INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELECTRICA

UNIDAD CULHUACAN.

"SEGURIDAD EMPLEANDO SISTEMAS CON MANEJO DE INFORMACION VIA IP"

T E S I S

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMUNICACIONES Y ELECTRONICA

PRESENTA:

ISRAEL CAMARILLO MARTINEZ

México D.F. **Abril de 2011**

Agradecimientos.

Al único y sabio Dios, que me ha mostrado su poder y su amor a través de mí vida, pero sobre todo gracias porque un día tuviste compasión de mi vida y me diste el regalo que nunca podría haber alcanzar con mi propia fuerza que es el conocerte y ser tu hijo amado y por eso hoy puedo agradecerte todas estas bendiciones recibidas.

Esta tesis está dedicada a mi Padres, a quienes agradezco de todo corazón por su amor, cariño y comprensión, además por sus consejos y ser guías en mi vida por ultimo quiero que sepan que en todo momento los llevo conmigo.

Agradezco a mi hermano por la compañía y el apoyo que me brinda y gracias porque sé que cuento con el siempre.

Agradezco a la familia Camarillo y Martínez porque fueron parte de mi inspiración.

Agradezco a Carolina por estar presente conmigo durante estos años y el compartir mi existencia con ella.

Agradezco a todo Centro Cristiano Zamar por permanecer en sus oraciones.

Agradezco a los amigos por su confianza y lealtad.

Agradezco a mi país porque espera lo mejor de mí.

Agradezco a mis maestros por su disposición y ayuda brindadas.

ISRAEL CAMARILLO MARTINEZ
INGENIERO EN COMUNICACIONES Y ELECTRONICA **Abril 2011**

Objetivo.

La finalidad de esta Tesis es presentar el diseño de un sistema de seguridad con Cámaras IP inalámbricas. Además se determinará el software que es necesario disponer para el monitoreo de las cámaras y el almacenamiento de imágenes y de video, así como la configuración del sistema de seguridad.

Con la instalación de un sistema de vigilancia de red, se puede monitorizar de forma local o remota la seguridad de las personas y las propiedades en cualquier lugar y en cualquier momento. La vigilancia de red permite enviar imágenes y audio en directo tanto para monitorizar, en labores de educación, detección y solución de problemas, transmitir por red eventos, o cualquier otra actividad que requiera presencia remota.

Justificación.

La delincuencia ha incrementado su accionar y se hace imprescindible plantear alternativas para contrarrestar la inseguridad que las personas viven cotidianamente.

Con la presentación de esta Tesis se busca dar una solución al problema de inseguridad utilizando la tecnología en beneficio de la comunidad, mediante el diseño de un sistema de seguridad que utiliza un conjunto de cámaras de video, para vigilar el ambiente externo, y un sistema de alarmas detectores de intrusión, para vigilar el ambiente interno de un hogar, edificio, unidades de negocio, sucursales bancarias, sucursales de comercio, establecimientos educativos, religiosos y turísticos, etc.

Resumen.

En el primer capítulo, se da a conocer todos los componentes de un sistema de seguridad, su funcionamiento y sus características más relevantes. Además, se definen los lineamientos básicos que se van a seguir para el diseño del sistema de seguridad, de tal manera que se pueda realizar la selección de equipos en el tercer capítulo.

Se especifican los criterios en los lineamientos básicos de la instalación del sistema de seguridad, donde se procede a buscar en el mercado tecnológico los equipos electrónicos que se adapten y cumplan los estándares de calidad y confianza que el usuario requiere.

Los equipos de sistema de seguridad escogidos son los principales argumentos del sistema de seguridad como Cámaras IP, equipos de monitoreo, almacenamiento y paneles de alarma, así como su configuración.

El diseño completo del sistema de seguridad definiendo el medio de transmisión, el diseño del Centro de Control, sistema de respaldo de información, protección eléctrica y respaldo de energía, entre otros aspectos más que permitirán trabajar de mejor manera al sistema completo.

Para tener una idea acerca de la inversión necesaria para la implementación del sistema de seguridad se realiza el presupuesto total presentando precios referenciales representados en Moneda Nacional de México.

En el último capítulo se presentan las conclusiones que se obtuvieron en la realización de la Tesis, y así mismo recomendaciones para la fase del diseño y correcta operación del sistema de seguridad.

Introducción.

Con el aumento del uso de la tecnología en todos los ámbitos, se ha dado lugar a una demanda sustancial en seguridad ó monitoreo a distancia por medio de servidores (computadoras), lo que a dado lugar a que las organizaciones confíen en un enlace corporativo que satisfaga sus necesidades para cumplir las funciones vitales de sus negocios.

Una de las tecnologías de monitorea actual, es el circuito cerrado partiendo de una serie de equipos interconectados entre sí (Servidores de Dominio).

El desarrollo de esta Tesis es para resolver los problemas relacionados con la seguridad de cualquier lugar utilizando herramientas tales como las Cámaras IP e Internet. Donde a través de dichas herramientas es posible contar con un sistema de vídeo vigilancia que permita el acceso al mismo utilizando cualquier PC con conexión a Internet. Actualmente es una necesidad contar con este tipo de sistemas que permitan la seguridad, la vigilancia por medio de un centro de monitoreo.

La vigilancia con cámaras IP o cámaras web permitirán capturar y enviar vídeo en tiempo real a través de una red, como una LAN, intranet o Internet, y admitirá a usuarios autorizados con facultades de poder ver y/o gestionar la cámara con un navegador Web a través de un software de captura de vídeo en cualquier equipo local o remoto conectada a una cierta red o dominio de un Servidor.

El sistema de monitoreo permitirá a los usuarios autorizados que se encuentren en distintas ubicaciones acceder simultáneamente a las imágenes captadas por la misma cámara de red.

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

Índice

Tabla de contenido

CAPÍTULO 1

Conceptos Básicos.

1.1 Seguridad en la Sociedad.

La inseguridad se entiende como la consecuencia de todo desorden social y económico: es argumento político, ético, económico, moral, y cultural para justificar la intervención de los poderes gubernamentales, mediáticos y financieros, en la esfera del espacio público y de la vida privada. Se tiene actualmente en la sociedad un monstruo llamado inseguridad, que transita entre lo paranoico imaginario y lo fáctico. La inseguridad no es producida necesariamente por la falta de seguridad. La inseguridad es un problema sistémico e integral más que un problema de falta de vigilancia.

Dado el alto índice de delincuencia, los niveles de inseguridad y las pocas respuestas que se pueden dar para prevenir actos delictivos, en el presente se proceden a dar una descripción de los sistemas de seguridad, de video vigilancia CCTV (circuito cerrado de televisión), sus componentes básicos y alarmas más comunes, que en la actualidad son utilizadas para proteger a la comunidad.

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

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

El ser humano siempre se ha movido por el impulso innato de satisfacer sus necesidades básicas, esto lo ha llevado a evolucionar para poder controlar, de cierta manera, su supervivencia. Sin embargo, también han surgido necesidades que ahora es necesario satisfacer. Una de ellas es la seguridad.

A medida que la sociedad evolucionó las causas de la inseguridad se tornaron más complejas lo que conllevó a que se planifiquen sistemas de seguridad de la misma índole, es por esto que notamos que varios elementos a nuestro alrededor cambiaron. Por ejemplo**,** las cerraduras ya no son lo mismo, como tampoco las puertas, ahora el sistema de seguridad incluye una puerta blindada con varios cerrojos y materiales impenetrables; las alarmas que antes eran sonoras ahora incorporan una conexión con vigilancia privada lo que hace que además de emitir un sonido disuasivo, nos garantiza la presencia de ayuda profesional.

Estos sistemas agregaron también el monitoreo mediante un microprocesador que incluye un comunicador digital; su efectividad depende de la seriedad y la eficiencia de la central de monitoreo contratada; en estos casos se recibe una conformación de que la llamada ha sido recibida pero si la central no es una empresa seria, los operadores terminan siendo ineficientes para manejar determinadas situaciones.

El concepto de "sistemas de alarmas" remonta su origen a principios de los años treinta a consecuencia del incremento de nuevas modalidades delictivas que afectaban a algunas ciudades y en virtud de la aparición de nuevas tecnologías en materia de seguridad y vigilancia.

Los sistemas de seguridad han ido evolucionando conforme se van desarrollando nuevas tecnologías y los usuarios exigen mejores soluciones a sus problemas, con un menor tiempo de respuesta, con mayor eficiencia y con un mínimo de fallas. Los sistemas se dividen en generaciones para poder clasificar su operatividad, esto garantiza al usuario la confiabilidad de que se cumplirán sus requerimientos con las últimas novedades tecnológicas.

Hay una gran variedad de sistemas de seguridad, pueden encontrarse desde sencillos dispositivos en red de seguridad poco compleja implementados para hogares, hasta edificios inteligentes en donde los dispositivos son capaces de tomar decisiones.

Existen 3 generaciones en la historia de los sistemas de seguridad, clasificadas dependiendo de la complejidad que involucra. La primera generación se involucraba únicamente a la implementación de un dispositivo capaz de dar aviso de cualquier violación y un medio que lo controlará.

La segunda generación ya consistía en un medio capaz de controlar los eventos y que además podía tomar decisiones de acuerdo a la situación. Esto permitió que el usuario dejará de realizar eventos manuales y que además disminuyeran el número de falsas alarmas, pues los dispositivos eran capaces de interpretar una situación y definir su en realidad era una situación de alarma o simplemente una situación poco usual.

Por ultimo en la tercera generación, ya se implementaron medios para poder monitorear todos los eventos que se realicen en un lugar sin que el usuario tenga que estar en la misma ubicación. Esto da flexibilidad al usuario para que al mismo tiempo que realiza otras actividades pueda estar revisando el estado en el que se encuentra la empresa o su hogar.

Además un sistema que monitoree actividades puede llevar una bitácora de los eventos realizados durante un periodo de tiempo lo que permite definir situaciones de riesgo o determinar ciertas acciones que mejoren el desempeño del sistema.

Las tecnologías en sistemas de redes van evolucionando al manejo de dispositivos como identidades independientes y autónomas. Dado que los sistemas de seguridad están representados por una comunidad de dispositivos conectados entre sí y que requieren de un intercambio de servicios, estos sistemas no están exentos de estos cambios.

En la actualidad los sistemas de seguridad requieren de un largo proceso de integración de servicios adicionales; es decir para que la comunidad reconozca a un nuevo dispositivo en la red se deberá ejecutar una configuración compleja.

Un sistema de seguridad debe integrarse a su medio ambiente tanto exterior como interior para producir el mínimo impacto, además de aprovechar todos los sistemas pasivos de climatización, ventilación e iluminación en forma natural y/o complementándose con sistemas electromecánicos eficientes. En la concepción del diseño es necesario considerar el sitio y el entorno, la localización, orientación, forma y diseño de las estructuras; el tipo de materiales constructivos y acabados

Por otra parte en necesario considerar los requerimientos de los usuarios, que van desde su actividad hasta el uso del espacio, rangos de comodidad, niveles adecuados de iluminación control de ruido y ambientación.

Por tanto el objetivo de este solucionar este problema, mediante una red de cámaras web en cada unidad móvil, monitoreadas por medio de Internet y en tiempo real, llevando a cabo los siguientes objetivos. Nuestro proyecto consiste en implementar un servicio de monitoreo mediante Internet, el cual nos proporcione la facultad de desplazarnos con un móvil a través del ambiente o evento que estemos monitoreando, ver figura 1.1.1

En este caso con el término monitoreo, nos referimos a grabar o tomar vídeo y cuando decimos por Internet, estamos hablando que este vídeo tomado, será enviado o transmitido por este medio de comunicación; ya sea a uno o varios usuarios.

Por otra parte no sólo transmitiremos vídeo por Internet a un usuario determinado, si no que también este usuario será capaz de mover o manipular el estado de la cámara que esté monitoreando. Todo el servicio será consultado en una página web.

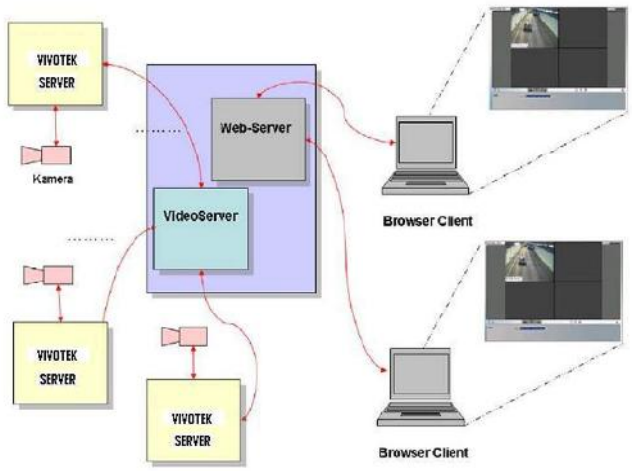


Figura 1.1 Componentes del sistema Vivotek

Todo lo anterior se puede ver en la figura 1.1 la cual es un diagrama general, en el cual se muestran los bloques que compone esta tesis.

Los requisitos recomendados del sistema para esta aplicación son los siguientes.

Sistema operativo:	MS Windows 2000/XP/98SE/Me
CPU:	Intel Pentium IV a 2,0 GHz o superior y AMD Athlon o superior
SDRAM:	512 MB SDRAM o superior para 16 canales 256 MB SDRAM para 9 canales
Disco duro:	40 GB
Tarjeta de vídeo:	nVidia, serie GeForce con memoria de vídeo de 32 MB ATI, serie Radeon con memoria de vídeo de 32 MB

Tabla 1.1.1 Requisitos recomendados de hardware del sistema

1.1.2 Bloques del Esquema General.

Como se mostró en el diagrama de la figura 1.1, tenemos varios bloques donde cada uno de los cuales representa un problema a solucionar o a cubrir. A continuación se enlistarán cada uno de los bloques describiendo a detalle lo que se tiene que hacer para cubrir los problemas planteados.

1.1.3. Bloque de Presentación.

En este bloque se hace referencia entre los servidores (CPU) y una página web donde se brindara el servicio de Administrador-usuario para el configuración y control de las cámaras.

Esta parte es fundamental, se podría decir que es la columna que sostiene la tesis, debido a que si el servidor falla, todo se viene abajo y no sólo nos referimos a que éste falle, sino que también si hacemos una mala instalación de este mismo, no tendría un desempeño adecuado.

1.1.4 Bloque de Servicio De Control.

Esta es una de las capas más complicadas a desarrollar, debido a que es la interfaz entre el servidor y el dispositivo móvil, es decir, en esta capa nos vamos a preocupar por programar y diseñar todo lo necesario para que las señales o instrucciones que la PC o servidor, mande por el puerto paralelo, sean bien recibidas y ejecutadas por el móvil.

Cabe mencionar, que la conectividad será inalámbrica por lo que se empleará un módulo transmisor de la señal de Internet (Tarjeta de Internet Inalámbrica) y receptor (software Vivotek, ver figura 1.1.2), Para lograr cubrir este bloque tenemos que:

1. Armar la interfaz entre la PC y el transmisor, de tal forma que los datos que mande la PC por el puerto paralelo sean enviados por el transmisor.

2. Armar el módulo receptor, el cual consistirá de un receptor, el cual ejecutará las instrucciones recibidas por el transmisor.

Figura 1.1.2 Tarjeta de Internet Inalámbrica

1.1.5 Bloque de Captura de Video.

En esta parte del proyecto nos enfocaremos a revisar algunos conceptos importantes sobre el vídeo streamig, que es el método que emplearemos para transmitir el vídeo. También revisaremos la arquitectura de los sistemas de vídeo streaming así como los protocolos con los cuales trabaja. Por último concluiremos cuál es el mejor software que se adapte mejor a nuestras necesidades.

El punto a resolver en esta etapa es precisamente elegir el software para vídeo streaming en base al análisis de los conceptos antes mencionados.

Los puntos anteriores se verán más a fondo en los siguientes capítulos que corresponden a la parte del desarrollo del proyecto. La finalidad de los puntos anteriores fue la de tener un panorama general del proyecto y de los puntos que se tienen que cubrir para hacerlo tangible.

1.1.6 Móvil y cámara.

En este bloque escogeremos el tipo de cámara y el tipo de móvil que vayamos a utilizar, este punto tiene una cierta flexibilidad, ya que en realidad el móvil y la cámara serán elegidos de acuerdo a una necesidad específica. En los capítulos posteriores describiremos distintos tipos de cámara que podrían ser útiles para cubrir determinados eventos, de la misma forma propondremos prototipos de distintos tipos de móviles que pueden cubrir distintos tipos de necesidades, de acuerdo al evento o lugar donde se necesite el monitoreo.

Para culminar, daremos a conocer el tipo de cámara y móvil que vamos a utilizar. Decidimos hacerlo de esta manera, porque conocer el tipo de móvil y el peso de la cámara son factores importantes que hay que conocer, principalmente en la fase de control del móvil y la etapa de potencia de este mismo. Ya que no es lo mismo controlar un móvil de una rueda que controlar un brazo mecánico.

1.1.7 Alcance del proyecto.

En esta tesis se demostrara la etapa de implementación del sistema, es decir, que no sólo tocaremos los puntos teóricos sino que queremos llegar a la parte práctica y experimental. En el punto anterior mencionamos que queríamos este proyecto para ocuparlo en nuestras casas, pero nuestro

sistema tiene un mayor alcance ya que se podría implementar en varios lugares como:

• Empresas: Para la supervisión de empleados o de la empresa en general y para seguridad.

• Escuelas: Los padres podrán ver a sus hijos, esto especialmente en guarderías, preescolar aunque también podría emplearse en primarias y hasta secundarias. Además de que tendrán la posibilidad de ver como los maestros dan las clases lográndose así una mejor retroalimentación entre directivos de la escuela y padres. Sería de gran utilidad, si por algún motivo el usuario no puede llegar a clase, la podría tomar por Internet.

• Centros de recreación: Para promocionar centros vacacionales, museos, exposiciones, etc.

• Calles de unidades habitacionales: actualmente en la zona metropolitana y algunos municipios del Estado de México, han hecho grandes cantidades de unidades habitacionales, este tipo de construcciones nos ofrecen la ventaja de que una área relativamente pequeña se aglomeran varias casas, por lo que sería relativamente sencillo instalar una o varias redes LAN donde los vecinos podrían monitorear sus calles con nuestro sistema por motivos de seguridad.

Los puntos anteriores muestran sólo algunos ejemplos en donde nuestro proyecto podría ser usado, es decir, hasta donde podría llegar nuestro sistema, en otras palabras el alcance que el sistema tendría. Para el caso de esta tesis sólo nos enfocaremos a diseñar e implementar el sistema en nuestros hogares o en la escuela para demostrar su funcionamiento.

La mayoría de empresas de seguridad prestan varios tipos de servicios tecnológicos, entre los cuales se tiene:

Alarmas de intrusión: aquellas que detectan intrusiones en un área específica y activan la alarma sonora.

Alarmas técnicas: un ejemplo de este tipo de alarmas son aquellas que se utilizan para detectar humo.

Alarmas personales: aquellas que sirven para monitoreo y seguimiento de un individuo, algunos incluyen cobertura médica.

Sistemas de video-vigilancia: también conocidos como circuito cerrado de televisión.

1.2 Necesidades.

En México se desarrolla muy poca tecnología ya que se compra la mayoría de ella en el extranjero, actualmente los países desarrollados son los que cuentan con sistemas de vigilancia muy avanzados y son más comunes verlos, no sólo se emplean en las empresas sino ya es usual ver aplicados estos sistemas en casas. En nuestro país no es muy común ver a casas con un avanzado sistema de seguridad sólo cuentan algunas empresas con ello.

Lo que se propone es no enfocar solamente esta tesis a nivel industrial sino al público en general planteando una nueva solución contra la inseguridad que se vive actualmente.

Un buen sistema de monitoreo no sólo debe hacer sonar una sirena; también debe mantener constantemente informado al usuario de todo lo que sucede en el lugar de origen del centro de monitoreo por medio del recurso de video y audio que es controlado Vía Internet en tiempo real.

1.3 Aplicaciones.

Con el incremento del volumen de datos, nuevas líneas de investigación, desarrollo tecnológico y competencia corporativa, muchas compañías se están percatando de que se necesita, no sólo proteger su información, sino también sus recursos humanos e infraestructuras que están al servicio de la compañía.

Los sistemas de televisión de circuito cerrado (CCTV) y los de vigilancia por video se están volviendo más comunes en los edificios de oficinas, estructuras externas, escuelas e incluso en las calles. La vigilancia se ha convertido en un componente integral de los métodos de control de acceso enriquecidos con biométricos y sistemas de rastreo. Este nuevo sistema de video permite transmisiones IP (Internet Protocol) de las señales de video a los dispositivos direccionales IP y pueden transmitirse en combinación con secuencias de voz y/o video.

Estas transmisiones pueden almacenarse o simplemente visualizarse en tiempo real. Se cubren los principios y evoluciones de estas tecnologías orientadas hacia las soluciones más novedosas en tecnologías de video digital IP juntamente con información importante acerca de necesidades de infraestructura y requisitos para su implementación. El sistema de cableado estructurado pueden soportar, no sólo el tráfico de red, sino también las necesidades de transmisión de video ya que es la infraestructura más robusta disponible actualmente en el mercado.

La característica plug and play permite instalar las cámaras direccionales IP en cualquier lugar dentro de la infraestructura. Los equipos electrónicos que manejan actualmente tráfico IP se han vuelto parte integrada de los sistemas de vigilancia. Ya que los videos se almacenan en formato digital (JPEG o MPEG), pueden ser vistos desde cualquier lugar de la red bajo nuevos parámetros de seguridad para los archivos administrados como parte de las políticas de seguridad de la red. Además, éstos pueden ser visualizados simultáneamente desde varios puntos de la red a través de una PC predeterminada para el control de las cámaras IP desde un centro de monitoreo. No sólo es fácil de implementar, sino también es extremadamente versátil. Las redes no se sobrecargan con otro protocolo. Las transmisiones son "nativas" en la infraestructura actual, eliminando la necesidad de sistemas de cableado separados.

CAPÍTULO 2.

Camara IP y sus Caracteristicas.

2.1 Móviles propuestos.

Un móvil puede ser tan sofisticado y por ende tan complicado como se quiera o se pueda llegar. Por ejemplo hay móviles que se mueven sobre el agua, que vuelan, submarinos, etc. Que pueden ser utilizados en casos y en ambientes muy específicos. En los siguientes puntos mostraremos algunos móviles que podrían ser útiles en ambientes un poco más comunes, como un salón de clases, un pasillo, un centro recreativo, un parque, etcétera.

Por último indicaremos el móvil que se empleará en el proyecto en cuestión.

2.1.1 Giratorio 360°.

Este tipo de móvil es ideal para cubrir eventos que sucedan en áreas relativamente pequeñas, donde el alcance visual de la cámara pueda cubrir la mayor parte del área. Un ejemplo sería un salón de clases, un salón de fiestas, la habitación de algún hogar. Se propone colocar este móvil en el techo para abarcar una mayor área, ver figura 2.1.

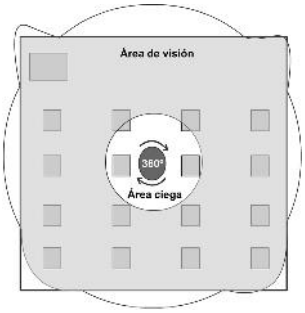


Figura 2.1. Vista aérea del área que cubriría la cámara.

En la figura 2.1, podemos ver que al montar este tipo de movimiento a la cámara. Existe un área ciega, que depende de la inclinación con la que esté montada la cámara y con el ángulo de visión de esta misma, ver figura 2.2.

Una solución para eliminar el área ciega, sería la de agregar un movimiento que nos permita manipular la inclinación de la cámara, como se puede observar en la figura 2.3. Con lo anterior tenemos una visión completa del recinto.

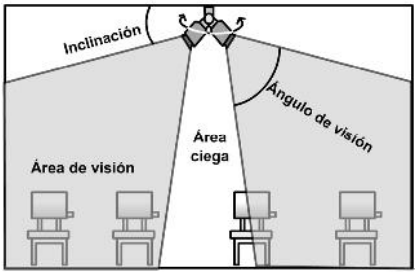


Figura 2.2. Inclinación y ángulo de visión de la cámara.

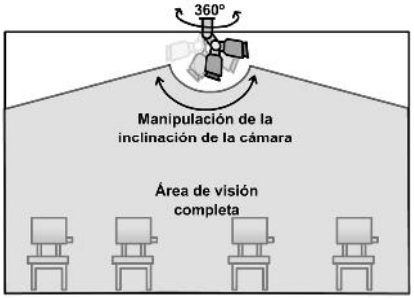


Figura 2.3 Movimiento adicional para eliminar el área ciega.

2.1.2 Con riel como guía.

Con este móvil se podría optimizar el uso de la cámara para cubrir ambientes que tengan un área larga y angosta, como es el caso de pasillos, andenes de metro, campos donde se practique algún deporte, etc. La ventaja de este diseño es que no se necesitarían varias cámaras para cubrir el área mencionada, sino que con una sola cámara y este móvil sería suficiente (ver figura 2.4).

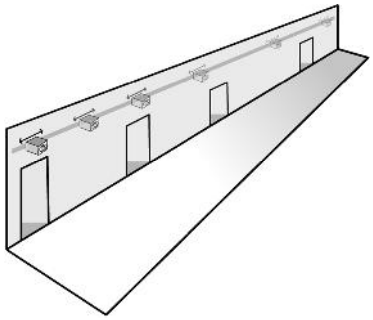


Figura 2.4 Cámara moviéndose a través del riel

2.1.3 Análisis de los costos.

La evaluación desde el punto de vista económico de este proyecto analiza la factibilidad y rentabilidad para instalar este sistema de vídeo vigilancia. El propósito de realizar un análisis de los costos del proyecto es que el usuario tenga conocimiento de la inversión que se requiere para implementar este sistema de seguridad, ver Tabla 1.

A continuación se mencionarán los costos que se requieren cubrir para llevar a cabo el sistema de seguridad en un área.

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

Tabla 1. Análisis económico del hardware para la implementación del proyecto

***Nota:** La unidad monetaria se ve reflejada en la Moneda Nacional de México (Pesos Mexicanos), y los costos son cotizados hasta el mes de Septiembre del 2010.

2.1.4 Tabla Comparativa de Distintas Cámaras propuestas.

La principal diferencia entre estos dos sistemas de vigilancia, IP y analógico, se da en el procesamiento de las imágenes obtenidas por las cámaras de video vigilancia.

En un sistema de vigilancia con cámaras analógicas y videograbador digital la carga de trabajo se sitúa en el videograbador. Las cámaras analógicas únicamente capturan las imágenes y las envían al videograbador, el cual tiene que realizar todo el proceso de digitalización, compresión, almacenamiento, y, muchas veces también el análisis de dichas imágenes. Añadir una cámara en estos sistemas implicaría aumentar carga de trabajo al procesador del videograbador disminuyendo su rendimiento.

Por el contrario, en un sistema de vigilancia con cámaras IP y videograbador IP esta sobrecarga de trabajo no se produce ya que son las propias cámaras las que digitalizan, comprimen y transmiten las imágenes. Esto hace posible añadir una o más cámaras sin afectar significativamente la carga de procesamiento del videograbador.

Por otro lado, las cámaras de video IP permiten el control de la velocidad de imagen, lo que significa que la cámara de video puede enviar imágenes a una velocidad configurada previamente, a diferencia del video analógico donde todo el vídeo se transmite desde la cámara de forma permanente, ver Tabla 2.

En cámaras analógicas la transmisión de la señal de audio, en el caso que la cámara incorpore esta funcionalidad, se la realiza a través de un medio de transmisión distinto al que lleva la señal de video, requiriendo cableado adicional para la transmisión del mismo.

Con cámaras IP la señal de audio puede integrarse fácilmente con la señal de video, ya que una red IP transporta cualquier tipo de datos. El audio también puede utilizarse en cámaras o servidores IP como un método de detección independiente, por ejemplo, para activar las grabaciones de vídeo y alarmas cuando se detectan niveles de audio por encima de un determinado umbral.

Con cámaras IP es posible la alimentación eléctrica a través de Ethernet (PoE o Power Over Ethernet), lo cual permite que la alimentación eléctrica se suministre al dispositivo usando el mismo cable que se utiliza para la conexión de red. Esto elimina la necesidad de utilizar tomas de corriente en las ubicaciones de la cámara, y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

	AXIS 231	DOMO IP	myDOME240	S2565NXW	N-CC2564
Sensor	¼"	¼"	¼"	¼"	¼"
L. focal	3.4 – 119	3.4 - 78	23x óptico	30x óptico	3.6 – 82.8
Resolución	480 líneas	480 líneas	480 líneas	480 líneas	480 líneas
Iluminación	0.08 lux	0.1 lux	0.1 lux	0.07 lux	0.03 lux
Presets	100	64	165	128	255
Compresión	MPEG - 4	MPEG - 4	MPEG - 4	H.264	MPEG - 4
Protección	66	65	66	66	66
Precio	1931	1546	1250	1100	1580

Tabla 2 Tabla comparativa de video cámaras (Características y/o propiedades).

***Nota:** La unidad monetaria se ve reflejada en la Moneda Nacional de México (Pesos Mexicanos), y los costos son cotizados hasta el mes de Septiembre del 2010.

2.2 Tipos de cámaras en el mercado.

El mercado de la tecnología es un campo muy diverso, en el cual se puede encontrar una amplia gama de equipos con diferentes características técnicas y precios. En el presente capítulo se analizará el espectro de equipos que existen en el mercado, que cumplan con los requerimientos obtenidos en el capítulo anterior, presentando su precio en el mercado y sus características relevantes. Los equipos a analizar en el presente capítulo son:

- Cámaras de vigilancia

- Servidores de procesamiento y almacenamiento de video

El resto de equipos son complementarios, pero no menos importantes, a los anteriormente citados, motivo por el cual, estos serán seleccionados en el desarrollo del diseño del sistema de seguridad.

2.2.1 Cámaras Web.

La primera cámara Web fue construida en los laboratorios de informática de la Universidad de Cambridge en 1991. Es una cámara sencilla y por lo regular bastante económica, fue diseñada especialmente para transmitir videos por Internet.

Este tipo de cámaras, en un principio, no contaban con una gran resolución, debido a que entre más resolución tuviera el video, era más grande la cantidad de flujo de datos a transmitir por lo que se necesitaba más ancho de banda para transmitir, con lo cual en ese momento muchas personas no contaban.

Ahora en varios países y México no es la excepción, existen una gran cantidad de usuarios que cuentan con servicio de banda ancha que va desde los 256Kbps hasta los 2 Mbps. Con esta consideración, las cámaras web han evolucionado y ahora tienen mejores resoluciones.

En general, este tipo de cámara podría considerarse estándar para cubrir casi cualquier evento. Por ejemplo para monitorear escuelas, hogares, calles, etc. A continuación se muestra una cámara Web que está disponible en el mercado (ver figura 2.5).

Figura 2.5 Cámara Web

2.2 2 Cámaras IP.

Las cámaras IP a diferencia de las cámaras web son más sofisticadas, ya que éstas no necesitan de una computadora para transmitir video. Los equipos escogidos son la estructura del sistema de seguridad de los cuales dependerá la elección del resto de equipos de cómputo y del diseño de todo el sistema de seguridad. La tendencia actual es que hay un crecimiento en las inalámbricas, esto debido al gran crecimiento de las redes inalámbricas.

Estas cámaras son de fácil instalación y representan una buena solución para transmitir video y al igual que las cámaras web, pueden cubrir casi cualquier evento.

Podríamos utilizar este tipo de cámaras en la implementación de este proyecto, pero iríamos en contra de los objetivos de éste mismo ya que como se planteó en un principio, la idea es instalar el servicio a partir de computadoras que ya se tenían, además que este tipo de cámaras son muy caras y en general, no almacenan lo que capturan, en dado caso, cuando traen esta función, como es de suponerse su costo se incrementa. Ahora se muestra un modelo de cámara que se encuentra en el mercado (ver figura 2.6).

Figura 2.6 Cámara IP

2.2.3 Telescópicas.

Para aplicaciones más específicas como observaciones astronómicas y la vigilancia en campos abiertos, las cámaras telescópicas son la solución. Una cámara telescópica no es más que una cámara y un telescopio unidos en un solo sistema, que da como resultado una cámara con un gran alcance. El sistema implementado podría ser una atracción llamativa en páginas web de planetarios, donde el usuario podría explorar el manto celeste desde la comodidad de su escritorio.

Estas cámaras también tienen un costo elevado pero debido a sus características, con adquirir una cámara sería más que suficiente para tener una buena implementación. Un modelo de cámara telescópica se muestra a continuación (ver figura 2.7).

Figura 2.7 Cámara telescópica

2.2.4 Tabla Comparativa de Cámaras.

En la tabla anterior se exponen algunos puntos relevantes que exponen y justifican de distinta manera, como cada una de estas cámaras podrían adecuarse a este proyecto, se puede apreciar que algo muy decisivo es el costo de dicho dispositivo, así como su mantenimiento que también se traduce en gastos económicos, que para algunos usuarios no podrían costear, sin mencionar que la instalación mientras mas sencilla sea también no se pueden incurrir en gastos innecesarios en técnicos o personal que se necesite de su auxilio y siendo esto mas sencillo el mismo usuario podría hacerlo, el factor inalámbrico es relevante en este proyecto, ya que es un sistema móvil, de esta manera el dispositivo no esta atado a un medio físico que puede ser una limitante en una cámara que sea alámbrica y considerando las dimensiones de dicha cámara es determinante para el diseño de los circuitos de potencia que mientras mas peso sostenga el móvil, mas voltaje consume, y eso al fin y al cabo se traduce en gastos económicos en suministros de baterías.

Se debe mencionar que si se desea adquirir una cámara IP se deben considerar que el simple costo de una cámara IP es elevado, se eleva más si esta es inalámbrica y hay un gasto mayor por la renta de la dirección IP.

	ETHIRIS	LUXRIOT	Zone MINDER	DiBos	NR7401	3TB RAID5
Formato	M-PEG4	M-PEG4 h.261	MJPEG-4 JPEG	M-PEG4	M-PEG4	MPEG4
Cámaras	16	20	Limitado por hardware	Hasta 32	9	64
Capacidad	Limitado por hardware	Limitado por hardware	Limitado por hardware	1600GB	750GB	3TB
Capacidad expandible	si	si	si	no	no	si
S.O.	Windows	Windows	Linux	Windows	Windows	Linux
Precio	2300	1500	Donación voluntaria	10,172	759	5171,28

Tabla 3 Tabla comparativa de Cámaras

***Nota:** La unidad monetaria se ve reflejada en la Moneda Nacional de México (Pesos Mexicanos), y los costos son cotizados hasta el mes de Septiembre del 2010.

Un punto a favor de este programa es el precio y el sistema operativo que usa. No debería presentar problemas de compatibilidad con otras aplicaciones como pasa con Linux, pues muchas aplicaciones no funcionan bajo ese entorno. Un punto a favor de los NRV basados en PC es que un equipo de buenas características en la actualidad se puede conseguir a precios cada vez más asequibles.

2.2.5 Cámara a emplear en este proyecto.

Para este proyecto se empleará una cámara conocida como mini cámara o cámara espía. Se eligió este tipo de cámara ya que necesitamos una cámara ligera y que también sea pequeña, ya que como se vio en el punto 2.1.3 utilizaremos un móvil con doble tracción trasera, lo que como veremos en puntos posteriores, se traduce en que necesitaremos dos motores.

Los cuales consumen corriente y entre más peso se les cargue, más corriente consumen, lo que nos da como resultado un mayor consumo de energía.

Lo anterior nos representa un problema, porque como ya vimos anteriormente el móvil será inalámbrico, entonces utilizará baterías. Además de que independientemente de que se esté

buscando una mayor duración de las baterías, siempre se debe de buscar consumir la menor energía posible. He aquí la importancia en este proyecto de primero elegir en primera instancia, lo que se va a mover y cómo se va a mover.

La cámara que empleamos en específico, es inalámbrica de 2.4 GHz de marca LLOYD'S modelo CA-1035. A continuación mostramos algunas de sus características principales:

Cámara	
Sensor de Imagen	0.847 cm CMOS
Total de Píxeles	628 x 582 (pixeles) 510 x 492 (pixeles)
Resolución Horizontal	380 Líneas
Vista de ángulo	60°
Iluminación Mínima	1 Lux
Control de Video	Automático
Frecuencia (MHz)	ISM 2400 a 2483 en 4 canales
Transmisión de energía	10 mW
Modo de Modulación	FM
Ancho de Banda	18 MHz
Alimentación de Energía	8 Volts
Consumo de corriente	80 mA
Rango Efectivo de Señal	100 metros (libres de obstáculos)

Receptor	
Recepción de Frecuencia (MHz)	2400 a 2483 en 4 canales
Frecuencia Inmediata	480 MHz
Desmodulación	FM
Alimentación de Energía	8 Volts
Consumo de Corriente	200 mA

Tabla 4 Especificaciones de Cámara LLOYD'S modelo CA-1035

CAPÍTULO 3

Caracteristicas del servicio al usuario.

En este capítulo hablaremos todo lo relacionado con el uso de la página web que prestará servicio al usuario; haciendo la aclaración de que se utilizara el mismo recurso que nos proporciona el software de las cámaras IP (Vivotek).

Actualmente esta aplicación es de los más sofisticados que permiten implementar aplicaciones más potentes, como páginas interactivas, animaciones, transmisión de video, etc.

3.1 Protocolo TCP/IP.

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas UNIX. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP/IP.

El nombre TCP/IP Proviene de dos protocolos importantes, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

El TCP/IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes LAN y WAN (Wide Area Network; red local del Servidor al cual se realiza la conectividad entre Internet y las Cámaras IP).

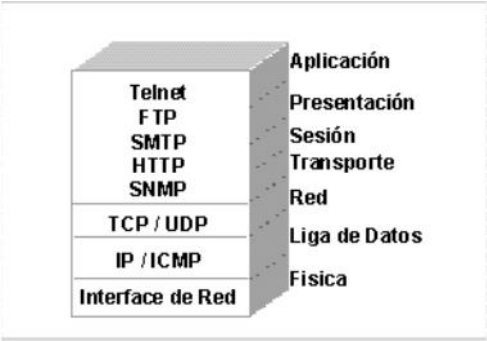
En términos generales, el software TCP/IP está organizado en cuatro capas conceptuales que se construyen sobre una quinta capa de hardware.

El número IP es la dirección lógica que identifica a tu ordenador en una red (ya sea local o externa). Esta dirección es única para cada equipo en el mundo o única dentro de cada red local- y la llamamos dirección lógica porque solamente con conocer el IP, cualquier enrutador es capaz de dirigir los datos al ordenador de destino (o a otro enrutador que probablemente sea capaz de enviar los datos al ordenador de destino.

Ya se ha comentado que el flujo de bytes que produce una determinada aplicación se divide en uno o más segmentos TCP para su transmisión. Cada uno de estos segmentos viaja en el campo de datos de un datagrama IP. Para facilitar el control de flujo de la información los bytes de la aplicación se numeran. De esta manera, cada segmento indica en su cabecera el primer byte que transporta.

Las confirmaciones o acuses de recibo (ACK) representan el siguiente byte que se espera recibir (y no el número de segmento recibido, ya que éste no existe). El formato de TCP

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



3.1.2 Modelo de capas de TCP/IP

El Protocolo IP proporciona un sistema de distribución que es muy confiable incluso en una base solida. El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP/IP es el datagrama.

Es la responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la maquina origen (esto lo hace el protocolo ICMP). El protocolo IP también define cual será la ruta inicial por la que serán mandados los datos.

3.2 ActiveX.

Es el nombre que Microsoft ha dado a un grupo de tecnologías y herramientas orientadas a objetos, tiempo atrás el contenido de las páginas web era estático (textos e imágenes en dos dimensiones), por lo que fue desarrollada con vistas a implementar páginas net (Internet e Intranet) más interactivas, permitiendo a su vez el desarrollo web de manera más fácil y rápida. Con ActiveX, se tiene la facilidad de crear aplicaciones web con contenido interactivo (efectos multimedia, objetos animados, entre otros).

La tecnología ActiveX está fundamentada en otras que igualmente son propias de Microsoft, como lo son Component Object Model (COM) y Object Linkink Embedding (OLE); la idea básica de estas tecnologías es diseñar aplicaciones capaces de intercambiar y compartir código de forma que sean accesibles una desde dentro de otra.

ActiveX solo puede ser ejecutado de manera directa utilizando el Internet Explorer de Microsoft, sin embargo existe un Plugin de ActiveX en la web con el cual es posible ejecutar dicha tecnología desde el Netscape Navigator.

Active-X es una tecnología desarrollada por Microsoft que apareció por primera vez con la salida de Internet Explorer 3.0.

Lenguaje desarrollado por Microsoft para la elaboración de aplicaciones exportables a la red y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores WWW. Permite dar dinamismo a las páginas web.

El objetivo de esta tecnología es el de insertar objetos de diferente tipo en una página web y no sólo se limita a eso, sino que esta tecnología nos da la posibilidad de tener interacción y comunicación con programas externos. Existen páginas que la mayoría de su contenido (si no es que todo) está formado por Active-X.

Los controles Active-X guardan un gran parecido con los Applets de Java y los plugins pero Active-X al ser de tecnología auto contenida presenta ventajas ante éstos.

La ventaja más importante es que Active-X no necesita de la instalación de algún programa en el navegador para cada objeto, como es el caso de los Plugs, sino que cada objeto tiene la suficiente información para ejecutarse a sí mismo sin la ayuda de alguna otra aplicación.

En la página de servicio al usuario, usaremos esta tecnología para insertar un objeto de Windows Media Player como se puede observar en la Figura 3.1

Figura 3.1. Ventana del reproductor de Windows, incrustada en la página Web.

Cabe mencionar que para que se visualice el reproductor en la página HTML, el usuario debe de tener instalado Windows Media Player lo que es muy común en la mayoría de las PC's.

A continuación se mencionará un panorama general de la capa de servicio de control, que es la capa de comunicación y manipulación del servidor con el móvil, en el desarrollo de este capítulo se explicarán todos los elementos involucrados tanto en hardware como en software para el control por el puerto paralelo, el cual se dará una breve descripción del mismo, así como los elementos finales de la parte del hardware que están involucrados, desde los circuitos de potencia de los motores como el uso de el micro controlador y el diseño de control mediante los bits de control interpretados por el mismo micro controlador, para dar acciones a los motores y el uso del circuito driver para la etapa de potencia de los motores.

Normalmente los dispositivos anteriores se tienen conectados, sin mencionar que todavía le vamos a conectar la cámara, entonces tendríamos demasiados dispositivos saturando los puertos USB, por eso es que decidimos implementar el control del móvil con el puerto paralelo.

Las aplicaciones ActiveX están conceptualmente divididas en servidores, hacen que sus métodos y propiedades estén disponibles para los demás (recibe peticiones del cliente, ejecuta las operaciones pertinentes y devuelve los datos procesados) y clientes, aplicaciones que usan objetos de servidor expuestos, métodos y propiedades (estación de trabajo que accede a los datos de una aplicación servidora y gestiona su información de datos como si fuera propia). ActiveX se compone de elementos con presencia en el lado del servidor web como del lado del cliente:

- Controles ActiveX. Son objetos interactivos en una página web que provee funciones controlables por el usuario y forman parte de la tercera versión de los controles OLE, los controles OCX, permitiendo a los desarrolladores integrar un ambiente de desarrollo de vanguardia y construir aplicaciones web capaces de interactuar de forma dinámica con otros servicios y componentes COM, brindando gran funcionalidad y versatilidad a los usuarios. Son pequeños módulos de programas construidos en cualquier lenguaje de programación y compilados en un lenguaje compatible con la tecnología COM, como son Visual Basic, Microsoft C++, Power Builder, VBScript, entre otros, y una vez compilados están listos para ser incluidos en aplicaciones finales.

- Documentos ActiveX. Estos permiten a los usuarios ver documentos no HTML, como documentos de Microsoft Excel (.xls), Word (.doc), .pdf, etc., a través del navegador de Internet.

- Script de ActiveX. Controla el comportamiento de varios controles ActiveX en conjunto y/u otros Applets de Java desde el navegador.

- ActiveX Server Framework. Ofrece funciones de seguridad, acceso a base de datos y otras.

- Máquina Virtual de Java. Permite al navegador ejecutar applets de Java e integrarlos con controles ActiveX.

- Autonomía Propia. Son capaces de definir cuando empieza o termina su ejecución. Cada objeto tiene suficiente información para ejecutarse él mismo sin ayuda de ninguna aplicación.

- Compatibilidad. El módulo generado (control) tiene la capacidad de interactuar con otros módulos ActiveX y/o programas ejecutables. Recibe entrada de ellos y envía salida de datos hacia ellos.

- Reutilización. Un mismo control ActiveX puede ser utilizado por varias aplicaciones clientes.

- Actualización. Esta ser transparente para las aplicaciones que utilizan el control, debe existir compatibilidad con versiones anteriores, de forma que las mejoras no afecten el método de acceder a la información ni la manera como la devuelve a los clientes, sino la forma de procesar la misma.

- Certificación. Para poder usar cualquier control ActiveX, éste debe estar oficialmente certificados por Microsoft (Authenticode) o mediante algún método de autentificación.

- Manejo de Propiedades, Métodos, Eventos y Funciones. Estos poseen propiedades, eventos y métodos de acceso particulares a cada control. El objeto contiene también funciones para manipular sus datos.

- Facilidad de Construcción. Un objeto ActiveX está aplicado como código binario, por consiguiente, puede estar escrito en cualquier lenguaje fuente.

- Encapsulamiento. El objeto está encapsulado en un archivo ejecutable o en una biblioteca de vínculo dinámico.

Ventajas y Desventajas.

- Un objeto ActiveX está aplicado como código binario, por consiguiente, puede estar escrito en cualquier lenguaje fuente.

- Una de las principales ventajas de los controles ActiveX, es que además de poder ser reutilizado por varias aplicaciones, a las que se les conoce como contenedores de componentes, existen en el mercado más de 1000 controles disponibles para los desarrolladores de sitios web.

- ActiveX provee un mecanismo estándar para extender cualquier lenguaje de programación, incluyendo Java, permitiendo a los programadores de este lenguaje integrar sus applets con lo útil de ActiveX. ActiveX une los applets con objetos creados en otros lenguajes, de manera que estos puedan hacer referencia a un componente ActiveX desde el programa.

3.3 Comunicación inalámbrica.

El objetivo es que las Cámaras IP sean controladas de manera inalámbrica vía Internet a través del software que nos proporciona el proveedor del servicio de Vivotek; así mismo tendrá más libertad de movimiento y alcance por medio de la opción de zoom.

Se realiza una búsqueda para ver los dispositivos que se adecuarán a nuestras necesidades, y se encontró un paquete que incluye todo lo necesario para cumplir nuestro objetivo, dicho paquete contiene los módulos de transmisión y recepción que incluyen el dispositivo transmisor y receptor con sus respectivos codificadores y decodificadores. Estos dispositivos son capaces de enviar y recibir señales que contienen los datos que el usuario quiera transmitir con un tamaño de 4 bits.

La comunicación inalámbrica (inglés wireless, sin cables) es el tipo de comunicación en la que no se utiliza un medio de propagación físico alguno esto quiere decir que se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión. En ese sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, como por ejemplo: Antenas, Laptops, PDAs, Teléfonos, Teléfonos Celulares, etc.

En general, la tecnología inalámbrica utiliza ondas de radiofrecuencia de baja potencia y una banda específica, de uso libre para transmitir, entre dispositivos.

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

Una forma de entender la comunicación inalámbrica es primero conocer el significado de la palabra "telecomunicación". De la palabra griega "tele" que significa "lejos", telecomunicaciones es el intercambio de información entre dos puntos a diferente distancia. Por lo que comunicación inalámbrica se obtiene usando ondas electromagnéticas en lugar de alambres para acarrear la información de un punto a otro. "[Comunicación] inalámbrica," Dr. Rappaport nos dice, "te da la movilidad que necesitas para conectarte y comunicarte sin necesidad de alambres."

Cuando pensamos en cualquier cosa que no tenga alambres, generalmente pensamos en los teléfonos celulares. Pero en realidad hay muchos productos que se encuentran ahora que usan comunicaciones inalámbricas. Muchas computadoras portátiles (laptops) ahora ocupan tarjetas inalámbricas que nos permiten conectarnos a la Internet desde cualquier lugar. Otros productos incluyen tableros de computadoras inalámbricos, audífonos, así como los tableros virtuales. "El control para abrir el garage y cualquier tipo de control remoto también usan comunicaciones inalámbricas,"

¿Por qué es la comunicación inalámbrica tan importante? porque "la gran demanda por tener el acceso a la Internet disponible inmediatamente va ha crear una gran demanda en la industria de comunicaciones inalámbricas…" Imagínate ser capaz de conectarte a la Internet en cualquier lugar a cualquier hora, por ejemplo mientras vas en el autobús ó cuando estás comiendo. Sin embargo, hay varios obstáculos mayores cuando estas manejando las comunicaciones inalámbricas. Primero, la tecnología inalámbrica es mucho más lenta que cualquier tipo de tecnología que ocupa alambres.

Siete errores comunes que se deben evitar.

Tras la evaluar sistemas de videoconferencia fallidos se han detectado siete errores más comunes que suelen cometer las empresas al desplegar sus sistemas de videoconferencia:

Evaluación: Error al evaluar la disposición previa de la red para la videoconferencia.

Provisión de ancho de banda: Error al aprovisionar el ancho de banda adecuado para cada sesión de videoconferencia.

Monitorización proactiva: Incapacidad para monitorizar proactivamente la calidad de cada sesión de videoconferencia.

Resolución de problemas: Incapacidad de resolver problemas de calidad durante una sesión de videoconferencia.

Establecimiento de sesión desprotegido: La falta de ancho de banda para las transacciones de establecimiento causan importantes retrasos al iniciar una nueva sesión de videoconferencia.

Limitaciones de la infraestructura previa: La confianza en que la infraestructura de red previa puede proporcionar la calidad necesaria para la videoconferencia.

Afectar a otras aplicaciones: La mala gestión de las videoconferencias causa un uso excesivo de ancho de banda que afecta al rendimiento de otras aplicaciones.

3.3.1. USB.

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

Algunas cámaras Web están instaladas a grandes distancias de las PC que se encargan del proceso. La única diferencia en este caso es que la imagen no podrá enviarse por cable. Es necesario un equipo transmisor junto a la cámara para convertir la imagen en señal de radio y un equipo receptor junto a la PC, que reconvierte la señal de radio en imagen, tal como normalmente llega un programa desde exteriores a un canal de televisión.

Antecedentes:

- Diseñado como una extensión en la arquitectura estándar del PC y orientado principalmente en la integración de periféricos, que aparecen como un solo puerto en lo que se refiere a utilización de recursos.
- Intel y otros líderes de la industria diseñaron el Bus Universal Serie.
- Dotación a la PC de un bus de alta velocidad.
- CTI (Computer Telephony Integrations; Integración de dispositivos telefónicos
- en los computadores).

Características del puerto USB:

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

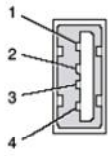


Tabla a. Señal del conector de USB

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

Figura 3.2 Diagrama de especificaciones del USB.

Funcionamiento.

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

A partir de las salidas proporcionadas por los concentradores raíz (generalmente conectores del tipo "A") y utilizando concentradores adicionales, pueden conectarse más dispositivos hasta el límite señalado. La información es enviada en paquetes; cada paquete contiene una cabecera que indica el periférico a que va dirigido.

Existen cuatro tipos de paquetes distintos: Token, Datos, Handshake, y Especial; el máximo de datos por paquete es de 8; 16; 32 y 64 Bytes respectivamente. Se utiliza un sistema de detección y corrección de errores bastante robusto tipo CRC (Cyclical Redundancy Check; Chequeo de Redundancia Cíclica).

El funcionamiento está centrado en el anfitrión, todas las transacciones se originan en él. Es el controlador anfitrión el que decide todas las acciones, incluyendo el número asignado a cada dispositivo (esta asignación es realizada automáticamente por el controlador "anfitrión" cada vez que se inicia el sistema o se añade, o elimina, un nuevo dispositivo en el canal), su ancho de banda, etc.

Cuando se detecta un nuevo dispositivo es el anfitrión el encargado de cargar los controladores oportunos sin necesidad de intervención por el usuario.

Ventajas:

- Es totalmente Plug and Play.
- Es reconocido e instalado de manera inmediata.
- Posee una alta velocidad.
- Permite alimentar dispositivos externos a través de él (5 volts).
- Ya casi toda máquina posee este puerto.
- Conexión más sencilla.
- Conexión en Caliente (Conectar y desconectar sin apagar la máquina).
- Son económicos por lo que un producto no aumenta mucho por el puerto.

Desventajas:

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

CAPÍTULO 4

Administración del servicio.

4.1 Introducción

Antes de meternos a la programación del servidor, es necesario explicar el término servidor en sí, para evitar confusiones más adelante. La palabra servidor se usa en informática para darle el nombre al software que realiza ciertas tareas en nombre de los usuarios.

La cuestión es que el término servidor también se usa para referirse a la computadora física, donde se almacena y se ejecuta el software mencionado anteriormente.

En otras palabras, si tenemos una computadora y le instalamos un software que permita ejecutar funciones de servidor, entonces esta computadora la podemos llamar servidor.

En un servidor se almacenan y ejecutan los archivos de cada sitio de Internet. En Internet existen una gran cantidad de servidores y de una gran variedad, un servidor puede ser desde una computadora personal (PC) hasta una supercomputadora, todo depende del servicio o aplicación que se esté dando.

Cuando nos conectamos a un sitio de Internet, lo que hacemos al ingresar la dirección es hacer una petición al servidor, para que nos envíe las páginas web a nuestra computadora. Lo anterior se puede observar en la siguiente figura 4.1.1.

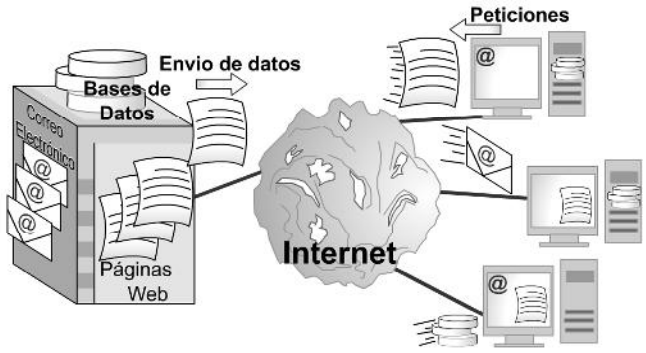


Figura 4.1.1 Comunicación entre el Servidor e Internet.

Existe una gran cantidad de servicios que pueden dar los servidores, a los que la mayoría de la gente tiene acceso, y son:

- Servicio Web.
- Servicio de correo.
- Servicio de base de datos.
- Servicio de vídeos.

4.1.2 Servicios Web.

Un servidor web es un programa que está diseñado para transferir hipertextos, páginas web o páginas HTML (HyperText Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música. El programa implementa el protocolo HTTP (HyperText Transfer Protocol) que pertenece a la capa de aplicación del modelo OSI. El término también se emplea para referirse al ordenador que ejecuta el programa.

Instalar un servidor web en nuestro PC nos permitirá, entre otras cosas, poder montar nuestra propia página web sin necesidad de contratar hosting, probar nuestros desarrollos vía local, acceder a los archivos de nuestro equipo desde un PC remoto (aunque para esto existen otras opciones, como utilizar un servidor FTP) o utilizar alguno de los programas basados en web tan interesantes que están viendo la luz últimamente.

El problema de usar nuestro ordenador como servidor web es que conviene tenerlo conectado a la corriente eléctrica por medio de un regulador de corriente permanentemente; para que esté accesible de forma continua como la mayoría de los sitios webs.

Una forma especial de servidor de correo, es aquel que es accedido vía WEB usando el protocolo http. Es especial, debido a que el protocolo http no es un protocolo definido en los servidores de correo como obligatorio. En este tipo de servidor, el archivo de datos del remitente o destinatario puede ser accedido sin requerir un cliente especifico en el mismo servido se integran programas para acceder a los correos del mismo. Ejemplos típicos de este servicio son: www.hotmail.com, www.yahoo.com, www.gmail.com, etc.

Ventajas de los servicios web.

- Aportan interoperabilidad entre aplicaciones de software independientemente de sus propiedades o de las plataformas sobre las que se instalen.
- Los servicios Web fomentan los estándares y protocolos basados en texto, que hacen más fácil acceder a su contenido y entender su funcionamiento.
- Al apoyarse en HTTP, los servicios Web pueden aprovecharse de los sistemas de seguridad firewall sin necesidad de cambiar las reglas de filtrado.

- Permiten que servicios y software de diferentes compañías ubicadas en diferentes lugares geográficos puedan ser combinados fácilmente para proveer servicios integrados.

- Permiten la interoperabilidad entre plataformas de distintos fabricantes por medio de protocolos estándar y abiertos. Las especificaciones son gestionadas por una organización abierta, la W3C, por tanto no hay secretismos por intereses particulares de fabricantes concretos y se garantiza la plena interoperabilidad entre aplicaciones.

Desventajas de los servicios web.

- No son tan desarrollados para realizar transacciones comparadas a otros sistemas como CORBA (Common Object Request Broker Architecture).

- Su rendimiento es bajo con otro comparado con otros sistemas como CORBA, DCOM o RMI, especialmente por el uso de protocolos y estándares basados en texto.

4.1.3 Servicios de correo.

Un servidor de correo realiza una serie de procesos que tienen la finalidad de transportar información entre los distintos usuarios. Usualmente el envío de un correo electrónico tiene como fin que un usuario (remitente) cree un correo electrónico y lo envíe a otro (destinatario). Esta acción toma típicamente 6 pasos.

1.- El usuario inicial crea un "correo electrónico"; un archivo que cumple lo estándares de un correo electrónico. Usara para ello una aplicación ad-hock. Las aplicaciones más usadas, en indistinto orden son: Outlook Express (Microsoft), Outlook (Microsoft), Mozilla Thuntherbird (Mozilla), Pegasus Mail (David Harris), IBM Lotus Notes (IBM); etc.

2.- El archivo creado es enviado a un almacén; administrado por el servidor de correo local al usuario remitente del correo; donde se genera una solicitud de envío.

3.- El servicio MTA local al usuario inicial recupera este archivo e inicia la negociación con el servidor del destinatario para el envío del mismo.

4.- El servidor del destinatario valida la operación y recibe el correo, depositándolo en el "buzón" correspondiente al usuario receptor del correo. El "buzón" no es otra cosa que un registro en una base de datos.

5.- Finalmente el software del cliente receptor del correo recupera este archivo o "correo" desde el servidor almacenando una copia en la base de datos del programa cliente de correo, ubicada en la computadora del cliente que recibe el correo.

A diferencia de un servicio postal clásico, que recibe un único paquete y lo transporta de un lugar a otro; el servicio de correo electrónico copia varias veces la información que corresponde al correo electrónico.

Este proceso que en la vida real ocurre de manera muy rápida aparte de que involucra el uso de muchos protocolos. Por ejemplo para obtener los mensajes del servidor de correos receptor, los

usuarios se sirven de clientes de correo que utilizan el protocolo POP3 o el protocolo IMAP para recuperar los "correos" del servidor y almacenarlos en sus computadores locales.

Un servidor de correo es una aplicación informática cuya función es parecida al Correo postal solo que en este caso los correos (otras veces llamados mensajes) que circulan, lo hacen a través de nuestras Redes de transmisión de datos y a diferencia del correo postal, por este medio solo se pueden enviar adjuntos de ficheros de cualquier extensión y no bultos o paquetes al viajar la información en formato electrónico.

Seguro o Inseguro.

Si tiene en cuenta el proceso, hay por lo menos una copia del correo en el servidor de envío y otra copia en el servidor de recepción.

Las políticas de funcionamiento de cada servidor, con o sin aviso a los usuarios remitente y/o destinatario, podrían:

1.- No recibir correos de acuerdo a algún parámetro.

2.- Destruir las copias de los correos, por ejemplo a transferirlos satisfactoriamente.

3.- Copiar los correos a algún otro registro o archivo.

4.- Enviar una o más copias a otros destinatarios.

5.- No destruir nunca los correos almacenados.

Es de suma importancia considerar que entidad, institución y funcionario son los responsables de administrar finalmente los servidores de correo que usamos. Los correos pueden en muchos casos ser fuente de invasión a la privacidad.

4.1.4. Servicio de base de datos.

El reciente establecimiento de redes de computadoras en diversas entidades nacionales, entre ellas los Centros de Educación Superior, ha permitido a las instituciones de información establecer servicios de consulta a bases de datos accesibles por los distintos puntos terminales de la red.

La consulta a bases de datos en ambiente de red de computadoras presenta múltiples ventajas, entre ellas:

- el horario de consulta a las bases de datos no depende del horario de los servicios de la institución de información sino del tiempo en funcionamiento del servidor, que por lo general funciona las 24 horas, con lo que se amplía considerablemente el tiempo en que la información se encuentra disponible.

- se elimina la necesidad de reservar tiempo para consultar las bases de datos, ya que se puede accesar simultáneamente una misma base de datos, incluso un mismo registro, por múltiples usuarios.

- los usuarios requieren de menos tiempo para la búsqueda de información, ya que no tienen que trasladarse de sus puestos de trabajo para efectuar una consulta.

- la información resultante de una búsqueda puede ser almacenada junto con otros ficheros del usuario dentro de su área de trabajo en el servidor, donde puede hacer uso de otras facilidades del trabajo en red para manipular esa información, por ejemplo el envío de esos datos a otros colegas mediante el correo electrónico.

Por otra parte, al no estar controlada esta consulta por el personal de la institución de información, puede presentarse algunos de los problemas siguientes:

- acceso, por parte de usuarios no autorizados, a algunas actividades que modifican los registros, poniéndose en peligro la integridad y seguridad de los datos.

- acceso, por parte de usuarios no autorizados, a información restringida para algunas categorías de usuarios dentro de la red, violándose las condiciones de seguridad de los datos.

- los usuarios desconocen las bases de datos disponibles, así como el contenido temático, alcance temporal, etc., de cada una de ellas.

- los usuarios confrontan dificultades para interactuar de manera efectiva con el sistema de recuperación de información (efecto de cada uno de los comandos u opciones, sintaxis del lenguaje de recuperación, alternativas disponibles, etc.)

Las entidades de información que han incursionado en la implementación de servicios de consulta de bases de datos en redes de computadoras se han visto obligadas a establecer algunos mecanismos que permitan reducir los efectos indeseables de estos problemas.

4.1.5 Servicios de videos.

Un servicio de alojamiento de videos permite a individuos subir videoclips a un sitio web de Internet. El alojador de videos almacenará el video en uno de sus servidores, y le mostrará al individuo diferentes tipos de código para permitir que otros vean su video. El sitio web es llamado sitio web de alojamiento de videos o sitio web de distribución de videos.

Un servicio de alojamiento de videos se refiere a un sitio web o al software donde los usuarios pueden distribuir sus videoclips. Algunos servicios pueden cobrar, otros ofrecen sus servicios gratuitamente. Muchos servidores tienen opciones de distribución privada y pública.

El video que se comparte se puede clasificar en varias categorías, el usuario puede compartir el video con otro sitio web, la plataforma de distribución del video y corregir el video en Internet. Obsérvese que los sitios web que son solamente motores de búsqueda y no proporcionan el alojamiento de los videos (como Yahoo! Video Search) no están incluidos en este artículo.

Los servicios generados por el usuario normalmente ofrecen servicios gratuitos donde los usuarios suben sus videos y los comparten con los usuarios. Muchos sitios aplican restricciones en el tamaño del video, duración, formato, etc.

La mayoría de los servidores no aceptan videos pornográficos, sin embargo, hay contenido que logra ser subido pero con advertencias o bloqueos. Algunos sitios muestran una previsualización del contenido antes de subirlo.

Propósitos del alojamiento de videos.

- Ahorrar en costos de banda ancha, a menudo eliminando los costos completamente.
- Crear un lugar común.
- Crear una experiencia sencilla y sin molestias, donde subir un video y hacer los procesos de streaming y embedding normalmente requerirían conocimientos avanzados de programación. Ahora esto es comúnmente logrado mediante un navegador web, con una experiencia nula o muy leve de programación.

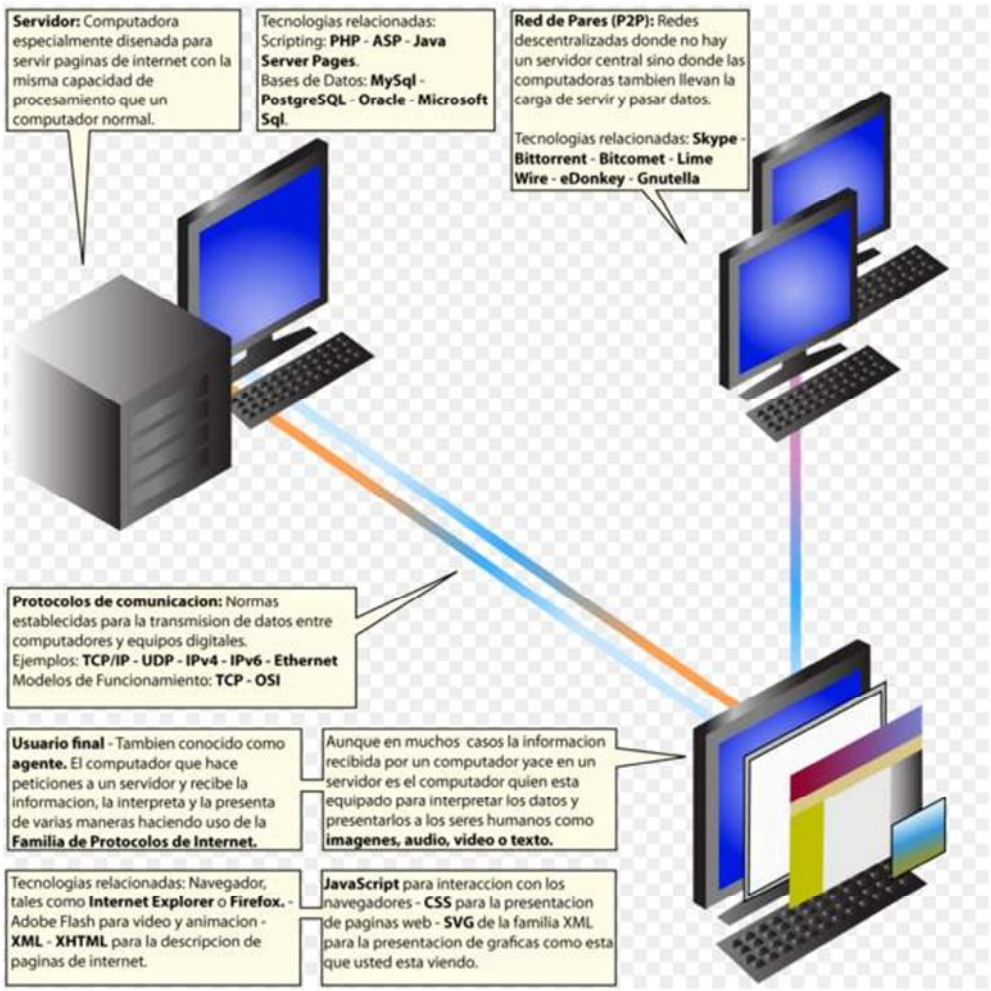


Figura 4.1.2 Tecnologías del internet

4.2 Instalación del servidor.

En este punto explicaremos más a detalle las características de IIS, también abarcaremos algunos conceptos de direcciones IP que son fundamentales para tener un servidor funcionando correctamente, ya que los equipos de los usuarios o clientes acceden al servidor mediante direcciones IP.

4.2.1 Instalación.

En general la instalación es la misma para diferentes versiones de Windows, la que mostramos a continuación es la instalación en Windows XP pero si se quisiera instalar en otras versiones, no hay cambios considerables, de hecho existen versiones de Windows que ya tienen preinstalado este software de servidor, por ejemplo Windows Server 2003 y Windows Vista. A continuación, se enlistan los pasos para la instalación del servidor:

Paso 1: Abrir panel de control.

Paso 2: Ir a "agregar y quitar programas".

Paso 3: Dentro de la ventana dar clic en "agregar o quitar componentes de

Windows" (ver figura 4.2).

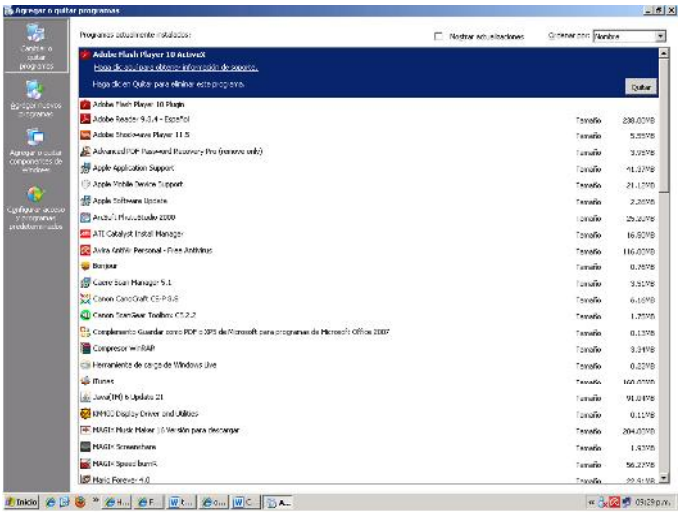


Figura 4.2. Agregar o quitar componentes de Windows.

4.2.1.1 Sitio Web predeterminado.

Para acceder al sitio predeterminado tuvimos que ingresar la dirección "http//:localhost/" en nuestro navegador, este sitio web se almacena en nuestro disco duro específicamente en "C:\Inetpub\wwwroot".

Si queremos agregar nuestras propias páginas web, lo que tenemos que hacer es simplemente moverlas a este directorio con todo y sus archivos correspondientes. Por ejemplo, si creamos una página llamada "Menu.html", ésta y todos sus archivos (imágenes, sonidos, vídeos, etc.), tienen que ser movidos al directorio "wwwroot" y para abrirla en el navegador, tenemos que colocar la

siguiente dirección “http//:localhost/Menu.html” y la página tiene que visualizarse en el navegador. Lo anterior sería útil para páginas sencillas o si sólo se tiene una página en el servidor.

Por ejemplo dentro de “wwwroot” creamos una carpeta y la llamamos “Web_1” y en este directorio movemos la página “Menu.html” para acceder a esta página mediante el servidor, tendríamos que escribir la siguiente dirección en el navegador “http//:localhost/Web_1/Menu.html”. Entonces podemos tener varios sitios Web almacenados en un mismo servidor.

Un sitio web predeterminado es al que se ingresa sin necesidad de especificar su nombre y para crearlo solo se tiene que dar el nombre de Default (predeterminado), a la página que queremos que sea nuestro sitio predeterminado por ejemplo, si en “C:\wwwroot\Web_1” tenemos la página “Default.html” entonces para acceder a este sitio, sólo tenemos que ingresar la dirección “http//:localhost/Web1/” e ingresa automáticamente al sitio “Default.html”, entonces se recomienda que a la página principal se le nombre Default.

4.2.1.2 Direcciones IP.

Entender las direcciones IP es fundamental a la hora de querer instalar un servidor. Como vimos antes cuando queríamos abrir una página con el navegador lo hacíamos mediante la dirección de “localhost”, esta forma de abrir sitios web es muy útil cuando estamos en la etapa de prueba de ésta y sólo se pueden abrir localmente, es decir, que sólo se pueda usar este método dentro el mismo servidor.

Ahora bien, si se quiere que otros usuarios dentro de Internet vean nuestras páginas y que de hecho ésa es la idea, estos tienen que acceder a nuestro servidor mediante la IP de éste. A continuación se muestran algunos conceptos básicos y clasificaciones de lo que son las IP.

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento, en el conjunto de redes visibles por el host.

En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Las direcciones IP se clasifican en:

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

Direcciones IP privadas (reservadas). Son visibles únicamente por otros host de su propia red o de otras redes privadas interconectadas por ruteadores.

Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un ruteador (o proxy) que tenga una IP pública, sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

Direcciones IP estáticas (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet, con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

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

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a, b .c, d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99.

¿Cuántas direcciones IP existen?

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

4.2.1.3 Firewall

Cada ordenador que se conecta a internet (y, básicamente, a cualquier red de ordenadores) puede ser víctima del ataque de un hacker. La metodología que generalmente usan los hackers consiste en analizar la red (mediante el envío aleatorio de paquetes de datos) en busca de un ordenador conectado. Una vez que encuentra un ordenador, el hacker busca un punto débil en el sistema de seguridad para explotarlo y tener acceso a los datos de la máquina.

Por muchas razones, esta amenaza es aún mayor cuando la máquina está permanente conectada a internet:

- Es probable que la máquina elegida esté conectada pero no controlada.
- Generalmente, la máquina conectada que se elige posee un ancho de banda más elevado.
- La máquina elegida no cambia las direcciones IP o lo hace muy ocasionalmente.

Por lo tanto, es necesario que tanto las redes de las compañías como los usuarios de internet con conexiones por cable o ADSL se protejan contra intrusiones en la red instalando un dispositivo de protección.

¿Qué es un Firewall?

Un firewall es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de firewall filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se trata de una pasarela de filtrado que comprende al menos las siguientes interfaces de red:

- una interfaz para la red protegida (red interna)
- una interfaz para la red externa.

El sistema firewall es un sistema de software, a menudo sustentado por un hardware de red dedicada, que actúa como intermediario entre la red local (u ordenador local) y una o más redes externas. Un sistema de firewall puede instalarse en ordenadores que utilicen cualquier sistema siempre y cuando:

- La máquina tenga capacidad suficiente como para procesar el tráfico
- El sistema sea seguro
- No se ejecute ningún otro servicio más que el servicio de filtrado de paquetes en el servidor

En caso de que el sistema de firewall venga en una caja negra (llave en mano), se aplica el término "aparato".

Cómo funciona un sistema Firewall.

Un sistema firewall contiene un conjunto de reglas predeterminadas que le permiten al sistema:

- Autorizar la conexión (permitir)
- Bloquear la conexión (denegar)
- Rechazar el pedido de conexión sin informar al que lo envió (negar)

Todas estas reglas implementan un método de filtrado que depende de la política de seguridad adoptada por la organización. Las políticas de seguridad se dividen generalmente en dos tipos que permiten:

- la autorización de sólo aquellas comunicaciones que se autorizaron explícitamente:

  "Todo lo que no se ha autorizado explícitamente está prohibido"

- el rechazo de intercambios que fueron prohibidos explícitamente

El primer método es sin duda el más seguro. Sin embargo, impone una definición precisa y restrictiva de las necesidades de comunicación.

Filtrado de paquetes Stateless.

Un sistema de firewall opera según el principio del filtrado simple de paquetes, o filtrado de paquetes stateless. Analiza el encabezado de cada paquete de datos (datagrama) que se ha intercambiado entre un ordenador de red interna y un ordenador externo.

Así, los paquetes de datos que se han intercambiado entre un ordenador con red externa y uno con red interna pasan por el firewall y contienen los siguientes encabezados, los cuales son analizados sistemáticamente por el firewall:

- La dirección IP del ordenador que envía los paquetes
- La dirección IP del ordenador que recibe los paquetes
- El tipo de paquete (TCP, UDP, etc.)
- El número de puerto (recordatorio: un puerto es un número asociado a un servicio o a una aplicación de red).

Las direcciones IP que los paquetes contienen permiten identificar el ordenador que envía los paquetes y el ordenador de destino, mientras que el tipo de paquete y el número de puerto indican el tipo de servicio que se utiliza.

La siguiente tabla proporciona ejemplos de reglas del firewall:

Regla	Acción	IP fuente	IP destino	Protocolo	Puerto fuente	Puerto destino
1	Aceptar	192.168.10.20	194.154.192.3	tcp	cualquiera	25
2	Aceptar	cualquiera	192.168.10.3	tcp	cualquiera	80
3	Aceptar	192.168.10.0/24	cualquiera	tcp	cualquiera	80
4	Negar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Los puertos reconocidos (cuyos números van del 0 al 1023) están asociados con servicios ordinarios (por ejemplo, los puertos 25 y 110 están asociados con el correo electrónico y el puerto 80 con la Web).

4.2.1.4 Host.

El término Host es usado en informática para referirse a los computadores conectados a la red, que proveen o utilizan servicios a/de ella. Los usuarios deben utilizar hosts para tener acceso a la red.

En general, los hosts son computadores mono o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores WWW, etc. Los usuarios que hacen uso de los hosts pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red.

Un host o anfitrión es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Comúnmente es descrito como el lugar donde reside un sitio web. Un host de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o

CAPÍTULO 5

Comunicación.

Introducción.

A continuación se mencionará un panorama general de la capa de servicio de control, que es la capa de comunicación y manipulación del servidor con el móvil, en el desarrollo de este capítulo se explicarán todos los elementos involucrados tanto en hardware como en software para el control por el puerto paralelo, el cual se dará una breve descripción del mismo, así como los elementos finales de la parte del hardware que están involucrados, desde los circuitos de potencia de los motores como el uso de el micro controlador y el diseño de control mediante los bits de control interpretados por el mismo micro controlador, para dar acciones a los motores y el uso del circuito driver para la etapa de potencia de los motores.

Otro bloque que se mencionará es para el módulo de comunicación inalámbrica, el cual como se observó desde el esquema general de este proyecto es un pequeño bloque primordial del mismo, ya que este bloque nos proporcionará la facilidad de movimiento del móvil.

Una vez hecho todo esto, se finalizara en el diseño y armado de los circuitos impresos de transmisión y recepción junto con los circuitos de potencia del móvil.

5.1 Configuracion del centro de monitoreo.

En la figura 5.1 se puede observar la configuración de nuestro centro de monitoreo donde se especifica la configuración de nuestro enlace entre los dispositivos electrónicos para el comienzo de nuestro monitoreo.

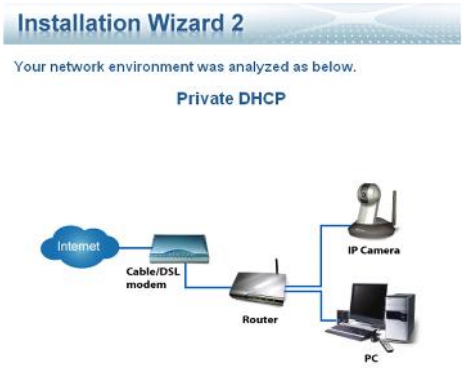


Figura 5.1 Configuración del centro de monitoreo.

La primera vez que se conecte, deberá configurar esta aplicación para conectarse a los productos remotos de la serie Servidor de vídeo / Cámara de red en “Menú de configuración \ Configuración de cámara”, como se indica en la Fig.5.1.2 deberá tener el privilegio raíz (administrador) para realizar la configuración.

Figura 5.1.2 Configuración de cámara.

En la figura 5.1.3 se detalla el proceso para ingresar la Dirección IP para el enlace entre la Cámara IP y el Servidor, en la Figura 5.1.4 se observamos la conexión para visualizar y tomar el control de nuestros dispositivos.

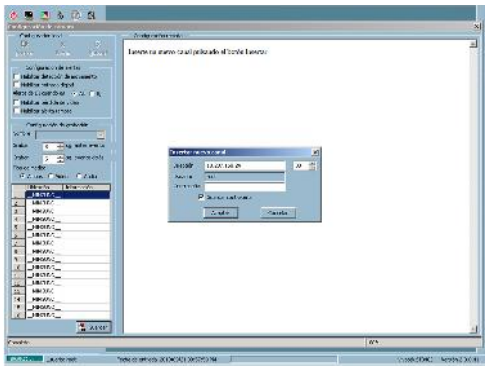


Figura 5.1.3 Insertando la Dirección IP.

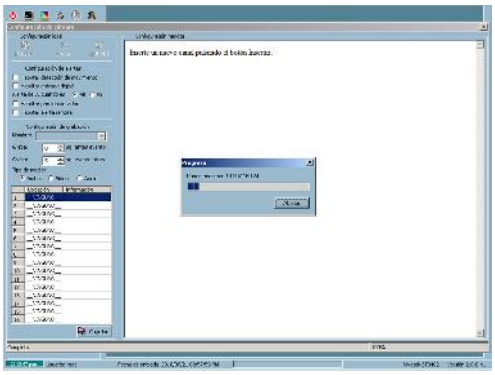


Figura 5.1.4. Conectando la Dirección IP con el servidor.

Una de las ventajas que nos proporciona el Software de Vivotek es el que podemos configurar la vista de todas las cámaras para un mejor monitoreo como lo podemos observar en la figura 5.1.5.

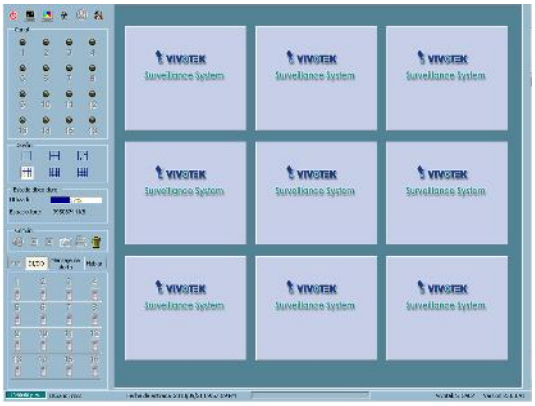


Figura 5.1.5 Visualización de las Cámaras IP

En esta sección se proporciona una visión general de la herramienta Monitor, como se muestra en la Fig. 5.1.6. En las siguientes secciones se proporciona información detallada sobre los componentes de esta herramienta.

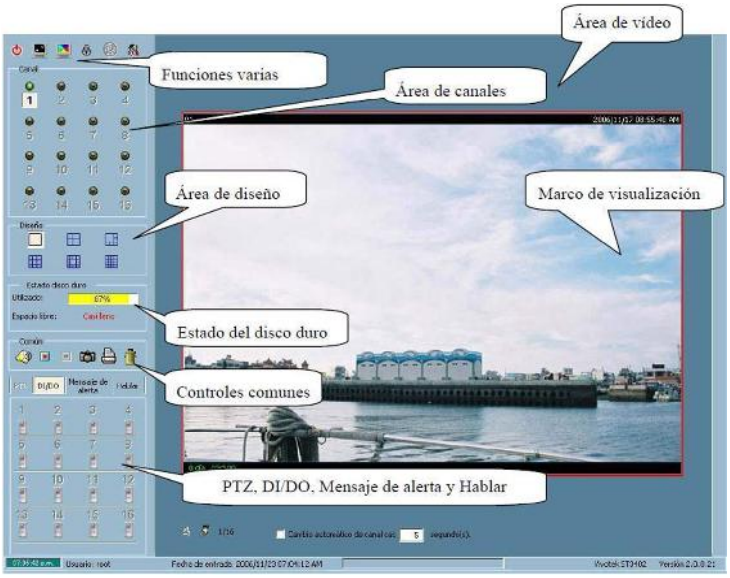


Figura 5.1.6. Visión general de la herramienta Monitor

5.2 El diseño de la configuración.

En esta sección tratamos la configuración local de la conexión y las configuraciones funcionales de cada cámara.

Si está interesado en la configuración remota de cada cámara, puede consultar el manual del usuario de cada producto de la serie Servidor de vídeo/cámara de red entregado con el hardware. En la siguiente Fig. 5.2 se muestra el diseño de la ventana Configuración de cámara.

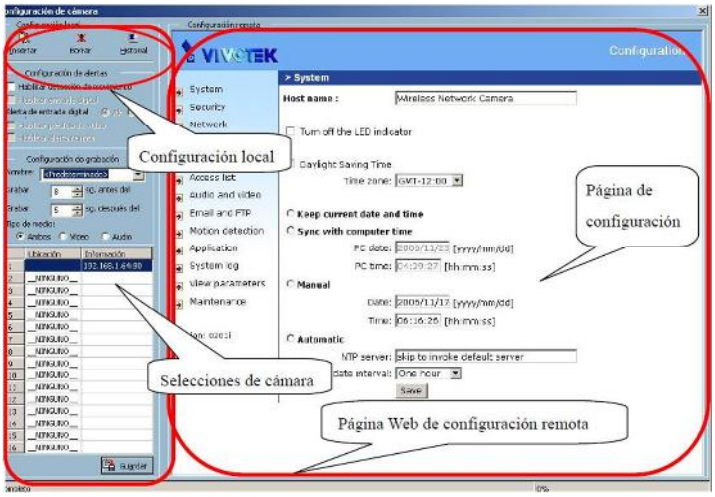


Figura 5.2 Diseños de configuraciones de las cámaras.

NOTA: En cuanto a la ubicación de la cámara seleccionada, deberá asegurarse de que la cadena de ubicación no incluya caracteres prohibidos como “"\ / : * ? " < > |”. En caso contrario, una cadena de ubicación errónea provocará el funcionamiento incorrecto de la aplicación. Puede cambiar la cadena de ubicación en “Video->Text on video” de la página web de configuración remota.

5.3 Configuración global.

Al finalizar la conexión para cada producto remoto de la serie Servidor de vídeo / Cámara de red, deberá configurar los parámetros globales de todos los servidores conectados, incluido el directorio de bases de datos de medios, el uso del disco duro, la configuración de Internet y la información de estado de la copia de seguridad.

Figura 5.3.1 Configuración global

Puede activar la ventana de configuración global desde “Menú de configuración \ Configuración global...”, como se muestra en la Fig. 5.3.1

ATENCIÓN: Aparecerá una ventana de advertencia para indicarle que se detendrán todos los procesos de grabación al activar la ventana de configuración global.

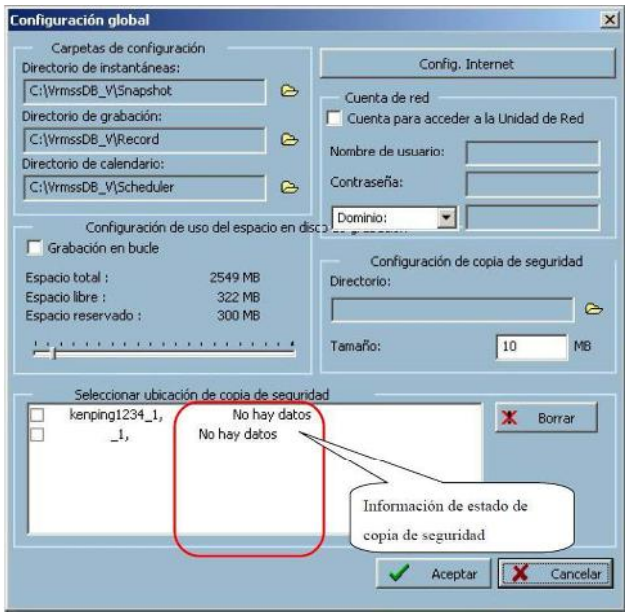


Figura 5.3.2 Ventana Configuración global

Carpetas de configuración:

- Directorio de instantáneas.- Es el directorio donde se guardan las instantáneas en formato *.bmp desde los canales como se muestra en la Fig. 5.3.2.

- Directorio de grabación.- Es el directorio para guardar los datos de medios grabados desde los canales remotos.

- Directorio de calendario.- Es el directorio donde se guardan los programas personalizados para el calendario de grabación de cada canal.

Configuración de uso del espacio en disco de grabación:

- Grabación en bucle.- Con este ajuste marcado, el sistema de base de datos de medios sobrescribirá los datos más antiguos si la base de datos actual alcanza su límite de almacenamiento. En otras palabras, grabará los datos de medios en círculos. Si no se marca este ajuste, aparecerá un mensaje de advertencia cuando se acerque el límite. Después, detiene la grabación al llegar al límite de uso del disco duro.

- Espacio reservado.- Indica el tamaño de disco duro que se reservará en el disco de grabación. Si los datos grabados superan este límite, los nuevos datos de medios entrantes sustituirán a los más antiguos si se ha seleccionado “Grabación en bucle”. El mecanismo de

búfer previo ocupará cierto espacio si ya está configurado algún canal pero no está grabando.

5.4 Configuración de Pantalla e IU.

Las opciones de pantalla de vídeo y la configuración de alerta se pueden modificar en el cuadro de diálogo Configuración de Pantalla e IU. La grabación y la supervisión pueden continuar al abrir este cuadro de diálogo. Puede activar el cuadro de diálogo Configuración de Pantalla e IU desde "Menú de configuración \ Configuración de Pantalla e IU..." como se muestra en la Fig. 5.4.1.

Figura 5.4.1. Configuración de Pantalla e IU

Figura 5.4.1 Ventana Configuración de Pantalla e IU

Configuración de alerta local:

Puede cargar un archivo *.wav personalizado para el sonido de la alerta. También puede escuchar la muestra del archivo de sonido elegido haciendo clic en el botón "Reproducir" (el botón con la punta de flecha negra a la derecha).

Configuración de alerta remota:

Como configuración de alerta remota, puede cargar un archivo *.wav para el sonido de activación de la alerta y el sonido se reproducirá en el lado remoto.

NOTA: Si el usuario no activa la configuración de la alerta que se describe en la sección 3.4.3, el sonido de alerta no se podrá reproducir cuando tenga lugar el evento correspondiente. Recuerde activar la configuración de alerta que desee.

Formato de instantánea:

Existen dos tipos de formatos de instantánea (.jpg y .bmp) que puede seleccionar el usuario.

Modo modulación:

Debe seleccionar el formato de la señal de entrada (NTSC, PAL o CMOS) para mostrar la resolución original de la secuencia de vídeo desde el producto remoto de la serie Servidor de vídeo / Cámara de red.

NOTA: Debe seleccionar el formato de la señal de entrada de acuerdo con el tipo de cámara o tipo de módulo CCD conectado al producto remoto de la serie Servidor de vídeo / Cámara de red, independientemente de si la línea conectada es de 50 o de 60 Hz.

Formatos del sistema PAL

El sistema de color PAL se usa habitualmente con un formato de vídeo de 625 líneas por cuadro (un cuadro es una imagen completa, compuesta de dos campos entrelazados) y una tasa de refresco de pantalla de 25 cuadros por segundo, entrelazadas, como ocurre por ejemplo en las variantes PAL-B, G, H, I y N. Algunos países del Este de Europa que abandonaron el sistema SECAM ahora emplean PAL D o K, adaptaciones para mantener algunos aspectos técnicos de SECAM en PAL.

Comparación PAL y NTSC

En PAL, también conocido por 576i, se utiliza un sistema de exploración de 625 líneas totales y 576 líneas activas, pues 49 líneas se utilizan para el borrado. En NTSC, también conocido por 480i, se utiliza un sistema de exploración de 525 líneas totales y 480 líneas activas (las que se restituyen en pantalla), pues 45 líneas, que no son visibles, se utilizan para el borrado. Debido a que el cerebro puede resolver menos información de la que existe realmente, podemos hablar de la "relación de utilización" o "factor de Kell", que se define como la razón entre la resolución subjetiva y la resolución objetiva. El factor de Kell para sistemas entrelazados como PAL y NTSC vale 0,7 (para sistemas progresivos vale 0,9). Entonces, tanto en PAL como NTSC tenemos que:

Resolución subjetiva / Resolución objetiva = 0,7

La resolución objetiva de PAL es 576 líneas, mientras que la de NTSC es de 480 líneas. De esta manera, en PAL tenemos una resolución subjetiva de 403,2 líneas; mientras que en NTSC se perciben 336 líneas. Por tanto, PAL ofrece una resolución subjetiva y objetiva de un 20% superior a NTSC.

El sistema de televisión NTSC consiste en una ampliación del sistema monocromático (blanco y negro) norteamericano, su desarrollo lo inició CBS al final de la década de los 30, pero fue en los años 50 cuando fue aprobado por la FCC. Este sistema consiste en la transmisión de cerca de 30 imágenes por segundo formadas por 486 (492) líneas horizontales visibles con hasta 648 píxeles cada una. Para aprovechar mejor el ancho de banda se usa video en modo entrelazado dividido en 60 campos por segundo, que son 30 cuadros con un total de 525 líneas horizontales y una banda útil de 4.25 MHz que se traduce en una resolución de unas 270 líneas verticales.

Para garantizar la compatibilidad con el sistema en blanco y negro, el sistema NTSC de color mantiene la señal monocromática blanco y negro como componente de luminancia de la imagen en color. Se modificaron ligeramente las frecuencias de exploración a 29.97 cuadros por segundo y 15.734 Hz de frecuencia horizontal. Mientras que la señal de color se ha agregado con una frecuencia que es múltiplo de la horizontal sobre una subportadora suprimida de 3.579545 MHz modulada por amplitud y por cuadratura de fase; la demodulación de los componentes de crominancia requiere necesariamente de sincronía, por lo que se envía al inicio de cada línea (pórtico anterior) una señal sinusoidal de referencia de fase conocida como "salva de color", "burst" o "colorburst"; esta señal tiene una fase de 180º y es utilizada por el demodulador de la crominancia para realizar correctamente la demodulación. A veces, el nivel del "burst" es utilizado como referencia para corregir variaciones de amplitud de la crominancia de la misma manera que el nivel de sincronismo se utiliza para la corrección de la ganancia de toda la señal de vídeo.

NTSC digital.

Lo dicho anteriormente se refiere al sistema NTSC en dispositivos analógicos. En los dispositivos digitales, como televisión digital, consolas de videojuegos modernas, DVD, etc. , ni siquiera importa la codificación de color empleada, y ya no hay diferencia entre sistemas, quedando el significado de NTSC reducido a un número de líneas igual a 480 líneas horizontales (240 para mitad de resolución, como VCD) con una tasa de refresco de la imagen de 29,970 imágenes por segundo, o el doble en campos por segundo para imágenes entrelazadas.

CAPÍTULO 6

Transmision y Recepcion del Video por Internet.

En este capítulo final se mencionará todo lo relacionado con la transmisión de video a través de Internet, la cual se logra con la instalación de un servidor de video streaming, así como los elementos que involucran el desempeño de este tipo de servidor, en el desarrollo se mencionará y justificará, algunos rasgos por lo cual la transmisión de video experimenta un retraso y algunos de los protocolos de video streaming, que se utilizarán para obtener una transmisión con la mayor calidad posible sin importar el ancho de banda, con la que trabaje el usuario, así como los tipos de streaming que existen y las diferencias que hay en ambos.

También se mencionarán los tipos de reproductores de video streaming comerciales y la elección del reproductor que se empleará en este proyecto y por último se describirá el programa que será capaz de dejarnos transmitir por Internet en la mayor calidad y menor tiempo de retraso posible que es el Windows Media Encoder.

6.1 Arquitectura de los sistemas de vídeo streaming.

Para instalar un servicio de video streaming se deben cubrir los bloques que se muestran en la figura 6.1.

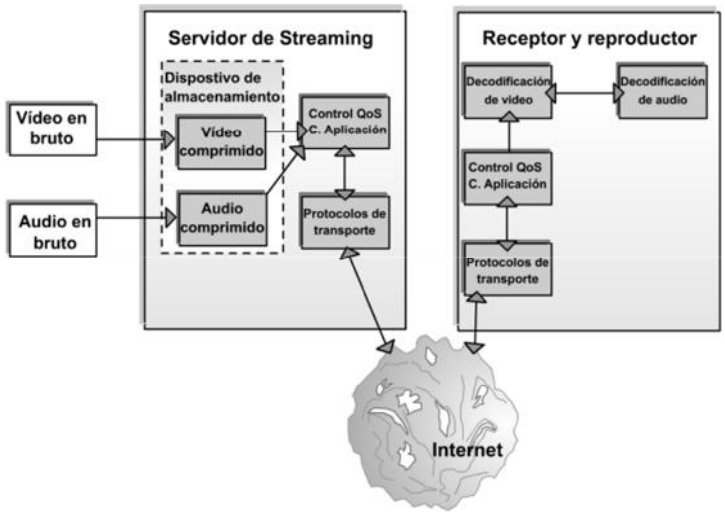


Figura 6.1. Arquitectura de un sistema de video streaming.

Primero se deben de tener los sistemas de captura, tanto de video como de audio, después en el bloque posterior se comprimen el video y audio, son almacenados en los dispositivos de almacenamiento masivo.

La capa de control de QoS (Quality of Service, Calidad del Servicio) sirve para mejorar la calidad del vídeo cuando existen pérdidas de paquetes. Después los flujos de bits comprimidos se convierten en paquetes en el bloque de protocolos de transporte para su envío por Internet o redes IP.

Lo anterior corresponde a la parte del servidor de streaming, pero también el receptor o usuario final, debe de tener instalado un reproductor que sea compatible con esta arquitectura. Como podemos ver también se necesita un bloque de protocolos de transporte y un control QoS que tienen prácticamente la misma función que en el servidor de streaming.

En el receptor se deben de tener decoficadores de audio y de video, además se debe de tener un bloque de sincronización debido a que el audio o el video se pueden desfasar debido a paquetes perdidos o retrasados.

Los bloques de esta arquitectura se explicarán más a detalle en los siguientes puntos.

6.1.1 Compresión de audio y vídeo.

Debido a que para transmitir el video o audio en bruto se requiere de un gran ancho de banda, es necesario codificar o comprimir éstos, para optimizar su transmisión, ya que vamos a transmitir en un medio que no cuenta con mucho ancho de banda.

La compresión de vídeo se consigue mediante la explotación de las semejanzas o redundancias que existen en una señal de vídeo típica. Los cuadros consecutivos de una secuencia de vídeo exhiben redundancia temporal, dado que generalmente contienen los mismos objetos con algún pequeño movimiento entre cuadros.

En un cuadro en particular encontraremos redundancia espacial, dado que las amplitudes de los píxeles cercanos generalmente están correlacionadas.

Otra meta de la compresión de vídeo es reducir la información irrelevante en la señal de vídeo. Esto significa que el sistema codificará características que tengan importancia perceptiva y no gastará valiosos bits en información, que no pueda ser percibida o que sea irrelevante.

6.1.2 Escalabilidad de la codificación.

A la hora de transmitir a varios usuarios a través de Internet, surge un gran problema. Como sabemos, los usuarios de Internet están conectados a diferentes velocidades, por ejemplo, un usuario puede tener una conexión de 2Mbps y otro podría tener una conexión de 56Kbps.

Este ejemplo es un caso extremo pero que se puede presentar con cierta frecuencia, de hecho no se necesita poner un caso tan extremo para ver que esta variación de velocidades es un problema, pongamos ahora otro ejemplo donde estamos transmitiendo un vídeo codificado a un tasa de bits fijo de 1.5Mbps y tenemos dos usuarios recibiendo esta transmisión, el primero con una conexión de 2Mbps y el segundo con una conexión de 1Mbps.

El primer usuario recibiría el vídeo sin problema alguno pero el segundo no podría recibir los bits necesarios para mostrar la secuencia en tiempo real, lo que se traduce en enormes retrasos en la reproducción del vídeo recibido.

Exactamente debido al problema anterior surgió la escalabilidad, y ésta se refiere a la capacidad de recuperar información desde imágenes o vídeo que tengan un significado físico, mediante la decodificación de secuencias de bits con información parcial.

Entonces si ahora transmitimos el video con codificación escalable, el usuario conectado mediante banda ancha verá el vídeo con la calidad completa y el usuario conectado que se conecta a 56Kbps podría bajar un subconjunto de la transmisión y vería al mismo tiempo el vídeo con una menor calidad. Un flujo escalable puede ofrecer la capacidad de adaptación para niveles de error variable en el canal y capacidad de procesamiento desigual en los receptores.

Actualmente se puede tener acceso a Internet casi en cualquier lugar donde estemos, esto gracias a la convergencia de tecnologías inalámbricas, y a que cada vez hay más dispositivos móviles capaces de tener acceso a Internet. Entonces la codificación tiene un papel vital para proporcionar acceso al medio, no importando el tipo de conexión ni el tipo de dispositivo que se esté empleando.

La codificación escalable se consigue usualmente suministrando versiones múltiples de un vídeo en términos de su resolución de amplitud, resolución espacial, resolución temporal, resolución en frecuencia o una combinación de estos tipos. En este trabajo nosotros emplearemos codificadores que tengan escalabilidad; ya que uno de los objetivos de la tesis, es poder instalar el servicio de monitoreo móvil, en cualquier lugar donde haya Internet y que la transmisión sea recibida donde se tenga acceso a este medio, sin importar tanto la velocidad de conexión.

6.1.4 Protocolos de transporte en tiempo real.

Se han desarrollado diferentes protocolos para facilitar el streaming en tiempo real de contenidos multimedia. Streaming significa que la velocidad media de cuadro del vídeo, que se ve en el reproductor es dictada por la velocidad de cuadro transmitida. La velocidad de entrega tiene que ser controlada para que los datos del vídeo lleguen justo antes de que éstos sean requeridos para la proyección en el reproductor.

En los puntos posteriores mencionaremos los protocolos de streaming que actualmente se están usando.

6.1.4.1 RTP.

El Protocolo de Tiempo Real (RTP) es un protocolo de transporte que fue desarrollado para los datos streaming. RTP incluye campos de datos extra que no están presentes en TCP. Permite el control del servidor para que el flujo de datos (stream) del vídeo sea servido a una velocidad correcta, para la proyección en tiempo real. Entonces, el reproductor utiliza estos campos RTP para reunir los paquetes recibidos en el orden y velocidad de reproducción correcta.

6.1.4.2 RTCP.

RTCP es usado junto a RTP. Ofrece a cada participante de la sesión RTP información de vuelta que puede ser usada para controlar la sesión.

Los mensajes incluyen informes de recepción, incluyendo el número de paquetes perdidos y las estadísticas de las perturbaciones (llegadas tempranas o retrasadas).

Esta información puede ser potencialmente utilizada por aplicaciones que se encuentran en capas superiores para poder modificar así la transmisión. Por ejemplo, podría cambiarse la velocidad de bit del flujo de datos (stream) para contrarrestar así la congestión de la red.

Este protocolo es de gran utilidad ya que en este proyecto estamos hablando de un cierto número de usuarios conectados a un servidor, dependiendo de este número, la calidad del stream puede ser mayor o menor y de esta manera la velocidad del bit del servidor varía automáticamente.

6.1.4.3 RTSP.

Es un protocolo de nivel de aplicación, utiliza como protocolo de transporte el TCP, soportando la recepción de información multimedia desde un servidor multimedia desde donde un cliente puede solicitar que el servidor le transmita información. Añade flujo multimedia a una presentación ya existente.

RTSP es un protocolo que establece y controla uno o varios flujos sincronizados de información multimedia continua como audio y vídeo. Difiere en ciertas cuestiones importantes con HTTP: RTSP es un protocolo de estado a diferencia de HTTP; tanto los servidores como los clientes RTSP pueden realizar peticiones; los datos son transportados mediante un protocolo diferente (datos transportados fuera de banda).

También tiene similitudes con HTTP: Formato de las peticiones/respuestas, códigos de estado, mecanismos de seguridad, formato de la URL, negociación de los contenidos y su sintaxis es muy similar.

Tiene la propiedad de multiservidor. Cada flujo dentro de una presentación puede residir en un servidor distinto, por ejemplo el flujo de vídeo y el de audio, en una presentación multimedia, pueden estar en servidores diferentes. Como se muestra en la figura 6.2.

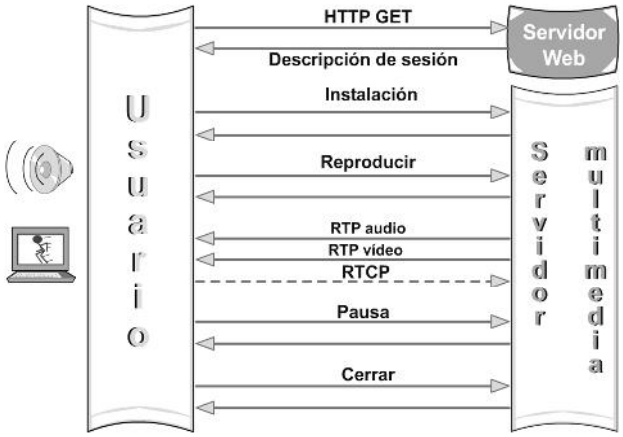


Figura 6.2 Transacciones de RTSP.

En la figura anterior, podemos ver las transacciones utilizadas por RTSP y son:

• **Instalación:** Hace que el servidor reserve los recursos necesarios para comenzar la transmisión del flujo y da comienzo la sesión RTSP.

• **Reproducir:** Inicia la transmisión de datos una vez que los recursos han sido reservados con instalación.

• **Pausa:** Provoca una parada temporal en el envío de datos, pero no libera los recursos asociados a la sesión.

• **Cerrar:** Da por finalizada la transmisión del flujo.

6.1.5 Distribución.

En la instalación de un servicio de vídeo streaming la parte de distribución tenemos que tomarla mucho en cuenta ya que es lo que une al cliente con el servidor (ver figura 6.1).

En principio, es muy simple mientras haya conectividad entre el servidor y el reproductor/cliente, pues la demanda de paquetes será satisfecha.

Lo anterior es el caso ideal, pero en los casos reales, la verdad no es nada fácil, porque Internet no fue diseñada originalmente para soportar flujos de datos (streams) continuos sobre conexiones constantes. Sin duda tendremos muchos retrasos en las transmisiones, así como frames dañados y en general errores en la visualización.

Diferentes avances están ayudando a las mejoras de la calidad de entrega. Por ejemplo se está aumentando cada vez más el ancho de banda, ya sea, a través de cable ADSL o modem. También como ya mencionamos se ha implementado UDP para ganar aun más velocidad. En cuanto a la calidad QoS desempeña un papel importante. La distribución depende mucho también del proveedor de servicios de Internet que se tenga.

Como conclusión podemos decir que la distribución jamás será ideal, que siempre se tendrán errores y pérdidas en la red. Entonces, haciendo una instalación correcta del servicio; podremos minimizar estos errores lo más que se pueda, para prestar un servicio con la suficiente calidad para nuestra aplicación

6.1.6 Receptor y reproductor.

El receptor es la parte final de la arquitectura del vídeo streaming y este receptor no es otra cosa que la computadora del usuario final, la cual se encarga de recibir la señal y por medio de un reproductor instalado en la computadora se encarga de procesar dicha señal.

Como es de suponerse, el reproductor debe de tener funciones especiales que le permitan recibir e interpretar correctamente, en la figura vemos que tiene protocolos de transporte, Control QoS en la capa de aplicación y decodificadores de audio y de vídeo. Un reproductor que tenga estas características podrá recibir y reproducir el flujo de streaming sin problema alguno.

Los reproductores que no soportan streaming, lo que hacen es primero descargar todos los datos en el disco duro y enseguida los reproducen de manera local. El streaming consiste en ir procesando por partes los datos o paquetes que se están recibiendo, y se hace una representación casi inmediata en el monitor y al final se descargan todos los datos.

Entonces no hay espera, no tenemos que descargar todo el vídeo para después enterarnos que no nos gustó, con un reproductor streaming, si lo que vemos no es de nuestro agrado, simplemente lo quitamos.

Para este proyecto los reproductores con capacidades de streaming son fundamentales, por el hecho de que queremos realizar una transmisión en tiempo real, queremos que lo que esté sucediendo del lado del servidor, sea vea en un lapso corto, después en el lado del usuario.

Por último mencionamos que una página web normal sólo es capaz de representar textos e imágenes. Para reproducir vídeos con reproductor con capacidades de flujo de streaming en una página web, necesitamos objetos Active-X y/o plug-ins que tienen que ser instalados en el lado del cliente. En el punto 3.3 se explica como incrustar un objeto Active-X.

6.2 Streaming Unicast.

La mayoría de archivos de audio y vídeo que se ven desde el ordenador, sea cual sea el reproductor que se utilice (Real, Windows Media), proviene de un servicio unicast. Este servicio consiste en un servidor que envía paquetes de datos a cada PC que solicita un stream (ver figura 6.3).

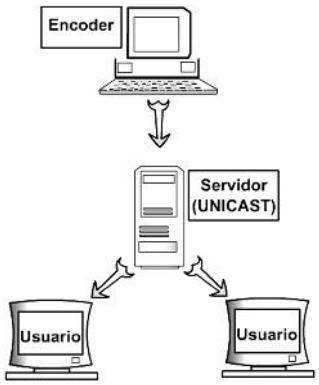


Fig. 6.3. Servidor UNICAST enviando paquetes de datos.

Unicast es una buena opción para recibir transmisiones en vivo, pero tiene sus desventajas; el servidor debe enviar el flujo de datos individualmente a todo aquel que quiere recibir la transmisión.

Si el conjunto de clientes que están recibiendo el stream es pequeño, no ofrece mayor inconveniente; pero si se trata de difundir un material a miles de usuarios, deberán considerarse entonces dos inconvenientes con el proceso unicast:

- Demasiadas peticiones.
- Demasiados paquetes.

Que se explicarán en los siguientes puntos.

6.3 Streaming Multicast.

Multicast utiliza una nueva forma de funcionamiento de redes. En vez de enviar streams desde un solo servidor a un sólo cliente, multicast envía una serie de paquetes que puede ser recibida por cualquiera, desde diversos puntos de distribución. Multicast permite un procesamiento estable del streaming en el servidor y alivia el tráfico en la red.

Multicast hace su trabajo de transmisión de manera similar a cómo funcionan los canales de televisión o las estaciones de radio: El archivo de audio/vídeo se emite desde la estación hacia los servidores conectados a la red, quienes se encargan de distribuir el stream a los usuarios. Cuando el espectro de usuarios se extiende, se agregan servidores, como se muestra en la siguiente figura.

Multicast envía una sola copia de los datos a los clientes que lo han solicitado, permite implementar aplicaciones multimedia en la red y minimizar al mismo tiempo la demanda de ancho de banda de estas aplicaciones.

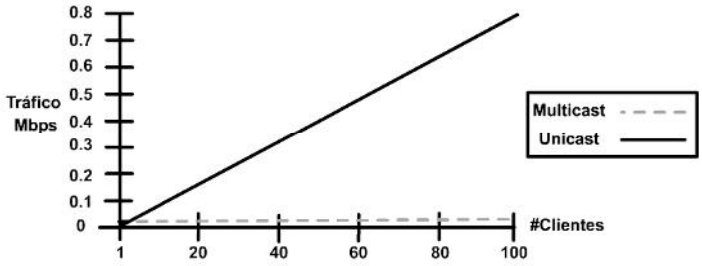


Figura 6.4 Tráfico difusión multicast/unicast.

De la figura 6.4, en la difusión unicast, el ancho de banda se incrementa directamente proporcional con el número de clientes conectados. Con la difusión multicast el ancho de banda se mantiene constante, como vemos multicast es una mejor opción de transmisión.

6.3.1 Recibiendo.

Debido a que multicast es una transmisión donde se envían una serie de paquetes de datos, no hay manera de que el receptor haga una petición de reenvío de paquetes. Lo anterior supone una pérdida de paquetes, pero gracias al control QoS (Servicio de Calidad) y a las técnicas explicadas anteriormente, el usuario no podrá notarlo. Multicast todavía no ha reemplazado a Unicast en Internet porque algunas partes de Internet no han sido conectadas a routers que entiendan el proceso multicast.

Sólo es cuestión de tiempo y claro de dinero para que Multicast sustituya casi por completo a unicast, ya que actualmente la mayoría de los nuevos routers pueden manejar multicast eficientemente, además, del lado del usuario la mayoría de las tarjetas de red en los equipos más recientes, también entienden el funcionamiento de multicast.

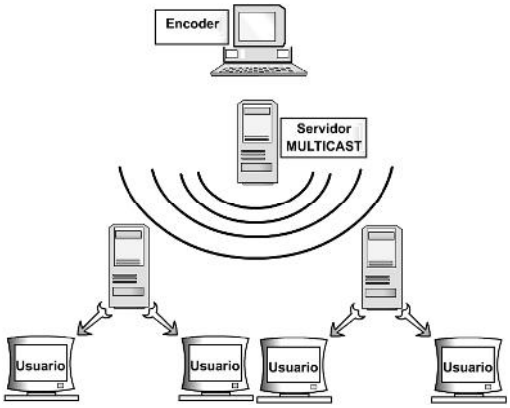


Figura 6.5 Servidor enviando paquetes de datos.

Un área donde la transmisión multicast tiene un gran auge es en las Intranets de las empresas, debido que en éstas, lo equipos de cómputo están modernizados y se aprovecha el gran ancho de banda que les proporciona la Intranet.

6.3.2 Enrutamiento.

Los ruteadores de la red y los protocolos que éstos ejecutan, llevan a cabo la mayor parte del trabajo necesario para permitir una conectividad multicast. En la actualidad, se usan varios protocolos de enrutamiento de multicast: el protocolo de enrutamiento de multicast por vector de distancia, el protocolo de abrir primero la ruta de acceso más corta de multicast y el multicast independiente de protocolo. La tarea de estos protocolos es crear rutas de entrega de multicast eficaces, a través de la red. Los protocolos de enrutamiento de multicast utilizan distintos algoritmos para lograr esta eficacia.

6.3.3 Ruta de los datos.

Una ruta de entrega eficaz implica que los datos de multicast viajen únicamente a los clientes que desean recibirlos, y que usen la ruta de acceso más corta a esos clientes. Si los datos viajan a cualquier otro lugar a través de la red, estarán usando un ancho de banda innecesario.

Puede imaginarse la red como una estructura de árbol. El origen de multicast envía los datos a través de las ramas del árbol. Los que son los responsables de enviar los datos por las ramas correctas a los otros ruteadores, y a las subredes en las que los miembros de un grupo están esperando los datos. Los ruteadores cortan las ramas en las que nadie desea datos y las vuelven a insertar en el árbol cuando un cliente de una nueva subred se une al grupo.

6.4 Arquitectura de codecs.

Un codec es una arquitectura de codificación o de compresión que sirve para codificar el video y audio en bruto. Existen una gran variedad de codecs, algunos son equivalentes entre ellos la única diferencia depende de la compañía que lo haya diseñado. Los codecs se dividen en dos ramas principalmente: codecs de código abierto y de código privado.

Dentro de estas divisiones puede haber dos códec que hagan lo mismo, la diferencia sólo sería que una es de código abierto y el otro sólo lo manejan empresas, y es de su uso exclusivo o en su defecto si alguien quisiera diseñar un sistema para implementarlo, tendría que pagar los respectivos derechos por usarlo.

En los siguientes puntos se mostrarán los códec más usados.

6.4.1 Codecs de código privado.

Hay una amplia variedad de arquitecturas como por ejemplo:

DirectShow, reproductor de medios CD, DVD, web y disco duro, fue desarrollada por Microsoft. Soporta MPEG1, MPEG2, .avi, .mov y otros.

Digital Vídeo, uso primario captura y grabación de vídeo, formato de vídeo de alta calidad, usado en cámaras digitales y tarjetas capturadoras.

Sorenson Vídeo, uso primario Web, vídeo basado en CD, método de compresión VQ (Advanced Vector Quantization), codec QuickTime.

6.4.2 Codecs de código abierto.

MPEG1, uso primario vídeo-CD, web. Buena calidad de imagen en ventanas pequeñas. Los codificadores por hardware permiten la compresión en tiempo real. La compresión por software es lenta.

MPEG2, uso primario TV, DVD y aplicaciones de vídeo de alta calidad y flujo elevado de datos. Basado en MPEG1, pero está optimizado para flujos elevados de datos y calidad de imagen escalable.

H.264, o MPEG-4 parte 10, es un códec digital de alta compresión. El estándar

ITU-T H.264 y el estándar ISO/IEC MPEG-4 part 10 (formalmente ISO/IEC14496-10) son técnicamente idénticos, y la tecnología es conocida también como AVC (codificación de vídeo avanzada).

Estándar que es capaz de proveer de una buena calidad de imagen con bit rates substancialmente menores (p.ej. la mitad o menos) que los estándares previos (p.ej. el MPEG-2, H.263 o MPEG-4 parte 2). Además de no incrementar la complejidad para que el diseño no sea costeable (demasiado caro) de implementar.

Otro objetivo fue que el estándar fuera lo suficientemente flexible para ser aplicado a una gran variedad de aplicaciones (p.ej. para alta y baja resolución de imagen) y para trabajar correctamente en una gran variedad de redes y sistemas (por ejemplo para radiodifusión, almacenamiento DVD, redes de paquetes RTP/IP o sistemas de telefonía multimedia ITU-T).

6.5 Reproductores de Streaming comerciales.

Dentro de las arquitecturas de codec más populares se encuentran: Apple QuickTime, Windows Media de Microsoft y Real Networks. Cada uno cuenta con un grupo de codecs diferentes, también estas arquitecturas forman parte de reproductores, que son compatibles con el flujo de streaming, es decir, que estos reproductores deben de estar instalados del lado del receptor o cliente, recibiendo el flujo de streaming y realizando las funciones que se explicaron en puntos anteriores.

A continuación analizaremos estos reproductores tan populares de streaming y sus propiedades de las cuales destacan la escalabilidad, ya que como mencionamos, de esta propiedad depende que cualquier receptor pueda recibir la transmisión de una forma adecuada, sin importar al ancho de banda con el que el usuario disponga.

6.5.1 Apple quick time.

QuickTime es la arquitectura de software multimedia y multiplataforma de Apple. El soporte inicial para la entrega IP fue por descarga progresiva. Actualmente soporta streaming verdadero, utilizando la estructura RTSP.

Algunas de las características que incluye QuickTime son las siguientes:

Múltiples canales de entrega: www, CD-ROM, DVD, banda ancha, presentaciones.

· Soporta, tanto Mac como Windows.

· Potentes capacidades interactivas.

· Incluye gráficos sincronizados, sonido, vídeo, texto, música, etc., para producciones multimedia.

QuickTime es la arquitectura dominante para el vídeo en CD-ROM. Goza de una cuota de mercado impresionante debido a su soporte de plataforma cruzada, la gran variedad de características y la licencia libre. Por estas razones QuickTime es utilizado en la inmensa mayoría de títulos de CDROM.

En cuanto la escalabilidad QuickTime ofrece la entrega a velocidades múltiples de bit a través de su característica de películas reemplazables. Al comienzo de la reproducción, el Plug-in de QuickTime, solicita una versión alterna de acuerdo a la configuración que el espectador ha configurado en su panel de control del QuickTime setting.

Los creadores de contenido pueden crear tantas alternativas como necesiten cuando estén codificando la película, y pueden especificar criterios complejos para cuando se proyecten versiones particulares. Esto tiene en cuenta la entrega de contenido basada en:

• El ancho de banda de la conexión del usuario.

• La plataforma de reproducción (Mac o Windows).

• La versión QuickTime, ver Figura 6.6.

• El lenguaje o la velocidad de la CPU.

Figura 6.6 Quick Time Player

6.5.2 RealNetworks.

RealNetworks promovió el streaming como un medio de comunicación aprovechable bajo el nombre de Progresive Networks. Antes de que surgiera el reproductor Real, el contenido audiovisual era entregado como una descarga para ser reproducido posteriormente en el disco local.

RealSystem G2 es una arquitectura de streaming desarrollada por RealNetworks que incorpora RealAudio y RealVídeo y está orientada a la red. Es una aplicación RealSystem es más apropiado

para la entrega de audio, vídeo y otros tipos de medios en la red, tales como texto y animaciones Flash. Es menos apropiado para la entrega de CD y DVDS debido a los altos requerimientos de la CPU en mayores anchos de banda. Los archivos Real no pueden ser editados o recomprimidos una vez que han sido codificados en el formato Real.

Los usuarios pueden ver películas RealSystem con RealPlayer, una aplicación cliente libre y disponible desde RealNetwork, ver Figura 6.7. RealSystem soporta SMIL (Lenguaje de Integración y Sincronización de Archivos Multimedia).

La escalabilidad de RealSystem ofrece stream dinámico conmutativo denominado SureStream. Durante la reproducción, el RealPlayer y el RealServer se comunican continuamente y pueden cambiar versiones repetidamente, para entregar el stream a la calidad más alta que la conexión del espectador pueda soportar en cualquier momento. Esta conmutación en tiempo real trata eficazmente las cambiantes condiciones de la red, tales como la congestión.

La conmutación de audio y vídeo es tratada independientemente incluso pudiendo indicar si debería ser el audio o el vídeo, el que tuviera preferencia cuando se reduzca el rendimiento específico del espectador.

Además de la característica del SureStream, el RealPlayer puede también eliminar los cuadros y/o degradar la calidad de imagen para mantener la reproducción en tiempo real sobre conexiones más lentas. Si el ancho de banda disponible desciende mucho, el RealPlayer puede omitir la pista de vídeo completamente y simplemente reproducir la pista de audio.

Figura 6.7 RealNetworks

6.5.3 Windows Media Player.

Windows Media es la solución completa de Microsoft para la entrega de archivos multimedia por Internet. La arquitectura incluye una serie de productos para la codificación, prestación de servicios y distribución.

El reproductor de Microsoft es Windows Media Player. La gestión de derechos permite a los creadores de contenido, establecer un sistema completo para vender o alquilar contenido. También se puede usar para la entrega de vídeos confidenciales.

Windows Media Server ofrece escalado de la velocidad de datos transmitida a través del uso de pistas múltiples de vídeo, denominado “streaming inteligente”. Al comienzo de la reproducción, el Media Player y el Windows Media Server negocian para seleccionar la pista de vídeo que mejor se adecua a la conexión del usuario.

Si la conexión degenera, el servidor enviará automáticamente un stream de vídeo de menor calidad. Si la cantidad de ancho de banda disponible decrece más, el servidor degradará más la

calidad del vídeo, hasta que sólo quede el audio. Esto asegura que el vídeo pueda ser seguido incluso durante la congestión desmesurada.

Para este trabajo elegimos Windows Media Player por las grandes prestaciones que ofrece, además por la gran cantidad de usuarios que ya tienen instalado este reproductor.

Figura 6.8 Windows Media Player

6.6 Windows Media Encoder.

Windows Media Encoder es un programa el cual permite la transmisión de vídeo a través de Internet, este software tiene ciertas ventajas que nos llamaron la atención, las cuales enumeramos a continuación:

1. Se puede descargar gratis desde el sitio oficial.

2. Permite también la transmisión de audio, ya sea vía micrófono (en vivo) o música de fondo para amenizar la transmisión (grabación).

3. Permite utilizar cualquier cámara que se pueda conectar a la PC, que hoy en día puede ser cualquier tipo de cámara que en general van desde cámaras Web, mini cámaras espía inalámbricas hasta cámaras semiprofesionales y profesionales (ver punto 2.2).

4. Permite seleccionar la calidad del vídeo, lo que permitirá que dependiendo de la velocidad de nuestra conexión elegir la calidad más adecuada, es decir la mejor calidad posible, lo que nos dice que tiene una buena escalabilidad (ver punto 6.1.2).

5. Permite integrar lo que está capturando en la página Web de una manera sencilla.

6. No se necesita instalar un Pulg-in extra en nuestro explorador, lo único que se necesita para reproducir el vídeo es el Windows Media Player instalado en tu sistema, el cual la mayoría de las PC's lo incluye.

Figura 6.9 Windows Media Encoder

6.6.1 Codificación CBR.

La codificación CBR ofrece mejores resultados al trabajar con la transmisión por secuencias. En ella, la velocidad de bits se mantiene bastante constante y similar a la velocidad de bits final durante toda la secuencia, dentro de un período reducido determinado por el tamaño del búffer.

La desventaja es que la calidad del contenido codificado no es constante. Dado que algunos fragmentos del contenido son más difíciles de comprimir que otros, algunas partes de una secuencia CBR son de menor calidad.

Además, la codificación CBR proporciona una calidad desigual de una secuencia a otra. En general, las variaciones en la calidad son más pronunciadas al utilizar velocidades de bits inferiores.

6.6.2 Codificación VBR.

La codificación VBR es más ventajosa cuando se codifica contenido que es una mezcla de datos simples y complejos. Por ejemplo, un vídeo que cambia entre cámara lenta y cámara rápida.

Con la codificación VBR, se asignan automáticamente menos bits a partes menos complejas del contenido, dejando bits suficientes disponibles para producir una buena calidad para partes más complicadas. Esto significa que el contenido que tiene una complejidad consistente (por ejemplo, una noticia del telediario) no se beneficiaría de la codificación VBR. Cuando se utiliza con contenido mezclado, la codificación VBR produce un resultado codificado mejor, tratándose del mismo tamaño de archivo al compararlo con la codificación CBR.

En algunos casos, puede terminar obteniendo un archivo codificado mediante VBR, que tenga la misma calidad que un archivo codificado mediante CBR con la mitad de tamaño de archivo.

6.7 Transmitiendo vídeo con Windows Media Encoder.

Una vez que mencionamos las ventajas del WME (Windows Media Encoder), procedemos ahora a describir como implementarlo en nuestro proyecto:

1. En este primer punto incluimos los primeros pasos a seguir. Cabe destacar que estos pasos son sencillos, pero importantes para nuestro objetivo. A continuación se mencionan dichos pasos: conectar la cámara a la PC, instalar y abrir el WME, colocar la cámara en un lugar adecuado (donde esté segura y que tenga el mejor ángulo para cubrir el evento).

2. Una vez que se abre el programa, inmediatamente aparece una ventana como la que se muestra en la figura 6.6 seleccionamos “Broadcast a live event”, que es la que está seleccionada en la imagen, y damos clic en aceptar.

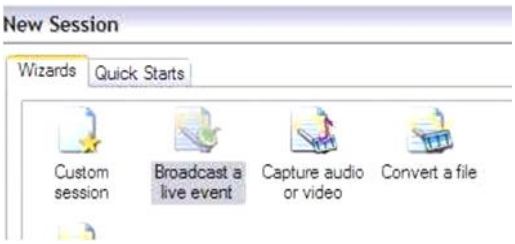


Figura 6.6 Crear una sesión.

3. Después elegiremos la fuente de vídeo así como la de audio, esto se logra a través de la ventana que se muestra en la figura 6.7. Todos los dispositivos de captura que estén instalados en nuestra PC, se desplegarán. Entonces seleccionamos los dispositivos deseados y pulsamos siguiente.

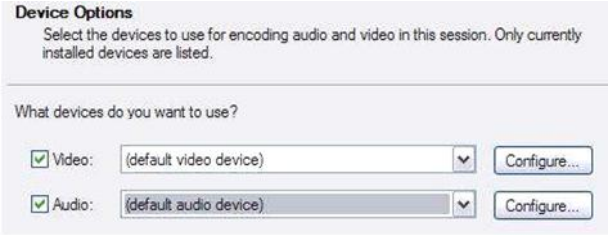


Figura 6.7 Dispositivos de captura.

4. A continuación se muestra la siguiente ventana (figura 6.8) y seleccionamos la opción que se muestra en la figura, que es la de "Pull from the encoder", con esta opción los usuarios verán la transmisión directamente.

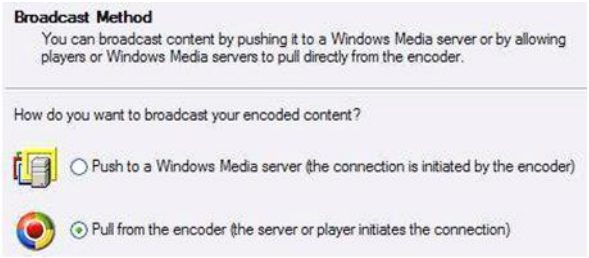


Figura 6.9 Método de broadcast

5. Luego definiremos el puerto que utilizaremos para la transmisión. Usualmente podemos utilizar el puerto "8080" que es el estándar, pero si requerimos de otro puerto podemos utilizar la opción de "Find free port" para encontrar otra alternativa. En el campo "URL for Internet connections" nos muestra la IP publica por la cual los usuarios accederán a nuestra transmisión. El campo "URL for LAN connections" nos indica la IP privada por la cual se accederá a la transmisión dentro de nuestra Intranet, la cual solo la podrán ver los equipos dentro de ésta.

Figura 6.10 Direcciones IP de la transmisión.

6. A continuación debemos seleccionar el tipo de codificación que tendrá el audio y vídeo de nuestra transmisión. Hay una gran variedad de opciones para seleccionar y todas dependerán de la capacidad de transmisión que tengamos. Para aprovechar la escalabilidad que nos ofrece este software, debemos de seleccionar la opción "Multiple bit rates video (CBR)". Con la cual los usuarios con diferentes velocidades de conexión podrán recibir la transmisión.

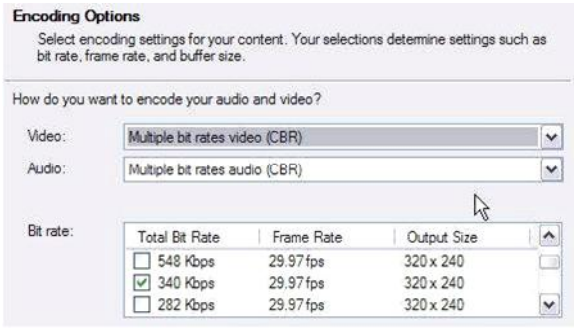


Figura 6.11 Opciones de compresión.

7. La siguiente ventana nos da la opción de guardar lo que se transmite, esto es muy útil, ya que no todo el tiempo estaremos viendo la transmisión remotamente y si quisiéramos ver lo que sucedió a lo largo del día, podríamos consultarlo en el archivo correspondiente. Sólo tenemos que indicar la ruta en donde queremos guardarlo.

8. Enseguida tenemos que escoger entre otras opciones, tales como incluir un vídeo de inicio y de fin. Como su nombre lo indica cuando un usuario se enlace para recibir la transmisión, lo primero que verá será este vídeo, como introducción. Algo similar sucederá cuando el usuario decida ya no recibir la transmisión, entonces se reproducirá el vídeo de fin a manera de despedida.

Cabe mencionar que estos vídeos deben de tener una duración corta que no vaya más allá de los 20 segundos, esto para que el usuario no pierda el interés en la transmisión debido a una presentación demasiada larga.

9. Otra opción que se brinda es la de llenar un formulario con el titulo de la transmisión, autor, derechos de autor, descripción, etc.

10. Por último surge una ventana donde se muestran un resumen las opciones elegidas previamente y le damos clic en finalizar.

11. Ahora sólo damos clic en “comenzar” para iniciar la transmisión de video a través de Internet.

Cabe mencionar que de los puntos 7,8 y 9 son meramente opcionales, no habría ningún problema para transmitir si nos lo saltásemos, o hablando específicamente del programa si les pusiéramos siguiente, no afectaría de ninguna manera a nuestra transmisión.

Otro aspecto resaltar, es que en el parámetro de la dirección también tenemos que incluir el número del puerto por el cual se está transmitiendo. Esto se muestra en el ejemplo anterior donde podemos ver que se puso el puerto 8080 que coincide con el asignado en la figura 6.10.

Por último la página en la que incrustemos el objeto Active-X, con los parámetros bien configurados, tenemos que guardarla en la carpeta del servidor. Ahora cuando un usuario entre a nuestra página podrá ver la transmisión del evento, ya sea en la página principal o en la parte de nuestro sitio donde más nos convenga.

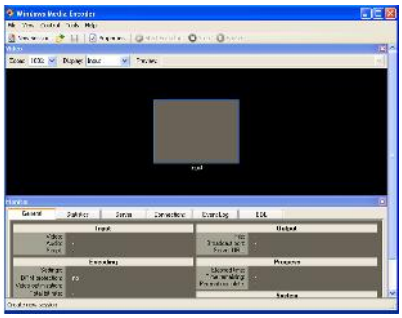


Figura 6.12 Windows Media Encoder

CAPÍTULO 7

Configuracion de la Videoconferencia desde el Centro de Monitoreo.

Hoy en día es posible, sin necesidad de grandes gastos, vigilar su hogar ó su negocio a través de internet, bien a través de un ordenador ó de un teléfono móvil 3G, la condición indispensable es que dispongamos de una línea ADSL y algunos conocimientos básicos de informática.

A continuación de describirán los pasos a seguir para la implementación de nuestro sistema antes mencionado para la realización del monitoreo desde una unidad móvil y el uso de una dirección IP dinámica.

Para el ahorro de tiempo y costo se utilizara el mismo Software que nos proporciona el Proveedor de las Cámaras IP (Vivotek).

Así mismo podemos obtener una amplia gama de utilidades para el desarrollo de nuestro monitoreo como podemos detallarlo a continuación:

Al cambiar a la nueva tecnología es interesante conocer algunas de las diferencias claves entre ellas:

-Interlacing. La tecnología análoga aun operando a 4CIF tiene problemas importantes de interlacing que produce imágenes borrosas de objetos en movimiento. Una cámara IP puede escanear progresivamente objetos en movimiento más claramente porque no usa líneas separadas para reproducir las imágenes.

-Energía. Energizar las cámaras análogas puede ser costoso y problemático. Primero debe instalar el cable coaxial para transportar el video y luego proveer el cableado eléctrico para energizar cada cámara. Las cámaras IP pueden operar usando un único cable para recibir la energía y transmitir el video (PoE).

-Protección Eléctrica. Una ventaja adicional de usar cámaras con PoE que muchas veces no es tomada en cuenta es el hecho de que la protección contra problemas eléctricos puede realizarse con un costo más efectivo y simple que si usara cámaras análogas. Tradicionalmente las cámaras análogas requieren disponer de una fuente de energía local para cada una por lo que proveer protección eléctrica para cada cámara puede ser muy costoso. En contraste, las cámaras IP con PoE reciben la energía inyectada a través del mismo cable UTP que se conecta al switch de datos en us Data Center donde están instalados sus UPS.

-Resolución. Las cámaras análogas no pueden proveer una resolución mayor a los estándares de los televisores de 0.4 mega-pixeles a 4CIF. Muchos equipos análogos usan una resolución aún menor (0.01 mega-pixeles) por restricciones de costo y tecnológicas.

Las cámaras IP pueden proveer resoluciones de hasta 15 veces la calidad de video análogo. Las últimas cámaras IP pueden ofrecer video con un índice de transferencia de 7Mbits/s.

-Inteligencia. La tecnología de video IP permiten que las cámaras incluyan un rango mayor de funciones. Por ejemplo, las cámaras pueden ser programadas para grabar solo cuando detectan movimiento reduciendo enormemente el tráfico de data. Adicionalmente ofrecen compensación contra la luz solar y la iluminación posterior de objetivos, tecnología de lentes duales, grabación digital interna, audio y análisis de video.

El video IP es una tecnología probada que tiene muchas ventajas sobre los tradicionales sistema análogos de video. La tecnología IP es fácil de mejorar y expandir. Con las nuevas tecnologías en desarrollo la vigilancia por video IP serán más "inteligentes" y con mayor retorno de inversión. El costo total de sistemas de video IP, incluyendo cámaras, cables y grabación es considerablemente menor que los análogos.

Nosotros ofrecemos una enorme variedad de soluciones para cada posible necesidad. Desde el levantamiento y diseño hasta la implementación y puesta en marcha.

7.1 ¿Cómo, donde, y a que se conectan las cámaras IP?

Se puede desglosar la conectividad que utilizaremos de la siguiente manera:

Utilizaremos un Servidor para administrar todas las conexiones (Cámaras IP) a través de una Dirección IP Dinámica.

1 Hub o un Router si se desea realizar mas conexiones entre 1, 2 o más servidores.

1 Modem inalámbrico para obtener el servicio de Internet y de esta manera establecer la conexión entre las cámaras y el servidor.

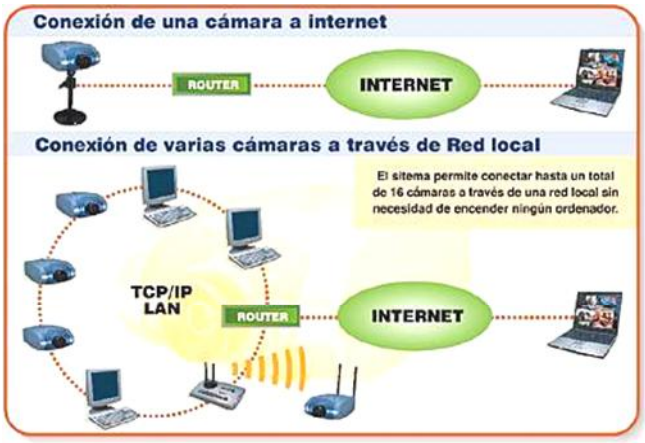


Figura 7.1 Conexión de una Cámara e Internet

Realizando este tipo de conexión podemos realizar una serie de preguntas como las que se describen a continuación:

¿Qué es necesario para utilizar cámaras ip?

Las cámaras ip actualmente se pueden instalar en cualquier sitio que disponga de conexión a Internet mediante Router ADSL o XDSL (Con dirección IP fija, aunque algunos modelos también permiten IP dinámica), incluso otros modelos de cámaras ip permiten que esa conexión no sea permanente y que cuando sea necesaria se pueda realizar por medio de un Modem convencional a la línea telefónica básica.

¿Cómo son internamente las cámaras ip?

Las cámaras ip internamente están constituidas por la "cámara" de Vídeo propiamente dicha (Lentes, sensor de imagen, procesador digital de señal), por un "motor" de compresión de imagen (Chip encargado de comprimir al máximo la información contenida en las imágenes) y por un ordenador" en miniatura (CPU, FLASH, DRAM, y módulo ETHERNET/ WIFI) encargado en exclusiva de gestionar procesos propios, tales como la compresión de las imágenes, el envío de imágenes, la gestión de alarmas y avisos, la gestión de las autorizaciones para visualizar imágenes, en definitiva, las cámaras ip son un equipo totalmente autónomo, lo que permite conectarlo en el caso mas sencillo directamente a un Router ADSL, y a la red eléctrica y de esta forma estar enviando imágenes del emplazamiento donde este situada.

También es posible conectar las cámaras ip como un equipo más dentro de una Red Local, y debido a que generalmente las redes locales tienen conexión a Internet, saliendo de esta forma las imágenes al exterior de la misma manera que lo hace el resto de la información de la Red.

¿Qué aplicaciones tienen las cámaras ip?

Algunas de las aplicaciones más frecuentes de las cámaras ip son la vigilancia de:

- Viviendas, permitiendo visionar la propia vivienda desde la oficina, desde un hotel, cuando estamos de vacaciones.

- Negocios, permitiendo controlar por ejemplo varias sucursales de una cadena de tiendas, gasolineras.

- Instalaciones industriales, almacenes, zonas de aparcamiento, Muelles de descarga, accesos, etc., incluso determinados procesos de maquinaria o medidores.

- Hostelería, Restauración, Instalaciones deportivas.

- Lugares Turísticos, cada día es mas frecuente que Organismos oficiales, como Comunidades Autónomas, Ayuntamientos, promocionen sus zonas turísticas, o lugares emblemáticos de las ciudades, instalaciones deportivas, etc., implementado en sus páginas Web las imágenes procedentes de cámaras ip estratégicamente situadas en esos lugares.

Estas son resumidas algunas de las aplicaciones cámaras ip con mas demanda.

¿Qué ventajas tiene las cámaras ip frente a los sistemas de vigilancia CCTV tradicionales?

Las cámaras ip poseen muchas ventajas frente a los sistemas tradicionales de vigilancia mediante Circuito Cerrado de TV (CCTV), las fundamentales son:

- Acceso Remoto: La observación y grabación de los eventos no tiene por que realizarse "in situ" como
requieren los sistemas CCTV.

- Costo reducido: La instalación es mucho más flexible ya que se basa en la infraestructura de la Red Local existente o nueva, o también en la conexión directa a un Router, bien por cable o de forma inalámbrica (Wireless LAN).

Se elimina el costo de los sistemas de grabación digital de los CCTV, ya que las grabaciones de las cámaras ip se realizan en el disco duro de un PC de la propia red local o en un PC remoto.

- Flexibilidad frente a la ampliación del sistema: Los sistemas tradicionales CCTV generalmente requieren duplicar los sistemas de monitorización cuando se amplia el sistema, los sistemas de cámaras ip permiten su ampliación sin necesidad de invertir en nuevos sistemas de monitorización.

¿Es posible transformar el sistema de vigilancia CCTV existente en un sistema de cámaras ip?

Sí, es posible convertir un Sistema de Vigilancia CCTV en cámaras ip, mediante los Servidores de Vídeo IP.

Un Servidor de Vídeo es una de las partes integradas en el interior de una cámara ip. El Servidor de Vídeo internamente está constituido por uno o varios "conversores" Analógico-Digitales (Chip que pasa la señal de vídeo analógica de las cámaras a formato digital), "motor" de compresión de imagen Chip encargado de comprimir al máximo la información contenida en las imágenes), y por un "ordenador" en miniatura (CPU, FLASH, DRAM, y módulo ETHERNET) encargado en exclusiva de gestionar procesos propios, tales como la compresión de las imágenes, el envío de imágenes, la gestión de alarmas y avisos, la gestión de las autorizaciones para visualizar imágenes, ... en definitiva es un equipo totalmente autónomo, lo que permite conectarlo, en el caso mas sencillo directamente a un Router ADSL, y a la red eléctrica y de esta forma poder enviar imágenes del sistema tradicional de CCTV.

¿Es posible en un sistema de cámaras ip disponer de los controles de movimiento de las cámaras, como en los sistemas CCTV tradicionales?

Sí, es posible controlar las cámaras ip como en los Sistema de Vigilancia CCTV tradicionales.

Dentro de la gama de cámaras ip existe una gran variedad en función de la aplicación que le vaya a dar, en general existen cámaras Fijas y Cámaras con movimiento. Las Cámaras "Pan-Tilt" (P/T) así llamadas por disponer de posibilidad de movimiento Horizontal y Vertical, permiten crear un

sistema de vigilancia con gran cobertura y gran flexibilidad, ya que en muchas ocasiones pueden sustituir a varias cámaras fijas.

La visualización de las cámaras ip con movimiento y el manejo de las mismas se puede realizar a distancia mediante el Internet Explorer, simplemente tecleando la dirección IP privada ó pública de las cámaras ip en función de que se visualicen desde la LAN ó la WAN.

Inmediatamente será solicitado introducir el Nombre de Usuario y Contraseña, y esto dará paso a la visualización de las imágenes. En la pantalla de visualización estarán presentes las herramientas de software que permiten girar la cámara, llevarla a la posición preestablecida etc.

¿Es posible conectar sensores externos de alarma a las cámaras ip?

Sí, es posible conectar sensores de alarma externos a las cámaras ip, todas las Cámaras y Servidores de Vídeo disponen de entradas para conectar opcionalmente Sensores Externos complementarios a los sistemas que incluyen de fabrica, por ejemplo detectores PIR convencionales para poder cubrir la detección de movimiento que pudiera provenir de ángulos no cubiertos por la cámara.

En general las cámaras ip así como los servidores de Vídeo disponen un complejo sistema de detección de movimiento mediante el análisis instantáneo y continuado de las variaciones que se producen en los fotogramas de vídeo que registra el sensor óptico. Este sistema permite graduar el nivel de detección de movimiento en la escena, y por ejemplo poder discriminar si en la escena ha entrado un “coche” o un “peatón”, incluso en algunos modelos es posible generar distintas áreas dentro de la escena, y cada una con distinta sensibilidad al movimiento.

¿Es posible accionar dispositivos de forma remota desde las cámaras ip?

Sí, es posible la conexión de un relé que maneje por ejemplo el encendido de luces, o por ejemplo la apertura de una puerta. Las cámaras ip y Servidores de Vídeo disponen de una salida Abierto-Cerrado, que se controla desde el software de visualización.

¿Es posible situar las cámaras ip en exteriores?

Las cámaras ip, y en general todas las cámaras de TV. Están diseñadas para su uso en interiores, en condiciones normales de polvo y humedad y temperatura.

Para la utilización de las cámaras ip o de las cámaras de TV en exteriores o en interiores donde las condiciones de trabajo sean extremas, es necesario utilizar Carcasas de Protección adecuadas a la utilización que se le vaya a dar. Existe gran variedad de carcasas, Estancas, con Ventilación, con Calefacción, Metálicas, de Plástico, cada aplicación aconsejará la elección del modelo adecuado.

¿Qué protección tiene el acceso a las cámaras ip?

Las cámaras ip y los Servidores de Video disponen en su software interno de apartados de seguridad que permiten en general establecer diferentes niveles de seguridad en el acceso a las mismas. Los Niveles son:

Administrador: Acceso mediante Nombre de usuario y Contraseña a la configuración total de la cámara.

Usuario: Acceso mediante Nombre de usuario y Contraseña a la visualización de las imágenes y manejo
del relé de salida.

Demo: Acceso libre a la visualización sin necesidad de identificación.

¿Cuántos usuarios se pueden conectar simultáneamente a las cámaras ip?

El número de observadores simultáneos que admiten las cámaras ip y los servidores de Vídeo en general es de alrededor de 10 a 20. También es posible enviar "snapshots" de forma automática y con periodo de refresco de pocos segundos, a una página Web determinada para que el público en general pueda acceder a esas imágenes.

¿Es posible transmitir Audio desde cámaras ip?

En general la mayoría de las cámaras ip disponen de micrófonos de alta sensibilidad incorporados en la propia cámara, con objeto de poder transmitir audio mediante el protocolo de conexión UDP.

¿Qué sistemas de compresión de vídeo utilizan las cámaras ip?

El sistema de Compresión de Imagen que utilizan las cámaras ip tiene como objetivo hacer que la información obtenida del sensor de imagen, que es muy voluminosa, y que si no se tratara adecuadamente haría imposible su envío por los cables de la red Local o de las líneas telefónicas, ocupe lo menos posible, sin que por ello las imágenes enviadas sufran deterioro en la calidad o en la visualización.

En definitiva los sistemas de compresión de imagen tienen como objetivo ajustar la información que se produce a los anchos de banda de los sistemas de transmisión de la información como por ejemplo el ADSL. Los estándares de compresión actuales son el MJPEG y MPG4, este último es el más reciente y potente.

¿Es necesario algún software específico para el acceso a las cámaras ip?

Para la visualización de las cámaras ip lo único que se necesita es que en el sistema operativo del PC se encuentre instalado el Microsoft Internet Explorer, mediante el mismo tendremos acceso a la dirección propia de la Cámara de Red, que nos mostrará las imágenes de lo que en ese momento este sucediendo. Esto resulta extremadamente útil, ya que permitirá poder visualizar la cámara desde cualquier ordenador, en cualquier parte del mundo, sin necesidad de haber instalado un software especifico.

No obstante, con las cámaras ip se adjunta un software de visualización de hasta 4 cámaras, permitiendo la visualización simultánea de las mismas, el control, la administración,... y por supuesto la reproducción de los videos que se hayan grabado mediante grabación programada, o como consecuencia de alarmas.

7.2 Configuración de la Cámara de Vivotek.

Los requisitos en los que nos hemos basado para la elección de la cámara han sido:

- Que pueda trabajar con IP dinámica ó estática, ya que en los hogares las líneas

ADSL contratadas llevan IP dinámica.

- Que sea para interior y tipo “Domo” para colocar en techo ó, pared,

- Que lleve algún sistema que nos permita ver de noche.

- Que nos permita recibir también audio

- Que pueda detectar intrusión y activar alguna luz ó sistema para intentar inquietar al intruso, a la vez que nos envía un correo con las imágenes de la intrusión.

- Que nos permita verla a través de un PC ó un teléfono móvil con tecnología 3G

- Y sobre todo que tenga una gran relación calidad/precio

Figura 7.2 Configuración de la Cámara de Vivotek

7.3 Descripción física de la cámara.

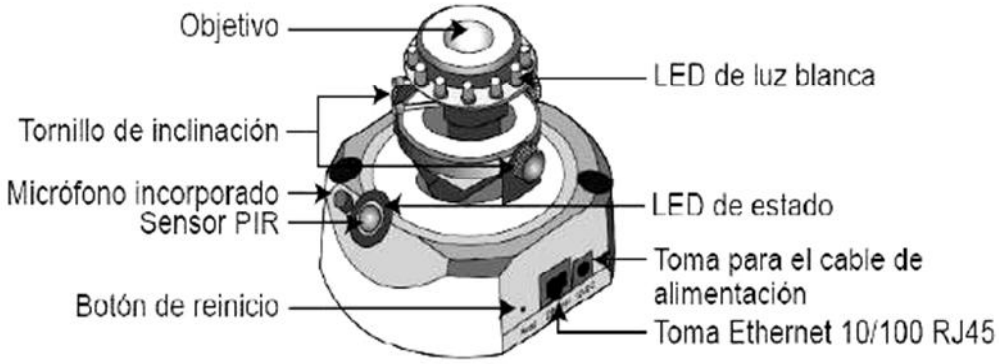


Figura 7.3 Descripción física de la cámara

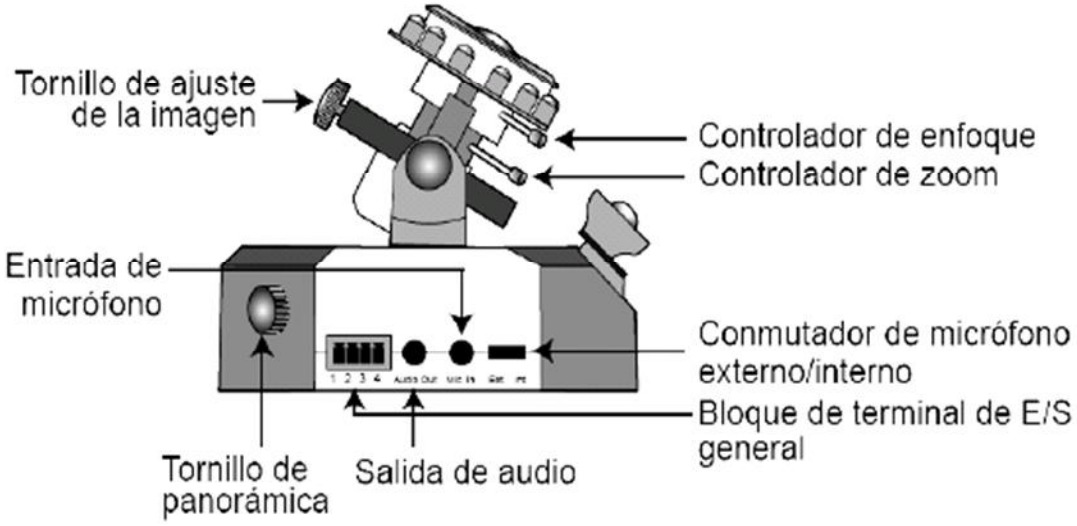


Figura 7.4 Descripción física de la cámara

7.4 Instalación hardware.

Empezaremos por la instalación física de la cámara que es muy sencilla. Para ello lo primero que debemos hacer es elegir la zona o zonas que queremos vigilar teniendo en cuenta el lugar más adecuado para nuestras necesidades.

La ubicación y colocación de la cámara no es muy compleja pero debe ser estudiada para conseguir una buena captura y un buen enfoque, y además hay que tener presente que el sensor PIR incorporado está diseñado para su activación cuando una persona entre en su rango de detección. Por lo tanto, resulta esencial instalar la cámara en un lugar donde el sensor PIR éste dirigido hacia la dirección que se desee. De ante mano saber que la sensibilidad de un detector PIR se rige por el tamaño del objeto y la diferencias de temperatura entre el objeto y el entorno como lo podemos observar en la Figura 7.5.1.

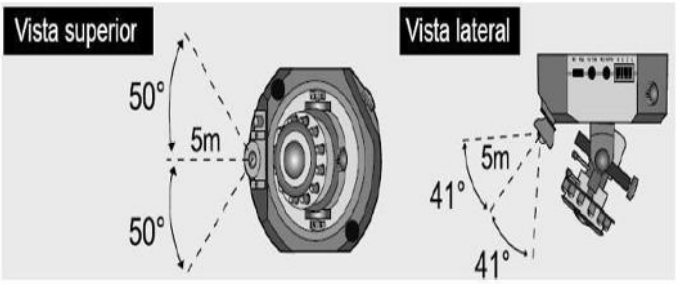


Figura 7.5.1. Vistas de la Cámara Vivotek

Empezaremos por desmontar la cubierta del domo usando el destornillador suministrado con la cámara. Tenemos dos opciones para montarla, tanto en techo como pared debido a que como ya sabemos, ésta cámara tiene posicionamiento triaxial, con lo cual podremos bascularla en tres diferentes ejes como se muestra en la Figura 7.5.2.

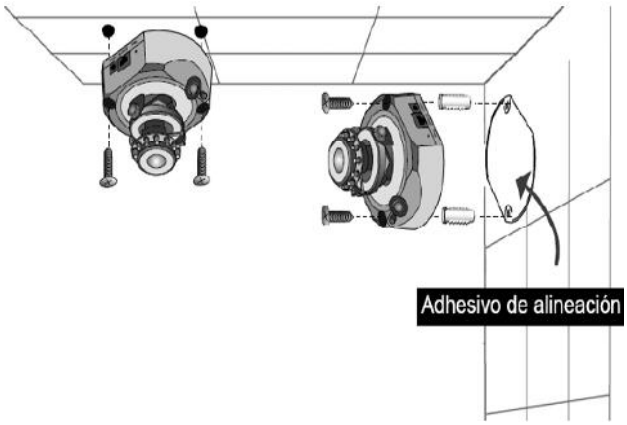


Figura 7.5.2. Opciones de montaje de nuestra Cámara IP

7.5 Conexión general de una cámara.

Hay varias formas de cómo conectar la cámara a Internet para poder acceder a ella desde cualquier lugar del mundo. A continuación realizaremos la conexión básica.

Conectaremos la cámara mediante un cable Ethernet al hub/ switch o directamente al router.

Conectaremos el adaptador jack de la fuente de la alimentación a la cámara, antes de enchufar la fuente de alimentación a la red eléctrica. Así evitaremos accidentes eléctricos como se muestra en la Figura 7.6.

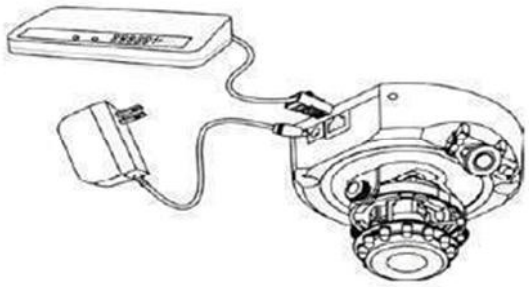


Figura 7.6. Conexión general de una Cámara

También deberíamos tener en cuenta que hay otra forma de conectar a Internet ciertos modelos, la cual sería mediante tecnología de conexión WIFI en la cual no es necesario el cable Ethernet para transmitir datos, aunque la cámara de Vivotek con la que estamos trabajando en concreto no sería una de ellas.

Para poder llevar a cabo este tipo de conexión es necesario disponer de un router WIFI con una buena potencia de emisión/ recepción de antena, al cual conectaremos la cámara inalámbricamente vía WIFI. Todas las cámaras WIFI de Vivotek incorporan antenas pero en ciertas ocasiones y dependiendo de donde ubiquemos estas cámaras necesitaremos ampliar la cobertura instalando una antena externa de más alcance que la que trae por defecto.

Ya tenemos nuestra cámara orientada hacia el lugar que queremos vigilar e instalada físicamente y sólo nos queda configurarla y examinar la opciones de vigilancia que nos ofrece este modelo.

7.6 Wi-Fi.

El router inalámbrico más popular es el WiFi por ser el más utilizado para acceder a Internet desde cualquier lugar donde haya un punto de acceso (Access Point o AP), sobre todo en portátiles y PDAs con tarjeta WiFi. También conocido como 802.11, es el dispositivo que reúne el conjunto de estándares para la WLAN (Wireless Local Area Network - red de área local inalámbrica). El estándar IEEE 802.11 es una frecuencia de radio desarrollado por el IEEE (Institute of Electrical and Electronics Engineers - Instituto de Ingenieros Eléctricos y Electrónicos), y la mayoría de los sistemas operativos lo soportan, así como muchos de los portátiles, celulares/móviles de última generación, consolas, impresoras y otros periféricos.

Los tipos de comunicación WIFI se basan en las diferentes clases de estándares IEEE, siendo la mayoría de los productos de la especificación b y de la g:

802.11a*, *802.11b*, *802.11g*, *802.11n

802.11a.

Emite a una velocidad de 54 Mb/seg (megabytes por segundo)

Volumen de información (Throughput) de 27 Mb/seg

Banda de frecuencia de 5 GHz

El IEEE creaba en 1997 el estándar 802.11 con velocidades de transmisión de 2Mb/seg, hasta que en 1999 desarrollaron el estándar 802.11a que era una revisión del estándar original y que utiliza el mismo juego de protocolos de base que este. También llamado WiFi 5, el estándar 802.11a opera en la banda de 5 GHz que está menos congestionada y utiliza la modulación OFDM (orthogonal frequency-division multiplexing) con 52 subportadoras, lo que le infiere dos notables ventajas respecto al 802.11b: incrementa la velocidad máxima de transferencia de datos por canal (de 11 Mbps a 54 Mbps) y aumenta el número de canales sin solapamiento.

Pero el uso de esta banda también tiene sus desventajas, puesto que restringe el uso de los equipos 802.11a sólo a puntos en línea de vista, siendo necesario la instalación de un mayor número de puntos de acceso 802.11a para cubrir la misma zona; debido a esto las ondas no pueden penetrar tan lejos como los del estándar 802.11b, ya que estas son más fácilmente absorbidas por las paredes y otros objetos sólidos en su camino pues su longitud de onda es menor.

802.11b.

Emite a una velocidad de 11 Mb/seg

Volumen de información (Throughput) de 5 Mb/seg

Banda de frecuencia de 2,4 GHz

Uno de los más usados, desarrollado en 1999, es una extensión directa de la técnica de modulación definida en el estándar original 802.11. Su espectacular incremento en throughput (volumen de información que fluye a través de las redes de datos) comparado con el estándar original junto con sustanciales reducciones de precios ha llevado a la rápida aceptación de 802.11b como la tecnología inalámbrica LAN definitiva.

Como desventaja los dispositivos 802.11b sufren interferencias de otros productos operando en la banda 2.4 GHz, como pueden ser hornos microondas, dispositivos Bluetooth, monitores de bebés y teléfonos inalámbricos. Por otro lado, los productos de estándar 802.11b no son compatibles con los productos de estándar 802.11a por operar en bandas de frecuencia distintas.

802.11g.

Emite a una velocidad de 54 Mb/seg

Volumen de información (Throughput) de 22 Mb/seg

Banda de frecuencia de 2.4 GHz

Desarrollado en 2003, el 802.11g es el tercer estándar de modulación y la evolución del 802.11b, es además el más usado en la actualidad. Los productos IEEE 802.11g poseen un alto grado de compatibilidad con versiones anteriores pues trabaja en la banda de 2.4 GHz como 802.11b, pero usa el mismo esquema de transmisión basado en OFDM como 802.11a, utilizando 48 subportadoras.

802.11g fue rápidamente adoptado por los consumidores en Enero de 2003, antes de su ratificación en Junio, debido al deseo de velocidades de transmisión superiores y reducciones en los costes de fabricación. Para el verano de 2003, la mayoría de los productos de doble banda 802.11a/b pasaron a ser dual-band/tri-mode (doble banda/tres modos), esto quiere decir que pueden funcionar en la banda de 2.4 GHz o de 5 GHz y en cualquiera de los tres modos aceptados por la IEEE: el a, b y g.

Como el estándar 802.11b, los dispositivos de estándar 802.11g les afectan las interferencias de otros productos operando en la banda de 2.4 GHz.

802.11n.

Emite a una velocidad de 600 Mb/seg

Volumen de información (Throughput) de 144 Mb/seg

Bandas de frecuencia: 2,4 GHz y 5 GHz

El estándar 802.11n (todavía en desarrollo) es una ratificación que mejora los previos estándares 802.11 añadiendo la tecnología MIMO que son antenas Multiple-Input Multiple-Output, unión de interfaces de red (Channel Bonding), además de agregación de marco a la capa MAC.

Channel Bonding, también conocido como canal 40 MHz, puede usar simultáneamente dos canales separados no superpuestos de 20 MHz, lo que permite incrementar enormemente la velocidad de datos transmitidos.

Uso simultáneo de las bandas de frecuencia de 2,4 GHz y de 5,4 GHz que hace que sea compatible con dispositivos basados en todas las ediciones anteriores de Wi-Fi.

La velocidad real de transmisión se prevé que podría llegar a los 600 Mbps, que es 10 veces más rápida que bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que bajo el estándar 802.11b.

Se espera que 802.11n se apruebe por la IEEE-SA RevCom en noviembre de 2009, aunque ya hay dispositivos que ofrecen de forma no oficial éste estándar.

7.7 Instalación software.

Antes de instalar el software de la aplicación, asegúrese de que el sistema cumpla los siguientes requisitos mínimos necesarios:

1.- Espacio máximo en disco duro que se admite 200 GB es el espacio máximo en disco duro que se ha comprobado que se admite.

2.- No se puede garantizar el rendimiento si el espacio en disco duro para la grabación es superior a los 200 GB. En sistemas Windows XP, cierre la restauración del sistema.- En Windows XP, la restauración del sistema le ayudará a volver al último punto de restauración que grabó una instantánea del equipo. Sin embargo, cuando se activa la restauración del sistema, la E/S del disco será mucho peor. Por lo tanto, la grabación de nuestra aplicación se vería drásticamente afectada. Por tanto, recomendamos desactivar la restauración del sistema para el disco de grabación de la aplicación. Puede hacerlo en la página Propiedades del sistema (Inicio \ Panel de control \ Sistema \ Restaurar sistema), como se muestra en la figura 7.7.

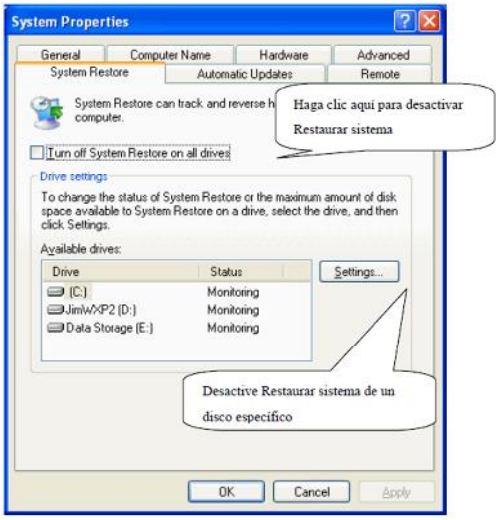


Figura 7.7 Restaurar sistema

PASO 1: Inserte el disco de instalación en la unidad de CD-ROM; la instalación debe iniciarse de manera automática. Si no es así, haga clic en "Inicio" en el vértice inferior izquierdo de la pantalla, abra "Mi PC" y haga doble clic en el icono del CD-ROM.

Aparecerá la ventana de instalación de la grabadora de vigilancia IP como en la siguiente Fig. 7.7.1.

Figura 7.7.1. Ventana de instalación de la grabadora ST3402 Smart VS-IP

PASO 2: En esta página aparecen los enlaces Quick Guide (Guía rápida), User's Manual (Manual del usuario), Release Note (Nota de la versión) e Install Software DVR (Instalar software DVR). Haga clic en "Install Software DVR" para iniciar el programa de instalación. Aparecerá InstallShield Wizard (Asistente de InstallShield) como se muestra en la Figura 7.7.2.

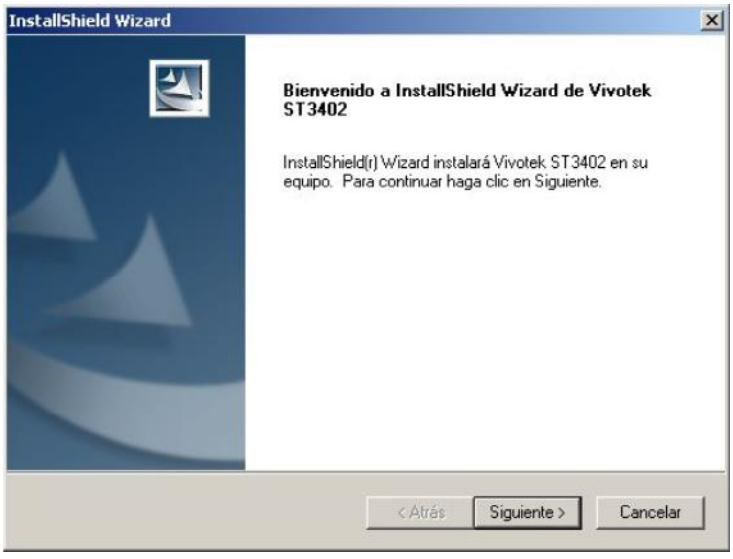


Figura 7.7.2. Página de bienvenida a Vivotek ST3402

PASO 3: Si hace clic en “Siguiente” y aparece la Figura 7.7.3, significa que ha instalado una versión anterior del software de grabación (la versión anterior es de sólo vídeo, por lo que no puede obtener secuencias de audio de los servidores). Si desea conservar la versión anterior, elija la segunda opción. Si es la primera vez que instala el software de grabadora Smart VS-IP, esta ventana no aparecerá; vaya al Paso 4.

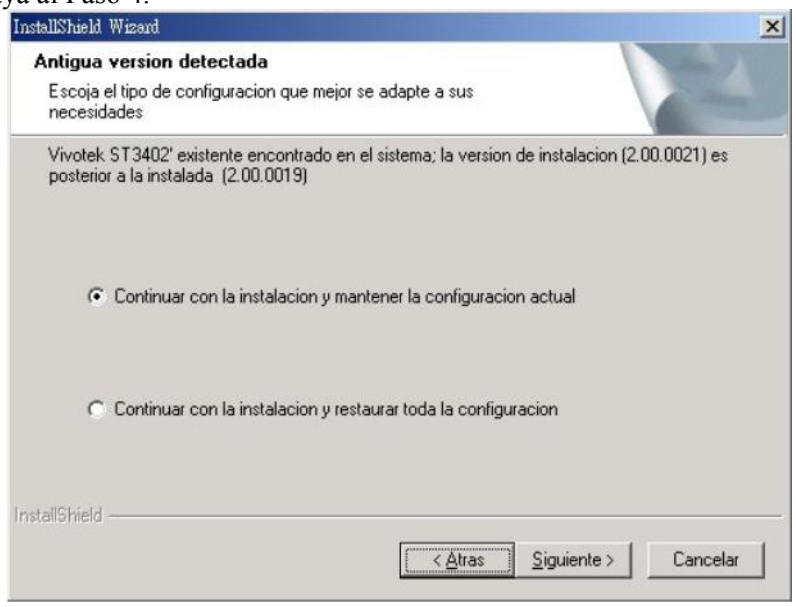


Figura 7.7.3. Se ha detectado una versión sólo de vídeo

PASO 4: Haga clic en “Siguiente” y aparecerá la ventana “Información del usuario” como en la Figura 7.7.4. Esta ventana le solicita que especifique un nombre de usuario y el nombre de la organización. Haga clic en “Siguiente” para continuar.

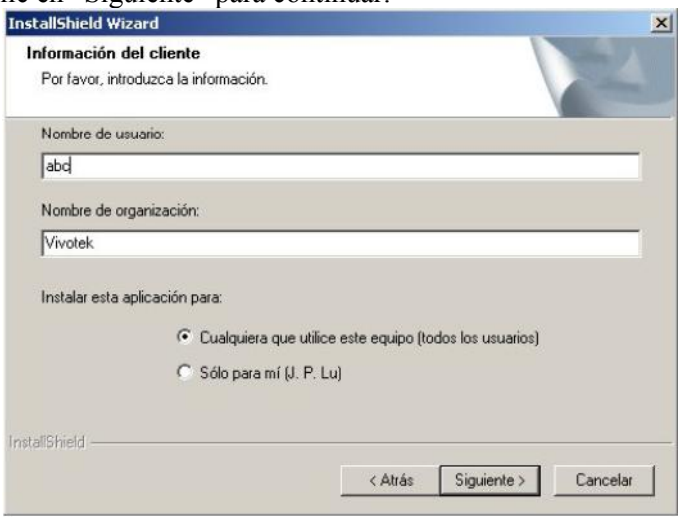


Figura 7.7.4. Información del usuario para la grabadora Smart VS-IP

PASO 5: Configure la contraseña del administrador especificando una contraseña y confirme la contraseña como se indica en la Figura 7.7.5. Haga clic en “Siguiente” para continuar.

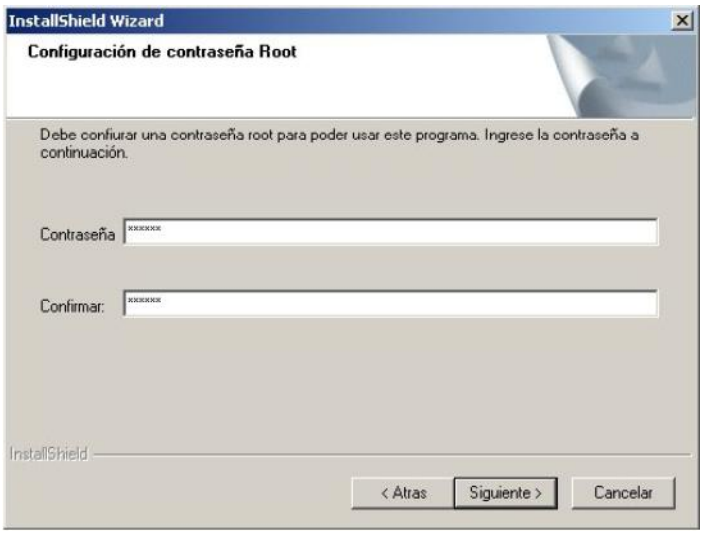


Figura 7.7.5. Confirmar contraseña

PASO 6: Seleccione el directorio de instalación para este software y haga clic en "Siguiente", como se indica en la Fig. 7.7.6. También puede cambiar el directorio de instalación del predeterminado haciendo clic en "Examinar…"

Figura 7.7.6. Ubicación de destino para la instalación

PASO 7: Seleccione una carpeta de programas en la que instalar el software de la aplicación y haga clic en "Siguiente", como se muestra en la Fig. 7.7.7.

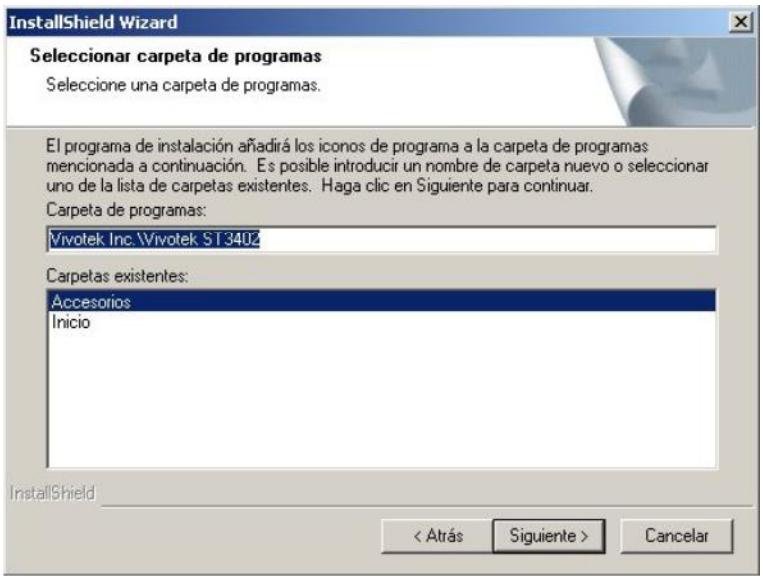


Figura 7.7.7. Seleccionar carpeta de programas

PASO 8: Después de comprobar toda la información de configuración que se muestra en la Figura 7.7.8, haga clic en "Siguiente" para comenzar la copia de archivos y la actualización del registro.

Figura 7.7.8. Comprobar la información de configuración

PASO 9: Haga clic en "Finalizar", como se muestra en la Figura 7.7.9., para finalizar la instalación. Así termina la instalación del programa.

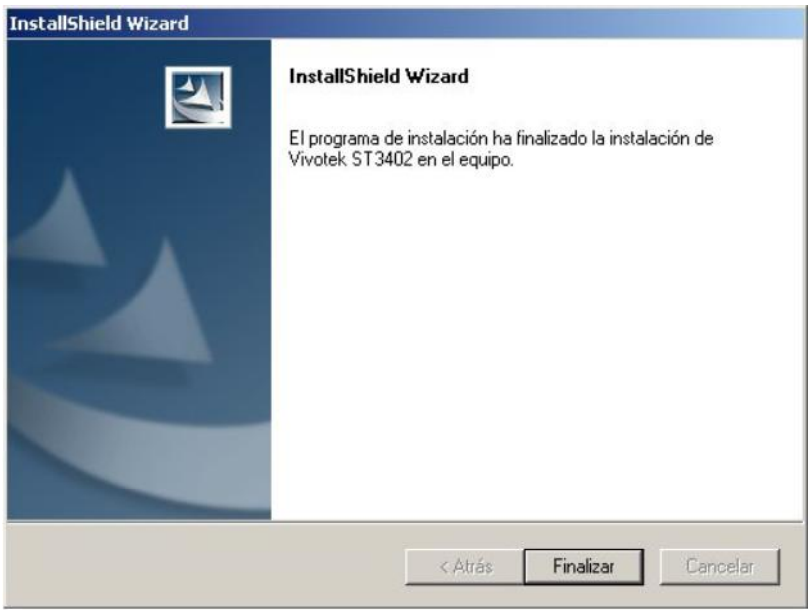


Figura 7.7.9. Fin de la instalación

7.8 Asignación de Dirección IP.

Inserte el disco de instalación en la unidad de CD-ROM; la instalación debe iniciarse de manera automática. Si no es así, haga clic en "Inicio" en el vértice inferior izquierdo de la pantalla, abra "Mi PC" y haga doble clic en el icono del CD-ROM.

Aparecerá la ventana de instalación de la grabadora de vigilancia IP como en la siguiente Figura. 7.8.1.

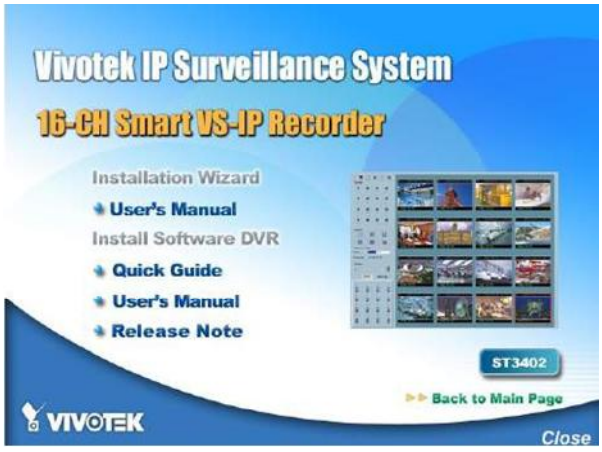


Figure 7.8.1 Ventana de instalación de la grabadora.

En la pantalla principal encontraremos los dispositivos Vivotek detectados en la red.

Figura 7.8.2 Pantalla principal de monitoreo.

A continuación seleccionaremos nuestra cámara cuya MAC y modelo coinciden con la etiqueta que posee nuestra cámara y que previamente habíamos anotado como se observa en la Figura 7.8.2

Figura 7.8.3 Obtención de la Dirección IP Dinámica en la Cámara IP

Si por algún motivo no se detecta nuestra cámara aún habiendo hecho varios “refrescos de dispositivos”, podemos cambiar la configuración de red de nuestro PC obligando a que se encuentre dentro del mismo rango de red que la dirección ip* de fábrica de la cámara (ip de fábrica: 192.168.0.99), por ejemplo:

La dirección ip de nuestro PC puede ser 192.168.0.4

La mascara de subred 255.255.255.0

La puerta de enlace debe ser 192.168.0.1

Este enlace se puede observar en la figura 7.8.4.

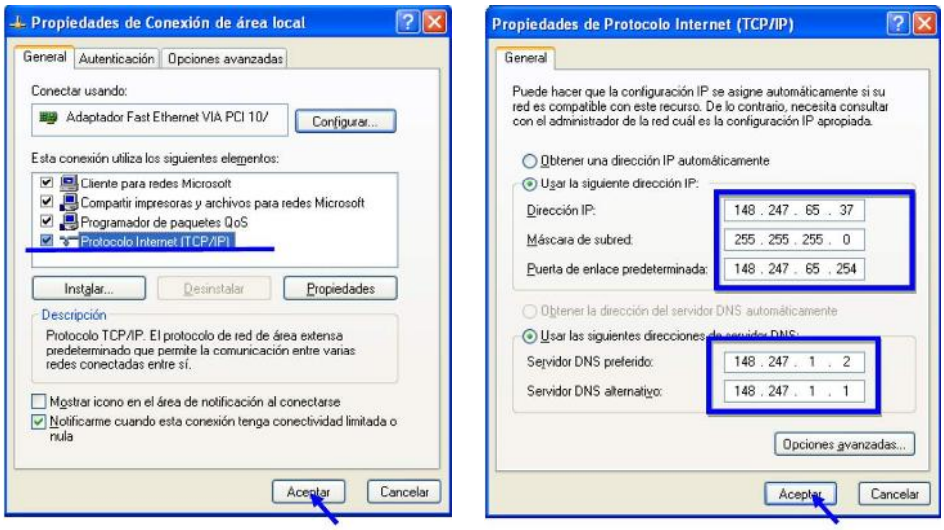


Figura 7.8.4. Configuración de la Dirección IP

7.8.1 Dirección IP.

Es un número que identifica de manera lógica y jerárquica a un dispositivo dentro de una red que utilice protocolo IP. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo asignado a la tarjeta de red por el fabricante, mientras que la dirección IP se puede cambiar.

Es habitual que un usuario que se conecta desde su hogar a Internet utilice una dirección IP.

Esta dirección puede cambiar al reconectar con nuestro servidor de Internet; y a esta forma de asignar una dirección IP se denomina una dirección IP dinámica.

Los sitios de Internet que necesitan estar permanentemente conectados, generalmente tienen una dirección IP fija o estática; es decir, no cambia con el tiempo o al reconectar, como son por ejemplo los servidores y páginas web.

Sin embargo hay conexiones como las de nuestras casas que utilizan una notación más fácil de recordar y utilizar, como son los nombres de dominio o DNS. Una forma de asignar direcciones IP dinámicas es mediante el protocolo DHCP (Dynamic Host Configuration Protocol).

7.8.2 Configuración del sistema.

Donde podremos dar nombre a la cámara, poner una contraseña de acceso de administrador (root) y configurar la fecha y la hora, ver Figura 7.8.5.

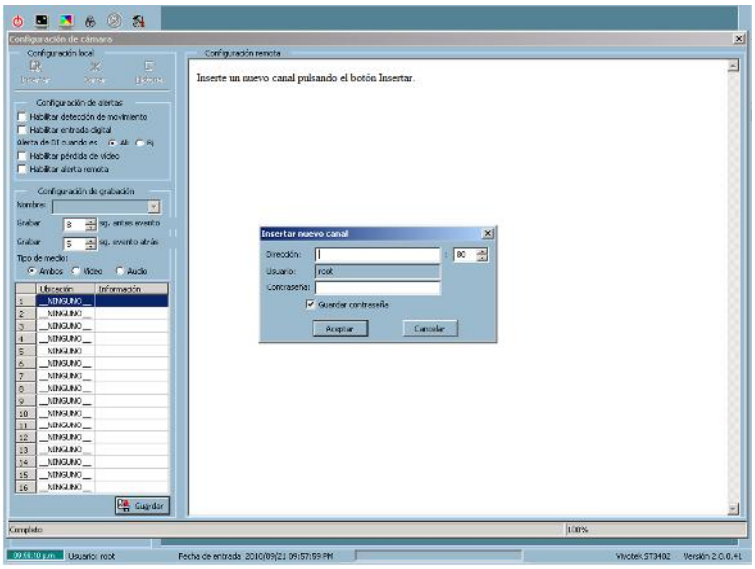


Figura 7.8.5. Configuración del sistema

7.8.3 Configuración de red.

En este apartado debemos asignar una dirección IP a la cámara para que se encuentre asignada dentro del rango de nuestra red, además de la mascara de subred y la puerta de enlace que será la misma que la IP del router como se muestra en la figura 7.8.6.

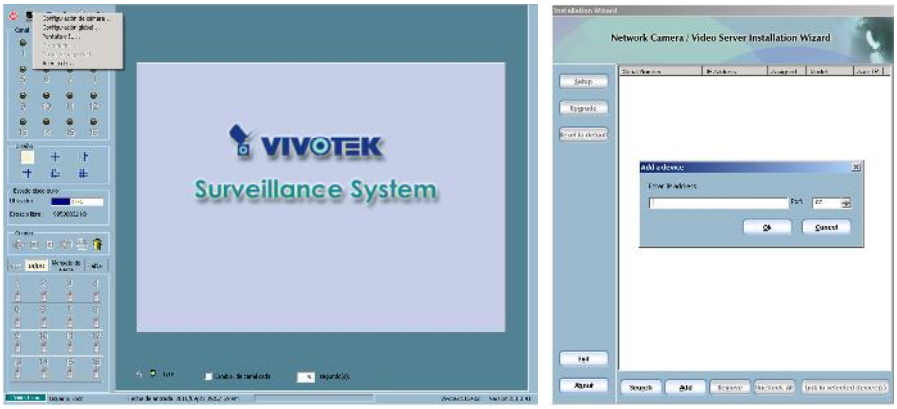


Figura 7.8.6 Configuración de red

7.8.4. Configuración de puertos.

Ahora configuraremos los puertos manualmente. Por defecto el "puerto http" es el 8080 y resulta aconsejable cambiarlo por otro para que no surjan conflictos con el navegador Internet Explorer ya que también utiliza este puerto 80. Esto sería en el caso de que la cámara la vamos a querer visualizar alguna vez desde otra red externa que no sea la nuestra; como por ejemplo, si queremos vigilar a través de las cámaras de nuestro negocio desde casa o cualquier otro lugar del mundo.

Para ello, pongamos un ejemplo:

Si nuestra IP que le hemos asignado a la cámara es la 192.168.1.54

El puerto que podemos poner por ejemplo es el 8054, así los últimos dígitos del puerto son iguales que los últimos dígitos del la dirección IP de la cámara, por lo tanto ese puerto de alguna manera podemos hacer que tenga referencia con esa cámara y nos resultará más fácil de recordar a la hora de acceder de una red que no sea la propia en la que se encuentra la cámara, como lo observamos en la Figura 7.8.7.

Figura 7.8.7. Configuración de puertos

Otra operación que debemos realizar para ello, es abrir o desviar ese puerto hacia esa dirección ip en nuestro router, al ser posible y si nos lo permite nuestro router, abrirlo tanto en el protocolo TCP y UDP. Quizás en este proceso anterior necesitemos ayuda de un informático o técnico si nuestros conocimientos no son muy amplios. Una vez hecho todo esto para acceder a la cámara y visualizarla deberíamos escribir en el navegador de Internet algo así como:

http://192.168.1.54:8054

↑..... **:** .....↑

Dirección ip privada puerto para acceder desde la propia red

http://217.125.156.164:8054

↑..... **:** .....↑

Dirección ip pública puerto o externa para acceder desde otra red

7.8.5 Resetear y restaurar valores.

En el supuesto caso de que tengamos una cámara que ya ha sido utilizada y/o que ha dejado de funcionar correctamente, y por lo tanto ya tenía asignada una dirección IP que no conocemos y que por medio de la aplicación Installation Wizard 2 no nos la detecta aún cambiando el rango de IP del PC al rango de la IP de fábrica de la cámara como ya se explicó anteriormente en el apartado de

"Asignación de IP"; deberíamos de resetear el sistema de la cámara para que vuelva a tener los valores de configuración de fábrica y así conseguir que vuelva a un estado normal, ver figura 7.8.8.

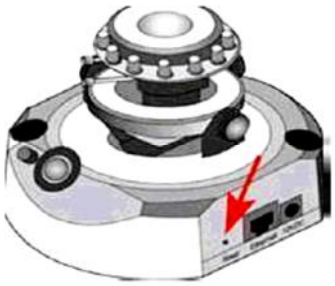


Figura 7.8.8. Reset a nuestra Cámara IP

Es tan sencillo como coger por ejemplo un clip o algún objeto con una punta muy pequeña que podamos introducir en dicho botón, presionándolo continuamente hasta que el led de estado naranja parpadee continuamente, una vez que se haya apagado el led dejaremos de presionar y tras ello el reseteo habrá finalizado satisfactoriamente y ahora parpadearán el led rojo y naranja.

No hay que ser impacientes con este proceso ya que puede llevar alrededor de 30 segundos en algunas ocasiones.

7.8.6. Herramientas de control de entrada/salida.

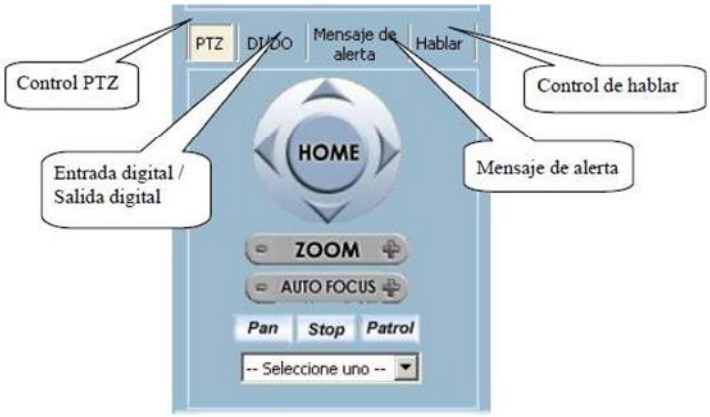


Figura 7.8.9 Herramienta de control de entrada/salida

Esta aplicación proporciona otras tres herramientas que se muestran en la Fig. 7.8.9, en el vértice inferior izquierdo, para controlar el producto remoto de la serie Servidor de vídeo/cámara de red del canal asociado. Puede hacer clic en los botones dedicados para pasar a una herramienta de control diferente, como Control de PTZ Panorámica/Inclinación/Zoom), Control de DI/DO (Entrada digital / Salida digital), receptor de Mensaje de alerta y Control de Hablar.

7.8. Conexión.

El Lanzador dispone de un mecanismo de autenticación. Si el usuario ha superado la autenticación en el Lanzador, se puede abrir Reproducción sin necesidad de más autenticaciones.

En caso contrario, aparecerá el cuadro de diálogo Autenticación del Lanzador y el usuario deberá superar la autenticación para poder usar Reproducción.

NOTA: La Reproducción la pueden iniciar los usuarios del grupo raíz o los usuarios avanzados. Para obtener más información acerca de los grupos de usuarios, consulte la sección 2.2.

7.9 Diseño.

Una vez conectado al sistema Reproducción, aparecerá la ventana principal en la parte superior de la pantalla y la resolución de pantalla cambiará automáticamente a 1024x768, si a resolución actual es inferior.

Como se muestra en la Figura 7.8.10, existen cuatro áreas principales en esta ventana: Área de visualización, Área de histogramas, Área de control y Área de estado. También existen tres indicadores visuales de los controles: Indicador de elección de área, Indicador de selección de marco y Barra de tracción.

Estas características proporcionan una búsqueda avanzada del vídeo específico grabado en la base de datos de vigilancia.

Figura 7.8.10 Ventana principal de Reproducción.

7.10 Configuración del Panel de Control.

Haga clic en el botón "Configuración" mostrado en la Fig. 7.8.11 en la herramienta de control el sistema y aparecerá el cuadro de diálogo de configuración en pantalla.

Figura 7.8.11. Herramienta de control del sistema

Ubicación de la base de datos.

El elemento más importante del cuadro de diálogo de configuración es la ruta de la base de datos. Deberá ajustarlo en el directorio que contiene la base de datos de vigilancia para que el programa funcione correctamente.

Ubicación de los archivos AVI

Así se ajusta el directorio de almacenamiento al exportar archivos AVI. Los archivos AVI exportados se guardarán en un subdirectorio debajo del directorio que haya seleccionado aquí.

Ubicación de los archivos de instantánea.

Ajusta el directorio cuando utiliza la instantánea para exportar archivos de mapa de bits. Los archivos de mapa de bits exportados se guardarán en un subdirectorio debajo del directorio que haya seleccionado aquí.

Modo de compresión AVI.

Sólo utilizamos una profundidad de colores de 24 bits para exportar el archivo AVI en este modo. En la selección del modo de compresión AVI, puede seleccionar uno de los métodos de compresión (tanto vídeo como audio) que admita su equipo para exportar el archivo AVI.

Los métodos de compresión pueden ser diferentes de un equipo a otro debido a los distintos métodos de compresión en las distintas instalaciones de equipos.

Modo Modulación.

El Modo modulación decide sobre el tamaño del vídeo de la pantalla. Depende del modo en que se grabó la secuencia de vídeo en el programa Monitor. Si ha seleccionado un modo de modulación

incorrecto, el vídeo visualizado aparecerá distorsionado. Para corregirlo, abra el cuadro de diálogo Configuración y cámbielo al modo correcto.

Posición del panel de control.

Ofrece un práctico modo de cambiar la posición del área de control, a la izquierda o a la derecha de la ventana principal, según sus preferencias.

Formato de hora.

Existen dos tipos de formatos de hora (12 o 24 horas) que puede seleccionar el usuario para determinar el formato de hora en la barra de estado superior del área de visualización.

Formato de instantánea.

El usuario puede seleccionar dos formatos (.jpg y .bmp) para determinar el formato de archivo de la instantánea.

7.11 La seguridad contra los ladrones, un "traje a medida" para cada hogar.

Proteger los hogares de posibles robos es una obsesión que aumenta cada día. La preocupación por la seguridad se ha instalado poco a poco en los hogares, cada vez mas equipados contra los “amigos de lo ajeno”. Según el Observatorio de la Seguridad Security Point, más de un 75 por ciento de 100 ciudadanos en la Ciudad de México consideran que los robos supone un problema “bastante o muy frecuente”, no obstante, existe un considerable número de ciudadanos (más de un 9.5 por ciento) que ni siquiera ha adoptado métodos o sistemas antirrobos en su vivienda.

Para poner obstáculos a los ladrones existe en el mercado un sinfín de soluciones y sistemas de seguridad que han ido perfeccionándose y haciéndose más eficaces, muchas veces de las nuevas tecnologías, para combatir los ataques de los ladrones: desde los sistemas mas básicos como las cerraduras antitarjetas hasta los últimos avances en llaves codificadas magnéticamente o los sofisticados sistemas de alarma que informan en tiempo real al usuario a través del móvil.

No obstante, se tiene en mente que no siempre lo más moderno es lo más eficaz contra los robos.

Necesidades de cada inmueble.

La seguridad de los hogares no consiste tampoco en acumular el mayor número posible de alarmas y sistemas de protección. La seguridad debe ser entendida, en cambio, como un “traje a la medida”, diseñado según las necesidades especificas de cada vivienda: “dependiendo de muchos factores, como el lugar donde se situé la casa, su altura, del numero de puertas y ventanas, etcétera”.

Una de las razones de la gran mayoría de los sistemas de seguridad se instala una vez que la vivienda ha sido adquirida y no durante su construcción.

No obstante, la seguridad sigue siendo entendida como un complemento, muchas veces voluntario o a petición de la necesidad del propio comprador de estos sistemas de alarmas como un elemento estructural más de la vivienda.

Desanimar a los ladrones.

El principal objetivo de todos los sistemas de seguridad es, ante todo, impedir a los ladrones de que intenten entrar en nuestros hogares. Más de un 80 por ciento de los asaltos son hijos de la oportunidad: la mayoría de los ladrones actúan aprovechando la mínima vulnerabilidad, casi siempre cuando la casa esta vacía, sobre todo en épocas de vacaciones.

Las alarmas son, sin duda, uno de los mecanismos mas utilizados contra los intrusos, sin embargo, los profesionales en la materia de seguridad recuerdan que deben ser siempre utilizadas como complementos a otros sistemas: persianas, puertas especiales y cerraduras. Las alarmas solo sirven para avisar que la casa ha sido allanada, pero no evitan el robo.

Puertas blindadas y acorazadas.

Las puertas son, en cambio, el principal punto que hay que reforzar para tener una casa segura, contra lo que se pueda pensar; los ladrones no suelen entrar por la ventana. De hecho, es la puerta principal la vía de acceso mas utilizada. Más de un 36 por ciento de los robos se realizan por ella (sobre todo en pisos, donde el porcentaje se eleva a casi un 47 por ciento), y un 11.4 por ciento lo hace por alguna puerta secundaria. Las ventanas si son más frecuentadas, donde un 39 por ciento de los robos se cometen a través de ellos.

Las puertas de seguridad, blindadas o acorazadas, son de hecho, los mecanismos más demandados por los hogares y empresas: más de 55 por ciento posee una puerta especial (ya sea blindada o acorazada) en sus hogares y más del 80 por ciento tienen al menos varios cerrojos en la entrada.

La confusión entre puertas blindadas y acorazadas suele ser un error muy usual entre los ciudadanos que se interesa en reforzar la entrada principal. Sin embargo, las diferencias son más que notables, tanto en sus precios como en la capacidad de seguridad que ofrecen unas y otras.

Las puertas blindadas son algo más vulnerables que las acorazadas, sobro todo a las palancas, aunque dan al hogar muchas garantías de protección, suficientes para las necesidades de algunas viviendas, y a menor precio.

No solo ofrecen un mayor grosor que las puertas comunes, sino que además, están reforzadas con una hoja de acero en cada una de sus caras, de más de dos centímetros de espesor y cerraduras especiales de potentes barras de acero que bloquean la puerta por los cuatro costados.

La puerta acorazada, por su parte, es aproximadamente un 25 por ciento más caras que las blindadas. El precio medio no suele bajar de los 30,000 pesos mexicanos, pero garantiza la total protección de la entrada de los hogares.

Están preparadas para hacer inútil el uso de palancas y de hecho, suelen ser utilizadas en museos o recintos públicos que necesitan de una especial seguridad. La principal diferencia con las blindadas es que los mecanismos de cierre están incorporados en el propio cuerpo de la puerta, y que no solo el interior de la hoja, sino también el marco e incluso el “premarco” (el quicio) están forrados con placas de acero. Ver Figuras 7.12.1 y Figura 7.12.2.

Figura 7.12.1 Tipo de puerta blindada.

Figura 7.12.2 Tipo de puerta acorazada.

Alarmas en la placa de la mano.

Las alarmas siguen siendo para muchos el principal símbolo de la seguridad. Mas del 24 por ciento, según el estudio de Security Pointy*, afirma que este es uno de los sistemas que mas tranquilidad les proporciona, incluso por encima de las puertas y las ventanas "antiladrones". Pese a esto, el porcentaje de españoles que posee actualmente una alarma en sus casas no supera el 17 por ciento.

*Nota: visitar el sitio web: http://www.belt.es/noticias/2005/julio/29/ladrones.asp.

Por encima de cualquier otro, las alarmas han sido los sistemas que más y mejor se han nutrido de los avances tecnológicos de la última década, sobre todo del despegue de las comunicaciones e Internet. Las ultimas tecnologías han facilitado las conexiones entre las viviendas y las centrales de vigilancia, aumentando considerablemente su eficacia y reduciendo los costos: hoy día un hogar puede estar perfectamente vigilado por un precio entre los 800 y los 2.000 euros* (precio en pesos mexicanos aproximado: $12,416.00 y $31.040.00 M.N.) , sin incorporar incluso cámaras de seguridad.

*Nota: Fuente (http://www.bancomer.com.mx).

Las sofisticadas instalaciones actuales han conseguido retar la pericia de los ladrones, como el sistema "habla-escucha", permiten a las agencias de vigilancias dirigirse por medio de interfonos a los ladrones, para disuadirles, una vez que han entrado en el edificio.

Las ultimas novedades en servicios de alarma permiten, incluso, recibir videoconferencias de nuestro hogar a través del teléfono móvil o por Internet, para ver que ocurre durante las veinticuatro horas, o recibir en "tiempo real" los daños que hayan causado los ladrones durante el robo.

Gracias a las imágenes de video, los vigilantes, o el propio inquilino, pueden reconocer si la causa de una alarma es realmente un allanamiento o, como suele ser habitual, ha sido activada por algún animal o un familiar conocido.

Sistema de Cerca Electrificada con Energizador.

Los sistemas de protección perimetral son diversos, estos se usan para delimitar propiedad y evitar intromisiones a casas, comercios, oficinas o cualquier tipo de área. El sistema de protección con energizador, tiene como finalidad proteger un área predeterminada por medio de una barrera de alto voltaje.

Principio de funcionamiento:

La cerca electrificada consiste de un generador de alto voltaje que hace circular una corriente directa de 12,500 volts y muy baja energía por un circuito de alambre (líneas de alto voltaje). Esta señal recorre el circuito y provoca una descarga cuando una persona la toca cerrando un circuito a tierra.

Cuando una persona toca algún punto del circuito, los pulsos encontraran un camino a tierra, revocando así una descarga que causa una fuerte contracción muscular, desorientación y en algunos casos perdida del sentido. Pero siempre sin efectos letales ya que la energía es muy baja. El objetivo del sistema es ahuyentar a posibles ladrones, no matarlos. La corriente generada es del orden de micro Ampers, a pesar del alto nivel de voltaje, por esto no representa un riesgo mortal.

Plano de ubicación del equipo:

Una vez determinado el tipo de barda, realice un plano de ubicación del resto del equipo en base a las siguientes consideraciones de la Figura 7.12.3.

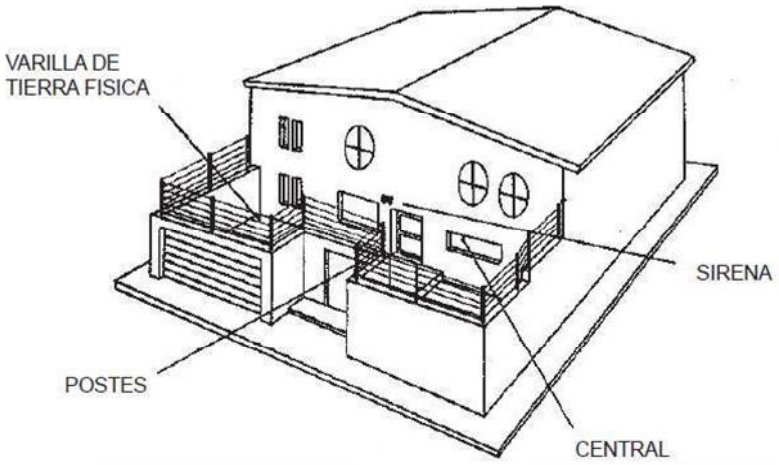


Figura 7.12.3 Ubicación de los elementos de Seguridad.

Tierra física: Esta es la base del buen funcionamiento del equipo, de preferencia debe de clavar una varilla de cobre (copperweld) en un lugar húmedo y no más lejos de 15 mts. del energizador.

Sirena: Deberá colocarse en el exterior de la vivienda de preferencia a mas de 2.5 mts. de altura para evitar que la corten.

Central: Deberá colocarse a no más de 10 metros del punto de conexión a la cerca para reducir el costo del cable de alto voltaje, ya que es costoso. Debe de colocarse lo menos visible posible y aunque es a prueba de agua es mejor que este bajo algún tipo de resguardo.

Varilla de tierra: Una buena tierra es fundamental para el buen funcionamiento de su sistema; clave una varilla de por lo menos un metro en un lugar húmedo y a no mas de 15 mts. del energizador. Conéctela al energizador con cable grueso (Calibre 12).

Diagrama de instalación general.

A continuación se observa en la figura 7.12.4 un ejemplo de la estructura de una cerca electrificada.

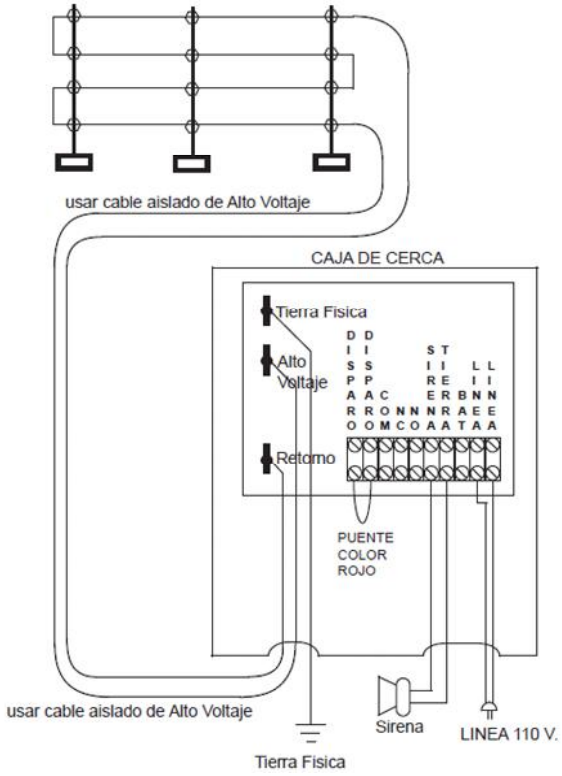


Figura 7.12.4 Configuración de una Cerca Electrificada.

Operación del equipo:

Para abrir el equipo gire los cuatro tornillos de la tapa un cuarto de vuelta en sentido anti horario. Tenga cuidado al abrir pues aunque se tienen unos retenes de nylon para sostener la tapa podrían soltarse y despegar el cable plano que une a la tablilla madre con la tablilla de focos.

Este equipo genera alto voltaje aun estando desconectado, ya que cuenta con baterías de respaldo.

Para evitar una descarga, antes de abrir la tapa asegúrese que el equipo esta apagado introduciendo la llave en la chapa situada en la parte inferior del equipo y girando en sentido contrario a las manecillas del reloj, el foco amarillo deberá apagarse. (Nota el foco verde siempre esta encendido cuando hay voltaje de línea).

En el frente hay tres focos que indican lo siguiente:

Rojo: Se enciende en el momento que hay un disparo por corte o por conexión a tierra.
Amarillo: Parpadea mientras haya alto voltaje en el circuito.

Verde: Indica que hay voltaje de línea y que las baterías se están cargando.

Localización: Encuentre el lugar apropiado para colocar el energizador y fíjelo al muro utilizando las perforaciones de la parte superior (donde la tablilla esta cortada en diagonal), estas perforaciones vienen tapadas y hay que abrirlas con un taladro.

Alarma: Hay tres formas de disparar la alarma:
1.- Conectando a tierra alguna sección de la cerca.
2.- Cortando alguna sección de la cerca.
3.- Manualmente abriendo el puente rojo colocado en las posiciones 1 y 2 de la tira de conexiones.

En los casos 1 y 2 la alarma sonara por cinco minutos y se encenderá el indicador rojo de alarma; además se cerrara el relevador auxiliar de las terminales COM, NC, NO (3, 4 y 5). Para apagar antes del tiempo preestablecido de deberá girar la llave de encendido para apagar y volver a encender.

Esta operación también apagara la lámpara de alarma (ROJA). En el caso 3 al abrir el puente sonara la alarma y activara el relevador auxiliar.

Prueba de funcionamiento

a) Prueba de sirena:
Apague el equipo girando la llave en sentido contrario a las manecillas del reloj (off).
- Abra la central y quite el puente que se encuentra entre los bornes “DISPARO” Y “DISPARO -” de la central.
- Cierre la central y encienda el equipo girando la llave en el sentido de las manecillas del reloj (on).
- La sirena se activará al encender el equipo.
- Una vez verificado el funcionamiento de la sirena, apague el equipo y coloque nuevamente el puente entre los bornes “DISPARO” y “DISPARO. -” de la central.
En caso de que la sirena no se haya activado, verifique el conexionado de la misma y realice la prueba nuevamente.

b) Alambrado:
Si la sirena se activa al encender el equipo girando la llave en el sentido de las manecillas del reloj (on):
- El circuito alambrado está abierto, falta algún puente con los que se unen las líneas.
- Una de las líneas está haciendo contacto con un árbol, enredadera, poste o barda.

c) Alarma de corte:
- Apague el equipo girando la llave en sentido contrario a las manecillas del reloj (off).
- Desconecte dos líneas removiendo el puente que las une.
- Encienda el equipo girando la llave en el sentido de las manecillas del reloj (on) y la sirena deberá activarse.
- Si la sirena se activó, apague el equipo girando la llave en sentido contrario a las manecillas del reloj (off), coloque nuevamente el puente que une las dos líneas y encienda la central.

Si la sirena no enciende, verifique la conexión de la sirena o si el alambrado tiene trayectorias en paralelo.

d) Puesta a tierra:

Apague el equipo girando la llave en sentido contrario a las manecillas del reloj (off).
Corte un tramo de alambre de 30 cm. y cuélguelo de la línea inferior de su cerca dejándolo caer sobre la barda.
La sirena se activará al encender el equipo.
Si la sirena no enciende, revise las conexiones de TIERRA FISICA, VOLTAJE Y REGRESO, así como la instalación de la varilla de tierra. Ver Figura 7.12.5.

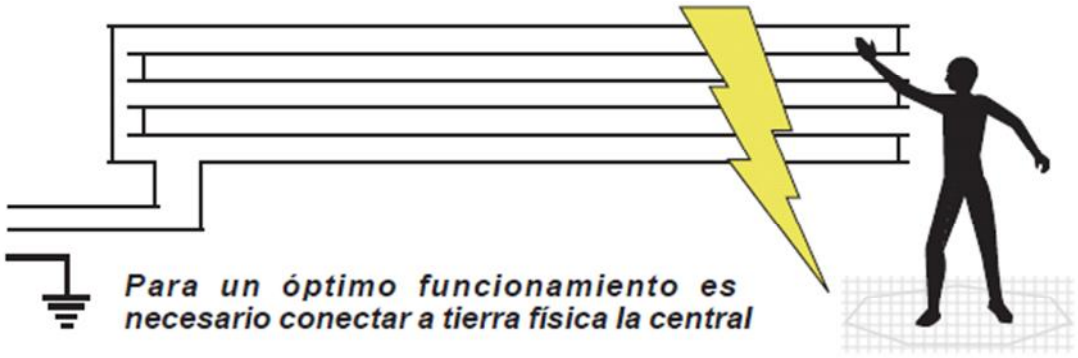


Figura 7.12.5 Configuración de una Cerca Electrificada.

La cerca electrificada consiste en un circuito de alto voltaje (12,500 Volts), que provoca un choque eléctrico a la persona que tiene contacto con ésta, causando dolores musculares intensos y desorientación.

La descarga no es letal, el objetivo del sistema es ahuyentar a los posibles intrusos.

Información adicional sobre la cerca eléctrica

1. ¿Es letal el cerco eléctrico?

El cerco eléctrico no es letal por que el shock eléctrico que recibe la persona o animal es de muy bajo amperaje y es un micro pulso que solo lo repelará causando dolores internos y un dolor intenso en el lugar que lo tocó, dolor que dura ocho días aproximadamente.

El amperaje es lo que permite que la persona se quede pegada o no a algún artefacto conductor de energía, en este caso el amperaje bajo ayuda que no produzca heridas ni causa que la persona muera al contrario, expulsa al individuo. Ya a un centímetro y medio la cerca expulsa a la persona.

2. ¿Es legal el cerco eléctrico?

El cerco eléctrico es un sistema de seguridad para salvaguardar su seguridad personal o física. En nuestro país no existe ley que impida la instalación de los cercos eléctricos en tanto se instale en lugares donde no afecte u obstruya espacios ajenos a su propiedad o espacios públicos.

3. ¿Es necesario algún permiso para la instalación del cerco eléctrico?

Hasta el día de hoy no se ha dado a conocer una ley o reglamentación que impida la colocación de cercos eléctricos.

4. ¿Qué ocurre cuando se va la luz?

En el caso de los cercos eléctricos de seguridad, el equipo cuenta con una batería, la duración de la misma es de 3 a 5 días en caso de no haber energía eléctrica.

5. ¿Qué mantenimiento es necesario para el cerco eléctrico?

El mantenimiento del cerco eléctrico es muy sencillo, básicamente consiste en la limpieza del polvo que se adhiere en los aisladores, pintado de los postes si es necesario, revisión de nivel de energía del retorno del alto voltaje, revisión de nivel de carga de la batería, cambio de aisladores si están cristalizados, letreros, limpieza del cable, revisión completa de la caja de control o energizado para el perfecto funcionamiento de la Cerca Eléctrica.

En lugares muy polvorientos o húmedos cada 4 meses. En lugares secos y de ambiente limpio cada 6 meses., etc.

6.- ¿Que pasa si rompen los aisladores?

Si los ladrones rompen un aislador con un combo, por presión o con el paso del tiempo (4 a 6 años por no dar mantenimiento) estos se cristalizan y rompen, ya no habría que separe al alambre del tubo y se activaría la sirena de inmediato, hay ocasiones en que el cable va rompiendo todos los aisladores y topa todos los cable, muro y tubos.

7. ¿Cuánto consumo eléctrico genera?

El cerco eléctrico no consume mucha energía puesto que los equipos se conectan a 110 o 220 voltios y el transformador hace que la cerca funcione con 12 voltios, con una descarga de 6000 a 13000 voltios, lo cual en significa que el equipo consume 1.15 KW

9.- ¿Funciona el cerco eléctrico si colocan materiales aislantes sobre los alambres?

Los intrusos pueden utilizar cualquier tipo de material sea cobijas, palos, ropa, saquillos, guantes de caucho, botas de caucho e incluso si utilizan todo un traje de caucho, la sirena se activa en el instante, gracias al sistema de anillos de paso que son los anillos que están alrededor del alambre en postes aisladores (de 1 ¼), eso es lo que nos diferencia de otras empresas. Entonces la respuesta a lo preguntado es **SI.** Cabe mencionar que los anillos antes mencionados se colocarán únicamente en zonas que sean posibles colocar ya que si colocamos en un lugar donde no es recomendable hacerlo pueden emitir falsas alarmas. Se garantiza un 98% de SEGURIDAD.

10. ¿Como sabemos si alguien quiere pasar el cerco eléctrico?

Al momento que alguien intente pasar la cerca se activará una SIRENA DE 30 WATTS, la descarga que emite el cerco eléctrico puede alcanzar a una persona a 2cm o 1 ½ cm., esto solo sucede con nuestros equipos porque emiten la mayor descarga en cuanto a cercos eléctricos se refiere.

11.- ¿Que pasa si cortan el alambre?

Este es otro motivo por el cual nos diferenciamos de otras empresas, el alambre que colocamos es alambre de **ACERO GALVANIZADO DE 2,67 mm DE ESPESOR, NO SE PUEDE CORTAR**, a menos que se utilice una cinzaya, pero aun así es muy difícil, la sirena se activa al instante que se coloque materiales conductores de energía en el alambre.

12.- ¿Que pasa si le cae un rayo a la cerca eléctrica?

No sucede absolutamente nada porque todo el sistema esta conectado a tierra, mediante una varilla de cooperwell (varilla de cobre), es decir cualquier descarga se ira directamente a tierra sin ocasionar daño alguno.

13.- ¿Interfiere la cerca eléctrica a señales de tv. Radio?

NO, porque la caja de control que utilizamos tienen dispositivos especiales, y es totalmente independiente de cualquier sistema. Justamente esta es una norma internacional que debe cumplirse.

14.- ¿Que pasa si un niño topa la cerca eléctrica?

La altura a la que esta colocada la cerca eléctrica disminuye considerablemente el que los niños la topen, la única forma para que ocurra una descarga es que topen el alambre no los tubos ni la pared ni las rejas solo si y solo si TOPAN EL ALAMBRE, si sucede esto no morirán solo se llevaran un buen susto, les dolerá por una semana la parte con la que toparon el cerco eléctrico pero no ocurrirá mayor cosa, **NO TENDRÁN HERIDAS PUNZO PENETRANTES.**

15.- ¿Produce Cáncer, Quema Equipos O Artefactos Eléctricos?

PARA NADA, el sistema es independiente si hay una fluctuación de voltaje (cuando viene muy fuerte la luz) las descargas serán enviadas a tierra o se quemará el fusible de la caja de control, la misma que tiene 2 fusibles. En cuanto al cáncer, no lo produce ya que la cerca no emite radiaciones ni produce campo magnético alguno.

Conclusiones.

La realización de la presente Tesis de titulación significa una fuente importante de nuevos conocimientos, y mediante las fases de preparación y desarrollo del mismo se han podido extraer las siguientes conclusiones:

Una mejora significativa que se puede apreciar en los sistemas de seguridad digitales es el aprovechamiento que se puede dar a una infraestructura existente, como las redes de telecomunicación IP, hacia la cual están migrando la mayoría de servicios y aplicaciones. Esto permite concluir que es posible incorporar en un solo sistema de seguridad varias aplicaciones como son la video vigilancia y sistemas de alarmas.

Existe una gran diferencia entre un CCTV o sistema de video vigilancia normal y un sistema de video vigilancia urbano debido a múltiples factores adicionales que deben considerarse en la etapa del diseño. Uno de estos factores tiene que ver con la elección del medio de transmisión pues la señal de video, en un sistema de vigilancia urbano, debe llegar a mayores distancias, lo cual implica esperar mayores niveles de atenuación.

La labor de recopilación de información sobre el funcionamiento de los sistemas descritos en la presente Tesis de Titulación, ha permitido obtener una visión más amplia respecto al diseño de una red de telecomunicación. Se puede concluir que para el correcto funcionamiento de la red se hace necesario el apoyo de otros sistemas adicionales como son: el sistema de respaldo de energía eléctrica, protección del sistema de alimentación eléctrica, sistema de respaldo de información, entre otros.

El uso de los sistemas digitales hace posible el uso de formatos de compresión que disminuyen los requerimientos de ancho de banda, tanto para la transmisión como para el almacenamiento, sin disminuir la calidad de la señal, optimizando la capacidad del canal de transmisión y aprovechando la red IP. De esto se puede concluir que fue correcto incluir el concepto de compresión de datos en el diseño de este proyecto.

También se han mejorado los sensores o alarmas que aprovechan nuevas tecnologías como: detectores de movimiento por infrarrojos, sensores magnéticos y dispositivos de menor tamaño y mejores prestaciones. La Central Receptora de Alarmas puede realizar procesos automáticos como la notificación automática a la policía o la Cruz Roja, envío y almacenamiento de reportes digitales de alertas, entre otros.

Se determina que al momento de que algún intruso ingresa a alguna casa o propiedad las Cámaras IP por medio de sus sensores de detectores de presencia activen una Sirena, así como la energización de una puerta electrificada que caerá sobre la entrada principal y una cerca electrificada en las ventanas para poder impedir la fuga del ladrón, también se recomienda que el interruptor eléctrico del inmueble no se encuentre a la vista para que este no se desenergice manualmente.

Bibliografía.

Referencias:

Leduc-Armand St. Pierre, Daniel ***HTML Creación y difusión de páginas Web*** Trillas 1999.

Kinnanman, Dave y Baltew, Lou Ann ***TCP-IP Accelerated MCSE*** McGraw-Hill.

Pratdepadua Bufill, Joan Josep ***Domine ASP .Net*** México, Alfa omega Ra- Ma 2004.

J. Reilly, Douglas ***Diseño de Aplicaciones con Microsoft ASP .Net*** McGraw Hill.

Tall, Eric y Ginsbury, Mark ***Aproveche las noches con Active X*** México, Prentice Hall 1998.

Deitel, Deite y Nieto I n t e r n e t ***& World Wide Web: How to Program P r e n t i c e*** Hall 2000.

Pérez López Cesar ***Domine Windows XP Profesional*** México, Alfa omega Ra-Ma 2002.

Tanembaun, Andrew S. ***Redes de Computadoras*** Pearson Education 2003.

Páginas de Internet.

http://es.tldp.org/Manuales-LuCAS/doc-curso-html/doc-curso-html/x5520.html

http://www.masadelante.com/faq-servidor.htm

http://es.gotdotnet.com/quickstart/aspplus/

http://www.desarrolloweb.com/manuales/36/ http://www.w3schools.com/tags/tag_object.asp

http://www.alegsa.com.ar/Dic/dll.php

http://logix4u.net/index2.php?option=com_content&do_pdf=1&id=18

http://www.diarioti.com/noticias/nov97/not971114c.htm

http://www.belt.es/noticias/2005/julio/29/ladrones.asp.

Glosario.

Agente: Implementación de un dispositivo capaz de realizar una o varias acciones determinadas para ayuda del usuario.

Applets: Un pequeño programa escrito en Java e incluido en una página HTML. Es independiente del sistema operativo en el que funciona. Se puede utilizar un applet para visualizar un texto que desfila en un área específica, o animaciones.

Angulo de visión: Es el ángulo en que un observador (ya sea una persona o un dispositivo) genere una percepción de visión apropiada al entorno que se esté observando.

Binario: Sistema numérico basado en el uso de dos posibilidades que las más requeridas son el 1 o el cero.

Buffer: Una área de almacenamiento temporal reservada para uso en las operaciones de entrada-salida, dentro de la cual los datos son leídos, o dentro de la cual los datos son escritos

Cable ADSL: Tipo de cable en un sistema de transmisión de datos que se implanta sobre las líneas telefónicas convencionales.

Cámara IP: Dispositivo de captura de imágenes que muy comúnmente es utilizado en sitios de Internet, utiliza una dirección IP y usualmente son costosas.

Carga Máxima: Es el máximo consumo de corriente que un dispositivo puede consumir a la salida de un circuito eléctrico.

Codec: (Codificador Descodificador) Sistema usado para convertir señales analógicas en señales digitales y reconvertirlas para la recepción en un sitio remoto, comprimiendo la señal para una fácil transmisión.

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

Corriente inversa: Es la corriente que puede regresar de la fuente que la originó de manera tal que es perjudicial para los dispositivos empleados en el circuito.

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

Crominancia: Es el componente de la señal de vídeo que contiene las informaciones del color. Por otra parte, la luminancia es el componente de la señal de vídeo que contiene las informaciones de la luz o brillo.

Datagramas: Unidad de información transmitida por los protocolos de nivel de red, esta información le permite al protocolo TCP/IP encaminar (transportar a través de internet) los datos desde el origen a su destino.

DIP: Dual Internal Package e la configuración de circuitos integrados para su fácil implementación y configuración.

Hexadecimal: Es una notación numérica usual tanto en el campo computacional como electrónico para denotar una cifra con conversión binaria o decimal u octal.

HDLC: HDLC (High-Level Data Link Control) es un protocolo de comunicaciones de datos punto a punto entre dos elementos. Proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros

ICMP: Protocolo de mensajes de control de internet, como su nombre lo indica es un protocolo de mensajes que envía a el usuario cuando ocurre un problema en la red con los datagramas, pero no corrige dichos problemas.

Intranets: Red local privada que sigue la estructura (y los protocolos) de Internet.

Interfaz: Conjunto de reglas y normas que gobiernan el intercambio de señales y servicios entre capas adyacentes o equivalentes.

IPv6: Versión 6 de una dirección IP, quiere decir que un equipo puede identificarse con este campo que es una evolución del IPv4, teniendo este 6 campos que van de 0.0.0.0.0.0 a F.F.F.F.F.F o de 0.0.0.0.0.0 a 255.255.255.255.255.255.

LAN: Local Área Netwok o red de área local, conexión de varias computadoras que conviven entre si intercambiando información, archivos, teniendo una longitud máxima de 2.5 km.

Lag: Es la cantidad de tiempo en segundos entre lo que un usuario escribe y otro lo lee. Es decir, si hay dos segundos de lag entre 'A' y 'B' entonces lo que A escriba, B lo va a ver hasta dentro de dos segundos después. Por lo tanto cuanto menos lag haya entre los usuarios, más ágil y rápida será la comunicación entre ellos.

Lenguajes de programación: Los lenguajes de programación son herramientas que nos permiten crear programas y software. Los lenguajes de programación de una computadora en particular se conocen como código de máquinas o lenguaje de máquinas.

Micro controlador: Es un circuito integrado de alta escala que incorpora la mayor parte de los elementos que configuran un controlador.

Módem: Aparato que permite a un ordenador enviar y recibir información a través de una línea analógica, normalmente la línea telefónica (Modulador- Demodulador).

Píxeles: Unidad mínima que representa una imagen digital.

Plugins: Programa que puede anexarse a otro para aumentar sus funcionalidades (generalmente sin afectar otras funciones ni afectar la aplicación principal). No se trata de un parche ni de una actualización, es un módulo aparte que se incluye opcionalmente en una aplicación.

Protocolos: Sistemas y reglas que comunican diferentes equipos sin importar el sistema operativo del equipo.

Programa de alto nivel: Son aplicaciones en lenguajes de programación que se asemejan a las lenguas humanas usando palabras y frases fáciles de entender.

Puertos: Dispositivos de entrada y salida de información en una computadora.

Pull-up: En electrónica se denomina pull-up bien a la acción de elevar la tensión de salida de un circuito lógico, bien a la tensión que, por lo general mediante un divisor de tensión, se pone a la entrada de un amplificador con el fin de desplazar su punto de trabajo.

Resolución: Se refiere a la calidad que presenta una imagen en pantalla.

Router o enrutador: Dispositivo que se utiliza para interconectar a equipos que trabajan en una capa de red diferente, el router trabaja en la capa tres que es de RED.

Sistema de monitoreo móvil: medio integrado basado en hardware y software capaz de captar señales del medio con la capacidad de desplazamiento dentro del medio a monitorear.

S.O: Abreviatura de sistema operativo, los más usados son los desarrollados por Microsoft el entorno de Windows y el de Unix que es Linux.

Tiempo real: Dentro de la perspectiva del usuario es cuando se recibe una muestra, la procesa y entrega el resultado de una manera casi "instantánea", esto de manera que el diseñador percibe mediante los tiempos establecidos por el mismo sin importar que éste sea a alta velocidad, pero procurando que no se presenten fallas.

TTL: Lógica Transistor Transistor por sus siglas en inglés es la familia de circuitos integrados que por lo regular consumen 5v.

UNIX: Es un sistema operativo desarrollado por Linux multiusuario y multitareas y sirve como control para estaciones de trabajo y servidores.

USB: Universal Serial Bus es un tipo de Puerto muy requerido en estos días para cualquier dispositivo, desde memorias flash hasta joystick, su demanda es gracias a su alta velocidad de transmisión de hasta 450 Mbps.

Video streaming: Este sistema consiste en que la reproducción de los clips o las películas no requiere una descarga previa en la computadora del usuario, sino que el servidor entrega los datos de forma continua, sincronizada y en tiempo real (al mismo tiempo que se envía, se está visualizando).

Glosario de Siglas.

ARP (Protocolo de Resolución de Direcciones)

ASCII (Código Estadounidense Estándar para el Intercambio de Información)

ASF (Formato de Difusión Avanzada)

ASP (Servidor de Páginas Activas)

CBR (Tasa de Bits Constante)

CCD (Dispositivo de Cargas Interconectadas)

CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía)

CCTP (Circuito Cerrado Par Trenzado)

CCTV (Circuito Cerrado de Televisión)

CFML (Lenguaje de Marcado de Cold Fusion)

CMOS (Semiconductor de Óxido Metálico Complementario)

COM (Modelo de Objeto Componente)

CRC (Chequeo de Redundancia Cíclica)

CSS (Hojas de Estilos en Cascada)

CTI (Integración de dispositivos telefónicos en los computadores).

DHCP (Protocolo de Configuración de Anfitrión Dinámico)

DNS (Sistema de Dominio de Nombres)

DOM (Modelo de Objetos de Documento)

DSP (Procesamiento de Señales Digitales)

DVR (Grabadora de Video Digital)

EBCDIC (Código Extendido de Binario Codificado Decimal)

EDL (Lista de Decisiones de Edición)

EMI (Interferencia Electromagnética)

FAT (Tabla de Asignación de Archivos)

FTP (Protocolo de Transmisión de Archivos)

HTML (Lenguaje de Marcado de Hipertextos)

HTTP (Protocolo de Transmisión Hipertexto)

ICMP (Protocolo de Mensajes de Control de Internet)

IEEE (Instituto de Ingenieros Eléctricos y Electrónicos)

IGMP (Protocolo de Administración de Grupos de Internet)

IIS (Servidor de Información de Internet)

IP (Protocolo de Internet)

JSP (Páginas de Servidor Java)

LAN (Red de Área Local)

MMC (Consola de Gestión de Microsoft)

MMS (Sistema de Mensajería Multimedia)

MPEG (Grupo de Expertos en Imágenes en Movimiento)

NAS (Almacenamiento de Redes Adjuntas)

OSI (Interconexión de sistemas abiertos)

PHP (Procesador de Hipertexto)

POP (Protocolo de Oficina Postal)

PTZ (Vista Panorámica, Inclinación y Ampliación)

SAN (Almacenamiento de Área de Redes)

SDK (Kit de Desarrollo de Software)

SMIL (Lenguaje de Integración Multimedia Sincronizada)

SMP (Multiproceso Simétrico)

SMTP (Protocolo de Transferencia Simple de Correo)

SNMP (Protocolo de Manejo de Red Simple)

RTSP (Protocolo de Flujo de Datos en Tiempo Real)

SSH (Capa de Seguridad)

TCP (Protocolo de Control de Transmisión)

TI (Tecnologías de la Información)

UDDI (Descripción, Descubrimiento e Integración Universal)

UDP (Protocolo de Datagrama de Usuario)

UPS (Sistema de Energía Ininterrumpida)

UTP (Par Trenzado no Blindado)

VBR (Tasa de Bits Variable)

VGA (Matriz Gráfica de Video)

VPN (Red Privada Virtual)

VTR (Grabadora de Video Cintas)

WMI (Instrumentación Administrativa de Windows)

XML (Lenguaje de Marcas Extensible)