UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS

CARRERA DE INGENIERÍA ELECTRÓNICA Y COMUNICACIÓN

TEMA:

"DISEÑO DE UN SISTEMA DE SEGURIDAD MEDIANTE CAMARAS IP PARA LA EMPRESA PROALPI DE LA CIUDAD DE PÍLLARO"

Proyecto de graduación modalidad Pasantia previo a la obtención del Título de Ingeniera en Electrónica y Comunicación

AUTOR:

Cecilia Elizabeth Izurieta Pazmiño

TUTOR:

Ing. Geovanni Brito

Ambato – Ecuador

Noviembre / 2006

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Investigación sobre el tema:

"DISEÑO DE UN SISTEMA DE SEGURIDAD MEDIANTE CAMARAS IP PARA LA EMPRESA PROALPI DE LA CIUDAD DE PÍLLARO ", de Cecilia Elizabeth Izurieta Pazmiño, estudiante de la carrera de Ingeniería Electrónica y Comunicación, de la Facultad de Ingeniería en Sistemas, Universidad Técnica de Ambato, considero que dicho informe investigativo reúne los requisitos y méritos suficientes para ser sometidos a la evaluación de conformidad con el Art. 68 del Capitulo IV de Pasantías, Del Reglamento de Graduación de Pregrado de la Universidad Técnica de Ambato.

Ambato, Noviembre 2006

EL TUTOR

…….

Ing. Geovanni Brito

DEDICATORIA

Dedico este trabajo a mis padres, que con amor y sacrificio me apoyaron incondicionalmente.

A mi hija por darme la fuerza que necesitaba para salir adelante.

A mi esposo, incondicional en todo momento.

A mis hermanas y hermano por su cariño y constancia.

AGRADECIMIENTO

A Dios por darme salud y permitirme culminar mi carrera, alcanzando una más de mis metas.

A Víctor y María, mis padres que confiaron en mí en todo momento.

A mis profesores, por ser quienes me formaron como profesional y de manera especial a mi tutor Ing. Geovanni Brito por su apoyo.

INDICE DE CONTENIDOS

PRELIMINARES

Capítulo I

El Problema

Capítulo II

Marco Teórico

Capítulo III

Metodología

RESUMEN EJECUTIVO

El presente trabajo esta enfocado en el diseño de un sistema de seguridad mediante cámaras IP para la empresa PROALPI.

PROALPI nace en el mes de diciembre de 1998, en la ciudad de Píllaro, con la finalidad de procesar productos lácteos fermentados. Además siempre desde una perspectiva de crecimiento global entre todos los actores directos e indirectos con la actividad industrial.

PROALPI está en la búsqueda de nuevas tecnologías, que facilite su crecimiento y a través del diseño de un sistema de seguridad mediante cámaras IP, puede realizar el control y supervisión de la misma en tiempo real y desde cualquier lugar gracias al Internet, ya que se puede mantener un contacto visual más a menudo entre los diferentes departamentos y tener un mejor rendimiento de sus trabajadores.

El diseño del sistema de seguridad beneficia tanto a la empresa como a sus consumidores, ya que permite evitar los delitos o poder identificar a los autores de un robo o de una conducta indebida.

El diseño del sistema de seguridad está planteado de la siguiente manera:

1. Estudio de planos
2. Análisis de áreas críticas
3. Definir áreas a proteger
4. Análisis de tecnología a utilizar
5. Costos
6. Ubicación del PC que hace de servidor
7. Diseño del cableado
8. Diseño del sistema de seguridad

Los equipos a utilizar son los siguientes:

- **CAMARA IP PANASONIC BL-C10**

  Con esta cámara podemos visualizar, grabar y tener acceso en tiempo real desde el Internet.

- **PANASONIC SOFTWARE PANASONIC GRABACION IP**

  Software de grabación para cámaras IP, se puede utilizar desde 4 cámaras hasta 10 cámaras y ser visualizadas simultáneamente.
- **CPU Pentium 4 de 3Ghz**

  Este CPU debe tener un disco duro de más de 300 GB, con el objetivo de tener suficiente espacio para la grabación de las imágenes.
- **Cable UTP categoría 5E**

  Este cable es utilizado para interconectar las cámaras con el switch.
- **Conectores RJ45**

  Los conectores son colocados a los extremos del cable UTP.
- **Jack**

  Es un adaptador que facilita la adaptación de las cámaras al cableado que se realiza.
- **Switch**

  Este dispositivo permite la conexión entre los elementos de la red y el Internet.
- **Canaletas**

  Son elementos que contribuyen o una mejor organización de los cables, así como a dar una buena imagen del sitio donde son colocadas.

El presupuesto obtenido para el sistema de seguridad es de $ 6596.40.

INTRODUCCIÓN

El presente trabajo esta enfocado en el diseño de un sistema de seguridad mediante cámaras IP para la empresa PROALPI.

PROALPI nace en el mes de diciembre de 1998, en la ciudad de Píllaro, con la finalidad de procesar productos lácteos fermentados. Además siempre desde una perspectiva de crecimiento global entre todos los actores directos e indirectos con la actividad industrial.

PROALPI está en la búsqueda de nuevas tecnologías, que facilite su crecimiento y a través del diseño de un sistema de seguridad mediante cámaras IP, puede realizar el control y supervisión de la misma, ya que se puede mantener un contacto visual más a menudo entre los diferentes departamentos y tener un mejor rendimiento, tanto de sus trabajadores como de sus productos.

La comunicación en tiempo real y desde cualquier lugar gracias al Internet permite a PROALPI realizar su trabajo en menor tiempo y con precisión; mientras más rápido se de una orden de acuerdo a los requerimientos se puede solucionar cualquier inconveniente en ese instante.

El diseño del sistema de seguridad beneficia tanto a la empresa como a sus consumidores, pues visualizar y controlar lo que esta sucediendo, tan solo con conectarse a Internet, la tranquilidad y seguridad cuando se esta ausente de un determinado sitio es posible, ya que permite evitar los delitos o poder identificar a los autores de un robo o de una conducta indebida.

El diseño está planteado de la siguiente manera:

9. Estudio de planos
10. Análisis de áreas críticas
11. Definir áreas a proteger
12. Análisis de tecnología a utilizar

13. Costos
14. Ubicación del PC que hace de servidor
15. Diseño del cableado
16. Diseño del sistema de seguridad

Beneficios de un sistema de seguridad

- Visualizar el entorno del trabajo
- Comodidad y seguridad
- Niveles de permisos para una mayor seguridad
- Inversión asegurada
- Sistema abierto
- Potencia y versatilidad

CAPITULO I

EL PROBLEMA

1.1. TEMA DE INVESTIGACIÓN

DISEÑO DE UN SISTEMA DE SEGURIDAD MEDIANTE CÁMARAS IP PARA LA EMPRESA PROALPI DE LA CIUDAD DE PÍLLARO

1.2. PLANTEAMIENTO DEL PROBLEMA

La búsqueda constante del hombre por satisfacer su necesidad de comunicación, ha sido el impulso que ha logrado la instauración en el mundo de instrumentos cada día más poderosos y veloces en el proceso comunicativo. Desde siempre, el hombre ha tenido la necesidad de comunicarse con los demás; de expresar pensamientos, ideas, emociones; de dejar huella de sí mismo. Así también se reconoce la necesidad de buscar, de saber, de obtener información creada, expresada y transmitida por otros, siendo estas acciones esenciales a la naturaleza humana. Tal vez por eso los grandes saltos evolutivos de la humanidad tienen como hito la instauración de algún nuevo instrumento de comunicación, desde la comunicación con señas, hasta la comunicación a distancia por medio de dispositivos tecnológicos avanzados.

Los medios de comunicación han constituido un papel importante dentro del desarrollo de la humanidad. A medida que la ciencia y la tecnología han evolucionado, surge la necesidad de utilizar varias herramientas que mejoren y faciliten la comunicación y que el hombre se desempeñe de una manera más eficiente y con mayor agilidad.

A partir de los cambios constantes y emergentes que se suceden son diversos los aportes que se han hecho, no sólo en cuanto al mejoramiento y optimización de sus particulares procesos de producción, sino en los modos de transmisión de sus mensajes, en la forma como se relacionan con el público y por supuesto, por tratarse también de organizaciones humanas, en su gestión gerencial estratégica, tanto interna como externa.

El impacto que la revolución tecnológica ha tenido en estos tiempos, es bastante evidente como para negar su utilidad; experimentando una revolución comercial y económica dentro de la sociedad mundial, porque traen consigo una infraestructura global, accesible y universal: Internet.

En un mundo presto a cambios, es conveniente ser parte de ello porque con esto podemos acceder a nuevas tecnologías que faciliten el trabajo en las diferentes áreas en las que el ser humano se desenvuelve.

Las empresas, especialmente las de producción están en la búsqueda de nuevas tecnologías, principalmente la empresa PROALPI; que a través del diseño de un sistema de seguridad mediante cámaras IP, puede realizar el control y supervisión de la misma, que a pesar de la inadecuada infraestructura que presenta, se puede mantener un contacto visual más a menudo entre el departamento de administración, el de producción y la maquinaria, para un mejor rendimiento de sus productos y un trabajo eficiente de sus empleados.

La comunicación en tiempo real y desde cualquier lugar gracias al Internet permite a las empresas realizar su trabajo en menor tiempo y con precisión; mientras más rápido se de una orden de acuerdo a los requerimientos se puede solucionar cualquier inconveniente en ese instante.

Es por esto que fue necesario el diseño de un sistema de seguridad mediante cámaras IP, pues permitió un mejor control tanto de la materia prima para evitar robos, como de sus trabajadores para que cumplan sus funciones en el tiempo y espacio adecuado.

1.2.1. FORMULACIÓN DEL PROBLEMA

¿Qué incidencia tiene el diseño de un sistema de seguridad mediante cámaras IP en la empresa PROALPI de la ciudad de Píllaro para la mejora de la producción, de sus productos y de la atención eficiente al cliente?

1.2.2. DELIMITACIÓN DEL PROBLEMA

El presente trabajo investigativo se realizó en la ciudad de Píllaro en la empresa PROALPI (Procesadora de Alimentos Píllaro) en el período Mayo – Septiembre de 2006 con el diseño de un sistema de seguridad mediante cámaras IP.

1.3. JUSTIFICACIÓN

El vigente trabajo resolvió los problemas de comunicación existentes en la empresa, y con el apropiado control y la utilización de tecnología de punta como son las cámaras IP, dimos solución al problema que poseía.

Los avances tecnológicos han permitido al hombre cada día realizar un trabajo con menos esfuerzo y en menor tiempo, motivo por el cual el sistema de seguridad a más de prestar vigilancia, permitió una comunicación inmediata con trabajadores de la empresa.

Todo esto permitió una mayor eficiencia en el trabajo y menor pérdida de insumos en la elaboración de los productos; así también un mejor trato a proveedores y clientes.

El trabajo realizado permitió aplicar los conocimientos adquiridos durante la carrera de Electrónica y Comunicaciones, dio solución a un problema como es la falta de seguridad en la bodega y sistema de producción de la empresa PROALPI de la ciudad de Píllaro y fue un aporte tecnológico que benefició tanto al propietario como a sus empleados y clientes, por cuanto mientras se tenga un excelente producto se mantendrá el prestigio y se producirá más trabajo y por ende un crecimiento económico acorde a la planificación de la empresa.

1.4. OBJETIVOS

1.4.1. GENERAL:

Diseñar el sistema de seguridad basado en cámaras IP para la empresa PROALPI de la ciudad de Píllaro para elevar la calidad de la producción.

1.4.2. ESPECÍFICOS:

- Determinar las potencialidades y falencias de la empresa.
- Analizar los parámetros requeridos para el sistema de seguridad.
- Mantener comunicación abierta e inmediata entre el departamento de administración y departamento de producción.
- Detectar el trato que se da a proveedores y a consumidores.
- Controlar al personal con cámaras IP.
- Elevar la calidad y producción de PROALPI.

CAPITULO II

MARCO TEÓRICO

2.1. ANTECEDENTES INVESTIGATIVOS

Revisado los archivos existentes en la Biblioteca de la Facultad de Ingeniería en Sistemas, se concluye que no se existen antecedentes sobre el estudio del tema de investigación planteado, que descarten su realización.

2.2. FUNDAMENTACIÓN LEGAL

PROALPI nace en el mes de diciembre de 1998, con la finalidad de procesar productos lácteos fermentados. Además siempre desde una perspectiva de crecimiento global entre todos los actores directos e indirectos con la actividad industrial.

PROALPI es una empresa alimenticia que procesa productos lácteos, a través de procesos tecnológicos adecuados sustentados en un sistema de Gestión de Calidad para satisfacer los requerimientos establecidos por el cliente en términos de calidad, precios competitivos e innovación de productos, apoyando la relación con una entrega oportuna, servicial y segura, prevaleciendo el mutuo beneficio con todos los involucrados en nuestra actividad.

Autorizaciones de creación

La empresa con su nombre comercial PROALPI, y siendo su principal actividad económica la producción de yogurt.

Se encuentra ubicado en la provincia de Tungurahua, cantón Santiago de Píllaro, en la parroquia Marcos Espinel.

2.3. CATEGORÍAS FUNDAMENTALES

INTERNET

Internet es sencillamente una red de computadora de trabajo que esta interconectada con otras para compartir información de cualquier índole. Siendo una red de computadoras a nivel mundial que agrupa a distintos tipos de redes usando un mismo protocolo de comunicación. Los usuarios de Internet pueden compartir datos, recursos y servicios.

Así también Internet, se puede concebir como una comunicación en cables que permite viajar (por así decirlo) hasta llegar a otra máquina remota, solicitando información o simplemente como consulta concediendo un mejor acceso y obtención de datos que permita agilizar la toma de decisiones o dar soluciones con mayor eficacia. O bien es la gran red de computadoras conectadas por las diversas autopistas de información y principal punto de acceso, que cualquier persona puede interactuar con miles de personas.

Internet tiene un impacto profundo en el trabajo, el ocio y el conocimiento. Gracias a la Web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea.

Comparado a las enciclopedias y a las bibliotecas tradicionales, la web ha permitido una descentralización repentina y extrema de la información y de los datos. Algunas compañías e individuos han adoptado el uso de los *weblogs*, que se utilizan en gran parte como diarios actualizables. Algunas organizaciones comerciales animan a su personal para incorporar sus áreas de especialización en sus sitios, con la esperanza de que impresionen a los visitantes con conocimiento experto e información libre.

Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos, en este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada para las personas.

Desde una perspectiva cultural del conocimiento, internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas proporciona una cantidad significativa de información y de una interactividad que sería inasequible de otra manera.

SISTEMAS DE SEGURIDAD

Con el incremento en datos, investigación y desarrollo y competencia corporativa, muchas compañías se están percatando de que se necesita no sólo proteger sus datos, sino también sus recursos humanos. Los sistemas de televisión de circuito cerrado (CCTV [Closed Circuit Television Systems]) y los de vigilancia por video se están volviendo más comunes en los edificios de oficinas, estructuras externas, escuelas e incluso en las calles citadinas. La vigilancia se ha convertido en un componente integral de los métodos de control de acceso enriquecidos con biométricos, sistemas de rastreo de seguridad y sistemas de rastreo de acceso.

Los sistemas tradicionales CCTV requieren una infraestructura separada que utiliza cable coaxial. Este cable fue diseñado para transmisiones punto a punto de video desde una cámara hasta una grabadora en el mismo sitio. El desarrollo de video digital permitió el progreso hacia cables de par trenzado y fibra óptica. Las secuencias de imágenes se almacenan en formato digital en servidores u otras computadoras en lugar de cintas de video, aliviando los problemas inherentes a medios magnéticos. La influencia creciente de la industria TI (Tecnologías de la Información) conduce los esfuerzos de fabricantes de cámaras, proveedores de

almacenamiento y diseñadores de chips a ofrecer full motion video en una gran variedad de plataformas.

Esta nueva especie de video permite transmisiones IP (Internet Protocol) de las señales de video a los dispositivos direccionables IP y pueden transmitirse en combinación con secuencias de voz y/o video. Estas transmisiones pueden almacenarse o simplemente mirarse en tiempo real. Este artículo cubre los principios y evoluciones de estas tecnologías enfocadas en lo último en tecnologías de video digital IP aunados con información importante de necesidades de infraestructura y requisitos para su implementación.

VIDEO DIGITAL SOBRE IP

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

TCP/IP se ha convertido en el estándar de facto para las redes. Su arquitectura abierta permite que varios sistemas puedan compartir el espacio de red, y aprovechar estas nuevas tecnologías para aumentar su capacidad, confiabilidad, escalabilidad u accesibilidad de los recursos de red. Con la habilidad de utilizar la infraestructura existente, un edificio

puede volverse totalmente automatizado utilizando un solo sistema de cableado. Esta automatización puede incluir no sólo CCTV, sino también control de accesos, sistemas de fuego y seguridad (de la vida), sistemas de automatización de edificios, voz y, por supuesto, tráfico de red. Los administradores y los usuarios de la red no estarán más encadenados a un solo puesto ya que el control y/o administración de estos sistemas puede realizarse desde cualquier estación de trabajo con acceso a la red. Esto mismo aplica para el personal de seguridad. Ellos pueden ubicarse en cualquier lugar. La cámara digital se vuelve ahora el punto de falla, no el centro de control, ya que es extremadamente fácil hacer redundantes los servidores digitales ya sea en un solo sitio o distribuidos en múltiples ubicaciones.

Las cámaras IP, servidores de video IP y teclados IP pueden colocarse en cualquier punto. Los teclados IP pueden controlar actualmente las funciones PTZ (Pan, Tilt and Zoom) de cualquier videocámara con base en su dirección IP. Como cualquier protocolo IP, las funciones de administración son incorporadas en la transmisión. Esto incluye DSP (Digital Signal Processing), manejo de alarmas, grabación, capacidades de búsqueda y/o archivo, calendarización y automatización. Estas funciones de administración y control utilizan SNMP (Simple Network Management Protocol) y otros cuadros de control, todas ellas parte del estándar IP.

Estas cámaras pueden equiparse con características avanzadas tales como sensores de movimiento, PTZ automatizado y, si se desea, salidas análogas de video. Las versiones más recientes vienen equipadas con DVRs internos que pueden replicarse con un servidor DVR centralizado.

Otro sistema basado en IP, CCTP (Closed Circuit Twisted Pair), fue introducido por una compañía llamada Anixter (www.anixter.com/cctp). Este sistema permite que las señales de video, control y alimentación eléctrica sean transmitidas en un solo cable de par trenzado. Este sistema

tipo chasis puede acomodar 40 cámaras fijas y 16 cámaras PTZ (pan-tilt-zoom) en un sólo chasis. La adición de alimentación eléctrica a la infraestructura provee un beneficio adicional al sistema al facilitar los movimientos adiciones y cambios así como instalaciones iniciales, ya que no se requiere instalar un cable eléctrico en paralelo con el sistema de cableado.

NORMAS DE COMPRESIÓN DE VIDEO

Las imágenes digitales de alta resolución necesitan mayor ancho de banda para transmisión y más espacio en disco para almacenamiento. El almacenaje y la transmisión de estas imágenes son muy problemáticos en las tecnologías e infraestructuras tanto en la intranet como en el Internet. Se han desarrollado algoritmos de compresión para ayudar a asegurar transmisiones de alta calidad sobre mecanismos de menor ancho de banda. Existe un conflicto entre la tasa de transferencia de paquetes y la calidad de la imagen. JPEG, JPEG2000, MPEG-1, 2, 4, Wavelet y H.261/H.263 son todos ellos métodos de compresión que tratan con estas transmisiones.
JPEG (Joint Photographic Experts Group) y MPEG (Motion Pictures Expert Group) son normas ISO/IEC que permiten transmisiones de video de alta calidad.

Cada vez son más las empresas que utilizan la transmisión de video como método para reducir gastos y para incorporar nuevos servicios de valor agregado para monitorear, supervisar y llevar el control a distancia en las sucursales y áreas estratégicas de las organizaciones.

El video permite poner a disposición de los usuarios un nuevo canal de comunicación que complementa a los tradicionales sistemas de circuito cerrado de televisión CCTV y que permite reducir gastos y tiempos de transporte, reducir tiempos en la toma de decisiones, vigilar infraestructuras y aumentar el impacto de supervisión.

En el campo de la vídeo vigilancia, se apuesta por la introducción permanente de soluciones que aumenten la seguridad de las instalaciones y personas. Las soluciones incorporan técnicas de detección de movimiento en imágenes y notificación de incidencias mediante el envío de alarmas e imágenes a los encargados de esta delicada área.

BENEFICIOS DE LA VIDEO VIGILANCIA

- Observa tu casa u oficina a través de Internet.
- Monitorea tu negocio para aumentar la productividad.
- Cuida a tus hijos y no pierdas detalle de ellos.
- Acceso desde cualquier lugar vía Internet.

VIGILANCIA IP

Los nuevos servicios de Banda Ancha, como el ADSL, han hecho posible la generalización del uso de sistemas de Video IP, y los fabricantes de cámaras han adaptado sus productos para trabajar bajo redes IP de bajo costo, transmitiendo sus imágenes a través de Internet y se controlan de forma remota, detectando cualquier movimiento e informando al momento de lo que esta sucediendo.

Para poder cumplir con las misiones de Video Vigilancia las nuevas cámaras vienen dotado con sensores de movimiento, que al ser activados empiezan a transmitir y a grabar de forma automática todo lo que sucede.

Las cámaras IP podrán supervisar su negocio desde un ordenador en cualquier lugar del mundo.

VIDEO SOBRE IP

Los nuevos protocolos de compresión de video junto con la aparición de la Banda Ancha por ADSL han hecho posible la transmisión de imágenes, a través de Internet. Esto unido a la aparición de nuevas cámaras de Video IP gestionables remotamente, convierten en una solución idónea los sistemas de Video Vigilancia a través de Internet.

CÁMARAS IP

La nueva generación de cámaras de Video IP permite la transmisión de imágenes en tiempo real, así como su almacenamiento remoto y su comunicación electrónica. También pueden incorporar la tecnología WiFi, permitiéndonos su instalación en cualquier lugar sin necesidad de cableado.

El software de vigilancia IP funciona con cámaras de red y servidores de vídeo y proporciona funciones de monitorización de vídeo, de grabación y de gestión de eventos. Los usuarios pueden realizar una grabación de vídeo continua, programada, activada por alarma y/o por detección de movimiento.

CONTROL REMOTO

Es fundamental, poder monitorizar todo lo que está sucediendo en tiempo real y a la vez es captando por las diferentes cámaras instaladas, para ello se utiliza un software que se encargara de esta misión, con el que podremos programar los modos y la actividad de cada cámara.

ALARMAS

Si se requiere se puede configurar las cámaras para que, en el caso de detectar movimiento, informen inmediatamente a un centro de ayuda lo que está sucediendo en ese momento.

Es así que el sistema de video seguridad ofrece una solución avanzada y total para disponer de un sistema de vigilancia programada o continua y grabación de cámaras de vigilancia. El sistema se basa en plataforma PC estándar, utilizando las últimas tecnologías en compresión de vídeo digital, comunicaciones, supervisión de señales de Entrada/Salida y gestión de vídeo grabaciones, tanto de forma local como remota.

El sistema está compuesto por dos partes importantes: el sistema de vigilancia, gestión y grabación local de vídeo y el sistema de vigilancia y gestión remota.

- ***Sistema de vigilancia, gestión y grabación local de vídeo*:**

  Formado por las placas de captura de vídeo y la aplicación software encargada de su gestión. Este sistema permite la vigilancia y la grabación de la información de vídeo de las cámaras.

- ***Sistema de vigilancia y gestión remota:***

  Se encarga de permitir el acceso tanto a las imágenes en vivo, como a las alarmas previamente generadas y al control remoto de señales desde una estación de trabajo remota, empleando para ello una LAN o Internet.

En este completo sistema de vigilancia de ultima tecnología que incluye grabación digital de imágenes y visión remota desde Internet. El sistema de vigilancia esta compuesto por un servidor de vídeo web, un grabador digital sobre disco duro y seis cámaras de alta resolución y 100 metros de cable con conectores para la conexión de las cámaras. Con este sistema de vigilancia puede ver las imágenes en directo o las imágenes grabadas, tanto de forma local como a través de Internet.

Todo el sistema de vigilancia funciona de forma autónoma, por lo que no hay que ocuparse de el en ningún momento, ya que no hay cintas que cambiar y no hay mantenimiento alguno, consiguiendo siempre imágenes con calidad digital y sin deterioro.

APLICACIONES DEL SISTEMA DE VIGILANCIA

- Sistema de Vigilancia de cadena de establecimientos, como tiendas, restaurantes, fábricas, hoteles, etc.
- Sistema de grabación distribuida para vigilancia local.
- Monitorización remota para distintas sucursales de una entidad.
- Vigilancia en industrias, plantas de fabricación, grandes naves industriales.
- Tele vigilancia para distintas oficinas de empresas multinacionales.
- Sistema de vigilancia para aparcamientos, almacenes, gasolineras, etc.

2.4. HIPÓTESIS

El diseño de un sistema de seguridad en la empresa PROALPI de la ciudad de Píllaro, permitirá elevar el nivel de calidad de sus productos y una atención eficiente a sus clientes.

2.5. DETERMINACIÓN DE VARIABLES

2.5.1. Variable Independiente

Sistema de Seguridad

2.5.2. Variable Dependiente

Cámaras IP

CAPITULO III

METODOLOGÍA

3.1. ENFOQUE

La actual investigación se centra dentro de las características cualitativas - cuantitativas, ya que busca analizar y comprender las causas y fenómenos tomando muy en cuenta todas las condiciones que rodea la teoría, así como la percepción que tienen los entes involucrados en esta realidad.

3.2. MODALIDAD BÁSICA DE LA INVESTIGACIÓN

En el presente trabajo de investigación, se utilizaron fuentes secundarias de recolección de datos como:

Investigación De Campo (fuentes referenciales de expertos en el área)
Investigación Experimental (establece relación causa – efecto)
Internet. (Páginas Web especializadas en el tema)

3.3. NIVEL O TIPO DE INVESTIGACIÓN

El estudio parte de una investigación de nivel exploratorio, pasa a la explicativa e identifica los elementos y características importantes de la variable dependiente con relación a la independiente y estableció el diseño del sistema de seguridad mediante cámaras IP adecuado para la empresa.

3.4. RECOLECCIÓN DE INFORMACIÓN

Para recolectar información se empleará recursos como: libros, documentación, Internet, consultas y entrevistas a los profesionales en el área de seguridad y la observación.

3.5. PROCESAMIENTO Y ANÁLISIS

El procesamiento de la información recolectada seguirá el siguiente procedimiento.

- Revisión de la información recolectada.
- Repetición de la recolección de la información en ciertos casos individuales para corregir fallas.
- Manejo de la información.
- Estudio estadístico de datos para presentación de resultados

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En primera instancia se realizó un sondeo del impacto que tendría en los empleados el diseño del sistema de seguridad mediante cámaras IP, con el que pude darme cuenta que este diseño serviría para aumentar la productividad y mejorar el trato entre las personas directa e indirectamente involucradas en la empresa.

El diseño del sistema de seguridad mediante cámaras IP para la empresa PROALPI de la ciudad de Píllaro, brinda mayor confiabilidad a su gerente general, ya que puede comunicarse con sus empleados en el instante que desee o cuando se presente algún inconveniente que requiera de solución inmediata y oportuna.

El presente diseño además a permitido aumentar la relación jefe – empleado, dando un realce a las relaciones humanas dentro de la empresa.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

De acuerdo a los objetivos propuestos y a la realización del presente trabajo investigativo se puede concluir lo siguiente:

- Una vez realizado el análisis de áreas críticas dentro de la empresa se pudo determinar los lugares que requerían una mayor vigilancia.
- Mientras mayor control tengan los empleados, mejor es su desempeño.
- Se observó una mejor utilización y optimización de los materiales para la elaboración de sus productos.
- Se determinó que no es necesaria la presencia física para la vigilancia del personal, tan solo hay que recurrir a los avances tecnológicos como es la utilización de las cámaras IP.
- El proyecto ayudó a mantener una mejor comunicación entre empleados y subalternos.
- Existió orden y mayor responsabilidad de los empleados en la realización de sus actividades.
- El uso del software y la grabación de video en el computador son de fácil reproducción y grabación.
- Se puede visualizar a distancia lo que sucede en la fábrica, mediante el uso de Internet.
- Por medio del Internet se puede tener manipulación sobre las cámaras y emitir ordenes desde cualquier lugar del planeta.
- El sistema de seguridad brinda mayor protección a la fábrica.

5.2. RECOMENDACIONES

Una vez realizado el trabajo se recomienda lo siguiente:

- Realizar un estudio y planificación sobre seguridad
- Utilizar cámaras IP, como sistema de seguridad ya que es muy útil y de fácil acceso.
- Establecer áreas de mayor vigilancia para realizar un mejor control de las mismas.
- Ubicar las cámaras en áreas imperceptibles y con su debida protección para evitar robos y manipulación.
- Usas discos duros mayores a 300Gb para tener un buen espacio para la grabación de las imágenes.
- El ancho de banda mínimo requerido debe ser de 64 Kb por segundo.
- Tener un computador único dedicado a la grabación y monitoreo constante de video.

CAPITULO VI

PROPUESTA

6.1. APARTADO 1

ANTECEDENTES

PROALPI nace en el mes de diciembre de 1998, en la ciudad de Píllaro, con la finalidad de procesar productos lácteos fermentados. Además siempre desde una perspectiva de crecimiento global entre todos los actores directos e indirectos con la actividad industrial.

PROALPI es una empresa alimenticia que procesa productos lácteos, a través de procesos tecnológicos adecuados sustentados en un sistema de Gestión de Calidad para satisfacer los requerimientos establecidos por el cliente en términos de calidad, precios competitivos e innovación de productos, apoyando nuestra relación con una entrega oportuna, servicial y segura, prevaleciendo el mutuo beneficio con todos los involucrados en nuestra actividad.

MISIÓN

Procesar y comercializar productos alimenticios seguros para el consumo humano, sustentados en un Sistema de Gestión de Calidad en el que prevalezca el mutuo beneficio para todos los involucrados en esta actividad.

VISIÓN

Encaminar nuestra organización hacia el éxito a través de la planificación y administración de actividades de forma sistemática y transparente. Así como con la implementación de nuevos productos y tecnologías.

OBJETIVOS

General

Tener un control adecuado de las actividades de fabricación

Específicos

- Entregar a nuestros clientes productos alimenticios que satisfagan necesidades específicas.
- Garantizar el cumplimiento de los estándares de calidad.
- Disponer de proveedores calificados.
- Comprometer al personal con el cumplimiento de las responsabilidades asignadas
- Emprender la superación personal, profesional y espiritual de todos los colaboradores de la empresa.
- Gestionar las actividades y recursos como un proceso para lograr resultados de calidad.
- Incrementar el volumen de producción y ventas mediante la participación eficaz y eficiente delos responsables de los procesos.

6.2. APARTADO 2

VIDEO

La transmisión de video sobre redes de telecomunicaciones está llegando al punto de convertirse en un sistema habitual de comunicación debido al crecimiento masivo que ha pretendido Internet en estos últimos años, es así que lo estamos utilizando para ver películas o comunicarnos con conocidos, pero también se usa para dar clases remotas, para hacer diagnósticos en medicina, videoconferencia, distribución de TV, video bajo demanda, distribuir multimedia en Internet.

Debido a la necesidad de su uso que se plantea en el presente y futuro, se han proporcionado distintas soluciones y sucesivos formatos para mejorar su transmisión; siendo los sistemas actuales de distribución de video aplicaciones de elevada demandan.

El video no es nada más que la reproducción en forma secuencial de imágenes, que al verse con una determinada velocidad y continuidad dan la sensación al ojo humano de apreciar el movimiento natural. Junto con la imagen, el otro componente es el sonido.

TRANSMISIÓN DE VIDEO DIGITAL

La transmisión digital y la distribución de información audiovisual permiten la comunicación multimedia sobre las redes que soportan la comunicación de datos, brindando la posibilidad de enviar imágenes en movimiento a lugares remotos. Pero no es todo tan bonito a la hora de transmitirlo por red, debido a que nos encontramos con sucesos como lentitud entre la reproducción de imágenes, errores de transmisión, o pérdidas de datos.

Existen dos formas de transmisión de datos, analógica y digital. Una de las características del video es que está compuesto por señales analógicas, con lo que

se pueden dar las dos formas de transmisión. En los últimos años la transmisión de datos se ha volcado hacia el mundo digital ya que supone una serie de ventajas frente a la transmisión analógica.

Al verse la información reducida a un flujo de bits, se consigue una mayor protección contra posibles fallos ya que se pueden introducir mecanismos de detección de errores, se elimina el problema de las interferencias, podemos disminuir el efecto del ruido en los canales de comunicación, conseguir codificaciones más óptimas y encriptado, mezclar con otros tipos de información a través de un mismo canal, y poder manipular los datos con ordenadores para comprimirlos.

Además si queremos difundir el video por vías digitales tendremos que digitalizarlo, con lo que debe ser capturado en su formato analógico y almacenado digitalmente logrando así que sea menos propenso a degradarse durante la transmisión.

Existen dos tipos de redes de comunicación, una es la de conmutación de circuitos y la otra de conmutación de paquetes. En la conmutación de circuitos, donde la comunicación está permanentemente establecida durante toda la sesión, un determinado ancho de banda es asignado para la conexión, y el tiempo de descarga del video puede predecirse, pero tienen la desventaja de que las sesiones son punto a punto y limitan la capacidad de usuarios.

En la conmutación de paquetes pueden acomodarse más fácilmente las conferencias multipunto. Aquí el ancho de banda esta compartido pero es variable, lo que supone una importante mejora puesto que, si el bit rate (número de bits por segundo) es fijo la calidad de la imagen variará dependiendo del contenido de los fotogramas. Cumpliéndose el ancho de banda, la resolución, y la compresión de audio sean idénticas para cada cliente que recibe el video.

El video es muy sensible al retardo de la red, ya que puede provocar cortes en las secuencias. La pérdida de alguna información en el video sin comprimir no es muy relevante, ya que al perderse un fotograma, el siguiente fotograma proporciona la suficiente información para poder interpretar la secuencia. En cambio el video comprimido es mucho más sensible a errores de transmisión, ya que las técnicas de compresión que se valen de la redundancia espacial y temporal pueden perder la información de esta redundancia y los efectos de la falta de datos pueden propagarse en los próximos fotogramas.

Es por eso que actualmente la comunicación con video vía Internet no promete una elevada fiabilidad de transmisión. Algunas técnicas de compresión compensan esta sensibilidad a la pérdida de datos enviando la información completa sobre un fotograma cada cierto tiempo, incluso si los datos del fotograma no han cambiado. Esta técnica también es útil para los sistemas de múltiples clientes, para que los usuarios que acaban de conectarse, reciban las imágenes completas.

Nos podemos preguntar cuál es la tecnología de red adecuada para las aplicaciones de video, pero siempre dependeremos del entorno en el que trabajemos. Por ejemplo si disponemos de una alto ancho de banda el tipo de red adecuada seria ATM; para un entorno de red de área local podríamos usar Fast Ethernet, y actualmente para que el usuario de Internet, ADSL.

COMPONENTES

Componentes digital o componentes análogos se refiere al estándar de la señal de video establecido por SEMPTE.

La señal de video analógica se compone por luminancia (Y), componente azul (Pb) y componente rojo (Pr). Al procesar la señal por componentes se obtiene la máxima calidad posible al día de hoy gracias a los avances de la electrónica.

Los componentes se mezclan al final sólo para transmitirse y entonces se vuelven video compuesto, que sto es la señal de video que tiene sus componentes necesarios: luminancia, crominancia y sincronía.

DIGITALIZACIÓN

La información a digitalizar serán las imágenes. Cada cuadro de imagen es muestreado en unidades de píxeles, con lo que los datos a almacenar serán los correspondientes al color de cada píxel.

Tres componentes son necesarias y suficientes para representar el color y para ser interpretado por el ojo humano. El sistema de codificación de color usado es el RGB (Red, Green, Blue).

La digitalización de una señal de video analógico es necesario muestrear todas las líneas de video activo. La información de brillo y color son tratadas de forma diferente por el sistema visual humano, ya que es más sensible al brillo que al color. Con lo que se usa un componente especial para representar la información del brillo, la luminancia, una para el color y la saturación, la crominancia. Cada muestra de color se codifica en señal Y-U-V (Y luminancia, U y V crominancia) partiendo de los valores del sistema RGB. Con este sistema las diferencias de color pueden ser muestreadas sin resultados visibles, lo que permite que la misma información sea codificada con menos ancho de banda.

Un ejemplo de conversión de señal analógica de televisión en color a una señal en video digital sería:

Sistema PAL: 576 líneas activas, 25 fotogramas por segundo, para obtener 720 píxeles y 8 bits por muestra a 13,5Mhz:

- Luminancia(Y): 720x576x25x8 = 82.944.000 bits por segundo
- Crominancia(U): 360x576x25x8 = 41.472.000 bits por segundo
- Crominancia(V): 360x576x25x8 = 41.472.000 bits por segundo

Número total de bits: 165.888.000 bits por segundo (aprox. 166Mbits/sg). Ninguno de los sistemas comunes de transmisión de video proporciona transferencias suficientes para este caudal de información

Las imágenes de video están compuestas de información en el dominio del espacio y el tiempo. La información en el dominio del espacio es provista por los píxeles, y la información en el dominio del tiempo es provista por imágenes que cambian en el tiempo. Puesto que los cambios entre cuadros colindantes son diminutos, los objetos aparentan moverse suavemente.

El valor de luminancia de cada píxel es cuantificado con 8 bits para el caso de imágenes blanco y negro. En el caso de imágenes de color, cada píxel mantiene la información de color asociada; una imagen completa es una composición de tres fotogramas, uno para cada componente de color, así los tres elementos de la información de luminancia designados como rojo, verde y azul, son cuantificados a 8 bits.

Pero la transmisión digital de video tiene también alguna desventaja respecto a la analógica, por ejemplo, en una videoconferencia, cuando distintos usuarios envían sonido al mismo tiempo, si el proceso fuera analógico las distintas ondas se sumarían y podríamos escuchar el conjunto de todas ellas. Al ser digital, los datos llegan en paquetes entremezclados, lo que dificulta la compresión.

TIPOS DE COMPRIMIDO / DESCOMPRIMIDO

Para cada punto de la imagen se asigna un determinado número de bits que representarán el color de dicho punto. Si la imagen es en blanco y negro, bastará 1bit para representarlo, mientras que para 256 colores serán necesarios 8 bits. De esta forma tendremos la imagen digitalizada, pero almacenar esta información dependerá del número de píxeles que utilicemos por imagen. Por ejemplo una imagen de 640 x 480 puntos con 256 colores ocupa 300Kb, y si tenemos una

secuencia de video a 25 fotogramas por segundo significaría que un solo segundo ocuparía 7.500Kb. y todo esto sin contar el audio. La información de video compuesta de esta manera posee una cantidad tremenda de información; por lo que, para transmisión o almacenamiento, se requiere de la compresión de la imagen.

La compresión del video generalmente implica una pérdida de información y una consecuente disminución de calidad. Pero esto es aceptable porque los algoritmos de codificación están diseñados para descartar la información redundante o que no es perceptible por el ojo humano. Aunque sabemos que la calidad del video es inversamente proporcional al factor de compresión.

La compresión es un arma de doble filo, ya que el video comprimido es más sensible a los errores. Un error en video comprimido puede hacer ilegible la imagen, con lo que se añade redundancia para recuperar esa información. El video comprimido en general debe transmitir información por un canal más pequeño del que necesitaría para ser transmitido y poder ser visualizado en tiempo real. Así la información de audio y video deben ser procesadas por los codecs antes de ser transmitidos. Los codecs derivan de las palabras compresor y descompresor, y los módulos de software permiten la compresión y descompresión de los ficheros de audio y video para que puedan ser transmitidos por redes de baja velocidad.

La digitalización y la compresión pueden darse conjuntamente y en tiempo real para facilitar la comunicación y la interacción. Los codecs más utilizados son los siguientes: Microsoft Video1, Microsoft RLE, Intel Indeo R2, Intel Indeo R3, Intel YUV9, CinePak, Captain Crinch, Creative Compressor.

Las señales recibidas deben ser decodificadas antes de poder ser visualizadas por el usuario. Durante este proceso se puede producir: el video fantasma o suavización de imagen, que es la forma con la que los codecs compensan los elevados flujos de información. Cuando ocurre esto, el codec comprime la información reduciendo el “frame rate” (número de imágenes por segundo), el

cual puede hacer que los movimientos rápidos parezcan borrosos. El codec también modifica la resolución para comprimir la información lo cual hace que la imagen se pueda ver desplazada. Entonces, para reducir estos efectos, se disminuye el flujo de información visual, pero también puede darse un retardo de audio.

En la red de Internet por ejemplo la mayoría de los usuarios están conectados a velocidades de 56.6Kbps, 33.6Kbps o 28.8Kbps, y el video descomprimido para ser enviado en calidad broadcast requiere un ancho de banda de red de 160Mbps, en calidad CD requiere aproximadamente 2.8Mbps, y con los modems actuales sería imposible conseguir las velocidades requeridas para su transmisión. Aquí tienen un papel importante los codecs que se optimizan para conseguir la mayor calidad posible en bajos índices de transferencia. Son usados para codificar el video en tiempo real o pregrabado y ser mandado por la red para que el usuario final solamente con una aplicación que lo descomprima pueda al instante visionar en su terminal.

COMPRESIÓN

La técnica de compresión de video consiste de tres pasos:

1. Pre-procesamiento de la fuente de video de entrada
   Aquí se realiza el filtrado de la señal de entrada para remover componentes no útiles y el ruido que pudiera haber en esta.
2. Conversión de la señal a un formato intermedio común (CIF)
3. Compresión
   Las imágenes comprimidas son transmitidas de forma digital y se hacen llegar al receptor donde son reconvertidas al formato común CIF y son desplegadas después de haber pasado por la etapa de post-procesamiento.

Mediante la compresión de imagen se elimina información redundante. Se ayuda de la redundancia espacial y temporal. La redundancia temporal es reducida primero usando similitudes entre sucesivas imágenes, usando información de las

imágenes ya enviadas. Cuando se usa esta técnica, sólo es necesario enviar la diferencia entre las imágenes, es decir las zonas de la imagen que han variado entre dos fotogramas consecutivos, lo que elimina la necesidad de transmitir la imagen completa.

La compresión espacial se vale de las similitudes entre píxeles adyacentes en zonas de la imagen lisas, y de las frecuencias espaciales dominantes en zonas de color muy variado. El método para eliminar las redundancias en el dominio del tiempo es el de codificación de intercuadros, que también incluye los métodos de compensación / estimación del movimiento, el cual compensa el movimiento a través de la estimación del mismo. En el otro extremo, las redundancias en el dominio espacial es llamado codificación intracuadros, la cual puede ser dividida en codificación por predicción y codificación de la transformada usando la transformada del coseno.

La transformada del coseno o DCT es una implementación específica de la transformada de Fourier donde la imagen es transformada de su representación espacial a su frecuencia equivalente. Cada elemento de la imagen se representa por ciertos coeficientes de frecuencia. Las zonas con colores similares se representan con coeficientes de baja frecuencia y las imágenes con mucho detalle con coeficientes de alta frecuencia. La información resultante son 64 coeficientes DCT. El DCT reordena toda la información y la prepara para la cuantización.

El proceso de cuantización es la parte del algoritmo que causa pérdidas. La cuantización asigna un número de bits específico a cada coeficiente de frecuencias y entonces comprime los datos asignando unos cuantos bits a los coeficientes de alta frecuencia, sin que lo note el observador. Los parámetros de la cuantización son optimizados, pero el proceso aún deteriora la calidad del video. Generalmente se acepta que un factor de compresión de 2:1 (aproximadamente 10Mb/seg), se pueden apreciar visualmente algunas pérdidas en la integridad del video. El proceso de decodificación es básicamente el inverso del proceso de codificación.

La compresión del audio está descrita por tres parámetros: ratio de muestreo (numero de muestras por segundo), bits por muestra (numero de bits para representar cada valor), y número de canales (mono o estéreo). Los estándares de video digital más conocidos son: MPEG, Quicktime, AVI, MOV, real video, ASF; y para video analógico: NTSC, PAL, SECAM.

TIPOS DE VIDEO

MPEG

MPEG (Grupo de Expertos en Imágenes en movimiento) es un estándar internacional, definido por un comité llamado MPEG formado por la ISO, para la representación codificada y comprimida de imágenes en movimiento y audio asociado, orientado a medios de almacenamiento digital

El algoritmo que utiliza además de comprimir imágenes estáticas compara los fotogramas presentes con los anteriores y los futuros para almacenar sólo las partes que cambian. La señal incluye sonido en calidad digital. El inconveniente de este sistema es que debido a su alta complejidad necesita apoyarse en un hardware específico.

MPEG aplica la compresión temporal y la espacial; requiere una intensiva computación para su codificación, aunque se consiguen ratios desde 50:1 hasta 200:1

Existen diferentes opciones dependiendo del uso:

MPEG-1

Guarda una imagen, la compara con la siguiente y almacena sólo las diferencias. Se alcanzan así grados de compresión muy elevados. Define tres tipos de fotogramas:

- Fotogramas I o Intra-fotogramas: son los fotogramas normales o de imagen fija, proporcionando una compresión moderada, en JPEG.

- Fotogramas P o Predichos: son imágenes predichas a partir de la anterior. Se alcanza una tasa de compresión muy superior
- Fotogramas B o bidireccionales: se calculan en base a los fotogramas inmediatamente anterior y posterior. Consigue el mayor grado de compresión a costa de un mayor tiempo de cálculo.

MPEG-2

Con una calidad superior al MPEG-1, fue universalmente aceptado para transmitir video digital comprimido con velocidades mayores de 1Mb/s aproximadamente, con MPEG-2 pueden conseguirse elevados ratios de hasta 100:1, dependiendo de las características del propio video, normalmente define dos sistemas de capas, el flujo de programa y el flujo de transporte. Se usa uno u otro pero no los dos a la vez.

El flujo de programa funcionalmente es similar al sistema MPEG-1. La técnica de encapsulamiento y multiplexación de la capa de compresión produce paquetes grandes y de varios tamaños. Los paquetes grandes producen errores aislados e incrementan los requerimientos de buffering en el receptor/decodificador para demultiplexar los flujos de bits. El flujo de transporte consiste en paquetes fijos de 188 bytes lo que decrementa el nivel de errores ocultos y los requerimientos del buffering receptor.

MPEG4

Es un estándar relativamente nuevo orientado inicialmente a las videoconferencias, y para Internet. El objetivo es crear un contexto audiovisual en el cual existen unas primitivas llamadas AVO (objetos audiovisuales). Se definen métodos para codificar estas primitivas que podrían clasificarse en texto y gráficos.

La comunicación con los datos de cada primitiva se realiza mediante uno o varios “elementary streams” o flujos de datos, cuya característica principal es la calidad de servicio requerida para la transmisión, que ha sido especialmente diseñado para

distribuir videos con elevados ratios de compresión, sobre redes con bajo ancho de banda manteniendo una excelente calidad para usuarios con buen ancho de banda, desde usuarios con modems de 10kbps a usuarios con 10Mbps.
Es rápido codificando el video de alta calidad, para contenidos en tiempo real y bajo demanda.

MJPEG

Motion-JPEG es una versión extendida del algoritmo JPEG que comprime imágenes. Básicamente consiste en tratar al video como una secuencia de imágenes estáticas independientes a las que se aplica el proceso de compresión del algoritmo JPEG una y otra vez para cada imagen de la secuencia de video. Existen cuatro modos de operación para el JPEG: secuencial, progresiva, sin perdida, y jerárquica. Normalmente se utiliza el modo secuencial.

La ventaja es que se puede realizar en tiempo real e incluso con poca inversión en hardware. El inconveniente de este sistema es que no se puede considerar como un estándar de video pues ni siquiera incluye la señal de audio. Otro problema es que el índice de compresión no es muy grande.

JPEG utiliza una técnica de compresión espacial, la intracuadros o DCT. El sistema JPEG solamente utiliza la compresión espacial al estar diseñado para comprimir imágenes individuales. Motion-JPEG es el metodo elegido para las aplicaciones donde se envia la misma informacióin a todos los usuarios, las broadcast.

STREAMING VIDEO

Streaming video, o video en tiempo real, es la tecnología que permite la transmisión y recepción de imágenes y sonidos de manera continua a través de una red. A diferencia de otros formatos de audio y video, en los que es necesario esperar que el archivo sea cargado en el equipo para su visualización, esta tecnología permite apreciar el contenido conforme se va teniendo acceso a la información del archivo.

EL servidor de streaming permite visionar el video de forma continua porque hace uso de un buffer, donde van cargándose algunos segundos de la secuencia antes de que sean mostrados; cuando se detecta un periodo de congestión de red, se visualizarán los datos que tenemos ya almacenados en el buffer. De esta forma el cliente obtiene los datos tan rápido como el servidor y la red lo permitan.

El streaming puede decirse que funciona de forma inteligente ya que asegura al usuario que recibirá la más alta calidad posible dependiendo de la velocidad de conexión o de los problemas de conexión de la red. Tradicionalmente la congestión de la red forzaba al usuario a detener la visualización del video almacenando en un buffer la información para posteriormente continuar mostrando la secuencia, asegurando una reproducción continua del video.

Para poder distribuir video sobre Internet bajo un sistema de stream video, se necesita un codificador para digitalizar el video y comprimirlo, un software de servidor web, y una conexión a la red con suficiente ancho de banda, así el usuario final necesitará solamente el programa cliente para descargar y visualizar los flujos de video.

VIDEOCONFERENCIA

En videoconferencia suele trabajarse con ventanas de 300x200 píxeles. El video estándar utiliza 30 imágenes (frames) por segundo, por tanto, 30 imágenes de 60 KB dan la friolera de 1,8 millones de bytes por segundo, la mayoría de los fabricantes se orienta hacia la adopción de la RDSI. Otra solución al cuello de botella del ancho de banda en videoconferencia es la compresión de las imágenes.

CÁMARAS

Son dispositivos electrónicos muy utilizados en la actualidad y prácticamente, todo el mundo tiene una, para poder grabar aquellos momentos especiales en la vida y de esta manera, se tendrá un registro para generaciones futuras.

La cámara de video es un dispositivo que captura imágenes convirtiéndolas en señales eléctricas, en la mayoría de los casos la señal de video, también es conocida como señal de televisión; una cámara de video es un transductor óptico.

Las cámaras de video, funcionan por medio de un lente, el receptor de imagen y el registrador, donde se encuentran las cintas de video. En las cuales quedará de manera definitiva, capturada la imagen para su inmortalidad.

El lente capta la imagen, con este se puede dar un mayor paso de luz, si la situación lo amerita; asimismo, se puede regular la cercanía o lejanía de la imagen, por medio de los sistemas de zoom, que existen en las cámaras de video.

La capacidad de los zoom, dependerá de cada una de las cámaras de video, generalmente todas aquellas funciones, las de luz, el zoom y otras, son manejadas de manera automática, ya que llevan consigo, procesadores inteligentes, que van controlando de manera automática, estas funciones.

El receptor de imagen, recibe la imagen y la convierte en una señal de video electrónica; o sea, una carga eléctrica. Luego el registrador, será el responsable de transformar esta señal y trascribirla o grabarla en una cinta magnética.

Las primeras cámaras de video, propiamente dichas, utilizaron tubos electrónicos como captadores; un tipo de válvulas termoiónicas que realizaban, mediante el barrido por un haz de electrones del target donde se formaba la imagen procedente de un sistema de lentes, la transducción de la luz en señales eléctricas.

En la época de los 80 del siglo XX, se desarrollaron transductores de estado sólido: los CCD que sustituyeron muy ventajosamente a los tubos electrónicos, favoreciendo una disminución en el tamaño y el peso de las cámaras de video. Además proporcionaron una mayor calidad y fiabilidad, aunque con una exigencia más elevada en la calidad de los lentes utilizados.

TIPOS DE CÁMARAS

Las cámaras pueden ser clasificadas en varios grupos:

- **Cámaras profesionales de video**

  Son utilizadas en televisión y en cine, ésta clase de cámaras tiene múltiples sensores de color (uno por cada color) para adicionar la resolución y la gama de colores que pueden obtener.
- **Cámaras de video**

  Estas cámaras graban directamente el video a un dispositivo de almacenamiento de memoria. Usualmente tiene un micrófono y una pantalla LCD para supervisar la filmación.
- **Cámaras web**

  Son cámaras digitales diseñadas para funcionar conectadas directamente con una computadora, usualmente son utilizadas para video conferencias, o también para grabaciones de video, algunos modelos incluyen micrófonos y opciones de acercamiento.
- **Cámaras IP**

  Una Cámara IP, también conocidas como cámaras Web o de Red, son videocámaras especialmente diseñadas para enviar las señales de video y audio a través de Internet desde un explorador, como el Internet Explorer o a través de un concentrador HUB o SWITCH en una Red de Área Local (LAN). En estas cámaras pueden integrarse aplicaciones como detección de presencia (incluso el envío de mail si detectan presencia), grabación de imágenes o secuencias en equipos informáticos, tanto en una LAN o en una red externa WAN, de manera que se pueda comprobar el porque ha saltado la detección de presencia y se graben imágenes de lo sucedido.

CARACTERÍSTICAS

Las principales características de las cámaras son:

1. **FORMATO**

   El video digital agrupa varios formatos, aunque el más extendido es el MiniDV, podemos encontrar cámaras basadas en formatos que hoy por hoy se han quedado obsoletos, como el Hi8 y el Digital8; que permite empequeñecer el tamaño de las cintas, y consecuentemente, el de la cámara.

2. **ÓPTICA CCD**

   Si bien un buen número de píxeles es recomendable para cualquier cámara digital, hay que recordar que las imágenes las veremos en una pantalla de televisión que, como mucho, tendrá algo más de 600 líneas.

   En modelos más avanzados, podemos encontrar que el tradicional montaje de un sensor CCD con tres filtros (para rojo, verde, y azul) se sustituye por 3 sensores independientes, uno para cada color, ofreciendo una interpretación más natural de la cromaticidad de la luz.

3. **ZOOM**

   El zoom que poseen las cámaras es una combinación del zoom óptico, con el zoom digital, que reduce la calidad de la imagen tomada. Así que es importante fijarse principalmente en el zoom óptico.

4. **PESO/TAMAÑO**

   Una cámara digital es para llevársela de un sitio a otro, y muchas veces es nuestra compañera fiel de vacaciones, viajes, y pasa tiempos; por ello, es más que necesario que tanto su peso como su tamaño sean reducidos. Lo ideal es encontrar una buena relación calidad de imagen/tamaño, ya que cuanto más pequeña sea la cámara, la óptica será más pequeña, y por lo tanto captará menos luz.

5. **PANTALLA Y VISOR**

   Aunque si hace mucho sol o queremos ahorrar batería utilizaremos el visor, cada vez la pantalla LCD que montan las cámaras de vídeo son más importantes. Muchas no sólo presentan la información de menús y grabaciones, sino que son táctiles, utilizándose como panel de control.

Es fundamental que la imagen que veamos, tanto por visor, como por pantalla, sea nítida y refleje bien los colores de lo que estamos grabando, para así poder determinar si necesitamos modificar algún parámetro de la grabación.

ELEMENTOS

El sistema completo de una cámara de vídeo recibe el nombre de cadena de cámara y consta de la cabeza de cámara, que es la parte que está en el plató o en el lugar de la producción, y la estación base -o base station- que es la parte de la cámara que la une con el resto del sistema de producción.

La cabeza de cámara y la estación base se unen entre si mediante varios cables, por donde van las señales desde el sistema a la cámara y de la cámara al sistema, así como las alimentaciones correspondientes; este cable múltiple puede ser sustituido por un cable coaxial llamado Triaxial, por el que las señales se introducen mediante multiplexión en frecuencia; también hay sistemas con conexionado inalámbrico, pero sólo son utilizados en casos muy concretos y especiales.

Atendiendo a la cadena de cámara completa, podemos distinguir varias partes diferentes.

En la cabeza de cámara tenemos:

- La óptica: sistema de lentes que permiten encuadrar y enfocar la imagen en el target del captador.
- El cuerpo de cámara: espacio donde reside la instrumentación electrónica encargada de la captación y la conversión de las imágenes.
- El adaptador triaxial, o el adaptador al sistema de conexionado elegido con la estación base: comunica la cabeza de cámara con la estación base.

En la estación base tenemos:

- El adaptador triaxial, o el adaptador al sistema de conexionado elegido: comunica la estación base con la cabeza de cámara.
- Sistema electrónico: conjunto de circuitos necesarios para la conexión de la cadena de cámara al resto de la instalación.

Funcionamiento de una cámara de vídeo

1. La luz que proviene de la óptica es descompuesta al pasar por un prisma de espejos diclóicos que descomponen la luz en las tres componentes básicas que se utilizan en televisión: el rojo (R o red), el verde (G o green) y el azul (B o blue).

   Los haces de luz roja, verde y azul son registrados por los captadores, actualmente dispositivos CCD, ubicados detrás de cada lado del prisma. El sistema óptico esta ajustado para que en el target de cada captador se reconstruya la imagen nítidamente.

2. Los circuitos de muestreo y lectura de los CCD deben estar sincronizados con la señal de referencia de la estación; para ello, todos los generadores de pulsos se enclavan con las señales procedentes del sistema de sincronismo de la cámara, que recibe la señal de genlock -normalmente negro de color- desde el sistema en el que se está trabajando o bien, se trabaja sin referencia exterior, como suele hacerse al utilizar cámaras de ENG.

3. En los circuitos preamplificadores se genera e inserta la señal de prueba llamada pulso de calibración -comúnmente llamada cal- la cual recorrerá toda la electrónica de la cámara y servirá para realizar un rápido diagnostico y ajuste de la misma. De los preamplificadores las señales se enrutan a los procesadores, donde se realizaran las correcciones de gamma, detalle, masking, pedestal, flare, ganancias, clípeos y limitadores.

4. Sistema de producción, es donde se envía la señal a los circuitos de visionado, los cuales muestran la imagen en el visor de la cámara y la transmiten mediante los correspondientes conectores de salida.

5. La salida básica, aun hoy en día, sigue siendo la del sistema analógico de TV elegido: PAL, NTSC o SECAM, por lo que el codificador está presente en todas las cámaras. Añadido al mismo estará el codificador de la señal a digital SDI 601; estas señales son mandadas mediante el adaptador triaxial o el correspondiente cable a la estación base, que se encargará de enrutarlas en el sistema de producción al que pertenece la cámara. Si la cámara está unida a un magnetoscopio -es un camcorder- entonces las señales se suministran a los circuitos indicados para su grabación en cinta o en cualquier otro sistema.

6. Todas las funciones de la cámara están controladas con un procesador, el cual se comunica con los paneles de control, tanto de ingeniería (MSP) como de explotación (OCP), y es el encargado de realizar ajustes automáticos y manuales pertinentes.

6.3. APARTADO 3

REDES DE DATOS

El hombre en su afán de comunicarse entre sí, lo ha llevado a buscar diversas maneras desde el uso de las señales de humo hasta lo que hoy día llamamos la maravilla de la rede de redes INTERNET.

Las comunicaciones en el momento actual se encuentran suficientemente implantadas y desarrolladas, la rápida evolución de los dispositivos electrónicos y en particular de la arquitectura de las computadoras y el desarrollo de software para control de procesos e interconexión de dispositivos, nos lleva a pensar que el futuro próximo traerá nuevas ideas, redes y posibilidades de utilización.

En principios, podemos decir que fundamentalmente la investigación actual va encaminada al desarrollo de una red única capaz de soportar simultáneamente todos los servicios de voz, textos, datos e imágenes con suficientes garantías y que permita la conexión a ella de todas las redes ya existentes, tanto de área local como de área extensa.

En una comunicación se transmite información desde una persona a otra persona o mas, genéricamente de un elemento a cualquiera otro. Para que se pueda realizar una transmisión de información, son necesarios tres elementos, sin los cuales tal información no existirá.

- El emisor: quien origina la información.
- El medio de transmisión: que permite la transmisión de esa información.
- El receptor: quien recibe la información.

REDES DE TRANSMISIÓN DE DATOS

Una red de transmisión de datos es un conjunto de elementos físicos y lógicos que permiten la interconexión de equipos y satisfacen todas las necesidades de comunicación de datos entre los mismos.

La evolución de estas redes puede abordarse desde distintos puntos de visita en primer lugar podemos referirnos al elemento físico que soporta la transmisión de datos, en este sentido, podemos decir que con independencia de la conexión de dispositivos para su uso exclusivo por parte de sus propietarios, la primera red que se utilizo fue la ya existente red telefónica. Esta red que ya empezó a utilizarse para la transmisión de datos en la década de los sesenta, y por otro lado, el coste reducido de la conexión y el servicio.

En la década de los setenta aparecen en la mayoría de los países redes especializadas en la transmisión de datos cuyo uso exclusivo aportaba una gran mejoría en calidad y seguridad frente a las redes telefónicas.

Las primeras redes fueron las que tenían un solo procesador central que daba servicio a todo el conjunto de terminales conectados; aparecieron más tarde redes multisistema, donde el control de la red es compartido por múltiples procesadores, posteriormente aparecen las redes distribuidas que permiten la conexión entre distintos tipos de redes, procesadores y terminales, en ella se encuentran conectados todo tipo de procesadores, redes de empresas, redes locales.

REDES DE ÁREA LOCAL Y REDES DE ÁREA EXTENSA

Las Redes de Área Local (RAL o LAN) han sido creadas para responder a estas necesidades de tratamiento de información a pequeñas distancias.

Sus características principales son las siguientes:

- Utilizar una red de transmisión privada para el entorno que se pretende cubrir.
- Pueden conectarse un gran número de dispositivos que compartirían recursos comunes (impresoras, discos, etc.).

- Pueden llegar a distancia de unos pocos kilómetros. Los entorno más típicos son: una sala, una planta de un edificio, todo el edificio, un complejo formado por varios edificios o similares.
- La velocidad de transmisión se encuentra entre 1 y 100 Mbps.
- Permiten la conexión a otras redes a través de pasarelas (Gateways en inglés).

Las características especiales de las redes locales hacen que su construcción, forma y métodos de acceso varíen substancialmente con respecto a las redes de área extensa.

Las Redes de Área Extensa son aquellas que surgen para satisfacer las necesidades de transmisión de datos a distancia superior a unos pocos kilómetros. Este tipo redes permite conexiones entre múltiples usuarios y dispositivos de todo tipo, las más comunes son las redes públicas de telecomunicación que de forma similar existen en casi todos los países del mundo y que se encuentran interconectadas. A ellas pueden conectarse cualquier usuario que lo desee.

Existen redes privadas de uso exclusivo que obedecen a exigencias fuertes de seguridad o necesidad de utilización donde no existen otra solución que este tipo de red.

INTERCONEXIÓN DE REDES

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades y para esto debe estar preparada, efectuando conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la Interconexión de Redes (internetworking) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario, sirviendo para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías. Algunas de las ventajas son:

- Compartición de recursos dispersos.
- Coordinación de tareas de diversos grupos de trabajo.
- Reducción de costos, al utilizar recursos de otras redes.
- Aumento de la cobertura geográfica.

TIPOS DE INTERCONEXIÓN DE REDES

Se pueden distinguir dos tipos de interconexión de redes, dependiendo del ámbito de aplicación:

- Interconexión de Área Local (LAN con RAL)
  Una interconexión de Área Local conecta redes que están geográficamente cerca, como puede ser la interconexión de redes de un mismo edificio o entre edificios, creando una Red de Área Metropolitana (MAN)

- Interconexión de Área Extensa (LAN con MAN y LAN con WAN)
  La interconexión de Área Extensa conecta redes geográficamente dispersas, por ejemplo, redes situadas en diferentes ciudades o países creando una Red de Área Extensa (WAN)

ACCESORIO DE REDES

Los accesorios de redes son también llamados dispositivos de interconexión de redes; y estos son:

Concentradores (Hubs)

El término concentrador o hub describe la manera en que las conexiones de cableado de cada nodo de una red se centralizan y conectan en un único dispositivo. Se suele aplicar concentradores a redes Ethernet, Token Ring, y FDDI (Fiber Distributed Data Interface) soportando módulos individuales que concentran múltiples tipos de funciones en un solo dispositivo. Normalmente los

concentradores incluyen ranuras para aceptar varios módulos y un panel trasero común para funciones de encaminamiento, filtrado y conexión a diferentes medios de transmisión (por ejemplo Ethernet y Token Ring).

Los primeros hubs o de "primera generación" son cajas de cableado avanzadas que ofrecen un punto central de conexión conectado a varios puntos. Sus principales beneficios son la conversión de medio (por ejemplo de coaxial a fibra óptica), y algunas funciones de gestión bastante primitivas como particionamiento automático cuando se detecta un problema en un segmento determinado.

Los hubs inteligentes de "segunda generación" basan su potencial en las posibilidades de gestión ofrecidas por las topologías radiales (Token Ring y Ethernet). Tiene la capacidad de gestión, supervisión y control remoto, dando a los gestores de la red la oportunidad de ofrecer un período mayor de funcionamiento de la red gracias a la aceleración del diagnóstico y solución de problemas. Sin embargo tienen limitaciones cuando se intentan emplear como herramienta universal de configuración y gestión de arquitecturas complejas y heterogéneas.

Los hubs de "tercera generación" ofrecen procesos basados en arquitectura RISC (Reduced Instructions Set Computer) junto con múltiples placas de alta velocidad. Estas placas están formadas por varios buses independientes Ethernet, Token Ring, FDDI y de gestión, lo que elimina la saturación de tráfico de los actuales productos de segunda generación.

A un hub Ethernet se le denomina "repetidor multipuerta". El dispositivo repite simultáneamente la señal a múltiples cables conectados en cada uno de los puertos del hub. En el otro extremo de cada cable está un nodo de la red. Un hub Ethernet se convierte en un hub inteligente (smart hub) cuando puede soportar inteligencia añadida para realizar monitorización y funciones de control. Los concentradores inteligentes (smart hub) permiten a los usuarios dividir la red en segmentos de fácil detección de errores a la vez que proporcionan una estructura de crecimiento

ordenado de la red. La capacidad de gestión remota de los hubs inteligentes hace posible el diagnóstico remoto de un problema y aísla un punto con problemas del resto de la LAN, con lo que otros usuarios no se ven afectados.

El tipo de hub Ethernet más popular es el hub 10BaseT. En este sistema la señal llega a través de cables de par trenzado a una de las puertas, siendo regenerada eléctricamente y enviada a las demás salidas. Este elemento también se encarga de desconectar las salidas cuando se produce una situación de error.

A un hub Token Ring se le denomina Unidad de Acceso Multiestación (MAU - Multiestation Access Unit). Las MAUs se diferencian de los hubs Ethernet porque las primeras repiten la señal de datos únicamente a la siguiente estación en el anillo y no a todos los nodos conectados a ella como hace un hub Ethernet. Las MAUs pasivas no tienen inteligencia, son simplemente retransmisores, las activas repiten la señal, la amplifican y regeneran; las MAUs inteligentes detectan errores y activan procedimientos para recuperarse de ellos.

Repetidores

El repetidor es un elemento que permite la conexión de dos tramos de red, teniendo como función principal regenerar eléctricamente la señal, para permitir alcanzar distancias mayores manteniendo el mismo nivel de la señal a lo largo de la red. De esta forma se puede extender, teóricamente, la longitud de la red hasta el infinito.

Un repetidor interconecta múltiples segmentos de red en el nivel físico del modelo de referencia OSI. Por esto sólo se pueden utilizar para unir dos redes que tengan los mismos protocolos de nivel físico. Los repetidores no segregan los paquetes generados en un segmento y los generados en otro segmento, por lo que los paquetes llegan a todos los nodos de la red. Debido a esto existen más riesgos de colisión y más posibilidades de congestión de la red.

Los repetidores se pueden clasificar en dos tipos:

- Locales: cuando enlazan redes próximas.
- Remotos: cuando las redes están alejadas y se necesita un medio intermedio de comunicación.

Normalmente la utilización de repetidores está limitada por la distancia máxima de la red y el tamaño máximo de cada uno de los segmentos de red conectados. En las redes Ethernet, por problemas de gestión de tráfico en la red, no deben existir más de dos repetidores entre dos equipos terminales de datos, lo que limita la distancia máxima entre los nodos más lejanos de la red a 1.500 m. (enlazando con dos repetidores tres segmentos de máxima longitud, 500 m).

Ventajas:

- Incrementa la distancia cubierta por la LAN.
- Retransmite los datos sin retardos.
- Es transparente a los niveles superiores al físico.

Desventajas:

- Incrementa la carga en los segmentos que interconecta.

Los repetidores son utilizados para interconectar LANs que estén muy próximas, cuando se quiere una extensión física de la red. La tendencia actual es dotar de más inteligencia y flexibilidad a los repetidores, de tal forma que ofrezcan capacidad de gestión y soporte de múltiples medios físicos, como Ethernet sobre par trenzado (10BaseT), Thick Ethernet (10Base5), Thin Ethernet (10Base2), Token Ring, fibra óptica.

Puentes (Bridges)

Son elementos inteligentes, constituidos como nodos de la red, que conectan entre sí dos subredes, transmitiendo de una a otra el tráfico generado. Al distinguir los tráficos locales y no locales, estos elementos disminuyen el mínimo total de paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a la congestión de la red.

Los puentes operan en el nivel de enlace del modelo de referencia OSI, en el nivel de trama MAC (Medium Access Control, Control de Acceso al Medio) y se utilizan para conectar o extender redes similares, es decir redes que tienen protocolos idénticos en los dos niveles inferiores OSI, (como es Token Ring con Token Ring, Ethernet con Ethernet, etc) y conexiones a redes de área extensa. Se encargan de filtrar el tráfico que pasa de una a otra red según la dirección de destino y una tabla que relaciona las direcciones y la red en que se encuentran las estaciones asignadas.

Las redes conectadas a través de puentes aparentan ser una única red, ya que realizan su función transparentemente; es decir, las estaciones no necesitan conocer la existencia de estos dispositivos, ni siquiera si una estación pertenece a uno u otro segmento.

Un puente ejecuta tres tareas básicas:

- Aprendizaje de las direcciones de nodos en cada red.
- Filtrado de las tramas destinadas a la red local.
- Envío de las tramas destinadas a la red remota.

Se distinguen dos tipos de puentes:

- Locales: sirven para enlazar directamente dos redes físicamente cercanas.
- Remotos o de área extensa: se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas.

Se puede realizar otra división de los puntes en función de la técnica de filtrado y envío (puenteo) que utilicen:

- Spanning Tree Protocol Bridge o Transparent Protocol Bridge (Protocolo de Árbol en Expansión o Transparente, STP).

  Estos puentes deciden qué paquetes se filtran en función de un conjunto de tablas de direcciones almacenadas internamente. Su objetivo es evitar la

formación de lazos entre las redes que interconecta. Se emplea normalmente en entornos Ethernet.

- Source Routing Protocol Bridge (Puente de Protocolo de Encaminamiento por Emisor, SRP).

  El emisor ha de indicar al puente cuál es el camino a recorrer por el paquete que quiere enviar. Se utiliza normalmente en entornos Token Ring.
- Source Routing Transparent Protocol Bridge (Puente de Protocolo de Encaminamiento por Emisor Transparente, SRTP).

  Este tipo de puente puede funcionar en cualquiera de las técnicas anteriores.

Ventajas de la utilización de puentes:

- Fiabilidad. Se segmentan las redes de forma que un fallo sólo imposibilita las comunicaciones en un segmento.
- Eficiencia. Se limita el tráfico por segmento, no influye el tráfico de un segmento en el otro.
- Seguridad. Se puede definir distintos niveles de seguridad para acceder a cada uno de los segmentos, siendo no visible por un segmento la información que circula por otro.
- Dispersión. Cuando la conexión mediante repetidores no es posible debido a la excesiva distancia de separación, los puentes permiten romper esa barrera de distancias.

Desventajas de los puentes:

- Son ineficientes en grandes interconexiones de redes, debido a la gran cantidad de tráfico administrativo que se genera.
- Pueden surgir problemas de temporización cuando se encadenan varios puentes.
- Pueden aparecer problemas de saturación de las redes por tráfico de difusión.

Las aplicaciones de los puentes está en soluciones de interconexión de LANs similares dentro de una interconexión de redes de tamaño pequeño-medio, creando una única red lógica y obteniendo facilidad de instalación, mantenimiento

y transparencia a los protocolos de niveles superiores. También son útiles en conexiones que requieran funciones de filtrado. Cuando se quiera interconectar pequeñas redes.

Encaminadores (Routers)

Son dispositivos inteligentes que trabajan en el nivel de red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra.

Convierten los paquetes de información de la red de área local, en paquetes capaces de ser enviados mediante redes de área extensa. Durante el envío, el encaminador examina el paquete buscando la dirección de destino y consultando su propia tabla de direcciones, la cual mantiene actualizada intercambiando direcciones con los demás routers para establecer rutas de enlace a través de las redes que los interconectan. Este intercambio de información entre routers se realiza mediante protocolos de gestión propietarios.

Los encaminadores se pueden clasificar dependiendo de varios criterios:

- En función del área:
  - Locales: Sirven para interconectar dos redes por conexión directa de los medios físicos de ambas al router.
  - De área extensa: Enlazan redes distantes.

- En función de la forma de actualizar las tablas de encaminamiento (routing):
  - Estáticos: La actualización de las tablas es manual.
  - Dinámicos: La actualización de las tablas las realiza el propio router automáticamente.

- En función de los protocolos que soportan:
  - IPX
  - TCP/IP
  - DECnet
  - AppleTalk

- XNS
- X.25
- OSI

- En función del protocolo de encaminamiento que utilicen:
  - Routing Information Protocol (RIP)

    Permite comunicar diferentes sistemas que pertenezcan a la misma red lógica. Tienen tablas de encaminamiento dinámicas e intercambian información según la necesitan. Las tablas contienen por dónde ir hacia los diferentes destinos y el número de saltos que se tienen que realizar. Esta técnica permite 14 saltos como máximo.

  - Exterior Gateway Protocol (EGP)

    Este protocolo permite conectar dos sistemas autónomos que intercambien mensajes de actualización. Se realiza un sondeo entre los diferentes routers para encontrar el destino solicitado. Este protocolo sólo se utiliza para establecer un camino origen-destino; no funciona como el RIP determinando el número de saltos.

  - Open Shortest Path First Routing (OSPF)

    Está diseñado para minimizar el tráfico de encaminamiento, permitiendo una total autentificación de los mensajes que se envían. Cada encaminador tiene una copia de la topología de la red y todas las copias son idénticas. Cada encaminador distribuye la información a su encaminador adyacente. Cada equipo construye un árbol de encaminamiento independientemente.

  - IS-IS

    Encaminamiento OSI según las normativas: ISO 9575, ISO 9542 e ISO 10589. El concepto fundamental es la definición de encaminamiento en un dominio y entre diferentes dominios; dentro de un mismo dominio el encaminamiento se realiza aplicando la técnica de menor coste y entre diferentes dominios se consideran otros aspectos como la seguridad.

Otras variantes de los routers son:

- Router Multiprotocolo

  Tienen la posibilidad de soportar tramas con diferentes protocolos de Nivel de Red de forma simultánea, encaminándolas dinámicamente al destino especificado, a través de la ruta de menor coste o más rápida. Son los routers de segunda generación. No es necesario, por tanto, tener un router por cada protocolo de alto nivel existente en el conjunto de redes interconectadas.

- Brouter (bridging router)

  Son routers multiprotocolo con facilidad de bridge. Funcionan como router para protocolos encaminables y para aquellos que no lo son se comportan como bridge, transfiriendo los paquetes de forma transparente según las tablas de asignación de direcciones.

  Operan tanto en el Nivel de Enlace como en el Nivel de Red del modelo de referencia OSI. Por El Brouter funciona como un router multiprotocolo, pero si encuentra un protocolo para el que no puede encaminar, entonces simplemente opera como bridge.

- Trouter

  Es una combinación entre un router y servidor de terminales. Permite a pequeños grupos de trabajo la posibilidad de conectarse a LANs, WANs, modems, impresoras, y otros ordenadores sin tener que comprar un servidor de terminales y un router. El problema que presenta este dispositivo es que al integrar las funcionalidades de router y de servidor de terminales puede ocasionar una degradación en el tiempo de respuesta.

  Ventajas de los routers:

  - Seguridad. Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.

- Flexibilidad. Las redes interconectadas con router no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con bridge.
- Soporte de Protocolos. Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.
- Relación Precio / Eficiencia. El coste es superior al de otros dispositivos, en términos de precio de compra, pero no en términos de explotación y mantenimiento para redes de una complejidad mayor.
- Control de Flujo y Encaminamiento. Utilizan algoritmos de encaminamiento adaptativos (RIP, OSPF, etc), que gestionan la congestión del tráfico con un control de flujo que redirige hacia rutas alternativas menos congestionadas.

Desventajas de los routers:

- Lentitud de proceso de paquetes respecto a los bridges.
- Necesidad de gestionar el subdireccionamiento en el Nivel de Enlace.
- Precio superior a los bridges.

Por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, son una excelente solución para una gran interconexión de redes con múltiples tipos de LANs, MANs, WANs y diferentes protocolos. Es una buena solución en redes de complejidad media, para separar diferentes redes lógicas, por razones de seguridad y optimización de las rutas.

PASARELAS (GATEWAYS)

Estos dispositivos facilitan el acceso entre sistemas o entornos soportando diferentes protocolos; operan en los niveles más altos del modelo de referencia OSI (Nivel de Transporte, Sesión, Presentación y Aplicación) y realizan conversión de protocolos para la interconexión de redes con protocolos de alto nivel diferentes.

Los gateways incluyen los 7 niveles del modelo de referencia OSI, y aunque son más caros que un bridge o un router, se pueden utilizar como dispositivos universales en una red corporativa compuesta por un gran número de redes de diferentes tipos.

Los gateways tienen mayores capacidades que los routers y los bridges porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de una red que transportan son compatibles con los de la otra red. Conectan redes de diferentes arquitecturas procesando sus protocolos y permitiendo que los dispositivos de un tipo de red puedan comunicarse con los de otro tipo de red.

Tipos de gateways:

- **Gateway asíncrono**

  Sistema que permite a los usuarios de ordenadores personales acceder a grandes ordenadores (mainframes) asíncronos a través de un servidor de comunicaciones, utilizando líneas telefónicas conmutadas o punto a punto. Generalmente están diseñados para una infraestructura de transporte muy concreta, por lo que son dependientes de la red.
- **Gateway SNA**

  Permite la conexión a grandes ordenadores con arquitectura de comunicaciones SNA (System Network Architecture, Arquitectura de Sistemas de Red), actuando como terminales y pudiendo transferir ficheros o listados de impresión.
- **Gateway TCP/IP**

  Proporcionan servicios de comunicaciones con el exterior vía LAN o WAN y también funcionan como interfaz de cliente proporcionando los servicios de aplicación estándares de TCP/IP.
- **Gateway PAD X.25**

  Son similares a los asíncronos; la diferencia está en que se accede a los servicios a través de redes de conmutación de paquetes X.25.

- **Gateway FAX**

  Los servidores de Fax proporcionan la posibilidad de enviar y recibir documentos de fax.

Ventajas:

- Simplifican la gestión de red.
- Permiten la conversión de protocolos.

Desventajas:

- Su gran capacidad se traduce en un alto precio de los equipos.
- La función de conversión de protocolos impone una sustancial sobrecarga en el gateway, la cual se traduce en un relativo bajo rendimiento Y puede ser un cuello de botella potencial si la red no está optimizada para mitigar esta posibilidad.

Su aplicación está en redes corporativas compuestas por un gran número de LANs de diferentes tipos.

CONMUTADORES (SWITCHES)

Los conmutadores tienen la funcionalidad de los concentradores a los que añaden la capacidad principal de dedicar todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos. Esto se consigue debido a que el conmutador no actúa como repetidor multipuerto, sino que únicamente envía paquetes de datos hacia aquella puerta a la que van dirigidos, gracias a que los equipos configuran unas tablas de encaminamiento con las direcciones MAC (nivel 2 de OSI) asociadas a cada una de sus puertas; haciendo posible que cada una de las puertas disponga de la totalidad del ancho de banda para su utilización. Estos equipos habitualmente trabajan con anchos de banda de 10 y 100 Mbps, pudiendo coexistir puertas con diferentes anchos de banda en el mismo equipo.

Las puertas de un conmutador pueden dar servicio tanto a puestos de trabajo

personales como a segmentos de red (hubs), siendo por este motivo ampliamente utilizados como elementos de segmentación de redes y de encaminamiento de tráfico. De esta forma se consigue que el tráfico interno en los distintos segmentos de red conectados al conmutador afecte al resto de la red aumentando de esta manera la eficiencia de uso del ancho de banda.

Hay tres tipos de conmutadores o técnicas de conmutación:

- **Almacenar – Transmitir.** Almacenan las tramas recibidas y una vez chequeadas se envían a su destinatario. La ventaja de este sistema es que previene del malgasto de ancho de banda sobre la red destinataria al no enviar tramas inválidas o incorrectas. La desventaja es que incrementa ligeramente el tiempo de respuesta del switch.

- **Cortar – Continuar.** El envío de las tramas es inmediato una vez recibida la dirección de destino. Las ventajas y desventajas son cruzadas respecto a Almacenar-Transmitir; este tipo de conmutadores es indicado para redes con poca latencia de errores.

- **Híbridos**. Este conmutador normalmente opera como Cortar-Continuar, pero constantemente monitoriza la frecuencia a la que tramas inválidas son enviadas; si este valor supera un umbral prefijado el conmutador se comporta como un Almacenar-Transmitir y al descender de este nivel se pasa al modo inicial.

  En caso de diferencia de velocidades entre las subredes interconectadas el conmutador necesariamente ha de operar como Almacenar-Transmitir.

Esta tecnología permite una serie de facilidades tales como:

- **Filtrado inteligente.** Posibilidad de hacer filtrado de tráfico no sólo basándose en direcciones MAC, sino considerando parámetros adicionales,

tales como el tipo de protocolo o la congestión de tráfico dentro del switch o en otros switches de la red.

- **Soporte de redes virtuales.** Posibilidad de crear grupos cerrados de usuarios, servidos por el mismo switch o por diferentes switches de la red, que constituyan dominios diferentes a efectos de difusión. De esta forma también se simplifican los procesos de movimientos y cambios, permitiendo a los usuarios ser ubicados o reubicados en red mediante software.
- **Integración de routing.** Inclusión de módulos que realizan función de los routers (encaminamiento), de tal forma que se puede realizar la conexión entre varias redes diferentes mediante switches**.**

TENDENCIAS TECNOLÓGICAS Y DEL MERCADO

Las principales tendencias del mercado de sistemas de interconexión de redes son las siguientes:

- **Tendencias de encaminamiento**

  El mercado está en expansión, cada vez hay más ofertas de productos y además estos incorporan nuevas facilidades de encaminamiento; tanto los fabricantes de concentradores como los de multiplexores están incorporando en sus productos capacidades de encaminamiento, unos con redes de área metropolitana y extensa, y otros incorporando facilidades de interconexión de LANs.
- **Equipos de interconexión a bajo coste**

  Los fabricantes están presentando equipos de bajo coste que permiten la interconexión de dependencias remotas. Las soluciones de encaminamiento son de diversos tipos: integradas en servidores de red, en concentradores, en pequeños equipos router, etc; siendo fáciles de gestionar, operar y mantener.
- **Routers multiprotocolo**

  Estos dispositivos han permitido a los usuarios transportar protocolos diferentes sobre la misma infraestructura de red, lo cual permitiría ahorrar en

costes de la infraestructura de transmisión y una potencial mejora de la interoperabilidad.

- **Interconexión de LAN/WAN bajo Switchers**

  Los conmutadores han evolucionado rápidamente dotándose de altas capacidades y velocidad de proceso. Pensados para soportar conmutación ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono) bajo una arquitectura punto a punto, han logrado gran implantación como mecanismo de interconexión de redes LANs heterogéneas, Token Ring y Ethernet en un mismo dominio. Esto se consigue dado que el conmutador permite la segmentación de la red en subredes conectadas a cada uno de sus puertos que puede gestionar de manera independiente.

- **Capacidad de gestión**

  Los dispositivos de interconexión están dotados con mayores capacidades de gestión que permitan la monitorización de la red mediante estaciones de gestión y control de los dispositivos de la red, enviando comandos por la red desde la estación de gestión hasta el dispositivo de la red para cambiar/inicializar su configuración.

INTERNET

Internet es un acrónimo del inglés INTERnational NET, que traducido al español sería Red Mundial. Internet es una red de redes a escala mundial de millones de computadoras interconectadas con un conjunto de protocolos, el más destacado es el TCP/IP. Cuando se dice red de redes se hace referencia a que es una red formada por la interconexión de otras redes menores.

Al contrario de lo que se piensa comúnmente, Internet no es sinónimo de World Wide Web, ésta es parte de aquella, siendo la World Wide Web uno de los muchos servicios ofertados en la red Internet; la Web es un sistema de información mucho más reciente que emplea Internet como medio de transmisión.

Algunos de los servicios disponibles en Internet aparte de la Web son el acceso remoto a otras máquinas (SSH y telnet), transferencia de archivos (FTP), correo electrónico (SMTP), boletines electrónicos (news o grupos de noticias), conversaciones en línea (IRC y chats), mensajería instantánea (MSN Messenger, ICQ, YIM, AOL, Skype, Jabber), transmisión de archivos (P2P, P2M, Descarga Directa), entre otros.

Cronología

En 1972, se realizó la Primera demostración pública de ARPANET, una nueva Red de comunicaciones financiada por la DARPA que funcionaba de forma distribuida sobre la red telefónica conmutada. El éxito de ésta nueva arquitectura sirvió para que, en 1973, la DARPA iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Para éste fin, desarrollaron nuevos protocolos de comunicaciones que permitiesen este intercambio de información de forma "transparente" para los ordenadores conectados. De la filosofía del proyecto surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas mediante los protocolos TCP e IP.

En 1983, el 1 de enero, ARPANET cambió el protocolo NCP por TCP/IP. Ese mismo año, se creó el IAB con el fin de estandarizar el protocolo TCP/IP y de proporcionar recursos de investigación a Internet. Por otra parte, se centró la función de asignación de identificadores en la IANA que, más tarde, delegó parte de sus funciones en el IR que, a su vez, proporciona servicios a los DNS.

En 1986, la NSF comenzó el desarrollo de NSFNET que se convirtió en la principal Red en árbol de Internet, complementada después con las redes NSINET y ESNET, todas ellas en Estados Unidos. Paralelamente, otras redes troncales en Europa, tanto públicas como comerciales, junto con las americanas formaban el esqueleto básico ("backbone") de Internet.

En 1989, con la integración de los protocolos OSI en la arquitectura de Internet, se inició la tendencia actual de permitir no sólo la interconexión de redes de estructuras dispares, sino también la de facilitar el uso de distintos protocolos de comunicaciones.

En el CERN de Ginebra, un grupo de Físicos encabezado por Tim Berners-Lee, crearon el lenguaje HTML, basado en el SGML y en 1990 el mismo equipo construyó el primer cliente Web, llamado WorldWideWeb (WWW), y el primer servidor web.

En el 2006, el 3 de enero, Internet alcanzó los mil cien millones de usuarios. Se prevé que en diez años, la cantidad de navegantes de la Red aumentará a 2.000 millones.

Internet y sociedad

Internet tiene un impacto profundo en el trabajo, el ocio y el conocimiento. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea. Un ejemplo es el desarrollo y la distribución de colaboración del software de Free/Libre/Open-Source (SEDA) por ejemplo GNU, Linux, Mozilla y OpenOffice.org.

Comparado a enciclopedias y a bibliotecas tradicionales, la web ha permitido una descentralización repentina y extrema de la información y datos. Algunas compañías e individuos han adoptado el uso de los weblogs, que se utilizan en gran parte como diarios actualizables. Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos, en este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada. Desde una perspectiva cultural del conocimiento, internet ha sido una ventaja y una responsabilidad, proporcionando una cantidad significativa de información y de una interactividad que sería inalcanzable de otra manera.

Ocio

La pornografía y la industria de juego representan buena parte del ocio en la WWW y proporcionan a menudo una fuente significativa del rédito de publicidad para otros sitios de la red. Un área principal del ocio en Internet es el sistema Multijugador.

Muchos utilizan el Internet para descargar música, películas y otros trabajos. Hay fuentes pagadas y sin pagar para todos éstos, usando los servidores centralizados y distribuido, las tecnologías del p2p. Otros utilizan la red para tener acceso a las noticias y el estado del tiempo. La charla, la mensajería y el e-mail son uno de los servicios de uso más extendido.

Trabajo

Con la aparición del Internet y de las conexiones de alta velocidad, el Internet ha alterado de manera significativa la manera de trabajar de millones de personas. Al contrario que con la jornada donde los empleados se desplazan al lugar de trabajo, internet ha permitido mayor flexibilidad en términos del horario y localización.

Censura

Una de sus mayores ventajas -para unos- o inconvenientes -para otros- es que nadie la controla, ni puede controlarla de forma global.

Sin embargo, la mayoría de los países en el mundo occidental no fuerzan a Internet Service Provider bloquear sitios. Hay una gran cantidad de programas disponibles que bloquean el acceso a sitios ofensivos (tales como pornografía o violento) en las computadoras o las redes individuales.

Tecnología de Internet

Internet incluye aproximadamente 5000 redes en todo el mundo y más de 100 protocolos distintos basados en TCP/IP, que se configura como el protocolo de la red.

Los servicios disponibles en la red mundial de PC´s, han avanzado mucho gracias a las nuevas tecnologías de transmisión de alta velocidad, como DSL y Wireless, se ha logrado unir a las personas con videoconferencia, ver imágenes por satélite, observar el mundo por webcams, hacer llamadas telefónicas gratuitas, o disfrutar de un juego multijugador en 3D, un buen libro PDF, o álbumes y películas para descargar.

El método de acceso a internet vigente hace alguno años es la telefonía básica y ha venido siendo sustitida gradualmente por conexiones más veloces y estables, entre ellas el ADSL, o el RDSI. También han aparecido formas de acceso a través de la red eléctrica, e incluso por satélite.

Internet también está disponible en muchos lugares públicos tales como bibliotecas, hoteles o cibercafés y una nueva forma de acceder sin necesidad de un puesto fijo son las redes inalámbricas, hoy presentes en aeropuertos, universidades o poblaciones enteras.

PROTOCOLOS UTILIZADOS EN INTERNET

La familia de protocolos de Internet es un conjunto de protocolos de red que implementa la pila de protocolos en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se la denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse y que son los más utilizados de la familia.

Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el HTTP (HyperText Transfer Protocol), que se utiliza para acceder a las páginas web, además el ARP para la resolución de direcciones,

el FTP para transferencia de archivos, y el SMTP y POP para correo electrónico, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC´s, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

IP

Acrónimo de Internet Protocol (Protocolo de Internet).

Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. La versión actual es IPv4 mientras que en el proyecto Internet2 se intenta implementar la versión 6 (IPv6), que permitiría mejores prestaciones dentro del concepto QoS (Quality of Service).

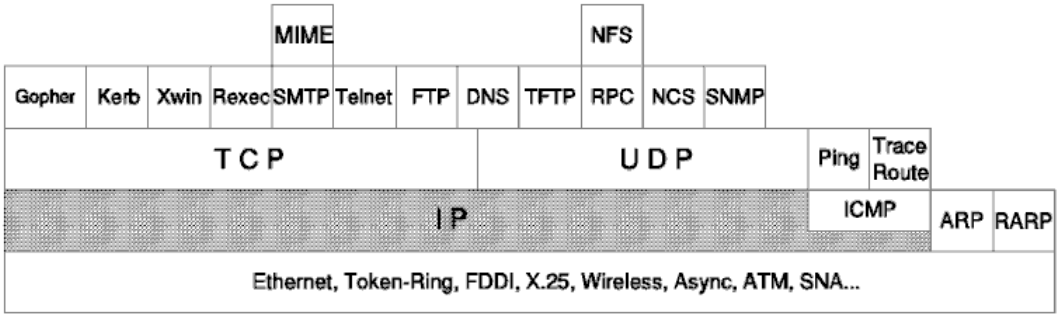
Una Dirección IP (dirección del *Internet Protocol*), es como un DNI para máquinas, es un número único que utilizan los dispositivos para identificarse y comunicarse entre ellos en una red que utiliza el estándar del Internet Protocol. Cualquier dispositivo que participa, incluyendo ordenadores, routers, FAX de Internet, y algunos teléfonos, debe tener su propia dirección única..

Los números usados actualmente en las direcciones IP van desde 0.0.0.0 a 255.255.255.255, aunque algunos de estos valores están reservados para propósitos específicos. Esto no proporciona bastantes posibilidades para que cada dispositivo de Internet tenga su propio número permanente, y el servidor Dynamic Host Configuration Protocol (DHCP) da a los clientes direcciones IP dinámicas que se reciclan cuando expira su período de uso.

Dispositivos tales como impresoras de red, servidores web y servidores de email, que están conectados permanentemente a Internet; sí reciben generalmente direcciones IP estáticas que identifican al dispositivo cuando están conectadas a la

red. Puesto que los números no son fáciles de recordar por los seres humanos, el Domain Name System proporciona un servicio similar a una guía de teléfonos llamado “domain name resolution" o "name resolution”. Hay servidores especiales de DNS en Internet que se dedican a realizar la traducción de un Nombre de Dominio (xej. Masadelante.com) a una Dirección IP y viceversa.

El Protocolo de Internet, es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.



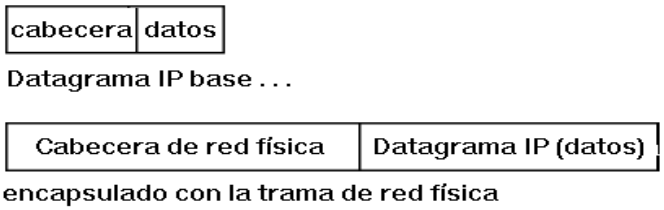
I

P es un *protocolo estándar* con número STD 5 que incluye también ICMP e IGMP.

No añade fiabilidad, control de flujo o recuperación de errores para el protocolo de interfaz de red subyacente. Los paquetes (datagramas) que envía IP se pueden perder, estar fuera de orden, o incluso duplicar.

Datagrama IP

El datagrama de Internet (datagrama IP) es el paquete de transferencia base en la familia de protocolos de Internet. Contiene una cabecera con información para IP, y unos datos que son relevantes sólo para los protocolos de más alto nivel.



El datagrama IP se encapsula en la trama de red subyacente, que tiene usualmente una longitud máxima o limitación de trama, dependiendo del hardware utilizado. En vez de limitar la longitud del datagrama IP a un tamaño máximo. En particular, el estándar IP no impone un tamaño máximo, pero dice que todas las subredes deberían ser capaces de manejar datagramas de al menos 576 bytes.

Todos los fragmentos de un datagrama tienen una cabecera, básicamente copiado del datagrama original, y los datos que le siguen. Se tratan como datagramas IP normales mientras se transportan a sus destinos.

Formato De Datagrama IP

La cabecera del datagrama IP tiene una longitud mínimo de 20 bytes:

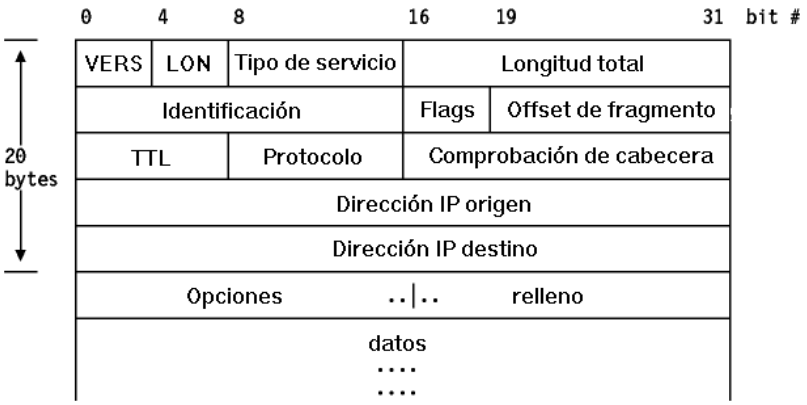
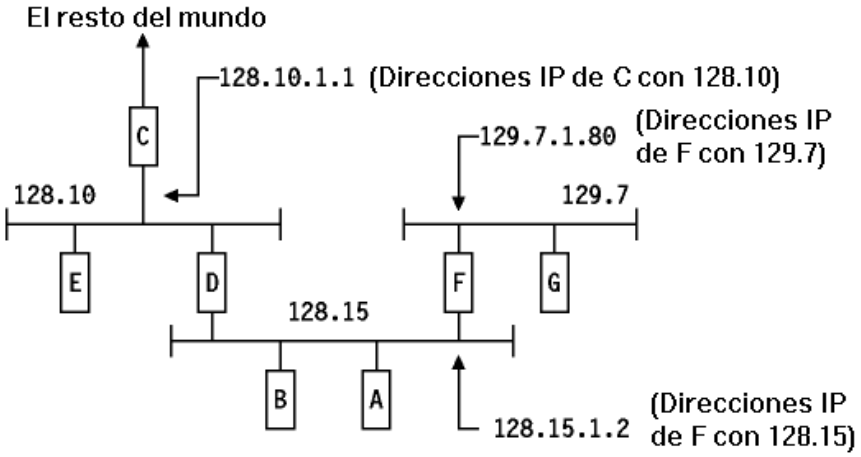


Tabla De Enrutamiento Ip

Cada host mantiene el conjunto de correspondencias entre direcciones IP de destino y las direcciones IP de los routers del próximo salto para esos destinos en una tabla denominada tabla de enrutamiento IP.

Se pueden encontrar tres tipos de correspondencia en esta tabla:

1. Rutas directas, para redes conectadas localmente
2. Rutas indirectas, para redes alcanzables vía uno o más routers
3. Una ruta por defecto, que contiene la dirección IP de un router que se usa para todas las direcciones IP que no cubren las rutas directas e indirectas.



6.4. APARTADO 4

SISTEMA DE SEGURIDAD

Podemos entender como sistema de seguridad, a un sistema que esta libre de todo peligro, daño o riesgo, y que es en cierta manera, infalible.

Es muy difícil de conseguir seguridad total, entonces podemos hablar de fiabilidad o probabilidad de que un sistema se comporte tal y como se espera. Más que de seguridad, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos:

- Confidencialidad
- Integridad
- Disponibilidad

La seguridad está constituida por tres tipos de medios que deben asociarse como partes integrantes de un todo.

- **Medios Humanos**: constituidos por el personal de seguridad, tanto Pública, Institucional y/o Privada.
- **Medios Técnicos**: Pasivos o físicos. Activos o electrónicos.
- **Medios Organizativos**: planes, normas, estrategias.

Los Medios Técnicos, los pasivos o seguridad física y los activos o seguridad electrónica, son los más importantes.

Medios técnicos pasivos o seguridad Física

Estos medios están enfocados a disuadir, detener o al menos, retardar o canalizar la progresión de la amenaza. El incremento del tiempo que estos elementos imponen a la acción agresora para alcanzar su objetivo resulta, en la mayoría de las ocasiones, imprescindible para que se produzca en tiempo adecuado la alarma-reacción.

El conjunto de medios pasivos constituye lo que se denomina seguridad física, que está formada por:

Elementos de carácter estático y permanente

Protegen y suponen el primer obstáculo que se presenta para la penetración de intrusos formando por la protección perimetral (vallas, cercados, setos, etc.), protección periférica (puertas, rejas, cristales, etc.) y protección del bien, que está constituido por recintos o habitáculos cerrados (cajas fuertes, cámaras acorazadas, etc.).

1. Protección Perimetral

Los principales elementos que la conforman son los constituidos de:

- Mampostería
- Metal
- Mixtos
- Barreras de detención de vehículos

2. Protección Periférica

Los principales elementos que conforman la protección periférica son:

- Puertas.
- Instalación de sistemas de esclusas
- Cristales blindados en ventanas.
- Rejas y contraventanas instaladas en las ventanas
- Rejillas y emparrillados protectores de huecos necesarios de ventilación.

3. **Protección del Bien**

- Cajas fuertes.
- Cámaras acorazadas.

4. **Fiabilidad**

   Es el grado de confianza que otorga un sistema de protección en el cumplimiento de la misión para la que se ha establecido.

   Viene determinada por los siguientes parámetros:

   - Seguridad de reacción.
   - Seguridad de falsas alarmas.
   - Vulnerabilidad al sabotaje.

Medios Técnicos Activos o Seguridad Electrónica.

La función de los medios activos es la de alertar local o remotamente de un intento de violación o sabotaje de las medidas de seguridad física establecidas.

El conjunto de medios activos constituye lo que se denomina seguridad electrónica. Pueden utilizarse de forma oculta o visibles.

Sus funciones principales son:

- Detección de intrusos en el interior y en el exterior.
- Control de accesos y tráfico de personas, paquetes, correspondencia y vehículos.
- Vigilancia óptica por fotografía o circuito cerrado de televisión.
- Intercomunicación por megafonía.
- Protección de las comunicaciones.

Un sistema electrónico de seguridad está formado por un conjunto de elementos electromecánicos y/o electrónicos relacionados entre sí por una adecuada

instalación, que, a través de la información que nos proporcionan, contribuyen al incremento del nivel de seguridad de un determinado entorno.

De una manera esquemática, un sistema electrónico de seguridad consta de los siguientes elementos:

- **Red**
- **Fuente de alimentación**

  La energía de alimentación representa el elemento de activación del sistema, por lo que se debe disponer de una fuente de alimentación, que automatice el sistema ante posibles faltas de suministro casuales o intencionadas. Esto se logra por medio de acumuladores de energía y baterías (SAI, sistema de alimentación independiente).

- **Equipo de seguridad**

  Es el cerebro de todo el sistema. Recibe los impulsos de los detectores y, tras analizarlos, los transforma oportunamente en señales que envía a los señalizadores o avisadores locales y/o remotos.

- **Detectores**

  Son dispositivos colocados tanto en el exterior como en el interior de objetivos con riesgo de intrusión, con la misión de informar a la central de las variaciones del estado ambiental de la zona que están protegiendo, indicando, por tanto, la intrusión en dichos objetivos.

DETECTORES DE INTERIOR		
PUNTUALES	Contactos Magnéticos Contactos Mecánicos	
LINEALES	Rayos infrarrojos Contactos en hilos	
SUPERFICIALES	Inerciales Piezoeléctricos	Péndulo Masa Mercurio Inerciales

	Alfombras de presión Redes conductoras	Piezoeléctricos Sin contacto
VOLUMÉTRICOS	Microondas Ultrasonidos Sonido Luz Capacitivo	
DETECTORES DE EXTERIORES		
PUNTUALES	Contactos Magnéticos Contactos Mecánicos	
LINEALES	Rayos infrarrojos Contactos en hilos	
SUPERFICIALES	Vibración en vallados Presión del suelo Barreras rayos infrarrojos Vibración en muros Cables de tensión Redes de fibra óptica	Sensores aislados Sensores continuados Hidráulicos Neumáticos Sensor aislado
VOLUMÉTRICOS	Microondas Ultrasonidos Sonido Luz Capacitivo	

- **Señalizadores o avisadores.**

  Representan una parte de vital importancia del sistema, puesto que si se consuma un intento de intrusión, se deberá conocer adecuadamente lo que está sucediendo y dónde está sucediendo, para poder reaccionar con eficacia.

  Según el lugar y la forma en que ejercen sus funciones, podemos clasificarnos de la siguiente manera:

SEÑALIZADORES O AVISADORES		
Locales	Acústicos	Sirenas electrónicas. Sirenas mecánicas
	Ópticos	Iluminación súbita. Luz lanza-destellos. Flash

A distancia	Llamada telefónica Telecomunicación	 Hilo. Radio
Especiales	Máquina fotográfica. Circuito cerrado de televisión	 Filmadora. Cámaras digitales, web, etc

Hacemos una referencia al CCTV como complemento a los elementos pasivos y activos.

El CCTV realizará las siguientes funciones:

- Vigilancia de todo el área perimetral y de los accesos existentes.
- Verificación de las alarmas que generan los sistemas perimetrales instalados.
- Grabación de imágenes de incidencias.
- Posibilidad de asociar al CCTV sistemas específicos de detección de riesgos (videocámaras).

En esencia, el CCTV consta de:

- Cámaras de televisión, que pueden ser fijas o dotadas de posicionador, y que pueden filmar de una manera continua o en determinados periodos de tiempo, según se considere oportuno.
- Monitores situados en la consola de la centralita de alarmas, que proporcionará la visión de lo que las cámaras están filmando.
- La instalación del CCTV debe programarse sobre la base de la necesidad de abarcar la totalidad de las áreas vigiladas y procurando asociar las distintas zonas con cada cámara, de modo que se facilite su actuación por medio de la señal de alarma producida.
- Armonizar la elección de cámaras fijas o cámaras dotadas de posicionador, para conjugar la obtención de panorámicas adecuadas y la operatividad correcta de atención a pantallas.

Como sistema de apoyo, el CCTV proporciona las siguientes ventajas:

- Extensión del ojo humano por encima de éste, en alcance y sensibilidad.
- Posibilidad de ubicarlo en lugares o ambientes inalcanzables para el hombre.
- Con un solo vigilante se controlan grandes áreas.
- Son el complemento ideal para el control de accesos y movimiento.
- Proporcionan un gran apoyo en la protección perimetral.
- Tiene grandes ángulos de visión y se pueden utilizar a grandes distancias.

La red es el punto donde todas las nuevas tecnologías de voz, datos y video convergen, por lo cual es vital contar con la infraestructura adecuada que cubra todos y cada uno de los aspectos requeridos para soportar su operación.

Seguridad y Vigilancia

Las cámaras IP se usan en sistemas de seguridad profesionales y permite ver el video en directo sólo a personal autorizado. Las cámaras IP se integran fácilmente en sistemas mayores y más complejos, pero también pueden funcionar como soluciones aisladas en aplicaciones de vigilancia de bajo nivel.

- Las cámaras IP pueden usarse para vigilar áreas sensibles como pueden ser edificios, casinos, bancos y tiendas. Las imágenes en video de estas áreas pueden ser monitorizadas desde salas de control, dependencias policiales y/o por directores de seguridad desde diferentes localizaciones.
- Las cámaras IP han mostrado igualmente ser efectivos sustitutos de las cámaras analógicas en aplicaciones tradicionales de refuerzo a las fuerzas de seguridad, como por ejemplo para mantener seguros determinados lugares públicos.
- Las cámaras IP pueden igualmente emplearse para el control de accesos. Las personas, al igual que los vehículos, pueden grabarse junto con la información de la fecha y hora de entrada, de forma que sea sencilla su revisión y localización. Las imágenes pueden almacenarse en un lugar remoto, imposibilitando el robo de esta valiosa información.

Monitorización Remota

Las cámaras IP se conectan fácilmente a las redes IP existentes y permiten actualizaciones en tiempo real de video de alta calidad para que resulte accesible desde cada uno de los ordenadores de una red. Las áreas sensibles como son la sala de servidores, la recepción o cualquier lugar remoto pueden ser monitorizadas detalladamente de una forma única y económica, a través de la red de área local o de Internet.

- Las cámaras IP mejoran la monitorización de un establecimiento comercial para asegurar que todo está en orden.
- Una cámara IP es una herramienta útil en la oficina. Áreas como la recepción y las salas de conferencias pueden estar monitorizadas para su control y además los usuarios pueden hacer seguimiento de quién ha entrado en el lugar y tomar las acciones pertinentes cuando haya problemas.
- Las cámaras IP son herramientas útiles en la industria de la fabricación; monitorizar robots, u otras máquinas, y las líneas de producción desde la oficina o desde casa y permitir a los ingenieros de servicio acceder a las cámaras remotamente.

Aporte del video IP a los sistemas de seguridad

En el mercado de video seguridad, el video IP está desplazando a los dispositivos analógicos y entre sus principales aportes tenemos:

- Escalabilidad de IP, la posibilidad de acceder al sistema desde cualquier lugar del mundo y la calidad de las grabaciones inherente al procesado digital de la señal de video.
- Rentabilidad de un sistema de televigilancia IP con respecto al CCTV tradicional es mayor cuando mayor es el número de cámaras involucradas, si bien es cierto que el coste inicial por cámara es mayor en los sistemas basados

en IP, pero el coste de la infraestructura es menor y el coste de ampliación por cámara es plano y no exponencial.

- Conectividad entre redes IP desde cualquier parte y de forma segura mediante Redes Privadas Virtuales, para transmitir la señal de video en paquetes IP y visualizar o grabar las imágenes de las cámaras remotamente gracias a la expansión de las redes IP y especialmente de Internet.
- Coste del almacenamiento digital es inferior al analógico, y la calidad es mayor.

Video Vigilancia

La video vigilancia permite que a través de cámaras de video instaladas en sitios estratégicos, cuyo objetivo es vigilar y dar apoyo a los entes de seguridad en su proceso operativo y a cualquier otro organismo del sector público o privado que por su objeto social, demande la información contenida por medio de una central de monitoreo.

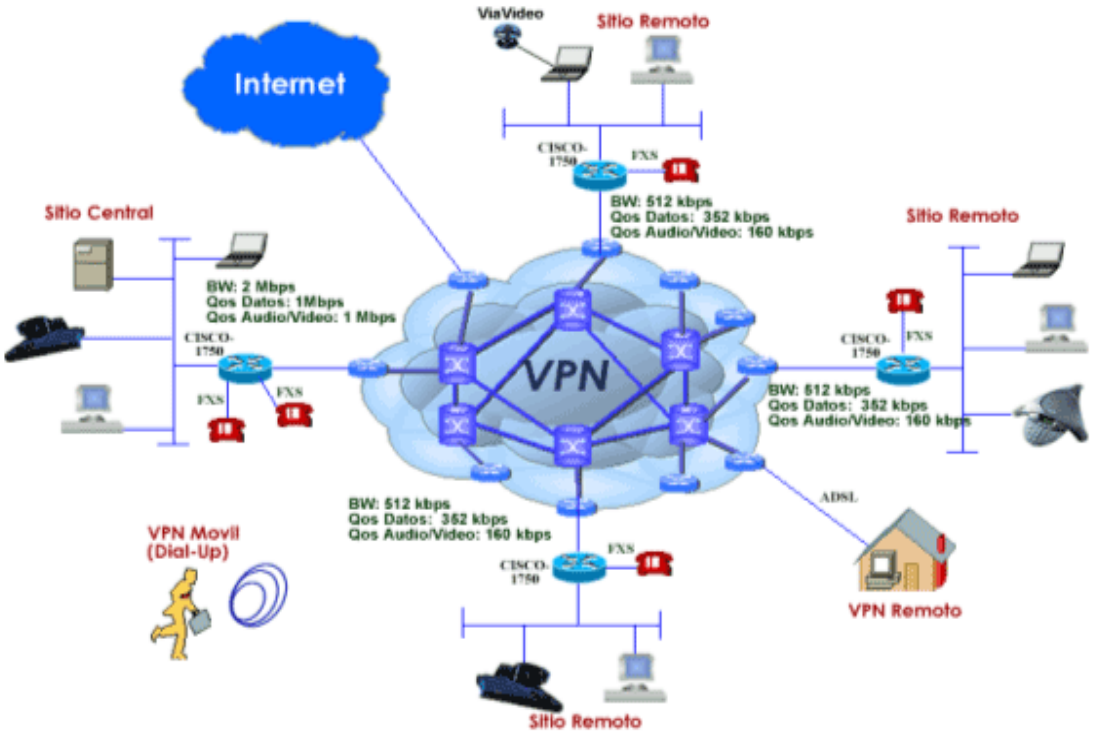
Beneficios

- Brindar a las empresas del sector público y privado una herramienta ágil y oportuna en la obtención en tiempos reales de las imágenes, de lo que esta ocurriendo dentro y fuera de los establecimientos que son objeto de vigilancia.
- Dar apoyo visual ante cualquier eventualidad, teniendo un tiempo de respuesta menor para la atención de la misma.
- Monitorear constantemente espacios públicos y privados, y observar la ocurrencia de actos delictivos.

COMUNICACIÓN IP

La convergencia de Voz, Datos y Video dentro de una misma red corporativa es el presente en los negocios exitosos, incorporado a esto el depender de un solo proveedor de servicios trae granes beneficios operacionales.

Actualmente los costos de la tecnología y los avances tecnológicos hacen inevitable evaluar el costo-beneficio que las empresas pueden obtener; ganancia de productividad, escala, economía de recursos y agilidad. Estos son los objetivos principales que la convergencia de las telecomunicaciones hacia IP pretende garantizar.



La convergencia de voz, datos y video terminan por estandarizar el uso de un único medio para transmisión. El contexto demuestra que la tecnología de red IP está despuntando como una de las vías principales de convergencia.

CÁMARAS IP

Una cámara IP o cámara de red puede ser descrita como la combinación de una cámara y una computadora en una sola unidad, la cual captura y transmite imágenes en vivo a través de una red IP, habilitando a usuarios autorizados a ver, almacenar y administrar el video sobre una infraestructura de red estándar basada en el protocolo IP.

Una cámara IP, también es una cámara de CCTV que transmite video en vivo a través del Internet a cualquier PC en el mundo mediante una red Ethernet.

Una cámara de red tiene su propia dirección IP que se conecta a la red, tiene internamente construidos una serie de aplicaciones, funciones y servicios, es decir un software propio para servidor web, servidor FTP, cliente FTP y cliente de correo electrónico, administración de alarmas, salida de relé y muchos otros que en su conjunto permiten inclusive realizar programación directamente en la cámara; las cámaras de red más avanzadas también pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de video analógico. Algo muy importante es que a diferencia de cualquier otro tipo de cámara, las cámaras de red no necesitan estar conectadas a una computadora ni dependen de ella, son totalmente independientes y auto administrables, lo cual incrementa su funcionalidad.

En resumen podemos decir que todo lo necesario para tomar y transmitir imágenes esta dentro de la cámara, lo único que se necesita afuera de ella es el medio para ver el video que es una computadora con un Explorador de Internet, las cuales se pueden encontrar prácticamente en cualquier lugar del mundo.

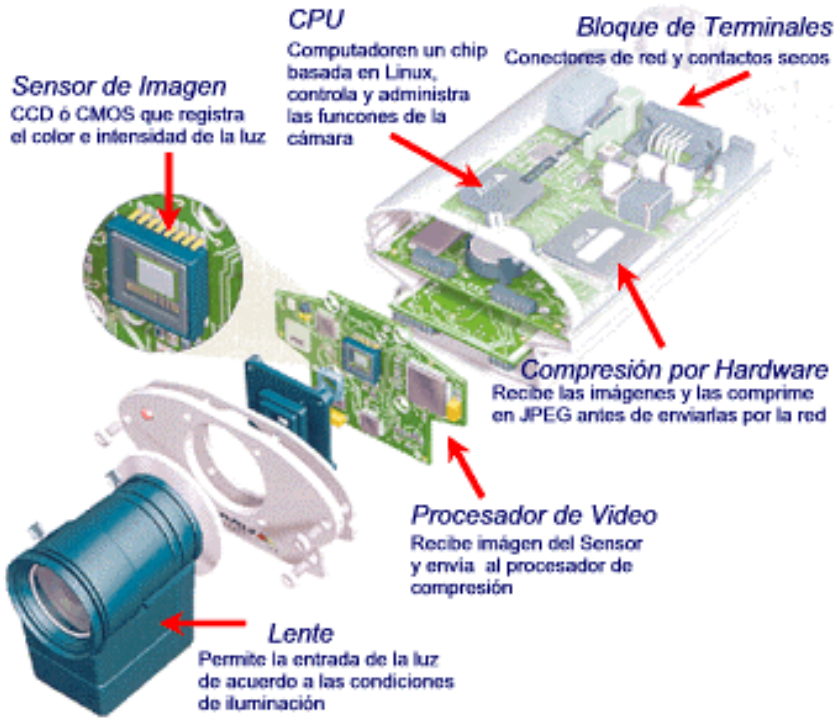
COMPONENTES

Básicamente una cámara IP se compone de:

- La " cámara " de video tradicional (lentes, sensores, procesador digital de imagen)
- Un sistema de compresión de imagen, para poder comprimir las imágenes captadas por la cámara a formatos adecuados como MPEG4
- Un sistema de procesamiento (CPU, FLASH, DRAM y un módulo Wireless ETHERNET/WIFI). Este sistema de procesamiento se encarga de la gestión

de las imágenes, del envío al modem, del movimiento de la cámara (si dispone de motor), y de la detección de movimiento.

Con todo esto únicamente necesitamos conectar la cámara al Router ADSL y a la alimentación eléctrica y si usamos la cámara en una red local, la conectamos a un HUB/SWITCH y pasa a ser un equipo más que se comunica con el resto de la LAN (y con el exterior si la LAN dispone de conexión a Internet)



El proceso que sigue la transformación de las imágenes ópticas a digitales se lleva a cabo a través de los componentes de la cámara que inicialmente captan las imágenes y convierten las diferentes ondas de luz a señales eléctricas que son convertidas a formato digital y transferidas a la función de cómputo que las comprime y envía a través de la red.

El lente de la cámara enfoca la imagen en el sensor (CCD/CMOS), que pasa a través del filtro óptico el cual remueve cualquier luz infrarroja (IR) para que los colores sean mostrados correctamente y finalmente el sensor de imagen

transforma las ondas de luz en señales eléctricas que a su vez se convierten en señales digitales en un formato que puede ser comprimido y transferido por la red.

El procesador realiza las funciones de administración y control de la exposición (Niveles de Luz), balance de blancos (Ajuste de Colores), brillo de la imagen y otros aspectos relacionados con la calidad de la imagen.

El conector de red Ethernet es el encargado de conectar periféricos en la red a 10/100 Mbits, con funciones avanzadas para el manejo de memoria directa (DMA) y un amplio rango de interfaces de entrada /salida (I/O).

El CPU, las memorias Flash y DRAM representan el "cerebro" de la cámara, ya que están diseñadas específicamente para aplicaciones de red y en su conjunto manejan las comunicaciones de la red y del servidor web.

A través del puerto de red Ethernet, una cámara de red de alta tecnología puede enviar imágenes directamente a 10 ó más clientes ó computadoras simultáneamente, si las imágenes son enviadas a un servidor web externo en lugar de a los clientes directamente, se pueden manejar prácticamente un número ilimitado de usuarios.

Ventajas de Una Cámara IP

Existen una gran cantidad de ventajas a favor de una cámara IP o de red cuando se compara ya sea con una cámara web basada en PC ó con una cámara de tecnología antigua como son las cámaras análogas; en primer lugar podemos mencionar que una cámara IP es una unidad independiente y no requiere de ningún otro dispositivo ó computadora para la captura y transmisión de imágenes ya que cuenta con su propio servidor web incluido que realiza todo este trabajo, lo único que se requiere es una conexión de red Ethernet estándar.

Una cámara IP tiene las siguientes ventajas:

1. **Flexibilidad** - Se puede conectar en cualquier lugar y se pueden utilizar dispositivos como modems, celulares, adaptadores inalámbricos ó la misma red cableada como medio de transmisión.
2. **Funcionalidad** - Todo lo que se necesita para transmitir video sobre la red esta incluido en la cámara.
3. **Instalación** - Solo se requiere asignar la IP para empezar a transmitir video.
4. **Facilidad de Uso** - Se puede administrar y ver el video en una computadora estándar con un navegador de internet.
5. **Estabilidad** - Ya que no requiere de componentes adicionales se tienen una mayor estabilidad.
6. **Calidad** - Proporcionan imágenes de alta calidad en formato MJPEG ó MPEG4.
7. **Costo** - El costo es muy bajo ya que el costo total para transmitir video es el de la cámara.

Usos de cámaras IP

Las cámaras IP proporcionan varias posibilidades de costo efectivo para el monitoreo y vigilancia remota de personas, propiedades, lugares, activos, maquinaria y equipo, zonas turísticas, aseguramiento de bienes y personas con ayuda de información de alarmas y detección de movimiento. Prácticamente las posibilidades son ilimitadas y tienen la ventaja de que el video al ser transmitido por la red puede ser consultado en cualquier lugar del mundo.

Algunas de las aplicaciones de monitoreo y vigilancia que actualmente se está utilizando con esta tecnología son:

1. Monitoreo y vigilancia Urbana y lugares públicos,
2. Monitoreo y vigilancia residencial con ó sin manejo de alarmas,
3. Monitoreo y vigilancia de oficinas, fabricas y negocios,
4. Monitoreo y vigilancia de escuelas y hospitales,

5. Monitoreo y vigilancia de casinos,
6. Monitoreo y vigilancia de Bancos, Casas de Bolsa, Aseguradoras, Casas de Cambio,
7. Monitoreo y vigilancia de Obras de Construcción,
8. Monitoreo y vigilancia de Museos,
9. Monitoreo y vigilancia de Carreteras y vías de comunicación,
10. Monitoreo y vigilancia de Equipo y Maquinaria,
11. Monitoreo y vigilancia de enfermos, niños, ancianos y mascotas,

Estos son solo algunos ejemplos del uso actual pero en realidad las posibilidades de vigilancia y monitoreo son ilimitadas

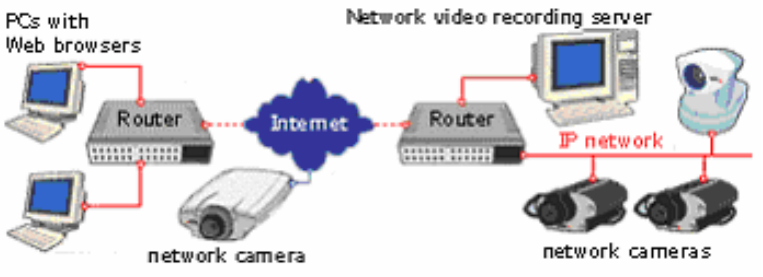
Instalación de una cámara IP

Instalar una cámara IP es muy sencillo y depende de cuan sofisticado sea el sistema que se desea instalar, para ello se debe seguir los siguientes pasos:

1. Colocar la cámara en una pared / techo / poste
2. Configurar la cámara
3. Conectarla a Internet

Si es un sistema sencillo, la cámara IP se conecta directamente al modem de Internet y si es un sistema sofisticado se necesita conectarla primero a un router ó switch, es decir si se quiere compartir Internet con otras cámaras ó computadoras de la red.

Normalmente, un modem cuentan con una salida y solo se le puede conectar una computadora o una cámara. En el caso que se desee conectar varias computadoras y cámaras a ese modem, necesitará un puente (ruteadores / switches) de salidas múltiples, al que se conectan las computadoras/ cámaras y después estos puentes al modem.



Implementos para el video remoto

Cableado Ethernet

Servicio de Internet con velocidad mínima de 256kbps

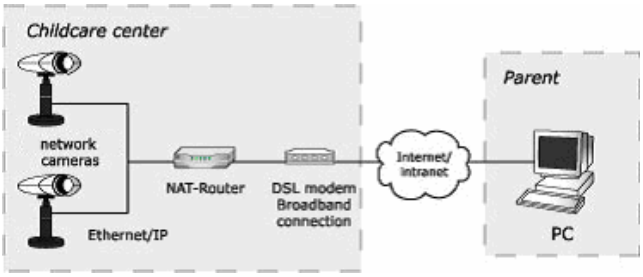
Numero de IP fijo. Este número es proporcionado por el proveedor de Internet.

Experiencia en computación ó tecnología informática.

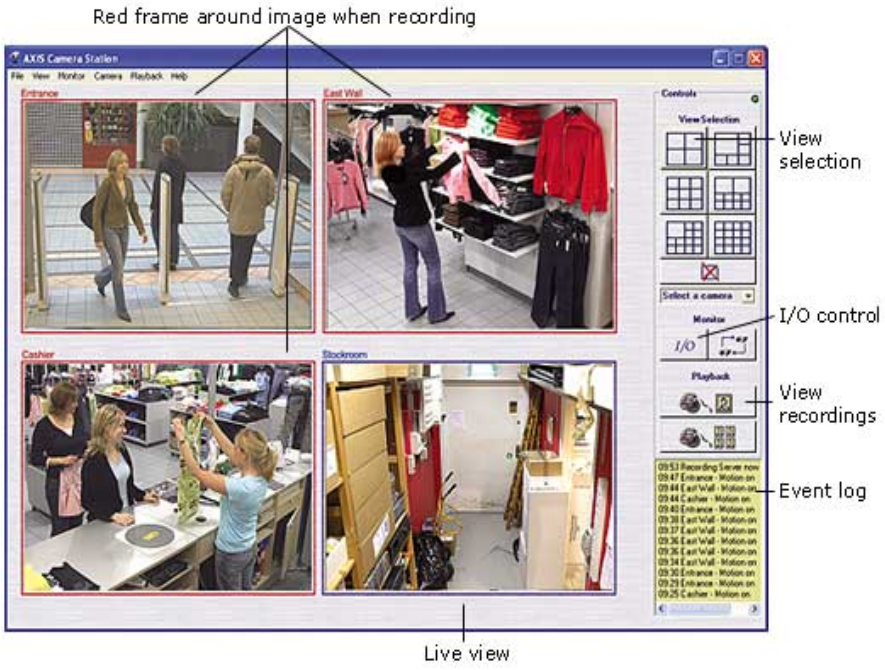
Un router con múltiples entradas (para compartir la señal de Internet).

Cámaras IP que se conectan directamente al modem / router de Internet.

Para acceder al video remotamente y vigilar no se requiere de otros componentes de cctv, como monitores ó secuenciadores, solo su computadora que puede estar en cualquier parte del mundo.

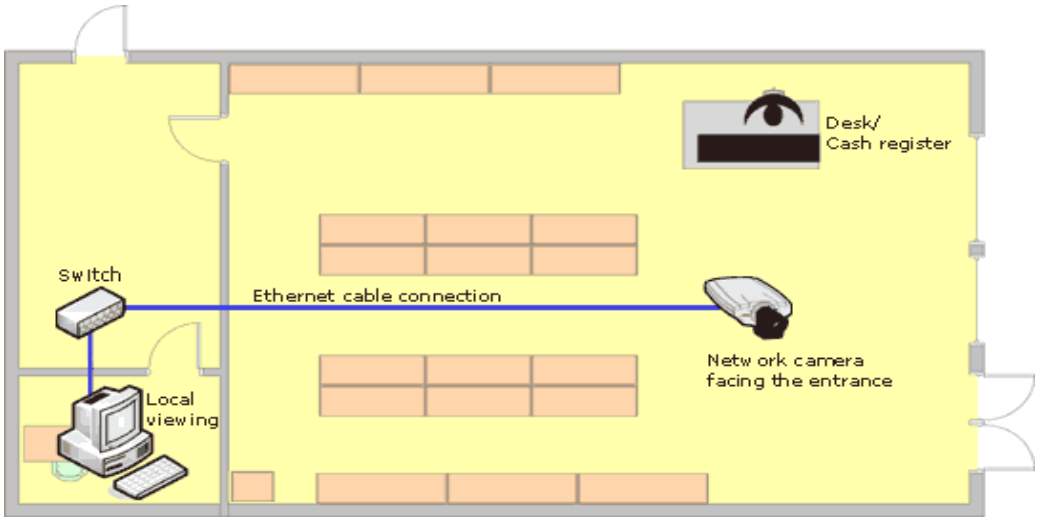


La única aplicación donde se requiere una PC, es cuando se necesita visualizar múltiples cámaras al mismo tiempo. En este caso, se necesitará una PC donde se instalan las cámaras y el software para almacenar el video en el disco duro. Cuando se accesa a esta PC remotamente, se podrá ver todas las cámaras simultáneamente; sin el software, se tendrá que recorrer cámara por cámara en su monitor. También se puede acceder a las grabaciones del disco duro.



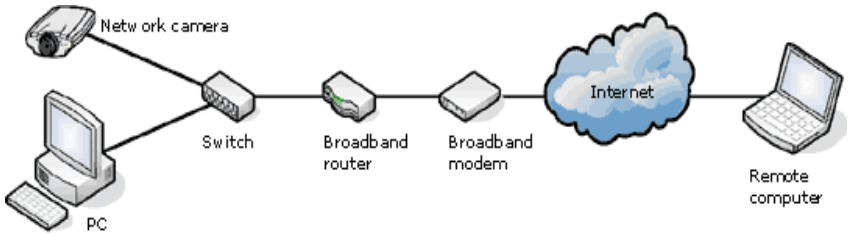
Conexión de una cámara IP a una red LAN

Para realizar la conexión de una cámara IP a una red LAN se debe colocar la cámara en cualquier punto de la red LAN y asignarle un número de IP; se podrá observar imágenes desde cualquier terminal en la red local ó a través del Internet.



conexión a una LAN sencilla

Para el caso en que residencias ó negocios carezcan de redes de computadoras, simplemente se debe conectar la cámara directamente al modem ó a un router de terminales múltiples.



La cámara IP se conecta directamente al Internet.

Ventajas de una cámara IP frente a un CCTV

Una cámara IP aporta grandes ventajas frente al tradicional CCTV:

- Posibilidad de acceso desde cualquier sitio del mundo. Un CCTV es, como su nombre indica, "cerrado", por ello hay que estar en el lugar del CCTV para poder ver las imágenes.
- Es más barato. Instalar cámaras IP es muy sencillo ya que es como instalar una red local LAN o conectarla directamente al Router. No se necesita las complicadas y caras instalaciones de CTV.
- Ampliable. Es muy sencillo añadir más cámaras IP a un sistema, mientras que en un CCTV necesitamos duplicar sistemas de monitorización durante la ampliación del sistema.

ACCESO A UNA CÁMARA IP

Una cámara IP, al igual que los servidores de Vídeo, dispone de un software interno sobre el tema de seguridad, que nos permiten establecer varios niveles de seguridad sobre el acceso:

- **Administrador**: Para poder configurar el sistema. Nos pide un nombre de usuario y una contraseña
- **Usuario**: Para poder ver las imágenes, manejar la cámara y manejo del relé de salida. Nos pide un usuario y una contraseña.
- **Demo**: permite un acceso libre. No pide ningún tipo de identificación.

Soluciones de seguridad en bancos, aeropuertos y casinos son sólo unos pocos ejemplos o aplicaciones profesionales basadas en cámaras de red, que son algo común en nuestros días.

Los últimos avances han hecho posible conectar cámaras directamente a una red de ordenadores basada en el protocolo IP. La tecnología de las cámaras de red permite al usuario tener una cámara en una localización y ver el video en tiempo real desde otro lugar a través de la red o de Internet.

El acceso puede ser restringido, de manera que sólo las personas autorizadas puedan ver las imágenes, o el video en directo puede ser incorporado al web site de una compañía para que todo el mundo pueda verlo.

SOFTWARE DE MONITOREO

Un software de monitoreo ó de vigilancia es un conjunto de programas que tienen la finalidad de convertir cualquier computadora en todo un sistema profesional de vigilancia y monitoreo, el cual permite organizar la información de las cámaras para que puedan ser vistas de forma individual ó por grupo, captar el video en línea y mostrarlo a los usuarios, almacenar el video y permitir que los usuarios lo puedan consultar posteriormente ya sea de forma local ó por la red.

Un Software de monitoreo en una computadora viene a reemplazar una gran cantidad de equipos que se tienen en los sistemas de CCTV tradicional, como son los multiplexores, secuenciadores y grabadoras, además de que permite incluir mucho mayor funcionalidad y eficiencia en estos sistemas para hacerlos más inteligentes cada día.

Funcionamiento

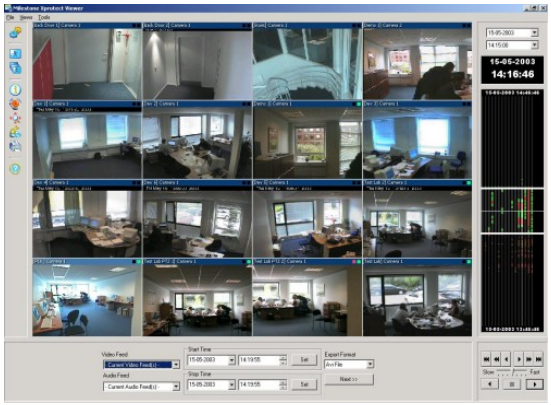
Existen varios Softwares comerciales en el mercado y varían entre ellos en cuanto a las funciones incluidas y formatos de ventanas, pero básicamente todos cumplen con la funcionalidad básica de organizar las cámaras y mostrar el video tanto en línea como el almacenado.

Es importante mencionar que existen algunos softwares que no almacenan video y solo tienen funciones de multiplexado (Visión de varias cámaras en una misma ventana) y/o secuenciación (Visión de una ó varias cámaras en grupo secuencialmente a intervalos de tiempo definido.

El proceso que siguen es muy simple y comienza con la cámara que obtiene las imágenes en vivo y las transmite al software quien las procesa ya sea para almacenarlas y/o analizarlas y activar alarmas.

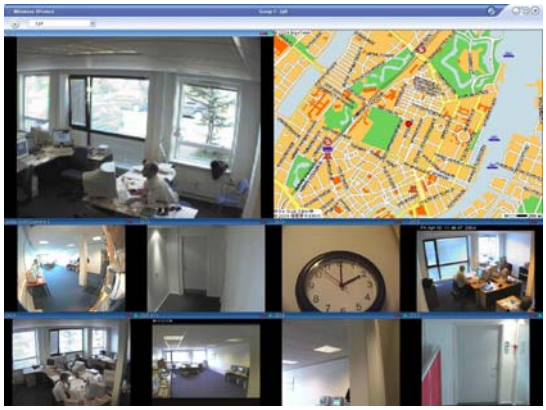
Cuando se tiene alguna solicitud por parte de algún cliente primero se validan los permisos y posteriormente si son adecuados le envía ya sea el video en línea, almacenado ó la información necesaria para recibirlo de la cámara.

El software de monitoreo nos permite:



Visualizar varias pantallas simultáneamente

Detección de movimiento



Monitoreo con mapa

Monitoreo de imágenes térmicas

Características

Las características pueden variar de un producto de software a otro, pero para que sean funcionales deben de contar con al menos las siguientes:

- **Facilidad de Uso** - Deben ser fáciles de usar ya que en muchas ocasiones quienes los operan no son personas con grandes conocimientos de computación y redes.
- **Perfiles de Usuario** - Deben permitir la definición de perfiles de usuario para evitar accesos no autorizados.
- **Vistas Individuales y por Grupo** - Deben manejar el desplegado de cámaras individuales y por grupo (más de una en una misma ventana), algunos pueden inclusive manejar secuencias individuales ó de grupo.
- **Definición de parámetros Independiente** - Algo importante es que debe permitir la definición de parámetros para monitoreo local, monitoreo remoto y grabación de manera independiente, esto permite optimizar los recursos de comunicaciones y almacenamiento en cualquiera de los tres casos.
- **Grabación** - Una característica vital es la grabación, hay productos que manejan hasta varias imágenes por segundo, minuto ú hora, estas ultimas permiten tener mucho más versatilidad; además la grabación programada ó por horarios, es decir que se grabe únicamente a un cierto horario, así como también grabación por detección de movimiento lo que permite optimizar los recursos de almacenamiento.
- **Manejo de Alarmas** - El manejo de alarmas que pueden enviar mensajes cuando se detecta algún cambio ya sea de la imagen ó de algún sensor conectado a los contactos secos de la cámara.
- **Monitoreo Remoto** - Es importante considerar que el software permita el acceso remoto al video en línea y al video almacenado.

ALARMAS

Un sistema de alarma esta compuesto por una central, un teclado, una sirena y distintos tipos de sensores tales como:

- **Sensores infrarrojos o de movimiento**: estos sensores actúan ante la detección de movimiento de cuerpos calientes (cuerpo humano). Existen algunos modelos que poseen inmunidad para las mascotas esto permite que las mascotas circulen libremente por la casa sin disparar el sistema tal como lo haría un humano.

- **Barreras Infrarrojas**: estos sensores crean un cerco invisible en el perímetro de la casa y accionan al ser interferidos por algún objeto de tamaño considerable.

- **Sensores Magnéticos o de Apertura**: Estos sensores se utilizan en puertas, ventanas y portones para detectar la apertura de las mismas. Estos se dividen en dos categorías interiores para puertas y ventanas y blindados para portones.

El CCTV (Circuito Cerrado de Televisión): Sus componentes pueden ser:

- **Monitor o TV**: Es donde se conectan las Cámaras para poder visualizarlas. Poseen de 2 a 12 entradas para cámaras. Algunos cuentan con un

Secuenciador (intercambia entre las cámaras conectadas automáticamente) o con un Quad (divide la pantalla en 4 cuadros mas chicos para visualizar 4 cámaras al mismo tiempo).

- **Cámaras**: Existen en varias formas y tamaños. Pueden ser de Color o B/N. Son sensibles a la luz infrarroja de modo que permiten la visión nocturna.

- **Gabinetes para Intemperie o Antivandalicos**: Son los que se utilizan para colocar las cámaras en lugares donde estas serian afectadas por las condiciones climáticas, también se utilizan para impedir el hurto de las cámaras.

- **Cámaras IP**: Estas cámaras se conectan directamente a Internet como una máquina mas de su red de computadoras y le permite visualizar su casa o negocio desde cualquier parte del mundo solo teniendo una computadora conectada a Internet.

6.5. APARTADO 5

PASOS PARA EL DISEÑO DE UN SISTEMA DE SEGURIDAD

Entre los pasos principales tenemos:

1. Estudio de planos
2. Análisis de áreas críticas
3. Definir áreas a proteger
4. Análisis de tecnología a utilizar
5. Costos
6. Ubicar el PC que hace de servidor
7. Diseñar el cableado
8. Diseño del sistema de seguridad

Beneficios de un sistema de seguridad

Visualizar y controlar lo que esta sucediendo es ahora muy sencillo como conectarse a Internet, la tranquilidad y seguridad cuando se esta ausente de un determinado sitio puede ser posible gracias a un completo sistema de vigilancia o de seguridad, que permita evitar los delitos o poder identificar a los autores de un robo o de una conducta indebida.

Dentro de los principales beneficios tenemos:

- **Visualizar el entorno del trabajo**

  Se podrá visualizar de forma remota y realizar el control del personal y, como consecuencia, aumento de productividad de los empleados, así como también logrará un control del consumo de productos con las diferentes cámaras instaladas estratégicamente, además de conseguir una notable seguridad en la empresa.
- **Comodidad y seguridad**

Las cámaras cuentan con un sistema de detección de movimiento, que en el momento de activarse esta, envía una notificación al mail informando la presencia de intrusos en la empresa, donde simplemente, sin salir de casa se podrá acceder a Internet y ver lo que sucede.

- **Niveles de permisos para una mayor seguridad**

  El sistema no limita el control a una única persona, sino que cuenta con niveles de permisos al acceso de las cámaras, donde solo personal autorizado y de entera confianza podrá monitorear el área o la sucursal según el nivel otorgado, asimismo podrá realizar un control del sistema de video vigilancia de la empresa.

- **Inversión asegurada**

  No es necesario ningún programa adicional para poder ver las cámaras de su empresa a distancia. Por otro lado los equipos pueden actualizarse remotamente cuando aparecen nuevas funciones y características, por lo que no se quedan antiguos ni obsoletos.

- **Sistema abierto**

  El sistema digital es abierto y permite un acceso local y remoto vía Internet o mediante redes, permitiendo movilidad y un control más amplio.

- **Potencia y versatilidad**

  Incluye gran cantidad de funciones como son: administración de usuarios, administración de cámaras, grupos, etc. Todo es configurado remotamente desde el navegador de Internet.

- **Usos múltiples**

  Un ejemplo sencillo del uso del sistema de vigilancia es que usando una cámara de vigilancia en el área de recepción de una empresa para ver movimientos durante la noche, puede ser parte de un sistema de control de acceso automatizado durante las horas de trabajo.

DISEÑO DEL SISTEMA DE SEGURIDAD MEDIANTE CÁMARAS IP

Para el cableado de las cámaras IP del sistema de seguridad se debe determinar lo siguiente:

Dmáx = 15.60 m

Dmin = 4.50m

Prom = 10.05m

Prom + 10%holgura = 11.055

Total = 11.055 m

Longitud ajustada promedio = 11 m

de tomas = 6

Longitud total del cable = 11m * 6 puntos

Longitud total del cable = 66 m

Longitud total del cable aproximado = 100 m

Planos:

MATERIALES

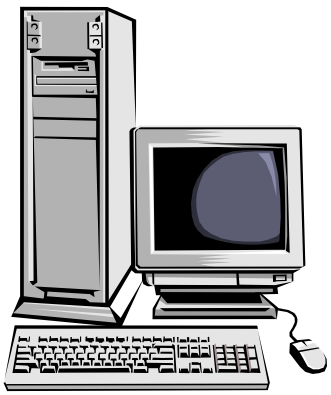
- **CAMARA IP PANASONIC BL-C10**

  Ref. PAN37BLC10

- **PANASONIC SOFTWARE PANASONIC GRABACION IP**

  Software de grabación para cámaras IP, se puede utilizar desde 4 cámaras hasta 10 cámaras.

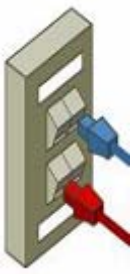
- **CPU Pentium 4 de 3Ghz**



- **Cable UTP categoría 5E**

- **Conectores RJ45**

- **Jack**



- **Switch**

- **Canaletas**

PRESUPUESTO

Item	Descripción	Cantidad	Costo unidad	Total
1	CAMARA IP PANASONIC BL-C10	6	867.68	5206.08
2	PANASONIC SOFTWARE PANASONIC GRABACION IP	1	310,02	310.02
3	CPU Pentium 4 de 3 GHz	1	950.00	950.00
4	Cable UTP categoría 5E	100 m	0.50	50.00
5	Conector RJ45	14	0.30	4.20
6	Jack	7	2.30	16.10
7	Switch	1	35.00	35.00
8	Canaletas	25 m	1.00	25.00
TOTAL				**6596.40**

BIBLIOGRAFÍA

Libros:

- Vigilante de Seguridad- Área técnico-profesional/Editorial CPD/ Madrid,1999
- Directores de Seguridad-Seguridad y Protección/ Editorial CPD/ Madrid, 1999
- Revista SEGURITECNIA.
- Internet Artículos de Macworld
- Comunicaciones y Redes de Computadores, William Stallings, Prentice Hall, 6ªed., 2000
- LAN wiring, James Truvole, McGraw-Hill, 2ªed., 2000

Páginas de Internet:

http://www.axis.com/es.

http://www.area-integral.net

http://www.casaactiva.com.ar

http://www.definicion.org

http://www.gscssoftware.com

http://www.ilustrados.com

http://www.la-fortaleza.com

http://www.lfmx.com

http://www.manualphp.es

http://www.masadelante.com

http://www.monografias.com

http://www.ofisec.net

http://www.ralco-networks.com

http://www.telenetcentral.es

http://personales.upv.es

http://www.rvcseguridad.com

http://www.terra.cl/tecnologia

ANEXOS:

Cámara IP PANASONIC BL-C10

Especificaciones Técnicas	
Interface de red	1 conector 10 Base-T / 100 Base TX Ethernet RJ45
Sensor infrarrojo Pyroeléctrico integrado	Angulo de detección: horizontal 30º y vertical sobre 85º. Rango de detección: hasta 5m a 20ºC
Montaje	En la pared o sobre trípode
Agujero de rosca para el trípode	En la parte posterior y en el fondo
Temperatura de funcionamiento	+5ºC a +40ºC
Rango humedad	20-80% Sin condensación
Dimensiones	74 x 98 x 61 mm
Peso	170g.
Alimentación	12 V DC (Adaptador incluido 100 - 240 V AC)
Consumo máximo	3.5w
Consumo en reposo	2.5w
Especificaciones de Servidor	
Compresión de imagen	JPEG
Formato de reproducción de video	Movimiento en JPEG
Resolución del video	640 x 480, 320 x 240, 160 x 120 pixeles
Niveles de compresión de imagen	3 niveles
Rango max.de frame	15 fps (320 x 240, 160 x 120) 7.5 fps (640 x 480)
Autentificación	ID / Password de autentificación Administración / Usuarios Generales(hasta 50)
Protocolos de red	TCP, UDP, IP, HTTP, FTP, SMTP,
Acceso maximo de ususarios	20
Buffer de imagen	250 fps
Transferencia de imagen	e-mail o ftp
Máximo control del ancho de banda	0.1, 0.2, 0.3, 0.5, 1.0 Mbps Ilimitado
Pantalla multicámara	hasta 12 cámaras

Especificaciones de la cámara	
Angulo de visión Horizontal	43º
Angulo de inclinación horizontal	-50 ºC a +50 ºC
Angulo de inclinación vertical	-40ºC a +10 ºC
Máxima velocidad de inclinación	50 º/ sec
Posiciones en preset	8
Sensor de imagen	1/4" 320,000 Píxeles CMOS
Enfoque	Fijo, Área de enfoque: 0.5 m ~ infinito.
Apertura	F2.8
Iluminación	1-10000LX

Requerimientos mínimos para ver en PC

- Sistema operativo: Windows 98 Se, Windows ME, 2000, XP
- Internet Explorer 6.0 o superior

PANASONIC SOFTWARE PANASONIC GRABACION IP

Características técnicas

- Software de grabación para hasta 10 cámaras IP para los modelos BL-C10, BL-C30, BB-HCM381 e BB-HCM311, utilizando Sistema Operativo Windows XP y Windows 2000.
- Número ilimitado de registros de cámaras para visualización (depende de la configuración del PC)
- Facilidad de grabación de imágenes de múltiples cámaras por la red Ethernet o Internet.
- Graba y reproduce imágenes con audio a través de las cámaras BB-HCM381 e BB-HCM311
- Programación de grabación a través de la función de Detección de Movimiento o por fecha y hora (hata 10 programas por cámara).
- Búsqueda de imágenes por fecha y hora, tipo de grabación, grabación por programación y detección de movimiento
- Limitador de capacidad de grabación, esta función permite programar el espacio máximo de datos, para ser grabado en el disco rígido del PC, regrabando sobre los datos mas antiguos.

- Zoom digital hasta 700% y reducción de hasta 25%
- Resolución de grabación: 640 x 480, 320 x 240 y 160 x 120
- Convierte todo o parte de la imagen grabada en formato de archivo JPEG

Especificaciones técnicas

Requerimientos mínimos en su PC

- Sistema operativo Microsoft Windows XP profesional Edition o Windows 2000 (Server Pack 2 o superiores)
- Navegador Internet Explorer 6.0 o superiores
- Sistema de ficheros NTFS (NT File System)
- Audio Salida de audio

Especificaciones hardware conectando 10 cámaras y conectando 4 cámaras

- CPU - Pentium 4 de 3 GHz o superiores o procesador compatible.
- Memoria - 512 MB o superior
- CPU Pentium 4 de 1.8 GHz o superiores o procesador compatible
- Memoría - 256 MB o superior

Contenido de PANASONIC SOFTWARE PANASONIC GRABACION IP

1 CD-ROM

1 Manual de usuario

1 set de códigos de registro para 3 PC's