CAPITULO 2

MARCO TEÓRICO

2.1 CONCEPTOS BÁSICOS DE UN SISTEMA DE CCTV

El Circuito cerrado de televisión o su acrónimo CCTV, que viene del inglés: *Closed Circuit Television*, es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades. Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores. [1]

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos u ordenadores. Las cámaras pueden estar sostenidas por una persona, aunque

normalmente se encuentran fijas en un lugar determinado. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, inclinación y zoom.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros... Todas estas cualidades hacen que el uso del **CCTV** haya crecido extraordinariamente en estos últimos años. Al principio se hacían este tipo de instalaciones para disuadir o detectar robos y, hoy en día, no sólo se utiliza para seguridad, sino también para otros propósitos específicos como pueden ser los de la medicina, la educación o la lucha contra eventos antisociales.

En muchos hogares se utilizan como sistemas de seguridad, aunque también pueden desarrollar otra función como es la de recopilar evidencia de violencia doméstica. También se colocan en bancos, casinos, centros comerciales, vías de circulación, aeropuertos, áreas e instalaciones públicas, entre muchos otros lugares. En el área industrial y minera es utilizada en procesos industriales.

Figura 2.1 Sistema de CCTV

Al tratarse una señal analógica, el único dato a considerar es la atenuación. Al aumentar las exigencias de seguridad de las instalaciones, se incrementa la cantidad de datos a transmitir, y con ello se necesita un mayor ancho de banda para esta transmisión. Esto lleva al empleo de la señal digital; cuya primera y más

evidente aplicación es la multiplexación de varias señales de forma de poder enviarlas por un solo canal, permitiendo de esta manera la transmisión simultánea de imagen, telemetría, voz, datos de control de barrera, etc.

La generalización, fiabilidad y abaratamiento de los sistemas informáticos (LAN, WAN, etc.) permiten la incorporación a estas redes del sistema de CCTV con la salida digital IP (Internal Protocol). Al estar este sistema incluido en una red Ethernet como un componente informático mas, todo el conjunto gana en flexibilidad y adaptabilidad, por ello, los sistemas de seguridad ganan en prestaciones. [2]

2.1.1 CCTV ANALÓGICA

Existen varios tipos de cámaras de CCTV analógico como son:

Cámaras fijas

En este caso, la señal captada por una cámara es transmitida en formato analógico por un cable, generalmente coaxial, hacia el centro de control. Allí es recibida y tratada al ojo humano a través de un conjunto de monitores, videograbadores, etc. Se trata de enlaces punto a punto, correspondiendo a cada cámara una entrada en el conjunto receptor y un cable transmisor.

En las cámaras móviles (domos), la señal de telemetría es transmitida mediante un cable de pares de cobre, paralelo al coaxial de la señal de video. Al tratarse de una señal analógica, su debilitamiento debido a la longitud del enlace, puede hacerla irreconocible por el receptor. Ante este problema se presentan dos soluciones: el empleo de regeneradores de señal o la transmisión por otro medio con menos pérdidas, como es la fibra óptica.

Para ello es preciso intercalar entre Tx y Rx dos convertidores optoelectrónicas cuya misión será convertir la señal de vídeo eléctrica en óptica y viceversa.

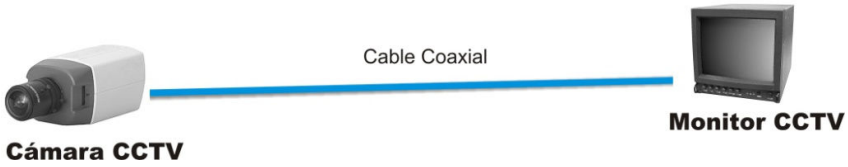

Figura 2.2 Transmisión por cámara fija

Las características básicas a considerar en este caso son las pérdidas admisibles por el conjunto Tx-Rx (diferencia entre la potencia emitida por el Tx y la sensibilidad del Rx), variables en función de las marcas y modelos de los equipos.

Cámaras PTZ (Domos)

Los enlaces a través de fibra óptica para este tipo de cámaras tienen lugar incorporando al circuito unos convertidores opto electrónicos (Tx y Rx) de doble canal:

- Canal de vídeo con entrada BNC y salida con conector óptico
- Canal de datos (Rs-232, RS422 ó RS485) con entrada de cable de pares (Conector Sud o bornes) y salida conector óptico

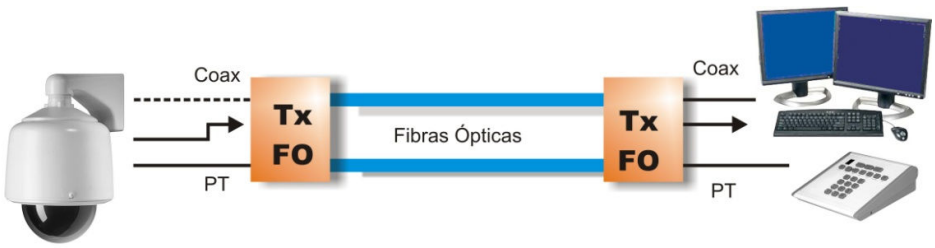

Figura 2.3 Transmisión de cámara domo por fibra óptica

El procedimiento de selección de las fibras es similar al señalado en el apartado anterior, utilizándose equipos de una sola fibra cuando la distancia a cubrir lo permite, tal y como se ha indicado para los duplicadores DWDM.

2.1.2 CCTV DIGITAL

[1]En este caso, la señal analógica procedente de la cámara CCTV es digitalizada por el convertidor opto-electrónico, conducida a través de una fibra óptica MM o SM y convertida nuevamente en señal analógica en el centro de control, y explotada por los monitores CCTV, teclado, registradores, etc.

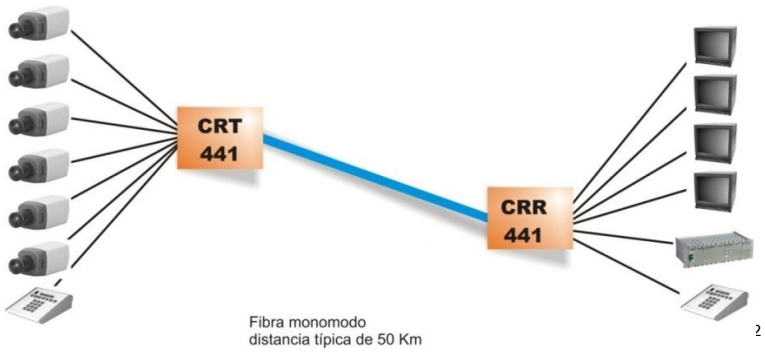

Figura 2.4 Esquema de CCTV digital

Las posibilidades de multiplexado de diferentes señales digitales por una sola fibra permiten la transmisión, por este medio, de forma simultánea de:

- Varias señales de vídeo sin comprimir, de alta calidad
- Audio
- Datos de control (Telemetría, barreras, alarmas, sensores de presencia, etc.)

De la misma forma que en casos anteriores, la utilización de duplicadores permite aumentar la capacidad de las fibras, al transmitir en dos longitudes de onda

[1] CRT (dispositivo de tubo catódico). CRR (Control Remoto de Robots)
[2] Centre for Wireless Communications (CWC). CAPI Voice Mail System (CVM). Multiplexación por división de longitud de onda (WDM). Central Outer Tracker (COT)

simultáneamente; con lo que se logra una máxima optimización de estas, llegando a transmitir por una f.o. SM hasta 64 canales de vídeo CTV.

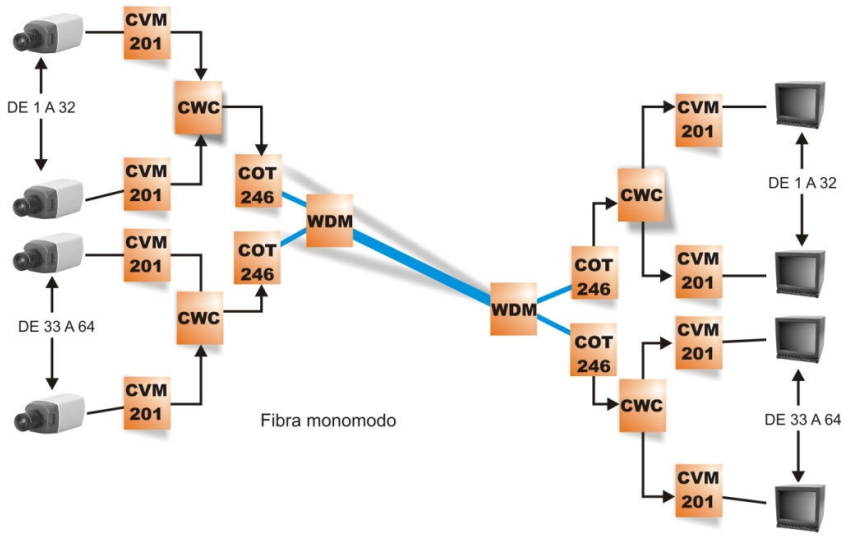

Figura 2.5 Diagrama de bloques de un enlace MxCCTV Digital

Este tipo de enlaces, de especial aplicación en instalaciones con grandes concentraciones de equipos (por ejemplo: pasarelas de control de autopistas, estaciones de peaje, estaciones de FFCC, accesos a factorías, etc.) precisa de fibras ópticas con gran ancho de banda, por lo que serán necesarias las de tipo SM G652 B (1300 nm) y G652 C (1550 nm).

En el caso de aplicaciones de este tipo de equipos sobre fibras ópticas MM, las características de la fibra condicionará la distancia máxima a alcanzar.

2.1.3 CCTV DIGITAL IP

De creciente aplicación en entornos con posibilidad de conexión a un entorno ofimático Ethernet, o formando redes dedicadas, este sistema consiste en la conexión a partir de un puerto f.o. o RJ 45 (Cobre) de cámaras con salida digital IP (Internet Protocol) a una red de datos (LAN o WAN).

La transmisión de todo tipo de señales captadas por los diferentes captadores (cámaras, sensores de presencia o de humos, audio, etc.) permite todo

tipo de combinaciones posibles: almacenar secuencias, tratarlas, verlas en tiempo real, etc.

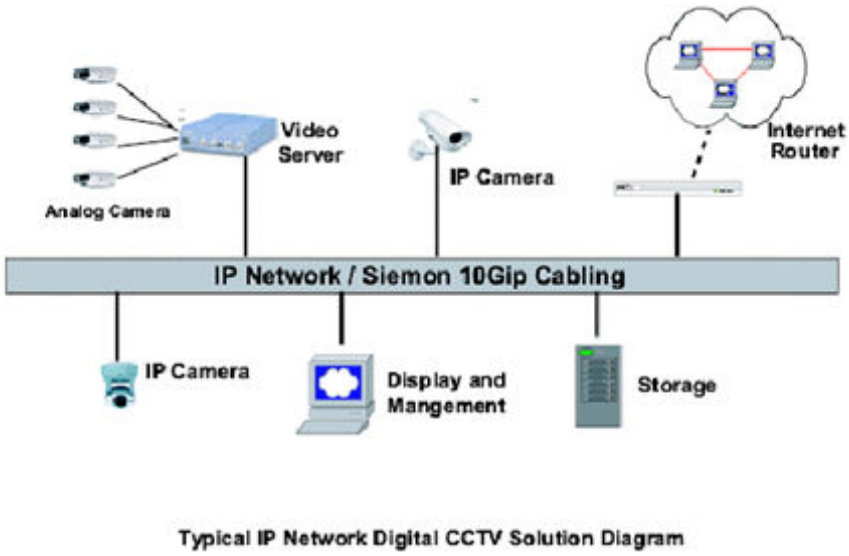

Figura 2.6 Diagrama de una red digital IP

Por la misma razón, este tipo de redes permite una más rápida y barata, al no ser ya preciso utilizar enlaces directos, inclusión de nuevas cámaras, desplazamiento de centros de control, redireccionamiento de señal, etc.

Los equipos se conectarán a la red mediante un conector RJ-45 (par trenzado de Cobre Cat. 5e o superior), o mediante un convertidor Cu - F.O. Ethernet para enlazarlos mediante fibra óptica si eso fuera preciso, como consecuencia del mayor ancho de banda necesario.

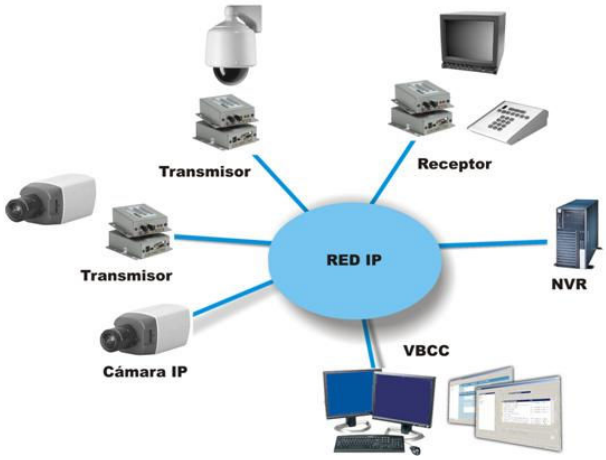

Figura 2.7 Esquema de red CCTV-IP

En efecto, las imágenes digitales de alta resolución necesitan un gran ancho de banda para la transmisión. Los programas de compresión (JPEG, JPEG2000, MPEG 1, 2, 4) precisan de una velocidad de transmisión de entre 3 y 6 Mbps para una buena resolución, y por ello una red a 100 Mbps soportará entre 19 y 30 cámaras, en función de la ocupación de la red y los datos accesorios a transmitir.

Esto hace aconsejable, para un mejor aprovechamiento de las ventajas de una red de vigilancia CCTV-IP, el implementar Gigabit Ethernet, con la fibra óptica precisa en todos sus enlaces en función de la distancia a cubrir por cada subsistema. Asimismo puede ser interesante, desde el punto de vista de la seguridad, el establecer redes dedicadas para un número de cámaras o domos superior a 50 unidades.

2.2 ESTRUCTURA DE LOS SISTEMAS DE CCTV

Entre los elementos que conforman una estructura de un sistema de CCTV. se pueden enumerar a los siguientes:

2.2.1 Elementos Captadores de Imagen (Cámaras)

Este grupo está conformado por las cámaras de TV. que pueden ser de varios tipos y los accesorios que pueden complementarlos. [3]

Cámaras de TV. en circuito cerrado

Las cámaras utilizadas son todas muy parecidas y la captación de imágenes puede hacerse en blanco y negro o en color. Descomponen la escena captada en líneas horizontales, analizan los diferentes niveles de luz de las mismas y los convierten en impulsos eléctricos en forma proporcional. Realizan esta función por medio de un chip denominado CCD o sensor de imagen, circuito integrado con la tecnología de los fotosemiconductores. Estos sensores no serían capaces de trabajar sin el aporte de una óptica que trabaja, al igual que en una cámara fotográfica, enfocando la imagen captada y controlando la cantidad de luz incidente, en este caso, sobre el CCD.

Existen diferentes tipos de ópticas dependiendo de las necesidades del sistema de captación. La elección dependerá, esencialmente, de la distancia a la que se encuentre el objeto a vigilar denominada "distancia focal" y la apertura del objetivo para captación de luz indicada por la letra "f'. Otras condiciones que se deben tener en cuenta es si necesitamos variar la distancia focal por tener que controlar un amplio espacio o necesitamos ver detalles interesantes en un momento dado, para esto lo necesario sería un objetivo tipo zoom.

La elección de una cámara se basará en definitiva en elegir un cuerpo de cámara y un objetivo adecuados a nuestras necesidades, guiándonos por los catálogos de los fabricantes. Para ello, conviene saber con qué parámetros podemos jugar y qué significado tienen.

Si del cuerpo de la cámara hablamos encontraremos parámetros como el tamaño del CCD, medido en pulgadas y pudiendo ir desde 1/2", 1/3" como más convencionales. Otro apartado importante es la resolución horizontal de la cámara definido en número de líneas de barrido de la imagen. Esta característica define la calidad de la reproducción sobre el monitor final, de modo que a mayor número de líneas mayor definición en la imagen. Hay cámaras con 330, 380, 470, etc.

La calidad del sensor CCD, depende de una zona de captación, medida en lo que podemos denominar puntos de captación de luz y que tecnológicamente

hablando se denominan pixeles. Podemos decir que la capacidad de captación de imagen aumenta con el número de pixeles. En este apartado existen CCD con valores de 290.000 a 440.000, aunque este es un dato que se incrementa día a día debido a la evolución de la tecnología.

Por último, uno de los datos más interesantes, sobre todo si hablamos de instalar equipos de CCTV en lugares con poca luminosidad, es el nivel de captación de luz del CCD. Este aspecto viene determinado por la medida de la intensidad de luz mínima que puede captar el CCD, pudiéndose encontrar valores de 2,5 lux, 2,0 lux, 1 lux o incluso menos de 0,3 lux. Claramente se puede comprender que cuanto menor sea el valor de iluminación mínima más sensible será la cámara, pero se ha de tener en cuenta que el fabricante relacionará el nivel de iluminación mínima de sus CCD con el nivel de apertura del objetivo a utilizar, que la denominábamos "f". Por eso hay fabricantes que en las características de iluminación mínima dan (por ejemplo) 0,3 lux (F 1.2), que especifica la abertura relativa del objetivo.

Una parte esencial en todo objetivo es el iris. Este elemento tiene forma de cortinilla y está situado entre la entrada de luz del objetivo y el sensor CCD (en el caso de una cámara de vídeo). Este dispositivo es el que regula el nivel de iluminación que atraviesa el objetivo de modo que impida el desajuste visual por niveles de iluminación excesivos. En las cámaras fotográficas, el iris es el que se abre en relación con la iluminación captada y la velocidad de disparo, y va conectado mecánica o eléctricamente al cuerpo de la cámara con el anclaje del objetivo en sí, normalmente de tipo bayoneta. En las cámaras de vídeo o CCTV, los objetivos incluyen un pequeño motor para ajustar el iris según el nivel de iluminación, y el conjunto normalmente se une al cuerpo de la cámara por medio de un roscado y un cable con una pequeña clavija para la alimentación del motor. En algunos objetivos encontramos, además de la motorización del iris, unos ajustes para realizar el ajuste fino final, una vez que la cámara haya realizado el suyo automáticamente. Estos ajustes suelen denominarse "ajustes de nivel de blancos".

Cámaras para estancias interiores.-

Existe una gran variedad de tipos, medidas y estilos.

Los más populares son los mini domos. Tanto para blanco y negro como para color, ofrecen una gran calidad y resolución. Son económicos y muy efectivos.

Asimismo existen cámaras en las cuales podemos elegir el tipo de objetivo, ya que las mismas están dotadas de roscas universales habilitando de esta forma el cambio de lente para poder adaptarnos a una determinada posición. También están las llamadas de infrarrojos. Estas tienen una corona de diodos infrarrojos que iluminan a una determinada distancia en ausencia total de luz. Son muy populares.

Cámaras ocultas: Son módulos de cámaras adaptables a diversos accesorios, tales como detectores de humos, relojes, muñecos, tpv, lámparas, etc. Suelen ser de gran efectividad con unos resultados muy buenos. Asimismo, existen cámaras ocultas listas para instalar. Las más populares son las que están simuladas en un detector de humos.

Cámaras con movimiento y control de lente, denominadas PTZ. Son cámaras motorizadas que permiten ser controladas por los videograbadores, así como pupitres de tele vigilancia. Casi todas disponen de un protocolo de comunicación estándar, con el que se comunican con el sistema de control y grabación. Estas cámaras nos permiten poderlas controlar a distancia, girándolas arriba, abajo, izquierda y derecha. Asimismo, algunos modelos nos permiten acercar y alejar la imagen. De momento son bastante costosas pero la efectividad que conseguimos es muy alta.

Cámaras para estancias exteriores.-

Son cámaras con las mismas características técnicas que las de interior excepto que están preparadas para soportar las inclemencias meteorológicas, tales como humedad, viento, agua, etc. Asimismo, muchas de las cámaras interiores se pueden adaptar al exterior a través de accesorios, tales como carcasas estancas. Dichas carcasas están dotadas de sistemas de calefacción con el fin de que no se forme vaho en el cristal exterior, de forma que impida la visión.

Cámaras de visión nocturna.-

Es una novedad dentro del campo de la tele vigilancia. Suelen ser cámaras infrarrojos como la descrita anteriormente. Existen además cámaras de color durante el día que conmutan a blanco y negro cuando decae la luz. En blanco y negro nos permite una mayor resolución e incluso mucha más velocidad cuando se trata de transmitir a través de internet. Una vez que se restaura los niveles de luz, vuelven a cambiar a color.

Cámaras ocultas.-

Cada día se fabrican cámaras más pequeñas y versátiles. Esto nos permite poder disimular cámaras en los más diversos objetos, techos, paredes, etc.
Existen módulos sueltos que nos permitirán alojar una cámara prácticamente en cualquier sitio. Asimismo, se comercializan ya cámaras integradas en sensores de detección de movimiento para alarmas, detectores de humos, libros, radio-despertadores, etc.

Son las mismas cámaras que se utilizan para una instalación convencional pero sin carcasas ni añadidos exteriores. Solamente la imaginación nos pondrá freno para pensar en el mundo de posibilidades que se nos abre con este tipo de cámaras.

Cámaras con movimiento: pan, tilt y zoom.-

Son las cámaras más sofisticadas de los sistemas de seguridad y tele vigilancia.

Están dotadas de movimiento, con una rotación de 360º, con un movimiento vertical de 270º y un zoom de hasta X22 (las más usuales). Suelen venir acompañadas de una tecnología muy sofisticada. El control de las mismas se hace a través de pupitres especiales o bien a través de la lan, internet, etc.

Los protocolos de comunicación que utilizan son universales, pudiéndose adaptar a la mayoría de los videograbadores y tarjetas. Las cámaras pueden ser programadas para que se vayan moviendo en una determinada secuencia: girando, subiendo, bajando, etc. También pueden ser programadas para que actúen de una determinada forma cuando alguien invade la zona a proteger, enfocando, ampliando la zona, e incluso siguiendo el objeto a vigilar. Este tipo de cámaras son bastante caras, y su utilización está bastante justificada para sitios bastante estratégicos. Tanto la instalación como el ajuste son mucho más complicados que las cámaras normales.

Muchas veces es más recomendable y, por supuesto más económico poner varias cámaras fijas cubriendo una determinada zona. Tendremos mayor control de la misma, ya que podremos acceder a las grabaciones de cada cámara individual, mientras que ésta solamente nos ofrecerá una sola grabación. El costo aproximado de cada cámara se sitúa aproximadamente en unos 1300 a 1.500 dólares.

Cámaras inalámbricas.-

Son cámaras muy pequeñas, que están compuestas por la propia cámara y un receptor que se conecta a un televisor o bien a un video-grabador. Son cámaras muy económicas que están continuamente transmitiendo. Existen cámaras en el mercado de muy buena calidad pero el costo de la misma supera con creces los 600 dólares la unidad.

Cámaras I.P.-

La combinación de los avances tecnológicos que se han venido produciendo en torno a los dispositivos de grabación de vídeo, la robótica y la posibilidad de transmitir imágenes y sonido a través de internet ha dado lugar a una nueva tecnología: la video vigilancia por IP.

Simplemente es: montar la cámara, configurar la ip, conectar al router y ya está.

Diferencia con el resto de las cámaras: su facilidad de funcionamiento. Poco a poco se van incorporando a un mercado de la video vigilancia y cada vez con más prestaciones. Desgraciadamente, también tiene sus inconvenientes:
Casi ninguna de las cámaras ip económicas incorpora un sensor ccd. Suelen venir con cmos. Muy poca resolución. Tengamos presente que la cámara profesional más económica recomendada para tele vigilancia suele tener un coste para el profesional de unos 40 dólares y viene con un CCD incorporado (el mismo tipo de componente que utilizan las videocámaras). Una cámara ip económica, actualmente está superando los 250 dólares.

Una cámara IP suele consumir mucho ancho de banda. La transmisión de imágenes utiliza muchos recursos de red. El peso de una red de cámaras ip, aparte del desembolso económico que supone, es una merma importante de recursos para cualquier empresa. El sistema de control de grabación de las imágenes hay que hacerlo de forma remota, teniendo en cualquier caso que recurrir a la contratación de servidores externos para soportar todas las secuencias. No obstante, son ideales para pequeñas instalaciones, donde no se requiera grandes prestaciones.

Conexiones de las cámaras

Podemos encontrar diferentes tipos, pero todas se basan en lo mismo.

Además de la conexión del iris automático, la cámara de CCTV llevará una salida de video a través de un conector BNC y mediante cable coaxial de 75 Ω, o 50 Ω en algunos casos. Tiene que llevar también el cable de alimentación de 220 V-50 Hz con toma de tierra.

Algunas cámaras incorporan un micrófono ambiental en su frontal. Por lo tanto, tienen que incluir también una salida de audio que podemos conectar a un equipo de audio en la sala de observación para escuchar el sonido ambiental. Para su conexión se utiliza una clavija tipo RCA macho y cable coaxial para audio de inferior sección al de video.

Control motorizado de cámaras

El sistema de motorización de las cámaras facilita el movimiento de las mismas, para su aplicación en lugares donde sea necesario realizar un barrido que puede ser en horizontal, vertical o ambos. Va incorporado en el propio soporte y consta de dos motores, uno para cada movimiento, teniendo uno inferior para el movimiento horizontal (izquierda-derecha) y otro en la parte superior de éste, que hace que el soporte en "U" invertida de la cámara se mueva de arriba abajo. [4]

El movimiento en horizontal es definido por el instalador por medio de dos pequeños finales de carrera situados sobre el motor inferior y sobre los que actúan dos piezas que giran con la cámara y que el instalador puede mover y ajustar a la conveniencia del sistema. El cableado de estos motores va dispuesto por medio de una manguera de seis conductores que es llevada hasta el mando de control de movimiento.

Mando de control de movimientos

Este elemento puede tener muchos formatos dependiendo del fabricante y de las necesidades, pudiendo ser de uso para una sola cámara o para varias. Al menos debe incluir entre sus posibilidades el control de motorización para un objetivo tipo zoom, así como un pulsador para hacer que el soporte realice un barrido automático en horizontal, constante (tecla AUTO) o bien mediante teclas en forma de flecha, realizar el movimiento deseado por el vigilante.

Como características a mencionar en el cableado, se debe tener en consideración que todo circuito de señales de vídeo debe tener una terminación en impedancia para equilibrarla con la del cable coaxial. Esta terminación debe venir dada por una resistencia de 75 Ω que en muchas ocasiones está incluida dentro de los monitores. Si no fuera así debe insertarse al final del circuito de cable dicha resistencia dentro de un conector BNC.

Como ajustes finales del monitor encontraremos los básicos de estos equipos, un ajuste primario de brillo, otro de contraste, así como dos ajustes para la sincronización de la imagen tanto vertical como horizontal.

2.2.2 Elementos reproductores de imagen

Los elementos de un circuito cerrado de T.V. que nos permiten reproducir las imágenes captadas por las cámaras son los monitores. Un monitor de T.V. en circuito cerrado es básicamente similar a un televisor doméstico, si bien carece de los circuitos de radiofrecuencia y dispone de selector de impedancia para la señal de entrada; también está diseñado para soportar un funcionamiento continuo.

Existen varios tamaños de la pantalla reproductora (tubo de rayos catódicos); habitualmente, en seguridad y para blanco y negro se emplean los de 9 ó 12 pulgadas (tamaño de la diagonal de la pantalla), pero pueden emplearse otros tamaños superiores para Salas de Control en que los monitores estén muy alejados del vigilante. Para color las pantallas más usuales son de 10 y 14 pulgadas. Como las imágenes formadas en los monitores están constituidas por las mismas líneas, es un error suponer que en un monitor mayor se verá mejor; el tamaño de pantalla debe elegirse solamente en función de la distancia desde la cual se verán las imágenes.

2.2.3 Elementos grabadores de imagen

La señal proveniente de una cámara de T.V. en circuito cerrado, que como hemos visto es la resultante de tres tipos diferentes de impulsos eléctricos, es susceptible de ser grabada, por medio de los dispositivos adecuados.

Los dispositivos grabadores de imágenes en movimiento, que utilizan cintas magnéticas, pueden ser de dos tipos:

a. Magnetoscopios, también llamados grabadores de bobina abierta, prácticamente han desaparecido del mercado del CCTV, quedando solamente versiones de alto precio para estudios profesionales.

a. Videocassettes o videograbadores, son los más empleados para vigilancia, sobre todo los que utilizan cassettes VHS con cinta magnética para 3 ó 4 horas (el doble a media velocidad) y proporcionan una resolución horizontal de 240 líneas (en color) ó 300 líneas (en blanco y negro), ampliable a 400 líneas en las versiones con S-VHS.

Otros dispositivos de grabación de imágenes, en este caso fijas, son:

- Los digitalizadores, que almacenan las imágenes digitalizadas en soportes informáticos.

- Las videoimpresoras, que las imprimen en papel como si fueran fotografías.

2.2.4 Elementos transmisores de la señal de video

La señal de vídeo que sale de la cámara debe llegar en las mejores condiciones posibles al monitor o monitores correspondientes, para lo cual se emplean:

- Líneas de transmisión
- Amplificadores de línea
- Distribuidores de vídeo

Las líneas de transmisión deben ser capaces de transportar la señal de vídeo, que puede alcanzar frecuencias de 8 MHz, con un mínimo de pérdidas, por lo que se utilizan habitualmente cables de tipo coaxial, adaptados a la impedancia nominal del circuito cerrado de T.V. (75 ohmios).

Los amplificadores de línea se utilizan para elevar y compensar las pérdidas, sobre todo en altas frecuencias, de la señal de vídeo, tanto para alimentar varios

monitores "en puente" (uno a continuación del otro), como para realizar transmisiones a mayor distancia de la que permitiría la longitud de los cables coaxiales.

Por último, si una misma señal de vídeo debe dirigirse a varios receptores (monitores o grabadores) y éstos se encuentran bastante alejados unos de otros, lo mejor es utilizar distribuidores electrónicos de vídeo, con los cuales podemos obtener varias señales iguales, manteniendo su máxima amplitud y sin las variaciones de impedancia que inevitablemente se producen si los conectamos en puente; además, los distribuidores pueden colocarse en el lugar más adecuado del edificio, lo que permite optimizar el cableado.

Si bien la transmisión por cable coaxial es la más usual, no es la única, pudiendo efectuarse también mediante:

- Cable de 2 hilos trenzados (señal simétrica).
- Cable de fibra óptica.
- Línea telefónica (vía lenta).
- Enlace por microondas.
- Enlace por infrarrojos.

Aunque debe tenerse en cuenta que para ello se precisan dispositivos tales como conversores, transductores, módems o conjuntos emisor/receptor, adecuados a cada caso.

Resulta evidente que con sólo los elementos captadores, transmisores y reproductores ya podemos formar un circuito cerrado de T.V., por ejemplo con una cámara, un cable y un monitor; sin embargo, en la mayoría de los casos la instalación no es tan simple, y son necesarios los elementos de control.

2.2.5 Elementos de control

Pueden ser de dos tipos:

a) Selectores de vídeo

Permiten seleccionar las imágenes provenientes de varias cámaras, tanto para dirigirlas a un monitor determinado como a un grabador de vídeo. Estos selectores suelen dotarse con dispositivos de conmutación automática, que reciben el nombre de secuenciales, aunque siempre debe ser factible la selección manual.

Vídeo Switchers

La función del Switcher en un sistema de seguridad de múltiples cámaras es conectar una especifica cámara a un especifico monitor (vídeo u otro dispositivo) y visualizar la imagen de vídeo en una secuencia lógica.

En pequeños sistemas de seguridad –varias cámaras y uno o dos monitores solamente- un Switcher puede no ser necesario si todas las cámaras pueden mostrar sus escenas en el monitor simultáneamente.

En medianos o grandes instalaciones, donde es necesario limitar el número de monitores en una consola de control, a one-to-one (una sola cámara con un solo monitor) no es práctica. El espacio físico puede ser limitado y el guardia de seguridad tal vez no pueda observar los múltiples monitores simultáneamente. Es recomendable para tales fines un monitor simple.

Ventajas de utilizar un monitor simple

1. Es más económico invertir en un solo monitor que en múltiples monitores.
2. Un monitor simple ocupa menos espacio que una consola de múltiples monitores.
3. Falta de atención al monitor o fatiga por parte del vigilante ocurre menos al usarse un monitor simple.
4. Requiere menos tiempo para realizarle el mantenimiento.

Desventajas de utilizar un monitor simple

1. Cuando se utiliza un solo monitor, es imposible observar todas las localidades que están siendo monitoreadas simultáneamente. Esta deficiencia es especialmente importante en situaciones que involucran un movimiento continuo, o en situaciones donde es importante observar las actividades que ocurren en diferentes localidades simultáneamente.
2. Cuando el Switcher cambia de cámara a cámara, un largo tiempo puede pasar antes de que el lugar que es monitoreado desde una cámara en particular pueda ser visto de nuevo. En el caso de 4 cámaras, el operador solo vera cada lugar ¼ del tiempo.
3. Si hay alguna falla en el monitor simple ninguna toma podrá ser mostrada hasta que sea reemplazado el mismo.

La función de switchear la información de vídeo desde cada cámara a los monitores puede ser dividida dentro de dos categorías básicas:

Single – Output Switching: switchear la señal de una o más cámaras a un cable de salida simple y este conectarlo a uno o más monitores.

Múltiple – Output Switching: switchear la señal de unas o mas cámaras a múltiples cables de salida y conectar estos a múltiples monitores. [3]

b) Telemandos de las cámaras motorizadas

Pueden ser:

- Telemando de un objetivo zoom motorizado, que permite gobernar a distancia el zoom, el foco y (si no es auto-iris) el diafragma.
- Telemando del posicionador, que permite cuatro movimientos: arriba, abajo, izquierda y derecha.
- Telemando de la carcasa intemperie, si ésta dispone de limpia cristal y bomba de agua.

Para instalaciones muy complejas, o en aquellas en que se desee una gran flexibilidad de explotación, son muy eficaces las matrices de conmutación de vídeo,

que permiten enviar la señal de cualquier cámara a cualquiera de sus salidas; son programables, admiten selección por señales de alarma y en muchos casos ya incorporan dispositivos para el telemando de las cámaras motorizadas; hay versiones que permiten su conexión a teclados remotos, con la que se facilita la implantación de puestos de control secundarios.

2.2.6 Video sensores

Una aplicación importante para vigilancia del circuito cerrado de T.V. consiste en incorporar al mismo los video sensores.

Se denominan video sensores o detectores de movimiento de vídeo a unos elementos que, analizando las variaciones en la señal de vídeo, permiten determinar si se ha producido algún movimiento en una parte determinada de la imagen.

Si bien existen versiones muy simples (solo válidas para interiores) que procesan la señal analógicamente, se están imponiendo los sistemas con procesado digital, que permiten una precisión mucho mayor en el análisis de la señal; de estos existen versiones para controlar interiores o exteriores de pequeño tamaño, y versiones de alto nivel, que analizan más de 1000 puntos de la imagen y pueden vigilar perímetros de grandes dimensiones, dentro del alcance visual de las cámaras.

Para obtener el máximo rendimiento es conveniente que las cámaras estén situadas en cascada, es decir, que cada cámara abarque el ángulo muerto de la anterior, y que la distancia entre ellas no exceda los 60 metros.

2.3 APLICACIONES DE LOS CIRCUITOS DE CCTV

- Hoy los sistemas de vigilancia por circuitos cerrados de tv dejaron de ser un sistema utilizado solo por grandes empresas, ya que debido a una reducción importante en los costos y a la concientización de la necesidad de su uso pasaron a ser elementos imprescindibles, no solo para seguridad si no también son muy

utilizados para control de personal o de zonas en las cuales las condiciones ambientales las constituyen en imprescindibles.

- CCTV ayuda a proteger vidas humanas debido a que mediante este sistema puede ser monitoreadas áreas distantes en lugares donde al momento de surgir algún accidente las personas involucradas en el mismo no puedan pedir ayuda. Permite darnos cuenta de: Que ha pasado, Cuando y donde está ocurriendo el problema, pudiendo de esta manera enviar el personal calificado para responder dicha emergencia con el equipo necesario para tal fin.

- CCTV reduce la posibilidad de que personas no autorizadas puedan accesar a informaciones confidenciales de la empresa o industria tales como parámetros de control de procesos, firmas de acuerdos importantes, entre otras.

- Permite observar áreas donde se manejan materiales o algunas maquinarias cuya acción puede causar daño físico e inclusive la muerte al personal que trabaja en dichas áreas (por ejemplo, lugares donde se manejan sustancias químicas, materiales radiactivos, sustancias con alto grado de inflamabilidad, entre otras).

- Significativos eventos pueden ser grabados cuando ocurren a medida que podamos integrar los sistemas CCTV con alarmas de sensores en un ciclo de tiempo real (un VCR puede servir para tal propósito).

- Muchas localidades pueden ser monitoreadas simultáneamente por una persona desde una posición central de seguridad. Esto puede permitir seguir la ruta de una persona o vehículo desde el momento en que ingresa a las instalaciones hasta su destinación central y así tener la posibilidad de interceptarlo por las fuerzas de seguridad. Además, el uso de sistemas CCTV elimina la necesidad de que guardias tengan que hacer rondas a localidades remotas.

2.4. CONCEPTOS BÁSICOS DE UN SISTEMA DE CONTROL DE ACCESOS

El control de acceso es vital tanto para la seguridad como para el control del personal. Existen productos, desde un simple abrepuerta, una barrera vehicular, hasta sistemas alta gama de hardware y software. Frente a posibles intrusiones, este sistema garantiza el control de cada uno de los accesos y proporciona información específica para mejorar la gestión empresarial.

2.4.1 CARACTERÍSTICAS DEL SISTEMA

- Con este sistema se tendrá la posibilidad de conceder o negar el acceso a determinadas áreas de una empresa.
- Administrar el flujo de cada uno de los movimientos en su empresa sin ninguna excepción.
- Crear su propia política de admisión.
- Llevar una base de datos con especificaciones horarias del movimiento del personal.
- Programar horarios. El empleado tendrá permitidas la entrada y la salida sólo durante su jornada laboral.
- Programar categorías, por las que los empleados tendrán libre acceso a algunas áreas.
- Mediante cronogramas preestablecidos, autorizar o denegar los accesos a determinadas áreas sensibles de su empresa.
- Generar restricciones totales en alguna banda horaria, en lugares de alta confidencialidad.
- Control de visitas, donde quedará registrada la estadía en la empresa. Supervisar la entrada y salida de vehículos.

2.4.2 OPCIONES PARA VERIFICACIÓN DE IDENTIDAD

- Tarjetas con código de barra.

- Tarjetas con banda magnética.
- Tarjetas de proximidad.
- Paneles de acceso con clave.
- Lectores biométricos.

Figura 2.8 Control de acceso dactilar y con banda magnética

2.4.3 SOFTWARE DE GESTIÓN

- Permite el manejo de distintos grupos de personas, empleados, personal externo, personal de mantenimiento, personal de seguridad, etc.
- Selecciona la categoría de la persona y posibilita capturar una fotografía en línea o de archivo.
- Se pueden registrar todas las huellas de la persona. Permite generar niveles de acceso parametrizables sin límite de niveles con la opción de usuarios administradores identificados por clave, por huella, o combinados.
- A la vez, admite generar reportes por personas, categorías, accesos y usuarios del sistema.

2.4.4 MÉTODOS DE AUTENTICACIÓN

Los métodos de autenticación están en función de lo que utilizan para la verificación y estos se dividen en tres categorías: [5]

- Sistemas basados en algo conocido. Ejemplo, un *password* (Unix) o *passphrase* (PGP).

- Sistemas basados en algo poseído. Ejemplo, una tarjeta de identidad, una tarjeta inteligente(*smartcard*), dispositivo usb tipo epass token, smartcard o dongle criptográfico.
- Sistemas basados en una característica física del usuario o un acto involuntario del mismo: Ejemplo, verificación de voz, de escritura, de huellas, de patrones oculares.

Cualquier sistema de identificación ha de poseer unas determinadas características para ser viable:

- Ha de ser fiable con una probabilidad muy elevada (podemos hablar de tasas de fallo de en los sistemas menos seguros).
- Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto).
- Soportar con éxito cierto tipo de ataques.
- Ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen.

2.4.5 MECANISMO GENERAL DE AUTENTICACIÓN

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización y/o auditoría oportunos.

El primer elemento necesario (y suficiente estrictamente hablando) por tanto para la autenticación es la existencia de identidades biunívocamente identificadas con un identificador único (valga la redundancia). Los identificadores de usuarios

pueden tener muchas formas siendo la más común una sucesión de caracteres conocida comúnmente como login.

El proceso general de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valida según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

2.4.6 SISTEMA DE CONTROL DE ACCESOS

Normalmente el acceso al edificio o instalaciones está restringido a personas y medios propios del lugar o vinculados al mismo. El diseño de un sistema de control de acceso es complicado pues los empleados y visitantes se sienten con el *legítimo derecho* de entrar o acceder a TODAS las áreas, en especial en las horas de trabajo o producción. El control de acceso en esas horas (las de trabajo o producción) es complicado además por la gran diversidad de visitantes, transportistas, empresas de suministros y empleados que están inter-actuando y que hay que controlar. [10]

El plan de seguridad debe contemplar *zonas de seguridad*. Estas zonas deben representar los diferentes niveles y variaciones de restricción y control de acceso, desde las zonas de acceso no restringido hasta las zonas de acceso prohibido. (Cuidando que durante la gestión del sistema los considerandos del diseño se respeten.) La precisión y determinación del *nivel de control* requerido es labor conjunta con el equipo de diseño y los futuros/actuales usuarios y gestores del edificio e instalaciones.

Las zonas deben agruparse por el *nivel de control exigido o exigible* mediante la creación de secciones o subsecciones dentro del edificio o instalaciones

o bien separando físicamente, de ser posible, las sección o áreas en función de su nivel de control exigible. Por ejemplo, es común colocar aquellas dependencias o áreas NO RESTRINGIDAS o de libre acceso - que no demanda control de acceso o requieren un mínimo de control - y de gran volumen de visitantes lo más cerca de la entrada o lobby del edificio. El acceso a estas áreas no puede implicar el paso por zonas de mayor nivel o exigencia de seguridad.

Diseñando en base a *zonas* se aumenta la efectividad y reduce los costes de los sistemas de control de acceso y de detección. Las áreas de producción deben estar debidamente sectorizadas pues los obreros/empleados deben ser sometidos a pocas interrupciones y distracciones durante sus movimientos en el trabajo.

LECTOR BIOMÉTRICO.-

El sistema de acceso implementado costa de un sensor biométrico de huella dactilar el cual se encarga de digitalizar la imagen de la huella para su posterior análisis.

El análisis se realiza sabiéndose que la huella está formada por una serie de crestas y surcos localizados en la superficie del dedo. La singularidad de una huella puede ser determinada por dos tipos de patrones: el patrón de crestas y surcos, así como los detalles.

Se puede distinguir entre otras cosas lo siguiente en una huella:

- Dibujos papilares: son los formados por las crestas papilares y los surcos inter papilares.
- Crestas papilares: son los relieves epidérmicos situados en la palma de las manos y en la planta de los pies.
- Surcos inter papilares: son lo que se determinan por las depresiones que separan dichos relieves o crestas.

- Dermis: es la capa interior y más gruesa de la piel, que contiene el dibujo papilar.
- Epidermis: es la membrana que cubre la dermis.
- Poros papilares: Son los diminutos orificios de forma y dimensiones variadas que en crecido número existen en las crestas papilares y por los cuales se expulsa el sudor.

Para el reconocimiento de una huella se tienen en cuenta también las siguientes propiedades: Los dibujos visibles de la epidermis son perennes, inmutables y diversiformes. Esto hace referencia a que las huellas se forman en el sexto mes de vida, son únicas y son inmutables.

Existen dos técnicas para realizar la verificación de las huellas:

- Basada en Detalles: Esta técnica elabora un mapa con la ubicación relativa de "detalles" sobre la huella, los cuales permiten ubicar con certeza a un individuo. Sin embargo, existen algunas dificultades cuando se utiliza está aproximación. Es muy difícil ubicar los detalles con precisión cuando la huella suministrada es de baja calidad. También este método no toma en cuenta el patrón global de las crestas y los surcos.

  Algunos detalles que podemos encontrar en una huella, se pueden visualizar en la figura. Cada individuo posee uno y solo uno, arreglo de detalles.

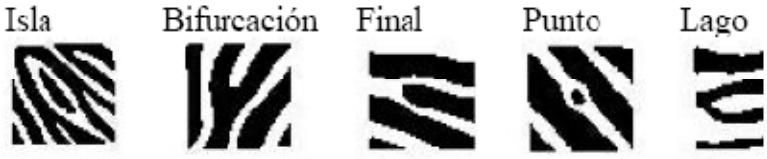

Figura 2.9 Detalles de las huellas

- Basadas en correlación: Este método toma un punto como referencia para iniciar la comparación, pero es limitado en cuanto a que cualquier rotación o traslación de la imagen puede influir ostensiblemente en el análisis. Una vez obtenida la huella digital es necesario clasificarla. Este proceso consiste en ubicar dicha huella dentro de los varios tipos existentes, los cuales proveen un mecanismo de indexado; esto con la finalidad de reducir el tiempo de búsqueda.

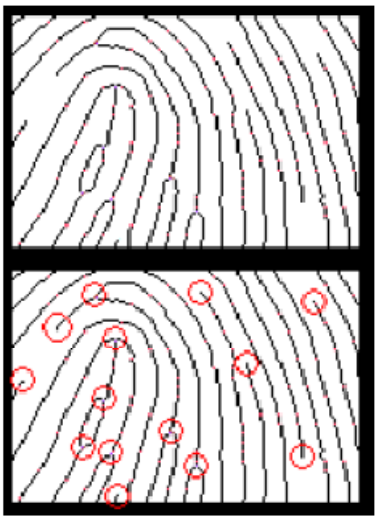

Figura 2.10 Trazado del patrón de detalles.

Los algoritmos existentes permiten clasificar la huella en cinco clases:

- Anillo de Crestas.
- Lazo Derecho.
- Lazo Izquierdo.
- Arco.
- Arco de Carpa.

Por último, un DAC (Digital-Analog Converter) convierte los datos analógicos en valores digitales.

Estos datos son enviados al computador y son procesados usando correlación con una base de datos que contiene huellas guardadas con anterioridad.

Con el proceso de correlación se determina si el usuario esta registrado en la base de datos para permitir o no el acceso, el cual en definitiva es energizar una cantonera en una puerta. [11]

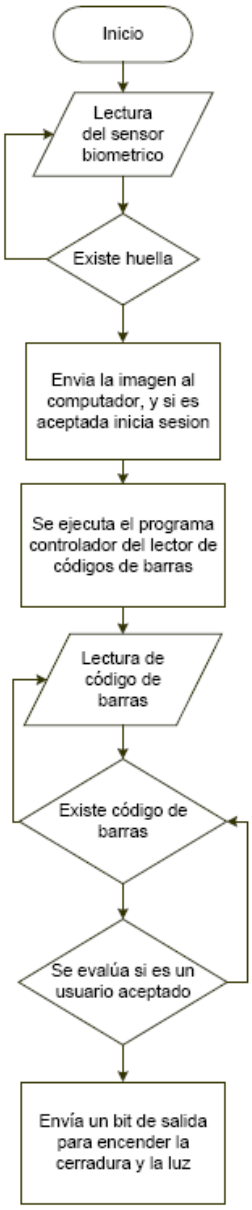

Figura 2.11 Esquema general del control de acceso.

LECTOR TARJETAS SIN CONTACTO.-

Cada vez es más frecuente ver tarjetas identificadoras sin contacto con el sistema de lectura. Este tipo de sistemas se llaman abreviadamente RFID (Radio Frequency Identification) Identificación por radiofrecuencia. Estos dispositivos

están sustituyendo poco a poco a las etiquetas de códigos de barras y a las tarjetas magnéticas en todas sus aplicaciones.

Aplicaciones actuales

Las aplicaciones más corrientes de estos sistemas son el control de accesos y la inmovilización de vehículos. En el control de accesos se gana en comodidad, no es necesario el contacto físico de la tarjeta con el lector, lo que lo hace más cómodo y más rápido de usar. Este es un sistema en el que el interrogador (el dispositivo que lee los datos) tiene que poder leer muchas tarjetas diferentes, tantas como usuarios haya autorizados.

Una aplicación muy frecuente y poco conocida del sistema RFID son los inmovilizadores de vehículos. Se basan en un sistema interrogador situado en el vehículo a proteger y en un identificador en la llave. El primer sistema de este tipo se empezó a usar en 1994 y era el sistema U2270B de Atmel. En este tipo de sistema un interrogador sólo da paso a una sola llave.

Funcionamiento

Todo sistema RFID se compone de un interrogador o sistema de base que lee y escribe datos en los dispositivos y un *"transponder"* o transmisor que responde al interrogador.

1. El interrogador genera un campo de radiofrecuencia, normalmente conmutando una bobina a alta frecuencia. Las frecuencias usuales van desde 125 Khz hasta la banda ISM de 2.4 Ghz, incluso más.
2. El campo de radiofrecuencia genera una corriente eléctrica sobre la bobina de recepción del dispositivo. Esta señal es rectificada y de esta manera se alimenta el circuito.
3. Cuando la alimentación llega a ser suficiente el circuito transmite sus datos.
4. El interrogador detecta los datos transmitidos por la tarjeta como una perturbación del propio nivel de la señal.

La señal recibida por el interrogador desde la tarjeta está a un nivel de -60 db por debajo de la portadora de transmisión. El rango de lectura para la mayoría de los casos está entre los 30 y 60 centímetros de distancia entre interrogador y tarjeta.

Podemos encontrar además dos tipos de interrogadores diferentes:

- Sistemas con bobina simple, la misma bobina sirve para transmitir la energía y los datos. Son más simples y más baratos, pero tienen menos alcance.
- Sistemas interrogadores con dos bobinas, una para transmitir energía y otra para transmitir datos. Son más caros, pero consiguen unas prestaciones mayores.

Protocolos y opciones

Normalmente el sistema de modulación usado es modulación de amplitud (AM) con codificación tipo Manchester NRZ.

Para conseguir mayor alcance y más inmunidad al ruido eléctrico se utilizan sistemas más sofisticados. En algunos casos se divide la frecuencia del reloj de recepción.

La mayor parte de los sistemas tienen una memoria EEPROM donde se almacenan datos. En algunos casos llevan datos grabados de fábrica y en otros también hay datos que puede grabar el usuario.

Algunos sistemas utilizan encriptación de clave pública para conseguir mayor seguridad ante posibles escuchas maliciosas.

Por otro lado podemos encontrar sistemas anticolisión que permiten leer varias tarjetas al mismo tiempo. En caso de que varias tarjetas estén en el rango de alcance del interrogador y dos o más quieran transmitir al mismo tiempo, se produce una colisión. El interrogador detecta la colisión y manda parar la transmisión de las tarjetas durante un tiempo. Después irán respondiendo cada una por separado por medio de un algoritmo bastante complejo.

2.5. CONCEPTOS DE REDES

Para realizar el diseño del CCTV y del control de acceso en una instalación se debe tomar en cuenta ciertas definiciones [6] y características que deben ser tomadas en cuenta para poder realizar comparaciones objetivas:

- Topología de la red.
- Tipos de arquitectura.
- Medios de transmisión.
- Velocidad de comunicaciones.
- Protocolo de comunicaciones.

2.5.1 Topología de la Red

La topología o forma lógica de la red se define como la distribución física de las estaciones de trabajo respecto al medio de comunicación (cable), estos pueden ser clasificados en bus, anillo, topología libre. Siendo las más utilizadas en edificios inteligentes las que se cita a continuación.

Bus

Esta topología permite que todas las estaciones reciban la información que se transmite, una estación transmite y todas las restantes escuchan. Esta característica puede ser ventajosa si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes. Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos de una red.

Anillo

Las estaciones están unidas unas con otras formando un círculo por medio de un cable común. El último nodo de la cadena se conecta al primero cerrando el

anillo. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. La desventaja del anillo es que si se rompe una conexión, se cae la red completa.

2.5.2 Tipos de Arquitectura

La arquitectura de un sistema inteligente, como la de cualquier sistema de control, especifica el modo en que los diferentes elementos de control del sistema se van a ubicar. Existen dos arquitecturas básicas: la arquitectura centralizada y la distribuida.

Arquitectura centralizada

Es aquella en la que los elementos a controlar y supervisar (sensores, luces, válvulas, etc.) han de cablearse hasta el sistema de control del edificio (PC o similar).

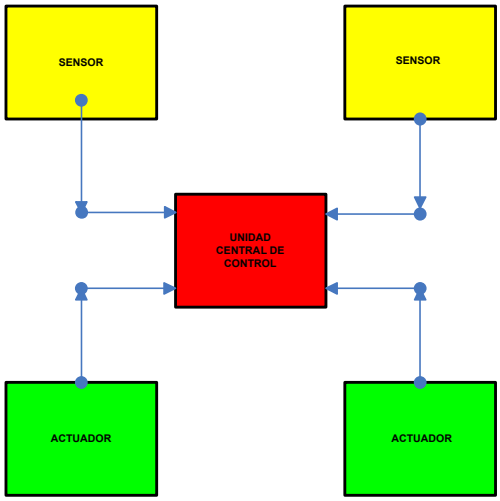

Figura 2.12 Arquitectura centralizada

Arquitectura distribuida

Es aquella en la que el elemento de control se sitúa próximo al elemento a controlar.

Este tipo de arquitectura es más abierta a cambios una vez realizada la instalación ya que su funcionamiento se basa en el concepto de elemento a controlar-controlador.

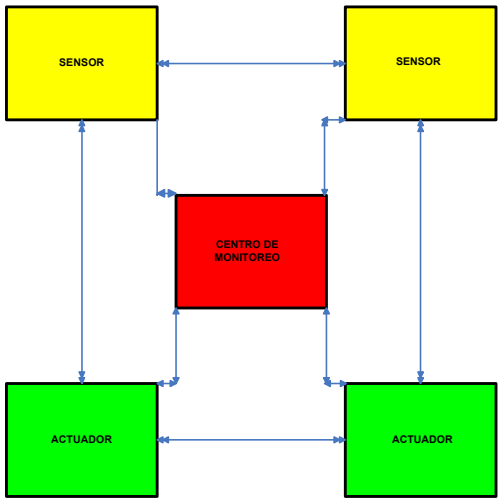

Figura 2.13 Arquitectura distribuida

Hay sistemas que son de arquitectura distribuida en cuanto a la capacidad de proceso, pero no lo son en cuanto a la ubicación física de los diferentes elementos de control y viceversa, sistemas que son de arquitectura distribuida en cuanto a su capacidad para ubicar elementos de control físicamente distribuidos, pero no en cuanto a los procesos de control, que son ejecutados en uno o varios procesadores físicamente centralizados.

2.5.3 Medios de Transmisión

Los medios de transmisión son el canal para que el transmisor y el receptor puedan comunicarse y puedan transferirse información. Es necesario saber que

existen varios factores externos que inciden sobre el canal que producen ruido e interferencia, por lo que es necesaria una buena relación señal a ruido para superar estos obstáculos. La selección adecuada del mejor servicio y medio de transmisión para cubrir las necesidades es de vital importancia para operar óptimamente. A continuación enumeramos los siguientes tipos de medios de transmisión:

Medios alámbricos

Líneas de distribución de energía eléctrica

Es una alternativa a tener en cuenta para las comunicaciones domésticas dado el bajo costo que implica su uso, ya que se trata de una instalación existente. Para aquellos casos en los que las necesidades del sistema no impongan requerimientos muy exigentes en cuanto a la velocidad de transmisión, la línea de distribución de energía eléctrica puede ser suficiente como soporte de dicha transmisión. Algunas características de este medio son:

- Bajo costo de la instalación
- Facilidad de conexión
- Poca fiabilidad en la transmisión de los datos
- Baja velocidad de transmisión

Par metálico

Los cables formados por varios conductores de cobre pueden dar soporte a un amplio rango de aplicaciones. Este tipo de cables pueden transportar voz, datos y alimentación de corriente continua.

Los denominados cables de pares están formados por cualquier combinación de los tipos de conductores que a continuación se detallan:

a. *Cables formados por un solo conductor***,** con un aislamiento exterior plástico, como los utilizados para la transmisión de las señales telefónicas.

b. *Par de cables,* cada uno de los cables está formado por un arrollamiento helicoidal de varios hilos de cobre. (Por ejemplo, los utilizados para la distribución de señales de audio.).

c. *Par apantallado*, formado por dos hilos recubiertos por un trenzado conductor en forma de malla cuya misión consiste en aislar las señales que circulan por los cables de las interferencias electromagnéticas exteriores. (Por ejemplo, los utilizados para la distribución de sonido alta fidelidad o datos).

d. *Par trenzado*, está formado por dos hilos de cobre recubiertos cada uno por un trenzado en forma de malla. El trenzado es un medio para hacer frente a las interferencias electromagnéticas. (Por ejemplo, los utilizados para interconexión de ordenadores).

Como medio de comunicación tiene la desventaja de tener que usarse a distancias limitadas (menos de 100 metros) ya que la señal se va atenuando y puede llegar a ser imperceptible si se rebasa ese límite.

Los cables de par trenzado más comúnmente usados como interfaces de capa física son los siguientes: 10BaseT (Ethernet), 100BaseTX (Fast Ethernet), 100BaseT4 (Fast Ethernet con 4 pares) y 1000BaseT (Gigabit Ethernet).

Existen dos tipos de cable par trenzado, el UTP (Unshielded Twisted Pair Cabling), o cable par trenzado sin blindaje y el cable STP (Shielded Twisted Pair Cabling), o cable par trenzado blindado. A continuación se muestran las diferentes categorías de cables UTP y su aplicación:

- Categoría 1: Voz solamente (cable telefónico)
- Categoría 2: Datos hasta 4 Mbps (LocalTalk [Apple])
- Categoría 3: Datos hasta 10 Mbps (Ethernet)
- Categoría 4: Datos hasta 20 Mbps (16 Mbps Token Ring)
- Categoría 5: Datos hasta 100 Mbps (Fast Ethernet)
- Categoría 5e: Datos hasta 1000 Mbps (Gigabit Etherne

Coaxial

Este tipo de cable consiste de un conductor central fijo (axial) sobre un forro de material aislante, que después lleva una cubierta metálica en forma de malla como segundo conductor. La capa exterior evita que las señales de otros cables o que la radiación electromagnética afecte la información conducida por el cable coaxial.

El cable coaxial puede transmitir información tanto en frecuencia intermedia (IF) como en banda base. En IF el cable coaxial se utiliza en aplicaciones de video. En banda base el coaxial se utilizó bastante en aplicaciones de datos en redes de área local (LAN) tanto en redes Token Ring como Ethernet a media y baja velocidad.

Fibra óptica

La fibra óptica es un medio de comunicación que utiliza la luz confinada en una fibra de vidrio para transmitir grandes cantidades de información en el orden de Gigabits (1x109 bits) por segundo. Para transmitir los haces de luz se utiliza una fuente de luz como un LED (Light-Emitting Diode) o un diodo láser. En la parte receptora se utiliza un fotodiodo o fototransistor para detectar la luz emitida. También será necesario poner al final de cada extremo un conversor de luz (óptico) a señales eléctricas.

Debido a que el láser trabaja a frecuencias muy altas, entre el intervalo de la luz visible e infrarroja, la fibra óptica es casi inmune a la interferencia y el ruido.

A continuación se detallan sus ventajas e inconvenientes:

- Fiabilidad en la transferencia de datos.
- Inmunidad frente a interferencias electromagnéticas y de radiofrecuencias.
- Alta seguridad en la transmisión de datos.
- Distancia entre los puntos de la instalación limitada, en el entorno doméstico estos problemas no existen.

- Elevado coste de los cables y las conexiones.
- Transferencia de gran cantidad de datos:

Medios inalámbricos

Infrarrojos

La comunicación se realiza entre un diodo emisor que emite una luz en la banda de IR, sobre la que se superpone una señal, convenientemente modulada con la información de control, y un fotodiodo receptor cuya misión consiste en extraer de la señal recibida la información de control. A continuación se detallan sus ventajas e inconvenientes:

- Presentan gran comodidad y flexibilidad y admiten un gran número de aplicaciones.
- Es inmune a las radiaciones electromagnéticas producidas por los equipos domésticos o por los demás medios de transmisión (coaxial, cables pares, red de distribución de energía eléctrica, etc.).
- Debe tomar precauciones en el caso de las interferencias electromagnéticas que pueden afectar a los extremos del medio.

Radiofrecuencia

A todo el rango de frecuencias se le conoce como espectro electromagnético. El uso de este espectro, define la comunicación por radiofrecuencia. Cada subconjunto o banda de frecuencias dentro del espectro electromagnético tiene propiedades únicas que son el resultado de cambios en la longitud de onda. Las ventajas e inconvenientes de los sistemas basados en transmisión por radiofrecuencias, son:

- Alta sensibilidad a las interferencias.
- Fácil interceptación de las comunicaciones.

- Dificultad para la integración de las funciones de control y comunicación, en su modalidad de transmisión analógica.

2.5.4 Velocidad de transmisión

Los diferentes elementos de control deben intercambiar información unos con otros a través de un medio alámbrico o inalámbrico (par trenzado, radio, infrarrojos, etc.). La velocidad a la cual se intercambian información los diferentes elementos de control de la red se denomina velocidad de transmisión.

2.5.5 Protocolos de Comunicaciones

El protocolo de comunicaciones no es otra cosa que el "idioma" o formato de los mensajes que los diferentes elementos de control del sistema deben utilizar para entenderse unos con otros y que puedan intercambiar su información de una manera coherente.

Dentro de los protocolos existentes, se puede realizar una clasificación atendiendo a su estandarización.

Protocolos estándar

Los protocolos estándar permiten la comunicación entre productos de diferentes marcas y compatibles entre sí, permitiendo que sean utilizados ampliamente por las empresas en todo el mundo. Entre los principales estándares tenemos, el X-10, el EHS, el EIB, Bacnet, etc.

Protocolos propietarios

Son desarrollados por una empresa en particular y solo los productos fabricados por ella son capaces de comunicarse entre sí.

2.6 HARDWARE DE REDES

Entre los principales componentes de una red podemos nombrar: [7]

2.6.1 BRIGDE O PUENTE

Unidad Funcional que interconecta dos redes de área local que utiliza el mismo protocolo de control de enlace lógico pero distintos protocolos de control de acceso al medio. Operan en el nivel 2 de OSI (Capa de Enlace de Datos). Estos equipos unen dos redes actuando sobre los protocolos de bajo nivel. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

2.6.2 ROUTER o ENCAMINADOR

Es un dispositivo que conecta dos redes locales y es el responsable de controlar el tráfico entre ellas y de clasificarlo. En sistemas complejos suele ser un filtro de seguridad para prevenir daños en la red local. Es posible conectar varias redes locales de forma que los ordenadores o nodos de cada una de ellas tengan acceso a todos los demás.

Estos dispositivos operan en el tercer nivel de red (Capa de Red) del modelo OSI, y enlazan los tres primeros niveles de este modelo. Los routers redirigen paquetes de acuerdo al método entregado por los niveles más altos.

Actualmente, son capaces de manejar un protocolo o varios protocolos a la vez.

Son también llamados sistemas intermediarios. Originalmente, fueron usados para interconectar múltiples redes corriendo el mismo protocolo de alto

nivel (por ejemplo; TCP/IP) con múltiples caminos de transmisión origen/destino. Entre los más usados en la actualidad se encuentran los de la empresa CISCO.

Consideraciones de ruteo

Ruteo Estático: Ocurre cuando uno requiere predefinir todas las rutas a las redes destinos.

Ruteo Dinámico: Ocurre cuando la información de ruteo es intercambiada periódicamente entre los routers. Permite rutear información basada en el conocimiento actual de la topología de la red.

Sobrecarga: Al intercambiar la información de ruteo entre router y actualizar las tablas de rutas internas, requiere una cierta cantidad de recursos adicionales. Estos recursos no son directamente involucrados en mover directamente información útil del usuario, esto pasa a ser un requerimiento adicional y son por lo tanto considerados como sobrecargas. Esta puede influir sobre tráfico de red, memoria y CPU.

Ventajas y desventajas del uso de routers:

- Los routers son configurables. Esto permite al administrador tomar decisiones de ruteo (rutas estáticas en caso de fallas), así como hacer sincronización del desempeño de la inter red.
- Son relativamente fáciles de mantener una vez configurados, ya que muchos protocolos pueden actualizar sus tablas de ruta de una manera dinámica.
- Los routers proveen características entre intereses, esto previene incidentes que pudieran ocurrir en una sub red, afectando a otras sub redes. Así como también previene la presencia de intrusos.
- Los routers no son afectados por los contrastes de los tiempos de retardos como ocurre en los bridges. Esto significa que los routers no están limitados topológicamente.

- Los routers son inteligentes y pueden seleccionar el camino más aconsejable entre dos o más conexiones simultáneas. Esto además permite hacer balances de la carga lo cual alivia las congestiones.
- Dentro de las desventajas se pueden mencionar que requieren una cantidad significativa de tiempo para instalarlos y configurarlos dependiendo de la topología de la red y de los protocolos usados. Los routers son dependientes del protocolo, cada protocolo a rutear debe ser conocido por el router.
- Tienen un mayor costo que los Bridges y son más complejos.

2.6.3 BROUTER

Este es un dispositivo que realiza las funciones de un brigde y un router a la vez.

2.6.4 GATEWAY

Es un equipo para interconectar redes con protocolos y arquitecturas completamente diferentes, a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos. En realidad es una puerta de acceso, teniendo lugar una conversión completa de protocolos hasta la capa 7 (Capa de Aplicación) del modelo de referencia OSI.

2.6.5 HUB O CONCENTRADOR

En un equipo integrador para diversos tipos de cables y de arquitectura que permite estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc. La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos. Generalmente te indican la actividad de la red, velocidad y puertos involucrados. Su funcionamiento es simple,

se lleva hasta él un cable con la señal a transmitir y desde el se ramifican mas señales hacia otros nodos o puertos. Entre los fabricantes que producen gran variedad de estos equipos se encuentran las empresas 3COM y Cisco.

2.6.6 REPETIDOR

Es un equipo que actúa a nivel físico. Prolonga la longitud de la red uniendo dos segmentos, amplificando, regenerando y sincronizando la señal. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio. Una desventaja de estos equipos es que también amplifican el ruido que pueda venir con la señal.

2.6.7 MODEM

Es un dispositivo que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas, esta comunicación se realiza a través de la modulación y demodulación de señales electrónicas que pueden ser procesadas por computadoras, las señales analógicas se convierten en digitales y viceversa. Los módems pueden ser externos o internos dependiendo de su ubicación física en la red. Entre los mayores fabricantes tenemos a 3COM, AT&T, Motorola, US Robotics y NEC.

La transmisión por modem se divide en tres tipos:

SIMPLEX: Permite enviar información solo en un sentido.

HALF DUPLEX: Permite enviar información en ambos sentidos pero no a la misma vez.

FULL DUPLEX: Permite enviar información en ambos sentidos simultáneamente.

NIC / MAU: Son tarjetas de interface de red (Network Interface Card o NIC) o también se le denominan unidades de acceso al medio (Medium Access Unit o MAC). Cada computadora necesita el "hardware" para transmitir y recibir información. Es el dispositivo que conecta la computadora u otro equipo de red con el medio físico. La NIC es un tipo de tarjeta de expansión de la computadora y proporciona un puerto en la parte trasera de ella al cual se conecta el cable de la red. Hoy en día cada vez son más los equipos que disponen de interfaz de red, principalmente Ethernet, incorporadas. A veces, es necesario, además de la tarjeta de red, un TRANSCEPTOR. Este es un dispositivo que se conecta al medio físico y a la tarjeta, bien porque no sea posible la conexión directa (10base 5) o porque el medio sea distinto del que utiliza la tarjeta. También se le denomina MAC al protocolo empleado para la propagación de las señales eléctricas. Define el subnivel inferior de la capa 2 del modelo OSI (Capa de Enlace).

2.6.8 SERVIDORES

Son equipos que permiten la conexión a la red de equipos periféricos tanto para la entrada como para la salida de datos. Estos dispositivos se ofrecen en la red como recursos compartidos. Así un terminal conectado a uno de estos dispositivos puede establecer sesiones contra varios ordenadores multiusuarios disponibles en la red. La administración de la red se realiza a través de estos equipos tanto para archivos, impresión y aplicaciones entre otros. Entre las empresas pioneras en la fabricación de potentes servidores tenemos a la IBM, Hewlett Packard y Compaq.

2.6.9 MULTIPLEXOR (MPX)

Es también conocido como Concentrador (de líneas). Es un dispositivo que acepta varias líneas de datos a la entrada y las convierte en una sola línea corriente de datos compuesta y de alta velocidad. Esto hace la función de transmitir "simultáneamente" sobre un mismo medio varias señales.

2.6.10 MULTIPLEXOR (MUX)

Es un equipo cuya función es la de seleccionar entre varias entradas una de ellas a la salida. Generalmente el Multiplexor esta unido a otros equipos como un modem o también un switch. Los multiplexores son circuitos realmente importantes en el diseño de sistemas que requieran un cierto tráfico y comunicación entre distintos componentes y se necesite controlar en todo momento que componente es quien envía los datos. En realidad se puede asimilar a un selector, ya que por medio de unas entradas de control se selecciona la entrada que se desee reflejada en la salida.

Esto se consigue utilizando principalmente puertas XOR, de ahi su nombre multiple_xor. Entre algunos fabricantes de multiplexores tenemos a General DataComm, Rad, Pan Datel, Ascom, Timeplex y Siliconix.

En el mercado se encuentran todo tipo de modelos con diversidad de anchos de entradas (por ejemplo MUXs de 2 entradas de buses de 8 bits y 1 salida de 8 bits, con lo que se estaría conmutando entre 2 buses de 2 dispositivos de 8 bits). Además de lo anterior, suele ser un hábito que exista también una entrada de Enable (habilitación general de integrado). Existen varios tipos de multiplexores:

Multiplexor de división de tiempo: Multiplexor que asigna determinado tiempo a una entrada para enviar el tráfico hasta la salida. Siempre se asignara ese lapso de tiempo aunque no exista tráfico. La multiplexación bajo este modelo se le conoce como TDM (Time Division Multiplexing).

Multiplexor estadístico: Multiplexor de división de tiempo, que asigna en forma "estadística", la rebanada de tiempo al siguiente dispositivo conectado, es decir, el determina cual de las entradas se requiere en la salida y se basa en al tráfico generado por dichas entradas. Si una entrada no genera tráfico le da la oportunidad a otra que si lo genere. La multiplexación bajo este modelo se le conoce como SDM (Statistical Division Multiplexing).

Multiplexor de frecuencias: Multiplexor que permite que varias entradas simultáneas puedan transmitir datos a una única salida pero en diferentes frecuencias. Se define un ancho de banda para tal fin, el cual se reparte entre las entradas existentes en un mismo lapso de tiempo. La multiplexación bajo este modelo se le conoce como FDM (Statistical Division Multiplexing).

2.6.11 SWITCH O CONMUTADOR

Es un dispositivo de switcheo modular que proporciona conmutados de alta densidad para interfaces Ethernet y Fast Ethernet Proporciona la posibilidad de trabajar en redes LAN virtuales y la posibilidad de incorporar conmutación múltiple con el Sistema Operativo de Cisco Internetwork. El diseño modular permite dedicar conexiones Ethernet de 10Mbps y conexiones Fast Ethernet de 100Mbps a segmentos LAN, estaciones de alto rendimiento y servidores, usando par trenzado sin apantallamiento, par trenzado apantallado y fibra óptica. Permiten una amplia velocidad de conmutación entre Ethernet y Fast Ethernet a través de una amplia gama de interfaces que incluyen Fast Ethernet, Interfaces de Distribución de Datos por Fibra (FDDI) y ATM.

Los conmutadores ocupan el mismo lugar en la red que los concentradores. A diferencia de los concentradores, los conmutadores examinan cada paquete y lo procesan en consecuencia en lugar de simplemente repetir la señal a todos los puertos. Los conmutadores trazan las direcciones Ethernet de los nodos que residen en cada segmento de la red y permiten sólo el tráfico necesario para atravesar el conmutador. Cuando un paquete es recibido por el conmutador, el conmutador examina las direcciones hardware (MAC) fuente y destino y las compara con una tabla de segmentos de la red y direcciones. Si los segmentos son iguales, el paquete se descarta ("se filtra"); si los segmentos son diferentes, entonces el paquete es "remitido" al segmento apropiado. Además, los conmutadores previenen la difusión de paquetes erróneos al no remitirlos.

Los factores que afectan la eficacia de una red son: la cantidad de tráfico, número de nodos, tamaño de los paquetes y el diámetro de la red, por lo que usar conmutadores presenta muchas ventajas, ya que aíslan el tráfico y aíslan la

congestión, separan dominios de colisión reduciéndolas, segmentan, reiniciando las normas de distancia y repetidores.

La congestión en una red conmutada, normalmente puede ser aliviada agregando más puertos conmutados, y aumentando la velocidad de estos puertos.

Los segmentos que experimentan congestión son identificados por su utilización y la tasa de colisión, y la solución es una nueva segmentación o conexiones más rápidas. Tanto los puertos conmutados Fast Ethernet, como los Ethernet pueden ser añadidos por debajo de la estructura del árbol de la red para aumentar las prestaciones.

2.7 PROTOCOLOS DE TRANSMISIÓN DE DATOS, VOZ Y VIDEO

Hasta hoy en día ha habido una división clara entre dos tipos de redes:

-**Redes de voz**, basadas en conmutación de circuitos, por lo que se ocupa un circuito y el enrutamiento durante una comunicación se realiza siempre por el mismo camino. Ej: Red Telefónica convencional

-**Redes de datos**, basadas en conmutación de paquetes, la información se discretiza en paquetes y cada paquete puede viajar por caminos diferentes.Ej: Internet.

Para poder mandar la información por las redes de datos tipo Internet basadas en conmutación de paquetes es necesario adoptar unos **protocolos** que permitan transmitir y recuperar la información.

El problema con la tecnología de conmutación de circuitos es que requiere una significativa cantidad de ancho de banda o bandwidth para cada llamada y el circuito no es empleado eficientemente ya que emplea un canal durante toda la duración de la llamada pero la mayoría de las conversaciones telefónicas están hechas de silencio

Las redes de datos, por el contrario, sólo transmiten información cuando es

necesario, aprovechando al máximo el ancho de banda y en la cual el retardo, la alteración del orden de llegada o la pérdida de paquetes no son un inconveniente, ya que en el sistema final se tiene una serie de procedimientos de recuperación de la información original; pero **para la voz y el video estos factores son altamente influyentes**, por lo tanto se requieren redes y protocolos que ofrezcan un alto grado de QoS (calidad de servicio).

2.7.1 VOZ SOBRE IP (VoIP)

Define los sistemas de enrutamiento y los protocolos necesarios para la transmisión de conversaciones de voz a través de Internet, la cual es una red de conmutación de paquetes basado en el protocolo TCP/IP para el envío de información. [8]

Actualmente existen, principalmente, dos arquitecturas de VoIP para la transmisión de voz por Internet que se utilizan de forma abundante:

SIP (Session Initiation Protocol)

SIP son las siglas en inglés del Protocolo para Inicio de Sesión, siendo un estándar desarrollado por el IETF, identificado como RFC 3261, 2002. SIP es un protocolo de señalización para establecer las llamadas y conferencias en redes IP. El inicio de la sesión, cambio o término de la misma, son independientes del tipo de medio o aplicación que se estará usando en la llamada; una sesión puede incluir varios tipos de datos, incluyendo audio, video y muchos otros formatos.

El protocolo SIP (Session Initiation Protocol) fue desarrollado por el grupo MMUSIC (Multimedia Session Control) del IETF, definiendo una arquitectura de señalización y control para VoIP. Inicialmente fue publicado en febrero del 1996 en la RFC 2543, ahora obsoleta con la publicación de la nueva versión RFC 3261 que se publicó en junio del 2002.

El propósito de SIP es la comunicación entre dispositivos multimedia. SIP

hace posible esta comunicación gracias a dos protocolos que son RTP/RTCP y SDP.

El protocolo RTP se usa para transportar los datos de voz en tiempo real (igual que para el protocolo H.323, mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.)

SIP fue diseñado de acuerdo al modelo de Internet. Es un protocolo de señalización extremo a extremo que implica que toda la lógica es almacenada en los dispositivos finales (salvo el ruteado de los mensajes SIP). El estado de la conexión es también almacenado en los dispositivos finales. El precio a pagar por esta capacidad de distribución y su gran escalabilidad es una sobrecarga en la cabecera de los mensajes producto de tener que mandar toda la información entre los dispositivos finales.

SIP es un protocolo de señalización a nivel de aplicación para establecimiento y gestión de sesiones con múltiples participantes. Se basa en mensajes de petición y respuesta y reutiliza muchos conceptos de estándares anteriores como HTTP y SMTP.

H.323

H.323 fue el primer estándar internacional de comunicaciones multimedia, que facilitaba la convergencia de voz, video y datos. Fue inicialmente construido para las redes basadas en conmutación de paquetes, en las cuales encontró su fortaleza al integrarse con las redes IP, siendo un protocolo muy utilizado en VoIP.[9]

H.323 fue diseñado con un objetivo principal: Proveer a los usuarios con tele-conferencias que tienen capacidades de voz, video y datos sobre redes de conmutación de paquetes.

Las continuas investigaciones y desarrollos de H.323 siguen con la misma finalidad y, como resultado, H.323 se convierte en el estándar óptimo para cubrir esta clase de aspectos. Además, H.323 y la convergencia de voz, video y datos permiten a los proveedores de servicios prestar esta clase de facilidades para los usuarios de tal

forma que se reducen costos mientras mejora el desempeño para el usuario.

El estándar fue diseñado específicamente con los siguientes objetivos:

- Basarse en los estándares existentes, incluyendo H.320, RTP y Q.931.
- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos en tiempo real.
- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes.

Los diseñadores de H.323 saben que los requisitos de la comunicación difieren de un lugar a otro, entre usuarios y entre compañías y obviamente con el tiempo los requisitos de la comunicación también cambian. Dados estos factores, los diseñadores de H.323 lo definieron de tal manera que las empresas que manufacturan los equipos pueden agregar sus propias especificaciones al protocolo y pueden definir otras estructuras de estándares que permiten a los dispositivos adquirir nuevas clases de características o capacidades.

H.323 establece los estándares para la compresión y descompresión de audio y vídeo, asegurando que los equipos de distintos fabricantes se intercomuniquen. Así, los usuarios no se tienen que preocupar de cómo el equipo receptor actúa, siempre y cuando cumpla este estándar. Por ejemplo, la gestión del ancho de banda disponible para evitar que la LAN se colapse con la comunicación de audio y vídeo también está contemplada en el estándar, esto se realiza limitando el número de conexiones simultáneas.

También la norma H.323 hace uso de los procedimientos de señalización de los canales lógicos contenidos en la norma H.245, en los que el contenido de cada uno de los canales se define cuando se abre. Estos procedimientos se proporcionan para fijar las prestaciones del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y como se codifica y decodifica. Por ejemplo, cuando se origina una llamada telefónica sobre Internet, los dos terminales deben negociar cual de los dos ejerce el control, de manera tal que sólo uno de ellos

origine los mensajes especiales de control. Un punto importante es que se deben determinar las capacidades de los sistemas, de forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

Como se ha visto, este estándar define un amplio conjunto de características y funciones, algunas son necesarias y otras opcionales. Pero el H.323 define mucho más que las funciones, este estándar define los siguientes componentes más relevantes:

·Terminal
·GateWay
·Gatekeeper
·Unidad de Control Multipunto
·Controlador Multipunto
·Procesador Multipunto
·Proxy H.323

1. Terminal

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

Un terminal H.323 consta de las interfaces del equipo de usuario, el códec de video, el códec de audio, el equipo telemático, la capa H.225, las funciones de control del sistema y la interfaz con la red por paquetes.

a. Equipos de adquisición de información: Es un conjunto de cámaras, monitores, dispositivos de audio (micrófono y altavoces) y aplicaciones de datos, e interfaces de usuario asociados a cada uno de ellos.

b. Códec de audio: Todos los terminales deberán disponer de un códec de audio, para

codificar y decodificar señales vocales (G.711), y ser capaces de transmitir y recibir ley A y ley μ. Un terminal puede, opcionalmente, ser capaz de codificar y decodificar señales vocales. El terminal H.323 puede, opcionalmente, enviar más de un canal de audio al mismo tiempo, por ejemplo, para hacer posible la difusión de 2 idiomas.

c. Códec de video: En los terminales H.323 es opcional.

d. Canal de datos: Uno o más canales de datos son opcionales. Pueden ser unidireccionales o bidireccionales.

e. Retardo en el trayecto de recepción: Incluye el retardo añadido a las tramas para mantener la sincronización, y tener en cuenta la fluctuación de las llegadas de paquetes. No suele usarse en la transmisión sino en recepción, para añadir el retardo necesario en el trayecto de audio para, por ejemplo, lograr la sincronización con el movimiento de los labios en una videoconferencia.

f. Unidad de control del sistema: Proporciona la señalización necesaria para el funcionamiento adecuado del terminal. Está formada por tres bloques principales: Función de control H.245, función de señalización de llamada H.225 y función de señalización RAS.

g. Capa H.225: Se encarga de dar formato a las tramas de video, audio, datos y control transmitidos en mensajes de salida hacia la interfaz de red y de recuperarlos de los mensajes que han sido introducidos desde la interfaz de red. Además lleva a cabo también la alineación de trama, la numeración secuencial y la detección/corrección de errores.

h. Interfaz de red de paquetes: Es específica en cada implementación. Debe proveer los servicios descritos en la recomendación H.225. Esto significa que el servicio extremo a extremo fiable (por ejemplo, TCP) es obligatorio para el canal de control H.245, los canales de datos y el canal de señalización de llamada.

2. Gateway

Un gateway H.323 es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.

3. Gatekeeper

El gatekeeper es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El gatekeeper puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways.
El Gatekeeper realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP o IPX, tal y como se describe en la especificación RAS. La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN.

4. MCU

La Unidad de Control Multipunto está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

5. CONTROLADOR MULTIPUNTO

Un controlador multipunto es un componente de H.323 que provee capacidad de negociación con todos los terminales para llevar a cabo niveles de comunicaciones. También puede controlar recursos de conferencia tales como multicasting de vídeo. El

Controlador Multipunto no ejecuta mezcla o conmutación de audio, vídeo o datos.

6. PROCESADOR MULTIPUNTO

Un procesador multipunto es un componente de H.323 de hardware y software especializado, mezcla, conmuta y procesa audio, vídeo y / o flujo de datos para los participantes de una conferencia multipunto de tal forma que los procesadores del terminal no sean pesadamente utilizados. El procesador multipunto puede procesar un flujo medio único o flujos medio múltiples dependiendo de la conferencia soportada.

7. PROXY H.323

Un proxy H.323 es un servidor que provee a los usuarios acceso a redes seguras de unas a otras confiando en la información que conforma la recomendación H.323.El Proxy H.323 se comporta como dos puntos remotos H.323 que envían mensajes call – set up, e información en tiempo real a un destino del lado seguro del firewall.

A continuación se explican los protocolos más significativos para H.323:

- *RTP/RTCP (Real-Time Transport Protocol / Real-Time Transport Control Protocol)* Protocolos de transporte en tiempo real que proporcionan servicios de entrega punto a punto de datos.

- *RAS (Registration, Admission and Status):* Sirve para registrar, control de admisión, control del ancho de banda, estado y desconexión de los participantes.

- *H225.0***:** Protocolo de control de llamada que permite establecer una conexión y una desconexión.

- *H.245:* Protocolo de control usado en el establecimiento y control de una llamada.

- *Q.931:* (Digital Subscriber Signalling) Este protocolo se define para la señalización de accesos RDSI básico.

- *RSVP* (Resource ReSerVation Protocol): Protocolo de reserva de recursos en la red para cada flujo de información de usuario.

- *T.120:* La recomendación T.120 define un conjunto de protocolos para conferencia de datos.

Entre los códecs que recomienda usar la norma H.323 se encuentran principalmente:

· *G.711***:** De los múltiples códecs de audio que pueden implementar los terminales H.323, este es el único obligatorio. Usa modulación por por pulsos codificados (PCM) para conseguir tasas de bits de 56Kbps y 64Kbps.

· *H.261y H.263***:** Los dos códecs de video que propone la recomendación H.323. Sin embargo, se pueden usar otros.

2.8 CONSIDERACIONES TÉCNICAS

a) PRESUPUESTO.-

Se debe tomar en cuenta las necesidades de la Fábrica, los requerimientos técnicos de los equipos para que cumplan de forma eficiente con su tarea. El desarrollo de la tecnología IP en el país todavía es escaso por lo que los equipos de esta tecnología son de costo elevado para nosotros.

b) SEGURIDAD DE LA RED.-

El desarrollo de redes globales a las que se accede desde cualquier parte del mundo con un costo bajo y desde cualquier hogar como es INTERNET, aumenta la probabilidad de que alguien no autorizado intente acceder a la red y causar un ataque pasivo o activo.

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo

transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos.

Los ataques activos implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos.

Existen cuatro categorías generales de amenazas o ataques que son las siguientes:

- Interrupción: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

- Intercepción: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un computador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para revelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

- Modificación: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

- Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes dañinos en una red o añadir registros a un archivo.

c) CALIDAD DE VIDEO.-

Cámaras fotográficas y de video, celulares y hasta computadores de mano tienen hoy en día la capacidad de grabar secuencias de video, con diferencias marcadas en cuanto a la calidad de las imágenes dependiendo del dispositivo. Este hecho, apoyado también por la disminución de precios de dichos aparatos, le ha dado gran impulso a una tendencia común en la actualidad: la creación de contenidos en video por parte de cualquier persona.

Uno de sus mayores cambios, además de haber dado el salto hace ya varios años de los formatos analógicos a los digitales, es la entrada en la era de la alta definición, como ya lo hicieron los televisores planos y el DVD (con los nuevos discos HD DVD y Blu-ray). Este formato ofrece video de mayor calidad y definición que una cámara digital común.

FORMATOS

Existen dos tipos de cámaras de alta definición, dependiendo del formato que utilizan para grabar y reproducir el contenido. Se debe tener en cuenta que los dos registran las imágenes con compresión, pues el video es un material que ocupa mucho espacio (contiene demasiada información) y debe adaptarse a medios de almacenamiento limitados como casetes, DVD o discos duros.

Esto no significa que las imágenes queden con la misma calidad de una cámara de definición estándar. Para grabar el material, las cámaras de alta definición utilizan un codec especial que comprime el video, pero le hace conservar sus atributos de alta calidad. Los codecs son pequeños programas cuya función es modificar la calidad del video con el fin de darle determinadas propiedades.

El primer formato de este tipo que salió al mercado y que todavía permanece vigente, llamado HDV, emplea el codec MPEG-2, que es el mismo que se utiliza para la grabación de DVD de cine y está incluido en la totalidad de computadores que se vende en la actualidad. De esta manera, la compatibilidad con los programas de edición de video existentes en el mercado es total.

De otra parte, se encuentra el formato AVCHD, lanzado a mediados del 2006 por Sony y Panasonic. En un comienzo fue muy criticado pues, al utilizar una tecnología nueva, no tenía mucho soporte por parte de los fabricantes de software y sus usuarios no podían grabar el material en el computador y editarlo. No obstante, en la actualidad se está solucionando el problema, ya sea con programas para captura de video incluidos con las cámaras o mediante soluciones de terceros que incorporan en sus más recientes productos la compatibilidad con el formato. AVCHD usa el codec MPEG-4 AVH que, según sus desarrolladores, es dos veces más eficiente que el MPEG-2, utilizado por el formato HDV. Esto implica que se puede grabar más video sin tener que ocupar tanto espacio.

Tabla 2.1 Comparación de codificadores

COMPARACIONES DE CODIFICADORES			
	MPEG 1	**MPEG 2**	**MPEG 4**
Tamaño típico de imagen	352*240	720*480	720*480
Ancho de banda típico	1.5 Mbps	5 Mbps	2 Mbps
Ancho de banda máximo	2.5 Mbps	15 Mbps	4 Mbps

RESOLUCIÓN

Las cámaras de video de alta definición, al igual que los televisores, están definidas por la resolución que manejan, con nomenclaturas como 1.080i, 1.080p o 720p. Esto no es más que el número de líneas que tiene la imagen y la forma como se presentan en la pantalla (el video de formato 1.080 ofrece más líneas, o sea mayor resolución).

Las letras al lado de cada número (i, p) se refieren al tipo de compresión que utiliza la imagen.

Como son conceptos que tienden a confundir, tenga en cuenta que, cualquiera que sea la resolución que tenga una cámara de video de este tipo, le ofrecerá video de alta definición.

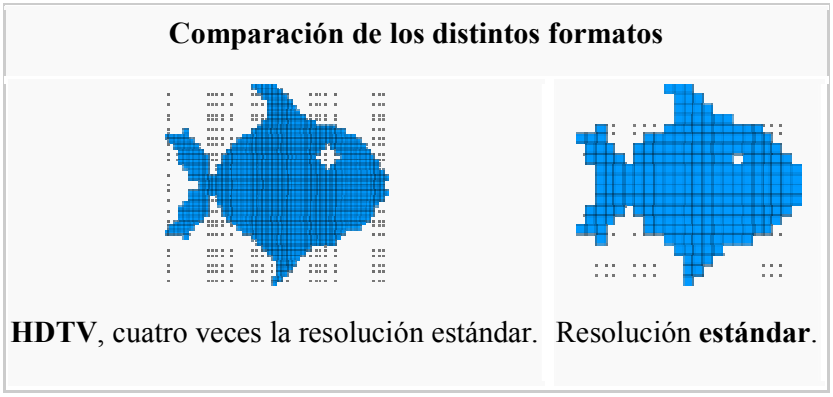

Figura 2.14 Comparación de formatos

En todas las transmisiones de vídeo analógico se define como estándar el número de líneas por frame (imagen) y el número de imágenes por segundo o Cuadros por segundo (frame per seconds - fps). El vídeo es en esencia una sucesión de cuadros que al verse a una determinada velocidad crea la ilusión de movimiento. En el vídeo NTSC, por ejemplo, se opera a 525 líneas por imagen y 30 imágenes por segundo.

Para video digital es importante conocer el término de pixel, es la figura más pequeña que hay para la creación de imágenes digitales. Es decir, si vemos una imagen digital en una computadora y empezamos a ampliarla, veremos que en un determinado momento pierde definición y se convierte en una serie de cuadrados muy pequeños de colores diferentes a partir de los cuales se empieza a componer la imagen.

La profundidad de bits que no es más que el número de bits que definen cada píxel, permite diferenciar y aplicar un número más o menos grande de colores. La mayoría de las cámaras digitales utilizan la profundidad de 24 bits del modo RGB (Red Green Blue), por lo que cada píxel contiene 3 bytes de información.

d) CAPACIDAD DE LA RED.-

La Fábrica de Municiones Santa Bárbara dispone de una red LAN 10/100/1000 Base-T, y con una con un ancho de banda para Internet de 512 Kbps.

e) DEMANDA DEL ANCHO DE BANDA.-

El video analógico no necesita gran estudio en este tema, debido a que la transmisión de señales se la realiza con cable dedicado y exclusivo para cada cámara, sea este coaxial, UTP o fibra óptica. La señal es transportada directamente hacia el DVR independientemente de la calidad de la imagen, teniendo que considerar de acuerdo al medio de transmisión y la distancia del enlace, el uso de acopladores de impedancias y de amplificadores de la señal. [12]

Para video digital, dependiendo de la configuración del sistema, el vídeo puede consumir grandes cantidades de ancho de banda de la red, por lo tanto es importante comprender el rendimiento de la red actual: dónde hay cuellos de botella y dónde pueden ocurrir si se instala un sistema de vídeo digital. Esto garantizará el nivel de rendimiento del que es preciso disponer para asegurar la operatividad de un sistema de seguridad, y al mismo tiempo previene que el consumo sea superior a la capacidad, con la consecuente reducción del rendimiento de otros sistemas de la misma red.

Es difícil definir el uso exacto del ancho de banda por parte de una cámara, debido a que dependerá de varios factores como:

- Tamaño de las imágenes
- Rango de imágenes por segundo
- Compresión
- Resolución de la imagen

La compresión puede ser de dos formas, Sin Pérdidas o Con Pérdidas:

En la compresión sin pérdidas, los datos de salida de la decodificación son idénticos bit a bit a los de la fuente original. Los factores de compresión conseguidos son pequeños, menores de 10:1 en el mejor de los casos. Una codificación sin perdidas no puede garantizar un factor de compresión determinado, pues depende de la cantidad de redundancia de la información original.

En la compresión con pérdidas, los datos de la salida de la decodificación no son idénticos bit a bit a los de la fuente original, lo que se pretende, es que estas diferencias sean lo menos perceptibles posible, los factores de compresión son altos 40:1, a 100:1, e inclusive en aplicaciones multimedia con factores de compresión que pueden llegar a ser de 200:1. Estas técnicas de compresión orientadas al sector multimedia se encuentran implementadas en pequeñas aplicaciones llamadas codecs, pequeños programas que incorporan los procesos necesarios para la compresión de una señal. En la tabla podemos observar algunos valores de compresión en diferentes aplicaciones:

Tabla 2.2 Velocidades de Transmisión

APLICACIÓN	VELOCIDAD DE TRANSMISIÓN	
	SIN COMPRESIÓN	CON COMPRESIÓN
Voz (8khz, 8 bits)	64 Kbits/seg	2-4 Kbits/seg
Audio Conferencia (8khz, 8 bits)	64 Kbits/seg	4-16 Kbits/seg
Audio Digital (Estéreo) (44.1 khz, 16 bits)	1.5 Mbits/seg	32-96 Kbits/seg
Video Conferencia (352 *240, 8 bits, Y)	10.13 Mbits/seg	64-768 Kbits/seg
Video CD-ROM (352*288, 2:1:0)	30.41 Mbits/seg	1.5 Mbits/seg
Video Broadcast (720*576, 4:2:2)	270 Mbits/seg	4-6 Mbits/seg
HDTV (1920*1152, 8 bits, 8:4:4)	884.7 Mbits/seg	16.25 Mbits/seg

En relación a la gestión del ancho de banda es importante conocer que los productos de vídeo (basados en la compresión MPEG) utilizarán el ancho de banda en función de su configuración, es decir comprimirán la imagen de acuerdo a su capacidad. Una imagen de alta resolución (4CIF) contiene cuatro veces más datos que una imagen a resolución normal (CIF).

CIF: El formato CIF (**Common Intermediate Format**) se utiliza para compatibilizar los diversos formatos de vídeo digital. Es un formato normalizado que es utilizado por cualquier codificador híbrido H.261. Éste estandariza la

resolución, tanto vertical como horizontal de los píxeles de secuencias YCbCr de las imágenes de vídeo digital. Su objetivo es ofrecer un formato de vídeo común reducido para los codificadores.
Muchas veces se le conoce como FCIF (Full CIF) para diferenciarlo del QCIF (Quarter CIF)
Está definido en la Recomendación H.261 de la ITU.

Características básicas

Define secuencias de vídeo de 29,97 imágenes por segundo, donde cada una de ella contiene 288 líneas con 352 píxels por línea. La imagen definida con estos parámetros presenta una relación de aspecto en formato 4:3.

Su diseño permite la fácil conversión a los estándares PAL de 625 líneas y NTSC de 525 líneas (Compromiso con el formato SIF), debido a que utiliza patrones extraídos del sistema Europeo y del Americano. Por ejemplo, presenta 352x288 muestras de resolución de luminancia (EUR) y 30Hz como frecuencia de imagen (EUA).

Características Avanzadas

Los parámetros Y, B y R se corresponden con la señal de luminancia y con las de color azul y rojo respectivamente.

La imagen está formada por la señal de luminancia y la señal de crominancia. La de luminancia se muestrea a 6.75MHz, mientras que la de crominancia se muestrea a 3.275MHz para aprovechar la particularidad que el sistema visual humano tiene menos sensibilidad a los colores que a la luminancia. Esto hace que se pueda transmitir el color utilizando un ancho de banda menor y sin afectar prácticamente a la calidad de la señal.

Tabla 2.3 Frecuencias y señales

Señales Muestreadas	Frecuencias de Muestreo	Estructura del muestreo	Relación de Aspecto
Y, Cb (Y-B), Cr (Y-R)	6,75MHz para *Y* y 3,375MHz para *Cb* i *Cr*	Ortogonal, no entrelazado	4: 3

Tabla 2.4 Comparación de resoluciones entre los formatos de vídeo reducidos

Formato	Resolución vídeo
SQCIF	128 × 96
QCIF	176 × 144
CIF	352 × 288
4CIF	704 × 576
16CIF	1408 × 1152

Para realizar el cálculo del ancho de banda que demanda el sistema, se utilizara la siguiente fórmula:

- Uso de ancho de banda de una cámara en Kbps = Tamaño de imagen X frames por segundo X 8 Kbps.

- Tamaño de imagen = Resolución en pixeles (4 CIF o CIF) X Numero de bits usados para definir un pixel.

Calculo 1:

Considerando que el número total de cámaras es de 6 y cada una de ellas transmitiendo video a 30 fps, cada píxel definido por 3 Bytes con una resolución 4CIF (704x506), tenemos:

Tamaño de imagen = 704 x 506 x 24bits = 8549376 bps = 8,55 Mbits.

Realizando una compresión de imagen con un factor de compresión de 100:1 obtenemos un tamaño de imagen de 85,5 Kbits.

85,5 Kbits x 30fps x 8Kbps=20520 Kbps= 20,520 Mbps para cada cámara.

20,496 Mbps x 6 cámaras = 122,976 Mbps.

El mínimo ancho de banda que se puede utilizar el sistema se obtiene de la siguiente manera:

- Reduciendo las imágenes por segundo a 17fps, valor que el ojo humano considera como una imagen continua,
- Disminuir el número de colores, es decir reducir el número de bits para definir un pixel 8 bits.
- Disminuir la resolución de la imagen, es decir a un formato CIF o SUBCIF,
- Aumentar la compresión de video hasta 200:1.

Calculo 2:

Considerando el mismo número de cámaras (6) y tomando en consideración los parámetros expuestos en el párrafo anterior, se tiene:

Formato CIF 352x288

Tamaño de imagen = 352 x 288 X 8bits = 811008 bps = 811 Kbits

Realizando una compresión de imagen con un factor de compresión de 200:1 obtenemos un tamaño de imagen de 4 Kbits.

4 Kbits x 17fps x 8Kbps = 544Kbps para cada cámara.

544 Kbps x 6 = 3264 Kbps = 3,264 Mbps.

Manejando diferentes valores que alteran o disminuyendo la calidad de la imagen se puede obtener un ancho de banda menor que se ajuste al disponible, pero con una buena calidad de video, el ancho de banda requerido es alto, pudiendo poner en riesgo la capacidad de la red.

REFERENCIAS BIBLIOGRÁFICAS DEL CAPÍTULO 2

[1] Wikipedia, Circuito Cerrado de Televisión, http://es.wikipedia.org/wiki/Circuito_cerrado_de_televisi%C3%B3n, 15 de Octubre del 2007.

[2] Optral, S.A., CCTV: Digital o analógico, por fibra óptica, http://www.fibraopticahoy.com/articulos/fa001.htm, 10 de Noviembre del 2007.

[3] Monografías.com, Circuito Cerrado de Televisión, http://www.monografias.com/trabajos/cctelevis/cctelevis.shtml?monosearch, 10 de Noviembre del 2007.

[4] IES de Sabón, Departamento de Electricidad, Instalaciones singulares en viviendas y edificios, Circuito Cerrado de televisión, 10 de Noviembre del 2007.

[5] Wikipedia, Autenticación, http://es.wikipedia.org/wiki/Autenticaci%C3%B3n, 10 de noviembre del 2007.

[6] Tanenbaum, Andrew, *Redes de Computadoras*, Cuarta Edición, Editorial Pearson Educación, México 2003.

[7] Hardware para redes, http://dmi.uib.es/~loren/docencia/webxtel/bibliografia/HARDWARE%20PARA%20REDES.html, 10 de noviembre del 2007.

[8] Arquitectura SIP, Protocolo SIP, http://www.voipforo.com/SIP/SIParquitectura.php, 10 de noviembre del 2007.

[9] Protocolos VoIp, Protocolo H.323, http://www.voipforo.com/H323/H323objetivo.php, 10 de noviembre del 2007.

[10] La seguridad integral en la concepción y el Diseño de edificios, La integración en el diseño de la seguridad, Segint 2003, 10 de noviembre del 2007.

[11] Jhon Faber Archila Díaz, Diego Alexander Tibaduiza Burgos, Luz Ángela Jiménez Pinilla, "Implementación de un sistema de control de acceso e Iluminación", Facultad de Ingeniería Mecatrónica, Universidad Autónoma de Bucaramanga.

[12] Axis Communications, Técnicas de compresión de video, Video e Imagen Digital para aplicaciones de vigilancia.