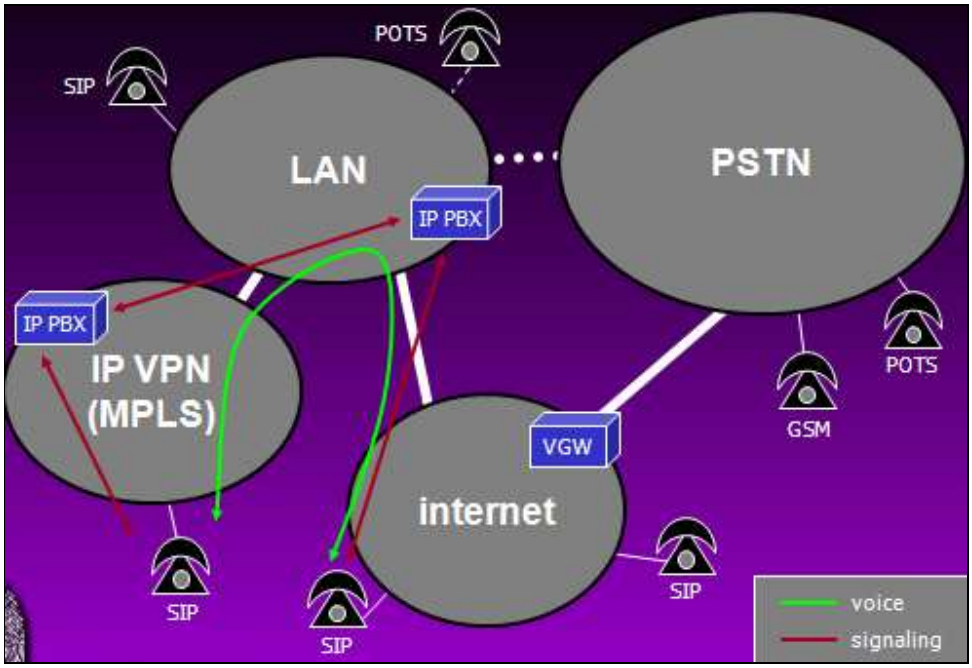

Figura 2.3 Arquitectura con Protocolo SIP en telefonía

2.3 VIDEO SOBRE IP

El sistema de video sobre IP permite al usuario transmitir imágenes y video de alta resolución en tiempo real a través de redes IP como internet para ser visualizada en la computadora con el navegador o con un software especial en caso de se utilicen múltiples cámaras y se desee grabar la información, controlar la cámara de forma remota.

Las principales ventajas de video sobre IP son:

Muy buena calidad en el video.

100% adaptables con sistemas de alarma y analógicos existentes.

Seguridad de acceso.

Flexibilidad y adaptabilidad.

La gestión de monitorear los lugares remotos permite a las organizaciones, empresas etc el obtener un mejor sistema de seguridad de una manera rápida y económica.

Los principales componentes de una red de video sobre IP son las cámaras IP o de red y una conexión a internet o una red IP. Otros elementos opcionales son las grabadoras de video digital (DVR´s) los discos de almacenamiento, ruteadores, Hubs, switches, etc.

En la figura 2.4 se observa los pasos necesarios para la transmisión de video.

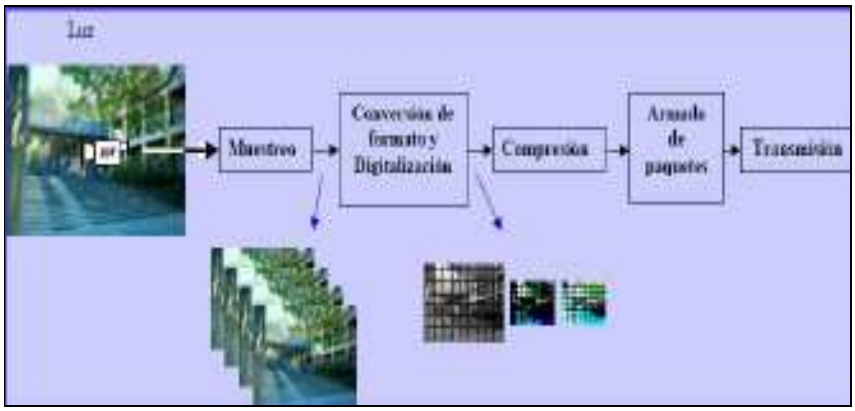

Figura 2.4 Digitalización de la información previo a su transmisión

2.3.1 DIGITALIZACION DE VIDEO

Digitalizar un video es transformar las imágenes y audio a un formato binario como una secuencia de fotos con sonido en pistas separadas, además hay que tomar en cuenta que entra en juego una tercera dimensión, el tiempo. Por lo tanto una secuencia de video se genera mediante la proyección de un número de imágenes en un tiempo determinado, que al pasar rápido ante nuestros ojos, dan sensación de movimiento.

El ojo humano es capaz de distinguir 20 imágenes por segundo, si se muestran más de esa cantidad, se crea la ilusión de imagen en movimiento.

2.4 TECNICAS DE COMPRESION

La digitalización requiere de bits en comparación con la capacidad de almacenamiento disponible y gran velocidad de transmisión en comparación con la máxima velocidad admisible por los sistemas de comunicación digital a través del que deben enviarse.

Comprimir es reducir el tamaño de la información o señal, existen 2 razones importantes para comprimir, la primera es colocar los archivos, datos, audio o video en un espacio menor.

La segunda razón aparece fundamentalmente con las redes de comunicaciones. Pues el tiempo que se necesita para poder acceder o descargar archivos de gran tamaño por la red; si están comprimidos se tardará menos en enviarlos o recibirlos, ya sea por correo electrónico, web, ftp o cualquier otro protocolo de transferencia de datos.

Un ejemplo de compresión sería, una película de 90 minutos sin comprimir requeriría unos 120 Gigabytes de espacio de almacenamiento, pero tan solo 4 Gigabytes de espacio si estuviese comprimido. En los medios de transmisión, un video sin comprimir necesita una velocidad de transmisión de 160 Megabits por segundo, mientras que una red típica puede alcanzar los 100 Mbps siendo además compartida por varios sistemas.

2.4.1 ALGORITMOS DE COMPRESION

La compresión es un proceso de reducción de la tasa de bits, esto implica la pérdida de información y una consecuente disminución de calidad. Pero esto es aceptable porque los algoritmos de codificación están diseñados para descartar la información semejante o redundante, información que resulta irrelevante al ojo humano.

Existen 2 tipos de algoritmos de compresión, estos son:

1. Algoritmo con perdida: Al utilizar los algoritmos de compresión con perdida, conocidos también como lossy, sobre los datos originales es imposible recuperar

los datos originales mediante algún procedimiento aplicado a los datos compresores.

La compresión con pérdida ha hecho crecer los sistemas multimedia, el trafico de imágenes, sonido y video presente en el internet es posible debido a la aplicación de estas técnicas de compresión a los contenidos antes de efectuarse la transmisión.

2. Algoritmos sin pérdida: También conocidos como lossless guardan absolutamente toda la información original, es decir es reversible, son utilizados en los casos en que no se puede dar perdida de información, como es en la compresión de datos; los datos originales pueden ser recuperados en su totalidad después de aplicar sobre los datos comprimidos un algoritmo compatible de descompresión.

   Estos algoritmos tienen la propiedad de disminuir el tamaño y conservar la totalidad de la información, la imagen reconstruida es matemáticamente y visualmente idéntica a la original.

   Se debe tener en cuenta que la compresión sin pérdida logra un índice de compresión muy bajo (aproximadamente 2:1), comparado con la compresión con perdida, con la cual una imagen pueda llegar a un índice de compresión de 25:1 con una pérdida mínima de la calidad de la misma.

   Esta forma de compresión se caracteriza porque la tasa de compresión que proporciona está limitada por la redundancia de datos de la señal original, es decir existe un límite teórico de compresión para los compresores sin perdida.

2.4.2 APLICACIONES DE LA COMPRESIÓN

Se dividen en dos grandes grupos:

a) Aplicaciones relacionadas con la transmisión de imagen: Son los casos en que se requiere enviar información en forma de imágenes de un emisor a un receptor ocupando el mínimo de ancho de banda posible o minimizando el tiempo de transmisión, por ejemplo.

Comunicaciones Interpersonales: entre ellas podemos mencionar el video conferencia o el fax. En el video conferencia interesa ajustar el ancho de banda disponible, mientras que en el segundo caso ocupar el mínimo de tiempo posible la línea telefónica.

Imágenes vía Internet: para reducir el tiempo de espera en la recepción, las imágenes están soportadas en formatos gráficos que incorporan compresión, como, por ejemplo, GIF, JPEG, etc.

b) Aplicaciones relacionadas con el almacenamiento:

Muchas veces guardamos información como imágenes de planos, fotos, etc. El almacenamiento de esta información puede ir principalmente a discos duros o CD-ROM, pero las capacidades de almacenamiento son limitadas por lo que se hace indispensable comprimir la información. Esto, se hace más notorio en el caso del video.

2.4.3 ESTÁNDARES DE COMPRESIÓN DE VIDEO

La compresión de imágenes se aplica sobre una imagen individual haciendo uso de las similitudes entre píxeles próximos en la imagen y de las limitaciones del sistema de visión humana. JPEG (Joint Photographic Experts Group, en español Grupo o conjunto

de expertos en fotografía), es un ejemplo de una técnica de compresión de imágenes. La compresión de vídeo se aplica sobre series consecutivas de imágenes en una secuencia de vídeo, haciendo uso de las similitudes entre imágenes próximas. Un ejemplo de este tipo de técnicas es MPEG (Moving Picture Experts Group, en español Grupo de Expertos en Imágenes Móviles).

La efectividad de una técnica de compresión de imágenes viene dada por el ratio de compresión, calculado como el tamaño del archivo de la imagen original (sin comprimir) dividido por el tamaño del archivo de imagen resultante (comprimida). A mayor ratio de compresión se consume menos ancho de banda manteniendo un número de imágenes por segundo determinado. O si el ancho de banda se mantiene constante se aumenta el número de imágenes por segundo. Al mismo tiempo, un mayor nivel de compresión implica menor nivel de calidad de imagen para cada imagen individual.

Cuanto más sofisticada sea la técnica de compresión utilizada, más complejo y caro resultará el sistema. Lo que ahorre en ancho de banda y almacenamiento encarecerá los costos de latencia, codificación y complejidad del sistema. Otro factor adicional a considerar son los costos de las licencias y los gastos asociados a un número de estándares de compresión.

2.4.3 ESTANDARES DE VIDEO MPEG

Existen 4 formatos dependiendo del uso MPEG-1, MPEG-2, MPEG-4 y MPEG-7.

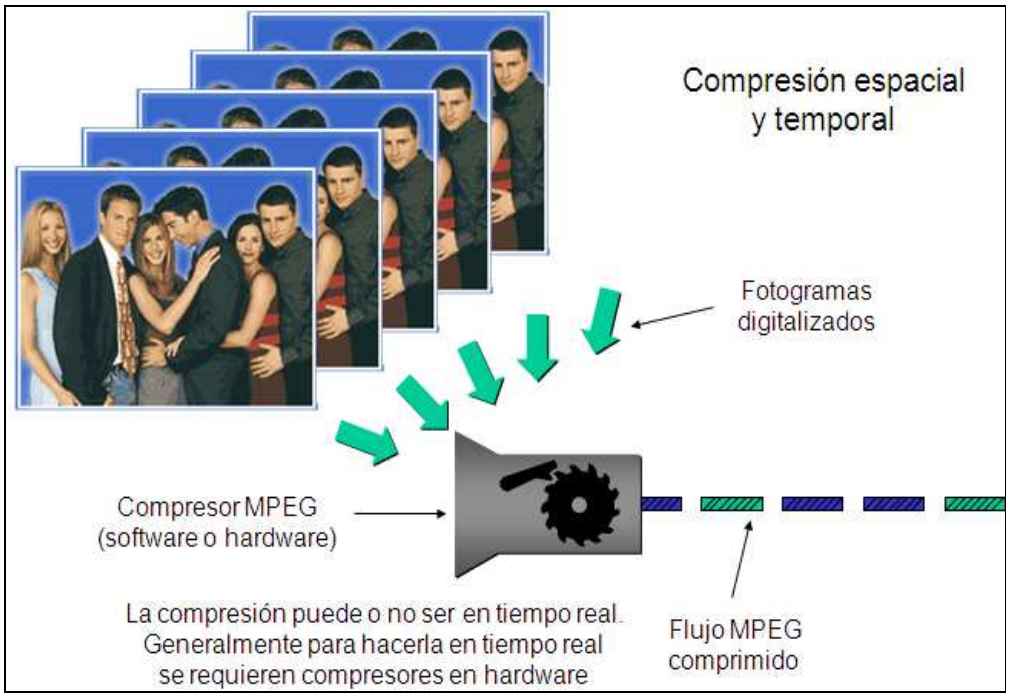

Figura 2.5 Compresión espacial JPEG y temporal por fotogramas

2.4.3.1 MPEG-1

Guarda una imagen, la compara con la siguiente y almacena solo las diferencias, se alcanza así grados de compresión muy elevados.

Está orientado al almacenamiento y reproducción de video digital en cd´s con un flujo de transmisión de datos del orden de 1,5 Mbps transportando tanto imagen como sonido. La compresión de video en éste estándar es de baja calidad por lo cual no es apto para algunas aplicaciones.

2.4.3.2 MPEG-2

Dado que MPEG-1 no era adecuado para el satélite y MPEG-2 estaba todavía en desarrollo, se creó una modalidad de MPEG llamada MPEG-1.5, que no siendo un estándar oficial, se usa todavía en algunas redes de satélite (p.ej. CNN Airport). MPEG-1.5 usa un gran ancho de banda multiplexado varios streams MPEG-1, lo cual permite cubrir la deficiencia de MPEG-1 de no poder transmitir varios programas de video a la vez sobre el enlace satélite.

La segunda fase de MPEG, llamada MPEG-2 se acabó convirtiendo en el estándar de facto en el mundo de la televisión digital ya que arregla muchos de los problemas inherentes a MPEG-1, tales como la resolución, escalabilidad y manejo de vídeo entrelazado. MPEG-2 permite imágenes de mucha más calidad (hasta niveles de HDTV. Alta definición) y permite que muchos canales de diferentes tasas de bit se multiplexen dentro de un mismo flujo de datos.

MPEG-2 también consta de tres capas (o estándares), cubiertas por la: ISO/IEC 13818-1 Sistemas MPEG-2 (ITU-T Rec. H.222.0), ISO/IEC 13818-2 Vídeo MPEG-2 (ITU-T Rec. H.262) y ISO/IEC 13818-3 Audio MPEG-2, aprobadas finalmente como estándar la ISO/IEC en Noviembre de 1994.

	MPEG-1	MPEG-2
Año	1992	1994
Aplicación	Vídeo digital en CD -ROM	TV digital y HDTV
Resolución Espacial	CIF	4CIF y 16CIF
Resolución Temporal	25 – 30 imágenes/s	50 – 60 y 100 – 120 campos/s
Tasa de bits	1,5 Mb/s	4 – 20 Mb/s
Calidad	VHS	TV (NTSC o PAL)
Tasa de Compresión	20 – 30	30 – 40

Tabla 2-1, Comparativa entre MPEG-1 y MPEG-2

2.4.3.3 MPEG-4

Al principio, el estándar MPEG-4 se creó como un intento para mejorar la calidad del vídeo codificado de bajas velocidades a través de la estandarización de nuevas técnicas mejoradas de compresión, orientado inicialmente a las videoconferencias e Internet. Más adelante, su progresión recondujo este estándar al mundo de la TV interactiva, la computación y las telecomunicaciones.

El objetivo es crear un contexto audiovisual en el cual existen unas primitivas llamadas AVO (objetos audiovisuales). Se definen métodos para codificar estas primitivas que podrían clasificarse en texto y gráficos.

Las nuevas características ofrecidas por este estándar se pueden resumir en:

- Las escenas se descomponen en 2 componentes básicas: audio y vídeo. Estos dos objetos son codificados de forma independiente.
- Los objetos pueden ser tanto vídeo natural (p.ej. generado por una cámara) como imágenes sintéticas (generadas por un ordenador).
- Ofrece soporte para manipulación de las imágenes sintéticas (soporte para animación, utilización de imágenes estáticas 2D-3D como logos etc.).
- Permite interacción de los usuarios sobre la escena que se está reproduciendo.
- Se ha mejorado la base del algoritmo MPEG para incrementar la robustez para el trato de errores.

La comunicación con los datos de cada primitiva se realiza mediante uno o varios "elementary streams" o flujos de datos, cuya característica principal es la calidad de servicio requerida para la transmisión.

Ha sido especialmente diseñado para distribuir videos con elevados ratios de compresión, sobre redes con bajo ancho de banda manteniendo una excelente calidad para usuarios con buen ancho de banda.

2.4.3.4 CODIFICACIÓN MPEG-4

El estándar MPEG-4 guarda muchas similitudes con el MPEG-1 y el MPEG-2, tal como la compresión basada en la DCT (Discreet Cosine Transformation o La transformada de coseno discreta) con frames I, P y B, todos dentro del GOPs (Group Of Pictures o Grupo de imágenes). Véase las figuras 2.6, 2.7 y 2.8 acerca de los frames I, P y B.

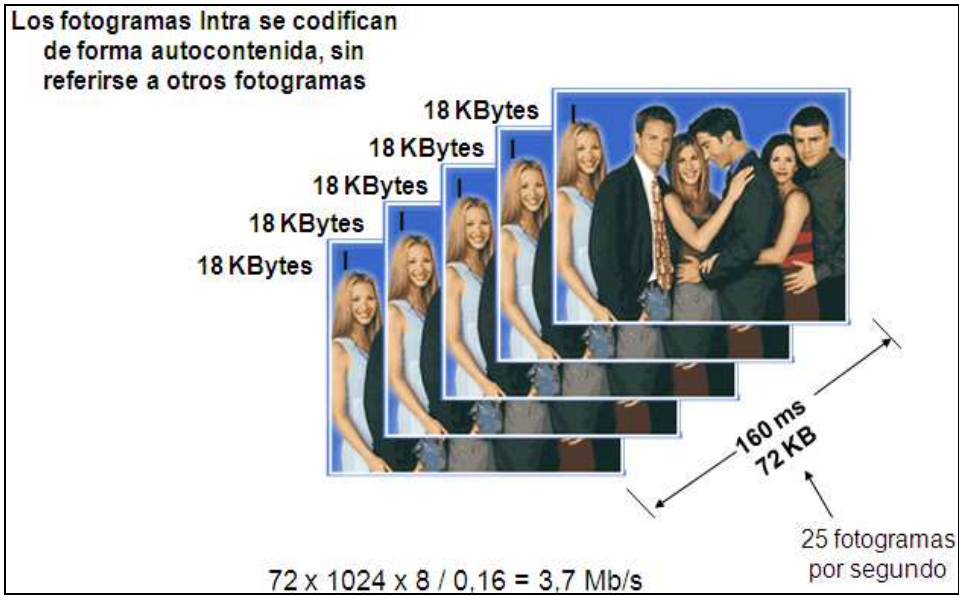

Figura 2.6 fotograma I (Intra)

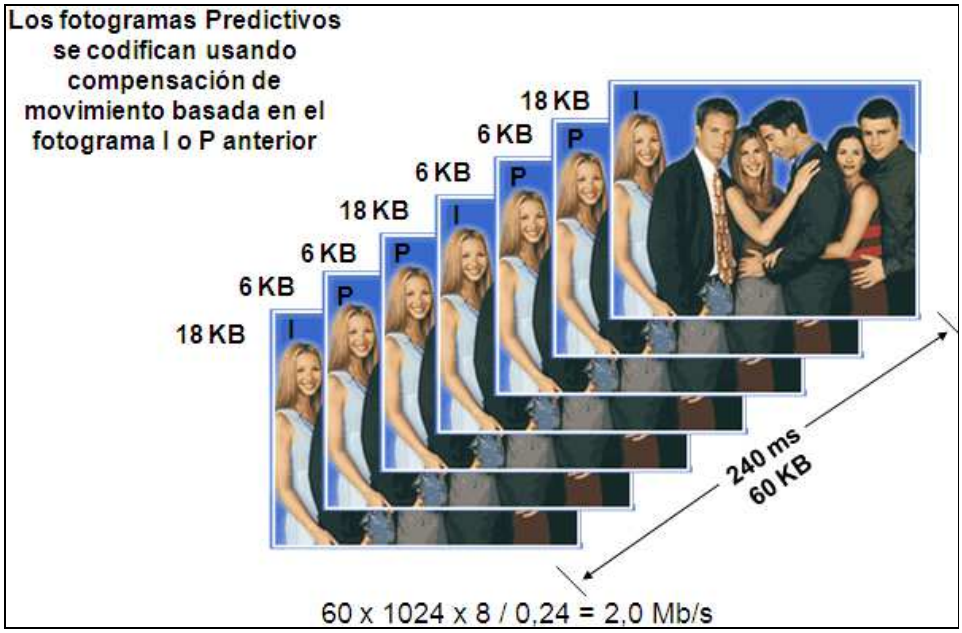

Figura 2.7 Fotograma P (Predictivo)

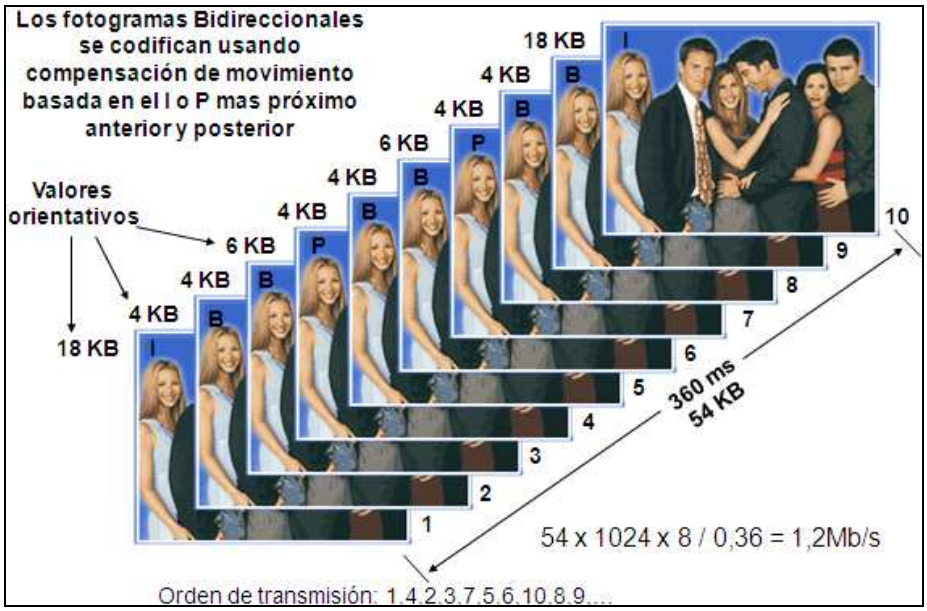

Figura 2.8 Fotograma B (Bidireccionales)

También tiene una serie de mejoras, especialmente para bajos flujos de datos, esto incluye mejor estimación de movimiento y filtraje de desbloqueo. Su calidad y flujo de datos (20Kbps hasta 1000Kbps) es enormemente mejor que en el MPEG-1 y, generalmente, más competitivo que otras soluciones Web.

En efecto, el MPEG-4 ofrece mejores características a bajos flujos de datos, típicos de la Web. A diferencia de otros códec para la Web, el MPEG-4 soporta contenido entrelazado, resoluciones de hasta 4096 x 4096 y un flujo de datos entre 5Kbps y 10Mbps.

Teóricamente, el MPEG-4 permite desde un ancho de banda muy bajo (telefonía móvil) hasta la televisión en alta definición (HDTV). Por supuesto, los dispositivos actuales no

soportan la reproducción de todo el rango de especificaciones pero, con el tiempo, se presentarán nuevos equipos en el mercado.

El códec de vídeo MPEG-4 soporta, nativamente el canal alfa, que es de 8 bits y que algunos programas de tratamiento de imágenes reservan para el enmascarado o la información adicional sobre el color, así se pueden hacer composiciones de vídeo sobre un fondo en tiempo real. Esto puede ser usado para una segmentación, ya que es posible separar internamente el fondo de la imagen sobre una escena. Esto es debido a la propia concepción del códec MPEG, que extrae la imagen en movimiento (principal) de la fija (secundaria) para realizar la compresión.

Para comprender la segmentación, imaginemos un vídeo donde un señor está leyendo, mientras camina por una sala. Con un códec convencional, cada vez que el señor va al principio de la sala y regresa, se está comprimiendo (transmitiendo) toda esa información.

Con la segmentación, el códec puede recordar la “imagen” de la sala una sola vez (fondo o background), y comprimir (transmitir) el resto de la información, en este caso, el señor que se pasea leyendo.

2.4.3.5 MPEG-2 VS. MPEG-4

El video es problemático en términos de almacenamiento y transmisión debido al extenso tamaño de los archivos. Un video no comprimido, de pantalla completa significa la necesidad de 30 archivos de imagen de 1MB, cada uno, por segundo, sin incluir las señales de sonido.

El estándar de compresión de video MPEG-2, a través de comparaciones entre una trama de video y las sucesivas, nos permite que se almacene o envíe solo la información de los cambios entre las tramas, el resto será repetida de la primera trama, de esta forma mucha de la data original puede ser dejada de transmitir, reduciendo el ancho de banda necesario.

Para ahorrar espacio, MPEG-4 reconoce objetos individualmente dentro de la trama.

Manipulando cada objeto en forma individual, MPEG-4 es capaz de desechar una mayor cantidad de información, obteniendo órdenes de compresión que van de 8 a 12 veces menos que los obtenidos en MPEG-2. Con MPEG-4 puede comprimirse la información de un DVD de 8 GB en un CD de 700MB.

En particular, para comunicaciones multimedia audiovisuales interactivas sobre redes móviles o de red pública conmutada, ofrece una buena calidad de video con bajas velocidades de transmisión es una funcionalidad importante del estándar MPEG-4. Los servicios ofrecidos comprenden la transmisión de video-teléfono, aplicaciones de video conferencia, acceso a servidores de video para aplicaciones multimedia, o vigilancia remota, por nombrar algunas posibilidades.

2.4.3.6 MPEG-7

El nombre formal para este estándar es interfaz de descripción del contenido multimedia, está orientado a los contenidos audiovisuales, trabaja con información de tipo: audio, voz, video, imágenes, gráficos y modelos 3D.

MPEG-7 se ha convertido en una gran ayuda para el avance de la nueva televisión interactiva con introducción de buscadores de contenidos, búsquedas de audiovisuales etc.

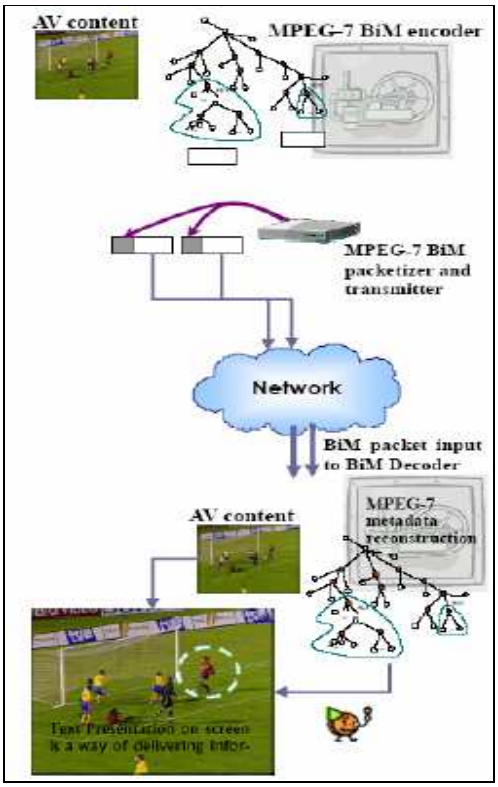

Figura 2.9 Estándar MPEG-7 orientado a multimedios

2.4.4 FORMATO MJPEG

Motion-JPEG, codifica el video digital como una secuencia de imágenes estáticas individuales a las que se aplica el proceso de compresión del algoritmo JPEG.

La ventaja de este formato es que al tratar las imágenes por separado, si se diera algún fallo en una imagen durante la transmisión, el resto del video no se verá afectado.

El inconveniente, es que tiene una compresión muy baja comparado con la calidad de video resultante.

Motion-JPEG es método elegido para las aplicaciones donde se envía la misma información a todos los usuarios, las broadcast.

2.4.5 FORMATO DivX

Es un códec de video basado en el formato MPEG-4 de gran calidad. El proceso de compresión es sencillo y consiste en suprimir las partes del archivo que se repiten. Por ejemplo, durante una conversación, el fondo de la escena no cambia, lo único que varia son las caras de los personales, por lo que no es necesario modificar el fondo y por ello se deja como está. Con esto se logra comprimir la película.

2.4.6 FORMATO XviD

A diferencia del formato DivX, se distribuye totalmente gratis. Tiene algunas similitudes con el formato anterior ya que algunos de los programadores pasaron de programas para DivX a programar para XviD.

Actualmente existen reproductores de DVD que también permiten leer estos formatos.

2.4.7 FORMATO ITU H.261

El estándar H.261 es parte del grupo de estándares H.320 para comunicaciones audiovisuales, fue diseñado para una tasa de datos múltiplo de 64 Kbps. Lo cual coincide con las tasas de datos ofrecidas por los servicios de RDSI (Red Digital de Servicios Integrados), se pueden usar entre 1 y 30 canales RDSI (64 Kbps a 1920 Kbps). Aplicaciones que motivaron el diseño de este tipo de estándar son: video conferencia, vigilancia y monitoreo, telemedicina y otros servicios audiovisuales.

2.5 PARÁMETROS QUE AFECTAN LA CALIDAD DEL VIDEO

La calidad del servicio de video que se transmite por Internet es afectada básicamente por los parámetros de la red y por el tipo de codificación implementada. Es claro por ejemplo que el efecto de la perdida de paquetes depende fuertemente del tipo de codificación utilizada; este factor resulta critico en aplicaciones de video de alta calidad en donde, con la finalidad de disminuir el ancho de banda consumido, se implementan codificaciones que hacen uso de cuadros predictivos (MPEG-1, MPEG-2, MPEG-4) cuya pérdida resulta en falta de información para decodificar los cuadros siguientes.

Otros factores importantes que afectan la calidad percibida están directamente relacionados con la fuente de video, encontrando en este grupo la resolución del cuadro, la luminancia (niveles de gris) y la profundidad del color (nº de bits por pixel) y la tasa de generación de cuadros.

La sincronización entre el audio y el video influye también sobre la opinión de la calidad, si bien no hay una relación directa entre ellos en lo que respecta al transporte (se transmiten por distintos canales y con distinta codificación).

Como se verá más adelante los efectos de la variación del retardo entre paquetes es el otro factor de crítico en la calidad percibida, aunque en este caso no es tan evidente a priori el porqué de esta fuerte influencia.

2.5.1 PERDIDA DE PAQUETES

Es la principal causa de degradación en una transmisión de video, si bien esto es atenuado por protocolos de transmisión que no verifican la entrega de paquetes haciendo fluida la comunicación, la perdida de paquetes con imágenes “I” que contienen la

información necesaria para decodificarla afectan directamente a las imágenes posteriores (“B” y “P”) que se generar a partir de ella. Por lo tanto, es necesario concluir que no importa solo la cantidad de paquetes perdidos sino que la distribución de estas pérdidas. Observar la figura 2.10 con los efectos de la pérdida de paquetes según codificación

Figura 2.10 Efectos de la pérdida de paquetes según codificación

La figura anterior muestra el efecto de la codificación de acuerdo a un estudio realizado acerca de la calidad de servicio percibida en servicios de voz y video sobre IP, en la imagen de la izquierda se puede observar el efecto que tiene la perdida de paquetes con codificación MPEG-1 y en la derecha con MPEG-4, en ambas imágenes se percibe perdida de Macro Bloques (MB) provocada por la pérdida de paquetes.

En codificación MPEG-1 el envío de imágenes “I” es fija, y la actualización de MB periódica, por lo que los errores en las imágenes serán corregidas con la llegada de otro MB “I”. En el caso de MPEG-4, los MB son de tamaño variable, y el uso de MB de tipo I es más concentrado en aquellas regiones de mayor movimiento. De esta forma la

pérdida de un MB afectará principalmente las regiones de baja cantidad de movimiento. Esto se ve claramente en el fondo de la imagen que presenta poco refresco de imagen.

2.5.2 RETARDO

Es el tiempo trascurrido entre que la primera parte (ej. El primer bit) o un objeto (ej. Un paquete) pasa por un punto de observación (ej. Donde el interfaz de tarjeta de red del ordenador se conecta al cable) y el tiempo en que la última parte (ej. El último bit) u objeto relacionado (ej. Un paquete de respuesta) pasa por un segundo (puede ser el mismo) punto de observación.

2.6 MEDIDAS ACTIVAS Y MEDIDAS PASIVAS

Muchas herramientas de monitorización han sido desarrolladas para medir las prestaciones de la red. En general, los esquemas convencionales de monitorización para medir la QoS y las prestaciones de la red, se clasifican en dos tipos: monitorización activa y monitorización pasiva.

2.6.1 MEDIDAS ACTIVAS

La monitorización activa consiste en probar directamente las propiedades de la red generando el tráfico necesario para realizar la medida. Esto permite utilizar métodos de análisis mucho más directos, pero también presenta el problema de que el tráfico introducido puede tener un impacto negativo en las prestaciones recibidas por otros tipos de tráfico.

Hay varios métodos activos para medir prestaciones de red tales como el ancho de banda disponible, el retardo, las pérdidas y para estimar las características enlace por enlace. Monitorizar la QoS del flujo de paquetes es una prueba para determinar la QoS de los

usuarios indirectamente. Esto implica que se asume implícitamente que la QoS de un usuario es la misma que los valores medidos con los paquetes de prueba.

A continuación se nombran ciertas desventajas en la toma de medidas activas:

- Si se usa un flujo de paquetes de prueba que simula el tráfico actual del usuario:
- El flujo de paquetes de prueba produce una no despreciable cantidad de tráfico extra en la red y esto afecta a la QoS/prestaciones del tráfico de usuarios.
- La QoS/prestaciones obtenidas de los paquetes de pruebas no es igual a la obtenida sin la influencia del flujo de paquetes de prueba.
- Si se usan paquetes pequeños de prueba y los enviamos en ciertos intervalos, como ping:
- El tráfico extra puede ser despreciable, pero la QoS/prestaciones obtenidas desde el paquete de prueba no es igual a las experimentadas por los usuarios, en general.
- Puede ser catalogado como tráfico hostil o intento de ataque. Por ejemplo, algunos routers rechazan tráfico ICMP o limitan su tasa, por si se trata de un intento de spoofing que es lo que se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada etc.

2.6.2 MEDIDAS PASIVAS

Las medidas pasivas dependen completamente de la presencia del tráfico apropiado en la red bajo estudio, y tiene la considerable ventaja de que pueden ser realizadas sin afectar al tráfico que lleva la red durante el período de medida. Sin embargo, puede ser mucho

más difícil, o imposible, extraer alguna de la información deseada desde los datos disponibles.

La monitorización pasiva se puede clasificar en dos tipos: monitorización en dos puntos y monitorización en un punto.

La monitorización en dos puntos requiere dos dispositivos de medida desplegados en los puntos de acceso y salida de la red. Estos dispositivos, toman paquetes de datos de forma secuencial y los parámetros de prestaciones de la red como el retardo o las pérdidas pueden ser calculadas comparando los datos de los correspondientes paquetes tomados en cada punto. Si se aplica la monitorización de dos puntos como medida de QoS/prestaciones:

- Todos los dispositivos deberían estar sincronizados en el tiempo.
- Requiere identificar cada paquete en los dos dispositivos por su cabecera y/o contenido. Este proceso de identificación puede ser tremendamente difícil cuando el volumen de paquetes es enorme, como en redes de gran escala, y este tipo de monitorización no es escalable.
- Para identificar los paquetes monitorizados, se debe recoger todos los paquetes de datos. Este proceso requiere un no despreciable ancho de banda.

CAPITULO 3

SISTEMAS DE VIDEO VIGILANCIA

Este Capitulo detalla los componentes, aplicaciones y selección de equipos para integrar un sistema de monitoreo con cámaras de video. Antes de entrar a detallar los sistemas, se explica los diferentes sistemas de seguridad por medio de cámaras que existen actualmente en el mercado, se describe de los que son más usados comúnmente.

- Circuito cerrado de video Analógico.
- Solución Hibrida de Video Analógico y servidor Digital.
- Solución Video Digital (Cámaras IP Inalámbricas)

3.1 CIRCUITO CERRADO DE VIDEO ANALÓGICO

Los sistemas de circuito cerrado de televisión están compuestos básicamente por cámaras analógicas fijas o con movimiento, ocultas o discretas y sus respectivos monitores. Para una mejor gestión o manejo de las cámaras hacia los monitores se utilizan las Matrices de video, que son sistemas capaces de direccionar a través de microprocesadores las entradas (cámaras) hacia las salidas (monitores). Con las matrices de video se pueden programar las secuencias de cámaras en un monitor. En la figura 3.1 se muestra un circuito cerrado de televisión.

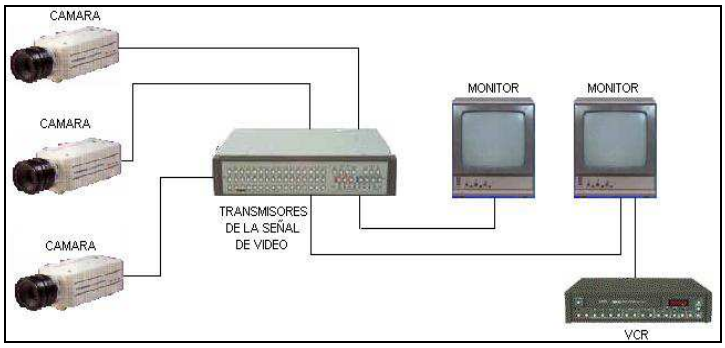

Figura 3.1 Circuito Cerrado de Televisión (CCTV)

Los sistemas modernos de CCTV permiten digitalizar las imágenes y comprimirlas para así mostrar en un solo monitor toda la información requerida. Estos sistemas son los llamados "Monitores Digiquad ". Con los respectivos sistemas de grabación que permiten grabar en tiempo real todas las cámaras comprimidas, y así tener una mejor secuencia de los hechos. En la figura 3.2 permite entender que las señales de las cámaras análogas se comprimen y se pueden digitalizar y ser vistas de forma óptima y secuencial.

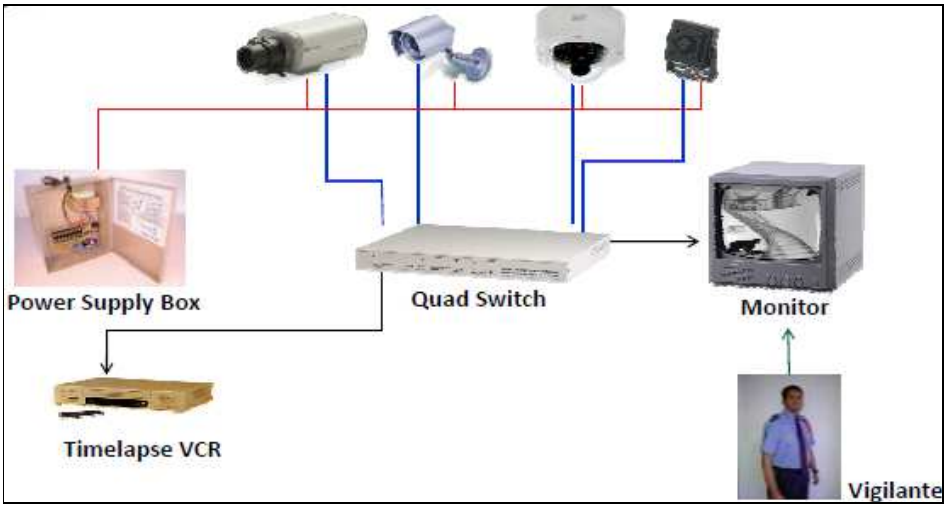

Figura 3.2 El Quad switch comprime imágenes para visualización secuencial

- Elementos captadores de imagen (cámaras)
- Elementos reproductores de imagen (monitores)
- Elementos grabadores de imagen (VCR)
- Elementos transmisores de la señal de vídeo (Matrices de video)
- Elementos de control
- Video censores (generan una alarma ante el movimiento registrado en el video)

Una cámara de CCTV está compuesta fundamentalmente por un dispositivo captador de imágenes, un circuito electrónico asociado (DSP) y una lente, que de acuerdo a sus características nos permitirá visualizar una escena determinada.

El dispositivo captador de imágenes, denominado comúnmente CCD o CMOS, está compuesto por cerca de 300.000 elementos sensibles denominados pixeles y su formato en las cámaras estándar es de 1/3” o 1/4”. Las especificaciones más importantes son:

Alimentación: 220 VCA, 24 VCA y/o 12 VCC

Tipo de sensor: CCD o CMOS y su respuesta espectral (color, blanco y negro y/o infrarrojo)

Tamaño del sensor: 1/4“, 1/3”, 1/2", 2/3", 1“

Resolución: representa la definición de la imagen, expresada en líneas de TV (TVL)

Audio: para escuchar el sonido del ambiente donde está instalada la cámara

3.1.2 SOLUCIÓN HIBRIDA DE VIDEO ANALÓGICO Y SERVIDOR DIGITAL.

En este tipo de solución, las cámaras generan una señal analógica que es convertida en señal digital por medio de los dispositivos DVR, que realizan la grabación en formato digital facilitando la búsqueda de video. Uno de los objetivos que se perseguía con la aparición de los DVR es reemplazar el video tape por el disco duro facilitando el almacenaje de la información, pero el DVR aún mantenía entradas para cables coaxiales y salidas analógicas. Ver figura 3.3 con DVR como el paquetizador de las señales de las cámaras.

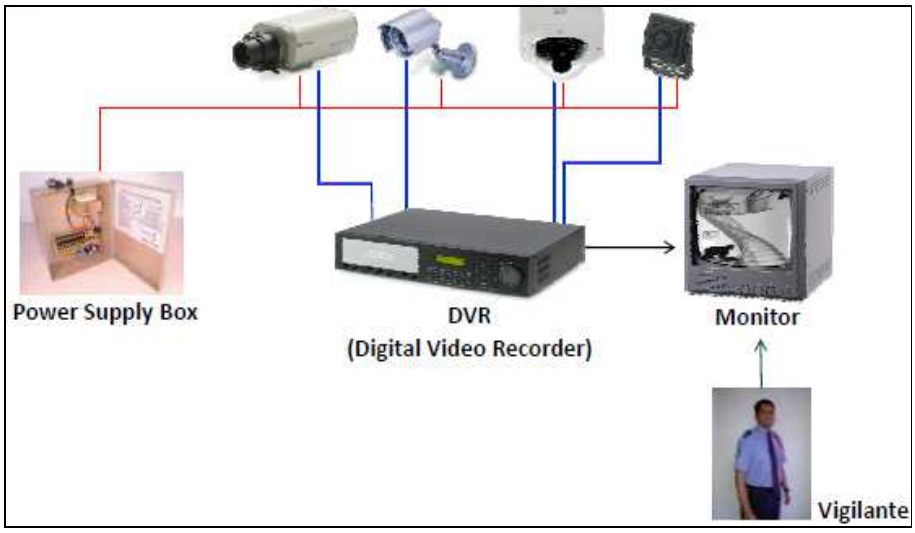

Figura 3.3 Sistema de video vigilancia con DVR

La segunda generación de DVR´s llegó con conexiones a red para poder utilizar una computadora como central de monitoreo. En los últimos años, prácticamente todos los DVR's están siendo entregados con una conexión de red o módem para que las

imágenes grabadas puedan ser monitoreadas remotamente, vía un software propietario de cada fabricante. Incluso en la actualidad, los DVR's más avanzados admiten la grabación de algunas cámaras IP del mismo fabricante. La figura 3.4 muestra el sistema hibrido con respaldo de servidor.

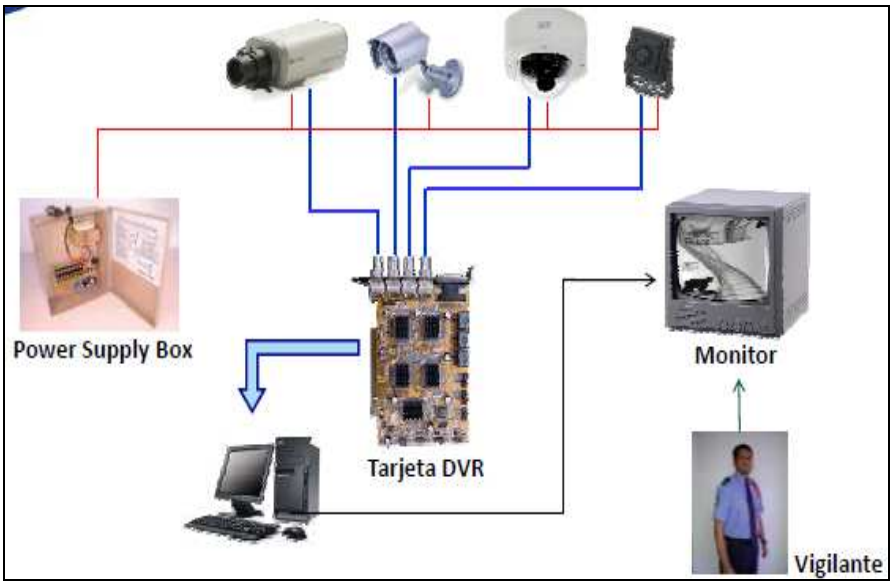

Figura 3.4 Sistema de video vigilancia con respaldo de servidor

3.1.3 SOLUCIÓN VIDEO DIGITAL

Es más fácil destacar las ventajas del vídeo IP si consideramos las desventajas del circuito cerrado de TV analógico, como también que a pesar de que el lanzamiento de los grabadores de vídeo digitales (DVR´s) ha mejorado la capacidad de grabación de los circuitos cerrados de TV, éstos también tienen limitaciones. Tienen que estar instalados cerca de la matriz analógica y a menudo se compromete la tasa de transmisión y la calidad de imagen. Las empresas quieren una única solución integral que se pueda

ampliar y ofrezca vigilancia por vídeo de alta calidad en diversas oficinas o lugares, y esto es precisamente lo que proporciona el vídeo IP.

Además, el vídeo IP ofrece un gran nivel de redundancia para grupos empresariales. En caso de emergencia, la capacidad de control puede transferirse fácilmente a cualquier otro punto de la red, ya sea en el mismo lugar o en otro diferente. Las redes redundantes permiten que el sistema siga funcionando incluso cuando falla un enlace o un interruptor, y los grabadores de vídeo en red protegen las grabaciones incluso cuando un grabador deja de funcionar o se destruye. Estas características permiten a los sistemas de vídeo IP ofrecer un nivel mucho mayor de integridad que el que ofrecen los sistemas de circuito cerrado de TV analógicos.

El hecho de contar con un sistema basado en una red posibilita diagnósticos a través de todo el sistema para garantizar que todo funciona correctamente. Cada dispositivo se puede controlar continuamente y, si falla cualquier cosa, salta una alarma. Esto no es posible con un sistema analógico, en el que las grabaciones se tienen que controlar manualmente para garantizar una operación sin problemas y existe la posibilidad de que un fallo pase desapercibido durante un largo periodo de tiempo.

Este problema existe especialmente en los DVR, ya que no siempre se señalan los fallos y se pueden perder durante mucho tiempo las grabaciones de todas las cámaras. Los sistemas analógicos pueden ejecutar diagnósticos limitados dependiendo de los diferentes componentes que se usen, pero esto no forma parte integral del sistema.

3.1.3.1 LAS CÁMARAS IP

Estas permiten ver en tiempo real qué está pasando en un lugar, aunque el usuario o supervisor esté a miles de kilómetros de distancia. Son cámaras de vídeo de gran calidad que tienen incluido un ordenador a través del que se conectan directamente a Internet.

Una cámara IP (o una cámara de red) es un dispositivo que contiene '3 funciones en 1':

- Una cámara de vídeo de gran calidad, que capta las imágenes
- Un chip de compresión que prepara las imágenes para ser transmitidas por Internet, y
- Un ordenador que se conecta por sí mismo a Internet

En la figura 3.5 se muestra un esquema de sistemas de video vigilancia con cámaras IP

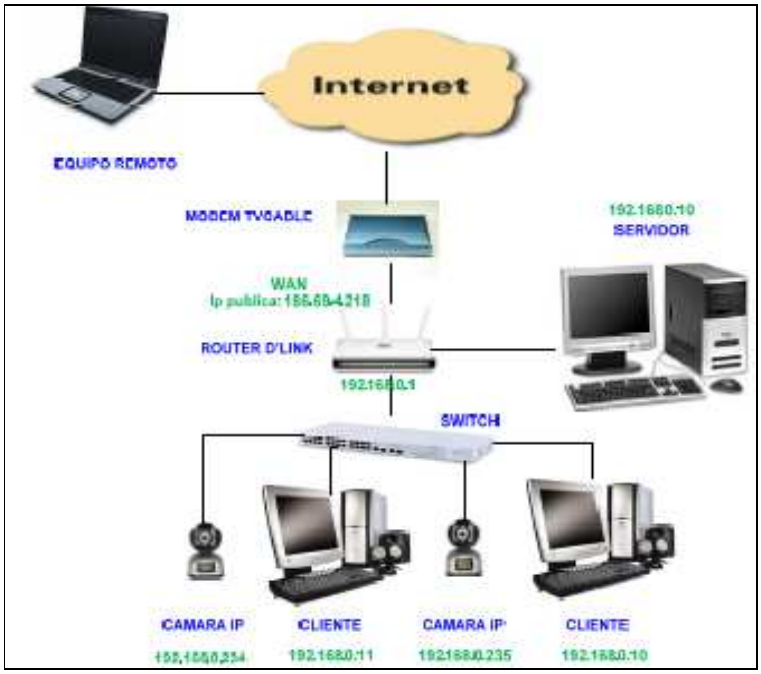

Figura 3.5 Esquema de video vigilancia remota con cámara IP

3.2 COMPONENTES DE SISTEMAS DE VIDEO VIGILANCIA

En esta parte se detalla con ejemplos, características y gráficos los componentes y/o accesorios de lo que integra un sistema de monitoreo con cámaras de video, empezamos con los tipos de cámaras, y así existen dependiendo, su aplicación.

3.2.1 CAMARAS DE VIDEO

Figura 3.6 Mini Cámara de Vigilancia

Dentro de la seguridad Electrónica, se tiene la Mini Cámara, Pinhole, 1/3", Color, Sensor Chip Sony, Lente Incorporado 3.6mm, 380 Líneas de Resolución.

Figura 3.7 Mini cámara oculta

Mini Cámara Oculta en Detector de Humo, 1/3”, Color, Sensor Chip Sony, Lente Incorporado 4.3mm, 380 Líneas de Resolución.

3.2.2 CAMARA TIPO BALA O BULLETS

Este tipo de cámara son muy utilizadas por su duración a ambientes extremos, sea de día o de noche, muchas de ellas pueden tener sistema infrarrojo y con alta resolución, así también existen de diferentes tamaños. La figura 3.8 muestra varias cámaras tipo bala.

Figura 3.8 Cámaras bullets

3.2.3 CÁMARA COMPACTAS Y PROFESIONALES

Este tipo de cámara así mismo puede tener infrarrojos, como un video grabador digital autónomo, su presentación es discreta y pueden tener dimensiones muy pequeñas así en presentación compacta existen las cámaras profesionales las cuales difieren por su alta resolución de grabación, las figuras 3.9 y 3.10 muestran cámaras compactas y las cámaras profesionales para sistemas de video vigilancia.

Figura 3.9 Cámaras compactas

Figura 3.10 Cámaras profesionales

3.2.4 CAMARAS DOMOS

Existen dos clases de domos dependiendo su tamaño las mini y los de tamaño mediano o normal; asi también existen las que son solo cámara sencilla es decir motorizadas que puede mover su lente y las que son motorizadas y además infrarrojo, estas cámaras son catalogadas como profesionales. En la figura 3.11 se muestran las mini domo sencillas y las que tienen infrarrojo.

Figura 3.11 Mini domo sencillo y mini domo tipo infrarrojo

Las domos de tamaño mediano aparte de ser motorizadas pueden tener los movimientos PAN, movimiento TILT y aparte con ZOOM, por eso se les llama PTZ. Las cámara domo PTZ incluye zoom óptico de 18, 22, 26, 32, 36 aumentos y enfoque automático motorizado. Tienen resolución HDTV, puede inclinarse 180° y hacer movimientos continuos en 360° a una velocidad de entre 0,05° y 450° por segundo. Su capacidad para recibir alimentación eléctrica es a través de Ethernet (IEEE 802.3at) simplifica la instalación al ser necesario un único cable para la alimentación, el vídeo y los controles de movimiento horizontal, vertical y zoom.

Estas cámaras pueden ser análogas o también se encuentran en versiones basadas en IP, la presentación en Domo permite realizar movimientos horizontales (Paneo) continuos de 360 grados y cuenta con la capacidad para girar la cámara verticalmente (Tilt) hasta 90 grados continuos con un auto-giro de 180 grados (auto-flip). Incluye la capacidad de hacer acercamientos (Zoom) de hasta 12x ópticos (desde 2x, 4x etc.) que permite ver la

placa de un carro hasta 60 metros de distancia. Véase la figura 3.12 con un ejemplo de enfoque a más de 50 metros de distancia.

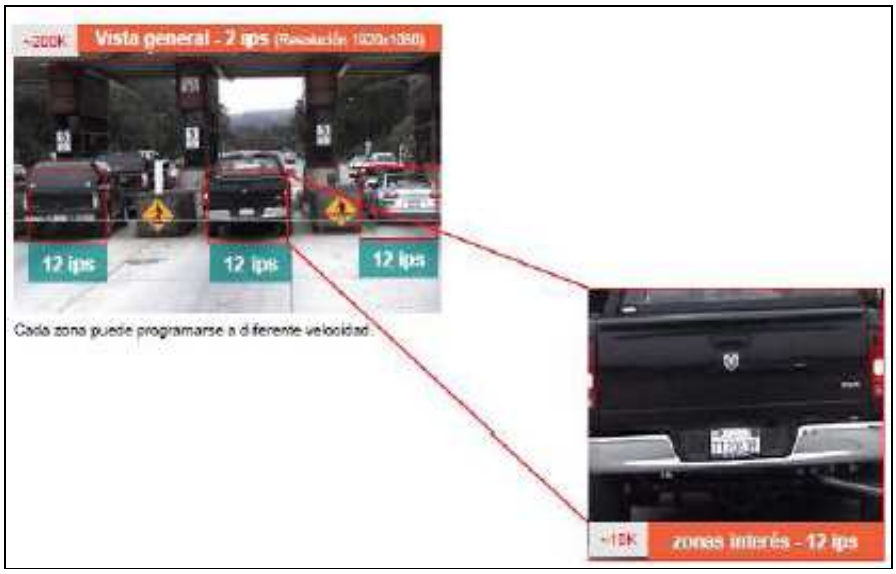

Figura 3.12 Aplicación de Zoom de 12x de una cámara domo PTZ

Además las cámaras domo, tiene la capacidad para almacenar hasta 165 posiciones predefinidas (Presets) para girar y enfocar la cámara a zonas específicas de interés en menos de 1 segundo. Cuenta con funciones de Recorrido (Tour) y Secuencia de "Presets" programables por el usuario, de esta manera la cámara se convierte en un vigilante permanente de múltiples zonas de interés. La cámara ofrece video a color de Día (mientras la zona esté iluminada); y Blanco y Negro en alta resolución de noche (sin luz) para un mejor monitoreo. La figura 3.13 presenta la parte interna de un domo PTZ

Figura 3.13 Domos PTZ (interno)

3.2.5 CÁMARAS IP

Hoy en día, la vigilancia IP se utiliza cada vez más como una efectiva solución de seguridad que ofrece monitorización y control avanzados, antiguamente las aplicaciones de monitorización y de vigilancia han sido ofrecidas por la tecnología analógica de circuito cerrado de televisión (CCTV). Sin embargo, con el auge de la era digital, se han obtenido numerosos beneficios respecto los anteriores sistemas CCTV.

La vigilancia IP consta de cámaras CCTV que utilizan el protocolo de internet (IP) para transmitir datos de imagen y señales de control por una red inalámbrica o Ethernet. Típicamente, esto se realiza instalando cámaras IP al lado de un grabador de vídeo de

red (NVR), lo que crea un sistema completo de grabación y reproducción. Básicamente una cámara IP se compone de:

- La " cámara " de video tradicional (lentes, sensores, procesador digital de imagen, etc.)
- Un sistema de compresión de imagen (para poder comprimir las imágenes captadas por la cámara a formatos adecuados como MPEG4.
- Un sistema de procesamiento (CPU, FLASH, DRAM y un módulo Wireless ETHERNET/WIFI). Este sistema de procesamiento se encarga de la gestión de las imágenes, del envío al modem. Del movimiento de la cámara (si dispone de motor), de la detección de movimiento.
- Con todo esto únicamente necesitamos conectar la cámara al Router ADSL y a la alimentación eléctrica y no necesitamos nada más o si pensamos usar la cámara en una red local, lo conectamos a un HUB/SWITCH y pasa a ser un equipo más que se comunica con el resto de la LAN (y con el exterior si la LAN dispone de conexión a Internet).

Dentro de sus características, tiene elementos totalmente digitales, con las mismas características Ópticas.

- ✓ Tienen un conversor análogo digital incluido.
- ✓ Tienen una tarjeta de red interna. El protocolo más difundido es TCP/IP. Salida directa a red (RJ45).

✓ Funcionan como un nodo de la red. Necesita programarle una dirección IP.

✓ Opcional: Salida de video normal.

✓ Se puede acceder desde cualquier browser a través de la red.

✓ Las características básicas como resolución y sensibilidad casi nunca son las mejores.

✓ Dependemos siempre del ancho de banda de la red.

Son cámaras con resolución superior a 1 mega píxel hasta 4 veces la calidad de una cámara análoga, 100% compatibles con PoE (power over ethernet), resolución y velocidad de fotogramas seleccionables, mayor cobertura de zonas, relaciones de aspecto diferentes (4:3 / 16:9). La figura 3.14 y la 3.15 nos muestra ejemplo de imágenes con alta resolución.

Figura 3.14 Resolución de cámaras

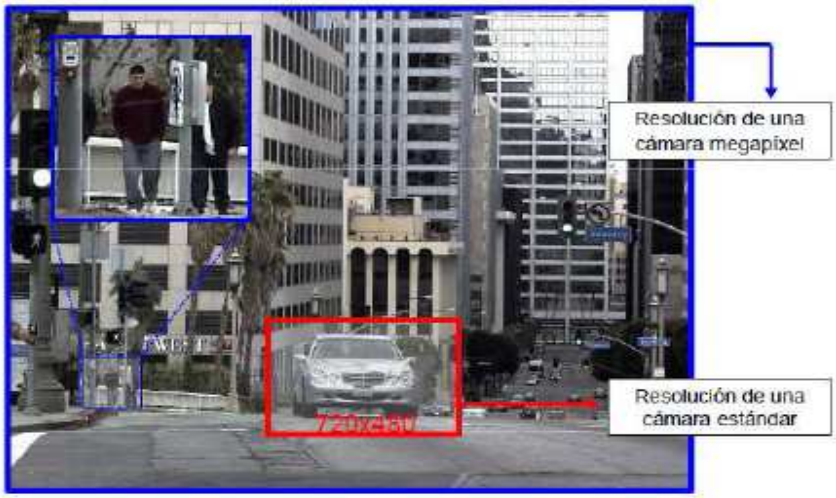

Figura 3.15 Resolución de cámara con 6 Mega pixeles

3.3 MEDIOS DE GRABACION

Tenemos las siguientes partes:

a) Tarjetas DVR (Digital Video Recording), ver figura 3.17

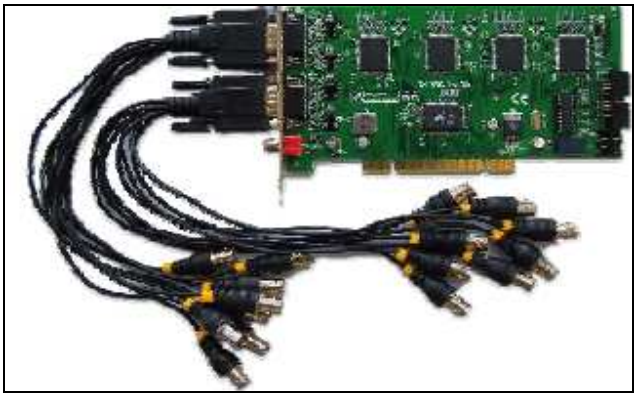

Figura 3.17 Tarjetas DVR

Una tarjeta de DVR es muy similar a la tarjeta de video por ordenador común en muchas PC. Sin embargo, cuando se trata de funcionamiento, hay muchas diferencias entre ellos. Las Tarjetas DVR vienen con software que puede utilizarse para visualizar y registrar la información de múltiples cámaras al mismo tiempo. Tienen bus PCI o PCI Express que se encarga de recibir la señal de las cámaras y digitalizarla mediante un software suministrado por el fabricante.

Se utilizan sobre todo en sistemas de vigilancia para procesar la información recibida de una fuente, como una cámara y pasarlo a un dispositivo de almacenamiento como un disco duro. En tal creación, no es más que una salida de video puerto. En estos puertos, la salida de las cámaras de seguridad está conectada a la tarjeta. Una vez instalado en el computador, la tarjeta se activa y se reconoce inmediatamente por la máquina gracias al software que incluye. Una vez instalado correctamente, la tarjeta DVR permite al usuario grabar en su disco duro para así poder observarla instantáneamente.

b) DVR (Digital Video Recording)

Es un dispositivo que almacena video en un disco duro proveniente de una o más cámaras de video. Generalmente son parte de un sistema de seguridad, es un dispositivo grabador de video basado en una computadora, puede contar con sistema operativo Linux en su mayoría libre de mantenimiento y al que se le conectan discos duros donde se almacena la información grabada. Trae un software de administración de cámaras muy práctico y se puede conectar a internet.

Figura 3.18 DVR Equipo

Una de las características principales de los DVR´s es el FPS (Frames Per Second), traza o cuadros de imágenes captadas en un segundo. Ver la figura 3.19 que detalla los cuadros por segundos.

Figura 3.19 FPS: 7

Una cámara muestra el movimiento al reproducir fotografías que toma de la imagen monitoreada. Para poder reproducir dicho movimiento en “tiempo real” debe reproducir 30 fotografías (frames) cada segundo. El estándar de calidad aceptable para un sistema de monitoreo normal es de 7.5 FPS. Para una solución crítica se necesita de los 30 FPS.

En la figura 3.20 las imágenes captadas están con 5 FPS; Cada imagen tiene un delay o retraso de 0.20 segundos con respecto a la siguiente correlativa.

Figura 3.20 Imágenes con 5 FPS

En la figura 3.21 esta con 9 FPS Cada imagen tiene un delay o retraso de 0.11 segundos con respecto a la siguiente correlativa.

Figura 3.21 Imágenes con 9 FPS

3.3.1 CARACTERÍSTICAS DE TARJETAS DVR

- Cantidad de canales 4, 8, 16, 32
- Expansibilidad o Simultaneidad (Stacking)
- FPS 30, 120,240, 480
- Resolución
- Software

Canales

Cada canal es una cámara, hay tarjetas y DVR de 4, 8, y 16 canales. Los frames por segundo se dividen entre las cámaras instaladas.

Así:

Tarjeta de 120 FPS con 4 cámaras= 30FPSc/u

Tarjeta de 120 FPS con 16 cámaras=7.5 FPS

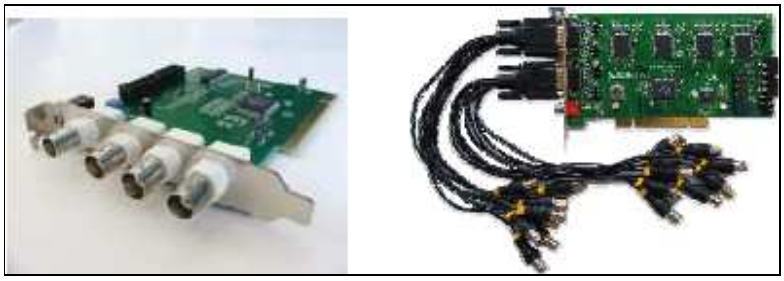

Figura 3.22 Tarjetas DVR

Expansibilidad:

Es la capacidad que tiene una tarjeta de permitir expansiones de 4 canales, hasta un máximo de 3 expansiones para lograr 16 canales de videos.

Figura 3.23 Expansibilidad de las Tarjetas DVR

Simultaneidad:

Es la capacidad de conectar dos o más tarjetas DVR o DVR para apilar varias soluciones como una sola.

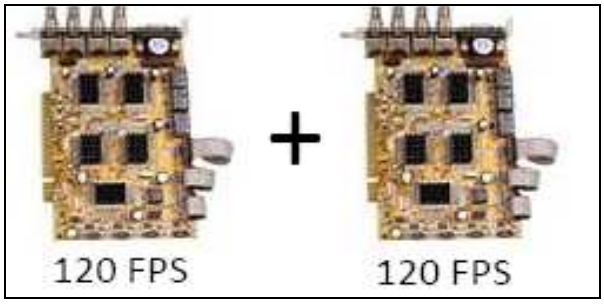

Figura 3. 24 Hace una tarjeta de 240 FPS, 8 canales.

A continuación tenemos varios modelos de tarjetas de DVR, con sus respectivas descripciones detalladas posteriormente:

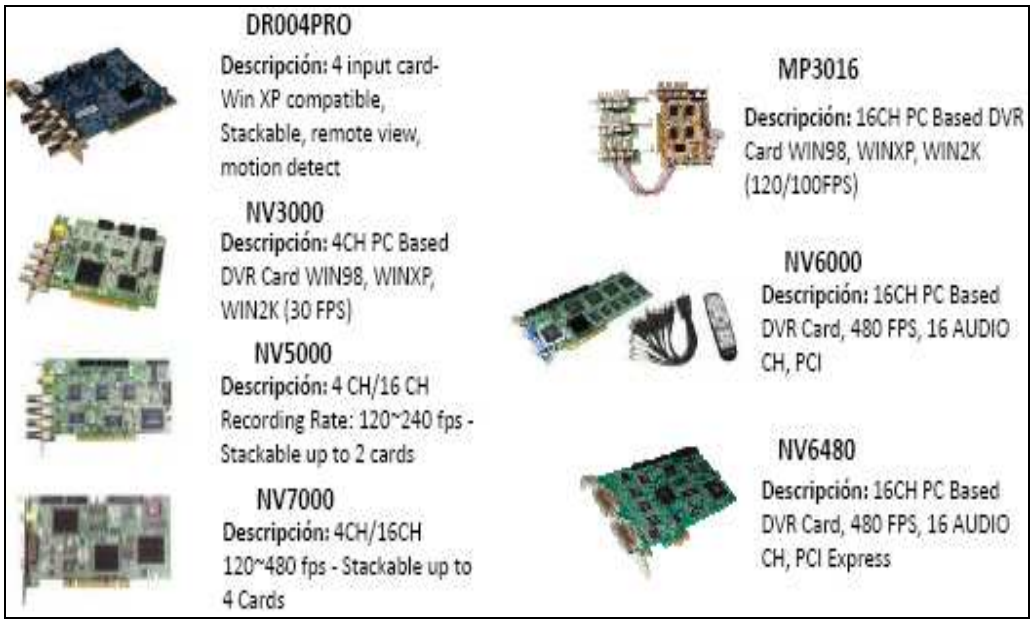

Figura 3.25 Tarjetas DVR de varios canales.

3.3.2 ESPECIFICACIONES PARA CONSTRUIR UN EQUIPO DVR

- ❖ CPU: Intel Core
- ❖ RAM: 4-8 GB
- ❖ Motherboard: Intel chipset
- ❖ Disco Duro: 2TB
- ❖ Video Pciex: 512 MB
- ❖ Sistema Operativo: Windows XP/ Vista/ 7

Disco Duro:

Para cada cámara:

- ✓ Tipo de Escena

Actividad (Baja/Media/Alta)

- ✓ Tipo de imagen que deseo obtener

Calidad (Baja/ Media/ Alta) (Formato de Comprensión)

Tasa de Actualización (FPS)

Resolución de la Imagen (1/4 de CIF (160x 120)…720x 480)

- Tipo de Grabación

- ✓ Continúa
- ✓ Por evento

Software:

Cada tarjeta DVR tiene su software independiente, de acuerdo al tipo de tarjeta. En un software de monitoreo y grabación se puede hacer:

• Búsqueda y reproducción de videos tomados con anterioridad.

• Favoritos.

• Mejora de calidad de video.

• Búsqueda potente, fechas, lugares, etc.

• Características especiales de reproducción.

• Reproducción a pantalla completa o por ventanas.

• Zoom digital.

• Exportación de video a formato AVI.

• Acceso remoto

• DDNS (Dynamic Domain Name Server)

• Control remoto PTZ

Figura 3.26 Presentador de imágenes en un Monitor

3.4 SOLUCIONES INALÁMBRICAS EN VIDEO VIGILANCIA

Los sistemas de video vigilancia, que contengan videos cámaras muy alejadas entre si, es decir, a más de 100 mts., pueden ser conectadas al sistema de forma inalámbrica. En la figura 3.27 se muestra un esquema de conexión inalámbrica entre cámaras y el equipo DVR.

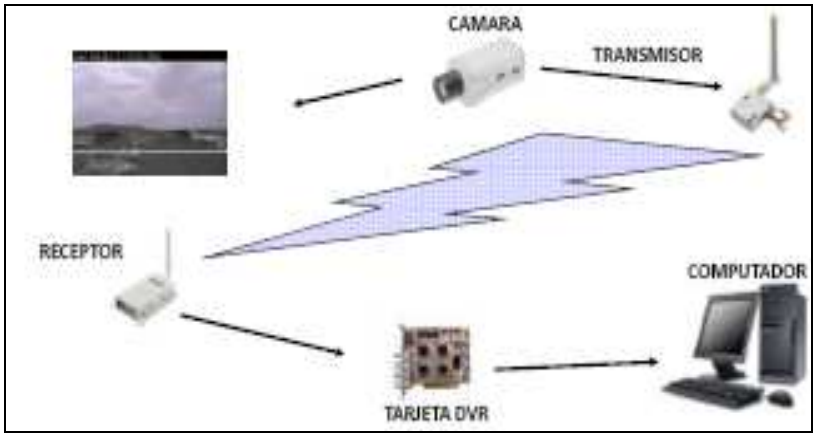

Figura 3.27 Solución Inalámbrica para video vigilancia

En distancia entre los 100 mts y 8.000 mts. Funciona bien una solución inalámbrica. La señal de video se modula con una frecuencia que pertenece a la banda de las microondas del espectro electromagnético, las frecuencias típicas que se usan para la transmisión de video están entre 1 GHz y 10 GHz y no existe interferencias entre ellas.

Las conexiones de microonda transmiten un ancho de banda muy grande de señales de video así como también otros datos si es necesario (incluyendo audio y /o control de PTZ). El ancho de banda depende del modelo del fabricante. Para una unidad bien construida, un ancho de banda entre 6 MHz y 7 MHz es suficiente para enviar señales de video de alta calidad sin una degradación visible.

Para un correcto enlace, se necesita tener visión óptica entre el transmisor y el receptor. Las distancias que se pueden alcanzar con esta tecnología dependen de la potencia de salida del transmisor y de la ganancia de las antenas.

Los equipos de radio que transmite la señal de video pueden trabajar en la banda de 2.4 GHz, aunque estas ahora en la actualidad muestran interferencias con otros sistemas que también utilizan la misma frecuencia. En la figura 3.28 se muestra los radios transceptores en la banda de 2.4 GHz

Figura 3.28 Radio Transceptores a 2.4 GHz

Hoy en día para las soluciones inalámbricas en los sistemas de video vigilancia el radio transceptor debe operar en la banda de los 5,8 GHz. Los equipos que más se utilizan son los Nano Station de la marca Ubiquiti. Estos equipos aparte de ser Radios Transmisores y Receptores también son Antenas, todo incluido en una misma pieza, en pocas palabras son antenas con un radio RF incorporados, y para interperie, con protección para rayos UV, etc.

Este equipo se alimenta a través del mismo cable de red usando la función POE (Power Over Ethernet), es decir, por el mismo cable de red, van los datos y la electricidad del equipo, facilitando así su instalación. A continuación se muestran en las figuras 3.29 y 3.30 los radios que no tienen solapamiento entre canales y son recomendados en sistemas inalámbricos de video vigilancia.

Figura 3.29 Radios de la marca Ubiquiti

Figura 3.30 PoE de radio Nano Station

Otro componente del sistema de video vigilancia son los cables coaxiales y los cables de red UTP, a continuación se describe las características del cable coaxial más utilizado en los sistemas de video vigilancia:

- Cubrimiento de distancia hasta de 200mts.
- RG59 es el estándar a usar para transmisión de video.
- 95% de Blindaje en Cobre.
- Conductor Central en calibre 18 AWG.
- Conectores BNC de ponchar.
- Empalmes con uniones BNC.
- Es necesario instalar a una distancia mínima de 30 cm de cables con voltajes superiores a 48V ya que es susceptible a ruido eléctrico.

3.5 CABLEADO EN VIDEO VIGILANCIA

Existen 2 alternativas para la conexión cableada en sistemas de video vigilancia, el cable coaxial y el cable UTP.

3.5.1 CABLE COAXIAL

La transmisión a través de cable coaxial es conocida como desbalanceada, debido a la forma constructiva del cable. El blindaje rechaza exitosamente interferencias electromagnéticas superiores a 50 KHz. Sin embargo, la radiación proveniente de las redes eléctricas de 50 Hz es más difícil de eliminar y depende fundamentalmente de la corriente que circula por los conductores cercanos. Por este motivo conviene alejar por lo menos 30 cm los cables coaxiales de video de los que transportan energía.

La manifestación visual de esta interferencia son barras o líneas horizontales que se desplazan hacia arriba o hacia abajo en la pantalla del monitor. La frecuencia de desplazamiento se determina por la diferencia entre la frecuencia de campo de video y la frecuencia de la red eléctrica. Varía generalmente entre 0 y 1 Hz. Las radiaciones electromagnéticas provocadas por rayos o vehículos se visualizan como ruidos irregulares.

3.5.2 PAR TRENZADO UTP

Cuando las distancias entre los distintos componentes de un sistema de CCTV exceden los 200 mts, la transmisión de video por par trenzado es una opción muy conveniente frente al cable coaxial con amplificadores de video ya que estos amplifican también las interferencias. La impedancia característica del UTP es de 100 ohm.

Toda interferencia electromagnética y ruido no deseado que llegue a ambos conductores, se cancelará debido a que el sistema admite señales en modo diferencial (distinta polaridad en cada conductor del par), ya que están balanceados con respecto de masa. Por este motivo se la conoce como transmisión balanceada y es necesario que los cables estén trenzados.

La adaptación entre los equipos y el cable se realiza a través de un BALUN. Los balunes pasivos no necesitan energía externa y son bilaterales, es decir trabajan indistintamente en ambos extremos de la línea. Con estos elementos se logran transmisiones de señal de video a distancias de hasta 300 mts. Para longitudes mayores (hasta 2400mts.) se utilizan balunes activos.

Se pueden utilizar cableados existentes de redes de computación.

Se pueden conectar hasta 4 cámaras con un solo cable.

Menor costo para tendidos superiores a 70 mts.

3.5.3 CONECTORES BNC

El conector BNC (Bayonet Neill-Concelman) es un tipo de conector para utilizarlo con el cable coaxial como RG-58 y RG-59 en aplicaciones de Radio Frecuencia que precisan de un conector rápido, también es apto para UHF (Ultra Alta Frecuencia), es de impedancia constante a lo largo de un amplio espectro. Muy utilizado por su versatilidad en equipos de radio de baja potencia, instrumentos de medición como osciloscopios, generadores, puentes, etc.

Los cables coaxiales RG-59 deben tener en sus terminales algún tipo de conector BNC. Este conector permite la interface física de la señal de video para que pueda viajar través del clave coaxial. En la figura 3.31 se muestran varios tipos de conectores BNC.

Figura 3.31 Varios tipos de conectores BNC

3.6 TRANSCEIVERS PASIVO

Permite enviar la señal (vídeo, datos +/- y alimentación) de 1 cámara por un solo cable UTP. Sistema formado por el emisor (splitter) y el receptor (inyector). El emisor dispone de conexión BNC (vídeo), datos (DATA+R / DATA-B) y jack de alimentación, para conectarle tanto la señal de vídeo, datos como alimentación de cualquiera de nuestras cámaras, así como un conector RJ45 para la conexión del cable UTP. El receptor dispone del mismo conector RJ45 y de conexión BNC, datos y jack de alimentación. De esta forma, se puede alimentar a distancia la cámara y obtener la señal de vídeo y RS485 (+/-) proporcionada por ésta. La longitud máxima entre el extremo que se conecta a la cámara y el extremo de salida es de 100 metros para señales en color.

Un transceivers pasivo no requiere de carga eléctrica, permite mejorar la señal hasta 600 mts de distancia (B/N), y dispone de un filtro de entrada para corregir interferencias.

Figura 3.32 Transceivers Pasivo

3.6.1 CARACTERISTICAS DEL TRANSCEIVER PASIVO

Están las siguientes:

Número de canales: 1 canal

Alimentación: No requiere

Entrada/Salida vídeo: BNC (macho)

Distancia transmisión: Max 300 m

Frecuencia de operación: DC - 10 MHz

Conector par trenzado: RJ45

Rechazo modo común: 70 dB

Impedancia de entrada: 75 Ω

Impedancia de salida: 100 Ω

Categoría de cable: UTP categoría 3, 4, 5, 5e o 6

Tipo de cable: UTP 2-24 AWG

3.6.2 TRANSCEIVER ACTIVO

Un transceiver activo requiere de carga eléctrica, permite mejorar la señal hasta 1800 mts de distancia, y también dispone de un filtro para corregir interferencias. Algunas de sus características son:

- Le permiten transmitir video a muy largas distancias, utilizando cables de pares trenzados categoría 5 ó 6 superando las limitaciones del cable de video convencional (RG59).
- Permite transmitir hasta 4 señales de video (cámaras) usando un mismo cable de UTP (4 pares de hilos).
- Disminuye dramáticamente las descargas eléctricas sobre las cámaras CCTV, DVR's y Monitores.
- Su inmunidad excepcional de interferencia asegura una alta calidad de las imágenes video.

Figura 3.33 Transceivers Activo

Los Transceivers Power Over Ethernet, permiten trasmitir 12 V o 24 V a través del mismo cable UTP por donde trasmitimos la señal de video, sin afectar la calidad de la misma. La calidad y el ponchado de los conectores es muy importante para evitar pérdidas de la calidad en la señal.

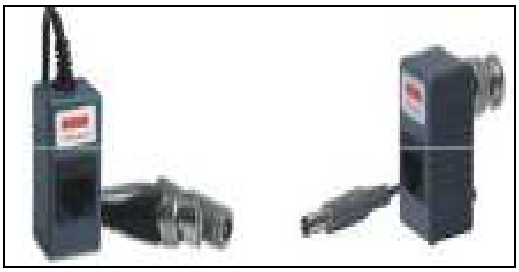

Figura 3.34 Conectores y Accesorios activos

3.7 ALIMENTACIÓN ELÉCTRICA EN VIDEO VIGILANCIA

Se puede administrar la alimentación eléctrica de dos formas, con adaptadores de corriente independientes para cada cámara o con cajas de alimentación centralizadas para todas las cámaras. De acuerdo al tipo de solución se debe pensar en cuál es la más indicada.

Figura 3.35 Alimentación Eléctrica

3.7.1 RESPALDO DE UPS

Es necesario tener un respaldo de energía en caso de cortes para toda solución de CCTV. También se sugiere el uso de Inversores y Plantas Eléctricas, así como supresores de pico y reguladores de alto desempeño. En la actualidad existen UPS (Uninterruptible Power Supply o fuente ininterrumpible de energía) cuidadosamente diseñado para suministrar energía eléctrica de altísima calidad a sus sistemas críticos como cuarto de servidores y equipos de telecomunicaciones.

Existen en las capacidades de 5, 10, 15, 20 y 30 kVA en los voltajes más comúnmente utilizados. En la figura 3.36 se muestra un sistema completo de video vigilancia.

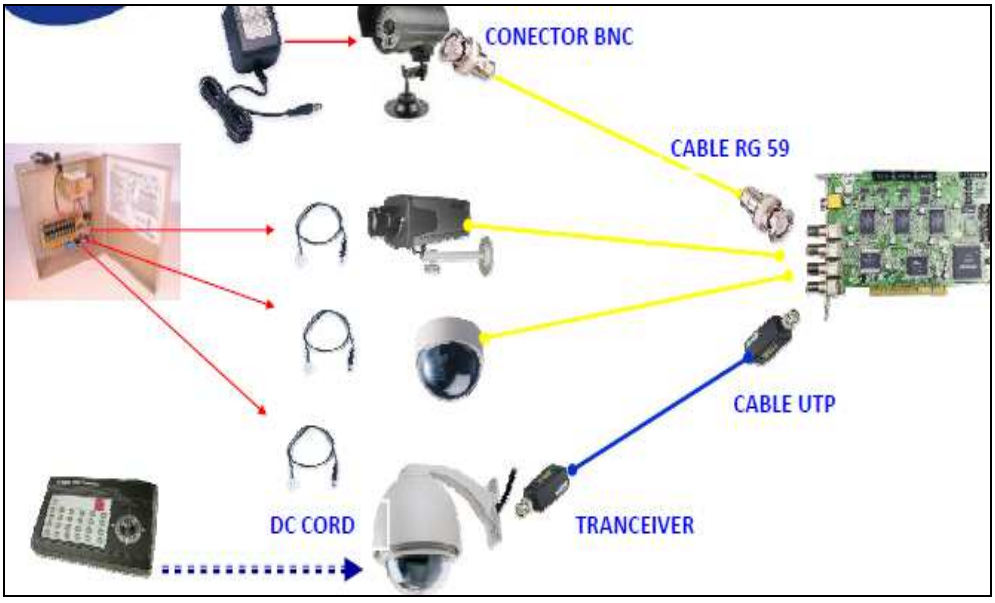

Figura 3.36 Sistema de video vigilancia sus conexiones

CAPITULO 4

DISEÑO E IMPLEMENTACION DE SISTEMA DE VIDEO VIGILANCIA PARA LA FACULTAD TECNICA CON RESPALDO DE SERVIDOR VIA IP

Para realizar el diseño y posteriormente la implementación del sistema de video vigilancia a la Facultad Técnica de la Universidad Católica, se escogió los siguientes pasos:

1. Determinar el propósito del Sistema de video vigilancia.
2. Definir el área que debe visualizar cada cámara.
3. Determinar la ubicación del o los monitores.
4. Definir la forma de transmisión de la señal de video desde las cámaras al monitor.
5. En base a los puntos anteriores, determinar la selección de equipos necesarios.

4.1 EL PROPÓSITO DEL DISEÑO

En base a la observación, criterios de seguridad y acontecimientos sucedidos, se ha definido que el diseño de un sistema de video vigilancia debe realizar los siguientes aspectos:

- Monitorear los ingresos y/o salidas de aulas y laboratorios de la Facultad Técnica para tener control de lo que sucede.
- Registrar en medio digital sucesos importantes y que requieren ser grabados.
- Prevenir primeramente robos o destrucción de bienes de la Facultad, mediante la "advertencia" al hacer notorio el sistema de monitoreo.
- Prevención de siniestros a terceros.
- Incrementar la seguridad para estudiantes, profesores y autoridades.

- ❖ Llevar control del aula o laboratorio monitoreados de manera remota.
- ❖ Tener un soporte digital en caso de necesitarse pruebas para demostrar un hecho pasado en aulas o laboratorios monitoreados.

4.2 DEFINICION DEL AREA A MONITOREAR

La Facultad técnica tiene 32 aulas para el uso educativo, es decir existen en cada una de ellas equipos y accesorios que son bienes activos, aparte existen 8 laboratorios de las carreras de Telecomunicaciones, Electrico-Mecanica, Control y Automatismo y así también los laboratorios para la elaboración de lácteos y cárnicos. Por ello un razonable criterio en la ubicación de las cámaras es que debe estar en los pasillos de las aulas y pasillos de laboratorios. En la siguiente figura se aprecia el pasillo a los laboratorios de informática y aula T2 hasta la T5.

Figura 4.1 Monitoreo a aulas y laboratorios de informática

Figura 4.2 Monitoreo a laboratorios de Electrico-Mecanica y Telecomunicaciones

4.3 UBICACIÓN DEL MONITOR Y DEL DVR

Se debe recordar que este sistema está basado con respaldo por servidor y por lo tanto este puede ser visualizado por cualquier computadora que esté conectado a internet, es decir cualquier persona que conozca el número del puerto remoto, además el usuario y contraseña, podría acceder a la monitorización de cámaras que están en la Facultad Técnica. A las autoridades de la Facultad se les explica el procedimiento para monitorear remotamente las cámaras de video.

El DVR estará ubicado en el cuarto de telecomunicaciones que tiene la Facultad Técnica. Allí se conecta con el switch y específicamente en un puerto que designo Centro de Cómputo para así tener conectividad a internet.

4.4 TRANSMISIÓN DE IMÁGENES DEL SISTEMA DE VIDEO VIGILANCIA

Se puede poner cámaras totalmente IP en todos los pasillos y puntos estratégicos de la Facultad técnica. Pero estos desde el punto de vista técnico colapsaría la red de nuestra Facultad, como así también en toda la universidad, el ancho de banda que se tiene por parte de Centro Computo de la Universidad Católica es insuficiente, esto técnicamente es imposible de realizar. Y desde el punto de vista económico poner un sistema completo y con la cantidad de 22 cámaras totalmente IP llegaría a sobrepasar los 20 mil dólares.

El mejor sistema para realizar la video vigilancia es un sistema hibrido, es decir que con cámaras análogas y por medio de un DVR se puede paquetizar las señales de video, en otras palabras el DVR convierte en paquetes el video tomado de las cámaras y así esta información puede viajar a través de la red y ser solicitada desde cualquier punto remoto, solo basta conocer el puerto remoto, usuario y contraseña.

4.5 SELECCIÓN DE LOS EQUIPOS

Se utilizaron en la implementación, 14 cámaras infrarrojos de la marca AVTECH

1 equipo DVR marca AVTECH de 16 puertos

14 balun´s

1 Disco duro de 1Tera byte

Figura 4.3 La selección de componentes para la implementación

4.6 UBICACIÓN DE LAS CÁMARAS EN LA FACULTAD TECNICA

Esta es la ubicación de las cámaras infrarrojos en los pasillos y puntos estratégicos a vigilar, ver figura 4.4 (círculos representan ubicación de cámaras).

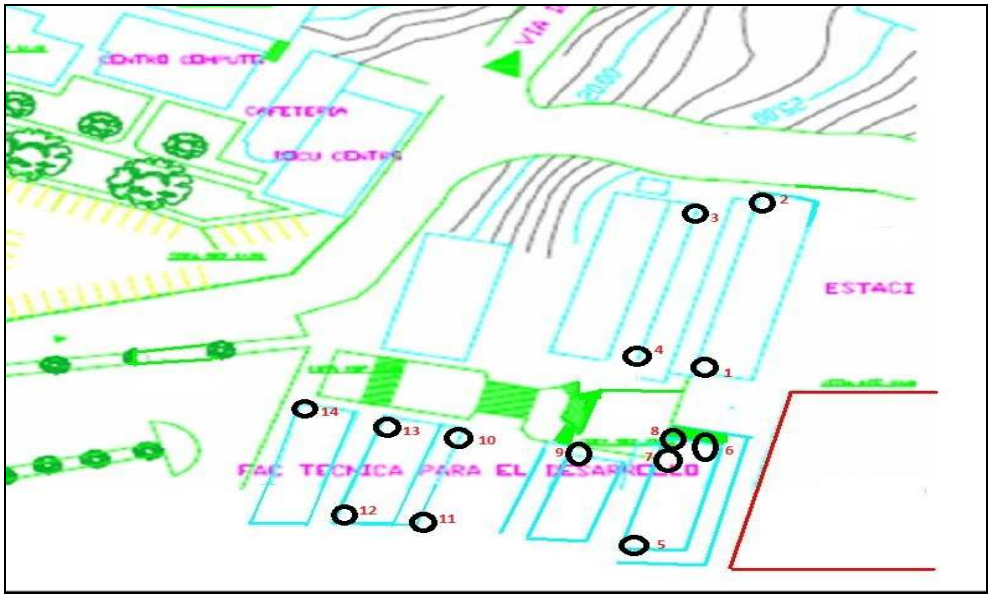

Figura 4.4 Ubicación de las 14 camaras en la facultad tecnica

Ahora bien, solo resta hacer un plano de cableado empotrado por cada edifico de aulas de la Facultad, se cuido la estética que no se vean cables que cuelguen ni que sean susceptibles a deterioros etc. Las siguientes imágenes muestran como se trabajo en la instalación de todo el sistema, los 4 integrantes de esta tesis realizo el trabajo bajo la supervisión del director de la tesis.

Figura 4.5 Equipos y dispositivo utilizados en sistema de video vigilancia

Para cada cámara se utilizo un balun o adaptador de impedancias este a su vez se conecta a un puerto del DVR, se presento la opción de utilizar un código de colores para la conexión de las cámaras hacia el DVR, ver figura 4.6

Figura 4.6 Conexión de balun´s con cámaras hacia DVR

Las siguientes imágenes muestran el rack del cuarto de telecomunicaciones lugar donde está el DVR y el puerto con la dirección IP que fue provista por Centro de Cómputo. La figura 4.7 muestra la ubicación de los equipos mencionados.

Figura 4.7 Conexión del puerto con la IP para el DVR

Dentro del cuarto de telecomunicaciones es más fácil poder revisar las conexiones en caso de que alguna cámara no funcione, esta la marcación de cada cable de red, en la figura 4.8, muestra el equipo DVR colocado dentro del rack, allí estará operando es decir paquetizando las imágenes captadas por las cámaras.

Figura 4.8 DVR ubicado en el rack de telecomunicaciones

Finalmente en el siguiente capítulo se realizó las pruebas finales para supervisar y monitorear remotamente el sistema de video vigilancia implementado en la Facultad Técnica para el Desarrollo.

CAPITULO 5

PRUEBAS DEL SISTEMA DE VIDEOVIGILANCIA

Antes de monitorear o visualizar a través de un monitor las imágenes captadas por las 14 cámaras, primero se procede a entrar al sistema, a continuación se detalla pasos para entrar al monitoreo en la Facultad Técnica.

5.1 OBTENCIÓN DE LOS PARÁMETROS DE RED

Si no se conocen los parámetros de la red en la que el DVR está conectado, es sencillo obtenerlos de la siguiente manera:

1- Hay que utilizar un computador que esté conectado a la misma red que el DVR.

2- En el menú “Iniciar” de la barra de tareas de Windows, existe un campo titulado “Buscar programas y archivos”.

3- En este campo, se escribe “cmd” y se pulsa Enter. Esto lo que hace es que se despliegue una pantalla negra al estilo MS-DOS donde se pueden insertar comandos.

4- En la pantalla negra se escribe “ipconfig” y se pulsa Enter. El resultado es que aparecen en pantalla los principales datos de la red a la que está conectado el computador (y, por extensión, el DVR).

5- Entre los datos que se despliegan en la pantalla, se pueden encontrar la máscara de subred y la puerta de enlace predeterminada.

5.2 ESTABLECER LA DIRECCIÓN IP

Con la puerta de enlace y la máscara de subred se puede establecer una dirección IP válida para el DVR. Hay que tener en cuenta que la dirección IP que se asigne al DVR tiene que tener el mismo rango que la puerta de enlace.

Dado por Centro de Cómputo se obtuvo la siguiente IP para el DVR: **172.16.9.65**

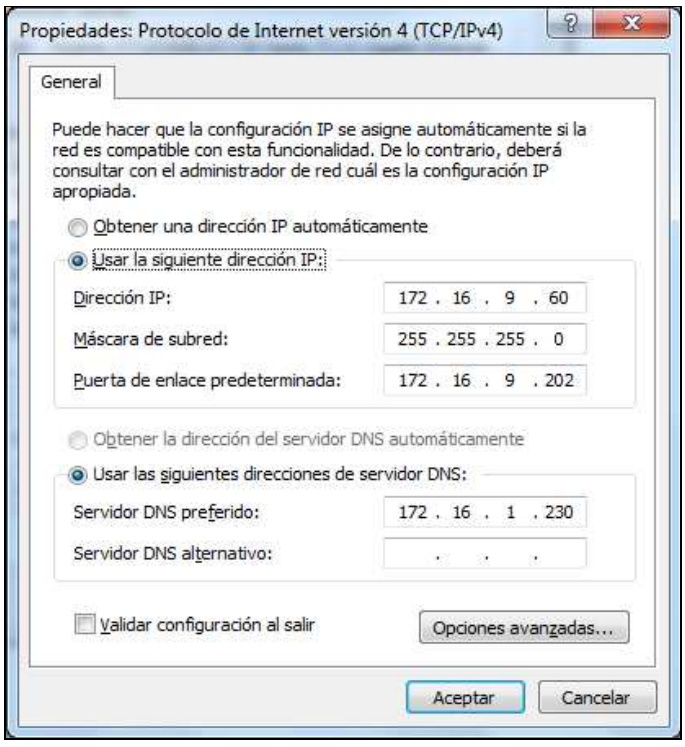

Figura 5.1 LA IP, PUERTA DE ENLACE Y DNS DADOS POR COMPUTO

5.3 ACCESO POR RED LOCAL

Una vez que el DVR tiene correctamente configurado el menú de red, es posible acceder a él en red local, a través de ordenadores que estén conectados en la misma red que el equipo.

Este acceso se puede hacer de dos maneras:

1- A través de un navegador web (Ejemplo: Internet Explorer)

2- A través del software que acompaña el DVR en el CD.

5.4 ACCESO EN REMOTO

Con los parámetros de red del DVR correctamente configurados, también es posible acceder a él desde un acceso remoto, situado fuera de la red local en la que esté conectado el equipo. La única diferencia es que, para poder acceder en remoto, no hay que utilizar la dirección IP que se ha establecido para el DVR (ya que ésta es una dirección IP de la red local), sino que hay que utilizar la dirección IP externa del router de la red.

5.4.1 OBTENCION DE DIRECCION IP

Para conocer la dirección IP externa del router de la red se puede consultar la siguiente página web: **http://www.cualesmiip.com/**

Se trata de una página web que directamente te indica tu dirección IP al acceder a ella, sin necesidad de hacer nada más.

5.4.2 PROBLEMAS EN EL ACCESO: CAMBIO DEL PUERTO HTTP

Es relativamente frecuente que el acceso en remoto falle si se utiliza el puerto 80 como puerto HTTP. Si se da este caso, es necesario cambiar el puerto 80 por otro puerto en el menú de “Red” de la configuración del vídeo grabador. Por ejemplo, es muy habitual utilizar el puerto 80.

Lógicamente, es necesario asegurarse de que el nuevo puerto seleccionado está abierto en el router, así como re-direccionarlo dentro del router si fuera necesario (todo esto a través del servicio NAT). Si se modifica el puerto HTTP, a la hora de acceder al vídeo grabador a través del navegador web es necesario indicar, además de la IP, el puerto por el que se quiere acceder. Por ejemplo, si la IP externa es 217.18.226.130, y se ha definido el puerto 80, para acceder a través del navegador web es necesario poner en la barra de direcciones lo siguiente: http://217.18.226.130:80

5.5 UTILIZACIÓN DE DDNS

El DVR está preparado para utilizar un servicio DDNS. La utilidad de este servicio consiste en que se sustituye el acceso a través de una dirección IP por un acceso a través de un nombre de dominio, más fácil de recordar. Además, si la IP del router de la red es dinámica y cambia, la utilización de DDNS permite actualizar la IP para un mismo

nombre de dominio, de modo que no es necesario preocuparse por este cambio en la dirección IP.

Los dos principales servicios DDNS que se pueden utilizar con estos equipos son:

1. DynDNS

2. No-IP

Para utilizar el servicio DDNS, hay que llevar a cabo los siguientes pasos:

1. Obtener una cuenta DDNS.

2. Configurar el vídeo grabador.

5.6. OBTENER UNA CUENTA DDNS UTILIZANDO DYNDNS

Las cuentas DynDNS se solicitan y gestionan de manera gratuita en la página web

http://www.dyndns.com/

Una vez dentro de esta página, se pincha en el botón “Sign up FREE”, que permite crear una cuenta DynDNS de manera gratuita

Básicamente, hay que rellenar lo siguiente:

Hostname: será la dirección que habrá que escribir en los navegadores para acceder al equipo. La extensión se puede escoger entre un grupo de extensiones que aparecen en el menú desplegable. La más habitual, no obstante, es dyndns.org.

Se selecciona el nombre que va a tener la cuenta (el dominio). Es un nombre a elegir, que IP Address.

A continuación se da clik en el botón “Add to cart” y se accede a otra pantalla donde se completan los datos, indicando un nombre de usuario, una contraseña y una cuenta de correo electrónico para que el servicio DynDNS pueda comunicarse con el cliente.

Aquí se indica la dirección IP a la que se quiere asociar el nombre de dominio.

5.6.1 CONFIGURACIÓN DE DDNS EN EL DVR

La utilización del DDNS se configura en el menú “Red”, dentro de “Menú principal en este menú, dentro del recuadro de la parte de debajo de la pantalla (configuración avanzada, como se muestra en la siguiente imagen), hay que descender por la barra de desplazamiento hasta encontrar la casilla llamada “DDNS”.

Para utilizar el DDNS hay que marcar la casilla a la izquierda del nombre, y para configurarlo hay que pinchar con el ratón dos veces en la línea del DDNS, apareciendo el siguiente menú:

En este menú hay que definir una serie de parámetros, que serán distintos según el tipo de servicio DDNS que se haya creado.

5.6.2 UTILIZANDO DYNDNS TIPO DDNS

Dentro del menú desplegable, se selecciona “DyndnsDDNS”.

IP del servidor dirección IP: 204.13.248.112.

Si se utiliza el nombre de servidor, hay que tener correctamente configurado el apartado DNS para que el equipo traduzca la dirección IP a la que se refiere el nombre de servidor indicado.

Se escribe el nombre del servidor “members.dyndns.org”, o bien su equivalente.

Puerto: Debe utilizarse uno de los puertos siguientes: 80, 8245.

Nombre Dominio página web: El nombre de dominio que se haya establecido al crear la cuenta DynDNS en la www.dyndns.com.

Usuario: El usuario que se haya establecido al crear la cuenta DynDNS en la página web

www.dyndns.com

Contraseña: La contraseña que se haya establecido al crear la cuenta DynDNS en la página web; www.dyndns.com

Además, hay que marcar la pestaña “Activar”, de la parte derecha superior de la ventana.

5.6.3 ACCESO AL DVR UTILIZANDO DDNS

Si se ha creado un nombre de dominio con una cuenta DDNS, el acceso al DVR en remoto es igual a como se ha comentado en el capítulo 3, pero en vez de escribir la dirección IP en la barra de direcciones del navegador web, se escribe el nombre de dominio que se definió al crear la cuenta DDNS. Por ejemplo, con una cuenta DynDNS: http://nombredominio.dyndns.org

Si, además, el puerto HTTP definido no es el 80, habrá que indicarlo de la siguiente manera (usando, por ejemplo, el 80): http://nombredominio.dyndns.org:80.

5.7 PRUEBAS DEL SISTEMA DE VIDEO VIGILANCIA

Se muestra en las siguientes imágenes la captación de las cámaras de video vigilancia ubicada en pasillos y puntos estratégicos en la Facultad, la prueba se la realizó en la noche, esto se cumplió ante la presencia del director de Carrera Ing. Pedro Tutiven, quien además siempre presto su colaboración y criterios para concluir de forma satisfactoria la parte final de la tesis.

Se abrió un explorador se digito la dirección 172.16.9.60:80

Figura 5.2 Pasillos de Laboratorios de Electrónica y otros

Figura 5.3 Video vigilancia de las escalinatas a las Aulas

Figura 5.4 Video vigilancia de Laboratrorios de Lacteos y 1º bloque de aulas

Figura 5.5 Asociación de Estudiantes y Parqueadero de la Facultad

Figura 5.6 Captación de todas las cámaras de video que componen el sistema

CONCLUSIONES

El sistema de video vigilancia remota con respaldo de servidor es la propuesta técnica y factible para monitorear las aulas y laboratorios de la Facultad Técnica.

Las 14 cámaras de video vigilancia cumplen una labor de prevención y hasta de persuasión (letreros de advertencias, estas siendo filmando) ante eventuales robos o daños en los bienes activos de la Facultad Técnica.

Las características técnicas de las cámaras son de óptimo rendimiento y con alcance tanto en interiores como en exteriores, además de una perfecta visión nocturna (son infrarrojos) y diurna.

El sistema de video vigilancia remoto permite grabar por día, semanas y meses y así esta información es posible guardarlo en un disco duro de capacidad de un Tera byte, el sistema de compresión de video es Mpeg-4.

El DVR (Grabador de Video Digital) recibe la señal analógica de las 14 cámaras y este equipo las transforma en paquetes, de esta forma puede viajar por internet.

La última generación de los sistemas de video vigilancia utiliza internet para trasmitir las imágenes, accediendo mediante un puerto gratuito 80. El sistema diseñado e implementado utiliza dicho puerto y que tan solo se necesita abrir un explorador y

digitar la IP: 172.16.9.60 luego colocar dos puntos (:) y el número de puerto para así monitorear remotamente.

Las imágenes podrán visualizarse a través de un monitor, o del teléfono móvil basta que tenga acceso a internet.

Los sistemas de video vigilancia con cámaras IP es una opción que demanda de un gran ancho de banda, para el caso de la Facultad Técnica el sistema hibrido es la mejor opción ya que con una sola IP no colapsaría la red de la Facultad Técnica ni de la UCSG.

RECOMENDACIONES

Se recomienda que el sistema de monitoreo remoto de video vigilancia tenga siempre en cada una de sus cámaras la alimentación de 110 0 120 vca y corriente 1.5 mA, Caso contrario las cámaras funcionan de forma irregular, parpadea la captación de imágenes etc.

El responsable de monitorear las aulas y laboratorios de la Facultad Técnica, debe tener un monitor exclusivo para la supervisión con acceso único de administrador, de esta forma se evitaría manipulación indebida del sistema de vigilancia.

Se debe dar mantenimiento de las cámaras por lo menos cada 4 meses, limpiando el polvo y revisando sus conectores, así se evita disfuncional trabajo del sistema o daños en el mismo.

De ser posible debe contar con respaldo de cámaras que puedan tener salida de voz y con movimientos robotizados. Se deja 2 puertos disponibles en el DVR para dos cámaras que se desee instalar a criterio del responsable del monitoreo.

El DVR debe grabar y una vez revisado según cronograma de análisis puede ser borrado las imágenes de semanas que ya han sido revisados para fin de que se mantenga listo el disco duro, para guardar nueva información de video.

Se puede potencializar el sistema con un respaldo de video vigilancia pero con conexiones inalámbricas pues los cables pueden estar propensos a cortes o sabotajes.

BIBLIOGRAFIA

[1] Kurose. J. *Redes de computadoras un enfoque ascendente basado en internet*. 2º Edición, Editorial Pearson Addison Wesley. Madrid, España 2005

[2] García T. *Alta velocidad y calidad de servicios en redes IP*, editorial Alfa omega RA-MA España 2004

[3] Stalling W. *Comunicaciones y redes de computadores*, 7º Edición, Editorial Pearson Pretince Hall, Madrid España 2004

Referencias de internet:

[5] http://www.securimport.com/tutorial.php?id=18

[6] www.rediris.es/media/gt/gt2004_2/capturavga.ppt

[7] www.video-computer.com/video.htm

[8] www.openh323.org

[9] www.siemon.com7la/

[10] www.idg.es/pcworldtech/index.asp?seccion=comunicaciones

ANEXOS

Configuración con código de colores para las 14 cámaras utilizadas en el sistema