Universidad del Azuay

Facultad de Ciencia y Tecnología

Escuela de Ingeniería Electrónica

"DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO Y VIDEO VIGILANCIA PARA LA UNIDAD EDUCATIVA PORVENIR CON LA UTILIZACION DE DISPOSITIVOS IP."

Trabajo de graduación previo a la obtención del título de

Ingeniero Electrónico

Autores:

Adrián Milton Ortega Zúñiga
Byron Paúl Fernández Carrión

Director:

Lcdo. Leopoldo Carlos Vázquez Rodríguez

Cuenca, Ecuador

2009

DEDICATORIA:

Dedico este trabajo, a mis amados padres, esposa, hijo y hermana, por ser incondicionales y brindarme todo su apoyo.

Byron Fernández Carrión

DEDICATORIA:

A mis padres Manuel y Guillermina, esencia de amor y ejemplo a seguir en mi vida.

Adrián

AGRADECIMIENTOS

Los trabajos en los cuales participa una sola persona son escasos y afortunadamente este no es uno de ellos.

Agradecemos a Dios y a todas las personas que de una u otra forma ayudaron a que este proyecto se haga realidad, especialmente a nuestro director Licenciado Leopoldo Vázquez, a los vocales miembros de tribunal, Ingeniero Eduardo Sempértegui e Ingeniera Cecilia Navas, por su apoyo y lealtad para con nosotros.

RESUMEN

El presente trabajo realiza el análisis de las características y funcionalidad de dispositivos domóticos, con el propósito de diseñar un sistema de seguridad y monitoreo para la Unidad Educativa Porvenir, que permita controlar el ingreso del personal administrativo, docente y personas particulares, seleccionando los equipos de vigilancia y control de accesos que más se ajusten a las necesidades del mismo, para obtener una mayor cobertura de vigilancia se determinarán las áreas de los lugares considerados de mayor riesgo por su fácil acceso, aplicando los sistemas de software y hardware adecuados considerando además los costos y la eficiencia de los mismos.

ABSTRACT

This monographic work makes analyses of the characteristics and how domotic devices work with the purpose of designing a Surveillance and Security System to be installed at "PORVENIR" High School. The system allows to control the people who is inside and outside the building, selecting the best equipment and the strategic areas to cover in a better way the risk places, applying the correct hardware and software considering besides the cost and the efficacy of them.

ÍNDICE DE CONTENIDOS

CAPÍTULO 4: DISEÑO DE UN SISTEMA INTEGRADO DE VIGILANCIA

FERNANDEZ CARRION BYRON PAÚL
ORTEGA ZÚÑIGA ADRIÁN MILTON
PROYECTO DE TESIS
LCDO. LEOPOLDO VAZQUEZ RODRÍGUEZ
MAYO DEL 2009

"DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO Y VIDEO VIGILANCIA PARA LA UNIDAD EDUCATIVA PORVENIR CON LA UTILIZACION DE DISPOSITIVOS IP."

INTRODUCCIÓN

Las innovaciones tecnológicas siempre han sido aplicadas y utilizadas en las viviendas, su incorporación ha contribuido a cambiar desde las relaciones familiares hasta la estructura de la ciudad. Recientemente la domótica, o el uso y adopción de las nuevas tecnologías de la información y la comunicación en el hogar, está empezando a inducir cambios en el uso y la función de la vivienda, acentuando las alteraciones en la percepción del espacio-tiempo que ya se detectan en otras instancias de la vida cotidiana. Se pude señalar entonces que la naturaleza y función de la vivienda están mutando considerablemente, lo cual plantea retos en la medida que constituye una de las instancias primarias de las relaciones sociales, de la interacción familiar, de la vida cotidiana y de la estructura de la ciudad.

En la literatura de ciencia ficción las alusiones a las viviendas del futuro han llegado hasta el punto de considerar posible que puedan entablar una conversación con las personas que las habitan, sugieren una relación un tanto diferente y fantástica entre un humano y una casa tan inimaginables como podríamos pensar.

Se han realizado estudios para crear sistemas de diálogo para un entorno domótico que permite dar órdenes orales a ciertos dispositivos del hogar y programar funciones verbalmente sin la necesidad de emplear comandos artificiales. La arquitectura del sistema se basa en agentes inteligentes distribuidos e interconectados que usan la red

eléctrica de la vivienda, lo cual implica que no se requiere un nuevo cableado, soportándose en sistemas informáticos, principalmente los estándares o lenguajes X10 y "*Lonworks"*.

Sistemas como el control de temperatura, circuitos cerrados CCTV, sistemas de control de acceso, ahorro de energía, casas con conexiones de red dentro de ellas y con otras casas, video vigilancia y seguridad, la utilización del internet como herramienta principal para la transmisión de ordenes desde cualquier parte en la que nos encontremos, nos sugiere que la vivienda está mutando, que nuestra relación con ella y los objetos que la definen puede potencialmente modificarse, aunque para algunos este fenómeno ya es todo un hecho.

La domótica, casa inteligente o "*Smart Home"* está al alcance sólo de algunos bolsillos, aunque la tendencia ha cambiado un poco por el efecto que sobre el precio tiene el ciclo de vida de los productos de alta tecnología. Algunas de sus implicaciones sociales más tangibles son las nuevas formas de entender la vivienda y el habitar, pues ya no funciona solo como dormitorio, por ejemplo; ahora es lugar de ocio y trabajo a la vez.

CAPÍTULO 1

INTRODUCCIÓN DE LA ELECTRÓNICA EN LA AUTOMATIZACIÓN DE INMUEBLES

Tras la entrada de la electricidad en las ciudades, convirtiéndose en parte de su sistema nervioso, los múltiples electrodomésticos que surgieron sólo llegaban a unos pocos. Aquellos bellos y mágicos artefactos para planchar, para tostar el pan y para lavar la ropa fueron considerados durante mucho tiempo como inasequibles para casi todos, especialmente para las capas sociales de bajos recursos. Pero con el tiempo la situación cambió. Y con el tiempo, a pesar de los matices que ello sugiere, también cambiará la proporción de hogares que utilicen sistemas domóticos.

1.1 RESEÑA

El origen de la domótica se remonta a la década de los setenta, cuando después de muchas investigaciones aparecieron los primeros dispositivos de automatización de edificios basados en la aun exitosa tecnología X-10. Durante los años siguientes la comunidad internacional mostró un creciente interés por la búsqueda de la casa ideal, comenzando diversos ensayos con avanzados electrodomésticos y dispositivos automáticos para el hogar. Los primeros sistemas comerciales fueron instalados en Estados Unidos y se limitaba a la regulación de la temperatura ambiente en los edificios de oficina. Más tarde con el auge de las PC (*Personal Computer*) a finales de la década de los 80 y principios de la de los 90, se empezaron a incorporar a estos edificios los *Sistemas de Cableado Estructurado* para facilitar la conexión de todo tipo de terminales

y periféricos entre sí, utilizando un cableado estándar y tomas repartidas por todo el edificio. Además de los datos, estos sistemas de cableado permitían el transporte de voz y la conexión de algunos dispositivos de control y de seguridad, por lo que a estos edificios se los comenzó a llamar edificios inteligentes. Los franceses incorporaron el término "*domotique"* a partir de 1998. Esta palabra, traducida al castellano significa domótica, que es originaria de la palabra latina "*domus"* (que quiere decir casa) y de la palabra francesa "*informatique"* (que significa informática), o según algunos autores, "*robotique"* (robótica).

Posteriormente, los automatismos diseñados y destinados a edificios de oficinas junto a otros específicos como la industria, se han aplicando también a viviendas de particulares y edificios de apartamentos, donde el número de necesidades a cubrir es más amplio, dando origen a la vivienda domótica.

En la actualidad, el número de viviendas domotizadas es relativamente bajo con respecto al total de viviendas, pero el interés en su adopción está creciendo progresivamente. Del mismo modo que en estos días no es permisible que en una casa falte la luz eléctrica, teléfono o agua, dentro de muy poco no se concebirán viviendas que no estén mínimamente domotizadas. Unos de los principales problemas que encuentran las personas para disponer de esta tecnología, es que los precios eran relativamente altos, pero con el actual descenso de los precios debido a la demanda que ahora presenta la domótica, el hecho de tener una casa domotizada es cada vez más asequible.

1.2 EL HOGAR DIGITAL Y LAS TELECOMUNICACIONES

La domótica se relaciona con todo lo que es tecnología, y por ende lo que concierne a las telecomunicaciones, convergiendo a ambas en un concepto que se lo conoce como hogar digital.

La gran evolución que ha sufrido las telecomunicaciones con el aparecimiento del Internet y su gran desarrollo, ha dado lugar al incremento exponencial para crear

información, almacenarla, transmitirla, recibirla, y procesarla. El acceso a la información, cada vez más fácil, ha contribuido a brindar una mayor facilidad para comunicarnos y establecer vías de diálogos con cualquier persona en y desde cualquier parte del mundo, en cualquier momento; lo cual nos da una pauta para buscarle nuevos usos a esta tecnología digital, tal como el control aplicado a la revolución de la domótica, donde las pasarelas residenciales, apoyadas con conexiones de banda ancha, servirán de enlace inteligente para conectar y controlar todos los dispositivos del hogar, soportando servicios interactivos que brindarán al usuario una mayor comodidad para realizar tareas a distancia.

Algunas de las ventajas que representa el vivir en un hogar digital son aspectos como (fig. 1):

- La programación del encendido y apagado de todo tipo de aparatos.
- Entretenimiento y "*confort*".
- Control de dispositivos del hogar desde un PC por Internet, o desde un teléfono móvil.
- Seguridad, control de accesos, aviso en caso de intrusión o avería.
- Ahorro de energía.

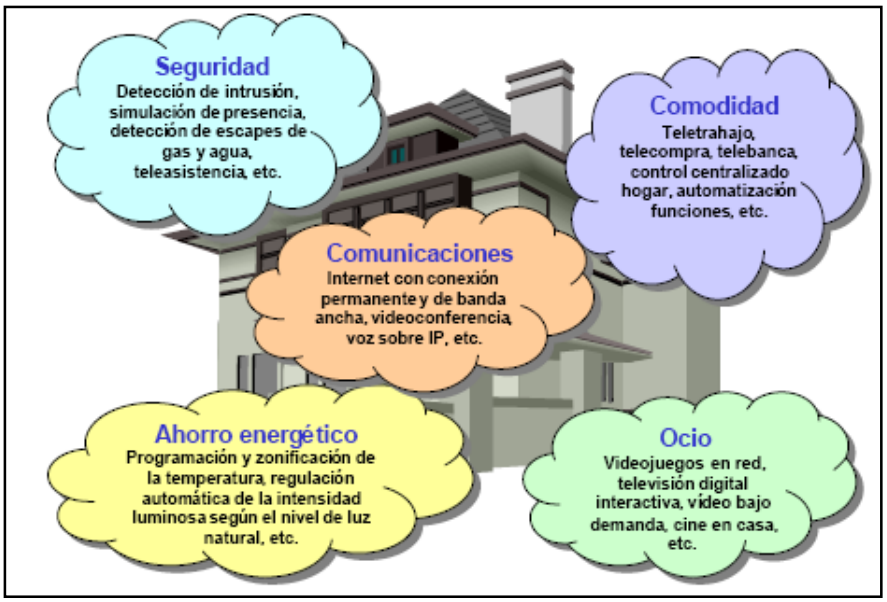


fig.1: *Esquema de una Instalación Domótica*

1.3 DOMÓTICA

En el Diccionario de la Real Academia Española aparece que la palabra domótica proviene del latín "*domus*" (casa) y del término informática, siendo el "*conjunto de sistemas que automatizan las diferentes instalaciones de la vivienda*"[1]. De alguna manera esta definición puede servir, pero en realidad va más allá de sólo unos sistemas de automatización.

La domótica puede definirse como la adopción, integración y aplicación de las nuevas tecnologías informáticas y comunicativas al hogar. Incluye principalmente el uso de electricidad, dispositivos electrónicos, sistemas informáticos y diferentes dispositivos de telecomunicaciones, incorporando la telefonía móvil e Internet. Algunas de sus principales características son: interacción, interrelación, facilidad de uso, tele operación o manejo a distancia, fiabilidad, y capacidad de programación y actualización. Su arquitectura puede ser centralizada o distribuida, aunque en realidad, por las ventajas de intercomunicación y ante los fallos, se emplea más la descentralizada. Los protocolos pueden ser estándar, es decir compatibles entre sí, y propietarios, que son los creados exclusivamente para un cliente o aplicación única. La configuración estándar cuenta con un sistema compuesto por ordenador u ordenadores, módem, tarjeta de sonido, dispositivos de amplificación de audio, baterías de emergencia, sondas de temperatura (exterior e interior), detectores de humo, gas y agua, video portero, sensores magnéticos para puertas y ventanas, detectores de presencia, mandos a distancia y emisores-receptores de señal.

El vertiginoso avance tecnológico experimentado en los últimos años ha contribuido eficazmente al desarrollo de la domótica, avances que han permitido su rápida penetración en el equipamiento con que se dota, actualmente, a los edificios modernos en las grandes ciudades y que hacen esperar que en el futuro encuentren su plena expansión gracias a las comodidades que brindan y su facilidad de uso.

---

[1] Real Academia Española 2001, p. 847. Este diccionario, y las versiones anteriores, puede consultarse en línea en <http://www.rae.es/>.

Por estas razones urge que los instaladores, constructores, ingenieros, arquitectos y diseñadores adquieran una rápida familiarización con las posibilidades de los nuevos dispositivos y su máximo conocimiento para aprovechar los beneficios que nos brinda esta nueva perspectiva de la electrónica, e incorporarlos como un requisito en la vida del hombre, así, de esta forma se incrementará su competitividad en el mercado mejorando precios e incluso calidad de los dispositivos domóticos.

1.3.1 DISPOSITIVOS

La amplitud de una solución domótica puede variar desde un único dispositivo, que realiza una sola acción, hasta amplios sistemas que controlan prácticamente todas las instalaciones dentro de la vivienda. Los distintos dispositivos de los sistemas de domótica se pueden clasificar en los siguientes grupos:

- **Controlador,** es un dispositivo que gestiona el sistema según la programación y la información que reciben. Puede haber un solo controlador, o varios distribuidos por el sistema.
- **Actuador,** es un dispositivo capaz de ejecutar y/o recibir una orden del controlador y realizar una acción sobre un aparato o sistema (encendido/apagado, subida/bajada, apertura/cierre, etc.).
- **Sensor**, es el dispositivo que monitorea el entorno captando información que transmite al sistema (sensores de agua, gas, humo, temperatura, viento, humedad, lluvia, iluminación, etc.).
- **Bus,** es el medio de transmisión que transporta la información entre los distintos dispositivos por un cableado propio, por la redes de otros sistemas (red eléctrica, red telefónica, red de datos) o de forma inalámbrica.
- **Interface,** refiere a los dispositivos: pantallas, móvil, Internet, conectores, y los formatos (binario, audio) en que se muestra la información del sistema para los usuarios u otros sistemas y donde los mismos pueden interactuar con el sistema.

Es preciso destacar que todos los dispositivos de un sistema domótico no tienen que estar físicamente separados, sino varias funcionalidades pueden estar combinadas en un

equipo. Por ejemplo un equipo de Central de Domótica puede ser compuesto por un controlador, actuadores, sensores y varios interfaces.

1.3.2 ARQUITECTURA

La Arquitectura de los sistemas domóticos hace referencia a la estructura de su red. La clasificación se realiza en base de donde reside la "inteligencia" del sistema domótico. Las principales arquitecturas son:

- **Arquitectura Centralizada,** En un sistema domótico de arquitectura centralizada, un controlador centralizado, envía la información a los actuadores e interfaces según el programa, la configuración y la información que recibe de los sensores, sistemas interconectados y usuarios (fig. 2). La desventaja de un sistema centralizado es que si falla el controlador, falla todo el sistema

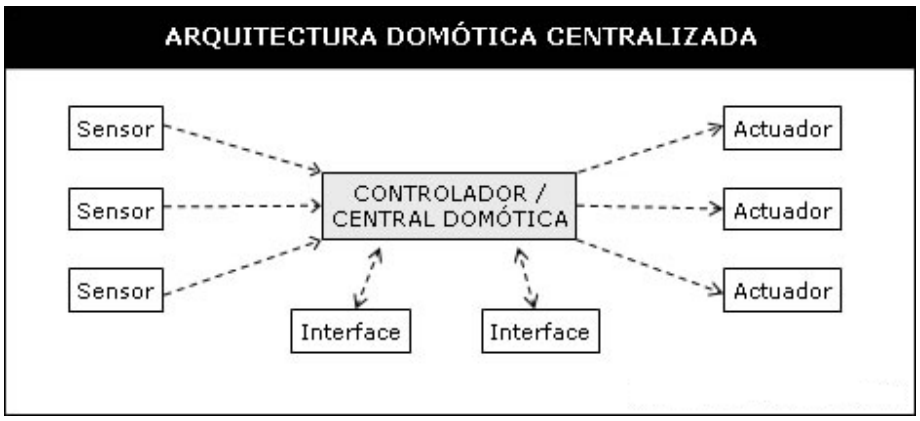


fig. 2: Esquema de Arquitectura de un Sistema Domótico Centralizado (Libro Blanco)

- **Arquitectura Descentralizada,** En un sistema domótico de arquitectura descentralizada, hay varios controladores, interconectados por un bus, que envía información entre ellos y a los actuadores e interfaces conectados a los controladores (fig. 3), según el programa, la configuración y la información que recibe de los sensores, sistemas interconectados y usuarios.

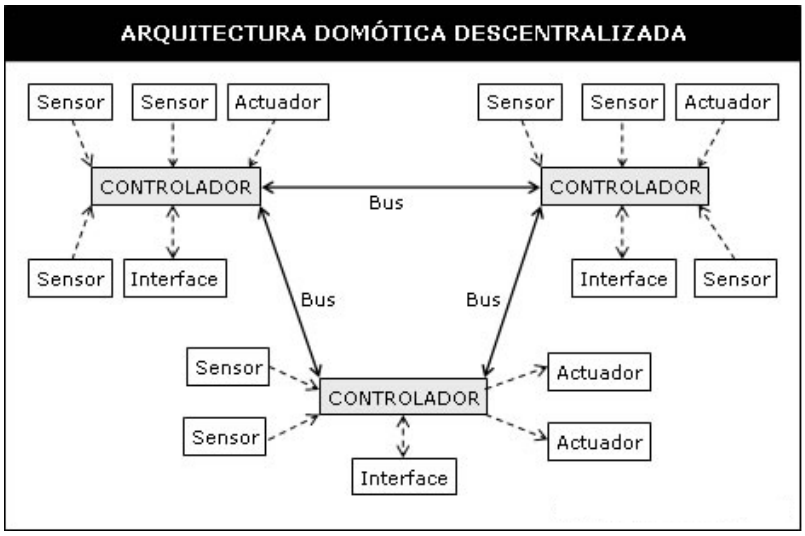


Fig. 3: Esquema de Arquitectura de un Sistema Domótico Descentralizado (Libro Blanco)

- **Arquitectura Distribuida,** En un sistema domótico de arquitectura distribuida (fig. 4), cada sensor y actuador es también un controlador capaz de actuar y enviar información al sistema según el programa, la configuración, la información que capta por sí mismo y la que recibe de los otros dispositivos del sistema.

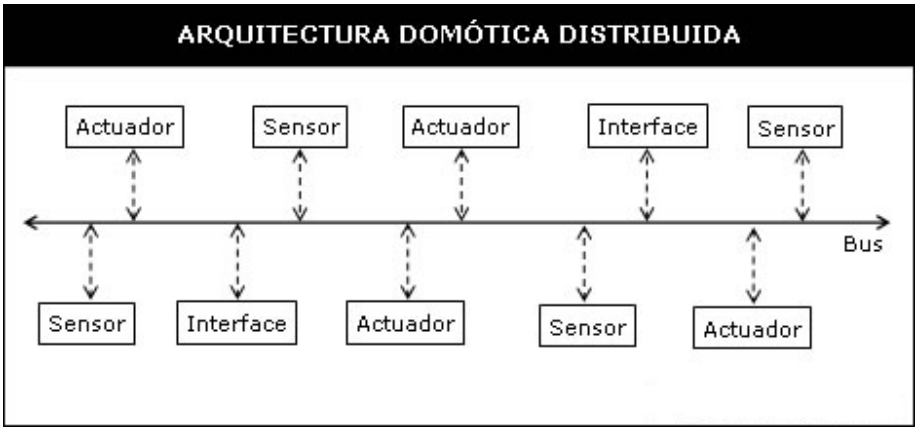


Fig. 4: *Esquema de Arquitectura de un Sistema Domótico Distribuido*

- **Arquitectura Híbrida o Mixta,** En un sistema domótico de arquitectura híbrida o mixta se combinan las arquitecturas de los sistemas centralizadas, descentralizadas y distribuidas (fig. 5), es decir que puede disponer de un

controlador central o varios controladores descentralizados, los dispositivos de interfaces, sensores y actuadores pueden también ser controladores y procesar la información según el software, la configuración, la información captada, y actuar enviándola a otros dispositivos de la red, sin que necesariamente pase por otro controlador.

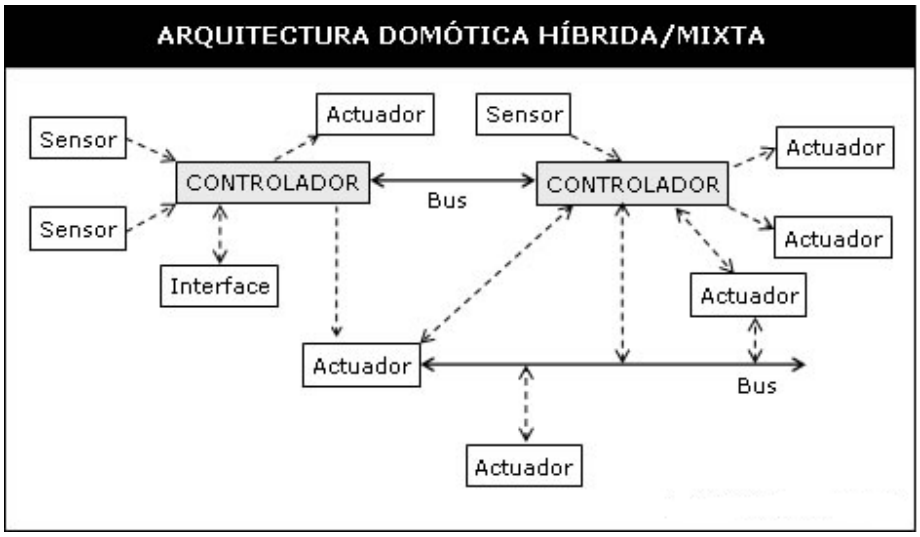


Fig. 5: *Esquema de Arquitectura de un Sistema Domótico Híbrido o Mixto*

CAPÍTULO 2

VIDEO IP (Protocolo de Internet)

En la actualidad, la industria de vigilancia mediante Vídeo IP dispone de una amplia gama de sistemas y dispositivos para la monitorización y protección tanto de personas como de propiedades. Para entender el ámbito y el potencial de un sistema integrado y completamente digitalizado, vamos a examinar en primer lugar los componentes principales de un sistema de vídeo IP: la cámara IP, el servidor de vídeo y el software de gestión de vídeo. Al elegir el sistema adecuado, es de gran utilidad comparar las diversas tecnologías disponibles en vista de la zona de aplicación propuesta y los requisitos en términos de rentabilidad, escalabilidad, facilidad de uso y flexibilidad.

2.1 ¿QUÉ ES EL VÍDEO IP?

El vídeo IP, a menudo conocido como vigilancia IP para determinadas aplicaciones en el ámbito de la vigilancia en seguridad y la monitorización remota, es un sistema que ofrece a los usuarios la posibilidad de controlar y grabar en video a través de una red IP (LAN/WAN/Internet).

A diferencia de los sistemas de vídeo analógicos, el vídeo IP no precisa cableado punto a punto dedicado y utiliza la red como eje central para transportar la información. El término video IP hace referencia tanto a las fuentes de video como de audio disponibles a través del sistema.

Los principales mercados verticales donde los sistemas de vídeo IP se han instalado satisfactoriamente son los siguientes:

- **Educación:** Para la monitorización remota y la seguridad de zonas de recreo, pasillos, aulas y entradas en escuelas, así como la seguridad de los propios edificios.
- **Transporte:** Para la monitorización remota de estaciones de tren, vías, autopistas y aeropuertos.
- **Banca:** Aplicaciones tradicionales de seguridad en bancos principales, sucursales y oficinas ATM.
- **Gobierno:** Con fines de vigilancia, para proporcionar entornos públicos seguros.
- **Comercios minoristas:** Con fines de monitorización remota y seguridad. Facilita y hace más eficaz la gestión de los comercios.
- **Industrial:** Para controlar los procesos de fabricación, los sistemas de logística y los sistemas de control de existencias y el almacén.

2.2 ¿QUÉ ES UNA CÁMARA DE RED IP?

Una cámara de red IP puede describirse como una cámara y un ordenador combinados para formar una unidad. Capta y transmite imágenes directamente a través de una red IP, permitiendo a los usuarios autorizados visualizar, almacenar y gestionar vídeo de forma local o remota. Una cámara de red tiene su propia dirección IP, no necesita estar conectada a un PC, funciona independientemente y puede colocarse en cualquier lugar donde haya una conexión de red IP.

Además del vídeo, una cámara IP también incluye otras funcionalidades e información que se transmiten a través de la misma conexión de red como por ejemplo, entradas y salidas digitales, audio, puerto(s) serie para datos o control de mecanismos con movimiento vertical, horizontal y “zoom”.

Para explicar de una forma más práctica, podríamos establecer diferencias entre las cámaras analógicas y las cámaras IP. Una cámara analógica es una portadora de señal unidireccional que finaliza a nivel del usuario y el DVR, mientras que una cámara IP es

completamente bidireccional, integrando e impulsando el resto del sistema a un nivel superior en un entorno escalable y distribuido. Una cámara IP se comunica con diversas aplicaciones en paralelo para realizar varias tareas, tales como la detección de movimiento o el envío de diferentes secuencias de vídeo.

Una cámara IP combina una cámara y un ordenador en una sola unidad, lo que incluye la compresión y digitalización del video así como un conector de red. El video se transmite a través de una red IP, mediante los conmutadores de red y se graba en un PC estándar con software de gestión de video, Esto representa un verdadero sistema de video IP donde no se utilizan componentes analógicos.

Un sistema de video IP, con cámaras IP, añade las siguientes ventajas:

- Cámaras de alta resolución (Mega píxel)
- Calidad de imagen constante
- Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica
- Funciones de movilidad, zoom, audio, entradas y salidas digitales a través de IP junto con el video
- Flexibilidad y escalabilidad completas

2.3 GENERACIÓN DE LA IMAGEN

2.3.1 CALIDAD DE LA IMAGEN IP

En la actualidad, existen dos técnicas diferentes disponibles para interpretar el vídeo: barrido entrelazado y barrido progresivo. La elección de una de estas técnicas dependerá de ***la aplicación y objetivo*** del sistema de vídeo y, en particular, de si será necesario captar objetos en movimiento y permitir la visualización al detalle de una imagen en movimiento.

a) **Barrido entrelazado:** Las imágenes que se basan en el barrido entrelazado utilizan técnicas desarrolladas para las pantallas de monitores de TV con tubo de

rayos catódicos (CRT), que constan de 576 líneas visibles (fig. 6), horizontalmente situadas a lo ancho de una pantalla de TV estándar. El entrelazado las divide en líneas pares e impares y, a continuación, las actualiza a 30 imágenes por segundo. El pequeño retraso entre las actualizaciones de una línea par e impar crea una distorsión o “jaggedness". Esto ocurre porque sólo la mitad de las líneas sigue la imagen en movimiento mientras que la otra mitad espera a ser actualizada.

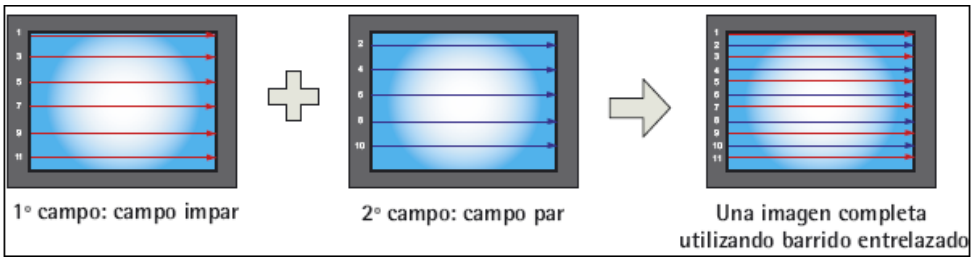


Fig. 6: Barrido Entrelazado(Domótica e Inmotica, Carlos Lozan)

El barrido entrelazado ha sido de gran utilidad durante muchos años en el mundo de la cámara analógica, la televisión y el vídeo VHS, y aún lo sigue siendo para determinadas aplicaciones. Sin embargo, ahora que la tecnología de la pantalla está cambiando con la llegada de la pantalla de cristal líquido (LCD), las cámaras digitales y los DVD, se ha creado un método alternativo de aportar imagen a la pantalla, conocido como barrido progresivo.

b) Barrido progresivo: El barrido progresivo *(progressive scan)*, a diferencia del entrelazado, escanea la imagen entera línea a línea cada 1/16 segundos (fig. 7). En otras palabras, las imágenes captadas no se dividen en campos separados como ocurre en el barrido entrelazado. Los monitores de ordenador no necesitan el entrelazado para mostrar la imagen en la pantalla. Las coloca en una misma línea a la vez en perfecto orden como por ejemplo, 1, 2, 3, 4, 5, 6, 7, etc. Por tanto, virtualmente no existe un efecto de “parpadeo”. En ese sentido, en una aplicación de vigilancia puede resultar vital para visualizar al detalle una imagen en movimiento como por ejemplo, una persona que está huyendo. Sin embargo,

se necesita un monitor de alta calidad para sacar el máximo partido de este tipo de barrido.

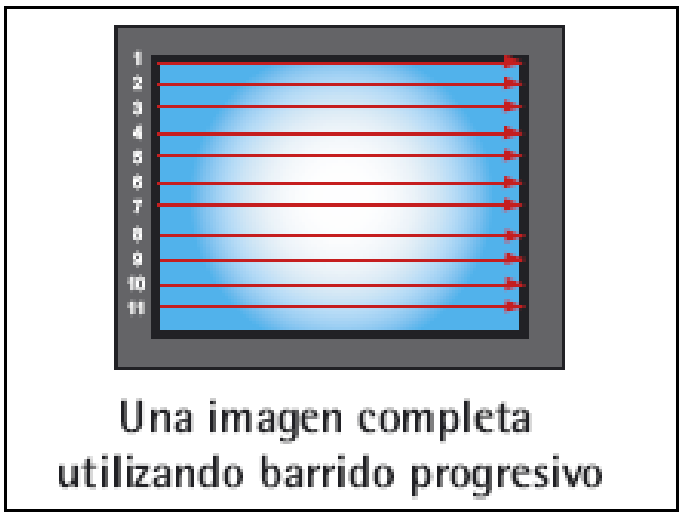


Fig. 7: Barrido Progresivo (Domótica e Inmotica, Carlos Lozan)

2.4. COMPRESIÓN

La compresión de imagen y de vídeo puede realizarse con un enfoque de pérdida o sin pérdida de datos.

En la compresión sin pérdida de datos, cada uno de los píxeles permanece inalterado, lo que se traduce en una imagen idéntica tras la compresión. La desventaja es que la relación de compresión o la reducción de datos, es muy limitada. Un formato de compresión sin pérdida de datos muy conocido es GIF. Como la relación de compresión es tan limitada, estos formatos resultan inadecuados para usar en soluciones de vídeo IP porque son demasiado pesados para almacenar y transmitir grandes cantidades de imágenes.

Es por lo detallado anteriormente que se han desarrollado varios métodos y estándares de compresión con pérdida de datos. La idea básica es reducir aquellas cosas que el ojo humano no puede percibir y al hacer esto es posible aumentar la relación de compresión de forma espectacular. Los métodos de compresión también implican dos enfoques

diferentes de los estándares de compresión: compresión de las imágenes fijas y compresión de vídeo.

2.4.1. ESTÁNDARES DE COMPRESIÓN DE IMÁGENES FIJAS

La compresión de imágenes fijas se enfoca sólo en una única imagen a la vez. El estándar más conocido y extendido es JPEG.

a) **JPEG:** Con JPEG, la descompresión y visualización pueden efectuarse a partir de navegadores web estándar. La compresión JPEG puede efectuarse a diferentes niveles de compresión definidos por el usuario. Éste nivel de compresión seleccionado está directamente relacionado con la calidad de la imagen solicitada. Además del nivel de compresión, la propia imagen también tiene un impacto en la relación de compresión resultante. Por ejemplo, una pared blanca puede producir un archivo de imagen relativamente pequeño (y una relación de compresión mayor), mientras que el mismo nivel de compresión aplicado a una escena de gran complejidad y entramado producirá un archivo de mayor tamaño con una relación de compresión inferior.

2.4.2. ESTÁNDARES DE COMPRESIÓN DE VIDEO

La comprensión de imágenes de video se enfoca en varias imágenes a la vez. Los estándares más conocidos son:

a) **MOTION JPEG (M-JPEG):** "Motion JPEG" es el estándar utilizado más habitualmente en sistemas de vídeo IP. Una cámara de red, como una cámara digital de imagen fija, capta las imágenes individuales y las comprime en formato JPEG (fig. 8). La cámara IP puede captar y comprimir, por ejemplo, 30 imágenes individuales por segundo (30 ips, imágenes por segundo) y, a continuación, las dispone en una secuencia continua de imágenes a través de una red hasta una estación de visualización. Con una velocidad de imagen de aproximadamente 16 fps y superior, el visualizador percibe una imagen animada

a pantalla completa (“full motion” video). Nos referimos a este método como “Motion JPEG” o M-JPEG. De la misma forma que cada imagen individual es una imagen JPEG completamente comprimida, todas ellas poseen la misma calidad garantizada, que se determina por el nivel de compresión elegido para el servidor de vídeo o cámara IP.

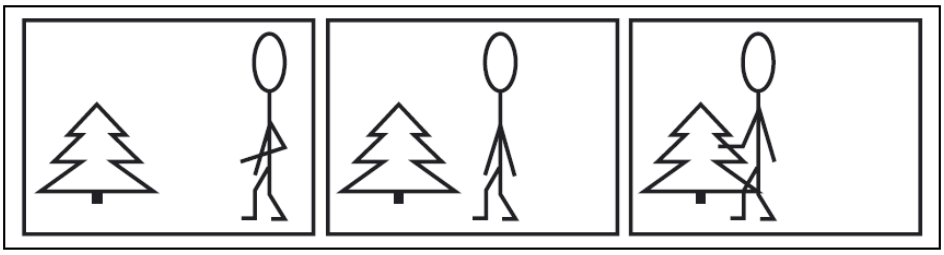


Fig. 8: Ejemplo de una secuencia de tres imágenes JPEG completas

b) H.263: La técnica de compresión H.263 se centra en una transmisión de vídeo con una tasa de bits fija. La desventaja de tener una tasa de bits fija es que cuando un objeto se mueve, la calidad de la imagen disminuye. H.263 fue originalmente diseñado para aplicaciones de videoconferencia y no para aplicaciones de vigilancia donde los detalles son más importantes que una tasa de bits fija.

c) MPEG: Una de las técnicas de transmisión de vídeo y audio más extensamente conocidas es el estándar MPEG. El principio básico de MPEG es la comparación de dos imágenes comprimidas que deben transmitirse a través de la red. La primera imagen comprimida se utiliza como fotograma de referencia y únicamente se envían partes de las siguientes imágenes que son distintas de la imagen de referencia. Seguidamente, la estación de visualización de red reconstruye todas las imágenes basándose en la imagen de referencia y los “datos de diferencias”. El siguiente ejemplo nos dará una mejor idea de ésta técnica de compresión, donde sólo se transmite información sobre las diferencias en el segundo y tercer fotograma (fig. 9).

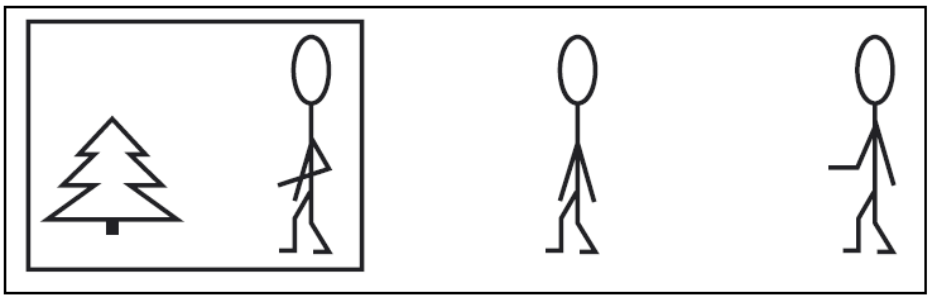


Fig. 9: Ejemplo de una secuencia de 3 imágenes MPEG incompletas

Naturalmente, MPEG es mucho más complejo que lo que se ha descrito anteriormente, y a menudo implica el uso de técnicas adicionales o herramientas para parámetros tales como la predicción de movimiento en una escena y la identificación de objetos. Existen diversos estándares MPEG diferentes:

MPEG-1, MPEG-2, MPEG-4

Donde MPEG-4 es la evolución de MPEG-2. Dispone de muchas más herramientas para reducir la tasa de bits necesaria para lograr cierta calidad de imagen en una aplicación o escena de imágenes determinadas. Además, la velocidad de imagen no se limita a 25/30 ips.

Sin embargo, la mayoría de las herramientas utilizadas para reducir la tasa de bits hoy en día, sólo son relevantes para aquellas aplicaciones que no sean en tiempo real. Esto ocurre porque algunas de las herramientas necesitan una fuerza de procesamiento tan elevada que el tiempo total para codificar y decodificar (el tiempo de espera) las convierte en inservibles para dichas aplicaciones (tiempo real).

La clave está en seleccionar una compresión de vídeo estándar, que garantice una alta calidad de imagen, como M-PEG o MPEG-4.

2.4.3. VENTAJAS E INCONVENIENTES DE “MOTION JPEG”, Y MPEG-4

Debido a su simplicidad, el ampliamente utilizado “Motion JPEG”, representa a menudo una buena elección. Existe un retraso limitado entre la captación de imágenes en una cámara, la codificación, la transferencia a través de la red, la descodificación y finalmente su representación en la estación de visualización. En otras palabras, “Motion JPEG” ofrece un tiempo de espera bajo debido a su simplicidad (compresión de imágenes e imágenes completamente individuales) y, por tanto, también es apto para el procesamiento de imágenes, como en la detección de movimiento o el seguimiento de un objeto.

El sistema garantiza la calidad de la imagen independientemente de su complejidad o movimiento, a la vez que ofrece la flexibilidad para seleccionar una calidad de imagen superior (compresión baja) o una calidad de imagen inferior (compresión alta) obteniendo así ficheros de imagen de tamaño inferior y un uso del ancho de banda y tasa de bits menores. La velocidad de imagen puede ajustarse fácilmente para limitar el uso de ancho de banda, sin perder la calidad de la imagen.

Sin embargo, “Motion JPEG” genera un volumen relativamente grande de datos para ser enviados a través de la red. En cambio, MPEG tiene la ventaja de enviar un volumen de datos menor por unidad de tiempo a través de la red (tasa de bits) en comparación con “Motion JPEG”, excepto en velocidades de imagen bajas.

Si el ancho de banda de red disponible se encuentra limitado o si el video debe grabarse a una velocidad de imagen elevada y existen limitaciones en el espacio de almacenamiento, MPEG puede ser la opción más adecuada.

Las exigencias de ancho de banda inferiores exigen una complejidad de codificación y decodificación mayor, que a la vez contribuye a un tiempo de espera más elevado en comparación con “Motion JPEG”. Otro punto que hay que tener en cuenta es que tanto MPEG-2 como MPEG-4 están sujetos a derechos de licencia. En la fig. 10 se muestra cómo se compara el uso de ancho de banda entre “Motion JPEG” y MPEG-4 en una escena de imágenes con movimiento.

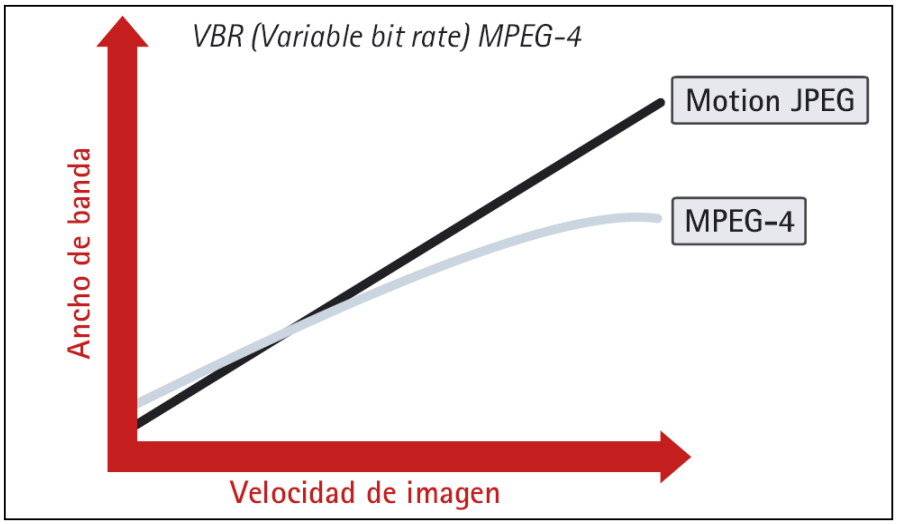


Fig. 10: Comparación del ancho de banda entre JPEG y MPEG-4
(D-Link Distribuidor)

Es obvio que a velocidades de imagen inferiores, donde la compresión MPEG-4 no puede utilizar similitudes entre fotogramas vecinos a un grado superior y, debido a la sobrecarga generada por el formato de transmisión de MPEG-4, el consumo de ancho de banda es similar al de "Motion JPEG". A velocidades de imagen superiores, MPEG-4 exige menos ancho de banda que "Motion JPEG".

2.4.4. RESOLUCIÓN MEGAPÍXEL

Cuanta más alta sea la resolución, más detalles pueden observarse en una imagen. Esto es un punto muy importante en las aplicaciones de vigilancia por vídeo, donde una imagen de alta resolución puede permitir la identificación de un delincuente. La resolución máxima en NTSC y PAL, en cámaras analógicas, después de que la señal de vídeo se haya digitalizado en un DVR o en un servidor de video, es de 400.000 píxeles (704x576 = 405.504). 400.000 equivale a 0,4 mega píxeles.

A pesar de que la industria del video vigilancia ha logrado siempre vivir con estas limitaciones, la nueva tecnología de cámaras IP hace posible hoy en día una resolución mayor. Un formato mega píxel común es 1.280 x 1.024, que ofrece una resolución de 1,3 mega píxeles, 3 veces más que en las cámaras analógicas. Las cámaras con 2 mega

píxeles y 3 mega píxeles también se encuentran disponibles, e incluso se esperan resoluciones superiores en el futuro.

2.5.CONSIDERACIONES SOBRE LA CÁMARA

Se deben aplicar algunas reglas básicas al buscar maximizar el rendimiento de un sistema de vídeo IP, a continuación veremos algunas reglas para la elección de los componentes de la cámara, la posición e instalación de la cámara y factores a tener en cuenta con tal de lograr el mejor detalle y calidad de imagen posibles, tanto en el interior como en el exterior.

2.5.1. TIPOS DE CÁMARAS

Si el sistema de vigilancia por vídeo que se va a instalar es un sistema nuevo y no existe ninguna cámara analógica, la mejor elección en la mayoría de casos es utilizar cámaras IP, que se encuentran disponibles en diversos modelos que satisfacen una amplia variedad de necesidades. Con esta gran variedad de cámaras IP disponibles en la actualidad, se cumplen la mayoría de requisitos de todos los mercados verticales y tamaños del sistema. Las cámaras IP se presentan en diferentes modelos: Cámaras IP fijas, Cámaras IP Domo fijas, Cámaras IP PTZ, Cámaras IP Domo, Cámaras IP PTZ no mecánicas.

Se encuentran disponibles diversas variaciones de los tipos de cámaras descritos anteriormente, entre las que se incluyen:

- Versiones a prueba de agresiones, en función de la carcasa de protección que se use.
- Versiones resistentes a las condiciones climáticas, en función de la carcasa de protección que se use.
- Versiones de visión diurna/nocturna, lo que significa que la cámara puede cambiar automática o manualmente entre modo diurno con video en color y modo nocturno con imágenes en blanco y negro en situaciones de poca luz que pueden mejorarse usando iluminadores de infrarrojos.

Una vez se ha seleccionado la cámara, el próximo paso es elegir las carcasas y objetivos adecuados. También se debería tener en cuenta un número de ensayos comunes relacionados con la posición de la cámara, que ayudarán a obtener la mejor calidad del sistema.

2.5.2. TAMAÑO DEL SENSOR

Los sensores de imagen están disponibles en diferentes tamaños, tales como 2/3”, 1/2”, 1/3” y 1/4”, los objetivos se fabrican para adaptarse a estos tamaños. Es importante seleccionar un objetivo apto para la cámara. Un objetivo hecho para un sensor de 1/2” funcionará con sensores de 1/2”, 1/3”, y 1/4”, pero nunca con un sensor de 2/3” pues este sensor no fue construido para este objetivo y por lo tanto no podrá adaptarse al mismo.

2.5.3. TIPOS DE OBJETIVOS

a) **Lente fija.** La longitud focal es fija, p. ej., 4 mm (fig. 11)

Fig. 11: Lente fija

b) **Lente varifocal.** Esta lente permite el ajuste manual de la longitud focal (campo de visualización). Cuando la longitud focal se cambia, el objetivo tiene que volver a enfocarse. El tipo más común es 3,5-8 mm (fig. 12).

Fig. 12: Lente varifocal

c) **Lente de zoom.** La longitud focal puede ajustarse dentro de un rango, p. ej., de 6 a 48 mm, sin afectar el enfoque. El objetivo puede ser manual o motorizado, para que pueda ser controlado de forma remota.

2.5.4. IRIS

Generalmente, las cámaras IP controlan la cantidad de luz que pasa al mecanismo de imagen a través del iris o ajustando el tiempo de exposición a diferencia de las cámaras convencionales, que el tiempo de exposición es fijo.

El papel del iris es el de ajustar la cantidad de luz que pasa a través del objetivo. Existen diferentes tipos de iris en los objetivos.

a) **Control de iris manual:** El iris en un objetivo de iris manual se configura normalmente cuando se instala la cámara para adaptarse a las condiciones de luz reinantes. Estos objetivos no pueden reaccionar ante cambios en la iluminación del lugar, por tanto el iris se ajusta a un valor “medio”, que se usa en condiciones de luz variable.

b) **Control automático:** Para situaciones exteriores, y donde la iluminación de la escena está cambiando constantemente, se prefiere un objetivo con un iris ajustable automáticamente. La apertura del iris está controlada por la cámara y está constantemente cambiando para mantener el nivel de luz óptimo para el sensor de imagen.

Los objetivos con iris automático *son los más recomendados* para aplicaciones exteriores. El iris ajusta automáticamente la cantidad de luz que alcanza la cámara y ofrece los resultados mejores, así como una protección del sensor de imagen ante el exceso de luz.

Un diámetro de iris pequeño reduce la cantidad de luz, ofreciendo una profundidad de campo mejor (enfoque a una distancia mayor). Un diámetro de iris grande, por otra parte, ofrece imágenes mejores en situaciones de luz escasa.

En escenas con luz limitada, se recomienda acoplar un filtro de densidad neutral delante del objetivo. Esto hace reducir la cantidad de luz que entra en el objetivo uniformemente a lo largo de todo el espectro visible y obliga al iris a abrirse completamente para compensar. Muchas cámaras IP ofrecen hoy en día un control de iris automático para garantizar que la imagen continúe siendo nítida a lo largo de todo el año y horas del día, ya que los niveles de luz cambian constantemente.

Si se va a instalar una cámara en exteriores o en entornos relativamente hostiles, necesita una carcasa impermeable y a prueba de agresiones para protegerla. Las carcasas para cámaras se presentan en diversos tamaños y calidades y algunas versiones disponen de ventiladores para su refrigeración y/o calefactores integrados.

Para obtener imágenes de alta calidad de una cámara, deben aplicarse unas cuantas reglas básicas. Dichas reglas se aplican por igual tanto a las cámaras IP como a cualquier otro tipo de cámara. Para obtener buenas imágenes hay que tener presente algunos aspectos importantes.

2.5.5. USAR GRAN CANTIDAD DE LUZ

La razón más habitual de que las imágenes tengan baja calidad es la falta de luz. Generalmente, cuanta más luz haya mejores serán las imágenes. Con poca luz, las imágenes se vuelven borrosas y de color mate por eso que algunos fotógrafos profesionales siempre usan lámparas de alta intensidad. El Lux es la unidad estándar para la medición de la cantidad de luz, se necesitan como mínimo 200 Lux para captar

imágenes de buena calidad. Una cámara de alta calidad puede ajustarse para que funcione a 1 Lux. Esto significa que una imagen puede ser captada a 1 Lux, pero no quiere decir que sea buena.

Deben evitarse las zonas brillantes en las imágenes (evitar el contraluz). Las imágenes brillantes pueden sobre exponerse (blanco brillante) y en consecuencia los objetos pueden aparecer demasiado oscuros. Este problema ocurre normalmente al intentar captar un objeto desde detrás de una ventana.

a) **Reducir el contraste:** La cámara ajusta la exposición para obtener un nivel medio de luz en la imagen. Al intentar captar una imagen de una persona que permanece de pie delante de una pared blanca, la persona generalmente suele aparecer demasiado oscura. Este problema se puede solucionar fácilmente si el color de fondo se sustituye por gris en lugar de blanco.

2.6. RECOMENDACIONES PARA EL MONTAJE DE UNA CÁMARA EN EL EXTERIOR

2.6.1. OBJETIVOS

Para las aplicaciones en el exterior, se debería utilizar un objetivo con iris automático. Un objetivo con iris automático ajusta automáticamente la cantidad de luz que llega al sensor de imagen, lo que optimiza la calidad de la imagen y protege el sensor contra los daños causados por la luz solar intensa.

2.6.2. LUZ SOLAR DIRECTA

Es importante aclarar que debe evitarse siempre el exponer una imagen a la luz solar directa ya que “deslumbrará” a la cámara y blanqueará de forma permanente los pequeños filtros de color del chip sensor. Si es posible, la cámara debería colocarse mirando en la misma dirección que el sol.

2.6.3. CONTRASTE

Visualizar una porción demasiado grande del cielo produce demasiado contraste. La cámara se ajustará a fin de lograr un nivel de luz adecuado para el cielo. En consecuencia, el objeto o paisaje enfocado aparecerá demasiado oscuro. Una forma de solucionar este problema es montar la cámara a gran distancia del suelo, usando un poste si fuera necesario. Siempre debería utilizarse un equipo de fijación resistente para evitar las vibraciones causadas por el viento fuerte.

2.6.4. REFLEJOS

Si la cámara se monta detrás de un cristal como, por ejemplo, en una carcasa, el objetivo deberá colocarse cerca del cristal. En caso contrario, los reflejos de la cámara y el fondo aparecerán en la imagen. Para reducir los reflejos, pueden aplicarse recubrimientos especiales a cualquier cristal que se use delante del objetivo.

2.6.5. ILUMINACIÓN

Cuando se usan cámaras por la noche, se puede necesitar una iluminación externa adicional. Esto debería prepararse para evitar reflejos y/o sombras. Para la seguridad encubierta, en lugar de la iluminación normal se pueden utilizar iluminadores de infrarrojos (IR), conocidos como “luz blanca”. La luz IR es imperceptible, lo que significa que aunque sea suficiente para captar imágenes desde cámaras IR, no es visible para el ojo humano. Es posible conectar cámaras IP sensibles a infrarrojos directamente a la red, o bien, conectar cámaras sensibles a infrarrojos tradicionales a la red a través de un servidor de vídeo.

Las cámaras a color no funcionan con luz infrarroja. Algunas cámaras pueden cambiar automáticamente entre un modo de color diurno y un modo IR adecuado para la visión nocturna donde la imagen aparecerá en blanco y negro de alta calidad.

CAPÍTULO 3

SISTEMAS INTEGRADOS, PROTOCOLO TCP/IP

La tendencia del mercado informático y de las comunicaciones se orienta en un claro sentido: unificación de recursos. Cada vez, ambos campos, comunicaciones e informática, se encuentran más vinculados, es necesario, implementar un protocolo adecuado y utilizar el cableado correcto para poder obtener una comunicación confiable y eficaz, para que el software a utilizar no tenga dificultades y funcione correctamente.

Hoy en día, el protocolo de Internet (IP) constituye el protocolo de comunicación informática más ampliamente utilizado. Es el protocolo básico empleado para la comunicación por Internet, como el correo electrónico, web y multimedia. Una de las razones de la aceptación de este protocolo es su escalabilidad, es decir, funciona perfectamente tanto en instalaciones muy pequeñas como en instalaciones muy grandes y es compatible con una gama cada vez más amplia de tecnologías y equipos de gran rendimiento, bajo costo y eficacia.

Las nuevas tecnologías, el ingreso de la informática en forma masiva en las actividades comerciales, administrativas y profesionales han dado lugar a la necesidad de nuevos cableados interiores que presenten una mayor confiabilidad en la transmisión de los datos y la voz. Este nuevo sistema de cableado se lo llama estructurado.

3.1. RED

Cuando se pretende unir entre sí un gran número de usuarios o dispositivos, resulta difícil por cuestiones fundamentalmente económicas la unión de todos con todos de forma directa. Por tanto, para conseguir un número importante de usuarios se establece

una red de comunicación que permita compartir los correspondientes recursos y así, el costo disminuirá y su utilización tendrán un mayor avance.

Una red de ordenadores es un sistema de comunicación de datos que enlaza dos o más ordenadores y dispositivos o periféricos (fig. 13).

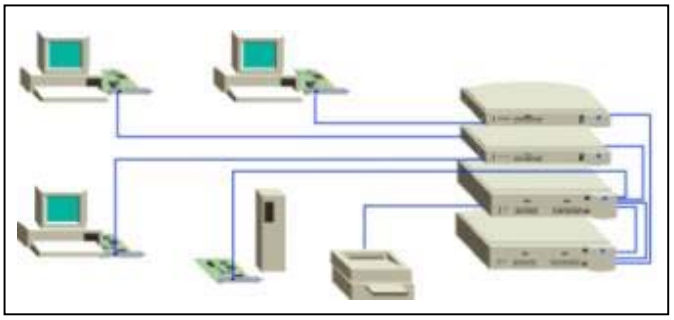


Fig. 13: Red de ordenadores (Cisco)

De entre las varias tecnologías de red, las más común es Ethernet. Una red puede estar basada en esta u otra tecnología.

3.1.1. CLASIFICACIÓN

Una red se clasifica dependiendo de su *extensión* y su *topología.*

3.1.1.1. EXTENSIÓN: Por su extensión una red puede ser:

- **LAN (*"Local Area Network"*):** Conjunto de elementos físicos y lógicos que proporcionan interconexión en un área privada y restringida. Por lo tanto, tiene entre otras las siguientes características:
    - Restricción geográfica: tiene el ámbito de una oficina, la planta de un edificio, un campus universitario... dependiendo de la tecnología con la que esté construido. La velocidad de transmisión debe ser relativamente elevada.
    - Debe ser privada: Toda la red debe pertenecer a la misma organización.
    - Fiabilidad en las transmisiones: la tasa de error debe ser muy baja, por lo que son redes muy seguras.

En cuanto a la funcionalidad de una LAN, ésta debe proporcionar los servicios de comunicación más comunes: estos se refieren a compartir recursos por parte de los usuarios de la red.

- **MAN (*"Metropolitan Area Network"*):** Las redes metropolitanas siguen estándares entre las LAN y la WAN. Una MAN es una red de distribución de datos para un área geográfica en el entorno de una ciudad; por ejemplo, en un polígono industrial.

  Su tasa de error es intermedia entre LAN y WAN. Es menor que en una LAN pero no llega a los niveles de una WAN; por ejemplo, Televisión por cable.

  Funcionalidad: El IEEE ha propuesto la norma 802.6 como estándar para este tipo de redes. Esta normativa propuso inicialmente velocidades de transferencia desde 34 Mb/s hasta 155 Mb/s.

- **WAN (*"Wide Area Network"*):** Redes de área extensa o extendida. Es una red que intercomunica equipos en un área geográfica muy extensa. Las líneas de transmisión que utilizan son normalmente propiedad de las compañías telefónicas. La capacidad de transmisión de estas líneas suele ser menor que las de una LAN; por ejemplo:

  - La RDSI,
  - los bancos,
  - Infovía,

  Funcionalidad de una WAN: Los protocolos de la WAN pueden estar o no orientados a la conexión. Es decir, según el protocolo y servicio solicitado habrá que efectuar una llamada. En general la mayor parte de los servicios proporcionados por las WAN son distribuidos; además, estas redes pueden interconectar redes de área local de tipos muy distintos, por ejemplo:

  - Infovía,
  - Redes de "frame relay",
  - Redes ATM.

3.1.1.2. TOPOLOGIA:

Los nodos de red (las computadoras), necesitan estar conectados para comunicarse. A la forma en que están conectados los nodos se le llama topología. Una red tiene dos diferentes topologías: una física y una lógica. La topología física es la disposición física actual de la red, la manera en que los nodos están conectados unos con otros. La topología lógica es el método que se usa para comunicarse con los demás nodos, la ruta que toman los datos de la red entre los diferentes nodos de la misma. Las topologías físicas y lógicas pueden ser iguales o diferentes. Las topologías de red más comunes son: bus, anillo, estrella y malla.

- ***Red en Bus:*** En una topología de bus (fig. 14), cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir, un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de la misma. El cable puede ir por el piso, por las paredes, por el techo, o puede ser una combinación de éstos, siempre y cuando el cable sea un segmento continuo.

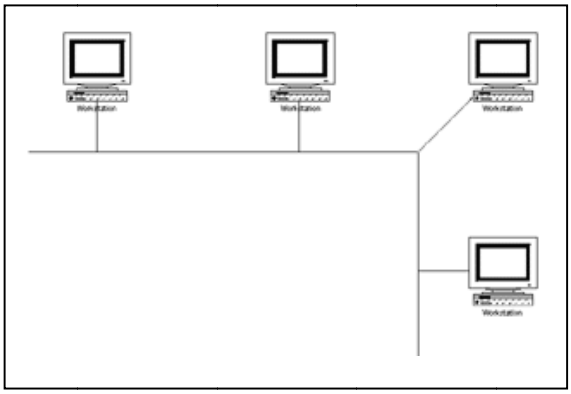


Fig. 14: Red en Bus

- ***Red en anillo:*** Una topología de anillo consta de varios nodos unidos formando un círculo lógico (fig. 15). Los mensajes se mueven de nodo a nodo en una sola dirección. Algunas redes de anillo pueden enviar mensajes en forma bidireccional, no obstante, sólo son capaces de enviar mensajes en una dirección cada vez. La topología de anillo permite verificar si se ha recibido un mensaje. En una red de anillo, las estaciones de trabajo envían un paquete de datos conocido como flecha o contraseña de paso.

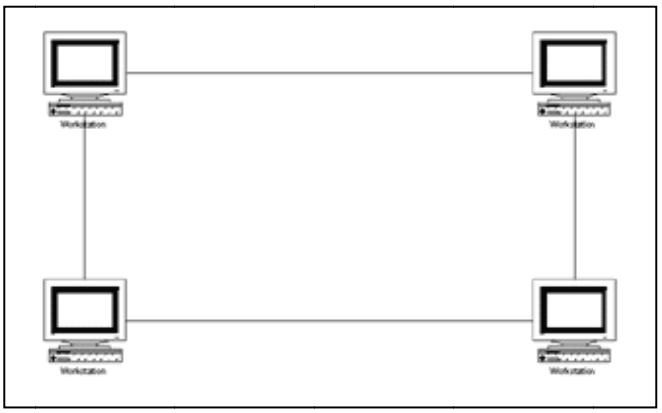


Fig. 15: Red en Anillo

- ***Red en estrella:*** Uno de los tipos más antiguos de topologías de redes es la estrella (fig. 16), la cual usa el mismo método de envío y recepción de mensajes que un sistema telefónico, ya que todos los mensajes de una topología LAN en estrella deben pasar a través de un dispositivo central de conexiones conocido como concentrador de cableado, el cual controla el flujo de datos.

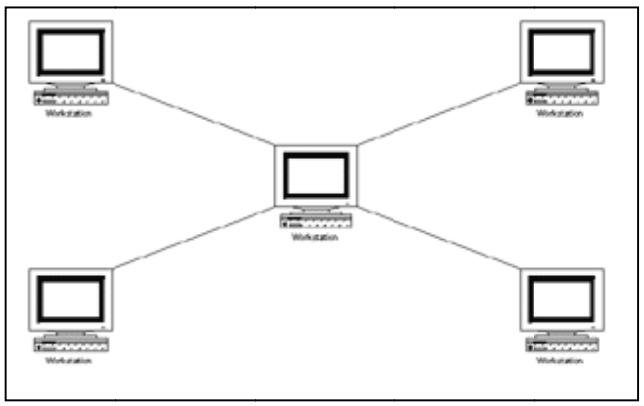


Fig. 16: Red en Estrella

3.1.2. PROTOCOLOS DE COMUNICACIÓN

Los protocolos son reglas y procedimientos para la comunicación. El término «protocolo» se utiliza en distintos contextos. Por ejemplo, los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma forma se aplican las reglas del protocolo al entorno informático. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.

Antes de decidir qué protocolo se utilizará, se debe tener presente que:

- Hay muchos protocolos. A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.

- Algunos protocolos sólo trabajan en ciertos niveles OSI. El nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red (NIC) y salgan al cable de la red.

- Los protocolos también puede trabajar juntos en una jerarquía o conjunto de protocolos. Al igual que una red incorpora funciones a cada uno de los niveles del modelo OSI, distintos protocolos también trabajan juntos a distintos niveles en la jerarquía de protocolos. Los niveles de la jerarquía de protocolos corresponden a los niveles del modelo OSI. Por ejemplo, el nivel de aplicación del protocolo TCP/IP corresponde al nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

La operación técnica en la que los datos son transmitidos a través de la red se puede dividir en dos pasos, discretos y sistemáticos. En cada paso se realizan ciertas acciones que no se pueden realizar en otro paso. Cada paso incluye sus propias reglas y procedimientos o protocolo.

Los pasos del protocolo se tienen que llevar a cabo en un orden apropiado y tiene que ser el mismo en cada una de los equipos de la red. En el equipo origen, estos pasos se tienen que realizar de arriba hacia abajo. En el equipo de destino, estos pasos se tienen que realizar de abajo hacia arriba, por ejemplo:

- Los protocolos en el equipo origen:

    1. Los datos se dividen en secciones más pequeñas, denominadas paquetes, que puede manipular el protocolo.
    2. Se añade a los paquetes información sobre la dirección, de forma que el equipo de destino pueda determinar si los datos le pertenecen.
    3. Prepara los datos para la transmisión a través de la NIC y enviarlos a través del cable de la red.

- Los protocolos en el equipo de destino constan de la misma serie de pasos, pero en sentido inverso.

    1. Toma los paquetes de datos del cable.
    2. Introducen los paquetes de datos en el equipo a través de la NIC.
    3. Extrae de los paquetes de datos toda la información transmitida eliminando la información añadida por el equipo origen.
    4. Copia los datos de los paquetes en un búfer para reorganizarlos.
    5. Pasa los datos reorganizados a la aplicación en una forma utilizable.

Los equipos origen y destino necesitan realizar cada paso de la misma forma para que los datos tengan la misma estructura al recibirse que cuando se enviaron.

3.1.2.1. MODELO OSI

La ISO (Organización Internacional de Normalización) en 1977 desarrolla una estructura de normas comunes dentro de las redes, estas normas se conocen como el *"Modelo de Referencia OSI (Interconexión de Sistemas Abiertos)",* modelo bajo el cual empezaron a fabricarse computadoras con la capacidad de comunicarse con otras computadoras de marcas diferentes. Este modelo está basado en el principio de Julio César: *"DIVIDE Y VENCERAS"* y está pensado para las redes del tipo WAN. Se diseñan redes como una secuencia de capas, cada una construida sobre la anterior, las capas se dividen en dos grupos:

- Servicios de transporte (niveles 1, 2, 3 y 4).
- Servicios de soporte al usuario (niveles 5, 6 y 7).

El modelo OSI no es un estándar de comunicaciones ya que es un lineamiento funcional para las tareas de comunicaciones, sin embargo muchos estándares y protocolos cumplen con el lineamiento del modelo.

La estructura del modelo OSI se puede resumir en 5 partes:

A. Se diseña una estructura multinivel con idea de que cada nivel resuelva solo una parte del problema de la comunicación, con funciones especificas.

B. Cada nivel se comunica con su homólogo en las otras máquinas, usando un mensaje a través de los niveles inferiores de la misma. La comunicación entre niveles se define de manera que un nivel N utilice los servicios del nivel N-1 y proporciona servicios al nivel N+1.

C. Entre los diferentes niveles existen interfaces llamadas “Puntos de Acceso” a los servicios.

D. Cada nivel es dependiente del nivel inferior como así también lo es del nivel superior.

E. En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel de la computadora receptora se entere de que la computadora emisora le está enviando un mensaje con información.

Cualquier nivel puede incorporar un encabezado al mensaje. Por esta razón se considera que un mensaje está constituido de dos partes, el *encabezado* y la *información.* La incorporación de encabezados al ser necesarios implica un lote extra de información, o sea, un mensaje corto puede ser voluminoso, pero no obstante, la computadora receptora retira los encabezados en orden inverso a como se enviaron desde la computadora emisora, el mensaje original no se afecta.

Siete Capas: El modelo OSI es conocido porque ofrece una explicación sencilla de la relación entre los complejos componentes de hardware y de protocolo de red. En el modelo OSI, la capa inferior corresponde al hardware y las capas sucesivas al software que usa la red.

El software de red, consiste en programas informáticos que establecen protocolos, o normas, para que las computadoras se comuniquen entre sí. Estos protocolos se aplican enviando y recibiendo grupos de datos formateados denominados paquetes. Los protocolos indican cómo efectuar conexiones lógicas entre las aplicaciones de la red, dirigir el movimiento de paquetes a través de la red física y minimizar las posibilidades de colisión entre paquetes enviados simultáneamente (Tabla 1).

3.1.2.2. MODELO TCP/IP

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el "*Protocolo de control de transmisión/Protocolo Internet (TCP/IP)"*.

7	APLICACIÓN	Se entiende directamente con el usuario final, al proporcionarle el servicio de información distribuida para soportar las aplicaciones y administrar las comunicaciones por parte de la capa de presentación.
6	PRESENTACIÓN	Permite a la capa de aplicación interpretar el significado de la información que se intercambia. Esta realiza las conversiones de formato mediante las cuales se logra la comunicación de dispositivos.
5	SESIÓN	Administra el diálogo entre las dos aplicaciones en cooperación mediante el suministro de los servicios que se necesitan para establecer la comunicación, flujo de datos y conclusión de la conexión.
4	TRANSPORTE	Esta capa proporciona el control de extremo a extremo y el intercambio de información con el nivel que requiere el usuario. Representa el corazón de la jerarquía de los protocolos que permite realizar el transporte de los datos en forma segura y económica.
3	RED	Proporciona los medios para establecer, mantener y concluir las conexiones conmutadas entre los sistemas del usuario final. Por lo tanto, la capa de red es la más baja, que se ocupa de la transmisión de extremo a extremo.
2	ENLACE	Asegura con confiabilidad del medio de transmisión, ya que realiza la verificación de errores, retransmisión, control fuera del flujo y la secuenciación de capacidad que se utiliza en la capa de red.
1	FÍSICO	Se encarga de las características eléctricas, mecánicas, funcionales y de procedimiento que se requieren para mover los bits de datos entre cada extremo del enlace de la comunicación.

Tabla 1: Capas del modelo OSI

El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de

la luz. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware, proporcionando una abstracción total del medio.

El TCP/IP es la base de Internet, y sirve para comunicar todo tipo de dispositivos, computadoras que utilizan diferentes sistemas operativos, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

EL MODELO TCP/IP está compuesto por cuatro capas o niveles, cada nivel se encarga de determinados aspectos de la comunicación y a su vez brinda un servicio específico a la capa superior. Estas capas son:

- Aplicación,
- Transporte,
- Internet, y
- Acceso a la Red.

Algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI (Tabla 2). Resulta fundamental no confundir las funciones de las capas de los dos modelos ya que si bien tienen aspectos en común, estas desempeñan diferentes funciones en cada modelo.

MODELO TCP/IP	**MODELO OSI**
Aplicación	Aplicación
	Presentación
	Sesión
Transporte	Transporte
Internet	Red
Acceso a la red	Enlace de datos
	Física

Tabla 2: Comparación entre los modelos TCP/IP y OSI

A. Capa de Acceso a la Red: También denominada capa de host de red. Esta es la capa que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico

real con los medios de la red. Esta capa incluye los detalles de la tecnología LAN y WAN y todos los detalles de las capas, física y de enlace de datos del modelo OSI.

Los controladores para las aplicaciones de software, las tarjetas de módem y otros dispositivos operan en la capa de acceso de red. La capa de acceso de red define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión. Los estándares del protocolo de los módem tales como el Protocolo Internet de enlace serial (SLIP) y el Protocolo de punto a punto (PPP) brindan acceso a la red a través de una conexión por módem. La mayoría de los protocolos reconocibles operan en las capas de transporte y de Internet del modelo TCP/IP.

La capa de Acceso a la Red tiene como funciones:

- la asignación de direcciones IP a las direcciones físicas,
- el encapsulamiento de los paquetes IP en tramas.

Basándose en el tipo de hardware y la interfaz de la red, la capa de acceso de red definirá la conexión con los medios físicos de la misma.

B. Capa de Internet: Esta capa tiene como propósito seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el Protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes ocurre en esta capa. Existen diferentes tipos de protocolos que operan en esta capa:

- **IP** proporciona un enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. El IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta de hacia el destino.
- **ICMP**, Protocolo de mensajes de control en Internet suministra capacidades de control y envío de mensajes.
- **ARP**, Protocolo de resolución de direcciones determina la dirección de la capa de enlace de datos, la dirección MAC, para las direcciones IP conocidas.
- **RARP**, Protocolo de resolución inversa de direcciones determina las direcciones IP cuando se conoce la dirección MAC.

Las funciones del Protocolo IP son:

- Define un paquete y un esquema de direccionamiento,
- Transfiere los datos entre la Capa Internet y las Capas de Acceso a la Red,
- Enruta los paquetes hacia los “hosts” remotos.

A veces, se considera a IP como protocolo poco confiable. Esto no significa que IP no enviará correctamente los datos a través de la red. Llamar al IP, protocolo poco confiable simplemente significa que IP no realiza la verificación y la corrección de los errores. De esta función se encarga TCP, es decir el protocolo de la capa superior ya sea desde las capas de transporte o aplicación.

C. **Capa de Transporte:** La capa de transporte proporciona servicios de transporte desde el host origen hacia el host destino. En esta capa se forma una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor. Los protocolos de transporte segmentan y re-ensamblan los datos mandados por las capas superiores en el mismo flujo de datos, o conexión lógica entre los extremos. La corriente de datos de la capa de transporte brinda transporte de extremo a extremo.

La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube (internet). El control de punto a punto, que se proporciona con las ventanas deslizantes y la confiabilidad de los números de secuencia y acuses de recibo, es el deber básico de la capa de transporte cuando utiliza TCP. La capa de transporte también define la conectividad de extremo a extremo entre las aplicaciones de los hosts. Los servicios de transporte incluyen los siguientes servicios Protocolos TCP y UPD):

- Segmentación de los datos de capa superior.
- Envío de los segmentos desde un dispositivo en un extremo a otro dispositivo en otro extremo.

Entre las características del protocolo TCP tenemos:

- Establecimiento de operaciones de punto a punto.
- Control de flujo proporcionado por ventanas deslizantes.
- Confiabilidad proporcionada por los números de secuencia y los acuses de recibo.

Se dice que internet es una nube, por que los paquetes pueden tomar múltiples rutas para llegar a su destino, generalmente los saltos entre “routers” se representan con una nube que representa las distintas posibles rutas. La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube. La nube maneja los aspectos tales como la determinación de la mejor ruta, balanceo de cargas, etc.

D. Capa de Aplicación: La capa de aplicación del modelo TCP/IP maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y asegura que estos datos estén correctamente empaquetados antes de que pasen a la capa siguiente. TCP/IP incluye no sólo las especificaciones de Internet y de la capa de transporte, tales como IP y TCP, sino también las especificaciones para aplicaciones comunes. TCP/IP tiene protocolos que soportan la transferencia de archivos, e-mail, y conexión remota, además de los siguientes:

- **a. FTP** (Protocolo de transferencia de archivos): es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten la transferencia FTP. Permite las transferencias bidireccionales de archivos binarios y archivos ASCII.
- **b. TFTP** (Protocolo trivial de transferencia de archivos): es un servicio no orientado a conexión que utiliza el Protocolo de datagrama de usuario (UDP). Es útil en algunas LAN porque opera más rápidamente que FTP en un entorno estable.
- **c. NFS** (Sistema de archivos de red): es un conjunto de protocolos para un sistema de archivos distribuido, desarrollado por “Sun Microsystems” que permite acceso a los archivos de un dispositivo de almacenamiento remoto, por ejemplo, un disco rígido a través de una red.
- **d. SMTP** (Protocolo simple de transferencia de correo): administra la transmisión de correo electrónico a través de las redes informáticas. No admite la transmisión de datos que no sea en forma de texto simple.
- **e. TELNET** (Emulación de terminal): Telnet tiene la capacidad de acceder de forma remota a otro computador. Permite que el usuario se conecte a un host de

Internet y ejecute comandos. El cliente de Telnet recibe el nombre de host local. El servidor de Telnet recibe el nombre de host remoto.

f. **SNMP** (Protocolo simple de administración de red): es un protocolo que provee una manera de monitorear y controlar los dispositivos de red y de administrar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad.

g. **DNS** (Sistema de denominación de dominio): es un sistema que se utiliza en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones IP.

3.2. ETHERNET

En las empresas de hoy en día, lo más probable es que sus computadores utilicen una red TCP/IP conectados a través de una red Ethernet. La mayoría de ordenadores modernos se suministran con una interfaz Ethernet integrada o permiten alojar fácilmente una tarjeta de interfaz de red Ethernet (NIC, “Network Interface Card”).

Entre los tipos de Ethernet más comunes tenemos:

- ***10 Mbit/s (10 Mbps) Ethernet:*** Este estándar es escasamente usado en las redes actuales de producción debido a su baja capacidad, y ha sido sustituido por Ethernet 100 Mbit/s. La topología más habitual para Ethernet 10 Mbit/s es 10BaseT, y utiliza 4 cables (dos pares trenzados) en un cable cat. 3 ó cat. 5. Un “hub” o “switch” se encuentra en el centro y posee un puerto para cada nodo. Se emplea la misma configuración para “Fast Ethernet” y para “Gigabit Ethernet”.

- ***Fast Ethernet (100 Mbit/s):*** Con tasas de transferencia de datos de hasta 100 Mbit/s, Fast Ethernet es el tipo de Ethernet más utilizado en las redes informáticas actuales. El estándar principal se llama 100BaseT. Aunque es más actual y rápido que Ethernet 10 Mbit, es idéntico en todos los otros aspectos. El estándar 100BaseT puede subdividirse en:

    - 100BASE-TX: Utiliza cableado de cobre de par trenzado (cat. 5).
    - 100BASE-FX: Ethernet 100 Mbit/s a través de fibra óptica.

Como dato importante, cabe mencionar que la mayoría de los "swithches" de red 100 Mbit admiten 10 y 100 Mbits para garantizar una compatibilidad con versiones anteriores, por tal motivo es llamado "*switch" de red 10/100*.

- ***Gigabit Ethernet (1000 Mbit/s):*** Este es el estándar actual recomendado por los distribuidores de equipos de redes para los ordenadores de sobremesa. Sin embargo, en la actualidad se emplean más frecuentemente para las redes troncales entre los servidores de red y los conmutadores de red por la gran velocidad de transmisión que presta. Usa como medios de transmisión cableado de cobre cat. 5 y cat. 6, fibra óptica monomodo y multimodo, donde la fibra de modo único cubre distancias de hasta 100km, que hace ver que es una solución para cubrir grandes distancias.

3.3. ALIMENTACIÓN A TRAVÉS DE ETHERNET

La alimentación a través de Ethernet *(Power over Ethernet, PoE)* es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red usando el mismo cable que se utiliza para una conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones de la cámara y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana. "Power over Ethernet" se regula en una norma denominada IEEE 802.3af y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos preexistentes que no sean compatibles. Esta característica permite a los usuarios mezclar en la red con total libertad y seguridad dispositivos preexistentes con dispositivos compatibles con PoE.

Éste estándar proporciona una alimentación de hasta 15,4 W en el lado del conmutador o "midspan", lo que se traduce en un consumo eléctrico máximo de 12,9 W en el lado del dispositivo/cámara, haciendo que resulte perfecto para cámaras de interior. Las cámaras de exterior así como las cámaras domo y PTZ poseen un consumo eléctrico superior a éste, por lo que la funcionalidad PoE resulta menos adecuada. Algunos fabricantes ofrecen también productos patentados que no son estándar y que proporcionan un suministro adecuado para esas

aplicaciones, aunque debería tenerse en cuenta que, al tratarse de productos no estándar, no es posible una interoperabilidad entre marcas distintas.

PoE funciona a través de un cableado de red estándar, es decir, cat 5, para suministrar alimentación directamente desde los puertos de datos a los que están conectados los dispositivos de red. Hoy en día, la mayoría de los "switches" de red vienen con soporte PoE incorporado, pero si se dispone de una estructura de red/conmutador existente, se puede obtener este beneficio añadiendo al "switch", un "Midspan", que añadirá alimentación al cable de red.

Todas las cámaras de red que no disponen de PoE incorporado, pueden integrarse en un sistema PoE usando un "Active Splitter". En la figura 17 se observa como la cámara IP recibe alimentación a través de un cable de red y es capaz de seguir funcionando cuando se produce un fallo eléctrico.

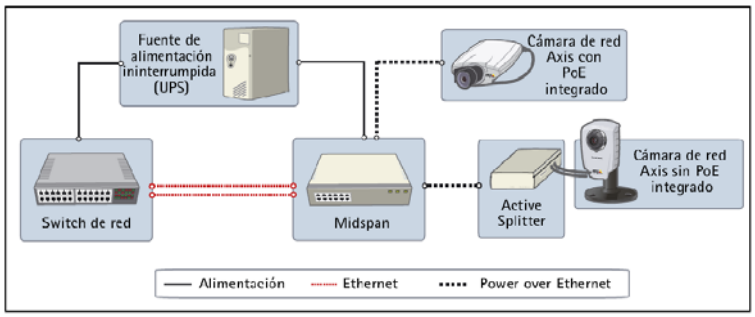


Fig. 17: Conexión a la red de una cámara IP con PoE. (Cisco)

3.4. REDES INALÁMBRICAS

Aunque en la actualidad las redes con cables están presentes en la mayoría de los edificios, en algunas ocasiones una solución sin cables es muy apreciada por el usuario, tanto desde el punto de vista económico como funcional. Son muy usadas en edificios, donde no es posible la instalación de cables sin dañar el interior, o bien, en una instalación donde sea necesario trasladar la cámara a otras ubicaciones de forma regular sin tener que añadir nuevos cables cada vez, como en los comercios. Otro uso habitual de la tecnología inalámbrica es unir dos edificios o lugares sin tener que realizar trabajos complejos y caros en la infraestructura de los edificios.

La tecnología inalámbrica existe tanto para los sistemas de vídeo IP como para los analógicos. Existen dos categorías principales para las comunicaciones inalámbricas:

- LAN Inalámbrica, y
- Acceso Inalámbrico de Banda Ancha.

3.4.1. LAN inalámbrica (también conocida como WLAN): Por definición, una LAN es una Red de Área Local, es decir, cubre distancias cortas y normalmente interiores. Hoy en día, los estándares LAN inalámbricos están bien definidos y los dispositivos de distintos distribuidores funcionan bien juntos.

Cuando es necesario conectar edificios o lugares con enlaces de alta velocidad, se precisará un enlace de datos punto a punto con capacidad para distancias largas y velocidades altas. Dos tecnologías utilizadas habitualmente son el microondas y el láser y las normas utilizadas para la conexión son:

- **Norma 802.11a:** Norma que usa una banda de 5 GHz y proporciona un rendimiento real de hasta ~24 Mbps a 30 m. / 100 pies en entornos exteriores. Existe una gama limitada de productos que lo admiten. El ancho de banda teórico es 54 Mbps.

- **Norma 802.11b:** La norma proporciona un rendimiento real de hasta ~5 Mbps a 100 m. / 300 pies en entornos exteriores. Usa la banda de 2,4 GHz. El ancho de banda teórico es 11 Mbps.

- **Norma 802.11g:** La norma utilizada más habitualmente que ofrece un rendimiento mejorado en comparación con la norma 802.11b. Rendimiento real de hasta ~ 24 Mbps a 100 m. / 300 pies en entornos exteriores. Usa la banda de 2,4 GHz. El ancho de banda teórico es 54 Mbps.

3.4.2. Acceso Inalámbrico de Banda Ancha: La norma utilizada es:

3.5. 802.16 – WiMAX:

IEEE 802.16, también conocida como WiMAX, es una especificación para las redes inalámbricas fijas de banda ancha de acceso metropolitano (MAN) que utilizan una arquitectura punto a multipunto. El estándar define el uso del ancho de banda entre las gamas de frecuencia con licencia 10GHz y 66GHz y sub 11GHz. 802.16 admite tasas de bits muy elevadas al cargar y descargar desde una estación base a una distancia de 50 km/30 millas, gestionando servicios como VoIP.

3.6. DIRECCIONAMIENTO IP

Una dirección IP (dirección del Protocolo de Internet) es un número exclusivo utilizado por los dispositivos para poder identificarse y comunicarse entre sí a través de una red, utilizando el estándar de Protocolos de Internet.

Las direcciones de Internet pueden ser simbólicas o numéricas. La forma simbólica es más fácil de leer, por ejemplo: *minombre@tcpip.com*. La forma numérica es un número binario sin signo de 32 bits, habitualmente expresado en forma de números decimales separados por puntos. Por ejemplo, *9.167.5.8* es una dirección de Internet válida. Los 32 bits de la dirección se dividen en cuatro octetos. El valor decimal de cada octeto puede ser entre 0 y 255 (el número binario de 8 bits más alto es 11111111).

Hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet "Corporation for Assigned Names and Numbers" (ICANN):

- **Clase A:** En la actualidad estas direcciones de clase a son reservadas para los gobiernos de todo el mundo, pero hasta hace poco eran usadas por empresas de gran envergadura.En una red de case A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es $2^{24} – 2$ (las direcciones reservadas de broadcast (últimos octetos a 255) y de red (últimos octetos a 0), es decir, 16777214 hosts, va desde la dirección 1.0.0.0 hasta la dirección 127.255.255.255.

- **Clase B:** Son direcciones que están reservadas para medianas empresas. En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{16} - 2, o 65 534 hosts, va desde la dirección 128.0.0.0 hasta la dirección 191.255.255.255.

- **Clase C:** Las direcciones de clase C se otorgan a todos los demás solicitantes. En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 2^8 - 2, o 254 hosts, va desde la dirección 192.0.0.0 hasta la dirección 223.255.255.255.

Cada clase de red permite una cantidad fija de equipos (hosts), esto se puede observar en el Anexo A.

- La dirección 0.0.0.0 es utilizada por las máquinas cuando están arrancando o no se les ha asignado dirección.
- La dirección que tiene su parte de host a cero sirve para definir la red en la que se ubica. Se denomina dirección de red.
- La dirección que tiene su parte de host a unos sirve para comunicar con todos los hosts de la red en la que se ubica. Se denomina dirección de “broadcast”.
- Las direcciones 127.x.x.x se reservan para pruebas de retroalimentación. Se denomina dirección de bucle local o “loopback”.

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no puede existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se sea a través de NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts)
- Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts)
- Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts)

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño a menudo se usa TCP/IP. Por ejemplo, los bancos pueden utilizar TCP/IP para conectar los cajeros automáticos que no se conectan a la red pública, de manera que las direcciones privadas son ideales para ellas. Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles.

Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas no se enrutará a través de Internet.

Tenemos dos tipos de direcciones IP:

1. ***IP dinámicas:*** Una IP dinámica es una IP asignada mediante un servidor DHCP ("*Dynamic Host Configuration Protocolo*") al usuario. La IP que se obtiene tienen una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

   Las IPs dinámicas son las que actualmente ofrecen la mayoría de operadores. Éstas suelen cambiar cada vez que el usuario reconecta por cualquier causa.

   - **Ventajas:** Reduce los costos de operación a los proveedores de servicios internet (ISP).

   - **Desventajas:** Obliga a depender de servicios que redirigen un host a una IP, y es ilocalizable es decir: en unas horas pueden haber varios cambios de IP.

   Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

   - **Manualmente:** cuando el servidor tiene a su disposición una tabla que emparejara direcciones MAC con direcciones IP, creadas manualmente por el administrador de la red. Sólo clientes con direcciones MAC válidas recibirán una dirección IP del servidor.

   - **Automáticamente:** donde el servidor DHCP asigna permanentemente una dirección IP libre, tomada de un rango prefijado por el administrador, a cualquier cliente que solicite una.

   - **Dinámicamente:** es el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un rango de direcciones IP para DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solcitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

2. ***IP fija:*** Una dirección IP fija es una IP asignada por el usuario, o bien dada por el proveedor ISP en la primera conexión. Las IPs fijas actualmente en el mercado tiene un costo adicional mensual. Estas IPs son asignadas por el proveedor en el momento de la primera conexión.

   Esto permite al usuario montar servidores web, correo, FTP, etc. y dirigir un nombre de dominio a esta IP sin tener que mantener actualizado el servicio DNS cada vez que cambie como ocurre con las IPs dinámicas.

   - **Ventajas:** Permite tener servicios dirigidos directamente a la IP.
   - **Desventajas:** Son más vulnerables al ataque, puesto que el usuario no puede conseguir otra IP, y su costo es más caro para los ISP puesto que esa IP puede no estar usándose las 24 horas del día.

3.7. DIRECCIONES IPv6

A partir de 1993, ante la previsible futura escasez de direcciones IPv4 debido al crecimiento exponencial de hosts en Internet, se empezó a introducir el sistema CIDR, que pretende en líneas generales establecer una distribución de direcciones más fina y granulada, calculando las direcciones necesarias y "desperdiciando" las mínimas posibles, para rodear el problema que las distribución por clases había estado gestando. Este sistema es, de hecho, el empleado actualmente para la delegación de direcciones.

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6. IPv6 est compuesta por 8 segmentos de 2 bytes cada uno, que suman un total de 128 bits, el equivalente a unos $3.4x10^{38}$ hosts que pueden ser direccionados. La ventaja con respecto a la IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación suele ser hexadecimal y para la separación de cada par de octetos se emplea el símbolo "**:**". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas acerca de la representación de direcciones IPv6 son:

- Los ceros iníciales, como en IPv4, se pueden obviar.
  Ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 →
  2001:123:4:ab:cde:3403:1:63

- Los bloques contiguos de ceros se pueden comprimir empleando "**::**". Esta operación solo se puede hacer una sola vez.

  Ejemplo: 2001:0:0:0:0:0:0:4 → 2001**::**4

3.8. MÉTODOS DE TRANSMISIÓN PARA VÍDEO IP:

Existen distintos métodos para transmitir datos en una red informática: Unidifusión, multidifusión y retransmisión.

- **Unidifusión (Unicasting):** el remitente y el receptor se comunican a un nivel de punto a punto. Los paquetes de datos son dirigidos únicamente a un recipiente y ningún otro usuario en la red necesitará procesar esta información.

- **Multidifusión (Multicasting):** comunicación entre un único remitente y múltiples receptores en una red. Las tecnologías multidifusión se utilizan para reducir el tráfico de la red cuando numerosos receptores desean visualizar la misma fuente de forma simultánea, ofreciendo una única transmisión de información a cientos de destinatarios. La mayor diferencia en comparación con la unidifusión es que la transmisión de vídeo debe enviarse una sola vez. La multidifusión (es decir, Multicasting-IP) se utiliza habitualmente junto con las transmisiones RPT.

- **Retransmisión (Broadcasting):** una transmisión de uno a todos. En una LAN, las retransmisiones normalmente se restringen a un segmento de red determinado y no se utilizan para transmisiones de vídeo en red.

3.9. QoS (Calidad de servicio)

En la actualidad, es común fusionar redes distintas en una sola red IP, así por ejemplo, las redes de telefonía y de vídeo (CCTV) están migrando a IP. En estas redes, es necesario controlar la forma de compartir los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es permitir que los enrutadores y conmutadores de la red se comporten de forma distinta en función de los diferentes tipos de servicios (voz, datos, vídeo) mientras el tráfico pasa a través de la red. Esta técnica se denomina Servicios Diferenciados *(DiffServ)*. Al hacer

uso de QoS, distintas aplicaciones de la red pueden coexistir en la misma red sin consumir el ancho de banda de la otra.

El término Calidad de Servicio hace referencia a las diversas tecnologías que garantizan una cierta calidad para los distintos servicios de la red. Un ejemplo de calidad puede ser un nivel de ancho de banda sostenido, un tiempo de espera reducido, ausencia de pérdida de paquetes, etc. Las ventajas principales de una red compatible con QoS son:

- Mayor fiabilidad en la red, gracias al control de la cantidad de ancho de banda que puede utilizar una aplicación y, en consecuencia, el control sobre las carreras del ancho de banda entre aplicaciones.

- La capacidad de priorizar el tráfico y, por lo tanto, permitir que los flujos importantes sean utilizados antes que los flujos de menor prioridad.

3.9.1 QoS Y VÍDEO IP

Para utilizar QoS en una red con productos de vídeo IP, deberán cumplirse los requisitos siguientes:

- Todos los conmutadores y enrutadores de la red deberán incluir un soporte para QoS. Esto resulta de suma importancia para lograr la funcionalidad integral de QoS.

- Los productos de vídeo IP utilizados deberán estar preparados para QoS.

Hay 2 casos particulares donde se realza la importancia del uso del QoS en una red.

- **Primer caso:** En este ejemplo (fig. 18), PC1 está viendo dos transmisiones de vídeo desde las cámaras 1 y 2, con cada cámara transmitiendo a 2,5 Mbps. De forma repentina, PC2 inicia una transferencia de archivos desde PC3. En este caso, la transferencia de archivos intentará hacer uso de la capacidad completa de 10 Mbps entre los “routers” R1 y R2, mientras que las transmisiones de vídeo intentarán mantener su velocidad total de 5 Mbps. Ya no puede garantizarse la cantidad de ancho de banda que se ofrece al sistema de vigilancia y posiblemente se reducirá la velocidad de imágenes de vídeo. En el peor de los casos, el tráfico FTP consumirá todo el ancho de banda disponible.

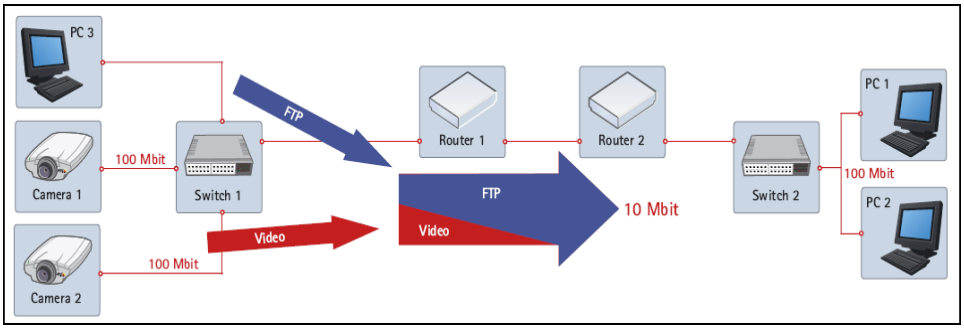


Fig. 18: Red con QoS (Libro Blanco)

- **Segundo caso:** El router R1 ha sido configurado para destinar hasta 5 Mbps de los 10 Mbps disponibles para la transmisión de vídeo. Se designa un tráfico para FTP de 2 Mbps, y HTTP y el resto del tráfico pueden utilizar un máximo de 3 Mbps. Al emplear esta división (fig. 19), las transmisiones de vídeo siempre dispondrán del ancho de banda necesario. Las transferencias de archivos son consideradas de menor importancia y obtienen un ancho de banda menor, pero seguirá existiendo un ancho de banda para la navegación Web y otro tipo de tráfico. Se debe tener en cuenta que los valores máximos sólo se aplican en caso de congestión en la red y si existiere un ancho de banda no utilizado, éste podrá ser empleado por cualquier tipo de tráfico.

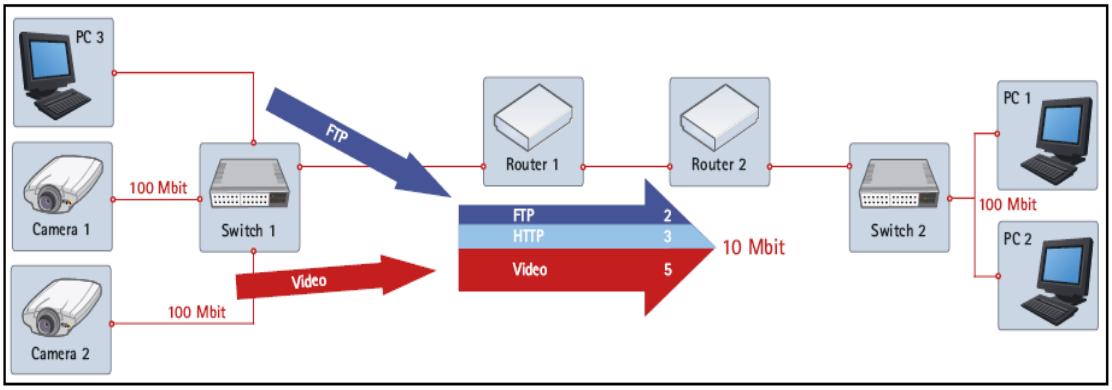


Fig. 19: Red con QoS (Libro Blanco)

3.10. CABLEADO ESTRUCTURADO

En el pasado había dos especificaciones principales de terminación de cableado: Los cables de datos y los cables de voz; en la actualidad, los sistemas de Cableado Estructurado (CE) soportan una gran cantidad de servicios y aplicaciones (voz, datos, video, texto, imágenes), tales como:

- Teléfonos, conmutadores
- TV, Audio estéreo, DVD, VCR
- Computadoras
- Modems, Máquinas de fax
- Home Theater
- Receptores de satélite
- Sistemas de seguridad
- Sistemas de Automatización
- Control de luces
- Enrutadores/switches/access points/

Un Sistema de Cableado Estructurado (SCE) es una serie de estándares definidos por la TIA/EIA que definen como *diseñar*, *construir* y *administrar* un sistema de cableado que es estructurado, es decir, que el sistema está diseñado en bloques que tienen características de desempeño muy específicas.

Un SCE se refiere a todo el cableado y componentes instalados en una red basados en un orden lógico y organizado.

El propósito de las organizaciones de estándares es formular un conjunto de reglas comunes para todos en la industria, en el caso del cableado estructurado para propósitos comerciales es proveer un conjunto estándar de reglas que permitan el soporte de múltiples marcas o fabricantes. Existen varias referencias SCE alrededor del mundo, tales como:

- **EIA/TIA 568A/B** El primer estándar de cableado estructurado Publicado en EUA por la EIA/TIA en 1991.
- **ISO/IEC 11801** Versión internacional del estándar 568.
- **CENELEC EN 50173** Estándar de cableado estructurado británico.

- **CSA T529** Estándar de cableado estructurado Canadiense.

El estándar de cableado estructurado EIA/TIA 568 fue diseñado para:

- Un sistema de cableado genérico de telecomunicaciones para edificios comerciales.
- Definir tipo de medio, topología, terminaciones y puntos de conexión y administración.
- Soportar ambiente de múltiples vendedores y productos.
- Dirección para diseño futuro de productos de telecomunicaciones para empresas comerciales.
- La habilidad para planear e instalar cableado de telecomunicaciones para edificios comerciales sin previo conocimiento de los productos que se utilizaran en el cableado.

Quizá la principal función de un SCE es prevenir**,** aislar**,** identificar y corregir fallas en una red de área local.

Un SCE consta de 6 subsistemas:

1. **Entrada al edificio:** La entrada a los servicios del edificio es el punto en el cual el cableado externo hace interfaz con el cableado de la dorsal dentro del edificio. Este punto consiste en la entrada de los servicios de telecomunicaciones al edificio (acometidas), incluyendo el punto de entrada a través de la pared y hasta el cuarto o espacio de entrada. Los requerimientos de la interface de red están definidos en el estándar TIA/EIA-569ª.

2. **Cuarto de equipos:** El cuarto de equipos es un espacio centralizado dentro del edificio donde se albergan los equipos de red (enrutadores, swiches, mux), equipos de datos (PBX), video, etc. Los aspectos de diseño del cuarto de equipos esta especificado en el estándar TIA/EIA 569A.

3. **Cableado de la dorsal (backbone):** El cableado de la dorsal permite la interconexión entre los gabinetes de telecomunicaciones, cuartos de telecomunicaciones y los servicios de entrada. Consiste en cables de “dprsalm cross–connects” principales y secundarios, terminaciones mecánicas y regletas o “jumperes” usando conexión dorsal – a – dorsal (tabla 3). Esto incluye:

    a. Conexión vertical entre pisos (risers),

b. Cables entre un cuarto de equipos y cable de entrada a los servicios del edificio,
c. Cables entre edificios.

Tipo de cables requeridos para la Dorsal

TIPO DE CABLE	DISTANCIAS MÁXIMAS DE LA DORSAL
100 ohm UTP (24 o 22 AWG)	800 metros (Voz)
150 ohm STP	90 metros (Datos)
Fibra Multimodo 62.5/125 µm	2,000 metros
fibra Monomodo 8.3/125 µm	3,000 metros

Tabla 3: Tipo de cables requeridos para la dorsal

4. **Gabinete o rack de Telecomunicaciones:** El rack de telecomunicaciones es el área dentro de un edificio que alberga el equipo del sistema de cableado de telecomunicaciones. Este incluye las terminaciones mecánicas y/o "cross–conects" para el sistema de cableado a la dorsal y horizontal.

5. **Cableado horizontal:** El sistema de cableado horizontal se extiende desde el área de trabajo de telecomunicaciones al rack de telecomunicaciones y consiste de lo siguiente:

   a. Cableado Horizontal,
   b. Enchufe de telecomunicaciones,
   c. Terminaciones de cable (asignaciones de guías del conector modular RJ-45, Anexo B),
   d. Conexiones de transición.

   Tres tipos de medios son reconocidos para el cableado horizontal, cada uno debe de tener una extensión máxima de 90 metros:

   - Cable UTP 100 – ohm, 4 pares, (24 AWG sólido),
   - Cable STP 150 – ohm, 2 pares,
   - Fibra óptica 62.5 / 1125 – µm, 2 fibras.

6. **Área de trabajo:** Las comunicaciones del área de trabajo se extienden desde el enchufe de telecomunicaciones hasta los dispositivos o estaciones de trabajo.

Los componentes del área de trabajo son los siguientes:

- *Dispositivos:* computadoras, terminales, teléfonos, cámaras, etc.
- *Cables de parcheo:* cables modulares, cables adaptadores / combersores, “jumperes” de fibra, etc.
- *Adaptadores:* deberán ser externos al enchufe de telecomunicaciones.

CAPITULO 4

DISEÑO DE UN SISTEMA INTEGRADO DE VIGILANCIA

La Unidad Educativa Porvenir es una empresa que ha sufrido una serie de actos vandálicos y robos, por lo que se ha visto en la necesidad de proteger sus bienes tomando ciertas medidas de seguridad como es la instalación de una cerca electrificada, que en cierta forma ha ayudado a disminuir estos actos pero no se los ha eliminado ni se ha dado con los culpables. En vista de los malos resultados obtenidos, la empresa ha decidido buscar un sistema de seguridad más efectivo que permita dar con los autores e impida que se sigan perpetuando dichos acontecimientos. Cabe recalcar que dichos actos delincuenciales no sólo han sido llevados a cabo por personas ajenas a la institución, sino que también han ocurrido robos en horas laborables, por lo que se presume hay individuos de mal proceder dentro de la misma, a consecuencia de lo mencionado anteriormente se propone un sistema integrado de video vigilancia y control de acceso para de esta forma ubicar a los responsables e impedir que sigan ocurriendo estos hechos.

4.1. UBICACIÓN DEL INMUEBLE

Para la elaboración de este proyecto se realizó un estudio previo del inmueble, donde se tomaron en cuenta aspectos tales como: el sector donde se encuentra ubicado el colegio, los alrededores, estacionamiento, áreas verdes, aulas, laboratorios y oficinas.

La Unidad Educativa Porvenir se encuentra ubicada en la calle Alfonso Jaramillo s/n (vía a Misicata) (Anexo D1), en un sector poco iluminado, no muy transitado por vehículos y transeúntes, además está oculto ya que se encuentra detrás de un cerro que impide su visibilidad desde la vía principal, creando un ambiente propicio para que los delincuentes hagan de las suyas.

La institución se encuentra rodeada en gran parte por casas (Anexo D1), a excepción del frente, en el que se encuentra la carretera y de una porción de la parte posterior en la que se encuentra un terreno baldío, por donde se presume ingresaron los delincuentes cuando se perpetuó el último robo realizado en horas de la noche.

4.2. ZONIFICACIÓN

Luego de haber efectuado el estudio de la ubicación y alrededores de la institución se procedió a realizar el estudio de la infraestructura interna de la misma, optando por dividirla en zonas para una mejor cobertura (Anexo D2), así:

- Zona 1: Zona de parqueo
- Zona 2: Canchas y espacio verde (frente de la institución)
- Zona 3: Oficinas
- Zona 4: Aulas
- Zona 5: Bar
- Zona 6: Espacio verde (Patio de preescolar)
- Zona 7: Juegos infantiles
- Zona 8: Laboratorios

El Sistema que se ha diseñado para la Unidad Educativa Porvenir tiene que cubrir un área de 2500 m^2 aproximadamente entre oficinas, aulas de clase, laboratorios y lugares de recreación (Anexo D2), para lo que se necesita 6 cámaras para exteriores, 3 cámaras para interiores, un sistema de control de acceso y dos dispositivos para limitar el ingreso a ciertos lugares.

4.3. UBICACIÓN DE LAS CÁMARAS

Las cámaras y control de acceso (anexo C1, C2, C3), serán ubicadas dependiendo de la necesidad y amplitud de la zona (anexo D2), tal como se detalla a continuación:

- **Cámara 1 (C1):** se ubicará en la zona 3, para dar cobertura a la zona 1.
- **Cámara 2 (C2):** se ubicará en la zona 4, para dar cobertura a la zona 2.
- **Cámara 3 y 4 (C3, C4):** se ubicarán en la zona 3 y están destinadas para cubrir las oficinas de planta baja y alta.

- **Cámara 5 (C5):** se ubicará en la parte posterior de la zona 4, para dar cobertura a la zona 5.
- **Cámara 6 (C6):** se ubicará en la parte posterior de la zona 4, para dar cobertura a la zona 6.
- **Cámara 7 (C7):** se ubicará en la zona 7, para dar cobertura a las zonas 6, 5 y 3
- **Cámara 8 (C8):** se ubicará en la zona 8, para dar cobertura al laboratorio de computación.
- **Cámara 9 (C9):** se ubicará en la zona 3 y cubrirá la puerta principal de ingreso a la institución.
- **Camara 10 (C10):** se ubicara en la zona 3 y cubrirá la puerta para el ingreso de los insumos necesarios para el bar.

Las cámaras a ser instaladas serán de diferentes tipos, dependiendo de las necesidades de la zona, es decir, habrán zonas donde será necesario utilizar cámaras adecuadas para exteriores, interiores, con infrarrojo, fijas y móviles.

En el mercado existe una gran variedad de marcas y modelos de cámaras, se las puede encontrar de distintos precios y para diferentes usos. Al momento de la selección de una cámara no sólo se debe tomar en cuenta la especificación y marca, sino también el costo de la misma para que esté al alcance del cliente, por ende la selección se restringe un poco más.

4.4. DISPOSITIVOS A UTILIZARSE

Para este proyecto se investigaron muchos modelos y marcas, encontrando las más adecuadas, tanto para garantizar la calidad del trabajo como para el presupuesto del cliente, y principalmente la disponibilidad en el mercado.

Por todo lo mencionado anteriormente, se utilizará cámaras de la marca “D-Link” debido a la fácil adquisición, calidad y precio de los equipos, principalmente. Las características primordiales se detallan a continuación:

- La cámara para los exteriores son del modelo DCS–3220, es una Cámara IP D-Link AUDIO, INTERNET 10/100 MBPS- 2WAY (Anexo C1), sus características principales son:

  - Conectividad “Fast Ethernet”,
  - Zoom digital 4x,
  - Soporte “Two way Audio”, para escuchar y hablar,
  - Detección de movimiento y notificación vía e-mail,
  - Facilidad “Smart Playback”.

- La cámara para los interiores son del modelo DCS–5300, es una Cámara IP D-Link 10/100 IP PTZ AUDIO, INTERNET (Anexo C2), sus características principales

  - Conectividad “Fast Ethernet”,
  - Monitoreo con movimiento horizontal y vertical,
  - Soporte de Audio,
  - Soporte para micrófono externo,
  - Detección de movimiento y notificación vía e-mail,
  - Soporte PTZ, con zoom digital hasta 4x.

Al no poseer las cámaras PoE y para abaratar costos, las cámaras se conectaran a la circuitería eléctrica ya existente en el inmueble

Para lo que corresponde al control de accesos, se investigaron sensores de varios tipos tales como los de proximidad, biométricos, lectoras, etc. La selección de estos dispositivos se basa en el uso que van a tener, porque hay sensores de gran seguridad que son utilizados en fábricas y empresas grandes como seguridad al espionaje industrial y hay otros que en cambio pueden ser utilizados en lugares más pequeños, donde la seguridad no exija tanto como es nuestro caso. Por ello los dispositivos seleccionados para realizar el control de accesos en esta institución y basados en las necesidades de la misma, son los que se detallan a continuación:

- Lector “Wiegand” 12 – 15 cm., HID COMPATIBLE (anexo C3),

  - Combina la tecnología de lector “Wiegand” con un teclado plenamente integrado.
  - Salida de datos del teclado disponible en formatos de 8 y 26 bit.
  - LED bicolor.

- Tarjeta de proximidad para TSP00, TSP01, RBM21, EM9918.
- Panel de proximidad 2 lectoras. Usuarios Protocolo Weig.

- Cerradura Eléctrica.
- Cierrapuertas de 50Kg marca Viro.

La Ubicación de las cámaras y dispositivos de control de acceso están especificadas en el plano del Anexo D2.

El cuarto de control estará ubicado en la parte posterior de la institución, es desde aquí que se realizará el control de todo el sistema, se escoge este lugar ya que es estratégico, pues como se realizará cableado estructurado se tienen que cumplir normas como, por ejemplo, el cableado desde el cuarto de control a un punto de conexión no debe exceder los 100 m., y desde este cuarto las distancias no exceden esta norma, y principalmente el cuarto tiene una infraestructura adecuada por lo que no hay necesidad de construir uno nuevo.

El inmueble cuenta con un cableado de red ya instalado para el laboratorio de computación y las oficinas, se pretendió dar uso a esta red pero no cumple con las normas requeridas, así que se propone realizar un nuevo cableado muy aparte del que se encuentra ya implementado, y además, es necesario realizar las conexiones eléctricas para la alimentación de las cámaras.

Con las cámaras y sensores que se detallaron anteriormente, se procedió a elaborar una tabla donde consta todo el presupuesto de la implementación del proyecto, el costo aproximado del proyecto se especifica a continuación:

4.5. PRESUPUESTO DEL PROYECTO

EQUIPO	MODELO	cant	P. UNITARIO	P. FINAL
Cámara IP D-Link AUDIO, INTERNET 10/100 MBPS- 2WAY	DCS - 3220	7	474.10	3318.70
Cámara IP D-Link 10/100 IP PTZ AUDIO, INTERNET	DCS - 5300	3	542.29	1626.87
Lector Wiegand 12 - 15 cm., HID COMPATIBLE	KE - P500H	2	240.91	481.82
Tarjeta de Proximidad para TSP00, TSP01, RBM21, EM9918	TST01	25	3.10	77.50
Batería de 12vdc 4amp	BTR12-4	1	21.81	21.81
Fuete de alimentación 12 Vdc/1.2A y 24Vdc/750mA	ST-PS1224	1	29.09	29.09
PANEL de proximidad 2 lectoras 65000 Usuarios Protocolo Weig	KE-PXL500W	1	975.00	975.00
Trasformador 40VA 110 a 16 Vac	RE - RT1640	1	14.55	14.55
Cerradura Eléctrica	AN - ASL - 3703	2	64.54	129.08
Cierrapuertas de 50 KG Marca Viro	CIERP50K	2	67.44	134.88
Cable UTP (metro)		500	0.35	175.00
Conectores RJ-45		30	0.50	15.00
Router D-Link	DI-400 108Mbps, 802.11b, 802.11g	1	75.00	75.00
Computador	HD 500GB, RAM 2GB, INTEL 2.5GHz,	1	1000.00	1000.00
Servicio Técnico e Instalación		1	500.00	500.00
Adaptador de Bateria emergente 12V.		1	100.00	100.00
			Sub Total	8674.30
			IVA	1040.92
			TOTAL	9715.22

CONCLUSIONES

En el mercado existe una gran gama de cámaras de muchas variedades, según la aplicación, es por ello que cuando se vaya a instalar una cámara, es necesario conocer las condiciones en las cuales va a trabajar a misma, para que, dependiendo de ello seleccionar la más indicada. Por ejemplo, no es nada recomendable usar una cámara diseñada para trabajar en interiores en un lugar donde va a estar expuesta a sol y agua o condiciones hostiles, la garantía del trabajo depende mucho de la correcta elección de los equipos.

La flexibilidad que presenta el software de gestión de video es muy beneficiosa para el usuario de un sistema de video vigilancia, por cuanto él puede elegir el modo de grabación dependiendo de la necesidad del recinto a vigilar. Ahora sabiendo utilizar este software, se puede llegar a obtener un gran sistema de vigilancia incorporando un juego de cámaras combinado con un sistema de control de accesos, pudiendo incluso a un bajo costo realizar un trabajo que esté óptimo para brindar una seguridad aprueba de espionaje, resultando útil para empresas que necesiten salvaguardar información importante, como es el caso de los bancos.

Los sistemas de video vigilancia ya sean cctv o catv, han dejado de ser necesarios al nivel empresarial solamente o un lujo que se podían dar ciertas familias de clase económica alta, ahora con el lamentable crecimiento del índice delincuencial, estos sistemas deberían ser aplicados en todas las residencias, para así prestar una mayor seguridad a las personas que habitan allí, para lo cual existen en el mercado modelos de cámaras que por su diseño, hacen juego con la decoración de una residencia, llegando a pasar desapercibido por su forma, de tal manera que no incomodaría a las personas que llegasen en caso de visita.

Debido a que en nuestro país el suministro de energía eléctrica no es óptimo, y a menudo se presentan los cortes y variación de energía eléctrica, es necesario que al sistema de video vigilancia se le implemente un UPS,de esta manera nuestro sistema será totalmente confiable, a demás de ayudarnos a mantener encendidas las cámaras

durante el apagón y así no perder detalle alguno de la grabación, los UPS, traen un regulador de corriente incorporado, suministrando al equipo las condiciones eléctricas adecuadas, lo cual es muy importante debido que las cámaras que no tienen alimentación PoE sino mediante la conexión a un transformador, suelen bloquearse al haber picos de tensión, lo cual es molesto para el usuario por cuanto le tocaría reiniciar el equipo cada vez que esto ocurra.

BIBLIOGRAFIA

REFERENCIAS BIBLIOGRAFICAS:

- Libro Blanco del Hogar Digital y las Infraestructuras Comunes de Telecomunicaciones, TELEFONICA de España.
- CASTRO Lozan o Carlos, DOMÓTICA E INMÓTICA, Editorial Alfaomega, 2da edición, México.
- TOMÁS Perales Benito, ¿Cómo ……. Domótica?
- HUIDOBRO José Manuel y Ramón J, Millán Tejedor, Domótica – Edificios Inteligentes, 3ª reimpresión.
- FERNÁNDEZ Valentín y Enrique Ruz, El Hogar Digital, Madrid – España.
- LORENTE Arenas Santiago, Juan J. Vinagre Díaz y José I. Rueda Benítez, La Comunidad Digital de Vecinos.
- ROLDÁN Viloria José y Roldán Díaz Alberto, Optimice la Gestión de su Hogar.
- ROMERO, C. Vázquez, F. Castro, Domótica e Inmotica. Viviendas y Edificios Inteligentes. Editorial Ra-ma, 2ª Edición. Madrid.
- LAMAS Graziani Javier, José María Quintero G., Juan D. Sandoval G., Sistemas de Control para Viviendas y Edificios, DOMOTICA, 2005, 1ª Edición.
- LAURA Raya González, José Luis Raya,Intranets y TCP/IP con Microsoft Windows Server 2003
- JESUS García Tomas, Alta Velocidad y Calidad de Servicio en Redes IP.
- SCOTT M. Ballew, Managing IP Networks With Cisco Redes

REFERENCIAS ELECTRONICAS:

- http://www.sistemasps.com/home.php SPS Compañía de Seguridad Electrónica.
- **http://www.osiriszig.com/** Tecnologia ZIGBEE.
- www.casadomo.com Casadomo, el portal de la domótica.
- http://www.amtel-security.com/spanish Empresa dedicada al Control de Acceso
- www.echelon.com Empresa propietaria de la tecnología Lon Works
- www.inproel.com Empresa distribuidora de equipos electrónicos
- www.tolder.es Empresa de toldos domóticos

- www.golmar.es Empresa de comunicaciones, porteros automáticos y controcl de accesos.
- www.seligrat.com Porteros automáticos y video porteros
- www.ce.philips.es sistemas de televisión CCTV
- www.domitel.com Domótica e Inmótica
- www.azedomo.com Domótica
- www.dominnova.com Domótica
- www.honeywell.es Proyectos caseros.
- www.lge.es LG electronics España
- http://www.ub.es/geocrit/sn/sn-146(136).htm , Empresa distribuidora de dispositivos domoticos.
- http://www.ciudadfutura.com/mundopc/redes Manejo del Hogar Digital
- http://www.angelfire.com/wi/ociosonet Dispositivos de Control
- http://www.itlp.edu.mx/publica/tutoriales/redes Diseño de redes demóticas.
- http://www.globalnet.com.mx Automatización de Oficinas
- http://www.pchardware.org/redes/redes_osi.htmcxvcx
- http://www.cableadovozdatos.com/ Redes de Transmisión, Voz/IP.
- http://www.hidglobal.com/espanol/productMatrix.php#Prox_16 Dispositivos para la Automatización.
- http://www.camarasip.cl/sistemas_de_video_digital_nuevas_instalaciones.htm Distribuidor de Cámaras IP.
- http://www.empretel.com.mx/CCTV/productos/nuuo/productos/hybrid.htm Curso de Redes, CISCO
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm Curso de Redes, CISCO
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm Curso de Redes, CISCO
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm Curso de Redes, CISCO

ANEXO A: Tabla de clases de direcciones IP.

CLASE	DIRECCION IP (R=RRED; H=HOSTS)	RANGO		# de Redes	# de Host	Mascara de Red	Broadcast
		INICIO	FINAL				
A	0RRRRRRR.HHHHHHHH.HHHHHHHH.HHHHHHHH	1.0.0.0	127.255.255.255	126	16777214	255.0.0.0	x.255.255.255
B	10RRRRRR.RRRRRRRR.HHHHHHHH.HHHHHHHH	128.0.0.0	191.255.255.255	16384	65534	255.255.0.0	x.x.255.255
C	110RRRRR.RRRRRRRR.RRRRRRRR.HHHHHHHH	192.0.0.0	223.255.255.255	2097152	254	255.255.255.0	x.x.x.255
D	1110 (dirección de Multicast)	224.0.0.0	239.255.255.255				
E	1111 (reservado para uso futuro)	240.0.0.0	255.255.255.255				

- La dirección 0.0.0.0 es utilizada por las máquinas cuando están arrancando o no se les ha asignado dirección.
- La dirección que tiene su parte de host a cero sirve para definir la red en la que se ubica. Se denomina dirección de red.
- La dirección que tiene su parte de host a unos sirve para comunicar con todos los hosts de la red en la que se ubica. Se denomina dirección de “broadcast”.
- Las direcciones 127.x.x.x se reservan para pruebas de retroalimentación. Se denomina dirección de bucle local o “loopback”.

ANEXO B: Asignaciones del conector modular RJ-45 de 8 Hilos.

El conector RJ-45 (“Registered Jack – 45”) de 8 hilos/posiciones es el más empleado para aplicaciones de redes. Estos conectores están numerados de 1 a 8, de izquierda a derecha, cuando el conector es visto desde la parte posterior al ganchito, como se muestra en la figura B1.

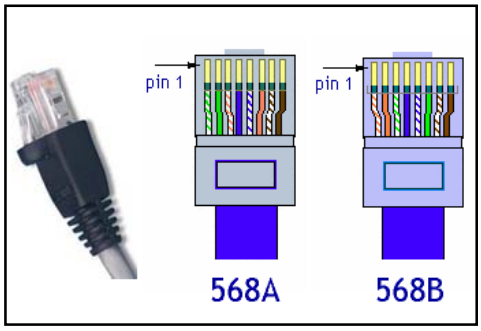
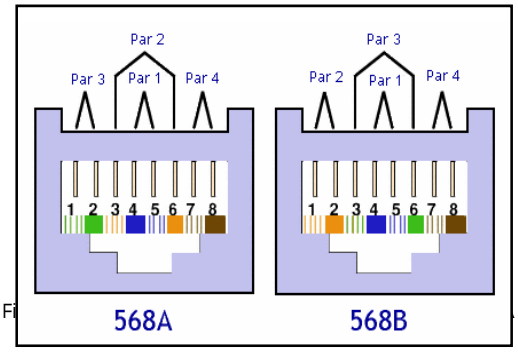


Fig. B1: Numeración de los pins del conector RJ45



Fi

Como se puede apreciar en la figura B2, la asignación de pins está definida por la EIA/TIA, el 58A y el 568B. Ambos esquemas son casi idénticos, excepto por los pares 2 y 3, que están al revés. Cualquier configuración puede ser usada para ISDN (Integrated Services Digital Network) y aplicaciones de alta velocidad. Las categorías de cables de transmisión 3, 4, 5, 5e y 6 son sólo aplicables a este tipo de grupos de pares. Para aplicaciones de RED (Ethernet 10/100 BaseT, o “Token Ring) solo son usados dos pares, los dos pares restantes se utilizarían para otro tipo de aplicaciones; por ejemplo, voz (tabla 4).

Pin#	Función	568A	568B
1	Tx	BLANCO/VERDE	BLANCO/NARANJA
2	Tx	VERDE	NARANJA
3	Rx	BLANCO/NARANJA	BLANCO/VERDE
4	-	AZUL	AZUL
5	-	BLANCO/AZUL	BLANCO/AZUL
6	Rx	NARANJA	VERDE
7	-	BLANCO/CAFE	BLANCO/CAFE
8	-	CAFE	CAFE

Fig. B2: Configuración de acuerdo a norma EIA/TIA

Para leer un cable modular hay que alinear los dos extremos del conector, con los dos contactos hacia el frente y comparar los colores de izquierda a derecha. Si los colores aparecen en el mismo orden en ambos conectores, entonces, el cable es directo, o 1 a 1. Si los colores aparecen invertidos, entonces el cable es cruzado.

Un cable directo sirve para conectar una computadora a un “Hub”, “Switch” ó “Ruter”, y ***un cable cruzado*** sirve para conectar dos PCs entre sí. Algunos “Hubs” o “Switches” pueden tener enchufes que cambien de directo a cruzado mediante un interruptor, otros tienen un enchufe especial para ese propósito marcado con “X”.

ANEXO C: Generalidades de los equipos

Anexo C1: Cámara DCS-3220

La cámara Internet de D-Link DCS-3220, es un sistema de seguridad que le permite a usted mirar y escuchar remotamente, desde su casa u oficina, el lugar que desee.

Con todas las facilidades, la DCS-3220 puede ser conectada a cualquier red Ethernet en una Oficina o Campus, o en Internet de Banda Ancha, para entregar audio y alta calidad de video. Ya que tiene incorporado un Servidor Web, micrófono, detección de movimiento para grabar, envío de mensaje de alerta, y un poderoso software para monitoreo y administración de múltiples cámaras, es la DCS-3220 un comprensivo y conveniente sistema de vigilancia, ya sea de forma local o remota. Está equipada con un sensor CCD de alta calidad, zoom, y capacidad para 2 vías de audio.

Principales Características y Facilidades

- "Two way" audio
- Sistema de monitoreo autónomo gracias a su Servidor Web Integrado
- Monitoreo Remoto vía Web
- Monitoreo de múltiples cámaras vía Software Windows, hasta 16 en forma simultánea.
- Activación de grabado de video, ante detección de movimiento
- Fácil y rápida implementación de sistema de video vigilancia
- Zoom digital de 4x
- Soporte de UPnP & DDNS

Anexo C2: Cámara DCS-5300

La cámara Internet de D-Link DCS-5300, está diseñada para ser un excelente sistema de seguridad que le permitirá a usted monitorear remotamente el lugar que desee.

Con todas las facilidades esperadas en éste tipo de cámara, la DCS-5300 puede ser conectada a cualquier red "Ethernet" o "Wireless", de una Oficina, Banco, "Super Market" o Campus, y monitorear dichos lugares desde la propia red LAN o desde Internet vía banda ancha, permitiendo ver en línea el sitio deseado, entregando además una alta calidad de video.

La DCS-5300 entre sus facilidades estándar incorpora un Servidor Web, detección de movimiento, que puede ser habilitado para grabar cuando exista movimiento, y grabación hacia dispositivo de almacenamiento masivo en línea. Pero además incorpora entre sus facilidades avanzadas movimientos horizontal y vertical (PAN/TILT), que pueden ser controlados a través del software de gestión (IP View) o directamente vía interfaz Web, o si lo prefiere vía control remoto.

La DCS-5300 es la solución de video vigilancia con la mejor relación costo/efectividad del mercado, ideal y conveniente para "Small&Medium Business".

Principales Características y Facilidades

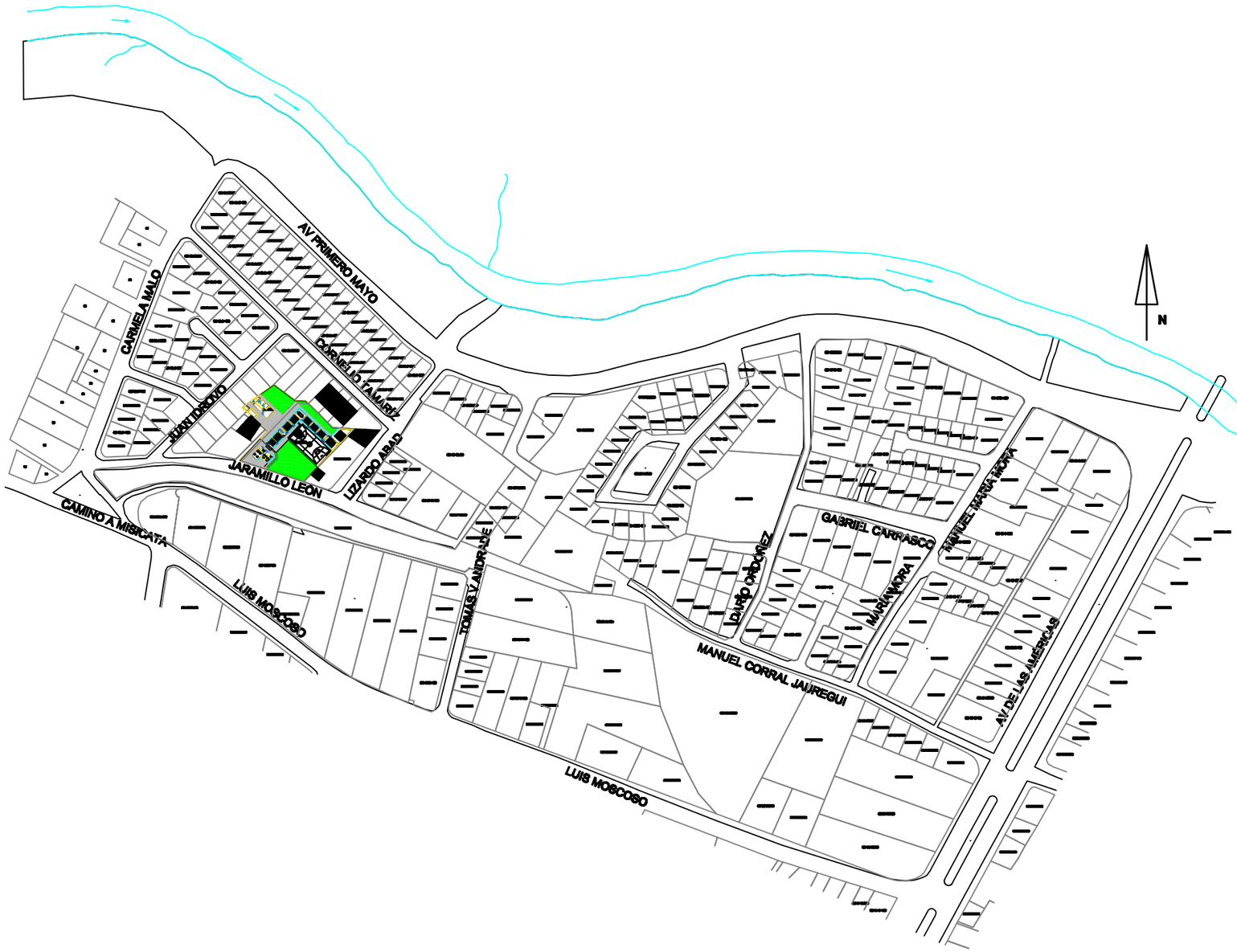
- Soporte PAN/TILT
- Sistema de monitoreo autónomo gracias a su Servidor Web Integrado,
- Monitoreo Remoto vía Web
- Monitoreo de múltiples cámaras vía Software Windows, hasta 16 en forma simultánea,
- Activación de grabado de video, ante detección de movimiento,
- Control remoto, para direccionar la cámara hacia el objetivo deseado
- Puerto de I/O para comunicación hacia dispositivo externo
- Audio incorporado,
- Soporte UnPnP y DDNS
- Salida de audio y video, para conexión hacia televisor, y
- Fácil y rápida implementación de sistema de video vigilancia.

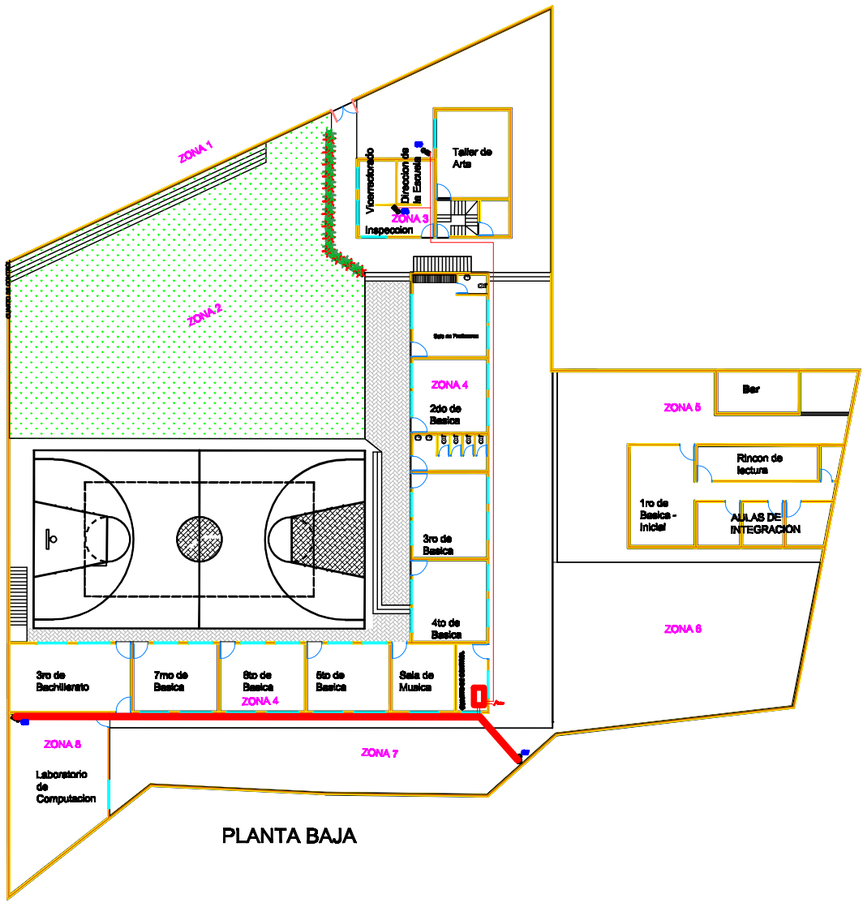
Anexo C3: Lector Wiegand

El lector “PINpad Wiegand” es un lector “Wiegand” y un teclado combinados en la misma carcasa robustecida. Está totalmente protegido de los elementos y tiene un amplio rango de temperatura operativa, lo que lo convierte en un lector ideal para su uso en exteriores incluso en las condiciones climáticas más extremas.

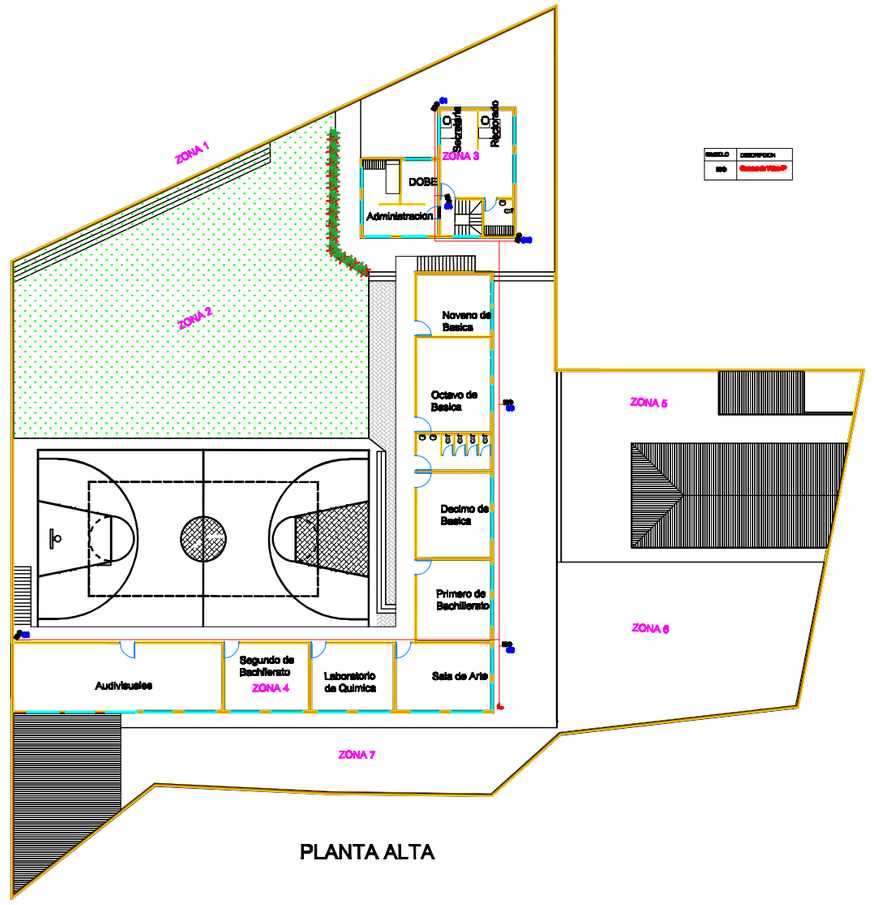
El lector “PINpad Wiegand” se instala directamente en una caja multipolar única para una fácil instalación. Su atractivo aspecto hace que sea un elemento bienvenido en cualquier lugar interior o exterior.

El lector “PINpad Wiegand” es ideal para el control de acceso, el control de horarios y otras aplicaciones en las que se necesiten datos de teclado y/o datos de tarjeta “Wiegand”. La mayoría de los controladores de acceso puede utilizar los datos de la tarjeta o los datos del teclado para acceder durante el horario laboral, y requieren un nivel superior de seguridad con los datos combinados fuera de dicho horario.


AV PRIMERO MAYO
CARMELA MALO
CORNELIO TAMARIZ
JUAN DROVO
JARAMILLO LEON
LIZARDO ABAD
CAMINO A MISICATA
LUIS MOSCOSO
TOMÁS Y ANDRADE
DARÍO CARDÓNEZ
GABRIEL CARRASCO
MANUEL CORRAL JAUREGUI
MANUEL MARÍA MORA
AV. DE LAS AMERICAS
LUIS MOSCOSO
N



PLANTA BAJA



PLANTA ALTA

SIMBOLO	DESCRIPCION
SD	Detector de Humo

UNIVERSIDAD DEL AZUAY

Escala: 1:100

Dibujo: Ing. Adrian Ortega A.
Revisó: Ing. Ayrton Fernandez A.
Fecha: -

Ing. Adrian Ortega A.
Ing.Electromecanica

Contiene:
CABLEADO PARA INSTALACION DE CAMARAS DE VIDEO VIGILANCIA

Proyecto:
SD – RSN – 2009

Hoja: