
**UNIVERSIDAD NACIONAL DE CHIMBORAZO**

**FACULTAD DE INGENIERÍA**

**ESCUELA DE INGENIERÍA ELECTRONICA Y TELECOMUNICACIONES**

**"Trabajo de grado previo a la obtención del Título de Ingeniero en Electrónica Y Telecomunicaciones"**

**TRABAJO DE GRADUACIÓN**

Título del proyecto

# DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD DE VIDEO VIGILANCIA MEDIANTE CAMARAS IP BAJO ADMINISTRACIÓN SNMP, UTILIZANDO UNA ALARMA GPRS

**Autor:** **Paúl Alexis Orta Jarrín**

**Director:** **Ing. Daniel Santillán**

**Riobamba – Ecuador**

**2013**

Los miembros del Tribunal de Graduación del proyecto de investigación de título**:** **Diseño é Implementación de un Sistema de Seguridad de Video Vigilancia mediante Cámaras Ip bajo administración SNMP, utilizando una Alarma GPRS,** presentado por: **Paúl Alexis Orta Jarrín** y dirigida por la: **Ingeniera Deysi Inca.**

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

| | |
|---|---|
| **----------** | **----------** |
| **Ing. Edmundo Cabezas** | |
| **Presidente del Tribunal** | **Firma** |
| **----------** | **----------** |
| **Ing. Daniel Santillán** | |
| **Director del Proyecto** | **Firma** |
| **----------** | **----------** |
| **Ing. Deysi Inca** | |
| **Miembro del Tribunal** | **Firma** |

## AUTORÍA DE LA INVESTIGACIÓN

La responsabilidad del contenido de este Proyecto de Graduación, corresponde exclusivamente a: Paúl Alexis Orta Jarrín, Ing. Deysi Inca e Ing. Daniel Santillán; y el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.

## AGRADECIMIENTO

El presente trabajo de tesis me gustaría agradecerle a Dios por bendecirme y guiarme, para llegar a la meta propuesta, porque se hizo realidad mi sueño anhelado, al igual a mis padres por su apoyo incondicional.

Me complace agradecer de manera muy especial a esta gran institución a la Universidad Nacional del Chimborazo en la Facultad de Ingeniería, Escuela de Electrónica y Telecomunicaciones y en ella a cada uno de los docentes quienes día a día supieron impartir sus conocimientos y experiencias para lograr nuestro propósito.

A mis directores de tesis, Ing. Deysi Inca y al Ing. Daniel Santillan por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado que pudiera terminar este trabajo de la mejor manera.

**DEDICATORIA**

Agradezco al creador de todas las cosas Dios por haberme permitido llegar hasta el final de este objetivo tan importante de mi vida y de mi familia por haberme dado la fortaleza y salud para lograr mis objetivos, derramando muchas bendiciones en el diario vivir y guiándome en cada uno de mis pasos en la vida.

A mis Padres Ángel Orta y Guadalupe Jarrín por haberme apoyado y brindado los recursos necesarios en todo momento, por la motivación constante que me ha permitido ser una persona de bien, por los ejemplos de perseverancia, fortaleza y constancia que los caracterizan con lo que me ha infundado siempre en la vida.

A mi hermana Paulina por ser el ejemplo de una mujer luchadora que a más de ser hermana mayor es una amiga con la cual me ha brindado su apoyo en todo momento de mi vida, a mi hermano Omar con el cual compartimos varios momentos difíciles tanto en lo personal como en nuestras vidas estudiantiles.

A mi esposa, que ha estado a mi lado dándome cariño, confianza y apoyo incondicional para seguir adelante para cumplir otra etapa en mi vida.

A mi hija, el motivo y la razón que me ha llevado a seguir superándome día a día, para alcanzar los más apreciados ideales de superación, dejándole a ella una enseñanza de querer es poder sin ningún obstáculo o impedimento que se presente por delante..

**Paúl A. Orta J.**

**ÍNDICE**

## ÍNDICE GENERAL

## ÍNDICE DE TABLAS

## ÍNDICE DE FIGURAS

## RESUMEN

La tecnología basada en el protocolo TCP/IP es una tecnología ampliamente difundida para el establecimiento de las redes de comunicaciones en áreas pequeñas o extensas, por lo que la tendencia actual es la digitalización de cualquier tipo de información como voz, datos o video a fin de ser transmitidos en este tipo de redes. Una tendencia muy marcada en la actualidad es la implementación de Sistemas de Vigilancia IP, es decir redes que permitan la transmisión de video o voz en paquetes sobre el protocolo TCP/IP, utilizando la tecnología inalámbrica o alámbrica la cual es de fácil despliegue y mantenimiento y a su vez permite cubrir áreas extensas.

La presente Tesis tiene objetivo diseñar e implementar un sistema de seguridad mediante cámaras ip, incluyéndole una alarma GPRS que finalmente se presente la Red de Seguridad idónea para el problema de Seguridad que presenta la Unidad Educativa San Miguel situada en la provincia Bolívar, cantón San Miguel.

Al utilizar la Tecnología IP nos permite hoy en día ventajas como: la gestión centralizada de todas las cámaras del sistema de seguridad desde cualquier PC en cualquier parte del mundo y la interacción remota con todo el sistema en tiempo real. A más de eso los dispositivos que trabajan con IP utilizan estándares abiertos por lo que no precisan trabajar con equipos de la misma marca. Esto permite la elección de dispositivos de distintos proveedores según la función y costos.

De esto se puede concluir que el uso de estándares abiertos favorece a la competencia y reduce costos.

## SUMMARY

The technology based on the TCP/IP protocol is a widespread technology for establishing communications networks in small or large areas so that the current trend is to digitize any kind of information such as voice, data or video in order to be transmitted in such networks. A strong tendency today is the implementation of IP Surveillance Systems, i.e. networks that allow the transmission of video or voice packets over TCP/IP, using wired or wireless technology which is easy to deploy and maintain, and at the same time it covers large areas.

The purpose of this thesis is to design and implement a security system using IP cameras, including a GPRS alarm which finally presents the ideal Security Network for the security problem found in *San Miguel Educative Unit* located in the Bolivar province, San Miguel canton.

Nowadays, the use of IP technology allows us these advantages: centralized management of all the security system cameras from any PC anywhere in the world and remote interaction with the whole system in real time. Besides this, the devices using IP work with open standards, so that they do not necessarily work with equipment of the same brand. This allows the choice of devices from different providers according to function and cost.

From this, we can conclude that the use of open standards favors competition and reduces costs.

# CAPÍTULO I

## 1. FUNDAMENTACIÓN TEÓRICA

### 1.1 INTRODUCCIÓN

El desarrollo tecnológico alcanzado por nuestro país en los últimos años se sintetiza en el desarrollo de las ciudades y su tecnología a nivel nacional, nuestra provincia Chimborazo no es ajena a esta realidad y esto nos incentiva la elaboración del proyecto de investigación de un Diseño e Implementación de un sistema de seguridad de video vigilancia mediante cámaras Ip bajo administración SNMP, utilizando una alarma GPRS.

La inseguridad es parte de la realidad que vivimos en el mundo, América Latina. Las escasas fuentes de empleo y la corrupción complementan el factor de crecimiento de la delincuencia.
El índice de robos en el Ecuador se ha incrementado notablemente por tal razón la sociedad en general ha empezado a tomar acciones correctivas, ya sea contratando servicios privados de seguridad o implementando sistemas de vigilancia inteligente.

En la actualidad la **UNIDAD EDUCATIVA FISCOMISIONAL "SAN MIGUEL"** no cuenta con un proyecto de estas características por lo tanto el presente proyecto de investigación nace de la necesidad de establecer el control y monitoreo de su institución para evitar que se cometan robos dentro de sus instalaciones.
Además es necesario realizar un control permanente del desempeño y de las labores de los empleados, profesores y alumnos de la Institución, a su vez la monitorización de las instalaciones permitirá controlar cualquier eventualidad que se pueda suscitar.

El desarrollo del proyecto debe tener las debidas especificaciones técnicas, además, debe contar con instrumentos de comunicaciones y de video como por ejemplo routers, cámaras ip entre otros para poder vigilar y administrar dicho proyecto. Por lo cual se necesita que el Sistema de seguridad de Video Vigilancia cuente con la instalación y conexión de los diferentes instrumentos de comunicación estén en un óptimo funcionamiento, que además deben tener una conexión a un equipo visualizador de las imágenes, en el cual se pueda acceder por medio del Internet.

Ante la necesidad de lograr tener seguridad en la Unidad Educativa San Miguel, se desarrollen con calidad y sobre todo garantice su durabilidad, es necesario implementar Sistema de seguridad de Video Vigilancia.

## 1.2 FUNDAMENTACIÓN TEÓRICA

### 1.2.1 ANTECEDENTES

El origen de las Lan inalámbricas (WLAN)[1] se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM[2] en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados publicados por el IEEE[3], pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología. Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema de espectro expandido. En mayo de 1985, y tras cuatro años de estudios, la Federal Communications Comisión, la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones asignó las bandas de Industrial, Scientific and Medical 902 – 928 MHz 2,400 – 2,4835 GHz, 5,725 – 5,850 GHz para uso en las redes inalámbricas basadas en Spread Spectrum, con las opciones DS[4] ( Direct Sequence ) y FH[5] ( Frequency

[1] Lan inalámbricas
[2] International Business Machines
[3] Institute of Electrical and Electronics Engineers
[4] Direct Sequence
[5] Frequency Hoping

Hoping ). La técnica de espectro ensanchado es una técnica de modulación que resulta ideal para las comunicaciones de datos, ya que es muy poco susceptible al ruido y crea muy pocas interferencias. La asignación de esta banda de frecuencias propició una mayor actividad en el seno de la industria y ese respaldo hizo que las WLAN empezaran a dejar ya el entorno del laboratorio para iniciar el camino hacia el mercado.

Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrolló hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativas que superaban la velocidad de 1 Mbit/s, el mínimo establecido por el IEEE 802.11 para que la red sea considerada realmente una LAN, con aplicación empresarial.

Hasta ese momento las WLAN habían tenido una aceptación marginal en el mercado por dos razones fundamentales: falta de un estándar y precios elevados de la solución inalámbrica. En estos últimos años se ha producido un crecimiento en el mercado de hasta un 100% anual. Este hecho es atribuible a dos razones principales: El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles que han permitido que los usuarios puedan estar en continuo movimiento manteniendo comunicación constante con otros terminales y elementos de la red.

En este sentido, las comunicaciones inalámbricas ofrecen recursos no disponibles en redes cableadas: movilidad y acceso simultáneo a la red. La conclusión de la definición de la norma IEEE 802.11 para redes de área local inalámbricas en junio de 1997 que ha establecido un punto de referencia y ha mejorado muchos de los aspectos de estas redes.

### **1.2.2 APLICACIONES DE LAS REDES WLAN** (Naranjo, 2007, pág. 3)

Las aplicaciones comunes de las redes de área local que podemos encontrar son las siguientes: Redes locales para situaciones de emergencia o congestión de la red cableada.

Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría instalar una infraestructura de red cableada. Con la solución inalámbrica es factible instalar una red de área local en un corto tiempo.

Interconexión de redes de área local que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red de área local inalámbrica para interconectar dos o más redes de área local cableada situadas en dos edificios distintos.

En ambientes industriales con severas condiciones ambientales. Este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.

Esta solución es muy típica en entornos cambiantes que necesitan de una estructura de red flexible que se adapte a los cambios.

### 1.2.3 CONFIGURACIONES DE LAS REDES WLAN

La complejidad de una red de área local inalámbrica es variable, dependiendo de las necesidades a cubrir y en función de los requerimientos del sistema que queramos implementar; podemos utilizar distintas configuraciones de red:

- Punto a Punto
- Cliente y Punto de acceso
- Uso de un punto de extensión
- Enlace entre varias LAN[6] o WMAN[7]

### 1.2.4 PUNTO A PUNTO

Las redes inalámbricas pueden ser configuradas de distintas formas para cubrir la mayor parte de las necesidades que permite su especial fisonomía. La forma más elemental se presenta al conectar dos ordenadores equipados con tarjetas

[6] Local Area Network
[7] Redes Inalámbricas de Área Metropolitana

adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual, peer to peer.

Cada máquina tiene únicamente acceso a los recursos de otra máquina pero no a un servidor central. Este tipo de redes no requiere administración o pre-configuración y todo el soporte de la red recae en los usuarios.

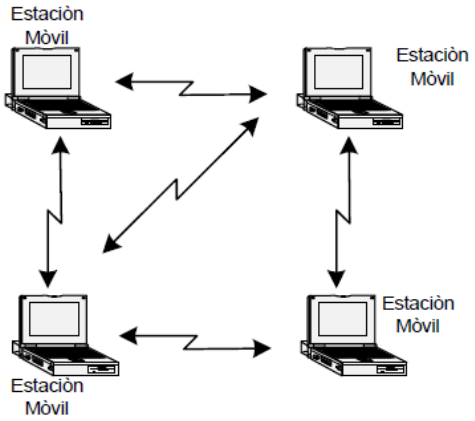



**Figura. 1.1. Conexión Peer to Peer (Punto a Punto)** (Naranjo, 2007)

### 1.2.5 CLIENTE Y PUNTO DE ACCESO

La configuración se puede mejorar sustancialmente instalando un punto de acceso (AP[8]), que permite no sólo doblar el rango entre el cual los dispositivos pueden comunicarse pues actúan como repetidores, sino que, además, desde el punto de acceso se puede conectar a la red cableada cualquier nodo inalámbrico para que tenga acceso a los recursos de la red y también actúan como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso puede servirá varios clientes, según la naturaleza y número de transmisiones que se puedan producir. Los puntos de acceso tienen un rango finito, del orden de 150 metros en lugares cerrados y 300 metros en zonas abiertas. En grandes zonas, como por ejemplo un campus universitario o naves industriales, es más que probable la necesidad de más de un punto de acceso, con los que poder cubrir por

[8] Access Point

completo la zona asignada con células que solapen sus áreas de influencia de modo que los usuarios puedan mover sus ordenadores sin pérdidas de 6 Punto de Acceso Estación Móvil conexión entre un grupo de puntos de acceso. Este método de funcionamiento es denominado roaming.

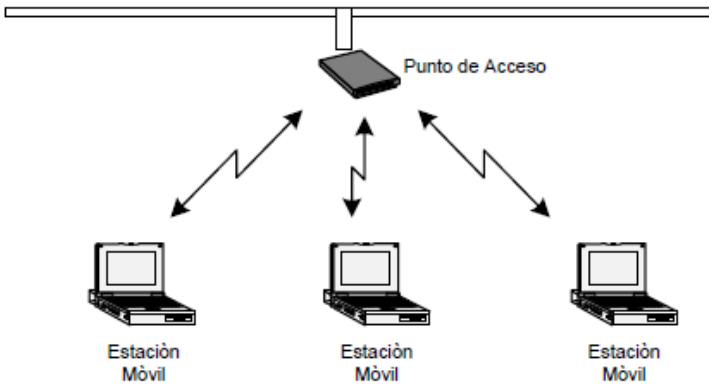



**Figura. 1.2. Conexión a la Red Lan por un Punto de Acceso** (Naranjo, 2007)

### 1.2.6 USO DE UN PUNTO DE EXTENSIÓN

Pero si las configuraciones propuestas hasta ahora no son suficientes para resolver los problemas más particulares y específicos, el diseñador de la red puede optar por usar un Punto de Extensión para aumentar el número de puntos de acceso a la red. Estas células de extensión actúan como AP a AP, pero no están "enganchados" a la red cableada como ocurre con los Puntos de Acceso propiamente dichos.

Los puntos de extensión funcionan, como su propio nombre indica, extendiendo el alcance efectivo de la red mediante la retransmisión de las señales de un cliente a un AP o a otro. Igualmente, los puntos de extensión pueden encadenarse para pasar mensajes entre un Punto de Acceso y clientes lejanos de modo que se construye un puente entre ambos.

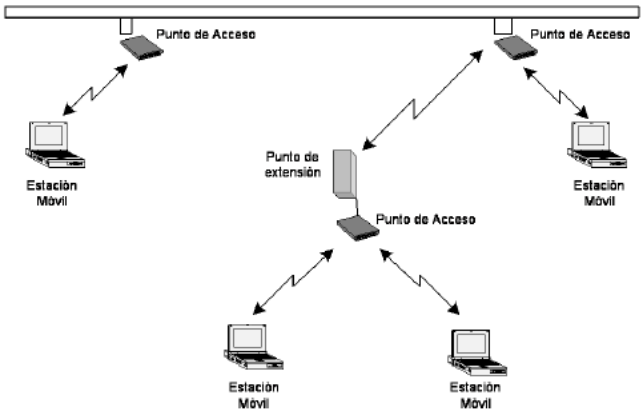



**Figura. 1.3. Conexión a la Red Lan por un Punto de Extensión** (Naranjo, 2007)

### 1.2.7 ENLACE ENTRE VARIAS LAN O WMAN

Para finalizar, otra de las configuraciones de red posibles es la que incluye el uso de antenas direccionales. El objetivo de estas antenas direccionales es el de enlazar redes que se encuentran situadas geográficamente en sitios distintos.

Un ejemplo de esta configuración lo tenemos en el caso en que tengamos una red local en un edificio y la queramos extender a otro edificio.

Una posible solución a este problema consiste en instalar una antena direccional en cada edificio apuntándose mutuamente.

A la vez, cada una de estas antenas está conectada a la red local de su edificio mediante un punto de acceso. De esta manera podemos interconectar las dos redes locales.

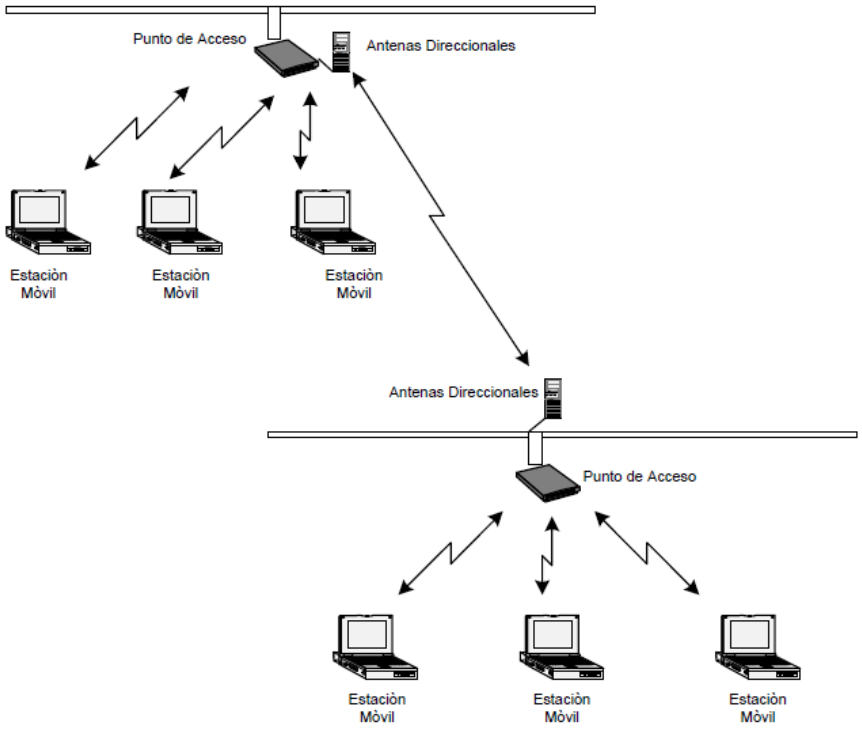



**Figura. 1.4. Enlace entre varias Lan** (Naranjo, 2007)

## 1.3. ESTÀNDARES PARA REDES LAN INALÀMBRICAS WLAN

### 1.3.1. ESTÀNDAR 802.11 (Naranjo, 2007, pág. 8)

El estándar 802.11 fue desarrollado por el Instituto de Ingenieros Electrónicos y Eléctricos IEEE. En su primera versión, proporcionaba unas velocidades de transmisión de 1 ó 2 Mbps y una serie fundamental de métodos de señalización y otros servicios. El primer problema que encontró este estándar, fue el de su baja tasa de transferencia de datos, incapaz de soportar los requerimientos de las empresas en la actualidad.

En consecuencia se trabajó en un nuevo estándar el 802.11b (también conocido como 802.11 High Rate), que apareció en 1999 y proporcionaba unas tasas de transferencia de hasta 11 Mbps. Gracias a las prestaciones ofrecidas por 802.11b, similares a las de las redes cableadas, ha logrado tener una buena aceptación en el mundo empresarial, siendo una de las tecnologías más expandidas y que posee un amplio abanico de productos y compañías que la soportan. Muchas de las

empresas dedicadas al desarrollo de equipamiento informático se han unido en una alianza denominada WECA[9], cuya misión es la de permitir la interoperabilidad entre productos 802.11b de distintos fabricantes y promocionar dicha tecnología en el ámbito empresarial, PY MES y hogar Cuando un producto es comprobado que funciona correctamente con otros dispositivos 802.11b, recibe el certificado de Wi-Fi[10] como garantía de interoperabilidad y buen funcionamiento. El estándar 802.11 define el protocolo y el equipo necesario para realizar una comunicación de datos por medio del aire, en una red de área local (LAN), usando la técnica CSMA/CA[11]. Además el protocolo incluye autenticación, prestación de servicios, encriptación de datos y gestión de la alimentación (para reducir el consumo de energía de estaciones móviles).En las redes LAN alámbricas, una dirección es equivalente a una ubicación física. En cambio para el estándar IEEE 802.11, se emplean las denominadas estaciones, las cuales contienen la capa de control de acceso al medio, la capa física y una interfaz con el medio inalámbrico. La estación se puede ver como un destino para un mensaje determinado, pero no como una ubicación fija.

**Versiones del estándar 802.11, 802.11b.-** es el estándar que lidera los desarrollos actuales de WLAN. Emplea solamente la tecnología de Secuencia Directa y utiliza modulación con forma de onda CCK[12] lo que permite alcanzar hasta 11 Mbps de velocidad en la banda de 2,4 GHz. 802.11a.- es una evolución del 802.11b, opera en la banda de 5 GHz y ofrece una capacidad de hasta 54 Mbps. El interfaz aire utiliza multiplicación OFDM[13] 802.11g tiene multiplicación OFDM que permite hasta 54 Mbps de capacidad máxima en la banda de 2,4 GHz . Permite interoperabilidad con el estándar 802.11b. 802.11h.- estándar 802.11h es una evolución del 802.11a que permite asignación dinámica de canales y control automático de potencia para minimizar los efectos interferentes.

[9] Wireless Ethernet Compatibility Alliance
[10] Wireless Fidelity
[11] Carrier sense multiple access protocol with collision avoidance
[12] Complementary Code Keying
[13] Orthogonal Frequency Division

### 1.3.2. TRANSMISIÓN MULTIMEDIA SOBRE REDES IP PARA LA APLICACIÓN A LA SEGURIDAD (Naranjo, 2007, pág. 27)

La transmisión de video sobre redes de telecomunicaciones está llegando al punto de convertirse en un sistema habitual de comunicación debido al crecimiento masivo que ha supuesto internet en estos últimos años. Lo estamos utilizando para ver películas o comunicarnos con conocidos, pero también se usa para dar clases remotas, para hacer diagnósticos en medicina, video conferencia, distribución de televisión, video bajo demanda. Debido a la necesidad de su uso que se plantea en el presente y futuro, a lo largo de los años se han proporcionado distintas soluciones y sucesivos formatos para mejorar su transmisión, los cuales serán mencionados posteriormente. En este capítulo se explican los procesos de digitalización y codificación de la voz y del video, así como los diversos formatos de compresión existentes, el ancho de banda requerido para la transmisión de video y los cuellos de botella que esto podría ocasionar.

### 1.3.3 RESEÑA HISTÓRICA DE LA TRANSMISIÓN DE VÍDEO SOBRE REDES.

El interés en la comunicación utilizando video ha crecido con la disponibilidad de la televisión comercial iniciada en 1940. Los adultos de hoy han crecido utilizando el televisor como un medio de información y entretenimiento, se han acostumbrado a tener un acceso visual a los eventos mundiales más relevantes en el momento en que estos ocurren. Nos hemos convertido rápidamente en comunicadores visuales. Es así que desde la invención del teléfono los usuarios han tenido la idea de que el vídeo podría eventualmente ser incorporado a éste. En 1964 AT & T[14] presentó en la feria del comercio mundial, de Nueva York, un prototipo de video teléfono el cual requería de líneas de comunicación bastante costosas para transmitir vídeo en movimiento, con costos de cerca de mil dólares por minuto. El dilema fue la cantidad y tipo de información requerida para desplegar las imágenes de vídeo. Las señales de video incluyen frecuencias

[14] American Telephone and Telegraph; NYSE

mucho más altas que las que la red telefónica podía soportar (particularmente la de los años 60's). El único método posible para transmitir la señal de video a través de largas distancias fue a través de satélite. La industria del satélite estaba en su infancia entonces, y el costo del equipo terrestre combinado con la renta de tiempo de satélite excedía con mucho los beneficios que podrían obtenerse al tener pequeños grupos de personas comunicados utilizando este medio. A través de los años 70's se realizaron progresos substanciales en muchas áreas claves, los diferentes proveedores de redes telefónicas empezaron una transición hacia métodos de transmisión digitales. La industria de las computadoras también avanzó enormemente en el poder y velocidad de procesamiento de datos y se descubrieron y se mejoraron significativamente los métodos de muestreo y conversión de señales analógicas (como las de audio y video) en bits digitales. El procesamiento de señales digitales también ofreció ciertas ventajas, primeramente en las áreas de calidad y análisis de la señal; el almacenamiento y transmisión todavía presenta obstáculos significativos. En efecto, una representación digital de una señal analógica requiere de mayor capacidad de almacenamiento y transmisión que la original.

Por ejemplo los métodos de video digital comunes de fines de los años 70 y principios de los 80 requirieron de relaciones de transferencia de 90 Mbps. La señal estándar de video era digitalizada utilizando el método común PCM[15] de 8 bits, con 780 pixeles por línea, 480 líneas activas por cuadro de las 525 para NTSC[16] y con 30 cuadros por segundo. La necesidad de una compresión confiable de datos digitales fue crítica. Los datos de video digital son un candidato natural para comprimir, debido a que existen muchas redundancias inherentes en la señal analógica original; redundancias que resultan de las especificaciones originales para la transmisión de video y las cuales fueron requeridas para que los primeros televisores pudieran recibir y desplegar apropiadamente la imagen. Una buena porción de la señal de video analógica está dedicada a la sincronización y temporización del monitor de televisión. Ciertos métodos de compresión de datos fueron descubiertos, los cuales eliminaron enteramente esta porción redundante de

[15] Modulación por codificación de pulsos
[16] Netware Transmission System Codification

información en la señal, con lo cual se obtuvo una reducción de la cantidad de datos utilizados de un 50 % aproximadamente, es decir 45 Mbps, una razón de compresión de 2:1. Las redes telefónicas en su transición a digitales, han utilizado diferentes relaciones de transferencia, la primera fue 56 Kbps necesaria para una llamada telefónica ( utilizando métodos de muestreo actuales ), enseguida grupos de canales de 56 Kbps fueron reunidos para formar un canal de información más grande el cual corría a 1,5 Mbps ( comúnmente llamado canal T1 ). Varios grupos de canales T1 fueron reunidos para conformar un canal que corría a 45 Mbps ( un T3 ). Así usando video comprimido a 45 Mbps fue finalmente posible, pero todavía extremadamente caro, transmitir video en movimiento a través de la red telefónica pública.

Estaba claro que era necesario comprimir aún más el video digital para llegar a hacer uso de un canal T1 (con una razón de compresión de 60:1), el cual se requería para poder iniciar el mercado. Entonces a principios de los 80's algunos métodos de compresión hicieron su debut, estos métodos fueron más allá de la eliminación de la temporización y sincronización de la señal, realizando un análisis del contenido de la imagen para eliminar redundancias. Esta nueva generación de video códec (Codificador / Decodificador) no sólo tomó ventaja de las redundancias, sino también del sistema de la visión humana. La razón de imágenes presentadas en el video en Norte América es de 30 cuadros por segundo, sin embargo esto excede los requerimientos del sistema visual humano para percibir movimiento, la mayoría de las películas cinematográficas muestran una secuencia de 24 cuadros por segundo. La percepción del movimiento continuo puede ser obtenida entre 15 y 20 cuadros por segundo, por tanto una reducción de 30 cuadros a 15 cuadros por segundo por sí mismo logra un porcentaje de compresión del 50 %. Una relación de 4:1 se logra obtener de esta manera, pero todavía no se alcanza el objetivo de lograr una razón de compresión de 60:1. Los codecs de principio de los 80's utilizaron una tecnología conocida como codificación de la Transformada Discreta del Coseno. Usando DCT[17] las imágenes de video pueden ser analizadas para encontrar redundancia espacial y

[17] Transformada Discreta del Coseno

temporal. La redundancia espacial es aquella que puede ser encontrada dentro de un cuadro sencillo de video, “áreas de la imagen que se parecen bastante que pueden ser representadas con una misma secuencia “. La redundancia temporal es aquella que puede ser encontrada de un cuadro de la imagen a otro “áreas de la imagen que no cambian en cuadros sucesivos “. Combinando todos los métodos mencionados anteriormente, se logró obtener una razón de comprensión de 60:1.

El primer códec fue introducido al mercado por la compañía Compression Labs Inc. (CLI[18]) y fue conocido como el VTS[19] 1.5, y el 1.5 hacía referencia a 1.5 Mbps o T-1. En menos de un año CLI mejoró el VTS 1.5 para obtener una razón de compresión de 117:1 (768 Kbps), y renombró el producto a VTS 1.5E. La corporación británica GEC y la corporación japonesa NEC entraron al mercado lanzando codecs que operaban con un T-1 ( y debajo de un T-1 si la imagen no tenía mucho movimiento ). Ninguno de estos codecs fueron baratos, el VTS 1.5 E era vendido en un promedio de $ 180000, sin incluir el equipo de video y audio necesarios para completar el sistema de conferencia, el cual era adquirido por un costo aproximado de $ 70000, tampoco incluía costos de acceso a redes de transmisión, el costo de utilización de un T-1 era de aproximadamente $1000 dólares la hora. A mediados de los 80’s se observó un mejoramiento dramático en la tecnología empleada en los codecs de manera similar, se observó una baja substancial en los costos de los medios de transmisión. Compression Labs Inc. introdujo el sistema de video denominado Rembrandt los cuales utilizaron ya una razón de compresión de 235:1 ( 384 Kbps ). Entonces una nueva compañía, Picture Tel (originalmente PicTel Communications), introdujo un nuevo códec que utilizaba una relación de compresión de 1600:1 ( 56 Kbps ). Picture Tel fue el pionero en la utilización de un nuevo método de codificación denominado HVQ[20]. CLI lanzó poco después el códec denominado Rembrandt 56 el cual también operó a 56 Kbps utilizando una nueva técnica denominada compensación del movimiento. Al mismo tiempo los proveedores de redes de comunicaciones

[18] Compression Labs Inc
[19] Video Teleconference System
[20] Cuantificación jerárquica de vectores

empleaban nuevas tecnologías que abarataban el costo del acceso a las redes de comunicaciones.

El precio de los codecs cayó casi tan rápido como aumentaron los porcentajes de compresión. En 1990 los codecs existentes en el mercado eran vendidos en aproximadamente, $30000; reduciendo su costo en más del 80 %, además de la reducción en el precio se produjo una reducción en el tamaño. El VTS 1.5E media cerca de 5 pies de alto y cubría un área de 2 y medio pies cuadrados y pesaba algunos cientos de libras. El Rembrandt 56 media cerca de 19 pulgadas cuadradas por 25 pulgadas de fondo y peso cerca de 75 libras. El utilizar razones de compresión tan grandes tiene como desventaja la degradación en la calidad y en la definición de la imagen. Una imagen de buena calidad puede obtenerse utilizando razones de compresión de 235:1 (384 Kbps) o mayores. Los codecs para videoconferencia pueden ser encontrados hoy en un costo que oscila entre los 250,00 y los 600,00 dólares. La razón de compresión mayor empleada es de 1600:1 ( 56 Kbps ), ya que no existe una justificación para emplear rangos de compresión aún mayores , puesto que utilizando 56 Kbps , el costo del uso de la red telefónica es aproximado al de una llamada telefónica. Esto ha permitido que los fabricantes de codecs se empleen en mejorar la calidad de la imagen obtenida utilizando 384 Kbps o mayores velocidades de transferencia de datos. Algunos métodos de codificación producen imágenes de muy buena calidad a 768 Kbps y T –1 que es difícil distinguirla de la imagen original sin compresión.

## 1.4. ESTUDIO DE LAS CÁMARAS IP

### 1.4.1. ¿QUE ES UNA CÁMARA DE RED? (Axis, pág. 1)

Una cámara de red, también llamada cámara IP, puede describirse como una cámara y un computador, combinados para formar una única unidad. Los componentes principales que integran este tipo de cámaras de red incluyen un objetivo, un sensor de imagen, uno o más procesadores y memoria. Los procesadores se utilizan para el procesamiento de la imagen, la compresión, el

análisis de video y para realizar funciones de red. La memoria se utiliza para fines de almacenamiento del firmware de la cámara de red y para la grabación local de secuencias de video. Como un computador, la cámara de red dispone de su propia dirección IP[21], está directamente conectada a la red y se puede colocar en cualquier ubicación en la que exista una conexión de red. Esta característica es la diferencia respecto a una cámara Web, que únicamente puede ejecutarse cuando está conectada a un computador personal por medio del puerto USB o IEEE 1394, que es un estándar multiplataforma para entrada/salida de datos en serie a gran velocidad. Asimismo, es necesaria la existencia de software instalado en el PC[22] para que pueda funcionar.


**Figura 1.5 Cámara de red conectada directamente a la red LAN.** (Naranjo, 2007)

Las cámaras de red pueden configurarse para enviar video a través de una red IP para visualización y/o grabación en directo, ya sea de forma continua, en horas programadas, en un evento concreto o previa solicitud de usuarios autorizados.

Las imágenes capturadas pueden secuenciarse como Motion JPEG, MPEG-4 o H.264 utilizando distintos protocolos de red. Asimismo, pueden subirse como imágenes JPEG individuales usando FTP (File Transfer Protocol), correo electrónico o HTTP (Hypertext Transfer Protocol).

Además de capturar video, algunas cámaras de red ofrecen gestión de eventos y funciones de video inteligentes como detección de movimiento, detección de audio, alarma anti-manipulación activa y auto-seguimiento. La mayoría de las cámaras de red también disponen de puertos de entrada/salida que habilitan las conexiones con dispositivos externos como sensores y relés. Igualmente, pueden

[21] Internet Protocol
[22] Computador Personal

incluir prestaciones como funciones de audio y soporte integrado para alimentación por Ethernet ( PoE[23]), es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como, por ejemplo, un teléfono IP o una cámara 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 los equipos.

### 1.4.2. LA EVOLUCIÓN DE LOS SISTEMAS DE VIGILANCIA POR VIDEO (Axis, pág. 2)

Los sistemas de vigilancia por video se originaron entre los años 50s. Avances en los 70s. Empezaron siendo sistemas analógicos al 100% y paulatinamente se fueron digitalizando. Los sistemas de hoy en día han avanzado mucho desde la aparición de las primeras cámaras analógicas con tubo conectadas a VCR[24].

En la actualidad, estos sistemas utilizan cámaras y servidores de PC para la grabación de video en un sistema completamente digitalizado. Sin embargo, entre los sistemas completamente analógicos y los sistemas completamente digitales existen diversas soluciones que son parcialmente digitales. Dichas soluciones incluyen un número de componentes digitales pero no constituyen sistemas completamente digitales.

### 1.4.3. SISTEMAS DE CIRCUITO CERRADO DE TV ANALÓGICOS USANDO VCR

Un sistema de circuito cerrado de TV analógico que utilice un VCR, representa un sistema completamente analógico formado por cámaras analógicas con salida coaxial, conectadas al VCR para grabar.

[23] Power over Ethernet
[24] VideoCcassette Recorder

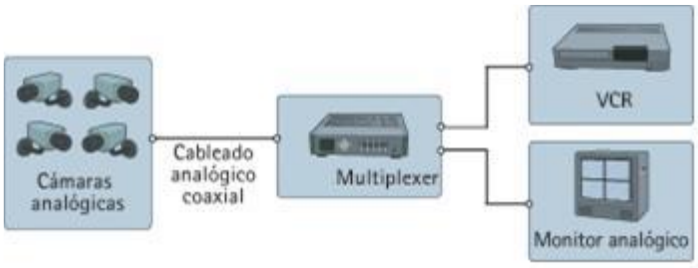



**Figura 1.6 Circuito cerrado de TV analógica usando VCR** (Naranjo, 2007)

El VCR utiliza el mismo tipo de cintas que una grabadora doméstica. El video no se comprime y, si se graba a una velocidad de imagen completa, una cinta durará como máximo 8 horas. En sistemas mayores, se puede conectar un multiplexor entre la cámara y el VCR. El multiplexor permite grabar el video procedente de varias cámaras en un solo grabador, pero con el inconveniente que tiene una menor velocidad de imagen. Para monitorizar el video, es necesario un monitor analógico.

### 1.4.3.1 SISTEMAS DE CIRCUITO CERRADO DE TV ANALÓGICOS USANDO DVR.

Un sistema de circuito cerrado de TV (CCTV[25]) analógico usando un DVR (digital video recorder), es un sistema analógico con grabación digital. En un DVR, la cinta de video se sustituye por discos duros para la grabación de video, y es necesario que el video se digitalice y comprima para almacenar la máxima cantidad de imágenes posible de un día.

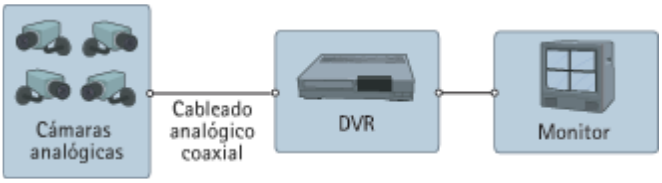



**Figura 1.7 Circuito cerrado de TV analógica usando DVR** (Naranjo, 2007)

[25] Sistema de circuito cerrado de TV

Con los primeros DVR, el espacio del disco duro era limitado, por tanto, la duración de la grabación era limitada, o debía usarse una velocidad de imagen inferior. El reciente desarrollo de los discos duros significa que el espacio deja de ser el principal problema. La mayoría de DVRs disponen de varias entradas de video, normalmente 4, 9 ó 16, lo que significa que también incluyen la funcionalidad de los multiplexores.

El sistema DVR añade las siguientes ventajas:

- No es necesario cambiar las cintas
- Calidad de imagen constante

### 1.4.3.2 SISTEMAS DE CIRCUITO CERRADO DE TV ANALÓGICOS USANDO DVR DE RED

Un sistema de circuito cerrado de TV (CCTV) analógico usando un DVR IP[26] es un sistema parcialmente digital que incluye un DVR IP equipado con un puerto Ethernet para conectividad de red. Como el video se digitaliza y comprime en el DVR, se puede transmitir a través de una red informática para que se monitorice en un PC en una ubicación remota.

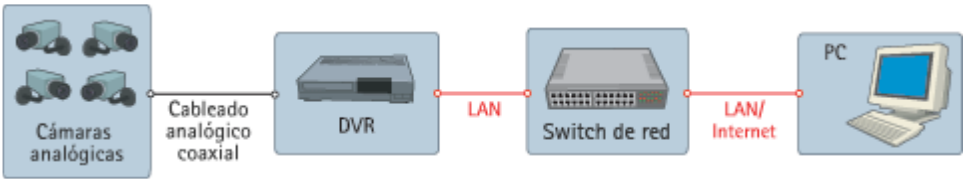



**Figura 1.8 Sistema de circuito cerrado de TV analógico usando DVR de red**

(Naranjo, 2007)

Algunos sistemas pueden monitorizar tanto video grabado como en directo, mientras otros sólo pueden monitorizar el video grabado. Además, algunos sistemas exigen un cliente Windows especial para monitorizar el video, mientras que otros utilizan un navegador web estándar, lo que flexibiliza la monitorización remota.

[26] Digital video recorder IP

El sistema DVR IP añade las siguientes ventajas:

- Monitorización remota de video a través de un PC
- Funcionamiento remoto del sistema.

### 1.4.3.3 SISTEMAS DE VIDEO IP QUE UTILIZAN SERVIDORES DE VIDEO

Un sistema de video IP que utiliza servidores de video incluye un servidor de video, un switch de red y un PC con software de gestión de video. La cámara analógica se conecta al servidor de video, el cual digitaliza y comprime el video.

A continuación, el servidor de video se conecta a una red y transmite el video a través de un switch de red a un PC, donde se almacena en discos duros. Esto es un verdadero sistema de video IP.

Un sistema de video IP que utiliza servidores de video añade las ventajas siguientes:

- Utilización de red estándar y hardware de servidor de PC para la grabación y gestión de video
- El sistema es escalable en ampliaciones de una cámara cada vez
- Es posible la grabación fuera de las instalaciones
- Preparado para el futuro, ya que este sistema puede ampliarse fácilmente incorporando cámaras IP

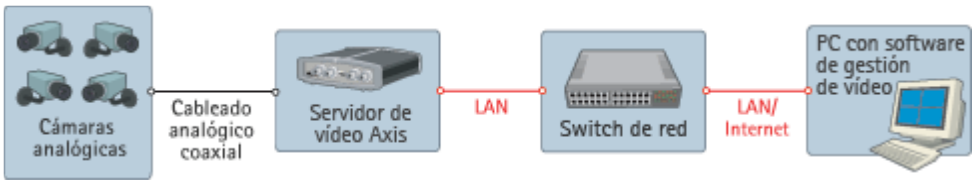



**Figura 1.9 Sistema de video IP que utiliza servidor de video** (Naranjo, 2007)

En la figura 1.9, se muestra un verdadero sistema de video IP, donde la información del video se transmite de forma continua a través de una red IP. Utiliza un servidor de video como elemento clave para migrar el sistema analógico de seguridad a una solución de video IP.

### 1.4.3.4. SISTEMAS DE VIDEO IP QUE UTILIZAN CÁMARAS IP[27]

Una cámara IP combina una cámara y un computador en una unidad, lo que incluye la digitalización y la compresión del video así como un conector de red.

El video se transmite a través de una red IP, mediante los switches 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 que utiliza cámaras IP añade las ventajas siguientes:

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

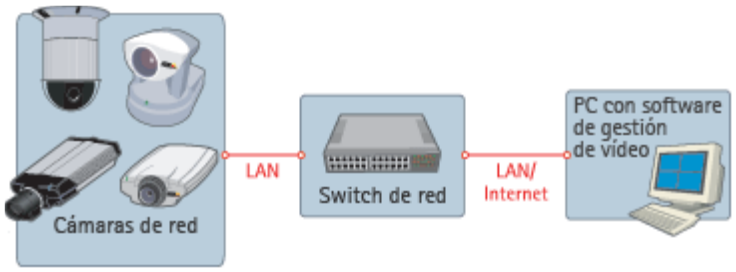



**Figura 1.10 Sistema de video IP que utiliza cámaras IP** (Naranjo, 2007)

En la Figura 1.10, se indica un verdadero sistema de video IP, donde la información del video se transmite de forma continua a través de una red IP, utilizando cámaras IP. Este sistema saca el máximo partido de la tecnología digital y proporciona una calidad de imagen constante desde la cámara hasta el visualizador.

La diferencia entre el Sistema de video IP que utilizan servidores de video y el Sistema de video IP que utiliza cámaras IP descrita en este subcapítulo, es que el

[27] Internet Protocol

Sistema de video IP descrita anteriormente utilizan cámaras análogas por ende para la transmisión hasta el servidor de video utilizan cable coaxial, en el servidor se digitaliza y comprime el video en la cual el servidor de video se enlaza con la red LAN, mientras que el Sistema descrito en este subcapítulo utiliza cámaras IP en la misma cámara incorpora un computador en el cual se digitaliza y comprime la señal de video para luego ser transmitido al servidor de video a través de la red LAN, en este sistema tanto las cámaras IP y el servidor forman la red LAN.

## 1.5. TIPO DE CÁMARAS DE RED (Axis, pág. 2)

Las cámaras de red se pueden clasificar en función de si están diseñadas únicamente para su uso en interiores o para su uso en interiores-exteriores. Las cámaras de red para exteriores suelen tener un objetivo con iris automático para regular la cantidad de luz a la que se expone el sensor de imagen. Una cámara de exteriores también necesitará una carcasa de protección externa, salvo que su diseño ya incorpore un cerramiento de protección. Las carcasas también están disponibles para cámaras para interiores que requieren protección frente a entornos adversos como polvo y humedad y frente a riesgo de vandalismo o manipulación.

Las cámaras de red, diseñadas para su uso en interiores o exteriores, pueden clasificarse en cámaras de red fijas, domo fijas, PTZ[28] y domo PTZ.

### 1.5.1. CÁMARA DE RED FIJAS

Una cámara de red fija, que puede entregarse con un objetivo fijo o varifocal, es una cámara que dispone de un campo de vista fijo (normal/telefoto/gran angular) una vez montada. Este tipo de cámara es la mejor opción en aplicaciones en las que resulta útil que la cámara esté bien visible. Normalmente, las cámaras fijas permiten que se cambien sus objetivos. Pueden instalarse en carcasas diseñadas para su uso en instalaciones interiores o exteriores.

[28] Pan-Tilt-Zoom

**Figura 1.11 Cámaras de red fijas** (Axis, Axis)

En la figura 1.11, se puede observar un sinnúmero de cámaras fijas las cuales incluyen versiones inalámbricas.

### 1.5.2. CÁMARA DE RED DOMO FIJAS.

Una cámara domo fija, también conocida como mini domo, consta básicamente de una cámara fija preinstalada en una pequeña carcasa domo. La cámara puede enfocar el punto seleccionado en cualquier dirección. La ventaja principal radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. Asimismo, es resistente a las manipulaciones.

Uno de los inconvenientes que presentan las cámaras domo fijas es que normalmente no disponen de objetivos intercambiables, y si pueden intercambiarse, la selección de objetivos está limitada por el espacio dentro de la carcasa domo. Para compensarlo, a menudo se proporciona un objetivo varifocal que permita realizar ajustes en el campo de visión de la cámara.

Las cámaras domo fijas están diseñadas con diferentes tipos de cerramientos, a prueba de vandalismo y/o con clasificación de protección IP66 cuyo valor significa, IP índice de protección, el primer digito 6 protección completa contra personas y entrada de polvo, el segundo digito 6 protección contra fuertes chorros de agua de todas direcciones, incluido olas. Generalmente, las cámaras domo fijas se instalan en la pared o en el techo.

**Figura 1.12 Cámaras de red domo fijas** (Axis, 2010)

### 1.5.3. CÁMARA PTZ

Las cámaras PTZ[29] pueden moverse horizontalmente, verticalmente y acercarse o alejarse de un área o un objeto de forma manual o automática. Todos los comandos PTZ se envían a través del mismo cable de red que la transmisión de video.

Algunas de las funciones que se pueden incorporar a una cámara PTZ:

Estabilización electrónica de imagen (EIS[30]). En instalaciones exteriores, las cámaras domo PTZ con factores de zoom superiores a los 20x son sensibles a las vibraciones y al movimiento causados por el tráfico o el viento. La estabilización electrónica de la imagen (EIS) ayuda a reducir el efecto de la vibración en un video. Además de obtener videos más útiles, EIS reducirá el tamaño del archivo de la imagen comprimida, de modo que se ahorrará un valioso espacio de almacenamiento.

Máscara de privacidad. La máscara de privacidad permite bloquear o enmascarar determinadas áreas de la escena frente a visualización o grabación para que en esa área no grave y aparezca en el video solo una franja blanca.

Posiciones predefinidas. Muchas cámaras PTZ permiten programar posiciones predefinidas, normalmente entre 20 y 100 posiciones. Una vez las posiciones

[29] Pan-Tilt-Zoom
[30] Estabilización electrónica de imagen

predefinidas se han configurado en la cámara, el operador puede cambiar de una posición a la otra de forma muy rápida.

En caso de que una cámara PTZ se monte en el techo y se utilice para realizar el seguimiento de una persona, por ejemplo en unos grandes almacenes, se producirán situaciones en las que el individuo en cuestión pasará justo por debajo de la cámara. Sin la funcionalidad E-flip, las imágenes de dicho seguimiento se verían del revés. En estos casos, E-flip gira las imágenes 180 grados de forma automática. Dicha operación se realiza automáticamente y no será advertida por el operador.

Auto-flip. Generalmente, las cámaras PTZ, a diferencia de las cámaras domo PTZ, no disponen de un movimiento vertical completo de 360 grados debido a una parada mecánica que evita que las cámaras hagan un movimiento circular continuo. Sin embargo, gracias a la función Auto-flip, una cámara de red PTZ puede girar al instante 180 grados su cabezal y seguir realizando el movimiento horizontal más allá de su punto cero. De este modo, la cámara puede continuar siguiendo el objeto o la persona en cualquier dirección.

Auto-seguimiento. El auto-seguimiento es una función de video inteligente que detecta automáticamente el movimiento de una persona o vehículo y lo sigue dentro de la zona de cobertura de la cámara. Esta función resulta especialmente útil en situaciones de video-vigilancia no controlada humanamente en las que la presencia ocasional de personas o vehículos requiere especial atención. La funcionalidad recorta notablemente el coste de un sistema de supervisión, puesto que se necesitan menos cámaras para cubrir una escena. Asimismo, aumenta la efectividad de la solución debido a que permite que las cámaras PTZ graben áreas de una escena en actividad.

Aunque las cámaras PTZ y domo PTZ comparten funciones similares, existen algunas diferencias entre ellas:

Las cámaras de red PTZ no disponen de un movimiento horizontal de 360 grados debido a la existencia de un tope mecánico. Esto significa que la cámara no puede seguir a una persona que esté andando de forma continua en un círculo completo alrededor del dispositivo. Son excepciones de ello las cámaras PTZ que disponen de la funcionalidad Auto-flip.

Las cámaras de red PTZ no están diseñadas para la operación automática continua o las llamadas rondas de vigilancia, en las que la cámara se mueve automáticamente de una posición predefinida a la siguiente.

### 1.5.3.1. CÁMARA DE RED PTZ MECÁNICA.

Las cámaras de red PTZ mecánicas se utilizan principalmente en interiores y en aplicaciones donde se emplea un operador. El zoom óptico en cámaras PTZ varía normalmente entre 10x y 26x. Una cámara PTZ se puede instalar en el techo o en la pared.

**Figura 1.13 Cámaras de red PTZ mecánica.** (Axis, Axis, 2010)

### 1.5.3.2. CÁMARA DE RED PTZ NO MECÁNICA

Las cámaras de red PTZ no mecánicas, ofrecen capacidades de movimiento horizontal, vertical y zoom sin partes móviles, de forma que no existe desgaste de potencia por lo que no existen motores para que realicen el movimiento. Con un objetivo gran angular, ofrecen un campo de visión más completo que las cámaras de red PTZ mecánicas.

**Figura 1.14 Cámara de red PTZ no mecánica.** (Axis, Axis, 2010)

Una cámara PTZ no mecánica utiliza un sensor de imagen megapíxel y permite que el operador aleje o acerque, de forma instantánea, cualquier parte de la escena sin que se produzca ninguna pérdida en la resolución de la imagen. Esto se consigue presentando una imagen de visión general en resolución VGA (640x480 píxeles) aunque la cámara capture una imagen de resolución mucho más elevada.

Cuando se da la orden a la cámara de acercar o alejar cualquier parte de la imagen de visión completa, el dispositivo utiliza la resolución megapíxel original para proporcionar una relación completa, en resolución VGA[31]. El primer plano resultante ofrece buenos detalles y una nitidez mantenida. Si se utiliza un zoom digital normal, la imagen acercada pierde, con frecuencia, en detalles y nitidez. Una cámara PTZ no mecánica resulta ideal para instalaciones discretas montadas en la pared.

### 1.5.3.3. CÁMARA DE RED DOMO PTZ[32]

Las cámaras de red domo PTZ pueden cubrir una amplia área al permitir una mayor flexibilidad en las funciones de movimiento horizontal, vertical y zoom.

Asimismo, permiten un movimiento horizontal continuo de 360 grados y un movimiento vertical de normalmente 180 grados. Debido a su diseño, montaje y dificultad de identificación del ángulo de visión de la cámara (el cristal de las cubiertas de la cúpula puede ser transparente o ahumado), las cámaras de red domo PTZ resultan idóneas para su uso en instalaciones discretas.

[31] Video Graphics Array
[32] Pan-Tilt-Zoom

Las cámaras de red domo PTZ también proporcionan solidez mecánica para operación continua en el modo ronda de vigilancia, en el que la cámara se mueve automáticamente de una posición predefinida a la siguiente de forma predeterminada o aleatoriamente. Normalmente, pueden configurarse y activarse hasta 20 rondas de vigilancia durante distintas horas del día. En el modo ronda de vigilancia, una cámara de red domo PTZ puede cubrir un área en el que se necesitarían 10 cámaras de red fijas ya que se pueden configurar para que vigilen en diferentes punto es decir que no solo graba el entorno total sino también puede grabar distintos puntos configurados. El principal inconveniente de este tipo de cámara es que sólo se puede supervisar una ubicación en un momento concreto, dejando así las otras nueve posiciones sin supervisar.

El zoom óptico de las cámaras domo PTZ se mueve, generalmente, entre valores de 10x y 35x. Las cámaras domo PTZ se utilizan con frecuencia en situaciones en las que se emplea un operador. En caso de que se utilice en interiores, este tipo de cámara se instala en el techo o en un poste o esquina para instalaciones exteriores.

**Figura 1.15 Cámaras de red domo PTZ[33].** (Axis, Axis, 2010)

### 1.5.3.4. CÁMARA DE RED CON VISIÓN DIURNA/NOCTURNA

La totalidad de los tipos de cámaras de red, fijas, domo fijas, PTZ y domo PTZ, dispone de función de visión diurna y nocturna. Las cámaras con visión diurna y nocturna están diseñadas para su uso en instalaciones exteriores o en entornos interiores con poca iluminación.

[33] Pan-Tilt-Zoom

Las cámaras de red a color con visión diurna y nocturna proporcionan imágenes a color a lo largo del día. Cuando la luz disminuye bajo un nivel determinado, la cámara puede cambiar automáticamente al modo nocturno para utilizar la luz prácticamente infrarroja IR (radiación infrarroja) para proporcionar imágenes de alta calidad en blanco y negro.

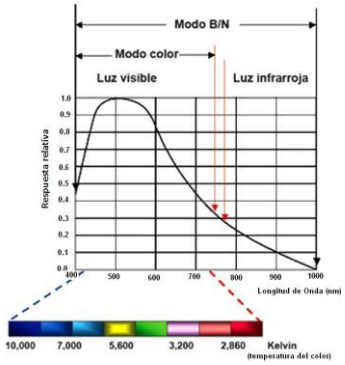



**Figura 1.16 Respuesta del sensor a la luz infrarroja visible**

En la figura 1.16, se muestra cómo un sensor de imagen responde a la luz infrarroja visible y a la luz próxima al espectro infrarrojo. La luz casi-infrarroja, se observa que implica con la longitud de onda desde 700 nanómetros (nm) hasta cerca de 1.000 nm, está más allá de la visión humana, pero la mayoría de los sensores de cámara pueden detectarla y utilizarla, pero como se puede observar en la figura que la respuesta relativa del sensor de imagen va disminuyendo frente a la longitud de onda. Durante el día, la cámara de visión diurna y nocturna utiliza un filtro de paso IR[34]. La luz de paso IR se filtra de modo que no distorsiona los colores de las imágenes en el momento en que el ojo humano las ve, como se puede observar en la figura cuando se tiene una longitud de onda entre los 500 nanómetros la respuesta relativa del sensor de imagen llega a un máximo, en esos puntos se puede obtener un comportamiento casi sin distorsión de colores frente a la imagen. Cuando la cámara está en modo nocturno (blanco y negro), el filtro de paso IR se elimina, lo que permite que la sensibilidad lumínica de la cámara alcance los 0,001 lux o un nivel inferior.

[34] Radiación infrarroja

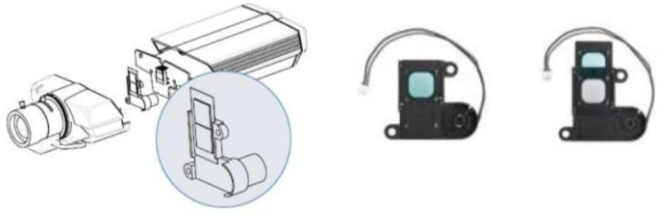


**Figura 1.17 Cámara de red con visión diurna y nocturna.** (Axis, Axis)

En la figura 1.17, se puede observar a la izquierda una cámara de red con visión diurna y nocturna y con filtro de paso IR; en el centro, posición de un filtro de paso IR durante el día y a la derecha, posición del filtro de paso IR durante la noche.

Las cámaras diurnas/nocturnas resultan útiles en entornos que restringen el uso de luz artificial. Incluyen vigilancia por video con escasa luz, vigilancia oculta y aplicaciones discretas, por ejemplo, en una situación de vigilancia del tráfico en la que las luces brillantes podrían entorpecer la conducción nocturna. Los iluminadores de infrarrojos que proporcionan luz próxima al espectro infrarrojo también pueden utilizarse junto con las cámaras de visión diurna/nocturna para mejorar la capacidad de producción de video de alta calidad en condiciones de escasez lumínica o nocturna.

**Figura 1.18 Comparación entre una imagen con ilustración infrarrojo y sin ilustración infrarrojo** (Axis, Axis)

En la figura 1.18, a la izquierda se observa una imagen en la noche sin iluminador de infrarrojos; a la derecha, imagen con un iluminador de infrarrojos, en la misma se puede distinguir claramente que cuando se tiene una cámara con ilustrador de infrarrojos se observa todo el entorno enfocado por la cámara.

### 1.5.3.5 CÁMARAS DE RED CON RESOLUCIÓN MEGAPÍXEL (Axis)

Las cámaras de red con resolución megapíxel, disponible en las cámaras fijas y domo fijas, incorporan un sensor de imagen megapíxel para proporcionar imágenes con un millón o más megapíxeles.

Se trata de una resolución como mínimo dos veces mejor que la que ofrecen las cámaras analógicas. Las cámaras de red fijas con resolución megapíxel pueden utilizarse de una de las dos formas siguientes: pueden permitir a los visualizadores ver detalles más concretos en una resolución de imagen más elevada, lo que puede resultar útil para la identificación de personas y de objetos.

Asimismo, pueden utilizarse para cubrir una parte más amplia de la escena si la resolución de imagen se mantiene como la de las cámaras sin resolución megapíxel. Actualmente, las cámaras con resolución megapíxel son, en general, menos sensibles a la luz que las cámaras de red que no incorporan esta tecnología.

Las secuencias de video de resolución más elevada generadas por las cámaras con resolución megapíxel también requieren requisitos más exigentes en el ancho de banda de la red y el espacio de almacenamiento para las grabaciones, aunque estas exigencias pueden reducirse utilizando el estándar de compresión de video H.264.

A continuación un resumen de los tipos de cámaras.

| Tipo de cámaras | Características | Variantes |
|---|---|---|
| Cámara de red fijas | • Dispone de un campo de vista (normal/telefoto/gran angular) | Puede elegir cámaras de red fijas con:<br>• Resolución megapíxel<br>• Funciones para exteriores<br>• Alimentación a través de Ethernet<br>• Sonido bidireccional<br>• Conectividad inalámbrica. |
| Cámara de red domo fijas | Una cámara domo fija es una cámara de pequeño tamaño que se alberga en una carcasa de forma abovedada. Su ventaja radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia que dirección apunta la cámara. Además, la carcasa abovedada de la cámara la protege de forma eficaz contra el redireccionamiento y el desenfoque. | Tiene a su elección diferentes domo fijos, entre ellas cámaras que ofrecen:<br>• Resolución megapíxel<br>• Carcasa a prueba de agresiones<br>• Gama de temperaturas mejorada<br>• Sonido bidireccional<br>• Alimentación a través de Ethernet<br>• Características especiales para autobuses y trenes. |
| Cámara de red PTZ mecánicas | Es una cámara de red PTZ mecánica en la que tanto el movimiento como la dirección de visualización sean visibles | La gama de cámaras PTZ incluye cámaras con:<br>• Zoom óptico de hasta 26x<br>• Funcionalidad de visión día/noche<br>• Una mecánica precisa y rápida de movimiento horizontal y vertical<br>• Resolución megapíxel<br>• Lámpara IR integrada<br>• Sonido bidireccional |

**Figura 1.19 Tipos de cámaras IP** (Axis, Concepto sobre cámara IP)

## 1.6. COMPONENTES QUE CONSTITUYEN UNA CÁMARA IP (Axis, Axis, 2010, pág. 27)

**Básicamente una cámara IP se compone de:**

- La " cámara " de video tradicional (lentes, sensores, procesador digital de imagen, etc)
- Un sistema de compresión de imagen (para poder comprimir las imágenes captadas por la cámara a formatos adecuados como MPEG4 [35]
- La CPU[36], la memoria Flash y la memoria DRAM representan el "cerebro" o las funciones informáticas de la cámara y están diseñadas específicamente para aplicaciones de red. Gestionan la comunicación con la red y el servidor Web.

[35] Moving Picture Experts Group
[36] Unidad Central de Procesamiento

- A través del puerto Ethernet, una cámara de red de gama alta puede enviar imágenes directamente a diez o más computadores de forma simultánea. Si las imágenes se envían primero a un servidor Web externo (en lugar de directamente a los usuarios que las visualizan), un número ilimitado de usuarios puede ver el video en tiempo real.

### 1.6.1. FUNCIONAMIENTO DE LAS CÁMARAS IP (Axis, Concepto sobre cámara IP)

Las cámaras IP se conectan directamente a la conexión LAN de la instalación de internet o red doméstica u oficina a través de un router, asignándole una dirección IP interna. Cada una de las cámaras envían la información por medio del servicio de banda ancha y se accede a ella a través de cualquier PC conectada a internet con sólo teclear en el navegador la dirección IP de la cámara que se quiere observar. Es decir, se ingresa a la página web del sistema, donde la visualización de las imágenes es sumamente sencilla y desde donde se puede mover las cámaras en diferentes direcciones es una cámara PTZ (Pan-Tilt-Zoom), se puede tomar fotografías, grabar videos y hasta escuchar el sonido del ambiente monitoreado.

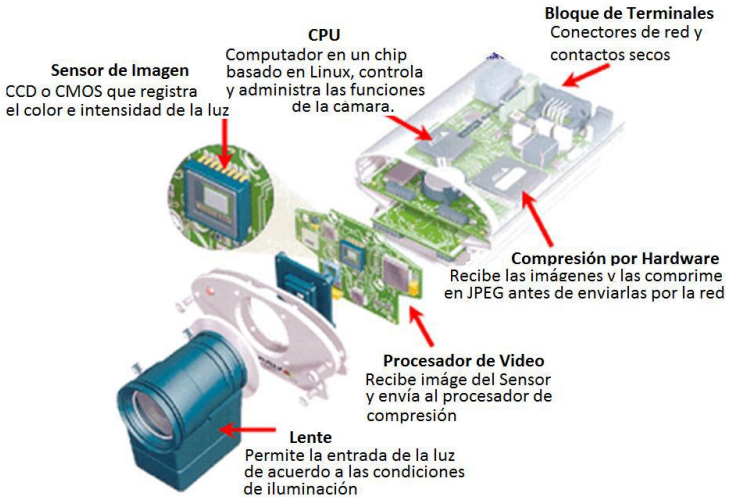



**Figura 1.20 Componentes de una cámara de red.** (Axis, Axis)

En la figura 1.20, se observa los componentes que constituyen una cámara IP, a continuación se explica el funcionamiento de una cámara IP:

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

b. El lente de la cámara enfoca la imagen en el sensor CCD / CMOS[37] antes de esto la imagen pasa a través del filtro óptico el cual remueve cualquier luz infrarroja (IR) para que los colores sean mostrados correctamente. En cámaras infrarrojas, este filtro es removible para que se pueda proporcionar imágenes de alta calidad en blanco y negro en condiciones de poca iluminación. Finalmente el sensor de imagen transforma las ondas de luz en señales eléctricas que a su vez se convierten en señales digitales en un formato que puede ser comprimido y transferido por la red.

c. El procesador realiza las funciones de administración y control de la exposición (Niveles de Luz), balance de blancos (Ajuste de Colores), brillo de la imagen y otros aspectos relacionados con la calidad de la imagen, también este procesador incluye un componente de compresión el cual comprime las imágenes digitales a un formato que contiene menos datos y que puede ser transmitido por la red de forma eficiente.

d. El conector de red Ethernet es habilitado por el chip ETRAX[38], desarrollado por Axis, el cual es una solución optimizada para conectar periféricos en la red. El chip ETRAX incluye un CPU de 32 bits, conectividad Ethernet de 10/100 Mbits, funciones avanzadas para el manejo de memoria directa (DMA) y un amplio rango de interfaces de entrada/salida.

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

[37] Ccharge-coupled device /Complementary Metal Oxide Semiconductor
[38] Ethernet, Token Ring, Axis

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

Con todo esto únicamente se necesita conectar la cámara IP al Router ADSL[39] y a la alimentación eléctrica, si se piensa usar la cámara en una red local se conecta la cámara a un HUB (es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás) o en un SWITCH y pasa a ser un equipo más que se comunica con el resto de la LAN (y con el exterior si la red LAN dispone de conexión a Internet).

### 1.6.2 ACCESO A UNA CÁMARA IP

El acceso a las cámaras se realiza vía Web Browser o mediante un software administrador, el mismo que permiten establecer varios niveles de seguridad sobre el acceso entre ellos se pueden mencionar:

**Administrador:** Para poder configurar el sistema, a este usuario se debe proteger mediante una contraseña ya que mediante este usuario se puede configurar todo el sistema.
**Usuario:** Para poder ver las imágenes, manejar la cámara y manejo del relé de salida. Pide un usuario y una contraseña.

### 1.6.3. ADMINISTRACIÓN DEL VIDEO (Axis, Axis, 2010)

Un aspecto importante del sistema de video-vigilancia es la gestión de video para la visualización, grabación, reproducción y almacenamiento en directo. Si el

[39] Asymmetric Digital Subscriber Line

sistema está formado por una sola cámara o por pocas cámaras, la visualización y la grabación básica de video se pueden gestionar mediante la interfaz Web incorporada de las cámaras de red y los codificadores de video. Cuando el sistema consta de más cámaras, se recomienda utilizar un sistema de gestión de video en red.

Actualmente, existen cientos de sistemas de gestión de video diferentes, cubriendo diferentes sistemas operativos (Windows, UNIX, Linux y Mac OS), segmentos de mercado e idiomas. Los aspectos que deben considerarse son la elección de plataforma de hardware (PC basado en servidor o uno basado en una grabadora de video en red); plataforma de software; características del sistema, que incluyen la instalación y configuración, gestión de eventos, video inteligente, administración y seguridad; y posibilidades de integración con otros sistemas, como punto de venta o gestión de edificios.

### **1.6.4. PLATAFORMA DE HARDWARE** (Axis, Axis, 2010)

Existen dos tipos diferentes de plataformas de hardware para un sistema de gestión de video en red: una plataforma de servidor de PC formada por uno o más PC que ejecuta un programa de software de gestión de video y uno basado en una grabadora de video en red que es un hardware patentado con software de gestión de video preinstalado.

 Plataformas de servidor de PC, una solución de gestión de video basada en una plataforma de servidor de PC incluye servidores de PC y equipos de almacenamiento que se pueden seleccionar directamente con el fin de obtener un rendimiento superior para el diseño específico del sistema. Una plataforma abierta de estas características facilita la opción de añadir funcionalidades al sistema, como un almacenamiento incrementado o externo, firewalls, protección contra virus y algoritmos de video inteligentes, en paralelo con un programa de software de gestión de video. Una plataforma de servidor de PC también se puede ampliar,

permitiendo añadir cuantos productos de video en red sean necesarios. El hardware del sistema se puede ampliar o actualizar para satisfacer nuevas necesidades de rendimiento. Una plataforma abierta también permite una integración más sencilla con otros sistemas como control de acceso, gestión de edificios y control industrial. Esto permite a los usuarios gestionar video y otros controles de edificios mediante un simple programa e interfaz de usuario.

 Plataforma NVR, un grabador de video en red se presenta como una caja de hardware con funcionalidades de gestión de video preinstaladas. En este sentido, un NVR es parecido a un DVR. (Algunos DVR, también llamados DVR híbridos, incluyen una función NVR, es decir, la capacidad también de grabar video basado en red). Un hardware de NVR normalmente está patentado y diseñado específicamente para gestión de video. Está dedicado a sus tareas específicas de grabación, análisis y reproducción de video en red y normalmente no permite que ninguna otra aplicación se conecte a éste. El sistema operativo puede ser Windows,

### 1.6.5. PLATAFORMA DE SOFTWARE

Se pueden utilizar plataformas de software diferentes para gestionar video. Implican el uso de interfaz Web incorporada, o el uso de un programa de software de gestión de video independiente que es una interfaz basada en Windows o en Web.

 Funcionalidad incorporada, se puede acceder a las cámaras de red por medio de la red introduciendo la dirección IP del producto en el campo Dirección/Ubicación de un navegador Web de un computador. Una vez se ha conectado con el producto de video en red, se visualiza de forma automática en el navegador la ―página inicial‖ del producto junto con los enlaces a las páginas de configuración del producto. La interfaz Web incorporada de los productos de video en red de Axis ofrece funciones de grabación simples: grabación manual de secuencias de video

(H.264, MPEG-4, Motion JPEG[40]) a un servidor haciendo clic en un icono; o grabación activada por evento de imágenes JPEG individuales a una o varias ubicaciones. La grabación activada por evento de secuencias de video es posible con productos de video en red que admiten almacenamiento local. Para obtener una mayor flexibilidad y más funcionalidades de grabación en términos de modos (por ejemplo, grabaciones continuas o programadas), se requiere un programa de software de gestión de video independiente. La configuración y gestión de un producto de video en red mediante su interfaz Web incorporada sólo funciona cuando se tiene un sistema con número reducido de cámaras.

Software basado el cliente de Windows, cuando se llega a programas de software independientes para gestión de video, los programas basados en cliente de Windows son los más populares. Los programas de software basados en Web también están disponibles. Con un programa basado en cliente de Windows, primero se debe instalar el software de gestión de video en el servidor de grabación. Después, se puede instalar un programa de software de cliente de visualización en el mismo servidor de grabación o en cualquier PC, ya sea localmente en la misma red donde se encuentra el servidor de grabación o remotamente en una estación de visualización ubicada en una red independiente.

En algunos casos, la aplicación cliente también permite a los usuarios cambiar entre diferentes servidores que tengan el software de gestión de video instalado y, de este modo, hacer posible la gestión de video en un sistema grande o en muchos sitios remotos.

 Software basado en web, primero se debe instalar un programa de software de gestión de video basado en Web en un servidor de PC que sirva tanto de servidor Web como de grabación. Esto permite a los usuarios de cualquier parte y con cualquier tipo de computador conectado a la red acceder al servidor de gestión de video y, así a los productos de video en red que gestiona, simplemente utilizando un navegador Web

[40] Joint Photographic Experts Group

### 1.6.6. GRABACIÓN DE VIDEO (Superinventos)

Se puede grabar video manualmente, de forma continuada y por activación (movimiento o alarma) y se pueden programar grabaciones continuas y activadas para que se ejecuten en horas seleccionadas durante cada día de la semana. Las grabaciones continuas suelen utilizar más espacio de disco que las grabaciones activadas por alarma. Una detección de movimiento de video o entradas externas por el puerto de entrada de una cámara o codificador de video puede que activen la grabación activada por alarma. Mediante las grabaciones programadas, se pueden configurar los horarios tanto para las grabaciones continuas como para las activadas por alarma o movimiento.

Una vez esté seleccionado el tipo de método de grabación, la calidad de las grabaciones se puede especificar seleccionando el formato de video (p. ej. H.264, MPEG-4, Motion JPEG), la resolución, el nivel de compresión y la frecuencia de imagen. Estos parámetros afectarán la cantidad de ancho de banda utilizado, así como el tamaño del espacio de almacenamiento requerido. Los productos de video en red pueden tener capacidades de frecuencia de imagen diversas en función de la resolución. Grabar y/o visualizar a frecuencia de imagen máxima (considerada como 30 imágenes por segundo en estándar NTSC y 25 en estándar PAL) en todas las cámaras y en todo momento supera lo que se requiere para la mayoría de aplicaciones. Las frecuencias de imagen en condiciones normales se pueden configurar a un nivel más bajo.

### 1.6.7. ALMACENAMIENTO (Superinventos)

La mayor parte de software de gestión de video utiliza el sistema de ficheros de Windows estándar para el almacenamiento, así que se puede utilizar cualquier disco del sistema o conectado a la red para el almacenamiento de video. Un programa de software de gestión de video puede activar más de un nivel de almacenamiento. Por ejemplo, las grabaciones se efectúan en un disco duro principal (el disco duro local) y el archivo se realiza en discos locales, conectados

a la red o discos duros remotos. Los usuarios pueden especificar cuánto tiempo deben permanecer las imágenes en el disco duro principal antes que se eliminen automáticamente o se muevan al disco de archivo. También pueden evitar que se eliminen automáticamente los videos activados por eventos, señalándolos de forma especial o bloqueándolos en el sistema.

### **1.6.8. RESOLUCIONES** (Axis, Axis, 2010)

La resolución en un mundo digital o analógico es parecida, pero existen algunas diferencias importantes sobre su definición. En el video analógico, una imagen consta de líneas o líneas de TV, puesto que la tecnología de video deriva de la industria de la televisión. En un sistema digital, una imagen está formada por píxeles cuadrados.

Los apartados que siguen a continuación muestran las distintas resoluciones que puede proporcionar el video en red. Estas son: NTSC[41], PAL[42], VGA[43], Megapíxel y HDTV[44].

#### **1.6.8.1. RESOLUCIONES NTSC Y PAL** (Axis, Axis, 2010)

Las resoluciones NTSC y PAL son estándares de video analógico. Son relevantes para el video en red, ya que los codificadores de video proporcionan dichas resoluciones al digitalizar señales de cámaras analógicas. Las cámaras de red PTZ actuales y las cámaras domo de red PTZ también ofrecen resoluciones NTSC y PAL, puesto que hoy en día utilizan un bloque (que incorpora la cámara, zoom, enfoque automático y funciones de iris automático) hecho para cámaras de video analógico, conjuntamente con una tabla de codificación de video integrada.

[41] National Television System Comité: Comité Nacional de Sistemas de Televisión
[42] Phase Alternating Line: Línea de Alternancia de Fase
[43] Video Graphics Array: Tabla de Gráficos de Video
[44] High Definition Television: televisión de alta definición

En Norteamérica y Japón, el estándar NTSC es la norma de video analógico que predomina, mientras que en Europa y en muchos países de Asia y África se utiliza la norma PAL. Ambos estándares proceden de la industria de la televisión. El NTSC tiene una resolución de 480 líneas y utiliza una frecuencia de actualización de 60 campos entrelazados por segundo (o 30 imágenes completas por segundo). Para este estándar existe una nueva convención llamada 480i60 (La imagen mide 720x480 pixeles, desplegada a 60 cuadros entrelazados por segundo), que define el número de líneas, el tipo de escaneado y la frecuencia de actualización. El PAL tiene una resolución de 576 líneas y utiliza una frecuencia de actualización de 50 campos entrelazados por segundo (o 25 imágenes completas por segundo). La nueva convención para este estándar es 576i50 (La imagen mide 720x576 pixeles, desplegada a 50 cuadros entrelazados por segundo). La cantidad total de información por segundo es la misma en ambos estándares.

Cuando el video analógico se digitaliza, la cantidad máxima de píxeles que pueden crearse se basará en el número de líneas de TV disponibles para ser digitalizadas. El tamaño máximo de una imagen digitalizada suele ser D1 (D1: en el estándar NTSC la imagen mide 720x480 pixeles, y D1: en el estándar PAL la imagen mide 720x576 pixeles), y la resolución más común es 4CIF. Cuando se muestra en una pantalla de computador, el video analógico digitalizado puede mostrar efectos de entrelazado como el desgaste, y las formas pueden aparecer ligeramente deformadas, ya que es posible que los píxeles generados no concuerden con los píxeles cuadrados de la pantalla, mientras que la relación de aspecto del video se corrige antes de visualizarlo para asegurarse, por ejemplo, de que un círculo de un video analógico siga siendo un círculo cuando se muestre en una pantalla de computador.

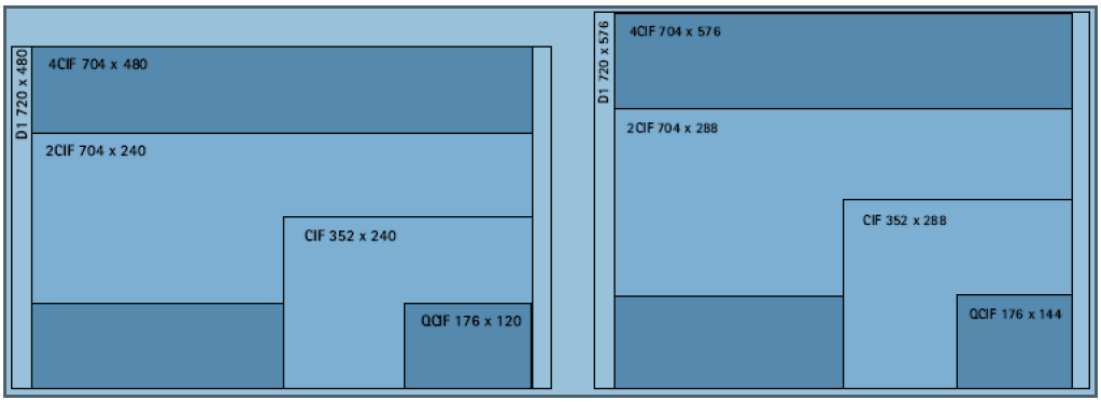



**Figura 1.21 Resoluciones de imagen NTSC y PAL** (Axis, 2010)

En la figura 1.21, se observan dos gráficos el primer gráfico el de la izquierda corresponde al estándar NTSC, que maneja una resolución máxima de la imagen de 720x480 pixeles, desplegada a 60 cuadros entrelazados por segundo, mientras que en el gráfico de la derecha se observa los diferentes resoluciones del estándar PAL, que maneja una resolución máxima de la imagen de 720x576 pixeles, desplegada a 50 cuadros entrelazados por segundo.

**1.6.8.2. RESOLUCIONES VGA** (Axis, Axis, 2010)

Con los sistemas 100% digitales basados en cámaras de red se pueden proporcionar resoluciones derivadas de la industria informática y normalizada en todo el mundo, de modo que la flexibilidad es mayor. Las limitaciones del NTSC y el PAL son insignificantes. VGA (Video Graphics Array: Tabla de Gráficos de Video), es un sistema de pantalla de gráficos para PC desarrollado originalmente por IBM. Esta resolución es de 640 x 480 píxeles, un formato habitual en las cámaras de red que no disponen de megapíxeles. La resolución VGA suele ser más adecuada para cámaras de red, ya que el video basado en VGA produce píxeles cuadrados que coinciden con los de las pantallas de computador.

Los monitores de computador manejan resoluciones en VGA o múltiplos de VGA.

| Formato de visualización | Píxeles |
|---|---|
| QVGA (SIF) | 320x240 |
| VGA | 640x480 |
| SVGA | 800x600 |
| XVGA | 1024x768 |
| 4x VGA | 1280x960 |

**Tabla 1.1 Formatos de resoluciones VGA.** (Axis, Axis, 2010)

### 1.6.8.3. RESOLUCIONES MEGAPÍXEL

Una cámara de red que ofrece una resolución megapíxel utiliza un sensor megapíxel para proporcionar una imagen que contiene un millón de megapíxeles o más. Cuántos más píxeles tenga el sensor, mayor potencial tendrá para captar más detalles y ofrecer una calidad de imagen mayor. Con las cámaras de red megapíxel los usuarios pueden obtener más detalles (ideal para la identificación de personas y objetos) o para visualizar un área mayor del escenario. Esta ventaja supone una importante consideración en aplicaciones de video vigilancia.

| Formato de visualización | Nº de megapíxeles | Píxeles |
|---|---|---|
| SXGA | 1.3 megapíxeles | 1280x1024 |
| SXGA+(EXGA) | 1.4 megapíxeles | 1400x1050 |
| UXGA | 1.9 megapíxeles | 1600x1200 |
| WUXGA | 2.3 megapíxeles | 1920x1200 |
| QXGA | 3.1 megapíxeles | 2048x1536 |
| WQXGA | 4.1 megapíxeles | 2560x1600 |
| QSXGA | 5.2 megapíxeles | 2560x2048 |

**Tabla 1.2 Formatos de visualización megapíxel.** (Axis, Axis, 2010)

La resolución megapíxel es un área en la que las cámaras de red se distinguen de las analógicas. La resolución máxima que puede proporcionar una cámara

analógica convencional tras haber digitalizado la señal de video en una grabadora o codificador de video es D1, es decir, 720 x 480 píxeles (NTSC) o 720 x 576 píxeles (PAL). La resolución D1 corresponde a un máximo de 414.720 píxeles ó 0,4 megapíxeles. En comparación, un formato megapíxel común de 1280 x 1024 píxeles consigue una resolución de 1,3 megapíxeles. Esto es más del triple de la resolución que pueden proporcionar las cámaras analógicas de CCTV. También se encuentran disponibles cámaras de red con resoluciones de 2 megapíxeles y 3 megapíxeles, e incluso se esperan resoluciones superiores en el futuro.

La resolución megapíxel también consigue un mayor grado de flexibilidad, es decir, es capaz de proporcionar imágenes con distintas relaciones de aspecto. (La relación de aspecto es la relación entre la anchura y la altura de una imagen). Una pantalla de televisión convencional muestra una imagen con una relación de aspecto de 4:3. Las cámaras de red con resolución megapíxel pueden ofrecer la misma relación, además de otras, como 16:9. La ventaja de la relación de aspecto 16:9 es que los detalles insignificantes, que suelen encontrarse en las partes superior e inferior de una imagen con un tamaño convencional, no aparecen y, por lo tanto, puede reducirse el ancho de banda y los requisitos de almacenamiento.


**Figura 1.22 Ilustración de las relaciones de aspecto 4:3 y 16:9.** (Axis, Axis, 2010)

**1.7. COMPRESIÓN DE VIDEO** (Axis, Axis, 2010)

Las técnicas de compresión de video consisten en reducir y eliminar datos redundantes del video para que el archivo de video digital se pueda enviar a través de la red y almacenar en discos informáticos. Con técnicas de compresión eficaces

se puede reducir considerablemente el tamaño del fichero sin que ello afecte muy poco, o en absoluto, la calidad de la imagen. Sin embargo, la calidad del video puede verse afectada si se reduce en exceso el tamaño del fichero aumentando el nivel de compresión de la técnica que se utilice.

Existen diferentes técnicas de compresión, tanto patentadas como estándar. Hoy en día, la mayoría de proveedores de video en red utilizan técnicas de compresión estándar. Los estándares son importantes para asegurar la compatibilidad y la interoperabilidad. Tienen un papel especialmente relevante en la compresión de video, puesto que éste se puede utilizar para varias finalidades y, en algunas aplicaciones de video-vigilancia, debe poderse visualizar varios años después de su grabación. Gracias al desarrollo de estándares, los usuarios finales tienen la opción de escoger entre diferentes proveedores, en lugar de optar a uno solo para su sistema de video-vigilancia.

### **1.7.1. CONCEPTOS BÁSICOS DE COMPRESIÓN** (Axis, Axis, 2010)

#### **1.7.1.1. CÓDEC DE VIDEO**

En el proceso de compresión se aplica un algoritmo al video original para crear un archivo comprimido y ya listo para ser transmitido o guardado. Para reproducir el archivo comprimido, se aplica el algoritmo inverso y se crea un video que incluye prácticamente el mismo contenido que el video original. El tiempo que se tarda en comprimir, enviar, descomprimir y mostrar un archivo es lo que se denomina latencia. Cuanto más avanzado sea el algoritmo de compresión, mayor será la latencia.

El par de algoritmos que funcionan conjuntamente se denomina códec de video (codificador/decodificador). Los códecs de video de estándares diferentes no suelen ser compatibles entre sí, es decir, el contenido de video comprimido con un estándar no se puede descomprimir con otro estándar diferente. Esto ocurre simplemente porque un algoritmo no puede decodificar correctamente los datos de

salida del otro algoritmo, pero es posible usar muchos algoritmos diferentes en el mismo software o hardware, que permitirían la coexistencia de varios formatos.

### 1.7.1.2. COMPRESIÓN DE IMAGEN

La compresión de imagen utiliza la tecnología de codificación intrafotograma. Los datos se reducen a un fotograma de imagen con el fin de eliminar la información innecesaria que pueden ser imperceptible para el ojo humano.

**Figura 1.23 Modo de compresión de imagen** (Axis, Axis, 2010)

En la figura 1.23, las tres imágenes de la secuencia se codifican y se envían como imágenes únicas y separadas (fotogramas I), sin que dependan unas de otras.

### 1.7.1.3. COMPRESIÓN DE VIDEO

Los algoritmos de compresión de video utilizan la predicción interfotograma para reducir los datos de video entre las series de fotogramas. Ésta consiste en técnicas como la codificación diferencial, en la que un fotograma se compara con un fotograma de referencia y sólo se codifican los píxeles que han cambiado con respecto al fotograma de referencia. De esta forma, se reduce el número de valores de píxeles codificados y enviados. Cuando se visualiza una secuencia codificada de este modo, las imágenes aparecen como en la secuencia de video original.

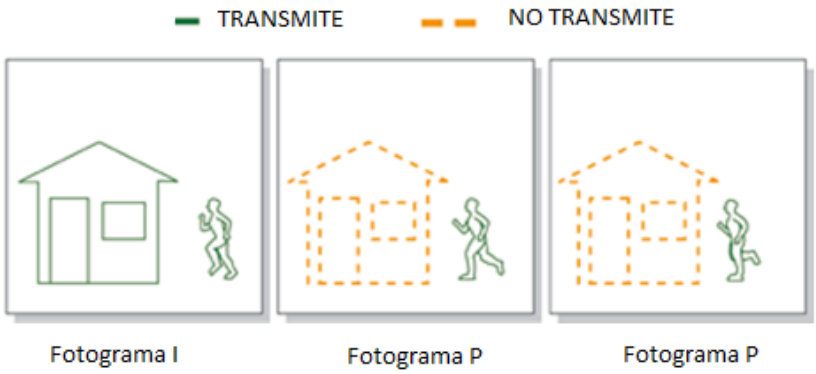



**Figura 1.24 Codificación diferencial** (Axis, 2010)

En la figura 1.24 con la codificación diferencial sólo la primera imagen (fotograma I) se codifica en su totalidad. En las dos imágenes siguientes (fotogramas P) existen referencias a la primera imagen en lo que se refiere a elementos estáticos, como la casa. Sólo se codifican las partes en movimiento (el hombre que corre) mediante vectores de movimiento, reduciendo así la cantidad de información que se envía y almacena.

Para reducir aún más los datos, se pueden aplicar otras técnicas como la compensación de movimiento basada en bloques. La compensación de movimiento basada en bloques tiene en cuenta que gran parte de un fotograma nuevo está ya incluido en el fotograma anterior, aunque quizás en un lugar diferente del mismo. Esta técnica divide un fotograma en una serie de macro bloques (bloques de píxeles). Se puede componer o ―predecir‖ un nuevo fotograma bloque a bloque, buscando un bloque que coincida en un fotograma de referencia. Si se encuentra una coincidencia, el codificador codifica la posición en la que se debe encontrar el bloque coincidente en el fotograma de referencia. La codificación del vector de movimiento, como se denomina, precisa de menos bits que si hubiera de codificarse el contenido real de un bloque.

### 1.7.1.4 FORMATOS DE COMPRESIÓN (Axis, Axis, 2010)

#### 1.7.1.4.1. MOTION JPEG

Motion JPEG o M-JPEG es una secuencia de video digital compuesta por una serie de imágenes JPEG[45] individuales. Cuando se visualizan 16 o más imágenes por segundo, el ojo humano lo percibe como un video en movimiento. Un video en completo movimiento se percibe a 30 imágenes por segundo en el estándar NTSC o a 25 imágenes por segundo en el estándar PAL.

Una de las ventajas de Motion JPEG es que cada imagen de una secuencia de video puede conservar la misma calidad garantizada que se determina mediante el nivel de compresión elegido para la cámara de red o codificador de video. Cuanto más alto es el nivel de compresión, menor es el tamaño del archivo y la calidad de imagen. En algunas situaciones, como cuando hay poca luz o la escena es compleja, el tamaño del archivo puede ser bastante grande y, por lo tanto, usar más ancho de banda y espacio de almacenamiento.

Al no haber dependencia alguna entre los fotogramas de Motion JPEG, un video Motion JPEG es resistente, lo que significa que si falla un fotograma durante la transmisión, el resto del video no se verá afectado.
Motion JPEG es un estándar que no requiere licencia. Tiene una amplia compatibilidad y su uso es muy habitual en aplicaciones donde se requieren fotogramas individuales en una secuencia de video por ejemplo, para el análisis y donde se utiliza una frecuencia de imagen de 5 fotogramas por segundo o inferior. Motion JPEG también puede ser útil para aplicaciones que requieren integración con sistemas que sólo son compatibles con Motion JPEG.

Sin embargo, el principal inconveniente de Motion JPEG es que no utiliza ninguna técnica de compresión de video para reducir datos, ya que consiste en una serie de imágenes fijas y completas. El resultado es una frecuencia de bits

[45] Joint Photographic Experts Group

relativamente alta o una relación de compresión baja para la calidad proporcionada, en comparación con otros estándares de compresión de video como MPEG-4 y H.264.

#### 1.7.1.4.2. MPEG-4

Cuando se menciona MPEG[46]-4 en las aplicaciones de video vigilancia, normalmente se refiere a MPEG-4 Parte 2, también conocido como MPEG-4 Visual. Como todos los estándares MPEG, requiere una licencia, es decir, los usuarios deben pagar una tasa de licencia por cada estación de supervisión. MPEG-4 es compatible con aplicaciones de ancho de banda reducido y aplicaciones que requieren imágenes de alta calidad, sin limitaciones de frecuencia de imagen y con un ancho de banda virtualmente ilimitado.

#### 1.7.1.4.3. H.264 o MPEG-4 Part 10/AVC

El H.264, también conocido como MPEG-4 Parte 10/AVC para Codificación de Video Avanzada, es el estándar MPEG más actual para la codificación de video. Se espera que el H.264 se convierta en la alternativa de estándar en los próximos años. Ello se debe a que, sin comprometer la calidad de la imagen, un codificador H.264 puede reducir el tamaño de un archivo de video digital en más de un 80% si se compara con el formato Motion JPEG, y hasta un 50% más en comparación con el estándar MPEG-4. Esto significa que se requiere menos ancho de banda y espacio de almacenamiento para los archivos de video, o visto de otra manera, se puede lograr mayor calidad de imagen de video para una frecuencia de bits determinada.

El H.264 ha sido definido conjuntamente por organizaciones de normalización del sector de las telecomunicaciones (ITU-T's[47]) y de las tecnologías de la información (ISO/IEC[48]), y se espera que tenga una mayor adopción que los

[46] Moving Picture Experts Group
[47] Video Coding Experts Group
[48] Moving Picture Experts Group

estándares anteriores. En el sector de la video vigilancia, H.264 encontrará su mayor utilidad en aplicaciones donde se necesiten velocidades y resoluciones altas, como en la vigilancia de autopistas, aeropuertos y casinos, lugares donde por regla general se usa una velocidad de 30/25 (NTSC/PAL) imágenes por segundo. Es aquí donde las ventajas económicas de un ancho de banda y un almacenamiento reducidos se harán sentir de forma más clara.

Se espera que H.264 acelere también la adopción de cámaras megapíxel, ya que con esta eficiente tecnología de compresión se pueden reducir los archivos de gran tamaño y las frecuencias de bits sin que la calidad de la imagen se vea afectada.

En cualquier caso, tiene sus exigencias: aunque H.264 permite ahorrar en costes de ancho de banda y almacenamiento, también necesita cámaras de red y estaciones de control de mejor rendimiento.

Los codificadores H.264 utilizan el perfil base, lo que supone que sólo se usan los fotogramas I y P. Este perfil es el ideal para cámaras de red y codificadores de video, ya que la latencia se reduce gracias a la ausencia de fotogramas B. La latencia baja es esencial en aplicaciones de video vigilancia donde se realice supervisión en directo, sobre todo si se emplean cámaras PTZ o domos PTZ.

### **1.8. SOPORTE DE AUDIO Y EQUIPOS** (Axis, Axis, 2010)

El soporte de audio es más fácil de implementar en un sistema de video en red que en un sistema analógico CCTV. En un sistema analógico, los distintos cables de audio y video se deben instalar de extremo a extremo, es decir: desde la ubicación de la cámara y el micrófono hasta la ubicación de visualización/grabación. Si la distancia entre el micrófono y la estación de vigilancia es demasiado grande, se deberá utilizar un equipo de línea equilibrada de audio, lo que aumenta el coste y las dificultades de instalación. En un sistema de video en red, una cámara de red con soporte de audio procesa el audio y envía tanto el audio como el video a

través del mismo cable de red para supervisarlo o grabarlo. Esto elimina la necesidad de un cable adicional y facilita la tarea de sincronización de audio y video.

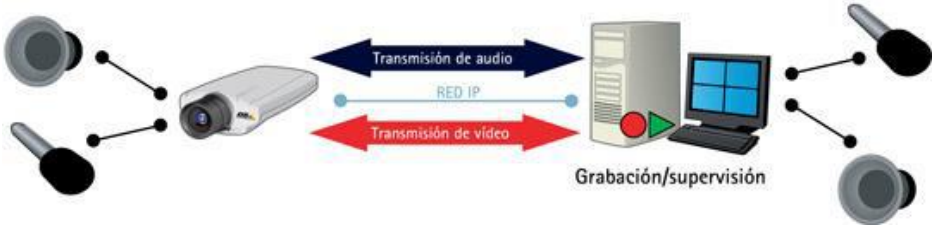



**Figura 1.25 Sistema de cámara IP con soporte de audio integrado** (Axis, Axis, 2010)

Las transmisiones de audio y video se envían a través del mismo cable. Una cámara de red con la funcionalidad de audio integrado incluye a menudo un micrófono integrado y/o toma de entrada de micrófono/línea. Con el soporte de entrada de micrófono/línea los usuarios tienen la opción de utilizar otro tipo o calidad de micrófono que el que integra la cámara o codificador de video.

También permite que el producto de video en red se conecte a más de un micrófono, y éste puede ubicarse a cierta distancia de la cámara. El micrófono se debería colocar siempre lo más cerca posible a la fuente de sonido para poder reducir el ruido.

### 1.8.1. MODOS DE AUDIO

En función de la aplicación, es posible que sea necesario enviar audio sólo en una dirección o en ambas direcciones, lo que puede hacerse de forma simultánea o en una dirección cada vez. Hay tres modos básicos de comunicación de audio: simplex, semidúplex y dúplex completo.

### 1.8.1.2. SIMPLEX

En el modo simplex, el audio sólo se envía en una dirección. En este caso, el audio se envía de la cámara al operador. Las aplicaciones incluyen supervisión a distancia y video-vigilancia.


**Figura 1.26 Modo simplex** (Axis, Axis, 2010)

En la figura 1.26 de modo simplex, el audio lo envía el operador a la cámara. Se puede utilizar, por ejemplo, para dar instrucciones de voz a una persona que se ve a través de la cámara.

### 1.8.1.3. SEMIDÚPLEX

En el modo semidúplex, el audio se envía en ambas direcciones, pero sólo puede enviar una de las partes cada vez. Este modo es similar a un walkie-talkie.

### 1.8.1.4. DUPLÉX COMPLETO

En el modo dúplex completo, el audio se envía a y desde el operador simultáneamente. Este modo de comunicación es similar a una conversación telefónica. El dúplex completo requiere que el PC cliente disponga de una tarjeta de sonido con soporte para audio dúplex completo.

## 1.9. SINCRONIZACIÓN DE AUDIO Y VIDEO (Axis, 2010)

La sincronización de datos de audio y video se realiza con un reproductor multimedia (un programa de computador que se usa para reproducir archivos

multimedia) o con un entorno multimedia como Microsoft DirectX, una colección de interfaces de programación de aplicaciones que maneja archivos multimedia.

El audio y el video se envían a través de una red como dos flujos de paquetes individuales. Para que el cliente o reproductor pueda sincronizar perfectamente las transmisiones de audio y video, dichos paquetes deben llevar un sello de fecha y hora. Es posible que la cámara de red no sea siempre compatible con el código de tiempo de los paquetes de video que utilizan la compresión Motion JPEG. En ese caso, y si es importante que el video y el audio estén sincronizados, el formato de video que deberá elegirse es MPEG-4 o H.264, puesto que dichas transmisiones de video, junto con las de audio, se envían con el RTP[49], que introduce un código de tiempo en los paquetes de audio y video. No obstante, existen muchas situaciones en las cuales el audio sincronizado no es tan importante o incluso no es adecuado (por ejemplo, si el audio debe supervisarse pero no grabarse).

### 1.9.1. MANEJO DE VIDEO EN REDES LAN

El video en red, al igual que muchos otros tipos de comunicaciones como son el correo electrónico, los servicios Web y la telefonía por computador, se realiza a través de redes IP[50] cableadas o inalámbricas. El video en red y las transmisiones de audio, así como otros datos, se efectúan a través de la misma infraestructura de red. El video en red proporciona a los usuarios, en particular a los del sector de vigilancia y seguridad, muchas ventajas con respecto a los sistemas CCTV (circuito cerrado de televisión) analógicos tradicionales.

#### 1.9.1.1. TECNOLOGÍA DE RED (Tanenbaum A. S., 2003)

Se utilizan diversas tecnologías de red para proporcionar las numerosas ventajas de un sistema de video en red.

[49] Real-time Transport Protocol
[50] Internet Protocol

### 1.9.1.2. RED DE ÁREA LOCAL CON TECNOLOGÍA ETHERNET

Una red de área local (LAN) es un grupo de computadores conectados a un área localizada para comunicarse entre sí y compartir recursos como, por ejemplo, impresoras. Los datos se envían en forma de tramas, para cuya transmisión se pueden utilizar diversas tecnologías. La tecnología LAN más utilizada es la Ethernet y está especificada en una norma llamada IEEE 802.3.

Ethernet utiliza una topología en estrella en la que los nodos individuales (dispositivos) están conectados unos con otros a través de un equipo de red activo como un switch. El número de dispositivos conectados a una LAN puede oscilar entre dos y cientos de dispositivos.

El medio de transmisión físico para una LAN por cable implica cables, principalmente de par trenzado, o bien, fibra óptica. Un cable de par trenzado consiste en ocho cables que forman cuatro pares de cables de cobre trenzados, y se utiliza con conectores RJ-45. La longitud máxima de un cable de par trenzado es de 100 m, mientras que para la fibra, el máximo varía entre 10 km y 70 km, dependiendo del tipo. En función del tipo de cables de par trenzado o de fibra óptica que se utilicen, actualmente las velocidades de datos pueden oscilar entre 100 Mbit/s y 10.000 Mbit/s.

Por regla general, las redes siempre deben tener más capacidad de la que se necesita. Para preparar una red para el futuro es una buena idea diseñar una red que solamente utilice el 70% de su capacidad. Hoy en día una red necesita cada vez más y más rendimiento, ya que hay cada vez más aplicaciones que funcionan a través de redes. Mientras que los switches de red (de los que se habla a continuación) son fáciles de actualizar con el paso del tiempo, el cable suele ser mucho más difícil de sustituir.

**1.9.1.2.1. SWITCH** (Axis, Axis)

Cuando sólo dos dispositivos necesitan estar comunicados directamente el uno con el otro por medio de un cable de par trenzado, se puede utilizar el llamado cable cruzado. El cable cruzado simplemente cruza el par de transmisión de un extremo del cable con el par de recepción del otro extremo y viceversa.

Sin embargo, para conectar diversos dispositivos a una LAN se requiere un equipo de red, como un switch. Con un switch de red se utiliza un cable de red convencional en lugar de un cable cruzado.

La función principal de un switch es remitir los datos de un dispositivo a otro en la misma red. Es un método eficaz, puesto que los datos se pueden dirigir de un dispositivo al otro sin que ello afecte a otros dispositivos que utilicen la misma red.

Un switch registra las direcciones MAC (Media Access Control) de todos los dispositivos conectados. (Cada dispositivo de red tiene una dirección MAC única, que está formada por una serie de números y letras establecida por el fabricante y suele encontrarse en la etiqueta del producto). Cuando un switch recibe datos, los remite sólo al puerto que está conectado a un dispositivo con la dirección MAC de destino adecuado.

Los switches suelen indicar su rendimiento en velocidades por puerto y en plano posterior o velocidades internas (ambas en velocidad de bits y paquetes por segundo). La velocidad por puerto indica la velocidad máxima en un puerto concreto. Esto significa que la velocidad de un switch, por ejemplo, 100 Mbit/s, suele ser el rendimiento de cada puerto.

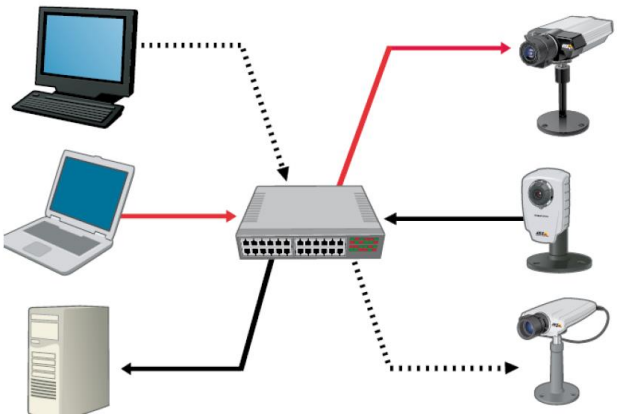


**Figura 1.27 Con un switch de red** (Axis, Axis)

En la figura 1.27, la transferencia de datos se gestiona de manera muy eficaz, ya que el tráfico de datos se puede dirigir de un dispositivo a otro sin afectar a cualquier otro puerto del switch.

Un switch de red normalmente admite distintas velocidades de transferencia de datos de forma simultánea. La velocidad más común solía ser 10/100, que admite tanto Ethernet 10 Mbit/s como Fast Ethernet. Pero 10/100/1000 se está posicionando rápidamente como el switch estándar y, por lo tanto, admite simultáneamente Ethernet de 10 Mbit/s, Fast Ethernet y Gigabit Ethernet. La velocidad y el modo de transferencia entre un puerto de un switch y un dispositivo conectado normalmente se determinan mediante la negociación automática, en la que se utiliza la velocidad de transferencia de datos más alta y el mejor modo de transmisión. Un switch también permite que un dispositivo conectado funcione en modo dúplex completo: por ejemplo, enviar y recibir datos al mismo tiempo, dando como resultado un mejor rendimiento.

Los switches pueden tener diferentes características y funciones. Algunas incluyen la función de router. Un switch también puede admitir Calidad de Servicio, que controla la cantidad de ancho de banda que utilizan las distintas aplicaciones.

### 1.9.1.2.2. ALIMENTACIÓN A TRAVÉS DE ETHERNET

La Alimentación a través de Ethernet PoE[51] permite proveer de energía a los dispositivos conectados a una red Ethernet usando el mismo cable que para la comunicación de datos. Su uso es muy frecuente en teléfonos IP, puntos de acceso inalámbricos y cámaras de red conectadas a una red LAN.

La principal ventaja de PoE es el ahorro de costes que conlleva. No es necesario contratar a un electricista ni instalar una línea de alimentación separada. Esto supone una ventaja, sobre todo en zonas de difícil acceso. El hecho de que no sea necesario instalar otro cable de alimentación puede suponer un ahorro de varios centenares de dólares, dependiendo de la ubicación de la cámara. PoE también facilita el hecho de cambiar la ubicación de la cámara o añadir otras cámaras al sistema de video-vigilancia.

Además, aumenta la seguridad del sistema de video. Un sistema de video-vigilancia con PoE se puede alimentar desde una sala de servidores, que a menudo está protegida con un SAI[52]. Esto significa que el sistema de video-vigilancia puede funcionar incluso durante un apagón.

Por las ventajas que tiene PoE, se recomienda usarla en tantos dispositivos como sea posible. La energía de un mid span con PoE debería ser suficiente para los dispositivos conectados, y éstos deberían admitir la clasificación de potencia.

Todo ello se explica a continuación con más detalle.

Norma 802.3af y High PoE, hoy en día, la mayoría de dispositivos PoE cumplen con la norma IEEE 802.3af, que se publicó en 2003. Esta norma utiliza cables estándares Cat-5 o superiores y asegura que la transferencia de datos no se vea afectada. En dicha norma, al dispositivo que proporciona la energía se le llama equipo de suministro eléctrico. Éste puede ser un switch o midspan habilitado

[51] Power over Ethernet
[52] Sistema de alimentación ininterrumpida

para PoE. El dispositivo que recibe la energía se conoce como dispositivo alimentado. Esta función normalmente está integrada en un dispositivo de red, como una cámara, o en un splitter independiente.

La compatibilidad con versiones anteriores de dispositivos de red que admiten PoE está garantizada. La norma incluye un método para identificar automáticamente si un dispositivo es compatible con PoE, y sólo se le proporciona energía una vez que se ha confirmado dicha compatibilidad. Esto también implica que el cable Ethernet conectado a un switch PoE no proporcionará energía alguna si no está conectado a un dispositivo habilitado para PoE, lo cual elimina el riesgo de una descarga eléctrica al instalar una red o renovar la instalación.

En un cable de par trenzado tiene 8 cables en su interior. PoE puede venir de dos formas posibles: una de las formas consiste en usar dos cables de datos de Ethernet como fuente de alimentación. Dicha forma permite transmitir datos y alimentar a la vez. La segunda forma usa otros dos cables alternativos para enviar la tensión, para implementar la segunda forma se requiere de a cables. Los switches con PoE integrada a menudo proporcionan la electricidad por medio de los dos pares de cables utilizados para la transmisión de datos, mientras que los midspans normalmente usan los dos pares de recambio. Un PD admite las dos opciones. Según la IEEE 802.3af, un PSE proporciona un voltaje de 48 V CC con una potencia máxima de 15,4 W por puerto. Pero, teniendo en cuenta que en un cable de par trenzado hay pérdida de potencia, un PD sólo garantiza 12,95 W. La norma IEEE 802.3 especifica varias categorías de rendimiento para los PD.

Los PSE como los switches o midspans normalmente proporcionan una potencia de entre 300 W y 500 W. En un switch de 48 puertos significaría una potencia de 6 a 10 W por puerto, en caso de que todos los puertos estuvieran conectados a dispositivos con PoE. Salvo que los PD admitan clasificación de potencia, los 15,4 W deben reservarse en su totalidad para los puertos que utilicen PoE, lo que implica que un switch con 300 W sólo puede alimentar 20 de los 48 puertos. Sin

embargo, si todos los dispositivos comunicaran al switch su condición de dispositivos de clase 1, los 300 W bastarían para alimentar a los 48 puertos.

| Clase | Nivel de potencia mínimo en PSE | Nivel de potencia máximo de un PD | Uso |
|---|---|---|---|
| 0 | 15.4 W | 0.44 W - 12.95 W | predeterminado |
| 1 | 4.0 W | 0.44 W - 3.84 W | opcional |
| 2 | 7.0 W | 3.84 W - 6.49 W | opcional |
| 3 | 15.4 W | 6.49 W - 12.95 W | opcional |
| 4 | Tratado como clase 0 | | Reservado para usos futuros |

**Tabla 1.3 Clasificaciones de potencia según IEEE 802.3af.** (Axis, Axis)

La mayoría de cámaras de red fijas pueden recibir energía por medio de PoE con la norma IEEE 802.3af, y normalmente se identifican como dispositivos de clase 1 o 2.

Con la norma en desarrollo IEEE 802.3at o PoE+, el límite de potencia aumenta hasta al menos 30W por medio de dos pares de cables de un PSE. Las especificaciones finales todavía están por determinar y se espera que la norma se ratifique en este 2009.

Mientras tanto, los midspans y splitters con la norma en desarrollo IEEE 802.3at (High PoE) pueden utilizarse para dispositivos como cámaras y domos PTZ con control motor, así como para cámaras con calefactores y ventiladores, que requieren más potencia de la que proporciona la norma IEEE 802.3af.

Midspans y splitters, también conocidos como splitters activos, son equipos que permiten que una red existente sea compatible con la alimentación a través de Ethernet.

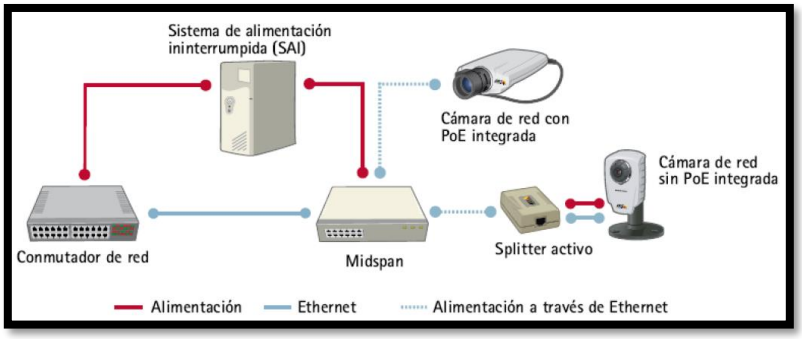



**Figura 1.28 Sistema de alimentación a través de Ethernet.** (Axis, Axis)

En la figura 1.28, se observa un sistema de alimentación a través de la red Ethernet, el mismo se puede observar que la línea roja corresponde a la alimentación eléctrica, la línea azul corresponde a la red Ethernet, y la línea azul entrecortado corresponde a la alimentación eléctrica que tiene a través de la red Ethernet. Los splitter se utilizan para alimentar a un dispositivo mientras que los midspan para alimentar a varios dispositivos.

El midspan, que proporciona más energía al cable Ethernet, se coloca entre el switch de red y los dispositivos alimentados. Para asegurarse de que la transferencia de datos no se ve afectada, es importante recordar que la distancia máxima entre la fuente de datos (el switch, por ejemplo) y los productos de video en red no debe ser superior a 100 m. Esto significa que el midspan y el splitter o splitters activos deben colocarse a una distancia no superior a 100 m.

Un splitter sirve para separar la energía y los datos de un cable Ethernet en dos cables separados, de modo que se puedan conectar a un dispositivo sin PoE integrada. Puesto que la PoE o High PoE proporciona 48 V CC, la otra función del splitter consiste en bajar el voltaje a un nivel adecuado para el dispositivo, por ejemplo, 12 ó 5 V.

### 1.9.1.2.3. COMUNICACIÓN A TRAVÉS DE INTERNET (Axis, Axis)

Para enviar datos entre un dispositivo conectado a una red de área local a otro conectado a otra LAN se requiere una vía de comunicación estándar, ya que es posible que las redes de área local utilicen distintos tipos de tecnologías. Esta

necesidad lleva al desarrollo de un sistema de direcciones IP y protocolos basados en IP para comunicarse a través de Internet, que conforma un sistema global de redes informáticas interconectadas. (Las LAN también pueden utilizar direcciones y protocolos IP para comunicarse dentro de una red de área local, aunque el uso de las direcciones MAC es suficiente para la comunicación interna). Antes de abordar el tema de las direcciones IP, a continuación se tratan algunos de los conceptos básicos de la comunicación a través de Internet, tales como los routeres, firewalls y proveedores de servicios de Internet.

#### 1.9.1.2.4. ROUTER

Para enviar paquetes de datos de una LAN a otra a través de Internet se debe utilizar un equipo de red llamado router. Un router guía la información de una red a otra basándose en las direcciones IP. Sólo remite los paquetes de datos que se deben enviar a otra red. Normalmente se utiliza para conectar una red local a Internet. Tradicionalmente se denominaba a los routers puertas de enlace.

#### 1.9.1.2.5. FIREWALLS

Los firewalls sirven para evitar los accesos no autorizados hacia o desde una red privada. Se pueden implementar tanto en el hardware como en el software, o en una combinación de ambos. Normalmente se utilizan los firewalls para evitar que usuarios no autorizados accedan a redes privadas conectadas a Internet. Los mensajes que entran y salen de Internet pasan por los firewalls, que los examina y bloquea aquellos que no cumplen con los criterios de seguridad especificados.

#### 1.9.1.2.6. CONEXIÓN A INTERNET

Para conectar una LAN a Internet se debe establecer una conexión de red a través de un proveedor de servicios de Internet (ISP). En una conexión a Internet se utilizan términos como velocidad de subida y velocidad de bajada. La velocidad de subida describe la velocidad de transferencia con la que se pueden subir datos

del dispositivo a Internet: por ejemplo, cuando se envía un video desde una cámara de red. La velocidad de bajada es la velocidad de transferencia con la que se bajan archivos: por ejemplo, cuando un monitor de computador recibe un video. En la mayoría de casos— como un portátil conectado a Internet, por ejemplo—la descarga de información desde Internet es la velocidad más importante a tener en cuenta. En una aplicación de video en red con una cámara de red situada en una ubicación remota, la velocidad de subida es más relevante, puesto que los datos (el video) de la cámara de red se subirán a Internet.

**1.9.1.2.7. DIRECCIÓN IP** (Tanenbaum A. s.)

Cualquier dispositivo que quiera comunicarse con otros dispositivos a través de Internet debe tener una dirección IP única y adecuada. Las direcciones IP sirven para identificar a los dispositivos emisores y receptores. Actualmente existen dos versiones IP: IP versión 4 (IPv4) e IP versión 6 (IPv6). La principal diferencia entre ellas es que una dirección IPv6 tiene una longitud mayor (128 bits, en comparación con los 32 bits de una dirección IPv4). Hoy en día, las direcciones IPv4 son las más comunes.

**1.9.1.2.8. DIRECCIÓN IPV4** (Tanenbaum A. S., 2003)

Una dirección IP se implementa con un número de 32 bit que suele ser mostrado en cuatro grupos de números decimales de 8 bits. Cada uno de esos números se mueve en un rango de 0 a 255 (expresado en decimal), o de 0 a FF (en hexadecimal) o de 0 a 11111111 (en binario). Las direcciones IP se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección 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 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 256 en total, 255 más la 0 (0000 0000).

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255, salvo algunas excepciones. Los ceros iniciales, si los hubiera, se pueden obviar (010.128.001.255 sería 10.128.1.255).

Hay tres clases de direcciones IP que una organización puede recibir de parte de la ICANN[53]: clase A, clase B y clase C. En la actualidad, ICANN reserva las direcciones de clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran envergadura, y las direcciones de clase B para las medianas empresas. Se otorgan direcciones de clase C para todos los demás solicitantes. Cada clase de red permite una cantidad fija de equipos (hosts).

En una red de clase 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 224 – 2 (las direcciones reservadas de broadcast [últimos octetos a 255] y de red [últimos octetos a 0]), es decir, 16777 214 hosts.

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 216 - 2, o 65 534 hosts.

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 28 - 2, ó 254 hosts.

La dirección 0.0.0.0 es utilizada por las máquinas cuando están arrancando o no se les ha asignado dirección. Se denomina dirección de red.

[53] Internet Corporation for Assigned Names and Numbers

| Clase | Rango | N° de Redes | N° de Host | Máscara de Red | Broadcast ID |
|---|---|---|---|---|---|
| A | 1.0.0.0 - 127.255.255.255 | 126 | 16.777.214 | 255.0.0.0 | x.255.255.255 |
| B | 128.0.0.0 - 191.255.255.255 | 16.384 | 65.534 | 255.255.0.0 | x.x.255.255 |
| C | 192.0.0.0 - 223.255.255.255 | 2.097.152 | 254 | 255.255.255.0 | x.x.x.255 |

**Tabla 1.4 Clases de dirección IPv4** (Tanenbaum A. S., 2003)

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 (Network Address Translation) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten a través del protocolo NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255.
- Clase B: 172.16.0.0 a 172.31.255.255.
- Clase C: 192.168.0.0 a 192.168.255.255.

### 1.9.1.2.9. MÁSCARA DE SUBRED

La máscara permite distinguir los bits que identifican la red y los que identifican el host de una dirección IP. Dada la dirección de clase A 10.2.1.2 se sabe que pertenece a la red 10.0.0.0 y el host al que se refiere es el 2.1.2 dentro de la misma. La máscara se forma poniendo a 1 los bits que identifican la red y a 0 los bits que identifican el host. De esta forma una dirección de clase A tendrá como máscara 255.0.0.0, una de clase B 255.255.0.0 y una de clase C 255.255.255.0.

Los dispositivos de red realizan un AND entre la dirección IP y la máscara para obtener la dirección de red a la que pertenece el host identificado por la dirección IP dada. Por ejemplo un router necesita saber cuál es la red a la que pertenece la dirección IP del datagrama destino para poder consultar la tabla de encaminamiento y poder enviar el datagrama por la interfaz de salida.

**1.9.1.2.10. PUERTOS** (Axis, 2010)

Un número de puerto define un servicio o aplicación concretos para que el servidor receptor (por ej. una cámara de red) sepa cómo procesar los datos entrantes. Cuando un computador envía datos vinculados a una aplicación concreta, normalmente añade el número de puerto a una dirección IP sin que el usuario lo sepa. Los números de puerto pueden ir del 0 al 65535. Algunas aplicaciones utilizan los números de puerto que les ha pre asignado la Autoridad de Números Asignados de Internet (IANA). Por ejemplo, un servicio web vía http se suele asignar al puerto 80 de una cámara de red.

**1.9.1.2.11. CONFIGURACIÓN DE LAS DIRECCIONES IPV4**

Para que una cámara de red o codificador de video funcione en una red IP, se le debe asignar una dirección IP. Hay básicamente dos formas de configurar una dirección IPv4 para un producto de video en red:
1. De forma automática con el DHCP[54]

2. Introduciendo manualmente una dirección IP estática en la interfaz del producto de video en red, una máscara de subred y la dirección IP del router predeterminado, o bien utilizando un software de gestión.

El DHCP, gestiona un conjunto de direcciones IP que puede asignar dinámicamente a una cámara de red/codificador de video. A menudo la función DHCP la realiza un router de banda ancha, que sucesivamente recibe sus direcciones IP de un proveedor de servicios de Internet. Una dirección IP

[54] Protocolo de configuración dinámica de host

dinámica significa que la dirección IP para un dispositivo de red puede cambiar de un día para otro. Para usar direcciones IP dinámicas se recomienda que los usuarios registren un nombre de dominio (por ejemplo, www.mycamera.com) para el producto de video en red en un servidor de DNS[55] dinámico, el cual siempre puede vincular el nombre de dominio del producto a cualquier dirección IP que tenga asignada. (Un nombre de dominio se puede registrar a través de algunos de los sitios web de DNS dinámico más conocidos, como www.dyndns.org.

#### 1.9.1.2.12. NAT[56]

Para que un dispositivo de red con una dirección IP privada pueda enviar información a través de Internet, debe utilizar un router compatible con NAT. Con esta técnica, el router puede traducir una dirección IP privada en una pública sin el conocimiento del host que realiza el envío.

#### 1.9.1.2.13. REENVÍO DE PUERTO (Cisco)

Para acceder a cámaras ubicadas en una LAN privada a través de Internet, la dirección IP pública del router se debería usar junto con el número de puerto correspondiente del codificador de video o la cámara de red en la red privada.

Dado que un servicio web a través de HTTP normalmente se asigna al puerto 80, en un escenario con varios codificadores de video o cámaras de red que utilizan el puerto 80 para HTTP en una red privada ocurre lo siguiente: en lugar de cambiar el número de puerto HTTP predeterminado en cada producto de video en red, se puede configurar un router para asociar un único número de puerto HTTP al puerto HTTP predeterminado y a la dirección IP de un producto de video en red concreto. Este proceso se denomina reenvío de puertos y funciona como se indica a continuación. Los paquetes de datos entrantes llegan al router a través de su dirección IP pública (externa) y un número de puerto específico. El router está configurado para reenviar los datos que entran por un número de puerto

[55] Domain Name System-Sistema de nombres de dominio
[56] Network Adress Traslation-Traducción De Dirección De Red

predefinido a un dispositivo específico de la parte del router correspondiente a la red privada. A continuación, el router sustituye la dirección del emisor por su propia dirección IP privada (interna). Para el cliente receptor, el router es el origen de los paquetes. Con los paquetes de datos salientes ocurre lo contrario. El router sustituye la dirección IP privada del dispositivo origen por la IP pública del propio router antes de enviar los datos a través de Internet.

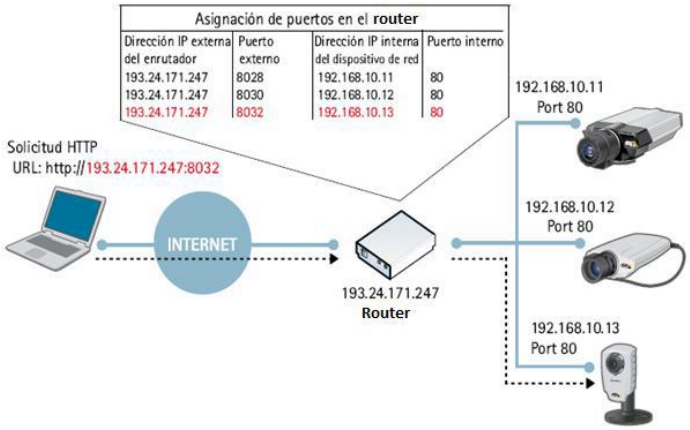



**Figura 1.29 Asignación de puertos en el router** (Cisco)

En la figura 1.29, se observa que gracias al reenvío de puertos del router, es posible acceder a cámaras de red de una red local con direcciones IP privadas a través de Internet. En la ilustración, el router reenvía los datos (solicitud) que recibe el puerto 8032 a una cámara de red con la dirección IP privada 192.168.10.13 a través del puerto 80. A continuación, la cámara empieza a enviar video.

### 1.9.1.2.14. PROTOCOLO DE TRANSPORTE DE DATOS PARA VIDEO EN RED

El Protocolo de control de transmisión TCP[57] y el UDP[58] son los protocolos basados en IP que se utilizan para enviar datos. Estos protocolos de transporte actúan como portadores para muchos otros protocolos. Por ejemplo, HTTP[59], que se utiliza para visualizar páginas web en servidores de todo el mundo a través de Internet.

[57] Transmission Control Protocol- Protocolo de Control de Transmisión
[58] User Datagram Protocol - Protocolo de datagramas de usuario
[59] Hyper Text Transfer Protocol-protocolo de transferencia de hipertexto

| Protocolo | Protocolo de transporte | Puerto | Uso habitual | Uso de video en red |
|---|---|---|---|---|
| FTP (Protocolo de transferencia de ficheros) | TCP | 21 | Transferencia de archivos a través de Internet/intranets | Transferencia de imágenes o video desde un codificador de video/cámara de red a un servidor FTP o a una aplicación |
| SMTP (Protocolo simple de transferencia de correo) | TCP | 25 | Envío de mensajes de correo electrónico | Un codificador de video/cámara de red puede enviar imágenes o notificaciones de alarma utilizando su cliente de correo electrónico integrado |
| HTTP (Protocolo de transferencia de hipertexto) | TCP | 80 | Se utiliza para navegar por la red, por ejemplo, para recuperar páginas web de servidores | Es el modo más habitual para transferir video de un codificador de video/cámara de red, en el que el dispositivo de video en red funciona básicamente como servidor web que pone el video a disposición del usuario o del servidor de aplicaciones que lo solicita |
| HTTPS (Protocolo de transferencia de hipertexto sobre capa de sockets seguros) | TCP | 443 | Acceso seguro a páginas web con tecnología de cifrado | Transmisión segura de video procedente de codificadores de video/cámaras de red |
| RTP (Real Time Protocol) | UDP/TCP | No definido | Formato de paquete RTP estandarizado para la entrega de audio y de video a través de Internet (a menudo utilizado en sistemas de transmisión multimedia o videoconferencia) | Un modo habitual de transmitir video en red basado en H.264/MPEG y de sincronizar video y audio, ya que RTP proporciona la numeración y la datación secuencial de paquetes de datos, lo que permite volver a unirlos en el orden correcto. La transmisión se puede realizar mediante unidifusión o multidifusión |
| RTSP (Protocolo de transmisión en tiempo real) | TCP | 554 | Utilizado para configurar y controlar sesiones multimedia a través de RTP | |

**Tabla 1.5 Protocolos y puertos TCP/IP habituales utilizados para el video en red** (CISCO)

TCP proporciona un canal de transmisión fiable basado en la conexión. Gestiona el proceso de división de grandes bloques de datos en paquetes más pequeños y garantiza que los datos enviados desde un extremo se reciban en el otro. La fiabilidad de TCP en la retransmisión puede producir retrasos significativos, por

lo que en general se utiliza cuando la fiabilidad de la comunicación prevalece sobre la latencia del transporte.

UDP es un protocolo sin conexión que no garantiza la entrega de los datos enviados, dejando así todo el mecanismo de control y comprobación de errores a cargo de la propia aplicación. No proporciona transmisiones de pérdida de datos, por lo que no provoca retrasos adicionales.

## 1.10. CONSIDERACIONES SOBRE ANCHO DE BANDA Y ALMACENAMIENTO PARA LAS CÁMARAS IP (compresión)

Los requisitos de ancho de banda y almacenamiento de red son aspectos importantes en el diseño de sistemas de video-vigilancia. Entre los factores se incluyen el número de cámaras, la resolución de imagen utilizada, el tipo y relación de compresión, frecuencias de imagen y complejidad de escenas.

### 1.10.1. ANCHO DE BANDA (Blade, 2004)

El ancho de banda es la medición de la cantidad de información que puede fluir desde un lugar hacia otro en un período de tiempo determinado. Existen dos usos comunes del término ancho de banda: uno se refiere a las señales analógicas y el otro, a las señales digitales. También suele usarse el término ancho de banda de un bus del computador para referirse a la velocidad a la que se transfieren los datos por ese bus, suele expresarse en bytes por, y se calcula multiplicando la frecuencia de trabajo del bus, en ciclos por segundo por el número de bytes que se transfieren en cada ciclo

El ancho de banda es un concepto muy útil. Sin embargo, tiene sus limitaciones. No importa de qué manera usted envía los mensajes, ni cuál es el medio físico que utiliza, el ancho de banda siempre es limitado. Esto se debe tanto a las leyes de la física como a los avances tecnológicos actuales.

La Tabla 1. 6, muestra la velocidad de algunos medios de transmisión, incluyendo las limitaciones de longitud, para algunos medios comunes de networking. Se debe tomar en cuenta que los límites son tanto físicos como tecnológicos.

| VELOCIDAD DE ALGUNOS MEDIOS TÍPICOS DE TRANSMISIÓN | | |
|---|---|---|
| **Medios típicos** | **Velocidad** | **Distancia física máxima** |
| Cable coaxial de 50 ohmios (Ethernet 10BASE2) | 10-100 Mbps | 185m |
| Cable coaxial de 50 ohmios (Ethernet 10BASE5) | 10-100 Mbps | 500m |
| Par trenzado no blindado de categoría 5 (UTP)(Ethernet 10BASE-T y 100BASE-TX) | 10 Mbps | 100m |
| Par trenzado no blindad mejorado categoría 5 (UTP) (Ethernet 10BASE-T, Fast Ethernet 100BASE-TX y 1000BASE-T) | 100 Mbps | 100m |
| Fibra óptica multimodo (62,5/125mm) 100BASE-FX, 1000BASE-SX | 100 Mbps | 2000m |
| Fibra óptica monomodo (nucleo de 9/125mm) 1000BASE-LX | 1000 Mbps (1.000 Gbps) | 3000m |
| Inalámbrico | 11Mbps | Unos 100 metros |

**Tabla 1.6 Velocidades de diferentes medios de transmisión** (Blade, 2004)

Existe otro concepto importante que se debe tener en cuenta: el rendimiento.

El rendimiento generalmente se refiere al ancho de banda real medido, en un momento específico del día, usando rutas específicas de Internet, mientras se descarga un archivo específico. Desafortunadamente, por varios motivos, el rendimiento a menudo es mucho menor que el ancho de banda digital máximo posible del medio que se está usando. Algunos de los factores que determinan el rendimiento y el ancho de banda son los siguientes:

- Dispositivos de internetworking
- Tipo de datos que se transfieren
- Topología
- Cantidad de usuarios
- Computador del usuario
- Computador del servidor

Al diseñar una red, es importante tener en cuenta el ancho de banda teórico. La red no será más rápida que lo que los medios permiten.
Para un perfecto funcionamiento de la imagen del sistema IP se debe tener en cuenta las siguientes características:

### 1.10.2. LA FRAME POR SEGUNDO (FPS) (compresión)

Es el número de fotogramas por segundo que envía el sistema. El mínimo número de fotogramas para ver video en Internet es de 15 FPS[60] por cada cámara.

Cada sistema de monitoreo tiene un número de FPS determinado, si se instalan varias cámaras se debe dividir este por el número de cámaras.
EJ: sistema de vigilancia con 30 FPS.
Si se tiene una cámara se tiene 30 FPS
Si se tiene 2 cámaras se tienen 15 FPS para cada cámara
Si se tiene 3 cámaras se tienen 10 FPS para cada cámara
Si se tiene 4 cámaras se tienen 7.5 FPS para cada cámara
Mientras más cámaras tenga activas en modo de visualización menor es el número de FPS y menor la velocidad de visualización, viéndose lento y pausado.

### 1.10.3. IP PÚBLICA FIJA:

Una única IP que identifica la red desde el exterior es asignada por el proveedor ideal para el monitoreo de las cámaras.

### 1.10.4. IP PRIVADA:

Una IP que identifica a un dispositivo conectado en la red interna.

[60] La Frame Por Segundo

### 1.10.5. VELOCIDAD REAL DE CONEXIÓN

Técnica utilizada por el proveedor de Internet para la conexión de los usuarios, estos se ubican en un mismo canal y se disminuye el ancho de banda real.
Es importante que se compruebe cual es la velocidad real que se está ofreciendo, de ello depende la óptima visualización de los sistemas de vigilancia DVR o IP.

### 1.10.6. CÁLCULO DE ANCHO DE BANDA Y ALMACENAMIENTO

Los productos de video en red utilizan el ancho de banda de red y el espacio de almacenamiento basándose en sus configuraciones y dependen de los siguientes factores:

 Número de cámaras

 Si la grabación será continua o basada en eventos

Número de horas al día que la cámara estará grabando

 Imágenes por segundo

 Resolución de imagen

 Tipo de compresión de video: Motion JPEG, MPEG-4, H.264

 Escena: Complejidad de imagen (p. ej. pared gris o un bosque), Condiciones de luz y cantidad de movimiento (entorno de oficina o estaciones de tren con mucha gente)

## 1.11. ADMINISTRACIÓN DE REDES (Navarro, pág. Cap. 8)

### 1.11.1. Administración de Redes Internet: SNMPv1 y MIB-II

#### 1.11.1.1 INTRODUCCIÓN

La administración de redes, dispositivos y hosts es referida en Internet como "ADMINISTRACIÓN DE RED", en cambio en OSI se conoce como "ADMINISTRACIÓN DE SISTEMAS".

Originalmente en Internet, la administración de redes se hacía usando el SGMP[61]. Luego, se definió el SNMP[62] para la administración de redes y dispositivos de red.

SNMP necesita, debajo de él, el soporte de las capas de transporte (proveyendo multiplexación y demultiplexación de servicios, y checksum para confiabilidad) y de red (ruteo entre redes, protección de entidades SNMP de las diferencias del medio físico, fragmentación y reensamblado de paquetes).

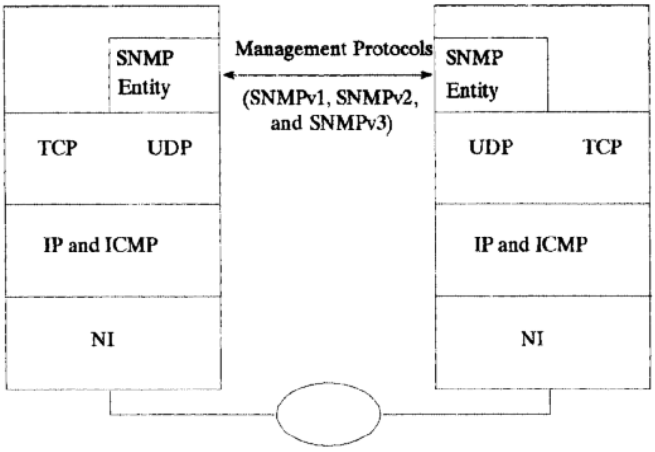



**Figura. 1.30 PROTOCOLOS DE ADMINISTRACIÓN SNMP** (Navarro)

Los objetos a ser administrados se definen en la MIB[63]. Estos objetos deben seguir un determinado conjunto de reglas como las mencionadas en la SMI[64].

En Internet, los OBJETOS son similares a los atributos de OSI[65], y un GRUPO DE OBJETOS es análogo a una clase de MO de OSI. Cada objeto puede tener una o más instancias, cada una de las cuales, a su vez, tiene uno o más valores.

[61] Simple Gateway Monitoring Protocol
[62] SIMPLE NETWORK MANAGEMENT PROTOCOL
[63] BASE DE INFORMACIÓN DE ADMINISTRACIÓN
[64] ESTRUCTURA DE INFORMACIÓN DE ADMINISTRACIÓN
[65] OPEN SYSTEM INTERCONNECTION

El SISTEMA DE ADMINISTRACIÓN DE RED consiste de una o más ESTACIONES DE ADMINISTRACIÓN DE RED (NMSs[66]), análogo a un manager, y uno o más ELEMENTOS DE RED (NEs[67]) con funciones de administración de red (desarrolladas en los agentes), información de administración y protocolos de administración.

Las NMSs tienen, principalmente, las siguientes funciones:

- Recuperar valores de los objetos en NEs usando agentes (mediante Get).
- Cambiar los valores de objetos en NEs usando agentes (mediante Set).
- Enviar requerimientos a los agentes.
- Recibir respuestas y "traps" (notificaciones) de los agentes.

Las ENTIDADES DE APLICACIÓN, que pueden ser Administrador o Agente, intercambian información de administración, y se conocen como ENTIDADES DE APLICACIÓN SNMP (SNMP AEs).

Los AGENTES residen en NEs conocidos como NODOS ADMINISTRADOS, que son dispositivos tales como hosts, routers, adaptadores LAN, módems, hubs, multiplexores, impresoras. Tienen las siguientes funciones:

- Recuperar información de administración de los objetos (recursos) que controla (Get).
- Alterar los valores de los objetos (Set).
- Recibir respuestas y traps de los objetos, y enviarlos, a su vez, a las NMSs.
- SNMP se usa para comunicar información de administración entre una estación de administración y los agentes.

[66] ESTACIONES DE ADMINISTRACIÓN DE RED
[67] ELEMENTOS DE RED

**FILOSOFÍA SEGUIDA PARA EL DISEÑO DE SNMP:**

Protocolo de administración simple y de bajo costo.

Administración de red robusta y capaz de proveer servicios aun cuando el estado de la red no sea confiable o cuando haya errores.

MIB extensible fácilmente: tendrá definidos objetos centrales y se podrán agregar objetos nuevos.

En la distribución de la carga de trabajo entre NMSs y agentes, la mayor carga de trabajo será descargada en las NMSs.

El transporte para llevar protocolos de administración es UDP sin conexión, porque un transporte orientado a la conexión agregaría complejidad.

Objetivo inicial: fácil migración a la administración de red de OSI. Hoy, ese objetivo está cuestionado: algunos están buscando el crecimiento independiente de la administración de red Internet.

### 1.11.1.2. MARCO DE REFERENCIA DE SNMPV1

El framework de administración de red original se conocía como "SNMP Versión 1" (SNMPv1) y consistía de los siguientes RFCs:

- 1155 (sintaxis y semántica para definir objetos para administración de red - SMI),
- 1157 (protocolo de administración para acceder a los objetos, monitorearlos y controlarlos - SNMP)
- 1212 (lineamientos para definir nuevos módulos sin generar redundancia – MIB Concisa).

Luego, se agregó el RFC[68] 1213 que provee las definiciones de un conjunto central de objetos – MIB II.

[68] Request For Comments

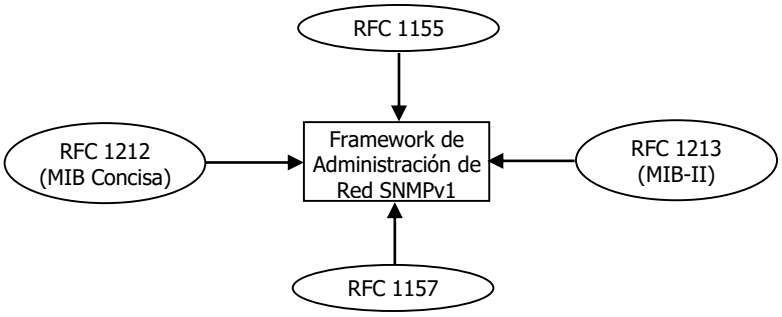



**Figura. 1.31 Framework de Administración de red** (Navarro)

Para lograr que SNMP sea un protocolo simple, se establecieron las siguientes restricciones (las tres primeras son algunas de las razones de elegir UDP sin conexión):

- Evitar la sobrecarga de tener que establecer, mantener y cortar una o más conexiones por cada operación de una entidad SNMP sobre un objeto.
- Obviar el re ensamblado de frames.
- Evitar la recuperación de fallas.
- Limitar las operaciones de recuperación o configuración de los valores de una variable.
- Los traps enviados desde los agentes son muy limitados para reducir tráfico en la red.
- Evitar los comandos imperativos o que disparan otras acciones.

Cuando una SNMP AE en un agente se asocia con un conjunto de SNMP AEs en uno o más administradores, este par se conoce como COMUNIDAD. Cada comunidad tiene un identificador conocido como NOMBRE DE COMUNIDAD.

Un MENSAJE SNMP (Fig. 8.23) consiste de un IDENTIFICADOR DE VERSIÓN, un NOMBRE DE COMUNIDAD SNMP y una PDU[69] SNMP. Los mensajes intercambiados entre una NMS y los agentes son independientes unos de otros. En

[69] Protocol data unit

la implementación de SNMP se recomienda que la longitud de los mensajes no sea más de 484 octetos.

El esquema de autenticación de comunidad SNMP determina cuándo los mensajes enviados entre AEs son auténticos.

#### 1.11.1.3. OBJETOS DE INTERNET

SNMP usa ASN.1 para definir objetos y las PDUs intercambiadas, usando sólo un subconjunto de TIPOS DE DATOS definidos en ASN.1 para OSI: INTEGER, OCTET STRING, OBJECT IDENTIFIER, NULL, SEQUENCE y SEQUENCE OF.

SNMP usa sólo un subconjunto del BER de OSI para sintaxis de transferencia.

El RFC 1155 establece CÓMO DEBEN DEFINIRSE LOS OBJETOS. La sintaxis de un objeto es como sigue:

- NOMBRE DE OBJETO: consiste del OBJECT DESCRIPTOR (nombre textual único, consistente de un string imprimible) junto con el OBJECT IDENTIFIER (del árbol jerárquico de registración de objetos). Ej.: sysLocation {system 6}: "sysLocation" es el DESCRIPTOR DE OBJETO y "{system 6}" es el IDENTIFICADOR DE OBJETO.
- SINTAXIS: TIPO de objeto, que debe mapearse con uno de los tipos de datos permitidos por ASN.1.
- DEFINICIÓN: descripción no ambigua del tipo de objeto.
- ACCESO: establece cómo los objetos pueden ser accedidos por operaciones de administración, y es el mínimo nivel soportado por un tipo de objeto. Los valores pueden ser: read-only (pueden usarse las operaciones de GetRequest y GetNextRequest; no se puede usar SetRequest), read-write (GetRequest, GetNextRequest y SetRequest), write-only (SetRequest) and not-accesible.
- ESTADO: mandatory, optional u obsolete.

El estándar SMI del RFC 1155 define además los siguientes TIPOS DE OBJETOS ADICIONALES:

- NETWORK ADDRESS: actualmente sólo se permite la familia Internet de direcciones de red.
- IP ADDRESS: se representa usando OCTET STRING.
- COUNTER: valor entero no negativo, que se incrementa de 0 a un máximo de $2^{32-1}$. Después de alcanzar el máximo, se pone a 0 y vuelve a ir incrementándose ("wrapping around").
- GAUGE: valor entero no negativo, que puede incrementarse o decrementarse. El máximo permitido es $2^{32-1}$. Después de alcanzar el máximo, comienza a decrementarse hasta llegar a 0 ("no wrapping around").
- TIMETICKS: entero no negativo que representa en centésimas de segundos el tiempo transcurrido desde una determinada acción.
- OPAQUE: permite a un objeto transmitir cualquier dato como un OCTET STRING (obsoleto; sólo para compatibilidad).

#### 1.11.1.4. DEFINICIONES SM

El SMI del RFC 1155 cubre el modelo de información de objeto y un conjunto de tipos genéricos usados para describir información de administración.

Se usa para definir las ESTRUCTURAS DE DATOS DEL SNMP.

Ej:

```
tokenRingPrice OBJECT-TYPE
        SYNTAX INTEGER
    ACCESS read-write
    STATUS optional
    ::= {enterprises 100]
```

#### 1.11.1.5. BASE DE INFORMACIÓN DE ADMINISTRACIÓN (MIB-II)

Los detalles de los objetos se almacenan en una base de datos llamada BASE DE INFORMACIÓN DE ADMINISTRACIÓN (MIB). Aquí, los objetos tienen el tipo de

objeto descripto por el OBJECT DESCRIPTOR junto con el OBJECT IDENTIFIER.

Las MIBs están definidas por diferentes RFCs.

El RFC 1212,"Definiciones de MIB Concisa", provee métodos para limpiar y remover las descripciones de objetos redundantes.

En el RFC 1213,"MIB – II para Administración de Redes de Internets basadas en TCP/IP", la MIB es otra mejora sobre los RFCs anteriores (1156 y 1158): agrega y refina objetos ya definidos, y usa el RFC 1212.

#### 1.11.1.6. JERARQUÍA DE REGISTRACIÓN INTERNET

Para manipulación con propósitos de administración, los objetos deben estar identificados unívocamente, lo cual se lleva a cabo usando IDENTIFICADORES DE OBJETOS, que son series de identificadores derivados por etiquetar los números adjuntos a los nodos, desde la raíz, en la jerarquía de registración, separados por puntos.

#### 1.11.1.7. IDENTIFICACIÓN DE INSTANCIAS DE OBJETOS

Para conocer el valor de una instancia de un objeto, se necesita identificar la instancia, usando el OBJECT IDENTIFIER.

#### 1.11.1.8. CONVENCIONES PARA IDENTIFICAR INSTANCIAS:

Objetos Escalares (o Variables Simples): tienen sólo una instancia asociada con cada objeto escalar, que se identifica por concatenar un valor 0 al OBJECT IDENTIFIER.

Objetos Columnares (o Tablas): las instancias de estos objetos se identifican en una tabla por la cláusula INDEX, que se refiere a una fila en una tabla.

Tablas y Filas Conceptuales: no tienen identificadores de instancias asociados.

Orden Lexicográfico: los OBJECT IDENTIFIERs están ordenados en forma creciente en las MIBs SNMP.

#### 1.11.1.9. MANIPULACIÓN DE TABLAS

En las tablas de la MIB-II, cada OBJETO está representado por una columna, y el valor de cada INSTANCIA de objeto por una fila. Se atraviesa completamente cada columna a lo largo, y luego uno se mueve a la columna siguiente.

Para agregar un valor a una instancia, se ingresa el valor en una fila con una operación Set.

Para borrar una entrada, nuevamente usando la operación Set, se pone el valor como inválido (se recomienda removerlo después).

#### 1.11.1.10. DETALLES Y OBJETOS DE LA MIB-II (RFC 1213)

Cuando se definen nuevas MIBs, es necesario seguir algunas reglas, para permitir la coexistencia de múltiples versiones de MIBs:

- Los tipos de objetos viejos no se borran, pero deben ser removidos en las versiones siguientes.
- Las semánticas de los tipos de objetos viejos no deberían cambiar entre versiones. Sin embargo, si se necesita cambiar la semántica, deben formarse nuevos tipos de objetos.

En la MIB, sólo se definen los objetos esenciales, siguiendo los lineamientos provistos por la SMI para definir nuevos objetos. Estos nuevos objetos pueden agregarse bajo el subárbol {experimental 3} o bajo {enterprises 4.1}.

A la MIB-II se le ha agregado los tipos de datos DisplayString (OCTET STRING de caracteres ASCII imprimibles, de 0 a 255 octetos), y PhyAddress (OCTET STRING usado para representar direcciones físicas).

Los objetos en Internet se clasifican en diferentes grupos, bajo {mgmt 2}. Los objetos bajo estos grupos deben implementarse como un grupo. Ej.: si se implementa el grupo TCP, entonces todos los objetos bajo el grupo TCP, tales como tcpRtoAlgorithm y tcpRtoMin, deben ser implementados.

#### 1.11.1.11. GRUPO SYSTEM (OBLIGATORIO)

Sus objetos especifican nombre, ubicación y descripción del EQUIPO: nombres y versiones del HW y SW, vendedor, nombre de dominio, etc.

La mayoría de estos objetos son útiles para administración de la configuración y de fallas.

system (mib-2 1)
- sysDescr (1)
- sysObjectID (2)
- sysUpTime (3)
- sysContact (4)
- sysName (5)
- sysLocation (6)
- sysServices (7)

#### 1.11.1.12. GRUPO INTERFACES (OBLIGATORIO)

Se refiere a las INTERFACES asociadas con una subred.

Consiste de detalles como cantidad de interfaces, objetos en la subred, fabricante de cada interface, protocolos de capa física y de enlace, ancho de banda, etc.

Útil para administración de performance y de fallas.

interfaces (mib-2 2)
- ifNumber (1)
- ifTable (2)

ifEntry (1)

ifIndex (1)

ifDescr (2)

ifType (3)

ifMtu (4)

ifSpeed (5)

ifPhyAddress (6)

ifAdminStatus (7)

ifOperStatus (8)

ifLastChange (9)

ifInOctets (10)

ifInUcastPkts (11)

ifInNUcastPkts (12)

ifInDiscards (13)

ifInErrors (14)

ifInUnknownProtos (15)

ifOutOctets (16)

ifOutUcastPkts (17)

ifOutNUcastPkts (18)

ifOutDiscards (19)

ifOutErrors (20)

ifOutQLen (21)

ifSpecific (22)

#### 1.11.1.13. GRUPO ADDRESS TRANSLATION (OBLIGATORIO)

Este grupo se provee para compatibilidad con MIB-I, y podría ser removida en versiones posteriores de MIB.

Tiene una tabla para mapear direcciones de red (como dir. IP) a direcciones físicas (como dir. MAC).

at (mib-2 3)

atTable (1)

atEntry (1)

atIfIndex (1)

atPhyAddress (2)

atNetAddress (3)

#### 1.11.1.14. GRUPO IP (OBLIGATORIO)

Provee estadísticas sobre DATAGRAMAS IP, y es útil para performance.

ip (mib-2 4)

ipForwarding (1)

ipDefaultTTL (2)

ipInReceives (3)

ipInHdrErrors (4)

ipInAddrErrors (5)

ipForwDatagrams (6)

ipInUnknownProtos (7)

ipInDiscards (8)

ipInDelivers (9)

ipOutRequests (10)

ipOutDiscards (11)

ipOutNoRoutes (12)

ipReasmTimeout (13)

ipReasmReqds (14)

ipReasmOKs (15)

ipReasmFails (16)

ipFragOKs (17)

ipFragFails (18)

ipFragCreates (19)

ipAddrTable (20)

ipAddrEntry (1)

ipAdEntAddr (1)

ipAdEntIfIndex (2)

ipAdEntNetMask (3)

ipAdEntBcasAddr (4)

ipAdEntReasmMaxSize (5)

ipRouteTable (21)

ipRouteEntry (1)

ipRouteDest (1)

ipRouteIfIndex (2)

ipRouteMetric1 (3)

ipRouteMetric2 (4)

ipRouteMetric3 (5)

ipRouteMetric4 (6)

ipRouteNextHop (7)

ipRouteType (8)

ipRouteProto (9)

ipRouteAge (10)

ipRouteMask (11)

ipRouteMetric5 (12)

ipRouteInfo (13)

ipNetToMediaTable (22)

ipNetToMediaEntry (1)

ipNetToMediaIndex (1)

ipNetToMediaPhysAddress (2)

ipNetToMediaNetAddress (3)

ipNetToMediaType (4)

ipRoutingDiscards (23)

#### 1.11.1.15. GRUPO ICMP[70] (OBLIGATORIO)

Provee estadísticas sobre MENSAJES ICMP, y es útil para administración de performance.

Básicamente tiene contadores sobre diferentes tipos y condiciones de mensajes ICMP.

icmp (mib-2 5)

[70] Internet Control Message Protocol

icmpInMsgs (1)

icmpInErrors (2)

icmpInDestUnreachs (3)

icmpInTimeExcds (4)

icmpInParmProbs (5)

icmpInSrcQuenchs (6)

icmpInRedirects (7)

icmpInEchos (8)

icmpInEchoReps (9)

icmpInTimestamps (10)

icmpInTimestampReps (11)

icmpInAddrMasks (12)

icmpInAddrMaskReps (13)

icmpOutMsgs (14)

icmpOutErrors (15)

icmpOut DestUnreachs (16)

icmpOutTimeExcds (17)

icmpOutParmProb (18)

icmpOutSrcQuenchs (19)

icmpOutRedirects (20)

icmpOutEchos (21)

icmpOut EchoReps (22)

icmpOutTimestamps (23)

icmpOutTimestampReps (24)

icmpOutAddrMasks (25)

icmpOutAddrMaskReps (26)

#### 1.11.1.16. GRUPO TCP[71] (OBLIGATORIO SI SE IMPLEMENTA TCP)

Provee algoritmos, parámetros y estadísticas sobre TCP. Supervisa segmentos enviados y recibidos, cantidad actual y acumulada de conexiones abiertas, estadísticas de errores.

Es útil para administración de performance.

tcp (mib-2 6)
- tcpRtoAlgorithm (1)
- tcpRtoMin (2)
- tcpRtoMax (3)
- tcpMaxConn (4)
- tcpActiveOpens (5)
- tcpPassiveOpens (6)
- tcpAttemptFails (7)
- tcpEstabResets (8)
- tcpCurrEstab (9)
- tcpInSegs (10)
- tcpOutSegs (11)
- tcpRetransSegs (12)
- tcpConnTable (13)
  - tcpConnEntry (1)
    - tcpConnState (1)
    - tcpConnLocalAddress (2)
    - tcpConnLocalPort (3)
    - tcpConnRemAddress (4)
    - tcpConnRemPort (5)
- tcpInErrs (14)
- tcpOutRsts (15)

#### 1.11.1.17. GRUPO UDP (OBLIGATORIO SI SE IMPLEMENTA UDP)

Provee estadísticas de tráfico UDP[72]: detalles sobre datagramas UDP y puntos extremos UDP.

[71] Transmission Control Protocol

udp (mib-2 7)
udpInDatagrams (1)
udpNoPorts (2)
udpInErrors (3)
udpOutDatagrams (4)
udpTable (5)
udpEntry (1)
udpLocalAddress (1)
udpLocalPort (2)

### 1.11.1.18. GRUPO EGP[73] (OBLIGATORIO SI SE IMPLEMENTA EGP)

Provee estadísticas de tráfico EGP: detalles sobre mensajes EGP generados, recibidos y no enviados, y condiciones de vecinos EGP.

egp (mib-2 8)
egpInMsgs (1)
egpInErrors (2)
egpOutMsgs (3)
egpOutErrors (4)
egpNeighTable (5)
egpNeighEntry (1)
egpNeighState (1)
egpNeighAddr (2)
egpNeighAs (3)
egpNeighInMsgs (4)
egpNeighInErrs (5)
egpNeighOutMsgs (6)
egpNeighOutErrs (7)
egpNeighInErrMsgs (8)
egpNeighOutErrMsgs (9)

[72] User Datagram Protocol
[73] Exterior Gateway Protocol

egpNeighStateUps (10)
egpNeighStateDowns (11)
egpNeighIntervalHello (12)
egpNeighIntervalPoll (13)
egpNeighMode (14)
egpNeighEventTrigger (15)
egpAs (6)

### 1.11.1.19. GRUPO SNMP (OBLIGATORIO SI SE SOPORTA SNMP)

Provee estadísticas de tráfico y operaciones SNMP. Como un nodo puede ser un agente o una estación administradora, en algunos casos los objetos de la lista pueden tener valor 0.

snmp (mib-2 11)
snmpInPkts (1)
snmpOutPkts (2)
snmpInBadVersions (3)
snmpInBadCommunityNames (4)
snmpInBadCommunityUses (5)
snmpInASNParseErrs (6)
(7) — No usado
snmpInTooBigs (8)
snmpInNoSuchNames (9)
snmpInBadValues (10)
snmpInReadOnlys (11)
snmpInGenErrs (12)
snmpInTotalReqVars (13)
snmpInTotalSetVars (14)
snmpInGetRequests (15)
snmpInGetNexts (16)
snmpInSetRequests (17)
snmpInGetResponses (18)

snmpInTraps (19)

snmpOutTooBigs (20)

snmpOutNoSuchNames (21)

snmpOutBadValues (22)

snmpOutGenErrs (24)

snmpOutGetRequests (25)

snmpOutGetNexts (26)

snmpOutSetRequests (27)

snmpOutGetResponses (28)

snmpOutTraps (29)

snmpEnableAuthenTraps (30)

### 1.11.1.20. CÓMO OPERA SNMPV1 (RFC 1157) (Navarro)

Las PDUs usadas en SNMPv1 son:

0. GetRequest
1. GetNextRequest
2. GetResponse
3. SetRequest
4. Trap

Cuando una entidad de protocolo envía una PDU GetRequest, GetNextRequest, o SetRequest, la respuesta es una PDU GetResponse. Cuando hay errores o casos especiales, se envían Traps de una entidad de protocolo a la otra. Los Traps son análogos a las notificaciones de OSI.

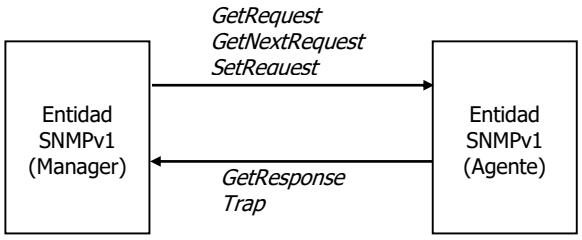



**Figura. 1.32 PDUS DEL PROTOCOLO DE ADMINISTRACIÓN SNMPV1** (Navarro)

Formato de las PDUs SNMPv1:

Las PDUs GetRequest, GetNextRequest, SetRequest y GetResponse tienen los siguientes campos:

- Tipo de PDU: número identificador de cada tipo de PDU (VER "PDUs usadas en SNMPv1"). Ej.: "0" = GetRequest.
- Request-id: usado como identificador para correlación de las respuestas, o para identificar respuestas duplicadas.
- Error-Status: indica el tipo de error (VER "Errores" posibles). Ej.: "1" = tooBig
- Error-Index: da la posición de la variable responsable del error.
- Variable-Bindings: combinación de nombre y valor de una variable (instancia). Puede ser una lista de variables.

FORMATO DE LOS MENSAJES SNMPV1 Y DE LAS PDUS SNMPV1:

Mensaje SNMPv1:

| Versión | Comunidad | Datos |
|---|---|---|

OR

PDUs GetRequest, GetNextRequest, GetResponse y SetRequest de SNMPv1:

| Tipo PDU | Request-Id | Error-Status | Error-Index | Variable-bindings |
|---|---|---|---|---|

PDUTrap de SNMPv1:

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | Enterprise | Agent-Address | Generic-Trap | Specific-Trap | Time-stamp | Variable-bindings |

Campo Variable-bindings:

| | | | | | |
|---|---|---|---|---|---|
| Nombre1 | Valor1 | ... | ... | NombreN | ValorN |

La PDU Trap, en cambio, debe tener lo siguiente:

- Tipo de PDU: número identificador del tipo de PDU = “4”.
- Enterprise: OBJECT IDENTIFIER del tipo de objeto generador del trap.
- Agent-Addr: dirección de red del objeto generador del trap.
- Generic-Trap: tipo de trap genérica. (VER “Traps Genéricas”). Ej.: “2” = linkDown.
- Specific-Trap: código específico, presente aunque “Generic-Trap” no sea “enterpriseSpecific”.
- Time-stamp: TimeTicks del tiempo transcurrido entre la última (re)inicialización de la entidad de red y la generación del trap.
- Variable-Bindings: información relevante.

Traps Genéricas:

- coldStart: cuando un agente se reinicializa y los detalles de configuración e implementación podrían cambiar.
- warmStart: cuando se reiniciliza no hay cambios en los detalles de configuración e implementación.
- linkDown: cuando los enlaces de comunicación usados se afectan (se refiere a una interface), y el nombre y el valor del enlace afectado se suministra en “variable bindings”.
- linkUp: ídem “linDown”.
- authenticationFailure: cuando un mensaje de protocolo falla en la autenticación.
- egpNeighborLoss: cuando un vecino EGP ya no está disponible.
- enterpriseSpecific: cuando los traps no pueden clasificarse específicamente en ninguno de los otros traps.

Errores que pueden ocurrir usando SNMPv1 (valores que puede tomar el parámetro Error-Status)

- noError
- tooBig (Demasiado grande) = La respuesta no entra en el mensaje.
- noSuchName = La operación especifica una variable que no existe.
- badValue = El valor dado en SetRequest no corresponde con el tipo, longitud o variable.
- readOnly = Se quiere modificar una variable de sólo lectura.
- genErrs para cualquier otro tipo de error.

Para recuperar información de administración, SNMP usa una combinación de traps y polling. Cuando hay un error, se envía un trap de un agente a una NMS; una vez que este trap es recibido, la NMS debe enviar una respuesta. Luego, usando polling, se recupera información más detallada.

## 1.12. SISTEMA GPRS (HERNANDO, 2004)

### 1.12.1. GSM: LA BASE DEL GPRS.

El sistema GSM[74] es el sistema de comunicación de móviles digital de 2ª generación basado en células de radio. Apareció para dar respuestas a los problemas de los sistemas analógicos.

Fue diseñado para la transmisión de voz por lo que se basa en la conmutación de circuitos, aspecto del que se diferencia del sistema GPRS[75]. Al realizar la transmisión mediante conmutación de circuitos los recursos quedan ocupados durante toda la comunicación y la tarificación es por tiempo. Más adelante veremos como estas limitaciones hacen ineficiente la transmisión de datos con GSM y como GPRS lo soluciona.

[74] Global System for Mobile
[75] General packet radio service

### 1.12.1.1 ARQUITECTURA DE UNA RED GSM.

Todas las redes GSM se pueden dividir en partes fundamentales y bien diferenciadas:

**1.- La Estación Móvil o Mobile Station (MS[76]):** Consta a su vez de dos elementos básicos que debemos conocer, por un lado el terminal o equipo móvil y por otro lado el SIM[77]. Con respecto a los terminales poco tenemos que decir ya que los hay para todos los gustos, lo que si tenemos que comentar es que la diferencia entre unos y otros radica fundamentalmente en la potencia que tienen que va desde los 20 watios (generalmente instalados en vehiculos) hasta los 2 watios de nuestros terminales.

El SIM es una pequeña tarjeta inteligente que sirve para identificar las características de nuestro terminal. Esta tarjeta se inserta en el interior del móvil y permite al usuario acceder a todos los servicios que haya disponibles por su operador, sin la tarjeta SIM el terminal no nos sirve de nada porque no podemos hacer uso de la red. El SIM está protegido por un número de cuatro dígitos que recibe el nombre de PIN[78] (bueno ya sabemos por qué se nos pide dicho número).

La mayor ventaja de las tarjetas SIM es que proporcionan movilidad al usuario ya que puede cambiar de terminal y llevarse consigo el SIM aunque todos sabemos que esto en la práctica en muchas ocasiones no resulta tan sencillo. Una vez que se introduce el PIN en el terminal, el terminal va a ponerse a buscar redes GSM que estén disponibles y va a tratar de validarse en ellas, una vez que la red (generalmente la que tenemos contratada) ha validado nuestro terminal el teléfono queda registrado en la célula que lo ha validado.

[76] La Estación Móvil
[77] Subscriber Identity Module
[78] Personal Identification Number

**2.- La Estación Base o Base Station Subsystem (BSS[79]):** Sirve para conectar a las estaciones móviles con los NSS, además de ser los encargados de la transmisión y recepción. Como los MS también constan de dos elementos diferenciados: La BTS o Base Station y la BSC[80]. La BTS consta de transceivers y antenas usadas en cada célula de la red y que suelen estar situadas en el centro de la célula, generalmente su potencia de transmisión determinan el tamaño de la célula.

Los BSC se utilizan como controladores de los BTS y tienen como funciones principales las de estar al cargo de los handovers, los frequency hopping y los controles de las frecuencias de radio de los BTS[81].

### 1.12.1.2. LIMITACIONES DE GSM PARA LA TRANSMISIÓN DE DATOS.

Las redes GSM tienen ciertas limitaciones para la transmisión de datos:

- Velocidad de transferencia de 9,6 Kbps.
- Tiempo de establecimiento de conexión, de 15 a 30 segundos. Además las aplicaciones deben ser reinicializadas en cada sesión.
- Pago por tiempo de conexión.
- Problemas para mantener la conectividad en itinerancia (Roaming).

La baja velocidad de transferencia limita la cantidad de servicios que Internet nos ofrece. Por ejemplo, a 9,6 Kbps no se puede navegar por Internet de una manera satisfactoria. Si, además, tenemos en cuenta que estamos pagando por tiempo de conexión, los costos se disparan. Esta es la eterna lucha, pues no se puede comparar una hora de conversación con una hora de navegar por Internet. La

[79] Estación Base
[80] Base Station Controller
[81] Base Transceiver Station

combinación de estos tres factores negativos hace que GSM sea una tecnología mayoritariamente utilizada para la voz y no para los datos.

Las tradicionales redes GSM no se adaptan adecuadamente a las necesidades de transmisión de datos con terminales móviles. Por ello surge una nueva tecnología portadora denominada GPRS[82] que unifica el mundo IP con el mundo de la telefonía móvil, creándose toda una red paralela a la red GSM y orientada exclusivamente a la transmisión de datos.

Al sistema GPRS se le conoce también como GSM-IP ya que usa la tecnología IP (Internet Protocol) para acceder directamente a los proveedores de contenidos de Internet.

#### 1.12.1.3. ¿POR QUÉ ES MEJOR GPRS QUE GSM?

Como hemos visto anteriorrmente el sistema GSM no se adaptaba del todo bien a la transmisión de datos. Vamos a ver ahora las características de GPRS:

- Velocidad de transferencia de hasta 144 Kbps.
- Conexión permanente. Tiempo de establecimiento de conexión inferior al segundo.
- Pago por cantidad de información transmitida, no por tiempo de conexión. Veamos unos ejemplos de los tamaños de información que descargaríamos:

**Envío de un e-mail** de 5 líneas de texto con un anexo (documento tipo de Word de 4 páginas), consumiría alrededor de **95 kbytes**.

**Acceder a un buscador**, buscar un término (ej. viajes) y recibir una pantalla de respuesta podría ocupar **100 kbytes** aproximadamente.

[82] General Packet Radio Service

**Recibir una hoja de cálculo** (documento tipo Excel de 5 hojas), consumiría aproximadamente **250 kbytes**.

**Bajarse una presentación** (documento tipo PowerPoint de 20 diapositivas y con fotos) equivale a unos **1.000 kbytes**.

Como vemos estas características se amoldan mucho mejor para la transmisión de datos que el tradicional sistema GSM.

### 1.12.1.4. VENTAJAS DEL GPRS PARA EL USUARIO.

Las ventajas que obtiene el usuario con el sistema GPRS son consecuencia directa de las características vistas en el punto anterior.

- Característica de "Always connected": un usuario GPRS puede estar conectado todo el tiempo que desee, puesto que no hace uso de recursos de red (y por tanto no paga) mientras no esté recibiendo ni transmitiendo datos.
- Tarificación por volumen de datos transferidos, en lugar de por tiempo.
- Coste nulo de establecimiento de conexión a la red GPRS, frente a los quantum de conexión existente actualmente en GSM.
- Mayor velocidad de transmisión. En GSM sólo se puede tener un canal asignado (un "timeslot"), sin embargo, en GPRS, se pueden tener varios canales asignados, tanto en el sentido de transmisión del móvil a la estación base como de la estación base al móvil. La velocidad de transmisión aumentará con el número de canales asignados. Además, GPRS permite el uso de esquemas de codificación de datos que permiten una velocidad de transferencia de datos mayor que en GSM.
- Posibilidad de realizar/recibir llamadas de voz mientras se está conectado o utilizando cualquiera de los servicios disponibles con esta tecnología.
- Modo de transmisión asimétrico, más adaptado al tipo de tráfico de navegación html o wml (un terminal GPRS 4+1 (4 slots downlink y 1 uplink) tendrá cuatro veces mayor capacidad de transmisión de bajada que de subida).

### 1.12.1.5. VENTAJAS DEL GPRS PARA LA OPERADORA.

Uso eficiente de los recursos de la red: los usuarios sólo ocupan los recursos de la red en el momento en que están transmitiendo o recibiendo datos, y además se pueden compartir los canales de comunicación entre distintos usuarios y no dedicados como en el modelo GSM.

#### 1.12.1.5.1. CÓMO SE ACCEDE A GPRS

Ya existen en el mercado un buen número de móviles adaptados al sistema GPRS. En la bibliografía se comentan algunas direcciones donde obtener los diferentes modelos que homologan las operadoras.

Los terminales GPRS presentan las siguientes características comunes:

**Capacidad Dual:**
Los terminales GPRS están adaptados para aprovechar la cobertura existente GSM para la voz y en GPRS para la transmisión de datos.
**Velocidad de transferencia:**
Los terminales GPRS utilizan varios canales simultáneos o slots.
El número de canales depende de cada terminal, variando de 1 a 4 para la recepción de datos y de 1 a 2 para el envío.
Cada canal representa una velocidad teórica de 13.4 kilobits (en GSM sólo 9 Kbits).

**Tarjeta SIM:**
La tarjeta SIM es la misma que para GSM. No es preciso cambiar de tarjeta para usar GPRS.

Existen tres tipos de terminales, cada uno con sus características:

CLASE A:

- Uso simultáneo de GSM y GPRS
- 1 Time-Solt para GSM y 1 o más para GPRS
- No hay degradación de ninguno de los dos servicios.

CLASE B:

- Registro GPRS y GSM
- Uno de los dos está en suspenso mientras el otro está activo. Prioridad para GSM.
- Degradación de QoS sólo para GPRS

CLASE C:

- Elección manual de GPRS o GSM
- No hay uso simultáneo.

Algunos de los terminales GPRS que se irán desarrollando con capacidades adicionales a medida que la tecnología vaya avanzando son:

- Teléfonos móviles similares a los actuales con visor cada vez mayor y con mejor resolución. Estos terminales permitirán el uso de información escrita o gráfica de forma resumida. Además actuarán de módem inalámbrico cuando se conectan a un ordenador portátil o de sobremesa.
- Terminales tipo Organizador Personal Digital (PDA "Personal Digital Assistant") con pantalla plana en color de mayor formato y gran capacidad gráfica.
- Ordenadores portátiles que utilicen para su conexión inalámbrica un teléfono móvil GPRS o una tarjeta PCMCIA con capacidad de comunicación móvil.

# CAPITULO II

## 2. METODOLOGÍA (Sampieri, 2009)

### 2.1 TIPO DE ESTUDIO

**Investigativa.-** Es una de las investigaciones más usadas ya que no tenemos la información y conocimientos sobre las cámaras IP que debemos de utilizar para realizar la implementación.

A la vez teníamos que conocer cuál podrá ser los problemas que pudieran surgir en el acoplamiento de las señales así como la debida calibración de los equipos de comunicación para su correcto funcionamiento.

**De Laboratorio.-** Hablamos de investigación de campo cuando se recolectan los datos en ambientes naturales o de la vida real es decir la que se realiza en lugares predeterminados para la investigación como bibliotecas, laboratorios de cómputo, de física, electrónica, etc.

**De Campo.-** Mediante esta investigación nos va a permitir conocer el diseño, la implementación, acoplamiento y calibración de los diferentes equipos esto se lo realizará con diferentes pruebas que se encuentre para verificar su correcto funcionamiento y experimentación del mismo.

Este proyecto de investigación ayudará con la seguridad que solicita la UNIDAD EDUCATIVA FISCOMISIONAL “SAN MIGUEL”.

**Métodos, Técnicas e Instrumentos**

**Métodos:**

- **Analítico.-** Ocuparemos este método ya que es de mucha ayuda para entender en forma intensiva cómo funciona cada una de los dispositivos de vigilancia

que van a ser implementados en el sistema de vigilancia para su correcta implementación, acople y correcto funcionamiento y la interfaz del hardware a software para su verificación, análisis y monitoreo de la misma.

- **Sintético.-** Como antes hemos dividido en partes los componentes o elementos ahora debemos reconstruir ya que son partes complementarias del hardware y software en el sistema.

**Técnicas:**

- **Observación:** es una de las técnicas más importantes del proyecto debido que estaremos realizando siempre pruebas para poder corregir y calibrar tanto la parte de los sistemas de vigilancia como la programación del router con ello descartaremos los errores y corregiremos en cada prueba para dejar el sistema en un óptimo funcionamiento.
- La observación de campo es el recurso principal de la observación descriptiva; se realiza en los lugares donde ocurren los hechos o fenómenos investigados. La investigación social y la educativa recurren en gran medida a esta modalidad.

**Instrumentos**

- En esta parte de los instrumentos ocupamos algunos como son libros, reglamentos, archivos y páginas web, para recopilar información referente a la implementación de los equipos como configuración de los dispositivos de medición (sensores) datasheets, planos y manuales. Así como los dispositivos que van a ser utilizados para el sistema de video vigilancia.

## 2.2 POBLACIÓN Y MUESTRA

### Población

Para la presente investigación la población se enmarca en la Unidad Educativa “San Miguel”, perteneciente al Cantón San Miguel, en la provincia de Bolívar.

## 2.3 OPERACIONALIZACIÓN DE VARIABLES

| VARIABLES | DIMENSIONES | INDICADORES | ITEMS |
|---|---|---|---|
| **Variable Independiente:**<br><br>El Diseño e Implementación de un Sistema De Video Vigilancia Mediante Cámaras Ip. | La estructura donde se ubicarán las cámaras IP.<br><br>Funcionamiento óptimo de las cámaras IP. | La Estructura<br><br>Visualización del funcionamiento por medio del software respectivo. | Por medio del software de las cámaras se podrá observar su funcionamiento óptimo en la visualización de los datos recibidos? |

| VARIABLES | DIMENSIONES | INDICADORES |
|---|---|---|
| **Variable Dependiente:**<br><br>Administración Del Protocolo Snmp**,** utilizando una alarma GPRS. | Según los requerimientos que se requieren y ajusten al proyecto | **Alarma GPRS:** Conectividad entre las cámaras Ip y configuración de envió sms. |

**Tabla. 2.1:** Operacionalización de Variables.

**Elaborado por:** Paúl Orta.

## 2.4 PROCEDIMIENTOS

El procedimiento a utilizar, para el desarrollo de manera adecuada el proyecto, con el fin de dar cumplimiento a los objetivos planteados es:

### 2.4.1 RECOPILACIÓN DE ANTECEDENTES PRELIMINARES.

En esta etapa se realizará la búsqueda de los diferentes equipos con soporte a SNMP[83] v1, v2c, v3 que se presentarán en el diseño e implementación del sistema de seguridad de video vigilancia en proyectos similares en nuestro país y el mundo.

### 2.4.2 DETERMINAR EQUIPOS DE CONMUTACIÓN, DE VIDEO, HERRAMIENTAS Y CABLES A SER UTILIZADOS.

Para cumplir con éste paso, se debe realizar las actividades descritas a continuación:

a) Investigar y buscar equipos de conmutación con soporte SNMP v1, v2c, v3.
b) Indagar y buscar Cámaras Ip de acuerdo a las especificaciones del diseño y requerimientos del sistema de seguridad de video vigilancia.
c) Determinar las herramientas como son ponchadoras rj45, Lan tester, cable UTP[84] cat 6 o 5e

### 2.4.3 DISEÑO DE LA RED LAN.

a) Realizar una evaluación visual de la cantidad de dispositivos de video y la ubicación de las mismas en lugares estratégicos.

[83] Simple Network Management Protocol
[84] Unshielded twisted pair

### 2.4.4 EFECTUAR LA EVALUACIÓN FUNCIONAL DEL SISTEMA POR MEDIO DEL SOFTWARE WIRESHARK.

Para cumplir con éste paso, se debe realizar las actividades descritas a continuación:

a) Realizar la implementación del sistema con todos los equipos primordiales de acuerdo a las solicitaciones de la Unidad Educativa “San Miguel”.
b) Efectuar las pruebas necesarias que circulan el tráfico en la red diseñada.
c) Digitalizar los datos de las capturas, por cuanto determinar el estado del sistema.
d) Comparar las capturas de SNMP con distintos programas desarrollados para el efecto.

### 2.4.5 IDENTIFICAR Y REALIZAR LAS MEDICIONES DE LOS DISPOSITIVOS POR MEDIO DE:

a) Efectuar las pruebas de comunicación por medio de ping y Tracerouter desde el software correspondientes como son Mg-Soft Net Inspector, OidView, iReasoning, Lansweeper.
b) Citar las posibles causas y efectos que producen comunicación o fallas de comunicación.

### 2.4.6 CITAR POSIBLES SOLUCIONES EN EL CASO DE HABER ALGÚN DESPERFECTO EN EL SISTEMA.

Identificados los equipos de comunicación y de video encontrados para el sistema de seguridad en la red se procede a citar posibles soluciones de reparación en el caso de algún desperfecto en todo el sistema.

Para el seguimiento de un procedimiento ordenado y adecuado se realizó un organigrama de la siguiente manera:

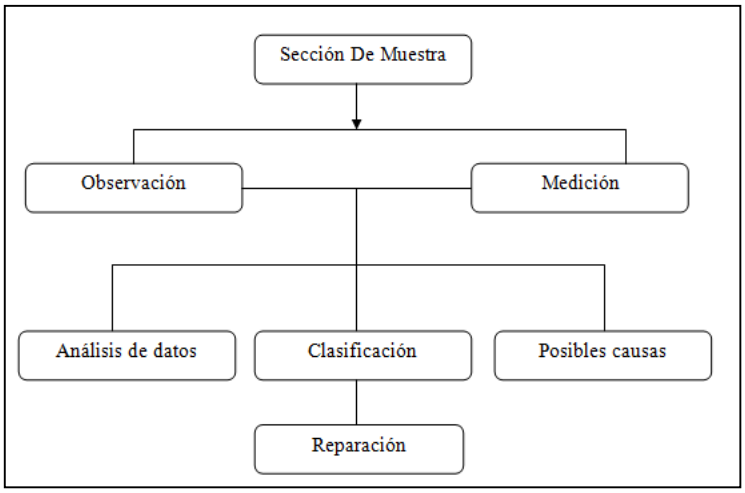



**Tabla 2.2:** Organigrama del procedimiento.

**Elaborado por:** Paúl Orta.

## 2.5 PROCESAMIENTO Y ANÁLISIS

Para realizar el diseño y la implementación del sistema de seguridad de video vigilancia que se presenta para la Unidad Educativa "San Miguel" se efectuó en base a los requerimientos y necesidades del mismo.

### 2.5.1 METODOLOGÍA

#### 2.5.1.1 ENFOQUE DE LA INVESTIGACIÓN.

El enfoque del estudio se desarrolló bajo el paradigma cuantitativo el cual se lo realizo a través de la investigación de campo en forma directa en el lugar de los hechos, en donde se recabo la información necesaria para la misma.

#### 2.5.1.2. INVESTIGACIÓN DE CAMPO.

La investigación tuvo una modalidad de campo para recolectar información en los siguientes aspectos: mayor seguridad a los estudiantes en la Unidad Educativa "San Miguel".

### 2.5.1.3 INVESTIGACIÓN DOCUMENTAL BIBLIOGRÁFICA

La investigación tuvo una modalidad bibliográfica ya que permitió profundizar diferentes tecnologías, conceptos y teorías aplicables a las variables dependientes e independientes para lo cual se empleó diferentes medios de investigación como libros, revistas de electrónica, etc.

### 2.5.1.4 PROYECTO FACTIBLE.

El estudio de este proyecto fue posible realizarlo debido el interés de la Unidad Educativa “San Miguel” por salvaguardar a los estudiantes del mismo, debido que este proyecto se desarrolló bajo una propuesta; practica y viable para la solución del mismo, luego de realizar una investigación de campo y fundamentar esta propuesta en una base teórica sostenible y confiable.

## 2.6. NIVEL DE INVESTIGACIÓN.

### 2.6.1 EXPLORATORIO.

La investigación tuvo una modalidad exploratoria, porque permitió saber cuál es la realidad del problema, y de esa manera encontrar las causas del mismo, alcanzo un nivel descriptivo para determinar cuáles fueron las implicaciones del problema.

### 2.6.2 RECOLECCIÓN DE INFORMACIÓN

Una vez cumplida la recolección de información de la investigación, se procedió al análisis de los datos obtenidos, lo que sirvió como un punto de referencia para el tema propuesto.

### 2.6.3 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

El procesamiento de la información recolectada siguió el siguiente procedimiento:

- Revisión de la información recolectada
- Repetición de la recolección de la información en ciertos casos individuales.
- Manejo de información

**Número de usuarios a realizar las encuestas:**

Para calcular el número de usuarios a ser encuestados se aplicara la siguiente fórmula:

$$n = \frac{N}{(N-1) * E^2 + 1}$$

Dónde:

n = Tamaño de la muestra.
N = Población a investigarse
E = Error máximo admisible (al 1%, 2%, 3%, 4%, 8%) a mayor error probable, menor tamaño de la muestra.

$$n = \frac{209}{(209-1) * 0{,}05^2 + 1}$$

$$n = \frac{209}{1{,}52}$$

$$n = 137.5$$

$$\mathbf{n = 138\ personas}.$$

Empleando la formula se calculó que el número de usuarios, que estarán inmersos y que evaluarán el Índice de Servicio Actual del Sistema de Seguridad.

### 2.6.4 CÁLCULO DEL ANCHO DE BANDA

A continuación se presenta el procedimiento para el cálculo del ancho de banda tomando como referencia la Tabla 2.3.

| RESOLUCIÓN | NIVEL DE COMPRESIÓN | FORMATO |
|---|---|---|
| NTSC 704x480 | 43KB | M-JPEG |

**Tabla 2.3 Datos para el cálculo del ancho de banda** (Blade, 2004)

Para el cálculo se toma una resolución de 704 x 480, que presenta un nivel de compresión bajo y 43KB en el formato M-JPEG que es uno de los formatos que más ancho de banda ocupa.

Determinación del número de tramas:

$$\text{Número de Tramas} = \frac{\text{Tamaño de la aplicación}}{\text{datos útiles de la trama Ethernet}}$$

$$\#\ \text{Tramas} = \frac{43\ \text{KBytes}}{1460\text{Bytes}}$$

$$\#\ \text{Tramas} = 29.45 = 30$$

Determinación de la sobrecarga que produce el paquete transmitido:

$$\text{Sobre carga total} = \#\ \text{tramas x sobre carga trama Ethernet}$$

$$\text{Sobre carga total} = 30 \text{ x } 66 \text{ Bytes}$$

$$\text{Sobre carga total} = 1980 \text{ Bytes}$$

Finalmente se establece el ancho de banda requerido por una sola cámara para una frecuencia de 10 imágenes por segundo, que es el parámetro promedio admisible en aplicaciones de video vigilancia.

$$\mathrm{AB}_{\mathrm{Camara1}} = \frac{359{,}84\ \mathrm{KBits}}{1\mathrm{imagen}} * \frac{10\ \mathrm{imagen}}{\mathrm{s}}$$

$$\mathrm{AB}_{\mathrm{Camara1}} = 3.59\ \mathrm{Mbps}$$

$$\mathrm{AB}_{\mathrm{Total}} = \#\ \mathrm{de\ camaras} * \mathrm{AB}_{\mathrm{Camara1}}$$

$$\mathrm{AB}_{\mathrm{Total}} = 3 * 3.59\ \mathrm{Mbps}$$

$$\mathrm{AB}_{\mathrm{Total}} = 10{,}77\ \mathrm{Mbps}$$

## 2.7. DISEÑO LÓGICO Y FÍSICO (Axis, Axis)

### 2.7.1 ASIGNACIÓN DE DIRECCIONES IP

En el diseño del sistema de video vigilancia se toma en cuenta los puntos de vulnerabilidad. El diseño es destinado únicamente para video vigilancia es decir, solamente tráfico de video, por lo tanto se tendrá una sola subred. Para el direccionamiento se tomará la dirección IP **192.168.15.1** una dirección Clase C privada que permite hasta 254 host con una máscara por defecto **255.255.255.0**

La subred utilizada será la 192.168.15.0 / 24, con un rango de 254 direcciones IP primera dirección válida 192.168.15.1, la última dirección válida 192.168.15.254 y dirección de broadcast es la 192.168.15.255.

| UBICACIÓN | DISPOSITIVO | DIRECCIÓN IP | MÁSCARA |
|---|---|---|---|
| **Rectorado Y Oficinas** | Cámara Vivotek | 192.168.1.6 | 255.255.255.0 |
| **Pasillo Primer Piso** | Cámara Agasio 1 | 192.168.1.8 | 255.255.255.0 |
| **Patio General** | Cámara Agasio 2 | 192.168.1.13 | 255.255.255.0 |
| **Cuartos De Equipos** | Router Huawei | 192.168.1.1 | 255.255.255.0 |
| | Router cisco | 192.168.1.2 | 255.255.255.0 |

**Tabla 2.4 Direccionamiento Ip**

**Elaborado por:** Paúl Orta.

Al diseñar un sistema de video en red, a menudo existe la intención de mantener la red sin contacto con otras redes por motivos tanto de seguridad como de rendimiento. Las subredes conforman una solución mejor y más rentable que una red independiente.

Solo los usuarios de un grupo específico pueden intercambiar datos o acceder a determinados recursos en la red.

En el diseño se creará una subred destinado solo para el sistema de video vigilancia de otro tipo de aplicaciones que puedan integrarse en el futuro como lo son redes de datos, de voz o incluso aplicaciones para control de acceso en la misma red de video vigilancia.

## 2.8 CAPACIDAD DE ALMACENAMIENTO DEL SERVIDOR DE VIDEO

(Axis, Axis, 2010)

### 2.8.1 ALMACENAMIENTO DIRECTAMENTE CONECTADO

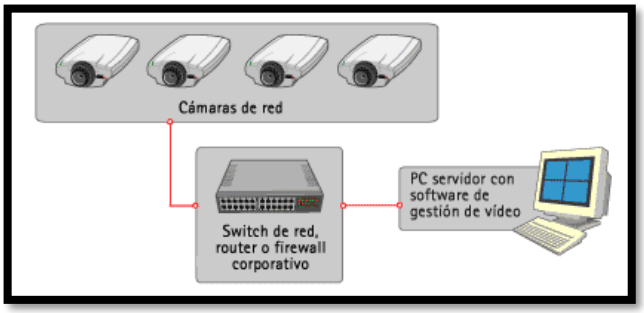



**Figura 2.1 Esquema de Almacenamiento Directo** (Axis, Axis)

Esta es la solución más habitual para el almacenamiento en discos duros en instalaciones de tamaño medio (50 dispositivos) y pequeño. El disco duro se encuentra en el mismo computador que ejecuta el software de gestión de vídeo.
El espacio viene determinado por las características del ordenador y del número de discos duros que puede admitir. La mayoría de computadores normalmente incluyen 2 discos. Actualmente se maneja capacidades de 1 TB[85] en discos de alto rendimiento, lo que daría una capacidad de 2 TB con 2 discos.

### 2.8.2. CÁLCULO DE CAPACIDAD DE ALMACENAMIENTO (Tanenbaum)

Se debe tomar en cuenta los siguientes factores para calcular las necesidades de almacenamiento:

El número de cámaras: 3 cámaras
El número de horas por día en que la cámara estará grabando: 24 horas o por programación del administrador.
El tiempo de almacenamiento: 2 semanas
Tipo de grabación: Detección de movimiento o grabación continua.
Velocidad de imagen, tipo de compresión, calidad de la imagen y complejidad.
El cálculo se realiza para las peores condiciones para lo cual se usará: El formato M-JPEG que maneja un método de compresión que brinda una excelente calidad de video pero demanda un ancho de banda mayor para su transmisión.

La resolución de imagen NTSC 352x240, con un nivel de compresión bajo de 10 KB y a 10 imágenes por segundo para una visualización aceptable.
A continuación se presenta los cálculos de almacenamiento para una cámara que realiza grabación continua y programada:
Capacidad de almacenamiento por hora.

$$\text{Capacidad/hora} = \text{TamañoImagen} * \#\ \text{de Imagenes}$$

[85] Terabyte

$$\text{Capacidad/hora} = \frac{10\ \text{KB}}{\text{imagen}} * \frac{10\ \text{imagen}}{\text{seg}} * \frac{3600\ \text{seg}}{1\ \text{hora}}$$

$$\text{Capacidad/hora} = 360\text{MB/hora}$$

Capacidad de almacenamiento por día.

Grabación Continua

$$\text{Capacidad/día} = \text{Capacidad/hora} * 24\ \text{horas}$$

$$\text{Capacidad/día} = \frac{360\ \text{MB}}{\text{hora}} * 24\ \text{horas}$$

$$\text{Capacidad/día} = 8640\ \text{MB/día}$$

Grabación Programada

$$\text{Capacidad/día} = \text{Capacidad/hora} * 12\ \text{horas}$$

$$\text{Capacidad/día} = \frac{360\ \text{MB}}{\text{hora}} * 12\ \text{horas}$$

$$\text{Capacidad/día} = 4320\ \text{MB/día}$$

Capacidad de almacenamiento total.

$$\text{Capacidad Total} = \text{Capacidad por día} * \#\ \text{de días de grabación}$$

$$\text{Capacidad Total} = 8640\ \text{MB} * 15\ \text{días}$$

$$\text{Capacidad Total} = 129{,}6\ \text{GB}$$

$$\text{Capacidad Total} = \text{Capacidad por día} * \#\ \text{de días de grabación}$$

$$\text{Capacidad Total} = 4320\ \text{MB} * 15\ \text{días}$$

$$\text{Capacidad Total} = 64{,}8\ \text{GB}$$

En la Tabla 2.5. Se resume de datos y cálculos de la capacidad de almacenamiento

| Cámara | # cámaras | Horas de grabación | MB / hora | GB / día | Días de grabación | TOTAL (GB) |
|---|---|---|---|---|---|---|
| Grabación Continua | 2 | 24 | 360 | 8.64 | 15 | 129.6 |
| Grabación Programada | 7 | 12 | 360 | 4.32 | 15 | 64.8 |

**Tabla 2.5 Resumen de Datos y Cálculos de la Capacidad de Almacenamiento**

(Tanenbaum A. s.)

## 2.9. ADMINISTRACIÓN DEL VIDEO (Blade, 2004)

Un aspecto importante del sistema de video vigilancia es la gestión de video para la visualización, grabación, reproducción y almacenamiento en directo. Si el sistema está formado por una sola cámara o por pocas cámaras, la visualización y la grabación básica de video se pueden gestionar mediante la interfaz web incorporada de las cámaras de red. Cuando el sistema consta de más cámaras, recomendable utilizar un sistema de gestión de video en red.

Actualmente, existen cientos de sistemas de gestión de video diferentes, con diferentes sistemas operativos (Windows, UNIX, Linux y Mac OS).

Los aspectos que deben considerarse son la elección de plataforma de hardware (PC basado en servidor o uno basado en grabadores de video en red); plataforma de software; características del sistema, que incluyen la instalación y configuración, gestión de eventos, video inteligente, administración y seguridad; y posibilidades de integración con otros sistemas.

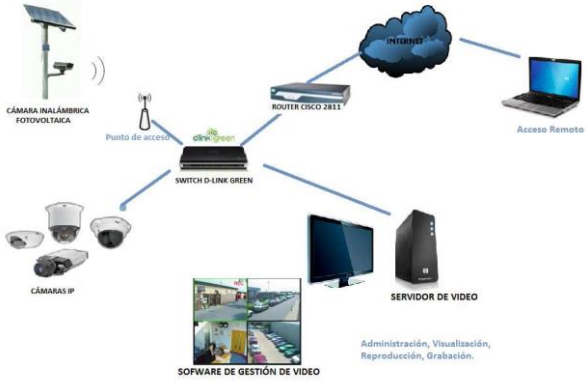



**Figura 2.2 Esquema de Solución con Plataforma de Servidor PC** (Blade, 2004)

En el diseño se utilizará para la administración de video la plataforma de servidor basado en PC pues este permitirá mayor escalabilidad para un futuro a diferencia de la utilización de un NVR cuyo trabajo está diseñado exclusivamente para gestión del video, lo cual no permitiría a futuro la integración de otras aplicaciones como control de acceso. Además, la plataforma de servidor basada en PC permitirá aplicar el concepto de tecnologías verdes sobre la virtualización de servidores en el caso que se desee integrar otras aplicaciones.

### 2.9.1. PLATAFORMA DE SOFTWARE

Se pueden utilizar plataformas de software diferentes para gestionar video.
Implican el uso de interfaz web incorporada, o el uso de un programa de software de gestión de video independiente que es una interfaz basada en Windows o en Web.

### 2.9.2. SOFTWARE CON FUNCIONALIDAD INCORPORADA.

Se puede acceder a las cámaras de red por medio de la red introduciendo la dirección IP del producto en el campo dirección/ubicación de un navegador web de un computador. Una vez se ha conectado con el producto de video en red, se visualiza de forma automática en el navegador la “página inicial” del producto junto con los enlaces a las páginas de configuración del producto. La interfaz Web

incorporada de los productos de video en red ofrece funciones de grabación simples: grabación manual de secuencias de video (H.264, MPEG-4, Motion JPEG) a un servidor haciendo clic en un icono; o grabación activada por evento de imágenes JPEG individuales a una o varias ubicaciones. La grabación activada por evento de secuencias de video es posible con productos de video en red que admiten almacenamiento local. Para obtener una mayor flexibilidad y más funcionalidades de grabación en términos de modos (por ejemplo, grabaciones continuas o programadas), se requiere un programa de software de gestión de video independiente. La configuración y gestión de un producto de video en red mediante su interfaz Web incorporada sólo funciona cuando se tiene un sistema con número reducido de cámaras.

### 2.9.3. SOFTWARE DE GESTIÓN PARA EL DISEÑO.

En el diseño se seleccionará un software de gestión del video que sea compatible con las cámaras Agasio y Vivotek. Además deberá tener la capacidad de administración de 9 o 16 cámaras por posibles expansiones de la red de video vigilancia en un futuro.

El sistema de gestión de video permitirá:

· Visualización simultanea de video desde varias cámaras

· Grabación de video y audio

· Funciones de gestión de eventos con video inteligente, como detección de movimiento de video.

· Administración y gestión de cámaras

· Opciones de búsqueda y reproducción

· Control de acceso de usuarios y registro de actividades.

### 2.9.4. VISUALIZACIÓN (vivotek)

Una función clave del sistema de gestión de video es la de permitir la visualización de video en directo y grabado de un modo eficiente y fácil de usar.

La mayor parte de aplicaciones de software de gestión de video permiten a múltiples usuarios visualizar en diferentes modos como: el de vista dividida (para visualizar diferentes cámaras al mismo tiempo), pantalla completa o secuencia de cámaras (donde se muestran de forma automática vistas de diferentes cámaras, una tras otra).


**Figura 2.3 Visualización en el Sistema de Gestión de Video** (Blade, 2004)

### 2.9.5. GRABACIÓN DE VÍDEO

El software de gestión de video, permite grabar video manualmente, de forma continuada y por activación (movimiento o alarma) y se pueden programar grabaciones continuas y activadas para que se ejecuten en horas seleccionadas durante cada día de la semana. Las grabaciones continuas suelen utilizar más espacio de disco que las grabaciones activadas por detección de movimiento.

Mediante las grabaciones programadas, se pueden configurar los horarios tanto para las grabaciones continuas como para las activadas por alarma o movimiento.

### 2.9.6. GRABACIÓN Y ALMACENAMIENTO

La mayor parte de software de gestión de video utiliza el sistema de ficheros de Windows estándar para el almacenamiento, así que se puede utilizar cualquier disco del sistema o conectado a la red para el almacenamiento de video. Un

programa de software de gestión de video puede activar más de un nivel de almacenamiento. Por ejemplo, las grabaciones se efectúan en un disco duro principal (el disco duro local) y el archivo se realiza en discos locales, conectados a la red o discos duros remotos. El administrador puede especificar cuánto tiempo deben permanecer las imágenes en el disco duro principal antes que se eliminen automáticamente o se muevan al disco de archivo.

### 2.9.7. GESTIÓN DE EVENTOS Y VÍDEO INTELIGENTE

Las funcionalidades de evento y video inteligente pueden funcionar juntas para hacer posible un sistema de video vigilancia para ser usado de forma más eficiente el ancho de banda de la red y el espacio de almacenamiento. La supervisión en directo de las cámaras de forma permanente no es necesaria, ya que las notificaciones de alerta a operadores se pueden enviar cuando se origina un evento.

### 2.9.8. DETECCIÓN DE MOVIMIENTO DE VÍDEO

La VMD[86] es una característica común en los sistemas de gestión de video. Es una manera de definir la actividad de una escena analizando los datos de las imágenes y las diferencias en las secuencias de imágenes. Con VMD, se puede detectar el movimiento en cualquier parte del campo visual de una cámara. El uso de VMD ayuda a priorizar las grabaciones, a reducir la cantidad de video grabado y facilita la búsqueda de eventos, lo cual favorecerá en el diseño del sistema de video vigilancia para ahorrar espacio en el disco y ahorrar energía en cámaras ya se utilizarán sus recursos únicamente cuando sea necesario (activación por movimiento).

[86] Detección de movimiento de video

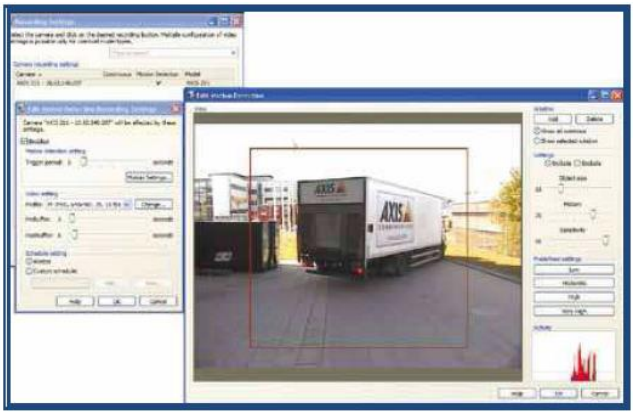


**Figura 2.4 Detección de movimiento en el Sistema de Gestión de Video**

(Blade, 2004)

### 2.9.9. ALIMENTACIÓN A TRAVÉS DE ETHERNET (POE)

La alimentación a través de Ethernet (PoE[87]) es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como, por ejemplo, un teléfono IP o una cámara 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 (UPS[88]) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

Power Over Ethernet está regulado en la norma 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 misma. 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.

[87] Power over Ethernet,
[88] Uninterruptible power supply


**Figura. 2.5 Alimentación POE** (Blade, 2004)

Esta norma utiliza cables estándares categoría 5 o superiores y asegura que la transferencia de datos no se vea afectada. En dicho estándar al dispositivo que proporciona la energía se le conoce como PSE[89]. El dispositivo que recibe la energía se conoce como dispositivo alimentado.

Esta función normalmente está integrada en un dispositivo de red, como una cámara, o en un splitter independiente. La norma incluye un método para identificar automáticamente si un dispositivo es compatible con PoE, y sólo se le proporciona energía una vez que se ha confirmado dicha compatibilidad. La norma 802.3af establece que un PSE proporciona un voltaje de 48 VCC con una potencia máxima de 15,4 W por puerto; pero debido a las pérdidas que se producen en un cable de par trenzado sólo se garantiza 12,95 W.

Actualmente existen en el mercado varios dispositivos de red como switches o hubs que soportan esta tecnología. Cuando un dispositivo no soporta PoE se usa los midspans y splitters que son equipos que permiten que una red existente sea compatible con la alimentación a través de un cable de red. El midspan es un dispositivo (con conectores RJ45 de entrada y de salida) con un adaptador de alimentación que recoge la electricidad; y el splitter es el dispositivo terminal (también con conectores RJ45) con un cable de alimentación que permite que el equipo final obtenga la energía necesaria para su funcionamiento.

[89] Equipo de suministro eléctrico

En el diseño se toma a PoE como una excelente solución amigable con el medio ambiente, eliminando la necesidad de instalar más cableado, conductos y enchufes, es decir, esta tecnología no es invasiva con el entorno natural o rústico.

Si en el diseño se hubiese optado por un sistema analógico de video vigilancia o sistemas mixtos de cámaras analógicas con grabadores digitales; tecnologías como PoE no podrían ser usadas. Los CCTV[90] analógicos usan cámaras y otros dispositivos, tales como los multiplexores y DVRs, que necesitan fuentes de alimentación individuales (cableado, salidas de c.a. y adaptadores tipo "Wall wart"), lo que implica la presencia de electricistas y adicionalmente en cada uno de los dispositivos se necesitaría la instalación de sistemas de alimentación ininterrumpida individuales, como prevención en caso de fallas eléctricas.

En el diseño la implementación PoE permitirá un ahorro de costos en fuentes de alimentación y cableado. Además, PoE ayuda a la administración de la red permitiendo a los administradores monitorear y manejar los dispositivos desde lejos. Los dispositivos PoE pueden ser reconfigurados de forma remota y el consumo de energía puede ser monitoreado, lo cual es conveniente cuando se habla de un diseño, pues por ejemplo se podría reconfigurar las opciones de apagado de una cámara que no esté siendo utilizada, o cambiando opciones como monitoreo por detección de movimientos en lugares no muy concurridos, lo que permitiría un ahorro de energía pues la cámaras en estas zonas no trabajarían a tiempo completo en vano.

**2.9.9.1. VENTAJAS DE POE** (vivotek)

PoE es una fuente de alimentación inteligente: Los dispositivos se pueden apagar o reiniciar desde un lugar remoto usando los protocolos existentes, como el Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol).

[90] Closed circuit television

PoE simplifica y abarata la creación de un suministro eléctrico altamente robusto para los sistemas permitiendo la centralización de la alimentación.
En los sistemas basados en PoE se pueden enchufar al sistema de alimentación ininterrumpida central.

Los dispositivos se instalan fácilmente donde pueda colocarse un cable LAN, y no existen las limitaciones debidas a la proximidad de una base de alimentación (dependiendo la longitud del cable se deberá utilizar una fuente de alimentación de mayor voltaje debido a la caída del mismo, a mayor longitud mayor pérdida de voltaje, superando los 25 metros de cableado aproximadamente).

Power Over Ethernet tiene el potencial de reducir el riesgo de daños eléctricos puesto que utiliza bajo voltaje en comparación con los dispositivos no alimentados por Ethernet en los que es necesario un voltaje más alto. La tecnología Power Over Ethernet también ayuda a proteger los equipos contra sobre voltajes momentáneos y picos de corriente.
POE también permite conseguir una localización óptima de las cámaras a fin de maximizar la cobertura, esto significa que los instaladores de cámaras de red no son limitados por la localización de las fuentes de alimentación existentes.

## 2.10 CÁMARAS IP

### 2.10.1 CRITERIOS DE SELECCIÓN DE CÁMARAS IP

Para escoger de la forma más acertada una cámara IP es necesario determinar los diferentes criterios de selección de las mismas, entre estos:

**Objetivo de vigilancia**

El objetivo de vigilancia puede ser de visión amplia o de detalle más elevado. El objetivo de la visión amplia es ofrecer la totalidad de una escena o los cambios generales de todos los elementos en movimiento.

Las imágenes con un nivel de detalle más elevado son útiles para la identificación de objetos o personas (reconocimiento de rostros, matrículas de vehículos, etc).

**Zona de cobertura**

La zona de cobertura determina el tipo y el número de cámaras que se utilizarán, para lo cual se debe establecer el número de zonas de interés y el grado de cobertura que se necesita dependiendo de la zona.

**Entorno o ambiente**

El entorno puede ser interior o exterior. El tipo de ambiente determina la sensibilidad lumínica, la utilización de carcasas cuando se requiere protección frente al polvo, la humedad o los actos vandálicos, mayoritariamente son empleados en ambientes exteriores.
Las cámaras con diseño oculto son empleadas en entorno interior en el cual es importante que la cámara pase desapercibida.

**Calidad de imagen.**

En el diseño se usarán cámaras IP que al utilizar tecnología digital tienen una buena calidad de la imagen. En el caso de que la prioridad sea capturar objetos en movimiento, es importante que la cámara incorpore tecnología de barrido progresivo.

**Resolución**

La resolución está relacionada con el nivel de detalle y el tamaño de la imagen. Para zonas donde se exige un alto nivel de detalle es necesaria la utilización de cámaras con mayor resolución.

**Compresión.**

Para mejorar el rendimiento de un sistema es importante que una cámara maneje por lo menos dos estándares de compresión. Los tres estándares de compresión de vídeo más utilizados para sistemas de video vigilancia son MPEG-4, Motion JPEG y H.264

**Funcionalidades de red**

Entre las principales funcionalidades de red se incluyen PoE, cifrado HTTPS para cifrado de secuencias de vídeo antes de que se envíen a través de la red, filtrado de direcciones IP, que permite o deniega los derechos de acceso a direcciones IP definidas.

**Aplicaciones de software.**

Los productos deben admitir una amplia variedad de soluciones de software de gestión de vídeo procedentes de diferentes marcas.
Su alimentación deberá ser mediante la tecnología POE en el caso de las cámaras para interiores y la cámara exterior con alimentación con energías alternativas.

### 2.10.2 DESCRIPCIÓN DEL TIPO DE CÁMARAS A USARSE

#### 2.10.2.1 CÁMARAS IP TIPO 1 (Vivotek)

Las cámaras IP tipo 1 tienen las características de una cámara IP de alto nivel, estas estarán ubicadas en zonas de rectorado dentro de estas están contempladas administración secretarial, y rectorado. Estas deben permitir tanto grabación continua como programada y adicionalmente la detección de movimiento para las zonas de tránsito. De esta forma se disminuirá la cantidad de grabación de forma innecesaria ahorrando espacio en el disco y ahorro de energía. Además soportarán tecnología PoE y como mínimo dos formatos de compresión.

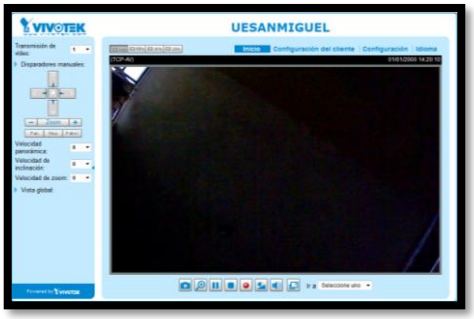



**Figura 2.6 Ubicación de Cámaras tipo 1 y cobertura.**

**Elaborado por:** Paúl Orta.

### 2.10.2.2 CÁMARAS IP TIPO 2 (Agasio)

Este tipo de cámaras serán usadas en los pasillos del primer piso y zonas de mayor afluencia de estudiantes. Estas cámaras permitirán la grabación tanto de día como de noche con grabación ininterrumpida o programada dependiendo de las necesidades de la administración. La cámara no soportará tecnología PoE y como mínimo dos formatos de compresión. Adicionalmente, tendrán la capacidad de alarmas vía mail, movimiento y sonido, enfoque remoto y protección ante posibles manipulación física por parte de delincuentes.


**Figura 2.7. Ubicación de Cámaras tipo 2 y cobertura.**

**Elaborado por:** Paúl Orta.

## 2.11 VIGILANCIA REMOTA (Agasio)

### 2.11.1 CONEXIÓN A INTERNET

Para conectar una LAN a Internet se debe establecer una conexión de red a través de un ISP[91]. En una conexión a Internet se utilizan términos como velocidad de subida y velocidad de bajada. La velocidad de subida describe la velocidad de transferencia con la que se pueden subir datos del dispositivo a Internet: por ejemplo, cuando se envía un video desde una cámara de red. La velocidad de bajada es la velocidad de transferencia con la que se bajan archivos: por ejemplo, cuando un monitor de ordenador recibe un video.

En la mayoría de casos como un portátil conectado a Internet, por ejemplo: la descarga de información desde Internet es la velocidad más importante a tener en cuenta. En una aplicación de video en red con una cámara de red situada en una ubicación remota, la velocidad de subida es más relevante, puesto que los datos (el video) de la cámara de red se subirán a Internet.

### 2.11.2 ACCESO REMOTO

Para acceder al sistema de vigilancia desde cualquier lugar del mundo se requiere una vía de comunicación estándar, como lo es el internet. El internet es un conjunto de redes independientes comunicadas entre sí a través del direccionamiento y los protocolos basados en IP. Para acceder a cualquier dispositivo basta escribir la dirección IP junto con el puerto en un browser, siempre y cuando la IP sea púbica y asignada de forma estática, caso contrario se deberá usar un sistema conocido como DDNS u otros existentes.

DDNS es un sistema dinámico de nombres de dominio que permite la actualización en tiempo real de la información sobre nombres de dominio situada

[91] Proveedor de servicios de Internet

en un servidor. DDNS[92] es muy útil cuando el ISP[93] asigna una IP pública dinámica, dada que la IP podría cambiar la única forma de localizar un equipo sería a través de un nombre de dominio. Mediante DDNS es posible localizar el router de una LAN privada para tener acceso a aplicaciones como un servidor de video, servidor web, servidor ftp, cámaras, etc.

Para hacer visible al router es necesario asociar su dirección IP con un nombre de dominio, esta acción la lleva a cabo un servidor DDNS, el más conocido y de suscripción libre es DynDNS accediendo a www.dyndns.com para crear una cuenta. El DynDns es un servicio que convierte nuestra dirección IP (que normalmente es dinámica) en una dirección con letras, algo así:
"uesanmiguel.dyndns.org" (dirección con letras) que es la que convertirá la dirección IP de números sin importar cuál sea esta.

#### 2.11.2.1 NAT (Network address translation – Traducción de dirección de red)

Para que un dispositivo de red con una dirección IP privada pueda enviar información a través de Internet, debe utilizar un enrutador compatible con NAT.
Con esta técnica, el enrutador puede traducir una dirección IP privada en una pública sin el conocimiento del host que realiza él envió.

#### 2.11.2.2 REENVÍO DE PUERTOS

El reenvío de puertos consiste en mapear la dirección IP pública a una dirección IP fija de una red privada. El reenvío de puertos hace posible el acceso a través de internet a dispositivos localizados en una red de área local, como servidores y cámaras, que tienen direcciones IP privadas.

Para acceder a dispositivos de red ubicados en una LAN privada a través de internet, se debería usar la dirección IP pública del router junto con el número de puerto de dicho dispositivo. Dado que por defecto las cámaras IP utilizan el

[92] Dynamic Domain Name System
[93] Proveedor de servicios de Internet

servicio HTTP (puerto 80), en un escenario con varios codificadores de video o varias cámaras de red, se tiene dos opciones; la primera es configurar un puerto diferente para cada una, o la segunda en lugar de cambiar el número de puerto predeterminado en cada cámara, para ello se puede configurar el router para asociar un único número de puerto HTTP[94] a la dirección IP y al puerto predeterminado de la cámara.

Los paquetes de datos entrantes llegan al router por medio de su dirección IP pública y del número de puerto. El router está configurado para reenviar los datos que entran por un número de puerto predefinido hacia un dispositivo específico de la parte del router correspondiente a la red privada. Luego el router sustituye la dirección del emisor por su propia dirección IP privada (interna). Para el cliente receptor el router es el origen de los paquetes y con los paquetes de salida ocurre lo contrario. El router sustituye la dirección IP privada del dispositivo origen por su IP pública del propio router antes de enviar los datos a través de Internet.

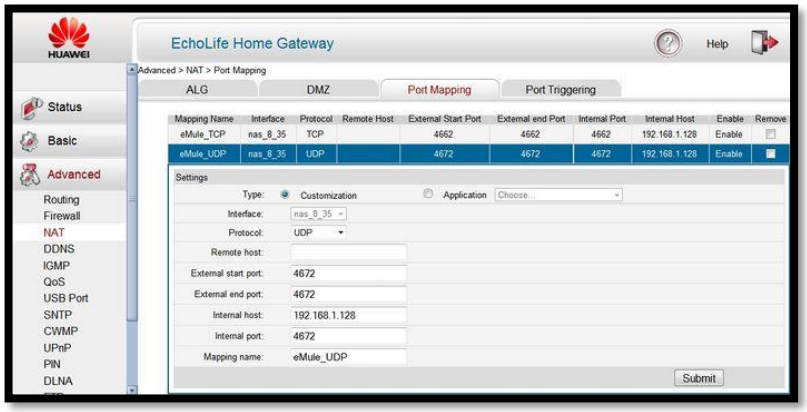



**Figura 2.8 Mecanismo Reenvío de Puertos** (Agasio)

En la Figura 2.8 el router reenvía la solicitud que recibe en el puerto 4672 hacia una cámara con la dirección IP privada 192.168.10.13 a través del puerto 80.
Cuando el enlace ha sido establecido la cámara empieza a enviar vídeo.

[94] HyperText Transfer Protocol

## 2.12 DESCRIPCIÓN DE LOS EQUIPOS (CISCO)

### 2.12.1 ELECCIÓN DE EQUIPOS ACTIVOS RED

#### 2.12.1.1 ROUTER (Cisco)

Este dispositivo permite aislar la Red LAN de Video Vigilancia de la Unidad educativa San Miguel de la Internet. Una interfaz Ethernet está conectada a la Red LAN que se propone instalar y una interfaz serial se utiliza en un enlace WAN[95] con el proveedor de servicios de Internet.

**Router Cisco Rv 120 W**

El router cisco brinda mayor seguridad para conexiones remotas y es más robusto y puede manejar grandes flujos de datos. Este router brinda la opción de expansión de la red en un futuro.

Además el router Cisco RV 120W permitirá establecer políticas de seguridad ya que todo el tráfico de la red se encamina por medio de este.

**Características del Router Cisco Rv 120W**

| Función | Descripción |
|---|---|
| Enrutamiento | ● Enrutamiento estático<br>● RIP[96] v1 y v2<br>● Enrutamiento entre VLAN[97] |
| Capa 2 | |

[95] Red de Área Amplia
[96] Routing Protocol Information
[97] Red de área local virtual

| | |
|---|---|
| | ● VLAN basadas en 802.1q<br>● 4 VLAN activas (intervalo de 1 a 4094) |
| Red | ● Servidor DHCP[98] (Protocolo de Configuración Dinámica de Host), agente de relé DHCP<br>● Protocolo de Punto a Punto en Ethernet (PPPoE), Protocolo de Túnel Punto a Punto (PPTP), Protocolo de Túnel de capa 2 (L2TP)<br>● Proxy DNS<br>● Proxy IGMP y reenvío de multidifusión<br>● Sistema de Nombres de Dominio Dinámico (DynDNS, TZO)<br>● Traducción de Direcciones de Red (NAT), Traducción de Direcciones de Puertos (PAT), Traducción de Puertos y Direcciones de Red (NAPT), Puerta de Enlace de Capa de Aplicación de Protocolo de Inicio de Sesión (SIP ALG), NAT transversal, NAT uno a uno<br>● Varios conjuntos DHCP<br>● Administración de puertos |
| IPv6 | ● IPv4 e IPv6 con pila dual<br>● Multicast Listener Discovery (MLD) para IPv6 (RFC2710)<br>● Configuración automática de dirección sin estado<br>● DHCP v6<br>● Protocolo de Mensajes de Control de |

[98] Protocolo de Configuración Dinámica de Host

| | |
|---|---|
| | Internet (ICMP) v6 |
| Seguridad | Control de acceso:<br>● Listas de control de acceso (ACL) IP<br>● Control de acceso inalámbrico basado en MAC<br><br>Firewall:<br>● SPI Firewall<br>● Activación y reenvío de puerto<br>● Prevención de Denegación de Servicios (DoS)<br>● Red perimetral (DMZ) basada en software<br><br>Filtrado de contenido:<br>● Bloqueo estático de dirección URL y bloqueo de palabras clave<br><br>Administración segura:<br>● HTTPS<br>● Nombre de usuario/contraseña<br><br>802.1X<br>● Autenticación RADIUS basada en puertos (Protocolo de Autenticación Extensible [EAP], EAP Protegido [PEAP])<br><br>Administración de certificados<br>● Certificados X.509 v3<br>● Carga de certificados con formato PEM |

| | |
|---|---|
| VPN | ● 10 túneles QuickVPN para el acceso remoto de clientes<br>● 10 túneles IPsec de sitio a sitio para la conectividad de sucursales<br>● 3DES[99], Estándar de Cifrado Avanzado (AES)<br>● Autenticación mediante el algoritmo MD5[100] y el algoritmo SHA1[101]<br>● Detección de punto muerto (DPD)<br>● IPsec NAT transversal<br>● Transferencia de VPN[102] de PPTP, L2TP, IPsec |
| QoS[103] | ● Prioridad 802.1p basada en puerto en el puerto LAN, prioridad basada en la aplicación en el puerto WAN<br>● 4 colas<br>● Compatibilidad con servicios diferenciados<br>● Medición de tráfico |
| **Función** | **Descripción** |
| Administración | ● Versiones 1, 2c y v3 del Protocolo Simple de Administración de Red (SNMP) |

[99] Estándar de Triple Cifrado de Datos
[100] Message Digest 5
[101] Secure Hash Algorithm
[102] Virtual Private Network
[103] Calidad de servicio

| | |
|---|---|
| | ● Registro de eventos: locales, registro de eventos del sistema (syslog) y alertas de correo electrónico<br>● Firmware que se puede actualizar mediante el navegador web; configuración importada/exportada en formato de texto<br>● Configuración Simple Basada en Navegador (HTTP/HTTPS)<br>● UPnP[104], Bonjour<br>● Diagnósticos de red con capturas de paquetes |
| Rendimiento | ● Rendimiento de NAT: 95 Mbps<br>● 1.000 sesiones simultáneas<br>● Rendimiento de VPN: 25 Mbps |

**Tabla 2.6 Características Router Cisco** (CISCO)

**Especificaciones de LAN inalámbrica**

En la Tabla 2.7 se detallan las especificaciones inalámbricas de Cisco RV120W.

| **Función** | **Descripción** |
|---|---|
| Hardware de WLAN | Punto de acceso basado en las normas IEEE 802.11n compatible con 802.11b/g<br>Tipo de modulación y radio:<br>● 802.11b: espectro de extensión de la secuencia directa (DSSS) |

[104] Universal Plug and Play

| | |
|---|---|
| | ● 802.11g/n: (OFDM[105])<br>● 2 antenas externas omnidireccionales de alta recepción de 1,8 dBi<br><br>Canales operativos:<br>● 11 en América del Norte<br>● 13 en la mayor parte de Europa<br>● Selección automática de canales<br><br>Potencia de transmisión:<br>● 802.11b: 17 dBm +/– 1,5 dBm<br>● 802.11g: 15 dBm +/– 1,5 dBm<br>● 802.11n: 12,5 dBm +/– 1,5 dBm<br><br>Sensibilidad del receptor:<br>● 802.11b: 11 Mbps@ –90 dBm<br>● 802.11g: 54 Mbps @ –74 dBm<br>● 802.11n: 270 Mbps @ –71 dBm<br><br>Servicios de Dominio Inalámbricos (WDS[106]):<br>● Permite que hasta 2 receptores compatibles repitan las señales inalámbricas<br>● WMM[107] con QoS (802.11e)<br>● Ahorro de energía WMM (WMM-PS) |
| Identificadores de conjuntos de servicios (SSID) | ● Hasta 4 redes virtuales separadas |

[105] Multiplexación por división de frecuencias ortogonales
[106] Wireless Domain Services
[107] Wi-Fi multimedia

| | |
|---|---|
| Redes VLAN inalámbricas | ● Compatibilidad con la asignación SSID a VLAN con aislamiento de cliente inalámbrico |
| Seguridad de WLAN | ● Acceso protegido Wi-Fi (WPA2, 802.11i) |

**Tabla 2.7** Especificaciones de LAN inalámbrica (CISCO)

**Especificaciones del sistema**

En la Tabla 2.8 se detallan las especificaciones del sistema de Cisco RV120 W.

| **Función** | **Descripción** |
|---|---|
| WAN | Puerto WAN Fast Ethernet 10/100 |
| LAN | Switch de 4 puertos 10/100 Mbps compatible con VLAN y QoS |
| WLAN | Punto de acceso inalámbrico 802.11n integrado de alta velocidad |
| Dimensiones físicas y peso | ● Ancho x largo x alto = 5,91 pulgadas x 5,91 pulgadas x 1,34 pulgadas (150 mm x 150 mm x 34 mm)<br>● Peso: 1,10 lb (0,5 kg) |
| Alimentación | 12 V 1 A |
| Certificación | ● FCC, Clase B<br>● CE |

| | |
|---|---|
| | ● IC<br>● Wi-Fi |
| Rango de funcionamiento ambiental | ● Temperatura de funcionamiento: 0 ° a 40 °C (32 ° a 104 °F)<br>● Temperatura de almacenamiento: –20 ° a 70 °C (–4 ° a 158 °F)<br>● Humedad de funcionamiento: 10% a 85% sin condensación<br>● Humedad de almacenamiento: 5% a 90% sin condensación |

**Tabla 2.8** Especificaciones del sistema (CISCO)

### 2.12.2. ELECCIÓN DE CÁMARAS (Agasio) (vivotek)

#### 2.12.2.1. CÁMARA IP FIJA – VIVOTEK FD 8136 (Recepción, Administración, Gerencia)

La VIVOTEK PD8136 está equipada con un sensor de 1MP permitiendo una resolución de 1280x800 a 30 fps. Los usuarios ya no necesitan buscar una cámara todo-en-uno capaz de capturar vídeo de alta calidad y alta resolución con control Pan/Tilt. Con un diseño de estilo, y tamaño reducido puede instalarse en cualquier ambiente, es la mejor opción para la vigilancia de interiores, como tiendas, oficinas o viviendas.

Con un movimiento flexible de 360º horizontal y 80º vertical, La PD8136 permite a los usuarios un control fácil del lugar monitorizado. La PD8136 integra el estándar industrial H.264 de tecnología de compresión, que reduce drásticamente el tamaño de los archivos conservando el preciado ancho de banda de la red.

Además, la PD8136 integra la función Power over Ethernet, haciendo su instalación fácil y más económica. Junto al paquete de software de grabación de hasta 32 canales multilingüe ST7501, los usuarios pueden disponer fácilmente un sistema de vigilancia IP de utilización sencilla.


**Figura 2.9. Cámara Vivotek** (vivotek)

**Características Cámara Ip VIVOTEK FD 8136**

| Información Sistema | |
|---|---|
| CPU | Multimedia SoC (System-on-Chip) |
| Flash | 16 MB |
| RAM | 128 MB |
| **Características de la cámara** | |
| Sensor de imagen | CMOS 1/4" Progresivo |
| Máxima Resolución | 1280x800 pixels |
| Tipo de lente | Focal fija |
| Distancia Focal | f = 3.6 mm |
| Apertura | F1.8 |
| Campo de Visión | 56° (horizontal)<br>41° (vertical)<br>71° (diagonal) |
| Obturador | 1/5 sg. a 1/32,000 sg. |
| Iluminación mínima | 0.47 Lux, 50 IRE |
| Velocidad Pan | 100° / sg. |
| Rango Pan | 360° (-180° ~ + 180°) |
| Velocidad Tilt | 100° / sg. |

| | |
|---|---|
| Pan/tilt/zoom | ePTZ |
| Funcionalidades | Zoom digital 16x (4x en IE plug-in, 4x integrado) |
| Almacenamiento interno | Ranura MicroSD/SDHC |
| **Vídeo** | |
| Compresión | H.264, MJPEG y MPEG-4 |
| Velocidad máx Imágen | H.264:<br>30 fps a 1280x800<br>MPEG-4:<br>30 fps a 1280x800<br>MJPEG:<br>30 fps a 1280x800 |
| Streams máximos | 2 streams simultaneos |
| Relación S/R | Mas de 50 dB |
| Vídeo Streaming | Resolucion, calidad y bitrate ajustables<br>Video cropping para ahorro de ancho de banda |
| Configuración de imágen | Tamaño imagen, Calidad y bit rate ajustables<br>Estampación de fecha y hora, "flip" y "mirror"<br>Brillo, contraste, saturación, nitidez, balance de blancos, control de exposición, ganancia, |

| | |
|---|---|
| **Audio** | |
| Capacidades Audio | Entrada Audio |
| Compresión | G.711 |
| Interfaz | Micrófono integrado |
| Alcance efectivo | 5 metros |
| **Red** | |
| Usuarios | Visión en directo de hasta 10 clientes |
| Protocolos | IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, y 802.1X |
| Interfaz | 10Base-T/100 BaseTX Ethernet (RJ-45) |
| ONVIF | Especificación disponible en www.onvif.org |

| | |
|---|---|
| **Vídeo Inteligente** | |
| Detección de movimiento | Triple ventana de detección de movimiento |
| **Alarmas y Eventos** | |
| Disparo de Alarmas | Detección de movimiento en vídeo, disparo manual, disparo periodico, arranque sistema, notificación de grabación, sabotaje de cámara |
| Evento de Alarmas | Notificación de Evento utilizando salida digital, HTTP, SMTP, FTP y servidor NAS<br>Subida de archivo vía HTTP, SMTP, FTP y servidor NAS |

**Tabla 2.9 Características Cámara Vivotek** (vivotek)

### 2.12.2.2. CÁMARA IP FIJA – AGASIO A603W (Pasillo Primer Piso y Patio General)

Cámara de red de alto rendimiento, con visión día/noche: La cámara de red AGASIO A603W es una cámara de gama media pensada para aplicaciones exigentes de vigilancia (24 horas), a través de redes IP. La cámara proporciona imágenes de alta calidad bajo cualquier condición de iluminación, lo que hace que sea la solución perfecta para aplicaciones en interior y exterior, tanto de día como de noche, como por ejemplo para vigilancia de patios, áreas públicas, garajes, estaciones de metro y aeropuertos.


**Figura 2.10. Cámara Agasio A603W** (Agasio)

**Especificaciones del producto**

- Cámaras Agasio adoptar, procesadores de alto rendimiento fuerte función de comunicación (RSIC 32-Bit)
- Alto sensor CMOS[108]
- Compresión de vídeo MJPEG optimizada, la transmisión de imágenes de alta definición.
- Soporta un máximo de 15 usuarios que ven al mismo tiempo, no hay límite para transportistas de servicio.
- Función de servidor web, navegadores estándar se utilizan para la monitorización en tiempo real y administración.
- Soportes 802,11 protocolos de redes inalámbricas Wi-Fi b / g.
- Soporta sistema de actualización remota.
- Soporta DDNS análisis, LAN e Internet (ADSL, Cable Modem).
- Es compatible con una variedad de protocolos de red:

**TCP / IP, UDP, SMTP[109], PPPoE[110], Dynamic DNS, Cliente DNS, SNTP[111], BOOTP[112], DHCP, FTP, SNMP**.

- Los modelos específicos se apoyan y audio bidireccional (la cámara al usuario, el usuario de la cámara).
- Soporta funciones de alarma de detección de movimiento.
- Soporta fotos de la imagen.
- La función de recuperación automática, la reconexión automática disponible cuando la interrupción de la red detecta.
- Función de alarma dinámica, alarma configurable cronograma.

[108] Complementary Metal Oxide Semiconductor
[109] Simple Mail Transfer Protocol
[110] Point-to-Point Protocol over Ethernet
[111] Simple Network Time Protocol
[112] Bootstrap Protocol

## 2.13. ELECCIÓN DEL SERVIDOR DE VIDEO

El servidor de video debe tener instalado un sistema operativo robusto de preferencia un Windows 7 dado la gran cantidad de información que procesa y almacena. Tendrá una capacidad total mínimo a 1 TB, este valor se deriva del cálculo de la capacidad de almacenamiento. Deberá cumplir el parámetro de ahorro de energía.

| **CARACTERÍSTICAS SERVIDOR DE VIDEO** | |
|---|---|
| Sistema Operativo | Windows 7 |
| Procesador | Core Duo 2 |
| Velocidad Procesamiento | 2 GHz o superior |
| Memoria RAM | 2 GB |
| # de discos duros | 1 mínimo |
| Capacidad Total | 500 GB o superior |
| Tarjeta de red | 1 tarjetas de 100/1000 Mbps |
| Monitor | 17” |

**Tabla 2.10 Características del servidor**

## 2.14 ELECCIÓN DE SOFTWARE PARA ANÁLISIS DEL FUNCIONAMIENTO DE LA RED. (Wireshark)

### 2.14.1 WIRESHARK

Antes que nada se escogió el software de Wireshark, antes conocido como Ethereal, es el mejor analizador de redes (sniffer) de la actualidad. Es capaz de diseccionar gran cantidad de protocolos, SMTP, HTTP, POP3, SNMP, 802.11, 802.3 (Ethernet), etc., entre otros. Su arquitectura modular facilita la creación e integración de nuevos decodificadores de protocolo, y por esto existe una gran comunidad que suele agregar un decoder para casi cualquier tipo de protocolo existente. Además de sus capacidades de decodificación, también son destacables sus diversas funcionalidades para la obtención de datos desde las capturas, gráficos y tendencias. Una de sus características más importantes son los filtros

que permiten filtrar la información obtenida desde la red y de esta manera llegar a comprender y centrarnos en los datos relevantes.

Es una herramienta que sirve para hacer análisis de protocolos sumamente útil al momento de solucionar problemas de red. Es compatible con más de 480 protocolos y varios sistemas operativos.

Luego de seguir los pasos de instalación incluyendo en Wireshark e instalado el WinPcap, podremos acceder a la interface gráfica del Programa para comenzar a trabajar. Obviamente si tenemos problemas de red en una pc debemos ir a otra para efectuar la descarga.

### 2.14.2. PROGRAMAS DE GESTION PARA SNMP

En este paso nos ayudaremos con distintos programas de gestión en los cuales podremos comprobar la gestión de snmp con:

- MG-SOFT Mib Browser
- OidView
- SoftPerfect Network Scanner
- Manage Engine Mib Browser
- Power SNMP Manager
- SnmpSource MibViewer

#### 2.14.2.1. **MG-SOFT MIB Browser** (Mg-soft)

MG-SOFT MIB Browser Professional Edition con MIB Compiler es, técnicamente excelente, potente y fácil de usar navegador SNMP extremadamente flexible. Todo lo que hace MG-SOFT MIB Browser el navegador más utilizado

SNMP[113] que se ejecuta en **Windows, Linux, Mac OS X** o el sistema operativo **Solaris.**

MIB Browser permite supervisar y gestionar cualquier dispositivo SNMP en la red (es decir, servidores, archivos o base de datos, modems, impresoras, routers, switches,...) utilizando el estándar SNMPv1, SNMPv2c y SNMPv3 protocolos IPv4 o más redes IPv6. En el modelo estándar SNMPv3 USM seguridad, MIB Browser también es compatible con el modelo de intercambio de claves Diffie-Hellman, de modo que SNMPv3 agentes basados en DOCSIS (es decir, los módems de cable, sistemas de terminación de módem de cable, set-top boxes, etc) puede ser perfectamente de contacto y gestionado.

MIB Browser permite realizar SNMP Get, GetNext SNMP, SNMP GetBulk y operaciones Set de SNMP.

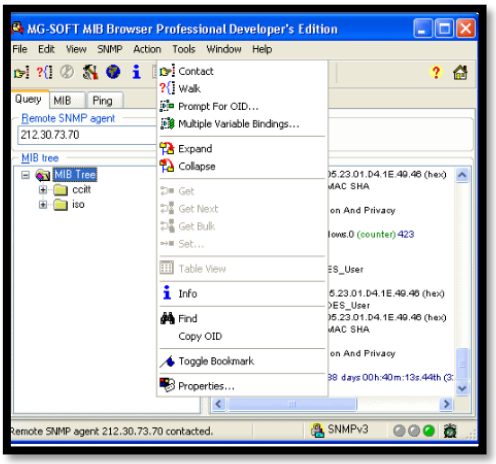



**Figura 2.11 MG-SOFT** (Mg-soft)

MIB Browser puede controlar varios dispositivos SNMP simultáneamente e incluye características como visor de SNMP Tabla, SNMP Tabla 'editor', capacidades de registro, presentación gráfica en tiempo real de los valores numéricos consultados, buscará MIB implementados en agentes, la comparación de las instantáneas del agente SNMP, la gestión de usuarios SNMPv3 USM en agentes SNMP remotos, etc.

[113] Simple Network Management Protocol

Ventana Seguimiento SNMP genérico muestra mensajes SNMP intercambiados entre MIB Browser y agentes SNMP. Mensajes SNMP se muestran en formato hexadecimal prima, así como en el formato decodificado, legible por humanos.

Por lo tanto, la ventana Seguimiento SNMP Genérico es particularmente útil para la depuración en el desarrollo de un agente SNMP y para resolver problemas cuando los agentes SNMP no responden adecuadamente a las consultas de MIB Browser. El adjunto del compilador MIB permite compilar cualquier proveedor archivo MIB específico. El archivo MIB compilado a continuación, puede ser cargado y utilizado por MIB Browser. Normalmente, los archivos MIB son suministrados por proveedores de dispositivos SNMP manejables, y contienen la descripción de la jerarquía de objetos manejables y atributos de los objetos en el dispositivo SNMP. En otras palabras, los archivos MIB sirven como una guía para la gestión de dicho dispositivo.

MG-SOFT MIB Browser Professional Edition está disponible para sistemas MS **Windows** operativo (Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2012, Windows 8), para los sistemas operativos **Linux** que se ejecutan en arquitecturas Intel x86 ( Red Hat, SuSE, Debian, Ubuntu, Mandriva ...), así como para Apple **Mac OS X** (binarios universales tanto para Intel x86 y plataformas PowerPC) y Sun **Solaris** (binarios disponibles para ambos, Sun Sparc y las plataformas Intel x86 ).

#### 2.14.2.2 OIDVIEW

OidView es un conjunto de herramientas modulares Análisis SNMP y MIB Browser para los entusiastas de gestión de red! A medida que surgen nuevas tecnologías ByteSphere produce nuevos módulos para su uso con OidView. La consola es el corazón de OidView, dando de control para el administrador en una variedad de maneras.

Administrar SNMP MIB Browser y sesiones de análisis, gráficas MIB Valores, PDU traza, la captura SNMP y MIB Compilar todo al toque de un botón.

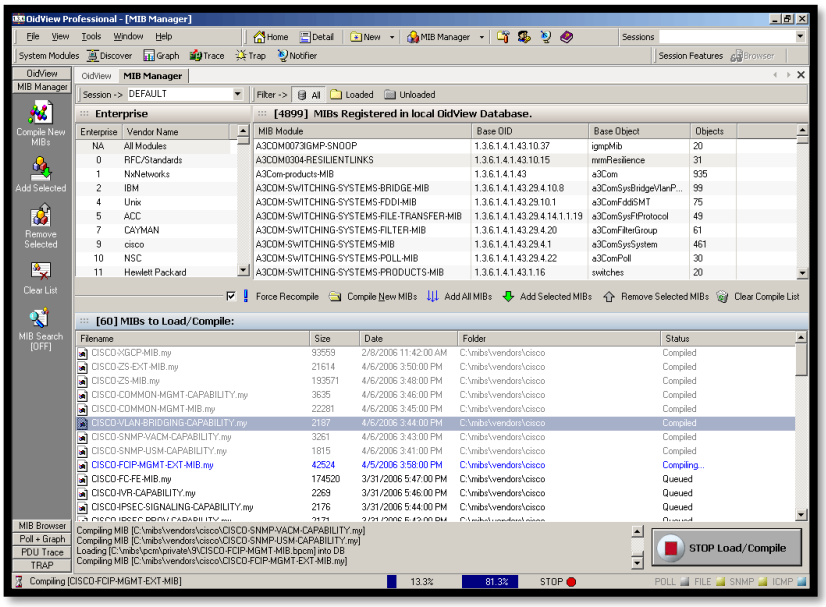



**Figura 2.12 OidView (OidView)**

Ofrece una amplia base de datos completamente únicos, MIB mano compilados por nuestro personal de apoyo que se han subido por los miembros de la comunidad a través de los años. Otros sitios pueden tener pretensión de tener más MIB pero contienen duplicado o de MIB fecha. Si usted encuentra una MIB duplicado o no actualizados por favor avísenos lo antes posible y / o no dude en enviar una versión actualizada. **Qué es una MIB.-** Una MIB[114] es un archivo de texto que se ha escrito utilizando el ASN. 1 (Notación de sintaxis abstracta) de formato. Este archivo de texto es legible, pero es especial, ya que puede ser compilado mediante un programa informático llamado compilador MIB, y luego dará lugar a la creación de objetos llamados identificadores de objetos (OID), que puede ser entendido por una estación de administración de red mediante el SNMP (Simple Network Management Protocol) método de comunicación. **¿Por qué es importante esto?** MIB de SNMP son cruciales para la gestión de la red y comprender los objetos subyacentes que están siendo recuperados de agentes SNMP.

[114] Management Information Base

### 2.14.2.3 SOFTPERFECT NETWORK SCANNER (Network Scanner)

SoftPerfect Network Scanner es una IP libre de multiproceso, SNMP[115] escáner con una interfaz moderna y muchas características avanzadas. Está dirigido a administradores de sistemas y usuarios en general interesados en la seguridad informática. El programa pings ordenadores, escáneres de puertos de escucha y muestra qué tipos de recursos se comparten en la red, incluyendo el sistema y los ocultos TCP / UDP.

Además, se puede montar carpetas compartidas como unidades de red, navegar por ellas utilizando el Explorador de Windows, filtrar la lista de resultados, y mucho más. SoftPerfect Network Scanner también puede comprobar si un puerto definido por el usuario, y que informe si uno está abierto. También puede resolver nombres de host y detectar automáticamente el rango de IP local y externa. Soporta el apagado remoto y Wake-On-LAN.

### 2.14.2.4 MANAGE ENGINE MIB BROWSER

SNMP MIB Browser es una completa herramienta para el seguimiento de los dispositivos habilitados para SNMP y servidores. Se pueden cargar, ver varios módulos MIB y realizar GET, GetNext y Set de SNMP. Esta herramienta es fácil de usar y le permite ver, configurar y analizar las capturas SNMP.

### 2.14.2.5. MIB BROWSER - Realizar GET SNMP, SNMP GET NEXT y SET Operación SNMP

Mib Browser le permite hacer operaciones de SNMP, como GET, GET NEXT y SET. También permite realizar operación GET A GRANEL para SNMP V2 y V3 versiones.

[115] Simple Network Management Protocol

- Compatible con SNMP v1, SNMP v2, SNMP v3
- SNMPv3 de seguridad tal como se define en USM (basado en usuarios modelo de seguridad) y VACM (Ver Control de acceso basado)
- Compatible con CFB-AES-128 junto con CBC-DES protocolo de privacidad
- Robusto y potente SMIv1/SMIv2 MIB parser
- Alerta al Operador / Administrador sobre el estado del dispositivo a través de e-mail

#### 2.14.2.6. SNMP TRAP RECEIVER

Trap Viewer ayuda a ver las trampas recibidos de los agentes SNMP. Se escucha a uno o más puertos a la vez y la trampa puede ser enviada desde cualquier host. Trap Viewer también puede mostrar mensajes INFORM.

Analizador de trampa SNMP se utiliza para configurar y analizar los acontecimientos trampa. Trampas contienen información críptico no es fácilmente comprensible para los usuarios, por lo analizadores trampa traducen o analizar trampas en, información significativa comprensible.

#### 2.14.2.7. **POWER SNMP MANAGER** (Power Manager)

Un software gratuito, con todas las funciones SNMP Administrador aplicación construida usando PowerSNMP de. NET. Descubra máquinas de la red, ver los árboles MIB, y analizar las solicitudes de red. Perfecto para las tareas de gestión de peso ligero ha moderado.

**Características**

- Fácil de usar, arrastrar y soltar interfaz simple
- Ping y supervisar máquinas de la red
- Vigilar las capturas SNMP
- Variables de consulta y ver SNMP versión 1, 2 y 3
- Genera notificaciones automáticas por correo electrónico cuando las variables se salen del rango
- Construido con robustos PowerSNMP de Dart para los componentes. NET

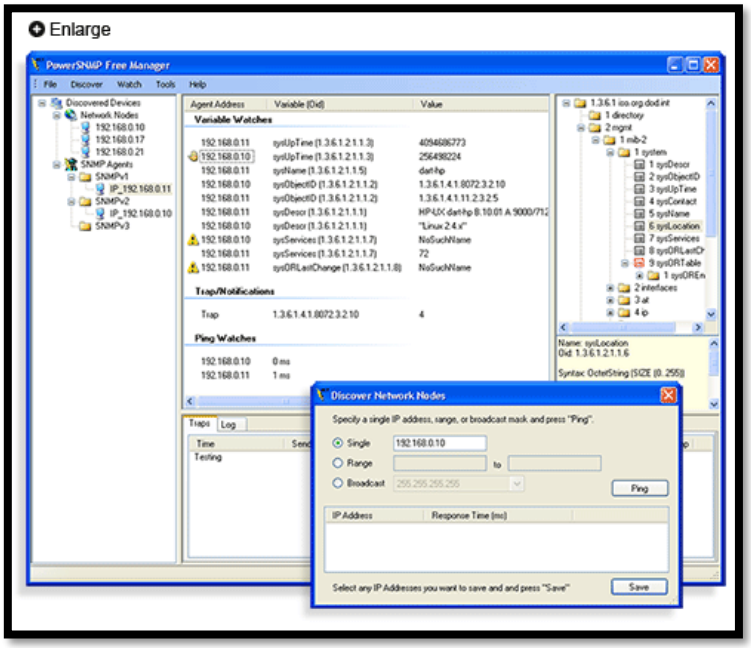



**Figura 2.13 Power SNMP Mananger** (Power Manager)

**2.14.2.8. SNMPSOURCE MIBVIEWER** (Power Manager)

**Un software de operación integral MIB para gestionar la red.**

Se trata de un visor Mib SNMP, un software de operación mib integral para la empresa para gestionar su red. Mib Viewer usuario da métodos muy flexibles para ver los archivos MIB, recuperar valores oid. Además, este software puede compilar los archivos MIB luego fusionarse para una vista de árbol.

**Aquí están algunas características clave de "SnmpSource MibViewer":**

· Cargar y analizar varios archivos MIB.

· Ver mib en vista combinada y vistas formato de archivo.

· Soporte SNMP v1, v2c protocolos V3.

· Soporte MIB vistas de tabla.

· Apoyar las vistas gráficas MIB.

· Monitorear vistas trampa.

· Soporta SNMP GET, SNMP Getnext, Set de SNMP, SNMP Walk, comandos SNMP[116]

GetBulk

· Ver los datos PDU binarios.

## 2.15. REALIZACIÓN DE SOFTWARE (Microsoft)

### 2.15.1 DISEÑO DE SOFTWARE PARA ENVIÓ DE SMS VÍA MODEN GPRS

Visual Studio 2010 es una de las versiones más recientes de esta herramienta, acompañada por .NET Framework 4.0. La fecha del lanzamiento de la versión final fue el 12 de abril de 2010.

Hasta ahora, uno de los mayores logros de la versión 2010 de Visual Studio ha sido el de incluir las herramientas para desarrollo de aplicaciones para Windows 7.

[116] Simple Network Management Protocol

Entre sus más destacables características, se encuentran la capacidad para utilizar múltiples monitores, así como la posibilidad de desacoplar las ventanas de su sitio original y acoplarlas en otros sitios de la interfaz de trabajo.

Existen varias versiones de Visual Studio como son:

**Visual Studio 2010 Ultimate**: Conjunto completo de herramientas de gestión del ciclo de vida de una aplicación para los equipos que garantizan unos resultados de calidad, desde el diseño hasta la implementación. Ya sea creando nuevas soluciones o mejorando las aplicaciones existentes, Visual Studio 2010 Ultimate le permite llevar sus ideas a la vida en un número creciente de plataformas y tecnologías - incluyendo la nube y la computación paralela.

**Visual Studio 2010 Premium**: Un conjunto de herramientas completo que simplifica el desarrollo de aplicaciones para personas o equipos que entregan aplicaciones escalables de alta calidad. Que este escribiendo codigo de aplicaciones o de bases de datos, creando bases de datos, o quitando los errores, puede aumentar su productividad usando herramientas poderosas que funcionan de la manera que usted trabaja.

**Visual Studio 2010 Professional**: La herramienta esencial para las personas que realizan tareas de desarrollo básico. Visual Studio 2010 Professional simplifica la compilación, la depuración y el despliegue de las aplicaciones en una variedad de plataformas incluyendo SharePoint y la Nube. También viene con el soporte integrado para el desarrollo con pruebas y con las herramientas de depuración que ayudan a garantizar unas soluciones de alta calidad.

## 2.15.2 DISEÑO DE LA VENTA PRINCIPAL DE SOFTWARE

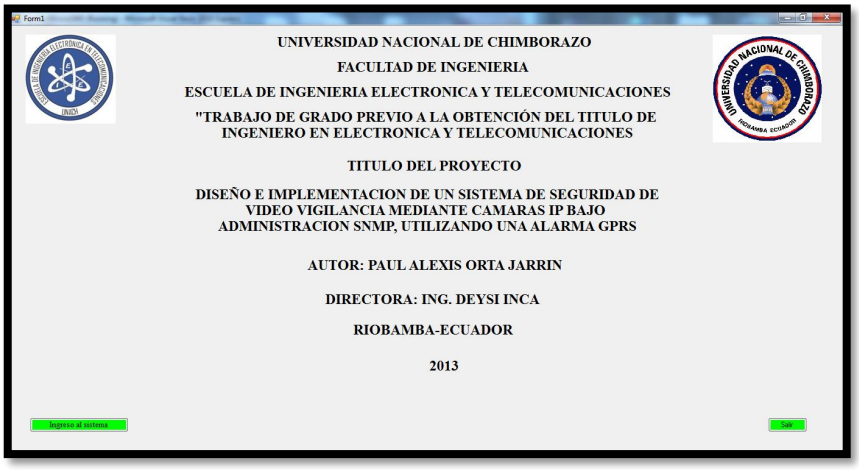



**Figura 2.14. Ventana Principal**

**Elaborado por: Paul Orta**

En la figura 2.12. nos representa el acceso al software diseñado el cual consta con estructuras representativas en donde podemos observar la autoría del programa realizado, a más de eso nos encontramos con dos botones principales que son:

### 2.15.2.1 BOTÓN INGRESO AL SISTEMA.

Fue programado para poder tener acceso al sistema de envió de mensaje SMS por medio de una interfaz gráfica que nos permitirá configurar los parámetros principales de moden GPRS, número de celular y mensaje a ser enviado en caso de existir una falla en el sistema de video vigilancia.

### 2.15.2.2. BOTÓN SALIR.

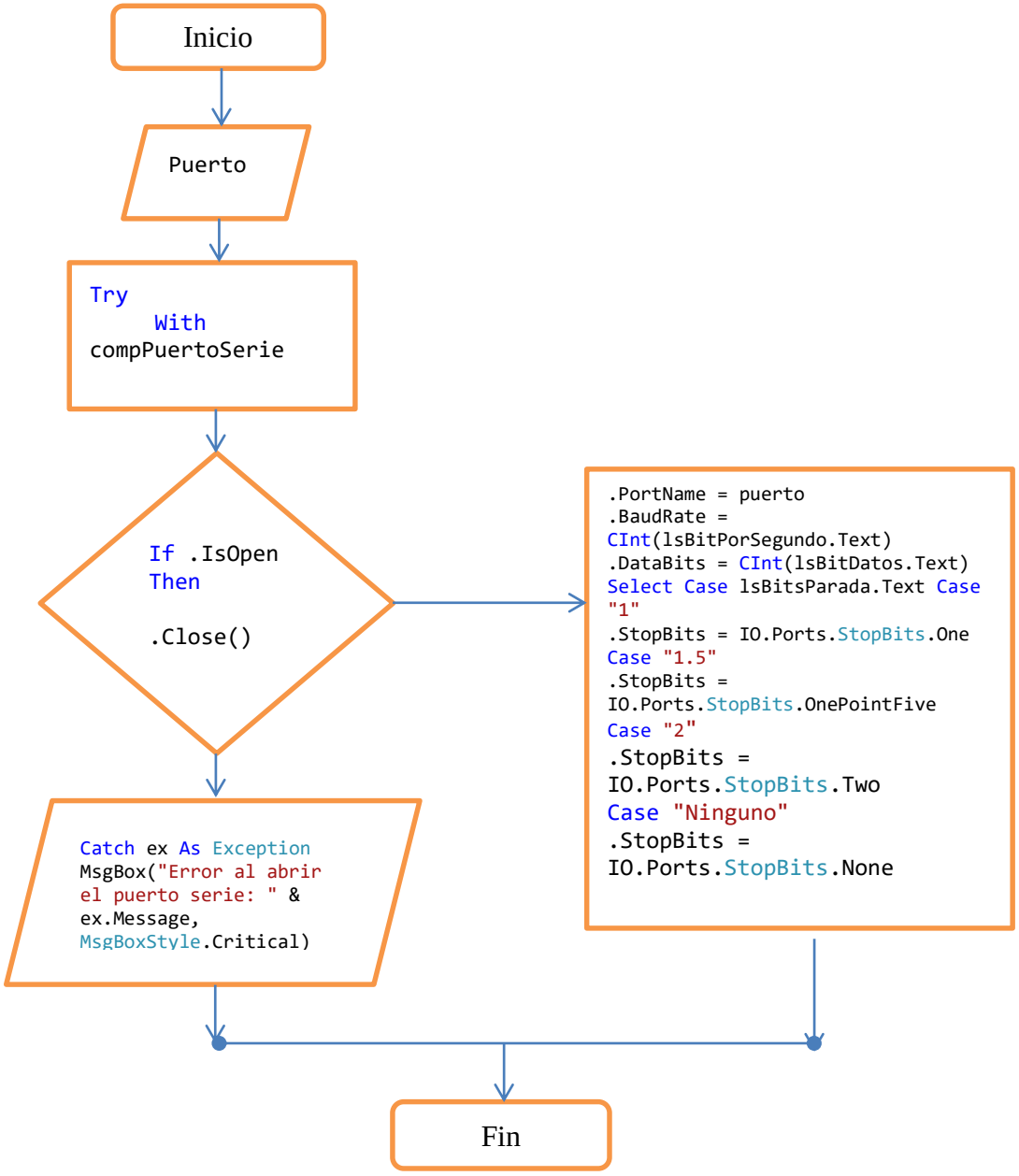
Fue programado para salir del programa por completo en caso de no conocer el usuario y contraseña.

### 2.15.3 DISEÑO DE INTERFAZ MODEM GPRS

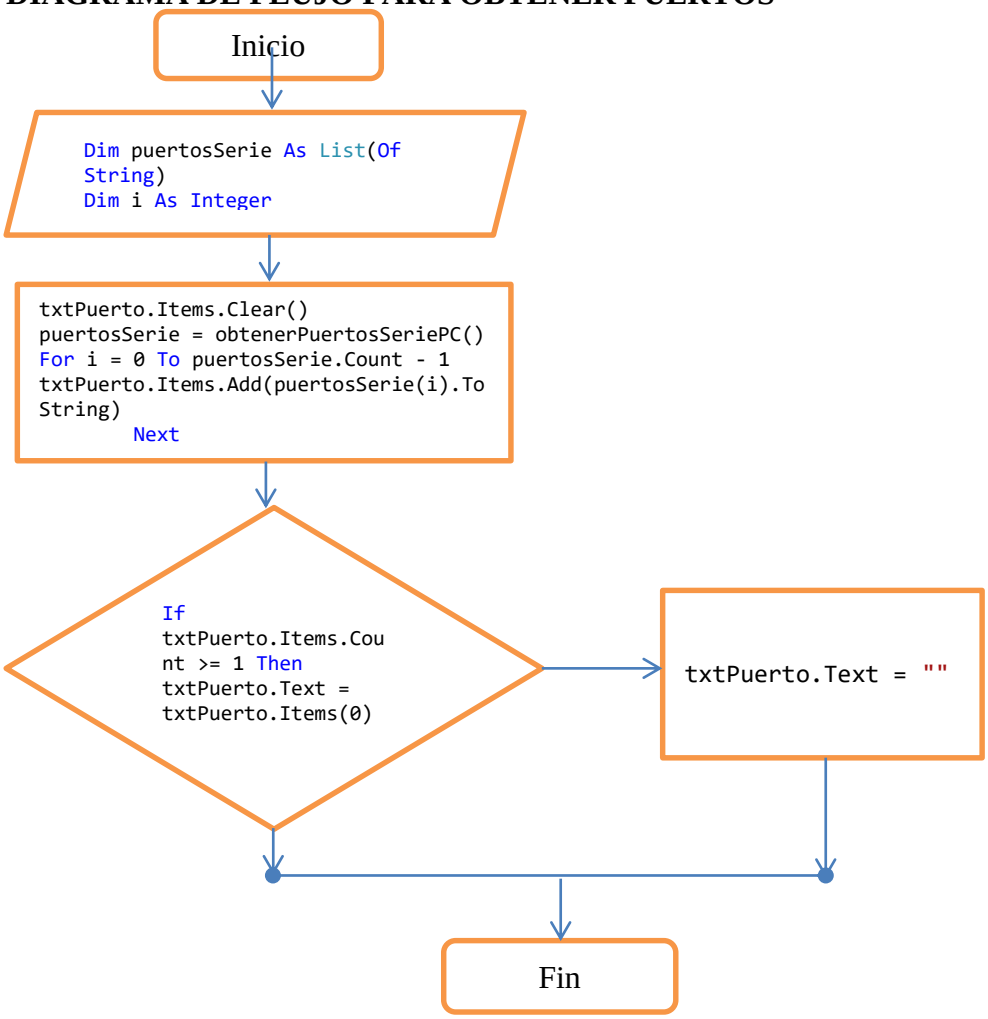
En esta sección utilizamos varias investigaciones en las cuales utilizamos comandos AT para poder realizar la conexión de modem GPRS y VB2010

Para la realización de dicho software utilizamos varios complementos como es la interfaz entre VB2010 y el moden GPRS, para guiarnos hemos realizado algunos diagramas de flujo.

### a) DIAGRAMAS DE FLUJO PARA ABRIR EL PUERTO



**b) DIAGRAMA DE FLUJO PARA OBTENER PUERTOS**




Para activar en modo SMS en dispositivo GSM:

- compPuertoSerie.Write("AT+CMGF=1" & Chr(13))

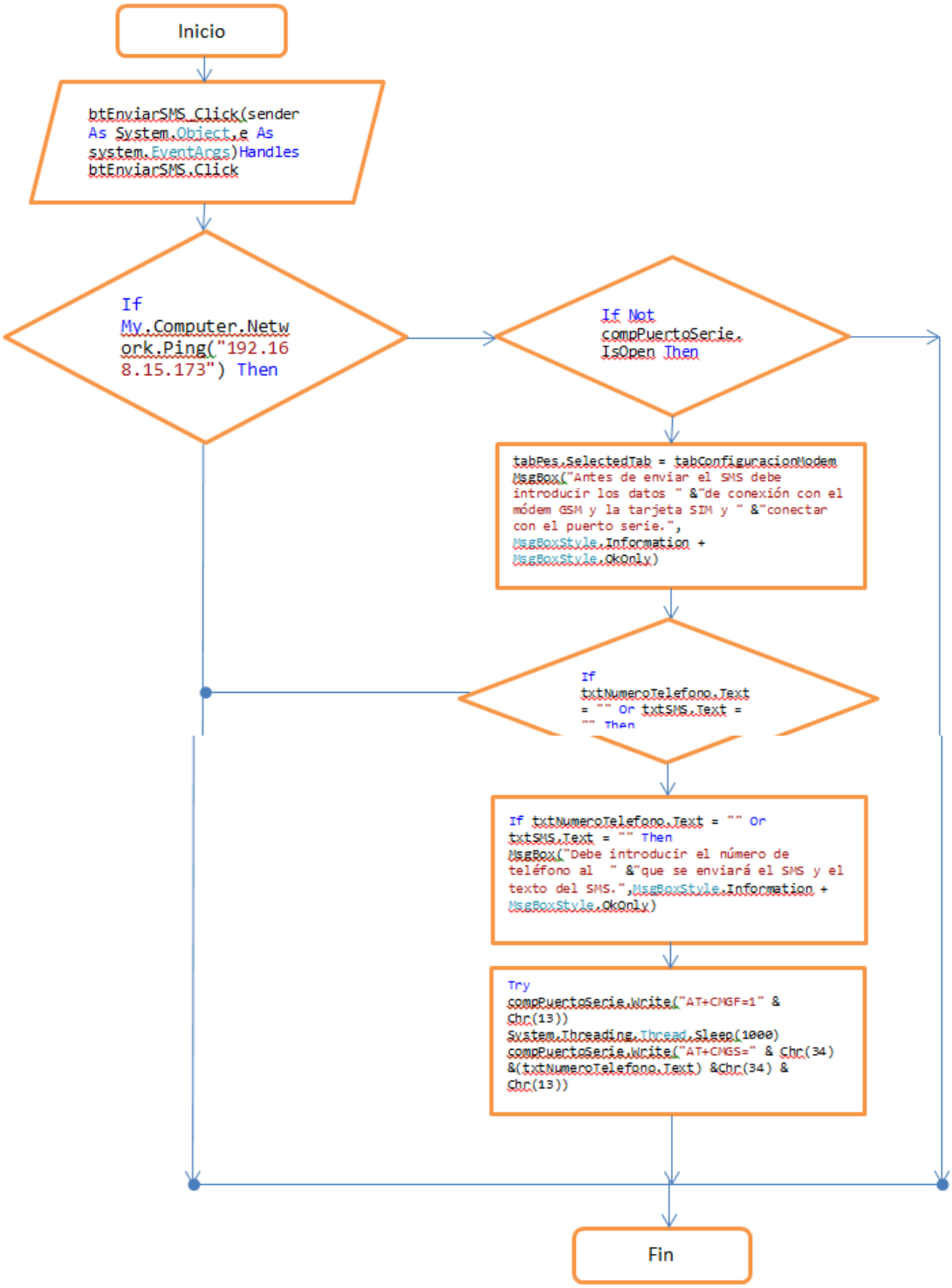
Para establecer número de teléfono de destino del SM:S

- compPuertoSerie.Write("AT+CMGS=" & Chr(34) & (txtNumeroTelefono.Text) & Chr(34) & Chr(13))

Para poder enviar el SMS a dispositivo GSM se utiliza los comandos:

- compPuertoSerie.Write(txtSMS.Text & Chr(26))

## c) DIAGRAMA DE FLUJO PARA ENVIO DE SMS



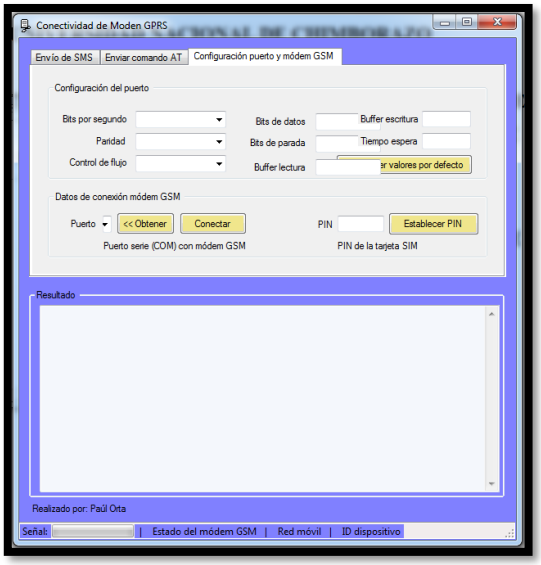



**Figura 2.15. Interfaz de Conexión Modem GPRS y VB2010**

**Elaborado por:** Paul Orta

### 2.15.3.1 CONSULTAS AT DEL DISPOSITIVO. (Bluehack)

Se desarrolló una sub interfaz en la cual podemos realizar consultas del dispositivo conectado como son:

- Imei
- Modelos del Dispositivo
- Contactos Telefónicos.
- Operadoras
- Numero IMSI (internacional)
- Estado de la tarjeta SIM


**Figura 2.16. Consultas de estado del dispositivo GPRS**
**Elaborado por:** Paul Orta

Para poder visualizar el IMEI[117] del dispositivo se utiliza el comando **AT+CGSN**

**AT+CGMI: [Request Manufacturer Identification]**

- Petición de identificación del Fabricante (Marca del teléfono).
- Sintaxis: AT+CGMM | <fabricante>
- Respuesta: ZTE Corporation

**AT+CGMM: [Request Model Identification]**

- Petición de identificación del modelo de teléfono.
- Sintaxis: AT+CGMM | <modelo>
- Respuesta: MF100

**AT+CGSN: [Request Product Serial Number Identification]**

- Petición de identicación del número de serie del producto.
- Sintaxis: AT+CGSN | <IMEI>
- Respuesta: 358517038731114

[117] International Mobile Equiptment Identity

**AT+CSQ: [Signal Quality]**

- Devuelve el estado de calidad de la señal de cobertura.
- Sintaxis: AT+CSQ | +CSQ: <rssi>,<ber>

  <rssi> = 0 indica -113 dBm o menos

  = 1 indica -111 dBm

  = 2..30 indica -109..-53 dBm

  = 31 indica -51dBm o más

  = 99 indica desconocido

  <ber> = 99 indica porcentaje desconocido
- Respuesta: +CSQ: 13,99

# CAPITULO III

## 3. RESULTADOS

Efectuado la metodología para cada aspecto que comprende la investigación, como es el diseño y la implementación del sistema de video vigilancia con cámaras ip, generando el trabajo de campo recopilando la información requerida para cada actividad, efectuado el trabajo de oficina procesando información y clasificando. Para una adecuada interpretación.

### 3.1 ANÁLISIS DE LOS RESULTADOS

La Unidad Educativa “San Miguel” requiere implementar un sistema de video vigilancia IP para monitorear la seguridad de sus instalaciones y controlar las actividades ocurridas en las zonas de trabajo, manteniendo un registro y un respaldo de los eventos durante las 24 horas del día.

La seguridad actual de las instalaciones de la Unidad Educativa está sustentada en la capacidad del personal que labora diariamente en las instalaciones, encontrándose limitada por el factor humano debido a la posibilidad reducida de cubrir y vigilar a todas las zonas en las que puede ocurrir varios problemas, los robos, además considerando que por las noches la visibilidad es muy reducida generando puntos ciegos para vigilar las instalaciones de esta manera se genera la posibilidad de alguna intrusión de personas ajenas a las instalaciones es constante.

En caso de alguna intrusión va a ser difícil identificar a estas personas sobre todo si la intrusión se la realizó durante la noche, también será difícil saber la zona por la cual ingresaron los individuos, para lo cual se analizarán e investigaran los puntos vulnerables a robos para realizar el sistema de seguridad.

## 3.2 ESTADO ACTUAL

La Unidad Educativa "San Miguel" de la ciudad de San Miguel de Bolívar, se encuentra ubicada al Centro de la ciudad de San Miguel de Bolívar.
Todos los empleados laboran de lunes viernes en horarios de 07h00 a 13:00 y de 14h00 a 16h00.

## 3.3 ENCUESTA

La siguiente encuesta se la realizo a los docentes que laboran diariamente en las instalaciones de la Unidad Educativa "San Miguel".

**OBJETIVO:** Obtener información esencial para diseñar el sistema de video vigilancia.
Instructivo:

- Lea detenidamente cada pregunta.
- Seleccione una de las alternativas.
- Responda con absoluta imparcialidad.

**Pregunta 1.- ¿Cree usted que la tecnología de video vigilancia IP aplicada a las empresas y negocios, son sistemas de seguridad necesarios para incrementar la seguridad?**

a) Totalmente de acuerdo
b) Neutral
c) En desacuerdo

| Detalle | Frecuencia | Porcentaje |
|---|---|---|
| Totalmente de acuerdo | 24 | 80% |
| Neutral | 6 | 20% |
| En desacuerdo | 0 | 0% |
| **Total** | **30** | **100%** |

**Tabla 3.1 Importancia de sistema de video vigilancia en la empresa.**
**Elaboración: Paúl Orta**

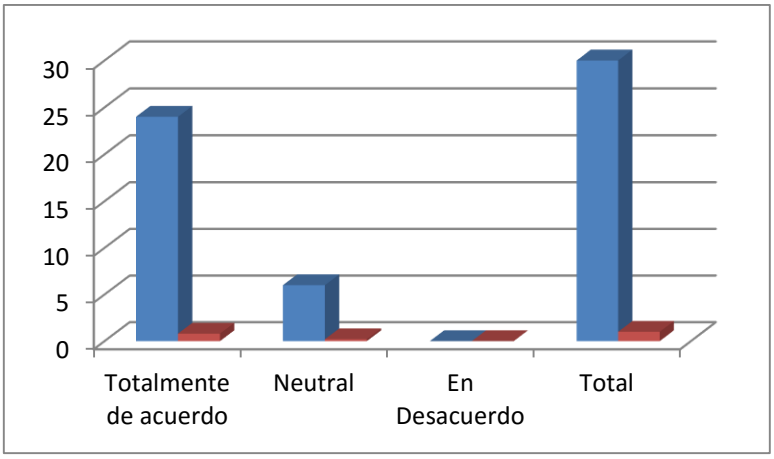



**Figura 3.1 Importancia de sistema de video vigilancia en la Unidad Educativa "San Miguel"**

**Elaboración: Paúl Orta**

**Análisis e Interpretación:**

En la tabla 3.1 el 80% de los Docentes encuestados afirman que están totalmente de acuerdo que los sistemas de video vigilancia son necesarios para incrementar la seguridad en la Unidad educativa, el 20% expresa una posición neutral.

Debido a que actualmente en la Unidad educativa no existe un sistema de seguridad inteligente la integridad y la seguridad de las instalaciones se encuentran en constante riesgo, razón por la cual la mayor cantidad de personas están de acuerdo en implementar el sistema.

**Pregunta 2: ¿Debería invertir el Municipio de San Miguel en sistemas de seguridad electrónicas?**

| DETALLE | FRECUENCIA | PORCENTAJE |
|---|---|---|
| **SI** | 280 | 70 |
| **NO** | 94 | 23,5 |
| **NULO** | 26 | 6,5 |

**Tabla 3.2 Sistema Electrónicos**
**Elaboración: Paúl Orta**

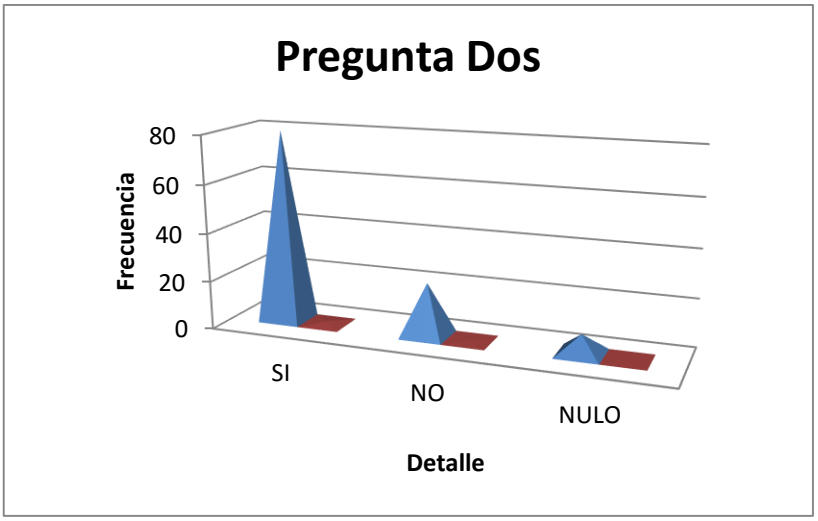



**Figura 3.2 Sistema de Seguridad**
**Elaboración: Paúl Orta**

**Análisis e Interpretación:**

En la segunda pregunta tenemos según la tabla 3.2 que el 70% de los encuestados respondieron (SI), el 23.5% (NO) y un 6.5% anulo la pregunta.

La mayor parte de las personas encuestadas está muy de acuerdo con un sistema de este tipo ya que el beneficio no sería solamente para la seguridad de los moradores sino también para las personas que nos visitan haciéndolas sentirse más seguras, lo cual crea una buena imagen para el sector turístico del cantón.

**Pregunta 3: ¿Está de acuerdo con que se implemente un plan de seguridad?**

| DETALLE | # PERSONAS | PORCENTAJE |
|---|---|---|
| **SI** | 100 | 100 |
| **NO** | 0 | 0 |
| **NULO** | 0 | 0 |

**Tabla 3.3 Plan de Seguridad**
**Elaboración: Paúl Orta**

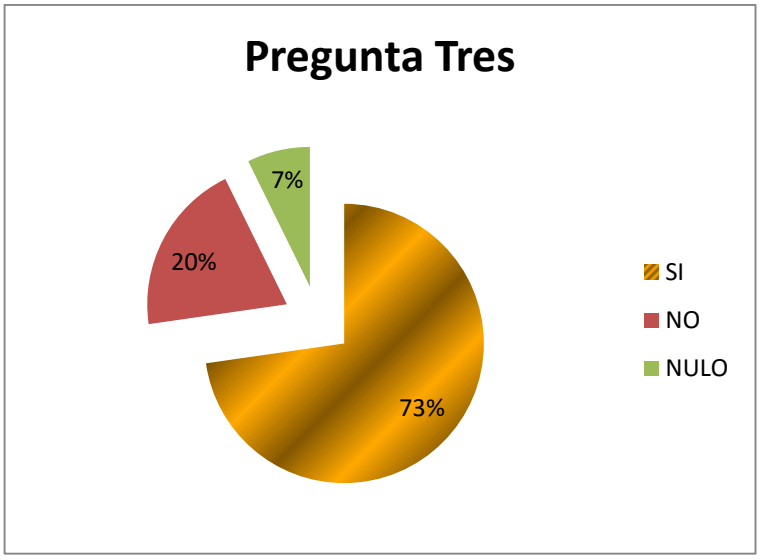



**Figura 3.3 Plan de Seguridad**

**Elaboración: Paúl Orta**

**Análisis e Interpretación:**

En la primera pregunta de la tabla 3.3. nos indica que el 100% de los encuestados respondieron (SI), el 0% (NO) y un 0% anulo la pregunta.

En esta pregunta todas las personas estuvieron de acuerdo en que se debería implementar un plan de seguridad.

**Pregunta 4: ¿Cree que es necesario instalar un Sistema de Cámaras, para ayudar a reducir los niveles delictivos en la ciudad?**

| DETALLE | # PERSONAS | PORCENTAJE |
|---|---|---|
| **SI** | 80 | 72,73% |
| **NO** | 22 | 20% |
| **NULO** | 8 | 7,27% |

**Tabla 3.4 Instalación de Sistema de Seguridad**

**Elaboración: Paúl Orta**

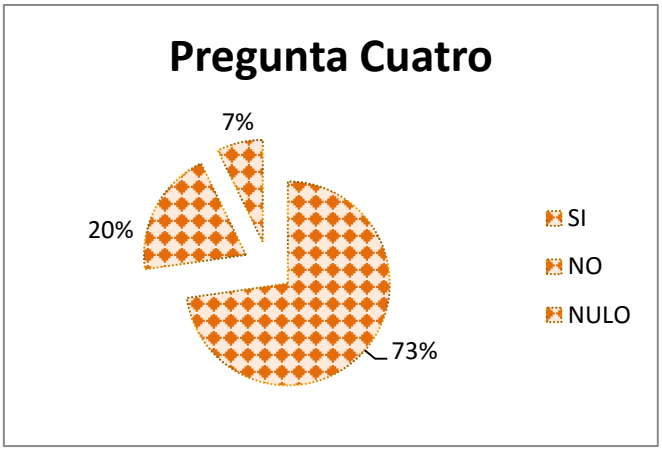



**Figura 3.4 Instalación de Sistema de Seguridad**

**Elaboración: Paúl Orta**

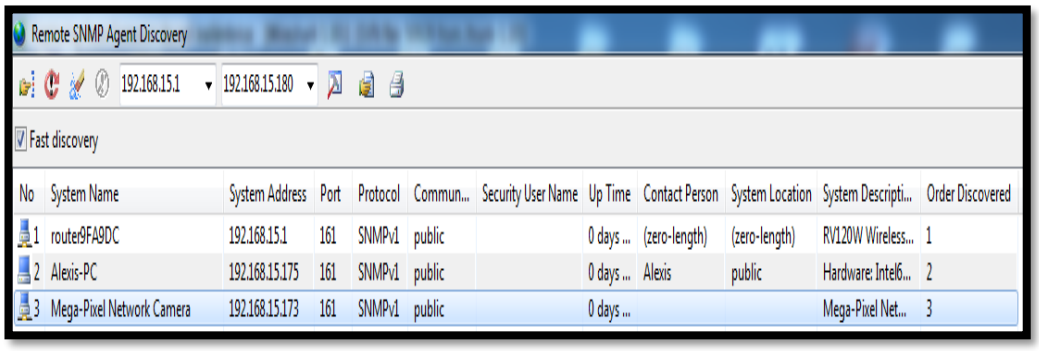
**Análisis e Interpretación:**

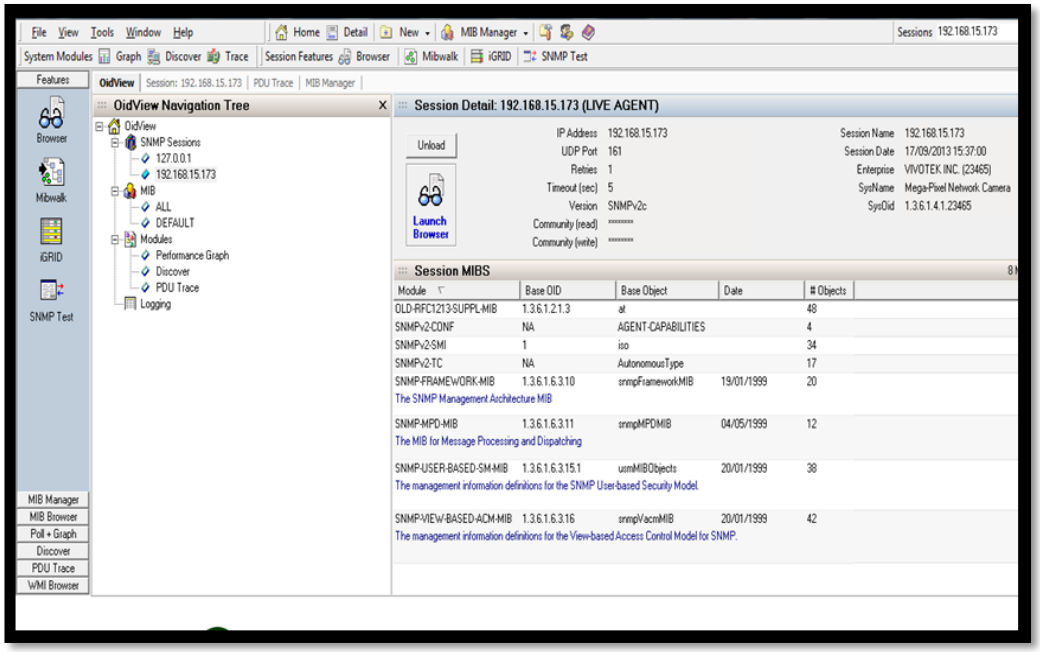
Según la encuesta realizada en la tabla 3.4 nos indica que el 73% de los encuestados respondieron (SI), el 20% (NO) y un 7,27% anulo la pregunta.

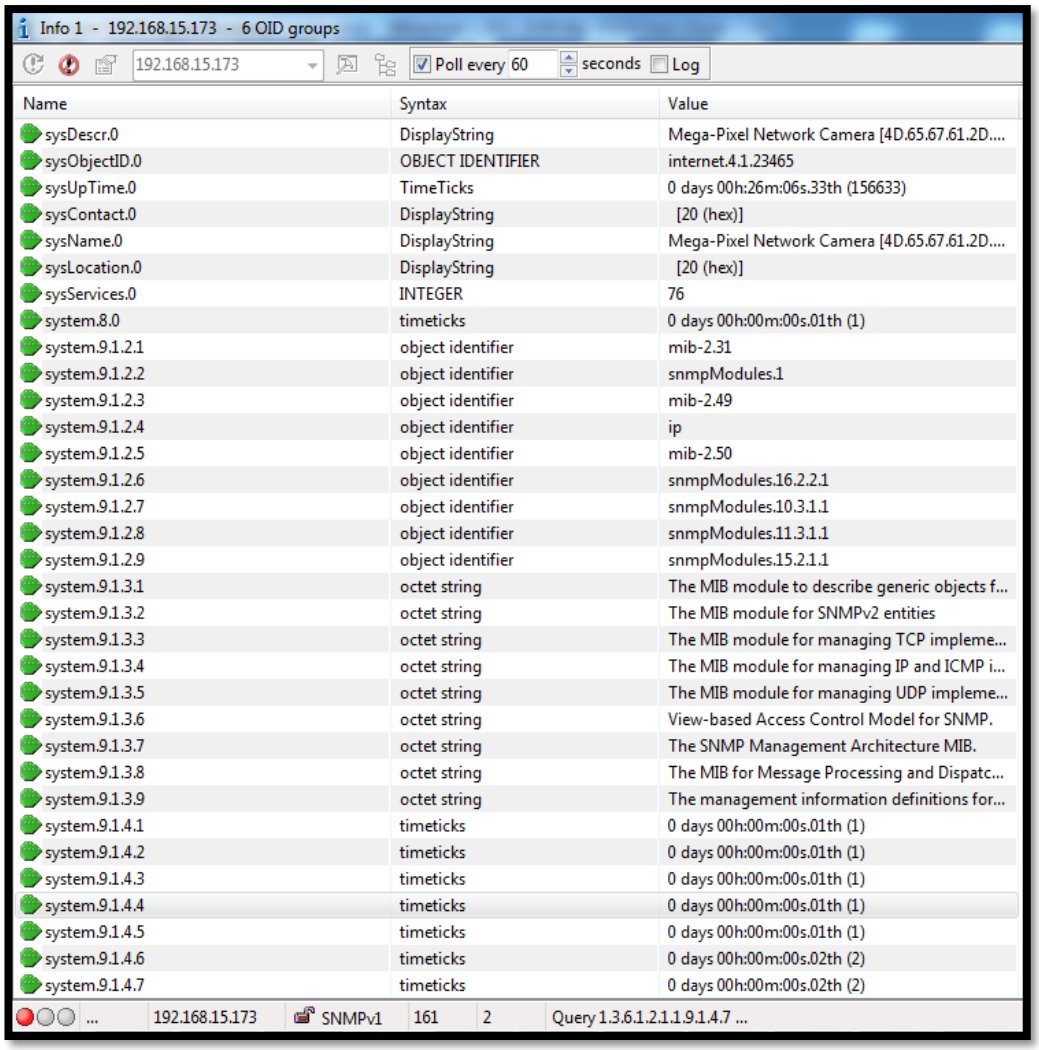
Los moradores del cantón han sido testigos de cómo malhechores cometen sus actos delictivos y recobran su libertad debido a la falta de pruebas o la falta de una intervención rápida de parte de la Policía Nacional.

## 3.4. MONITOREO SNMP Y COMPARACIÓN CON LOS PROGRAMAS PERTINENTES.

### 3.4.1 REMOTE SNMP AGENT DISCOVERY




File View Tools Window Help
Home Detail New MIB Manager
System Modules Graph Discover Trace
Session Features Browser Mibwalk iGRID SNMP Test
Sessions 192.168.15.173
Features
Browser
Mibwalk
iGRID
SNMP Test
OidView Navigation Tree
OidView
SNMP Sessions
127.0.0.1
192.168.15.173
MIB
ALL
DEFAULT
Modules
Performance Graph
Discover
PDU Trace
Logging
Session Detail: 192.168.15.173 (LIVE AGENT)
Unload
Launch Browser
IP Address 192.168.15.173
UDP Port 161
Retries 1
Timeout (sec) 5
Version SNMPv2c
Community (read)
Community (write)
Session Name 192.168.15.173
Session Date 17/09/2013 15:37:00
Enterprise VIVOTEK INC. (23465)
SysName Mega-Pixel Network Camera
SysOid 1.3.6.1.4.1.23465
Session MIBS
Module
Base OID
Base Object
Date
# Objects
OLD-RFC1213-SUPPL-MIB 1.3.6.1.2.1.3 at 48
SNMPv2-CONF NA AGENT-CAPABILITIES 4
SNMPv2-SMI 1 iso 34
SNMPv2-TC NA AutonomousType 17
SNMP-FRAMEWORK-MIB 1.3.6.1.6.3.10 snmpFrameworkMIB 19/01/1999 20
The SNMP Management Architecture MIB
SNMP-MPD-MIB 1.3.6.1.6.3.11 snmpMPDMIB 04/05/1999 12
The MIB for Message Processing and Dispatching
SNMP-USER-BASED-SM-MIB 1.3.6.1.6.3.15.1 usmMIBObjects 20/01/1999 38
The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB 1.3.6.1.6.3.16 snmpVacmMIB 20/01/1999 42
The management information definitions for the View-based Access Control Model for SNMP.
MIB Manager
MIB Browser
Poll + Graph
Discover
PDU Trace
WMI Browser


Info 1 - 192.168.15.173 - 6 OID groups
192.168.15.173
Poll every 60 seconds Log
Name
Syntax
Value
sysDescr.0 DisplayString Mega-Pixel Network Camera [4D.65.67.61.2D....
sysObjectID.0 OBJECT IDENTIFIER internet.4.1.23465
sysUpTime.0 TimeTicks 0 days 00h:26m:06s.33th (156633)
sysContact.0 DisplayString [20 (hex)]
sysName.0 DisplayString Mega-Pixel Network Camera [4D.65.67.61.2D....
sysLocation.0 DisplayString [20 (hex)]
sysServices.0 INTEGER 76
system.8.0 timeticks 0 days 00h:00m:00s.01th (1)
system.9.1.2.1 object identifier mib-2.31
system.9.1.2.2 object identifier snmpModules.1
system.9.1.2.3 object identifier mib-2.49
system.9.1.2.4 object identifier ip
system.9.1.2.5 object identifier mib-2.50
system.9.1.2.6 object identifier snmpModules.16.2.2.1
system.9.1.2.7 object identifier snmpModules.10.3.1.1
system.9.1.2.8 object identifier snmpModules.11.3.1.1
system.9.1.2.9 object identifier snmpModules.15.2.1.1
system.9.1.3.1 octet string The MIB module to describe generic objects f...
system.9.1.3.2 octet string The MIB module for SNMPv2 entities
system.9.1.3.3 octet string The MIB module for managing TCP impleme...
system.9.1.3.4 octet string The MIB module for managing IP and ICMP i...
system.9.1.3.5 octet string The MIB module for managing UDP impleme...
system.9.1.3.6 octet string View-based Access Control Model for SNMP.
system.9.1.3.7 octet string The SNMP Management Architecture MIB.
system.9.1.3.8 octet string The MIB for Message Processing and Dispatc...
system.9.1.3.9 octet string The management information definitions for...
system.9.1.4.1 timeticks 0 days 00h:00m:00s.01th (1)
system.9.1.4.2 timeticks 0 days 00h:00m:00s.01th (1)
system.9.1.4.3 timeticks 0 days 00h:00m:00s.01th (1)
system.9.1.4.4 timeticks 0 days 00h:00m:00s.01th (1)
system.9.1.4.5 timeticks 0 days 00h:00m:00s.01th (1)
system.9.1.4.6 timeticks 0 days 00h:00m:00s.02th (2)
system.9.1.4.7 timeticks 0 days 00h:00m:00s.02th (2)
... 192.168.15.173 SNMPv1 161 2 Query 1.3.6.1.2.1.1.9.1.4.7 ...

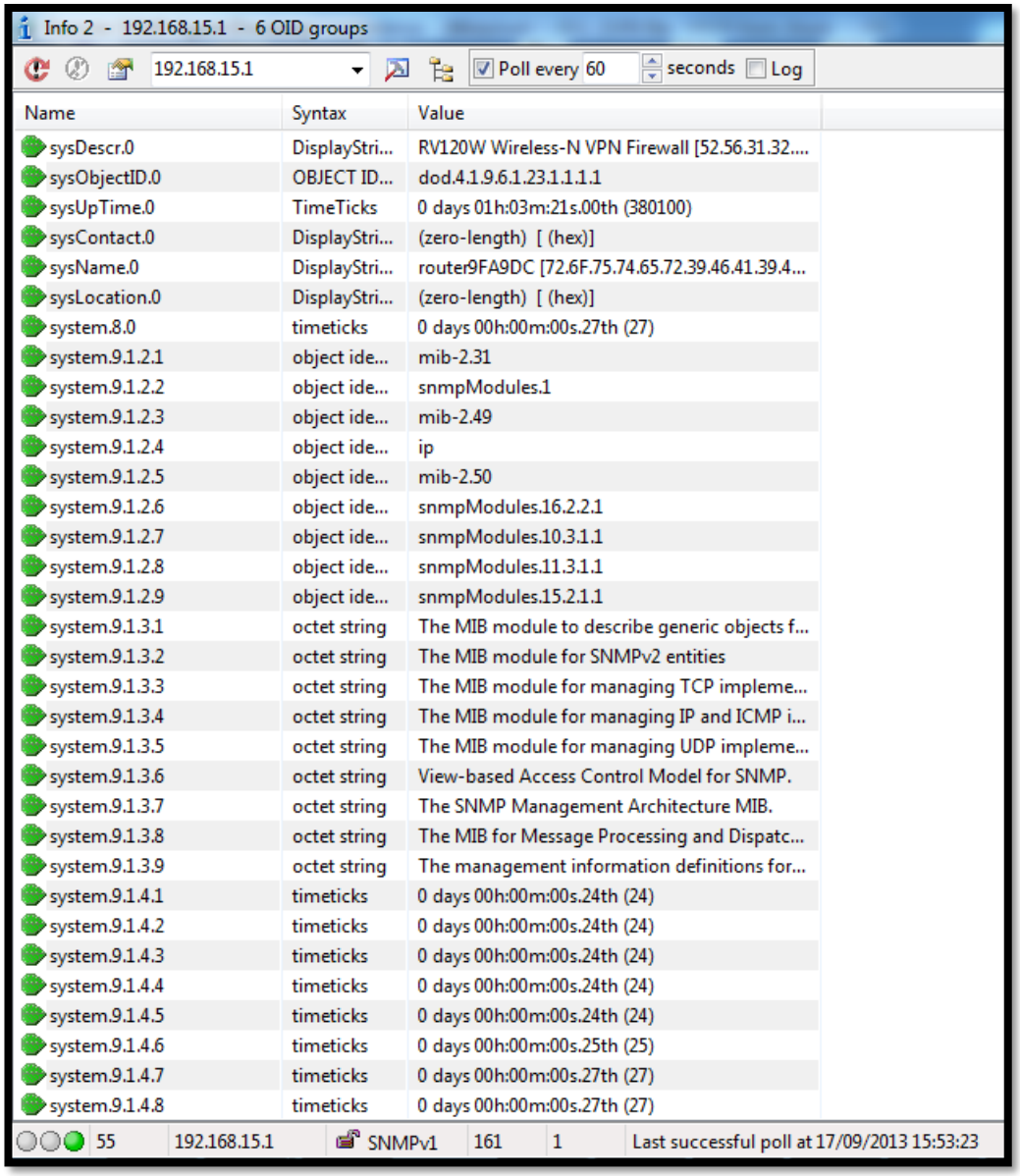
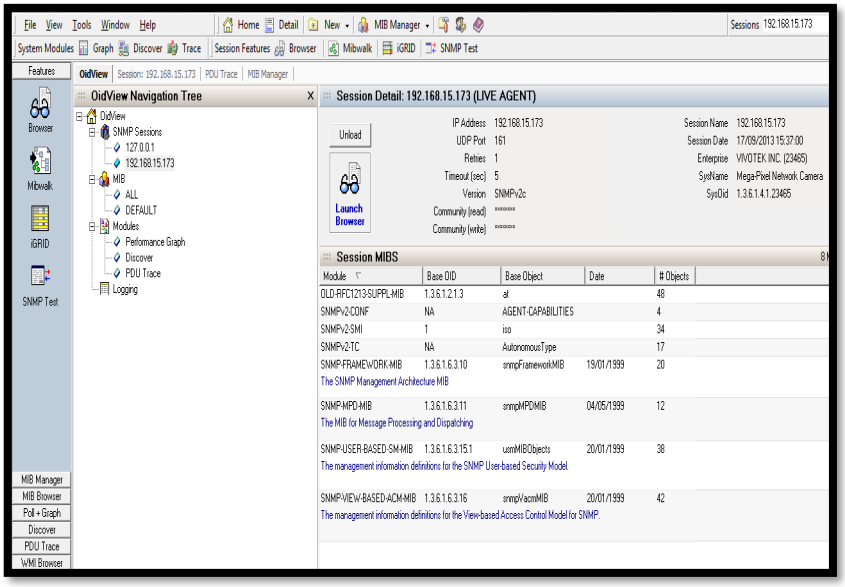



**Figura 3.5. OID Grupos**
**Elaboración: Paúl Orta**

En la fig. 3.5 por medios del programa remote snmp agent discovery nos muestra todos los identificadores OID del router cisco dentro del grupo system la cual nos ayuda a monitorear los dispositivos conectados dentro de la red, como son nombres, ubicación y descripción del equipo tanto en hardware y software.

### 3.4.2 OIDVIEW




Wireshark capturando los get- response, getBulkrequest

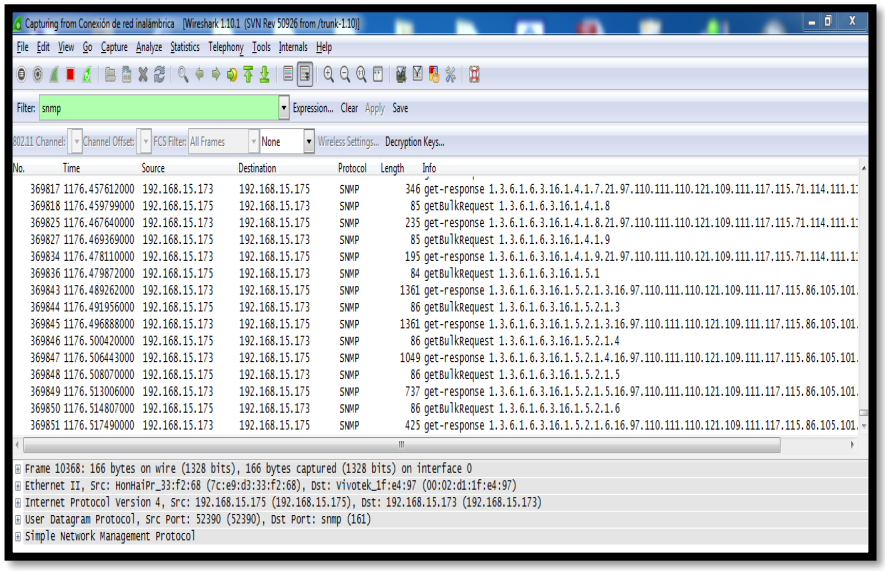
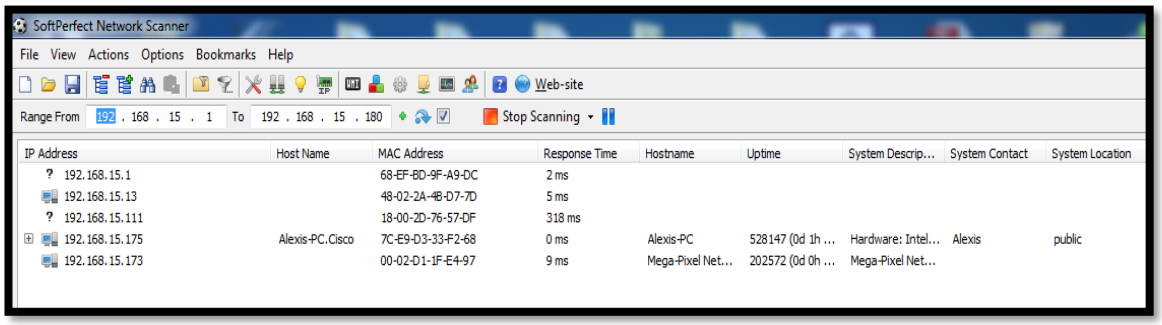


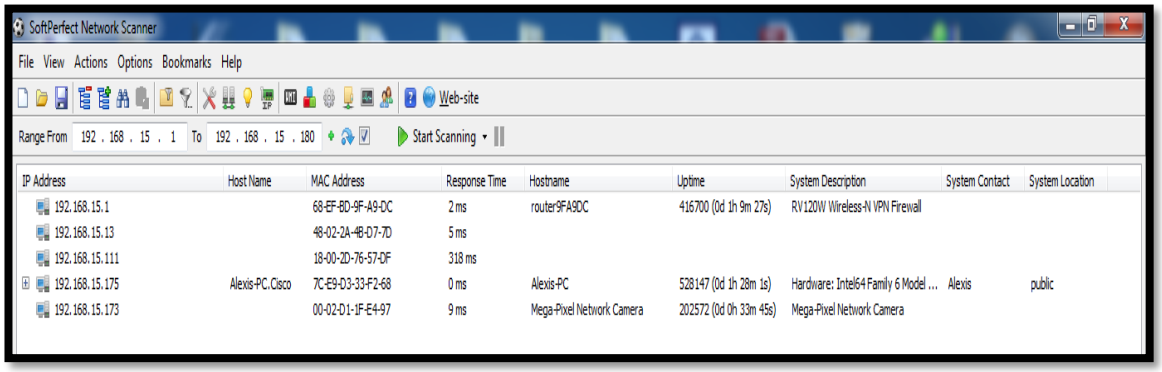

**Figura 3.6. Paquetes Capturados por Wireshark desde cámara Vivotek**

**Elaboración: Paúl Orta**

En la fig. 3.6 nos muestra todos los paquetes enviados hacia la cámara vivotek a través de red lan.

### 3.4.3. SOFTPERFECT NETWORK SACANNER

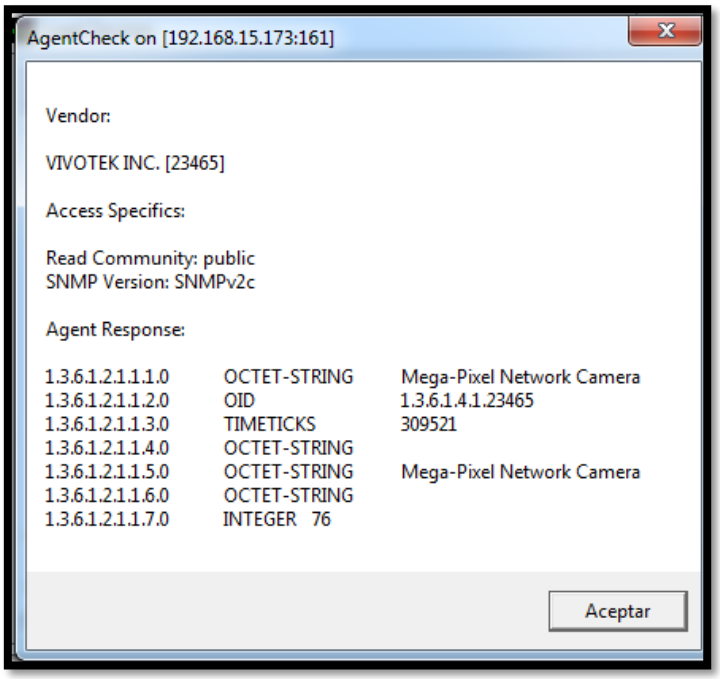



**Elaboración: Paúl Orta**

Por medio de este programa hemos encontrado todos los dispositivos conectados en la red.

### 3.4.4. OIDViEW VIVOTEK



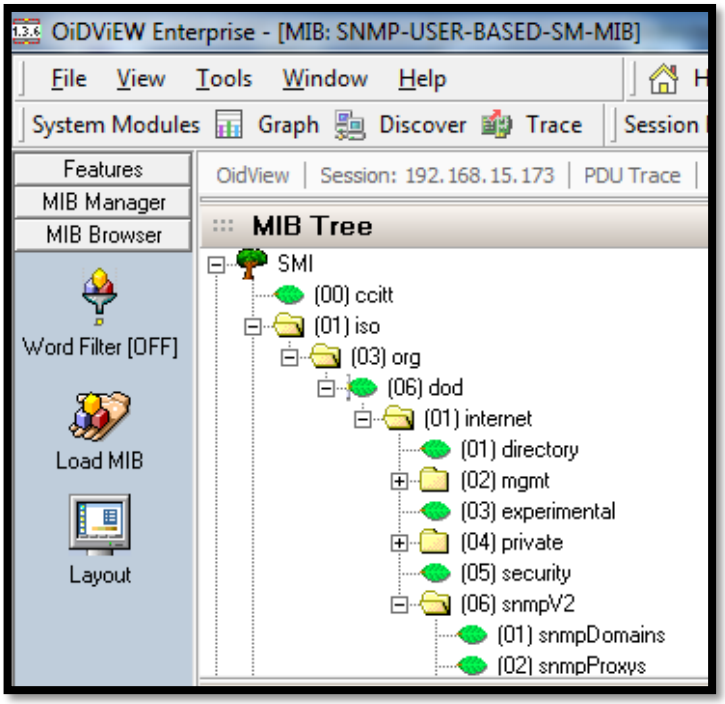
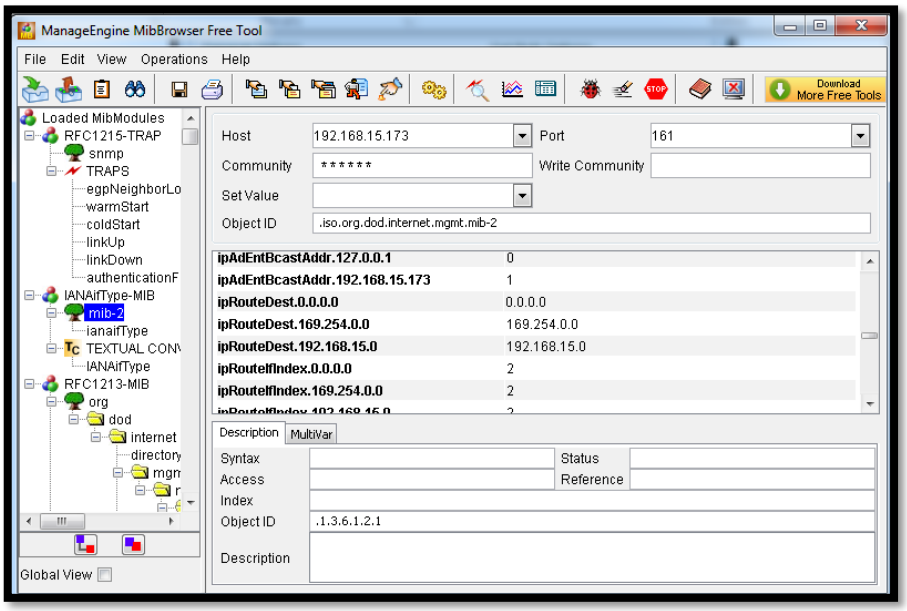



**Figura 3.7: Árbol Mib Vivotek FD 8136**
**Elaboración: Paúl Orta**

En la fig. 3.7 con la ayuda del programa oidview nos muestra parte del árbol mib de la cámara ip vivotek fd8136

### 3.4.5. MANAGEENGINE MibBrowser



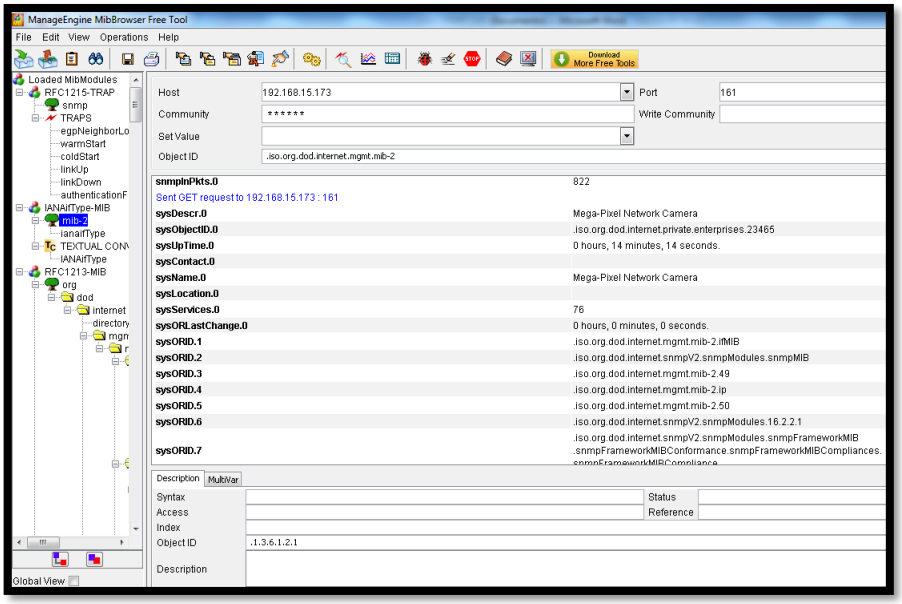
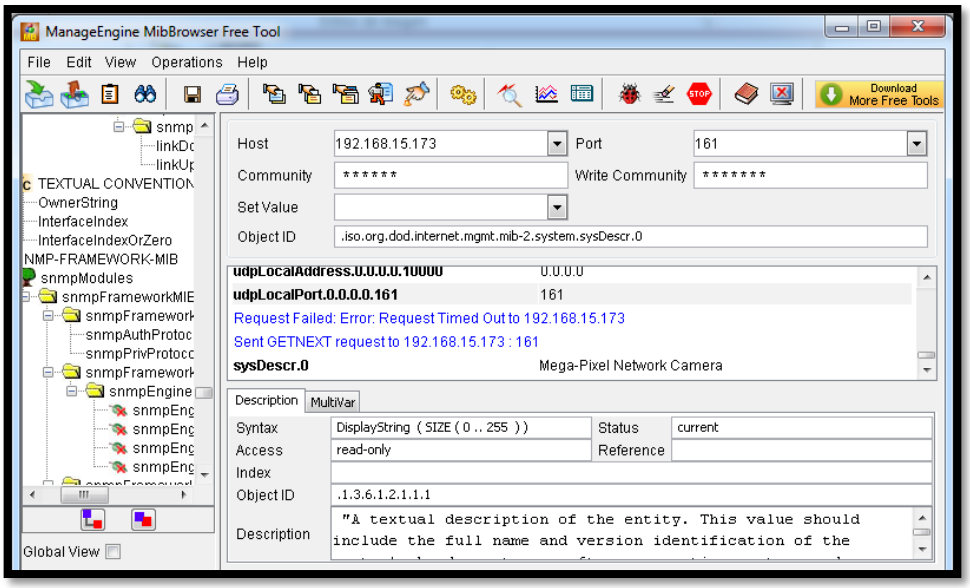



**Figura 3.8: Árbol mib del grupo system de la Cámara IP Vivotek**
**Elaboración: Paúl Orta**

En la fig. 3.8 por medio del programa manage engine mib browser enviamos un get con el identificador system el cual nos devuelve la información de todos los parámetros dentro del grupo system.

Get next




En esta figura enviamos un get next el cual nos del vuelve la información única del grupo system con el OID .1.3.6.1.2.1.1.1 el cual pertenece a la descripción del dispositivo el cual es Mega-Pixel Network Camera.

Get bulk

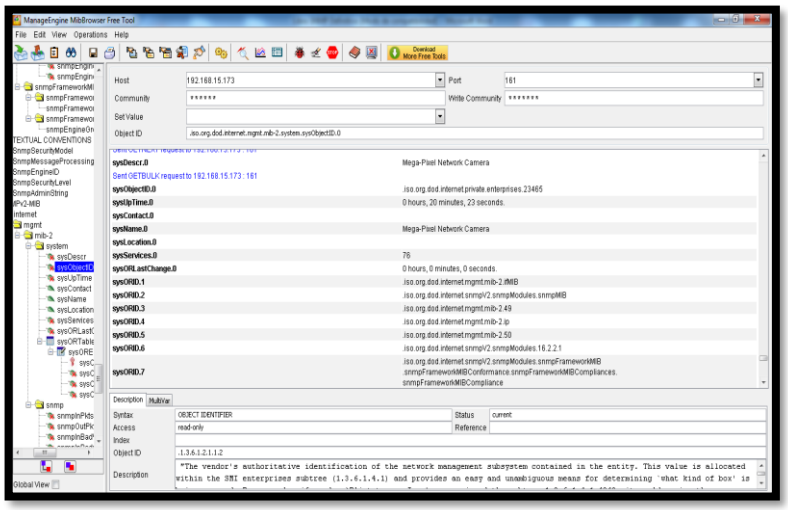


**Figura 3.9. Get bulk enviadas**
**Elaboración: Paúl Orta**

En la fig. 3.9 enviamos un get bulk con el OID .1.3.6.1.2.1.1.2 perteneciente a la identificación del dispositivo el cual nos devuelve la información de todos los OID apartir del OID identificador en adelante.

### 3.4.6. MG-SOFT Mib Browser

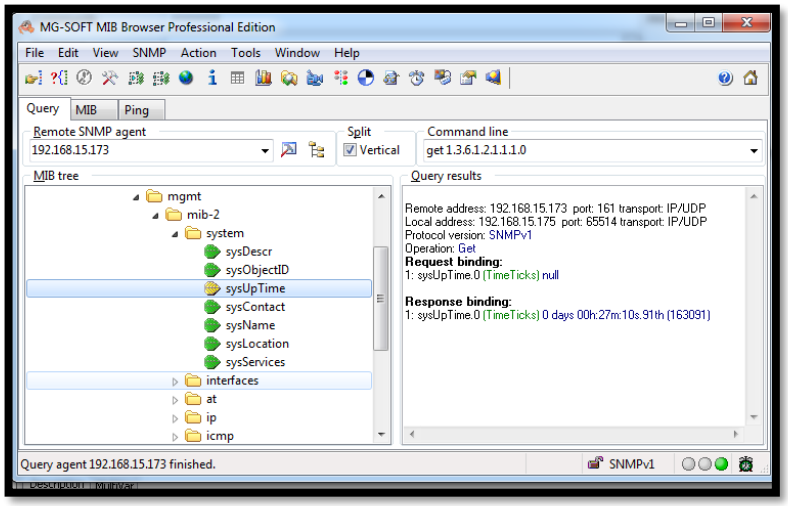



**Figura 3.10. Árbol mib y envió Get**
**Elaboración: Paúl Orta**

En la fig. 3.10 con la ayuda del software mg-soft mib browser en viamos un get con un OID 1.3.6.1.2.1.1.1.0 perteneciente a un system up time el cual nos indica el tiempo en uso del dispositivo.

**Capturando paquetes snmp enviado hacia la cámara IP Vivotek**

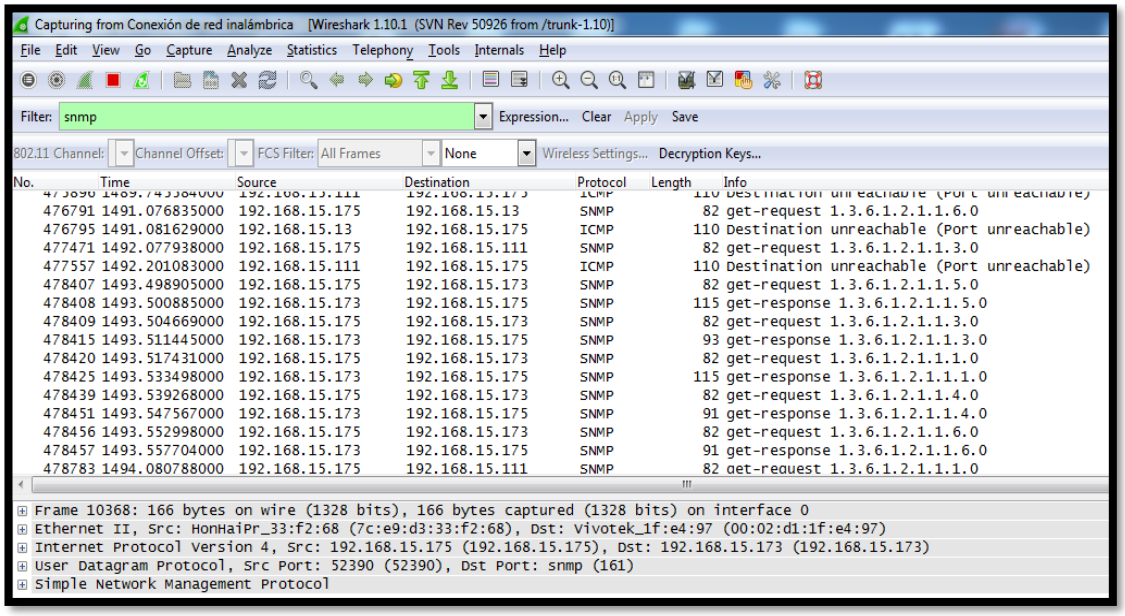



**Figura 3.11. Captura de paquetes SNMP**

**Elaboración: Paúl Orta**

En la fig. 3.11 nos muestra la captura de todo el tráfico de la red enviado al dispositivo de la cámara vivotek por medio de los distintos software de gestión snmp.

# CAPÍTULO IV

## 4. DISCUSIÓN

Prosiguiendo con el análisis se citó una guía con los programas de gestión de red como son los:

- MG-SOFT Mib Browser
- OidView
- SoftPerfect Network Scanner
- Manage Engine Mib Browser
- Power SNMP Manager
- SnmpSource MibViewer

En los cuales nos ayuda a entender de mejor forma cada árbol mib de los dispositivos a administrarles por medio de snmp sea en la V1, V2c y V3 las cuales cada una tienes sus ventajas y desventajas como por ejemplo en la versión 3 se tiene mayor seguridad en las cuales nos pide un usuario y contraseña que por medio de snmp el primer paso antes de enviar la trampa realiza una verificación y autenticación del equipo con él envió por medio del software.

Además existen varios programas similares como, Router-Stats, escrito por Iain Lea, el autor del famoso programa lector de correo. Router-Stats actualiza los gráficos una vez al día y muestra información estadística muy interesante sobre la utilización por horas y otros aspectos, pero el problema es que se apoya con muchos programas externos.

Hay otra categoría de software que da un paso más allá en la tarea de gestión de redes, ofreciendo una solución completa tanto para monitorizar como para configurar toda la red. Este tipo de solución permite obtener una compleja representación gráfica de la red y ojear fácilmente los nodos que la componen, verificando detalles de configuración específicos y otras cuestiones de interés. Pero la desventaja fundamental es que sus costos son elevados ya que este protocolo se utiliza para empresas o instituciones en las cuales manejen varias

redes o subredes como universidades de gran extensión, instituciones públicas y privadas que necesiten mayores seguridades y monitoreo de sus redes como: Bancos, Cooperativas, instituciones de seguridades de estado, etc.

Otra de las causas principales que no utilizan la administración es debido a que sus equipos son robustos es decir en tecnología por ende se utiliza en rede wan donde necesitan saber si un dispositivo esta con falla y en donde se encuentra para poder determinar su solución inmediata.

De acuerdo con la implementación del sistema realzado en la Unidad Educativa San Miguel se ha encontrado con rangos de visibilidad de acuerdo a la ubicación de las cámaras del tipo 1 y del tipo 2 que se efectuó el análisis por tipos de dispositivos.

# CAPÍTULO V

# 5. CONCLUSIONES Y RECOMENDACIONES

## 5.1 CONCLUSIONES

- Al realizar el análisis de las diferentes tecnologías para Sistemas de Video Vigilancia se puedo establecer que la mejor alternativa para un Sistema de Seguridad para la Unidad Educativa, es un sistema digital con transmisión sobre IP, que permite mayor escalabilidad y convergencia a futuro de diferentes servicios tales como de voz sobre IP o redes de datos.
- La Tecnología IP permite hoy en día ventajas como: la gestión centralizada de todas las cámaras del sistema de seguridad desde cualquier PC en cualquier parte del mundo y la interacción remota con todo el sistema en tiempo real.
- Los dispositivos que trabajan con IP utilizan estándares abiertos por lo que no precisan trabajar con equipos de la misma marca. Esto permite la elección de dispositivos de distintos proveedores según la función y costos.
- De esto se puede concluir que el uso de estándares abiertos favorece a la competencia y reduce costos.
- En el diseño la utilización de POE[118] permite un ahorro de costos en fuentes de alimentación y cableado. Además, POE permite tener un diseño más amigable con el medio evitando dañar estéticamente al ambiente natural de la institución.
- Los sistemas digitales hacen posible el uso de formatos de compresión que disminuyen los requerimientos de ancho de banda, tanto para la transmisión como para el almacenamiento, sin disminuir la calidad de la señal.
- Se analizó que la aplicación de video vigilancia requiere un alto recurso de la red, mientras mayor es el número de cámaras en el sistema; de ello se puede concluir que para el diseño de un sistema de video vigilancia se debe realizar un apropiado dimensionamiento del ancho de banda.

[118] Power over Ethernet

- Con respecto a la mibs de snmp para los distintos dispositivos no se encuentran con facilidad para lo cual es necesario la utilización de software especiales para la búsqueda de las mibs
- Las mibs para las cámaras Vivotek son de clase b es decir son mib b y no como las mib de os dispositivos como son de cisco que son mib c.
- Cuando vemos la necesidad de crear una mib por intermedio de la IANA es un proceso muy demorado debido a que en primer lugar solo lo realizan los fabricantes de los dispositivos que tienen con soporte de snmp, en segundo plano una vez solicitado a la IANA tiene un periodo de aproximadamente un año en darnos nuestro requerimiento.

## 5.2 RECOMENDACIONES

De la experiencia adquirida al desarrollar este trabajo se puede extraer las siguientes recomendaciones:

- Se deberá efectuar el monitoreo del sistema de seguridad de video vigilancia en periodos cortos de tiempo, en cuanto estas estén con un nivel de severidad apropiado para efectuarse una reparación, evitando que el sistema entre en un estado severo provocando daños en los dispositivos y así disminuir el periodo de diseño.
- Para el dimensionamiento del ancho de banda de red se recomienda siempre sobredimensionar la red tomando en consideración futuras ampliaciones y aumento de equipos.
- Se recomienda implementar políticas de seguridad para acceso a la información almacenada, claves, niveles de acceso y administración.
- Se recomienda realizar limpieza periódica de los equipos sobre todo de las cámaras exteriores debido a que las condiciones ambientales pueden afectar el correcto funcionamiento todo el sistema.
- Antes de efectuar un mantenimiento se deberá realizar un análisis apropiado utilizando un entendido en sistemas de seguridades para poder determinar la falla existente.

- Durante la reparación del sistema de video vigilancia deberá existir personal autorizado por la institución o encargado del mantenimiento de la red.
- Es muy importante tomar muy en cuenta que una administración con SNMP se lo realiza con frecuencia en redes WAN debido a los dispositivos de gama alta con tecnología superiores a las Cámaras Ip u otros dispositivos que se utilizarán como usuario final por consiguiente es recomendable realizar pruebas o ejercicios con dispositivos de capa 3 o capa 2.

# CAPÍTULO VI

## 6. PROPUESTA

### 6.1 TÍTULO DE LA PROPUESTA

Implementación de un Sistema de Seguridad de Video Vigilancia mediante Cámaras Ip, utilizando una Alarma GPRS.

### 6.2 INTRODUCCIÓN.

El problema de la inseguridad ciudadana constituye una constante preocupación debido a que en los últimos meses se ha considerado el progresivo aumento de delitos de mayor connotación en el Cantón de San Miguel tales como asaltos, robos, ubicados en el centro de la ciudad y sus alrededores; se hace necesario e indispensable la utilización de video cámaras de vigilancia, ubicadas en puntos estratégicos del casco central de la ciudad para combatir a la inseguridad.

La iniciativa nace de la notoria preocupación de los moradores del cantón, y distintas autoridades que han visto este grave problema y con el propósito de entregar mejores niveles de seguridad en el sector céntrico y educativo.

Se ha visto la necesidad de un sistema de video vigilancia, que en coordinación con la Policía Nacional se lograr controlar y reducir el riesgo de este mal que ha ido progresando últimamente, lo cual ayudaría al control del constante crecimiento de la ciudad, así como también en el libre desempeño de entidades públicas y privadas. El sistema que vigilara diariamente actos que se realicen fuera de la ley como robos, asaltos, etc.

Todo este sistema estará bajo la responsabilidad de un funcionario delegado, quien contara con personal capacitado en el área de seguridad y video vigilancia, que además contara complementariamente con los equipos necesarios para lograr la operatividad del sistema.

Se necesita de medidas efectivas e inmediatas que hay que realizar para entregar a los habitantes la seguridad ciudadana que tanto lo necesitan, sean estos nacionales o extranjeros.

## 6.3 OBJETIVOS.

### 6.3.1 OBJETIVO GENERAL.

- Implementar y Realizar un estudio para la Implementación de un Sistema de Seguridad de Video Vigilancia mediante Cámaras Ip en lugares estratégicos.

### 6.3.2 OBJETIVOS ESPECÍFICOS.

- Efectuar varias visitas a la Unidad educativa y analizar intuitivamente en lugares estratégicos para una futura ampliación del sistema realizado.
- Clasificar e identificar los puntos estratégicos observados a fin de analizar el comportamiento de los estudiantes y docentes.

## 6.4 FUNDAMENTACIÓN CIENTÍFICO - TÉCNICA.

La Unidad Educativa está ubicada en el sector centro del cantón San Miguel provincia de Bolívar.

La Unidad Educativa al unir las regiones interandina y litoral, la provincia tiene un clima variado que va desde el frío de los páramos hasta el cálido de las zonas subtropicales con temperaturas entre 22 y 25 grados centígrados. El territorio es quebrado y montañoso, cruzando por la cordillera de Chimbo que viene desde la meseta occidental del Chimborazo a una altura de 4 mil metros. La zona occidental que se encuentra en las estribaciones de la cordillera es baja y goza de un clima subtropical.

## 6.5 DESCRIPCIÓN DE LA PROPUESTA.

### 6.5.1 ANÁLISIS DE LA INFORMACIÓN.

Antes de instalar cámaras Ip se debe reparar los lugares más vulnerables que tiene la institución, es importante identificar primero su ubicación y extensión, tipo de visión diurna y nocturna por lo cual se realizó varios recorridos por la institución educativa. Se deberá determinar si los lugares establecidos como vulnerabilidades son observadas que indican problemas estructurales actuales o futuros, considerando las condiciones actuales y las condiciones de carga anticipadas para el futuro.

Antes de especificar las reparaciones es necesario establecer las causas de la figuración. Se deberían revisar los planos, especificaciones y registros de construcción y mantenimiento.

Si estos documentos, junto con las observaciones recogidas con la institución, no proporcionan la información necesaria, antes de proceder con las reparaciones se debería efectuar una investigación y un análisis completo.

### 6.5.2 DETERMINACIÓN DE LA UBICACIÓN DE LAS CÁMARAS.

La ubicación de las cámaras, así como el estado general de la institución, esto se realizara mediante una observación directa.
Observación directa − Se realizara un registro de las ubicaciones, tipos y anchos de los lugares donde se necesitará tener una visión tanto en el día como en la noche. A demás a estos registros se pueden complementar con fotografías que documenten la condición de los lugares más propensos al ingreso de personas no autorizadas más aun en la noche, al momento de la investigación.

### 6.5.3 DESARROLLO EXPERIMENTAL:

Esta actividad agrupa las acciones necesarias para visualizar las posibles zonas huecas que se hayan encontrado en la institución.
Los materiales adecuados para la ejecución de esta actividad son: cámaras Ip vía wifi para poder analizar las zonas en toda la institución, un cuaderno para los apuntes necesarios para notificar a la institución.

### 6.6 ORGANIGRAMA ESTRUCTURAL

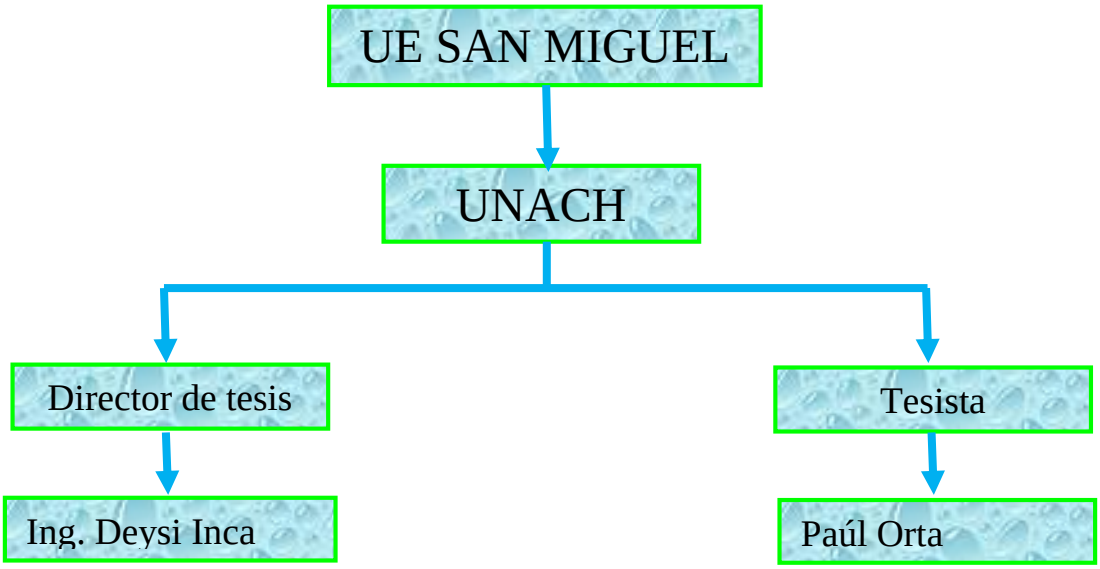



**Tabla 6.1. Organigrama Estructural de Desarrollo de la Propuesta.**

**Elaborado por:** Paúl Orta.

### 6.7 MONITOREO Y EVALUACIÓN DE LA PROPUESTA

**EL MONITOREO.-** Este se relaciona directamente con la gestión administrativa y consiste en un examen continuo o periódico que se efectúa durante la implementación del proyecto, en las etapas de inversión y/u operación.

El monitoreo emite juicios de valor, basados sobre todas las actividades programadas en las propuestas, planes o proyectos, especialmente, aquellas que se consideran esenciales, según la prioridad de cada instancia.

**LA EVALUACIÓN.-** Nos Permitirá tomar decisiones a través de la comparación de distintas alternativas. En los diferentes proyectos, en general, sean estos sociales o productivos, públicos o privados, se requiere de la evaluación para adoptar decisiones racionales.

La evaluación es la última fase del proceso de planificación, la cual consiste en la comparación de los resultados con los objetivos propuestos en la propuesta. En este sentido, la evaluación constituye una herramienta de gestión que permite tomar decisiones al proveer información acerca del grado de cumplimiento de los objetivos de la propuesta, los desvíos en el cumplimiento de los objetivos y sus causas, así como los principales problemas y cuellos de botella que requieren atención.

Los productos de este proceso son los informes de evaluación de la propuesta, los cuales se deben elaborar trimestral y semestralmente a partir de los informes de monitoreo.
Para su estudio de investigación se obtuvo y se procesó la información, luego se analizó la información necesaria tanto de campo como de oficina. Todo esto nos da como resultado una evaluación no destructiva real de la Unidad Educativa “San Miguel”, tipos de lugares denominados huecos predominantes en la Institución, y sus respectivos procesos de reparación adecuada en los casos de haberlos.

Se realizó la evaluación mediante los siguientes pasos:

1. Encuestas realizadas a los docentes y estudiantes.
2. Realización de inspección visual de las instalaciones.
3. Clasificación de los posibles lugares de ubicación de cámaras ip.
4. Soluciones adecuadas.

   Encuestas realizadas.

**Figura 6.1. Encuesta realizada al Rector de la institución.**

**Elaborado por:** Paúl Orta.

**Figura 6.2. Encuestas realizadas.**

**Elaborado por:** Paúl Orta.

Inspección visual.

**Figura 6.3. Inspección Visual**

**Elaborado por:** Paúl Orta.

**Figura 6.4. Inspección Visual**

**Elaborado por:** Paúl Orta.

Clasificación de los posibles lugares de ubicación de cámaras Ip.

**Figura 6.5. Clasificación de lugares.**

**Elaborado por:** Paúl Orta.

.

# CAPÍTULO VII

## 7. BIBLIOGRAFÍA

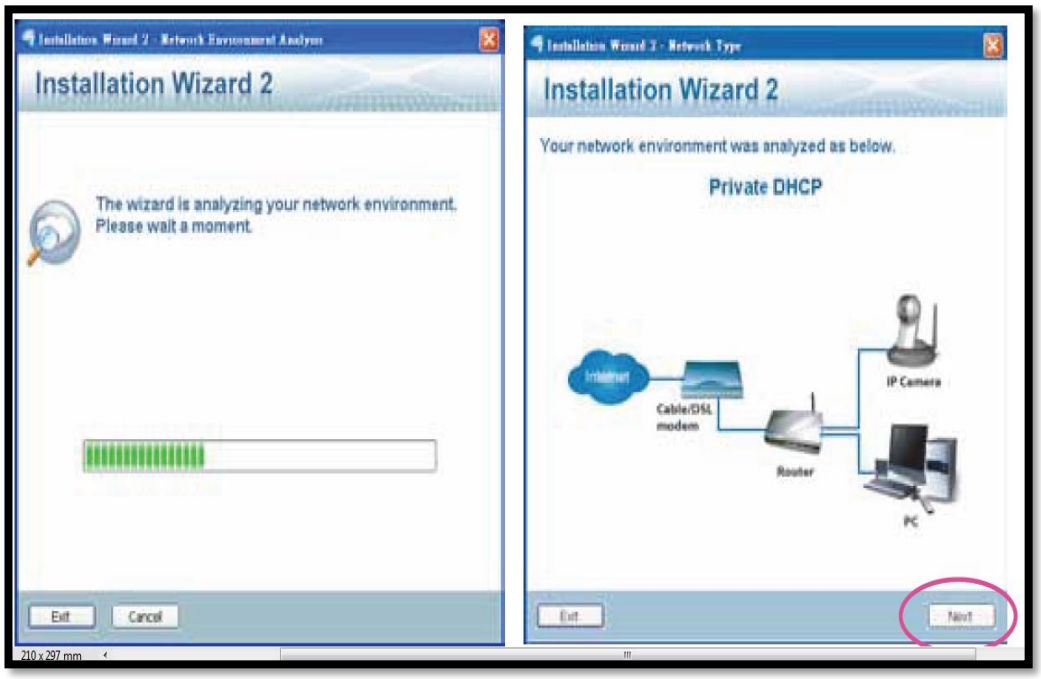

- Axis. (2010). Recuperado el 20 de Septiembre de 2013, de http://www.axis.com/products/video/about_networkvideo/audio.htm
- Agasio. (s.f.). Agasio. Recuperado el 10 de Mayo de 2013, de support agasio: www.agasio.com
- Axis. (2010). Axis. Recuperado el 20 de Septiembre de 2013, de http://www.axis.com/products/video/camera/about_cameras/netcam_tech.htm
- Axis. (s.f.). Axis. Recuperado el 20 de Septiembre de 2013, de Red de área local y Ethernet y tipos de rede Ethernet": http://www.axis.com/products/video/about_networkvideo/ip_networks.htm
- Axis. (s.f.). Concepto sobre cámara IP. Recuperado el 20 de Septiempbre de 2013, de http://www.axis.com
- Blade. (2004). Redes de computadoras. Barcelona.
- Bluehack. (s.f.). Recuperado el 27 de Agosto de 2013, de Bluehack: www.bluehack.elhacker.net
- Cisco. (s.f.). Recuperado el 10 de Mayo de 2013, de Cisco: www.cisco.com
- CISCO. (s.f.). www.cisco.com. Recuperado el 25 de Enero de 2013, de Cisco: www.cisco.com/en/US/products
- compresión, T. d. (s.f.). Economizadores. Recuperado el 20 de Septiembre de 2013, de Tamaño de imageny compresión: http://www.economizadores.net/productos/sistemas-de-vigilancia.html
- GPRS, M. (s.f.). Gprs. Recuperado el 15 de Julio de 2013, de www.mobilegprs.com
- HERNANDO, J. M. (2004). COMUNICACIONES MOVILES (2ªED.). EDITORIAL UNIVERSITARIA RAMON ARECES.
- Mg-soft. (s.f.). Recuperado el 16 de Julio de 2013, de Mg-soft: www.mg-soft.com
- Microsoft. (s.f.). Recuperado el 4 de Septiembre de 2013, de Microsoft: http://msdn.microsoft.com

- Naranjo, F. R. (2007). Diseño de un Sistema de Seguridad Bajo pPataforma IP. Guayaquil, Ecuador.
- Navarro, F. D. (s.f.). Administración de redes. En F. D. Navarro, Administración de redes (pág. Cap. 8).
- Network Scanner. (s.f.). Recuperado el 16 de Julio de 2013, de Network Scanner: www.softperfect.com
- Power Manager. (s.f.). Recuperado el 17 de Julio de 2013, de Power Manager: www.powersnmpmanager.com
- Sampieri, R. H. (18 de Enero de 2009). Metodología de la Investigación.
- Superinventos. (s.f.). Recuperado el 20 de Agosto de 2013, de http://www.superinventos.com/S220215.htm
- Tanenbaum, A. S. (2003). Redes de computadoras. Mexico: PEARSON.
- Tanenbaum, A. s. (s.f.). Rede de computadoras. PEARSON.
- vivotek. (s.f.). Recuperado el 15 de Abril de 2013, de www.vivotek.com
- Wireshark. (s.f.). Recuperado el 13 de Agosto de 2013, de Tutorial: www.wireshark.com
- STALLINGS, William, "Comunicaciones y Redes de Computadores", 6ta Edición 2000, Prentice-Hall.
- STREMLER, Ferrel, "Sistemas de Comunicación", Segunda Edición, Editorial Alfaomega, México 1982.

# CAPÍTULO VIII

## 8. ANEXOS

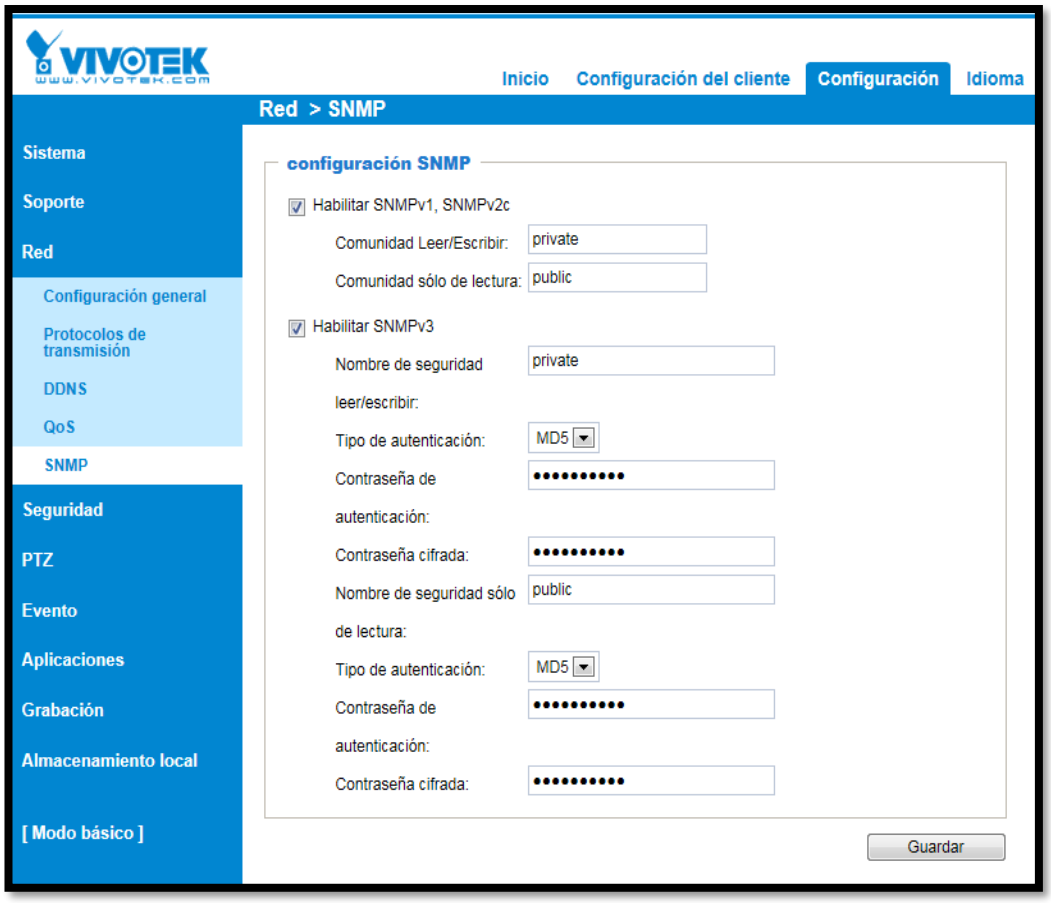
### 8.1 ANEXO A: Configuración de Cámara Ip Vivotek FD8136





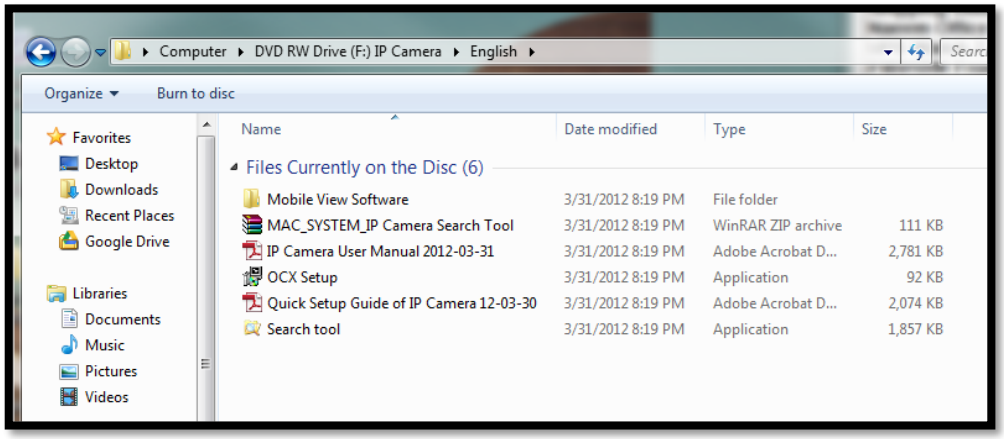
**Elaborado por:** Paúl Orta.

## Configuración de SNMP



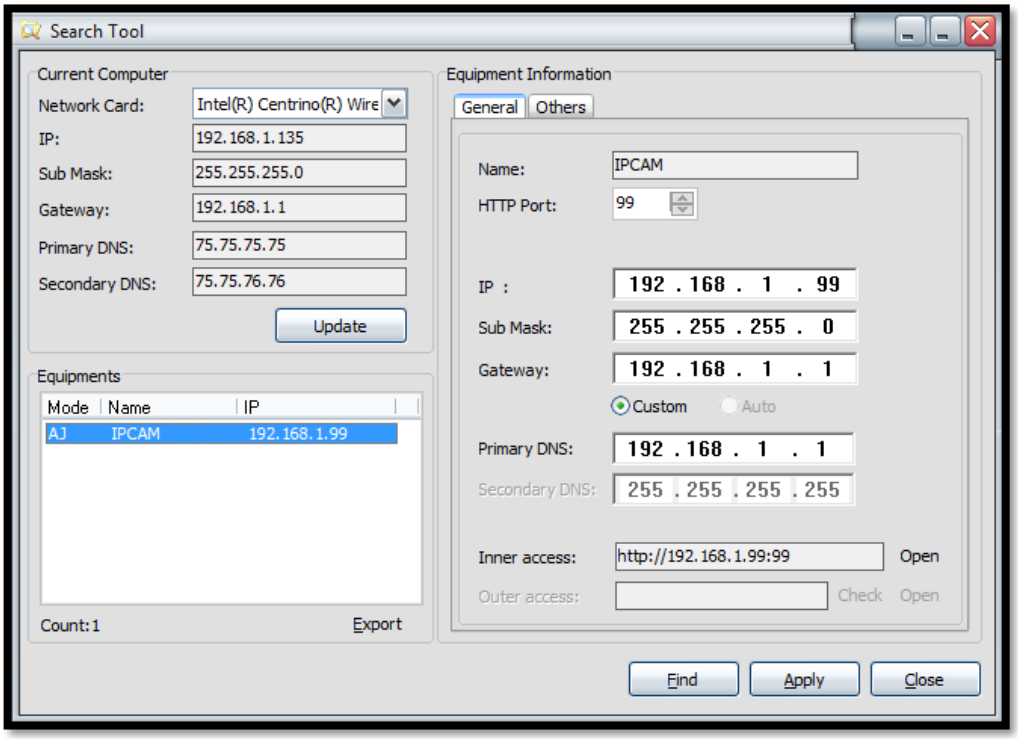
## 8.2 ANEXO B: Configuración de Cámara Ip AGASIO A603W

**Ejecutar OCX y Search tool.**



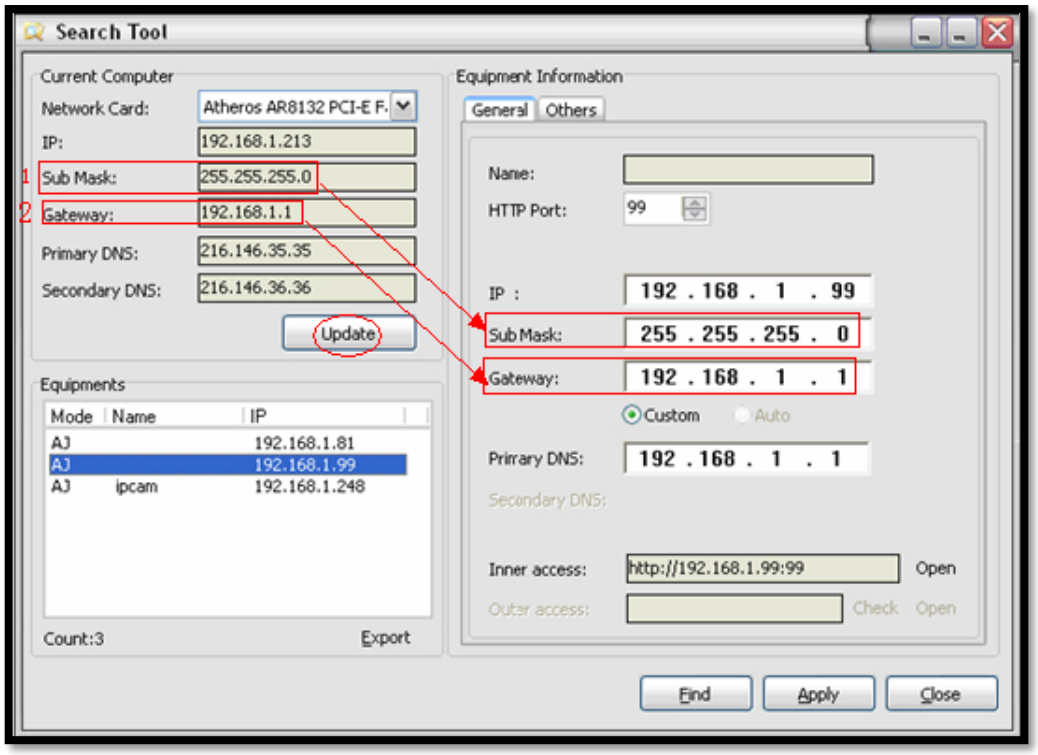

**Elaborado por:** Paúl Orta

**Buscar a la Cámara IP Agasio**



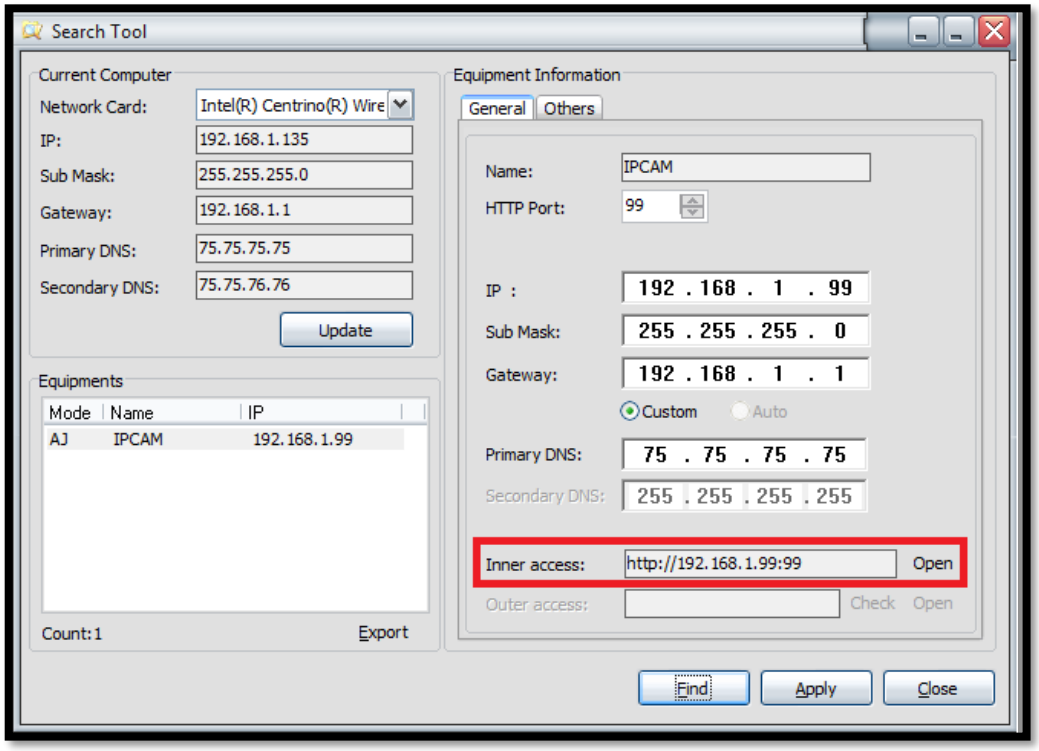

**Elaborado por:** Paúl Orta

**Poner Mascara, Dirección Ip, DNS primario, Puerta de Enlace**



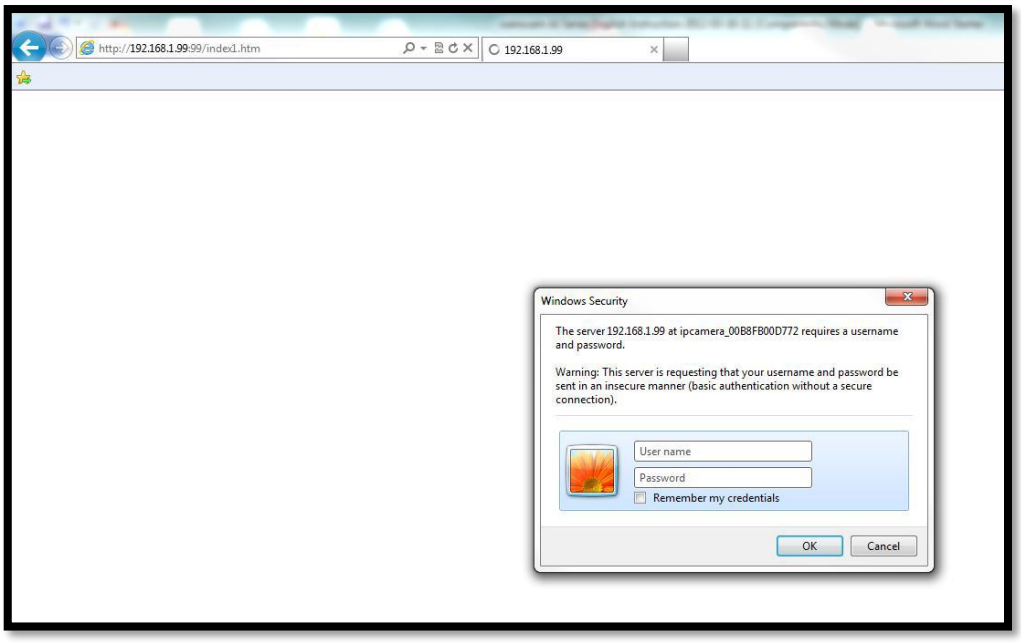

**Elaborado por:** Paúl Orta

**Abrir Web de Agasio.**



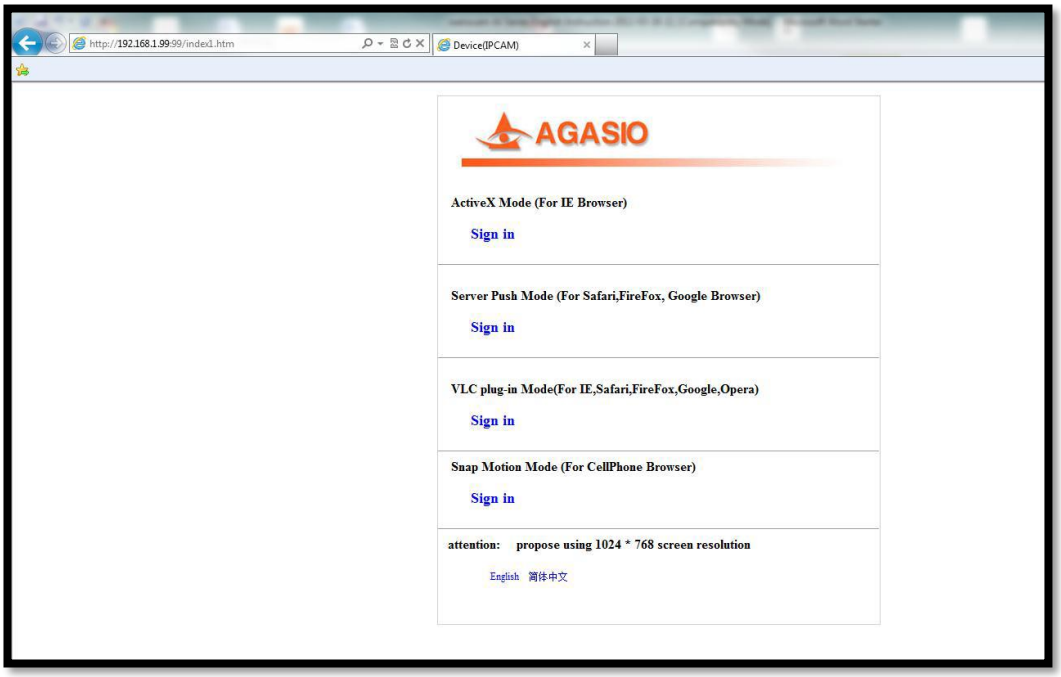

**Elaborado por:** Paúl Orta

**Ingresar Usuario y Contraseña**




**Elaborado por:** Paúl Orta

**Escoger una de las opciones.**

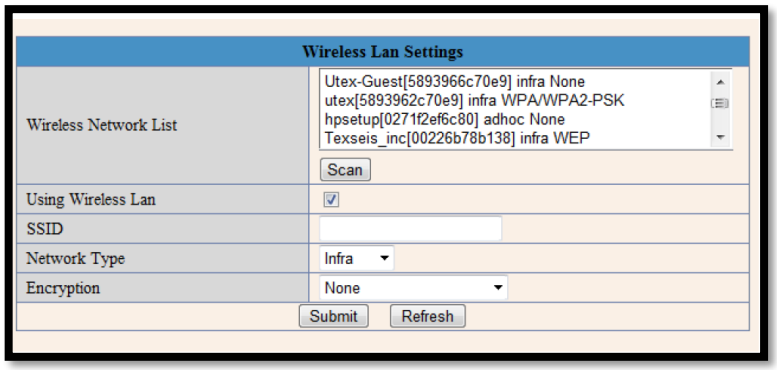



**Elaborado por:** Paúl Orta

**Visualización de la Cámara Agasio.**

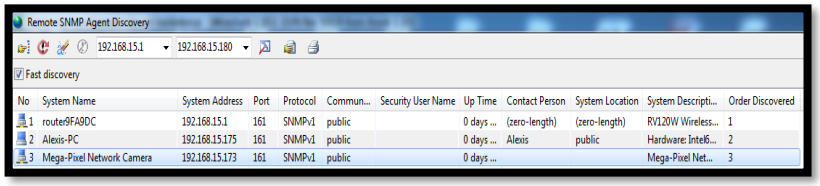

**Elaborado por:** Paúl Orta

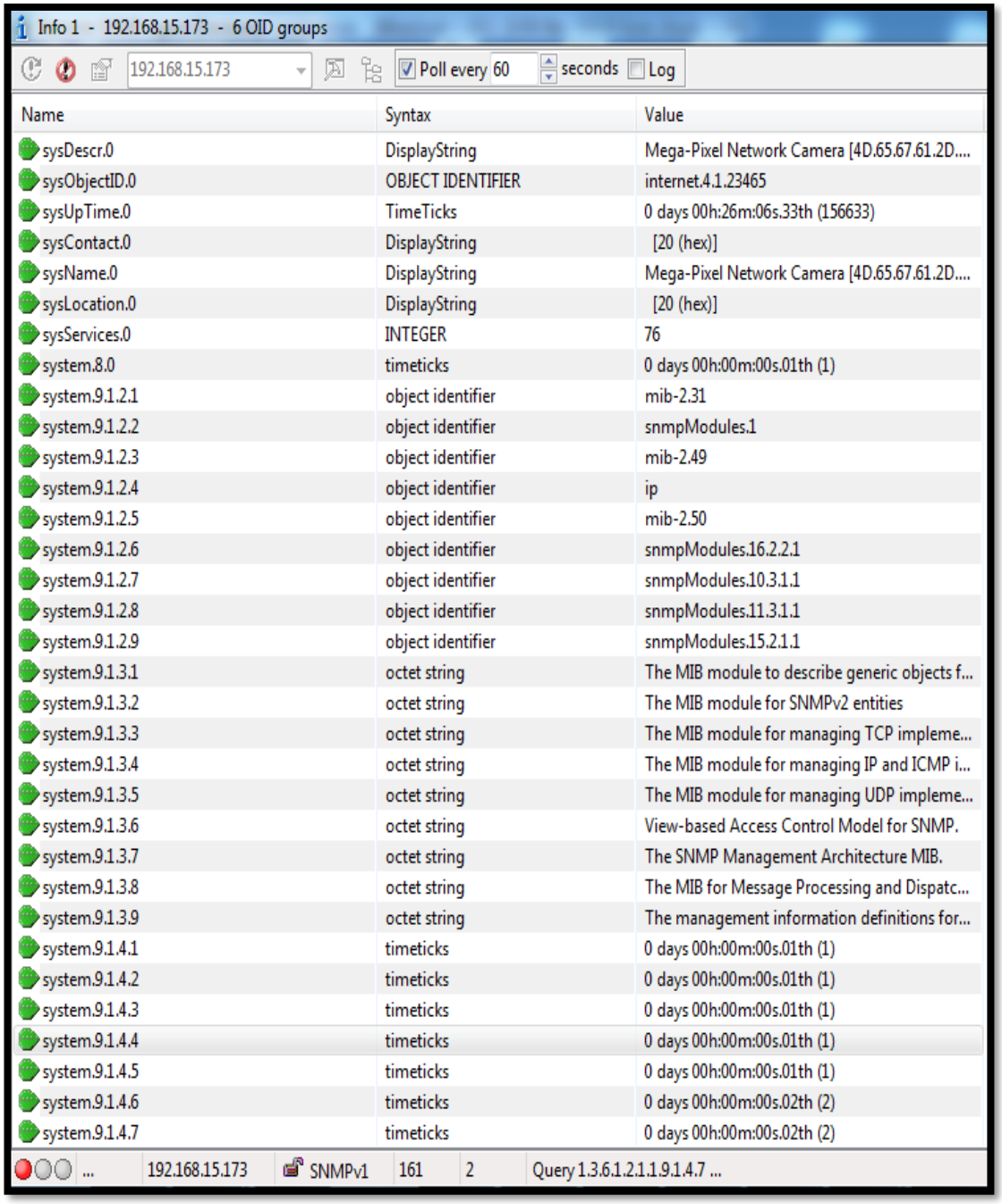
**Configuración de Wireless**



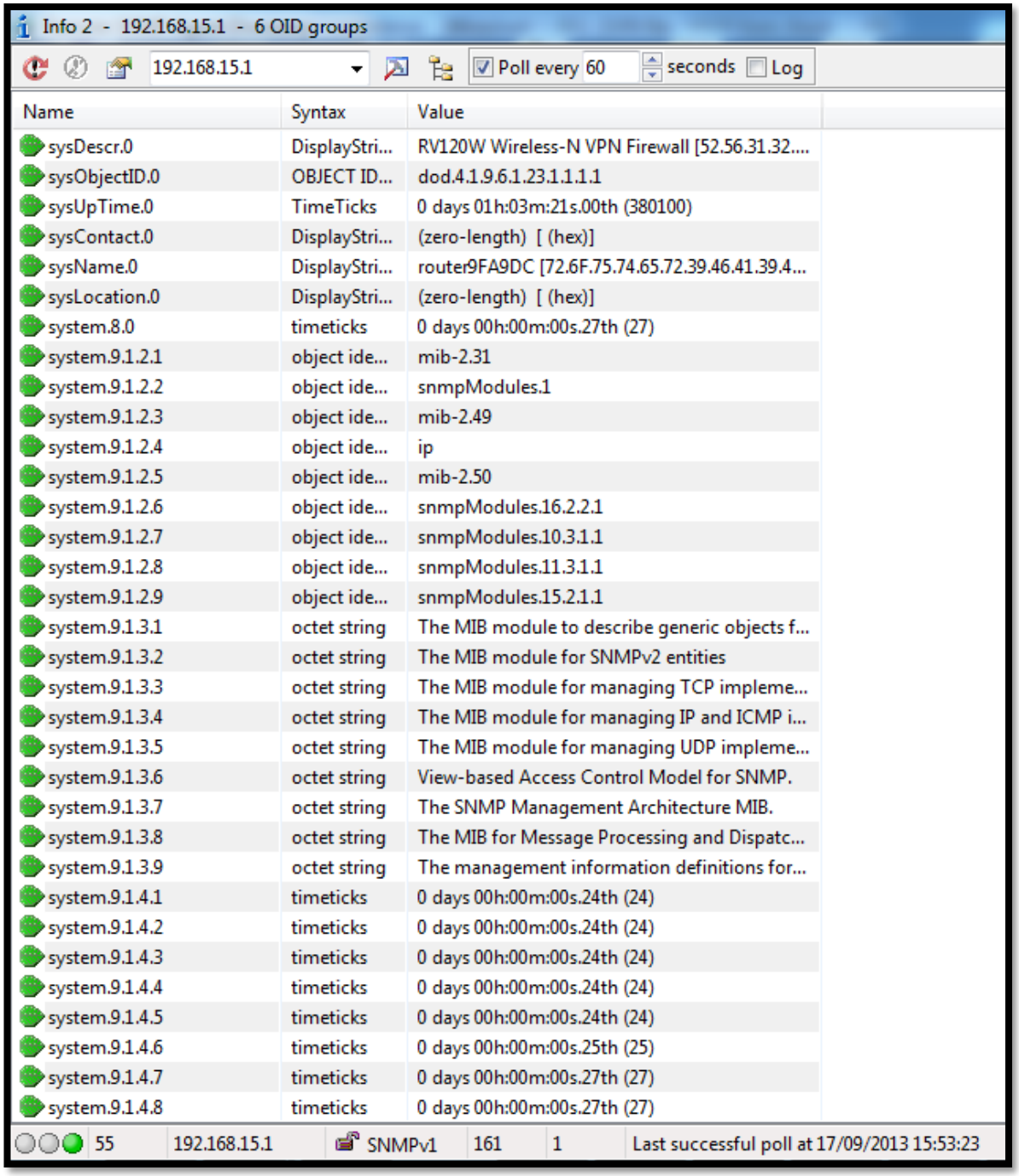

**Elaborado por:** Paúl Orta

**Configuración y prácticas SNMP V1**



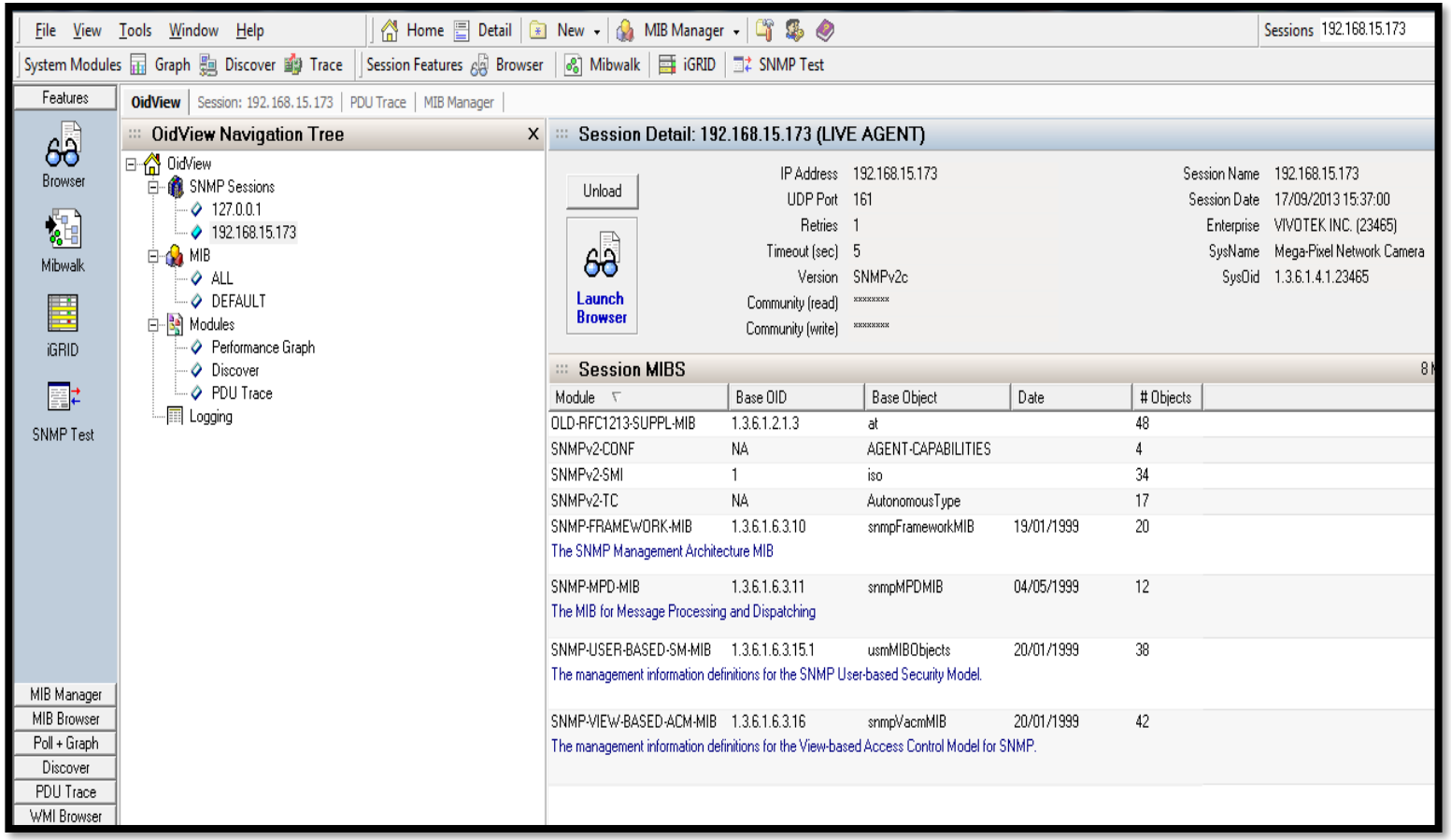



**Elaborado por:** Paúl Orta.

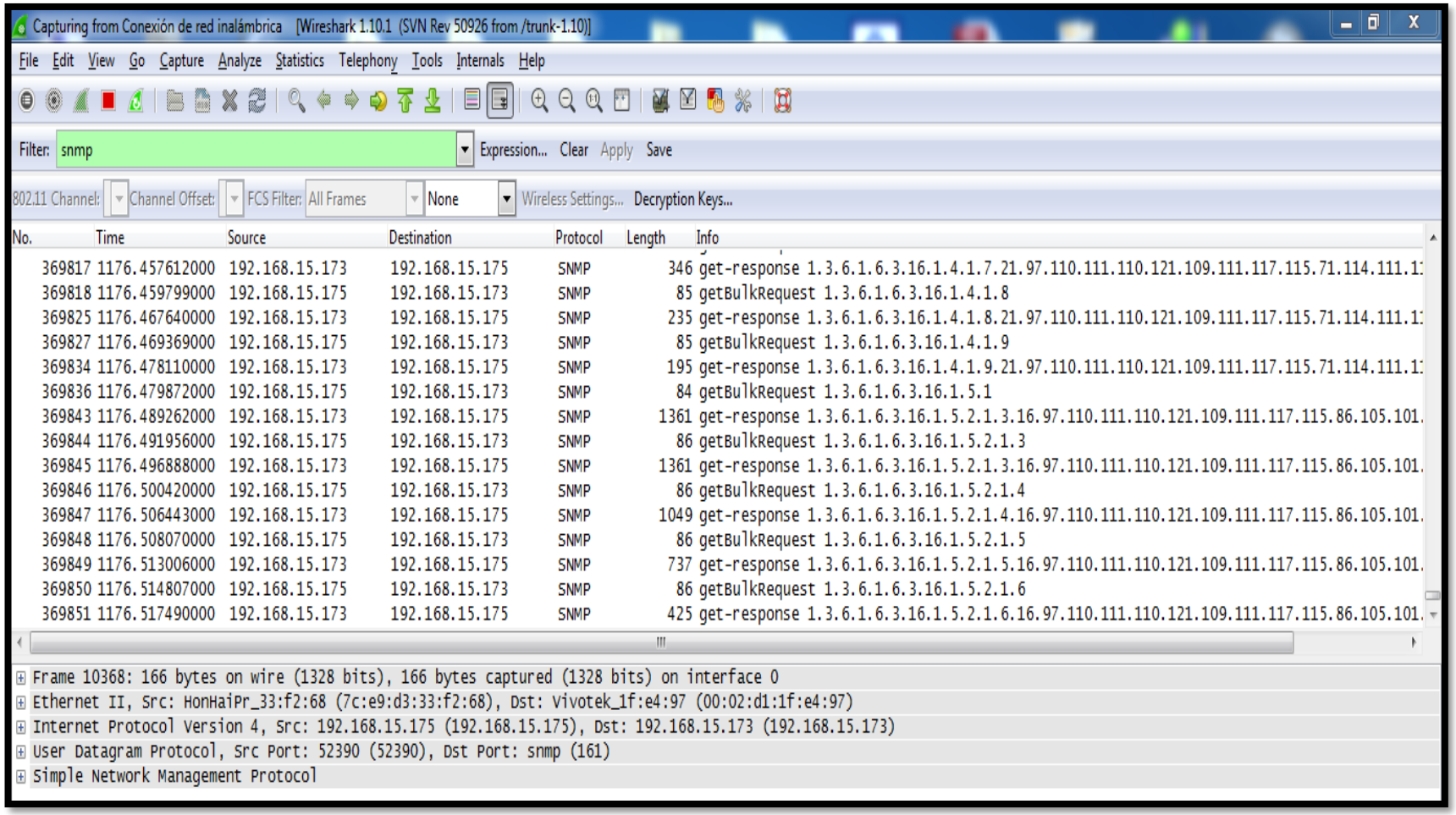



**Elaborado por:** Paúl Orta.

## 8.3 ANEXO C: Configuración y practicas SNMP V2

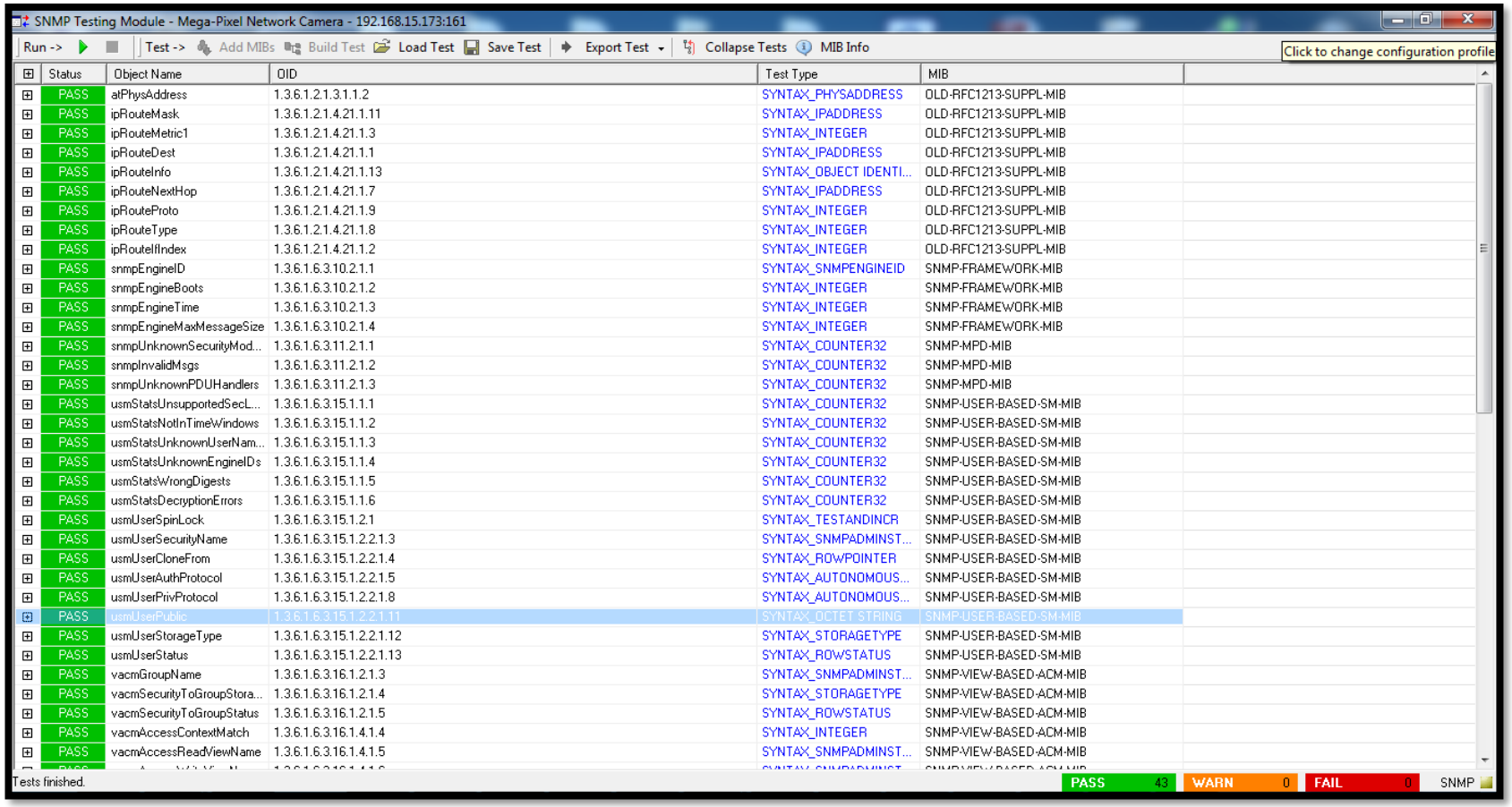



**Elaborado por:** Paúl Orta



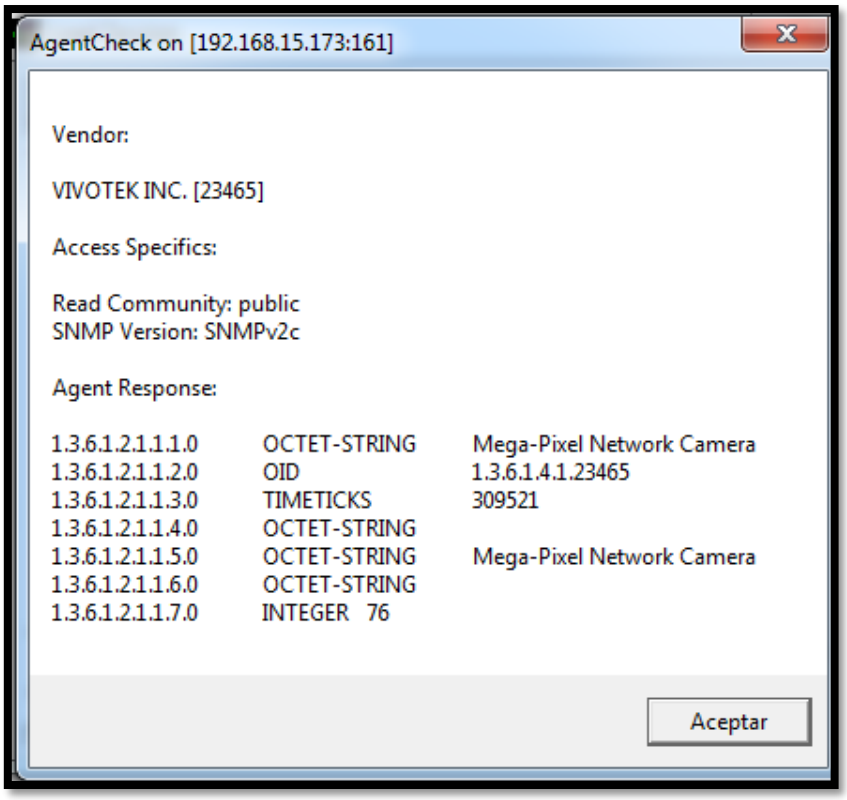

**Elaborado por:** Paúl Orta

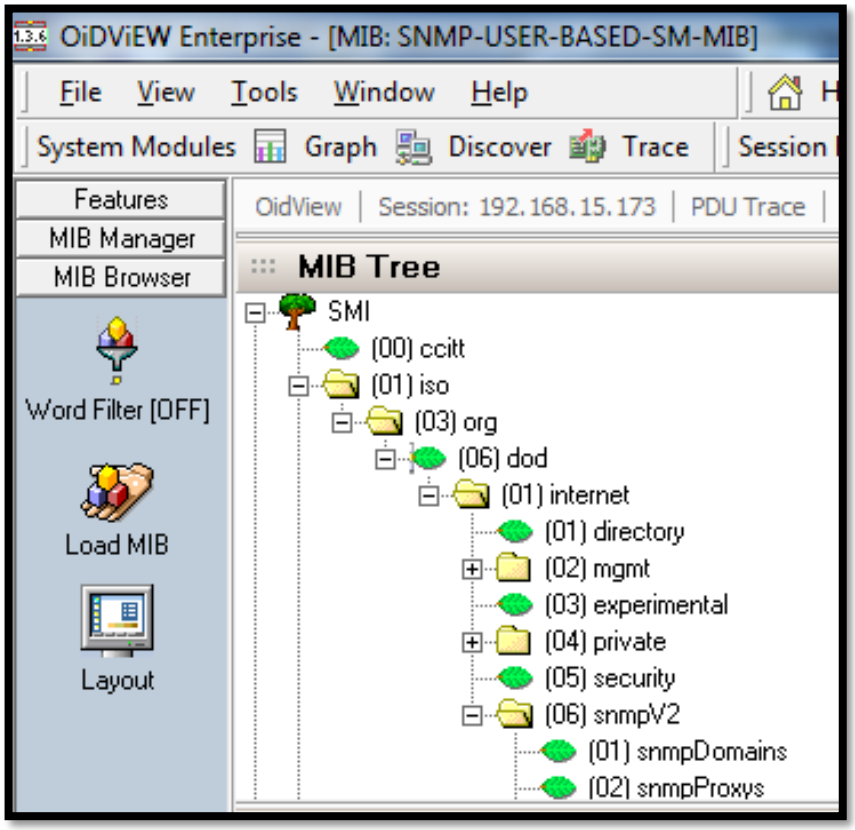
**Comprobación de Arbol Snmp**



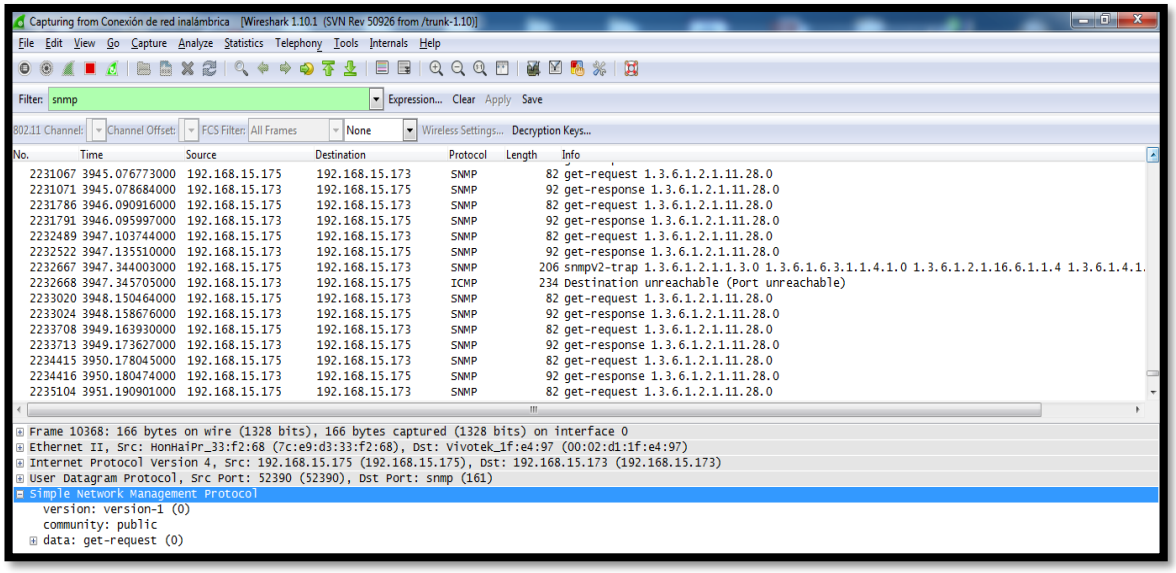

**Elaborado por:** Paúl Orta

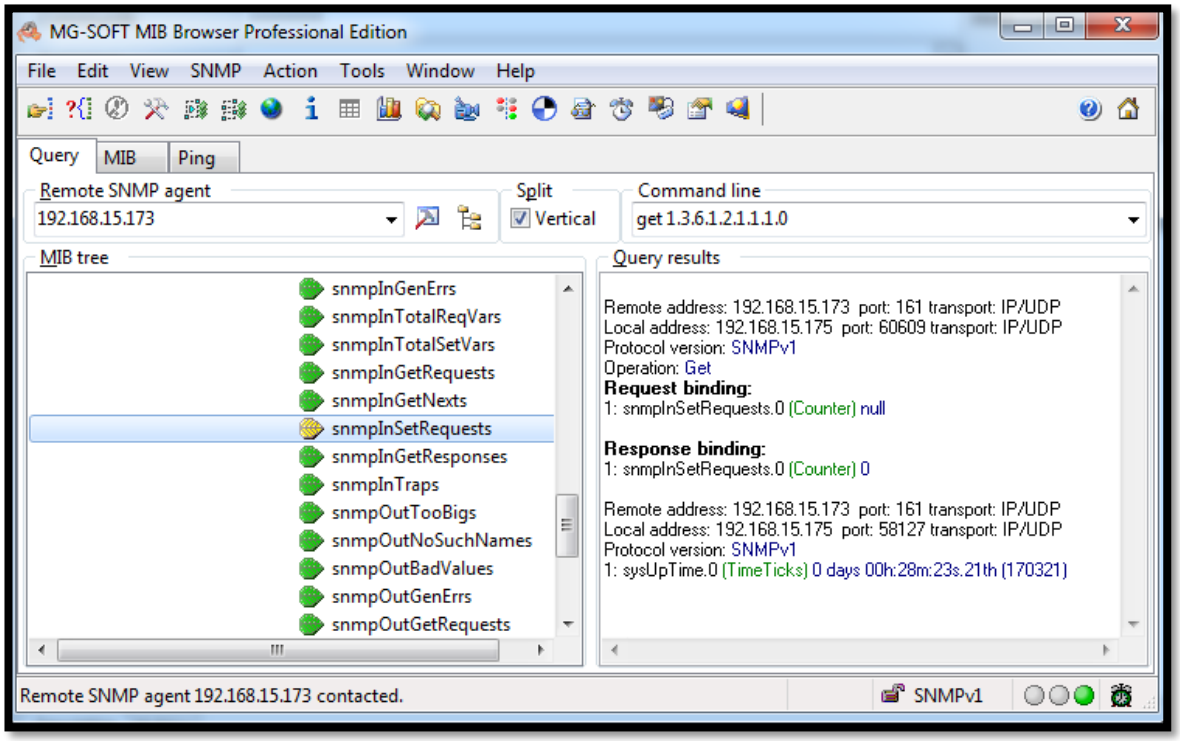
**Capturas SNMP V1, V2c Vivotek FD 8136**




**Elaborado por: Paúl Orta**



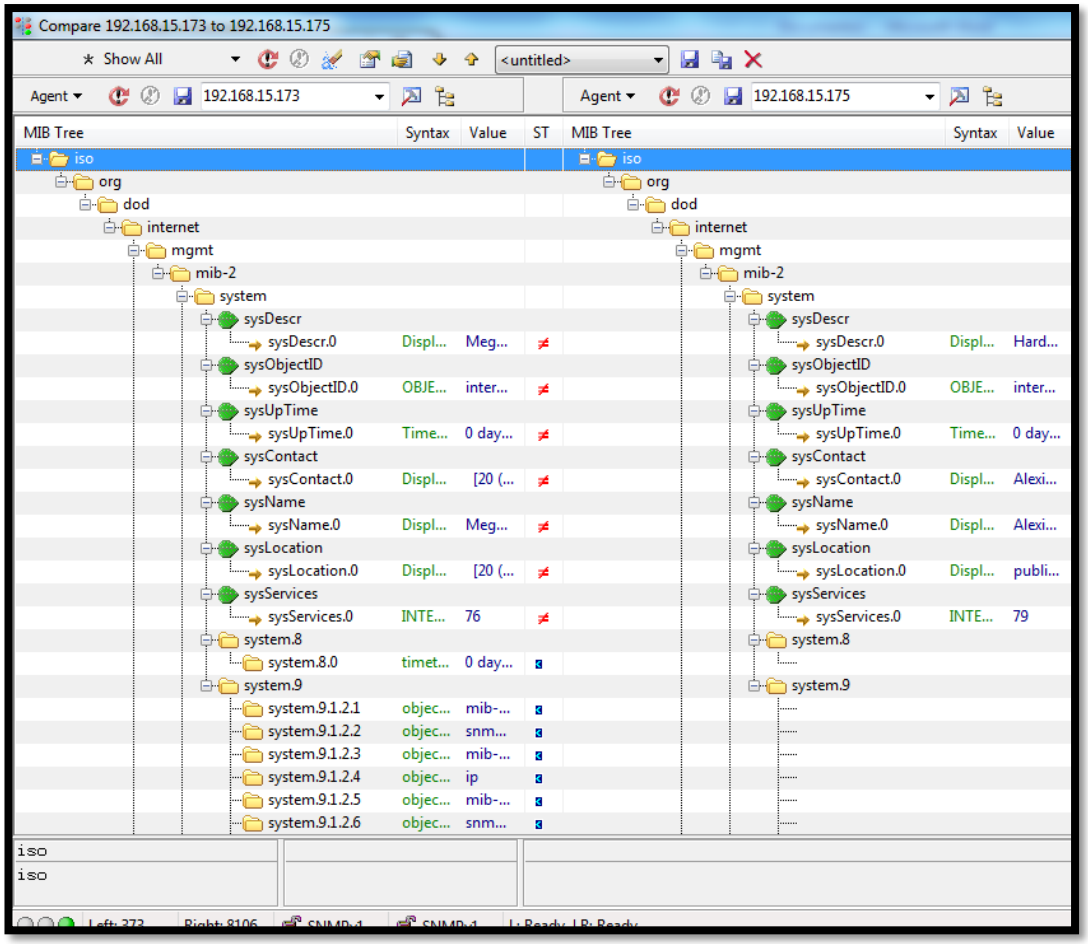



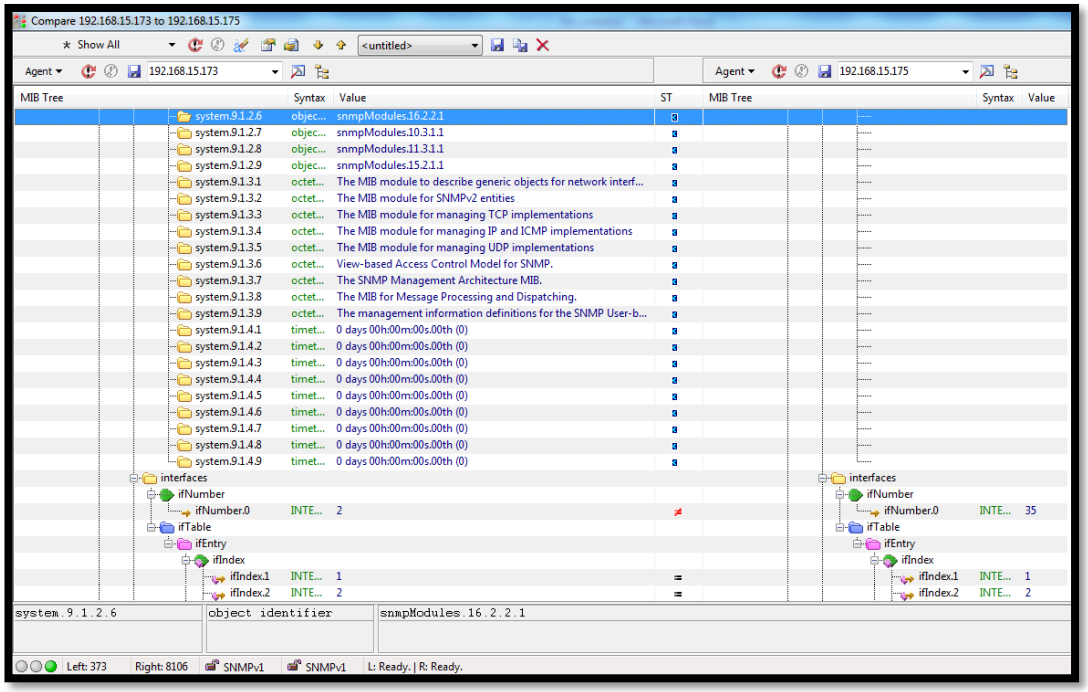

**Elaborado por: Paúl Orta**

**Envió de consultas SNMP vía móvil android**

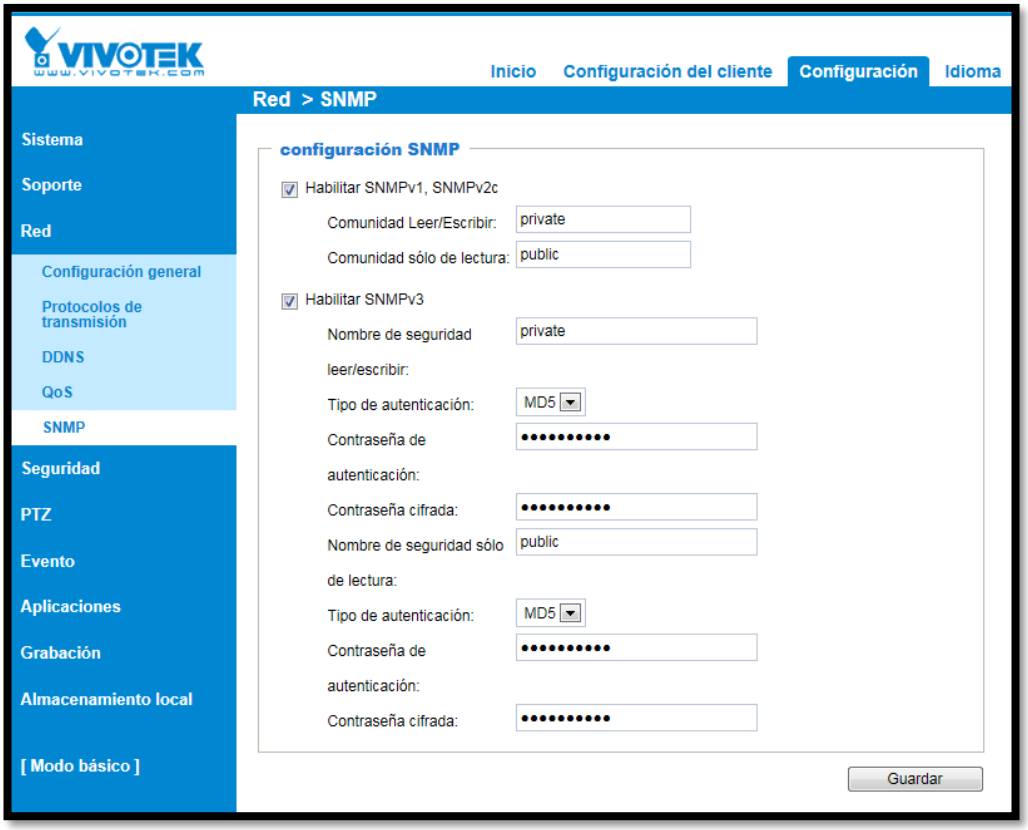


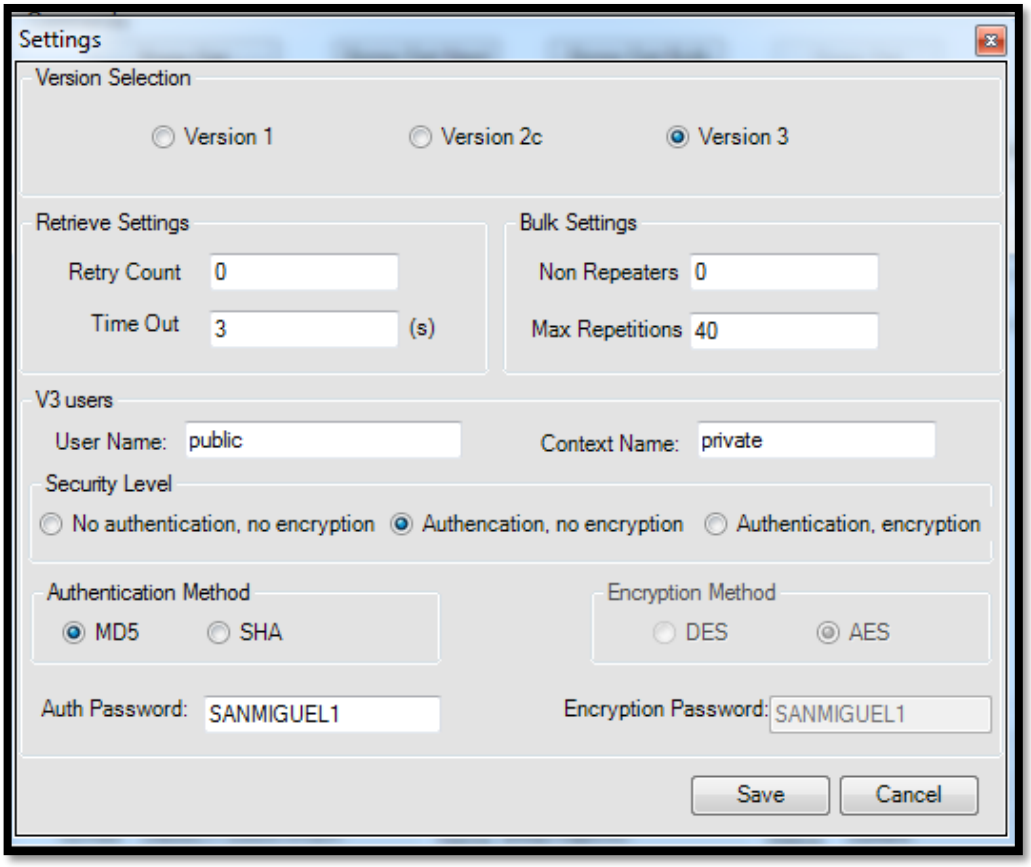
## 8.4. ANEXO D: COMPARACION ENTRE LA CAMARA VIVOTEK Y LA PC-LAPTOP HP I5



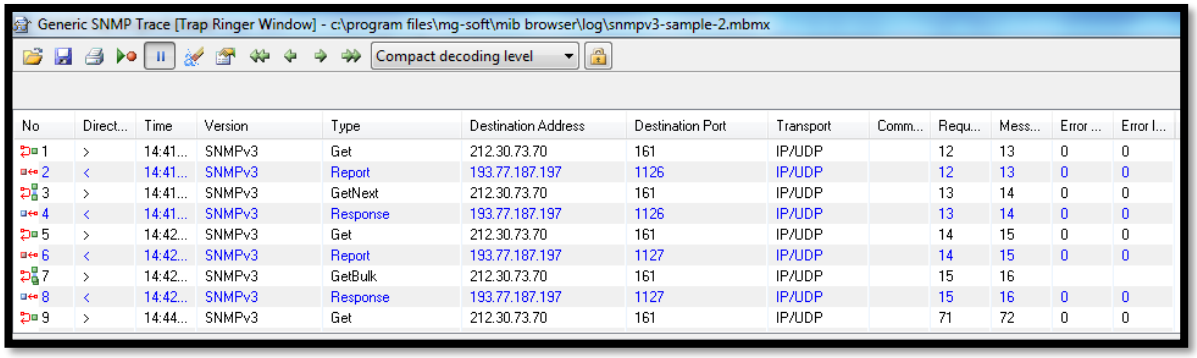



## SNMP V3, CAMARA VIVOTEK FD 8136





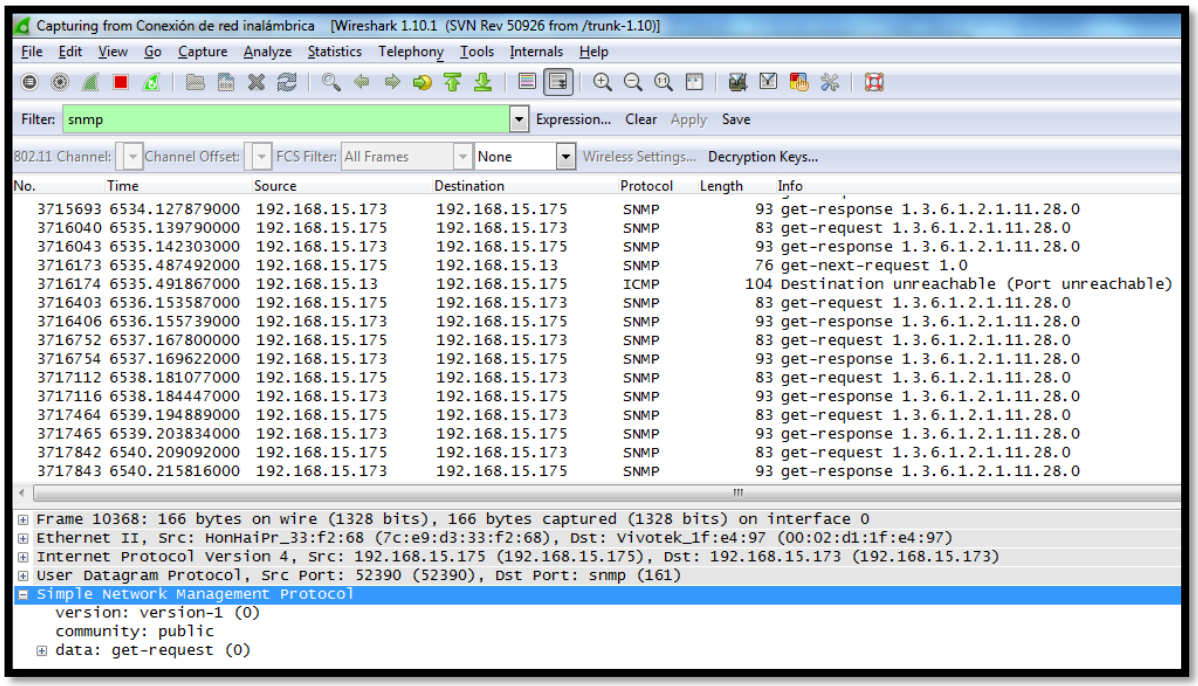

**Envio Get, Get Next, Get Bulk, Response de SNMP V3**




| No | Direct... | Time | Version | Type | Destination Address | Destination Port | Transport | Comm... | Requ... | Mess... | Error ... | Error I... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | > | 14:41... | SNMPv3 | Get | 212.30.73.70 | 161 | IP/UDP | | 12 | 13 | 0 | 0 |
| 2 | < | 14:41... | SNMPv3 | Report | 193.77.187.197 | 1126 | IP/UDP | | 12 | 13 | 0 | 0 |
| 3 | > | 14:41... | SNMPv3 | GetNext | 212.30.73.70 | 161 | IP/UDP | | 13 | 14 | 0 | 0 |
| 4 | < | 14:41... | SNMPv3 | Response | 193.77.187.197 | 1126 | IP/UDP | | 13 | 14 | 0 | 0 |
| 5 | > | 14:42... | SNMPv3 | Get | 212.30.73.70 | 161 | IP/UDP | | 14 | 15 | 0 | 0 |
| 6 | < | 14:42... | SNMPv3 | Report | 193.77.187.197 | 1127 | IP/UDP | | 14 | 15 | 0 | 0 |
| 7 | > | 14:42... | SNMPv3 | GetBulk | 212.30.73.70 | 161 | IP/UDP | | 15 | 16 | | |
| 8 | < | 14:42... | SNMPv3 | Response | 193.77.187.197 | 1127 | IP/UDP | | 15 | 16 | 0 | 0 |
| 9 | > | 14:44... | SNMPv3 | Get | 212.30.73.70 | 161 | IP/UDP | | 71 | 72 | 0 | 0 |

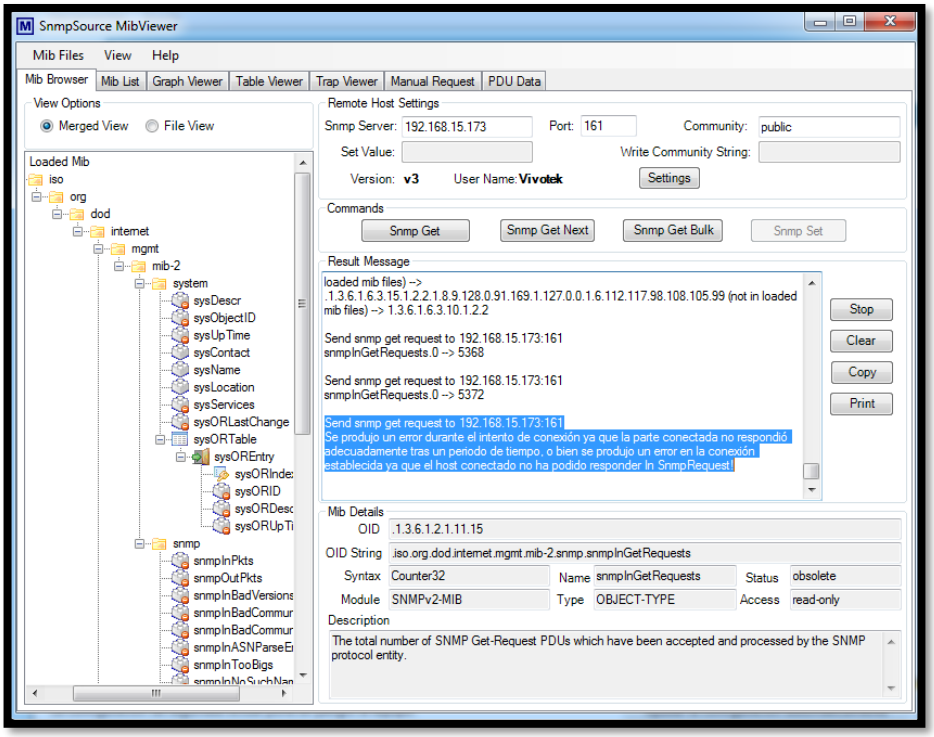
**Elaborado por:** Paúl Orta

## Capturas SNMP



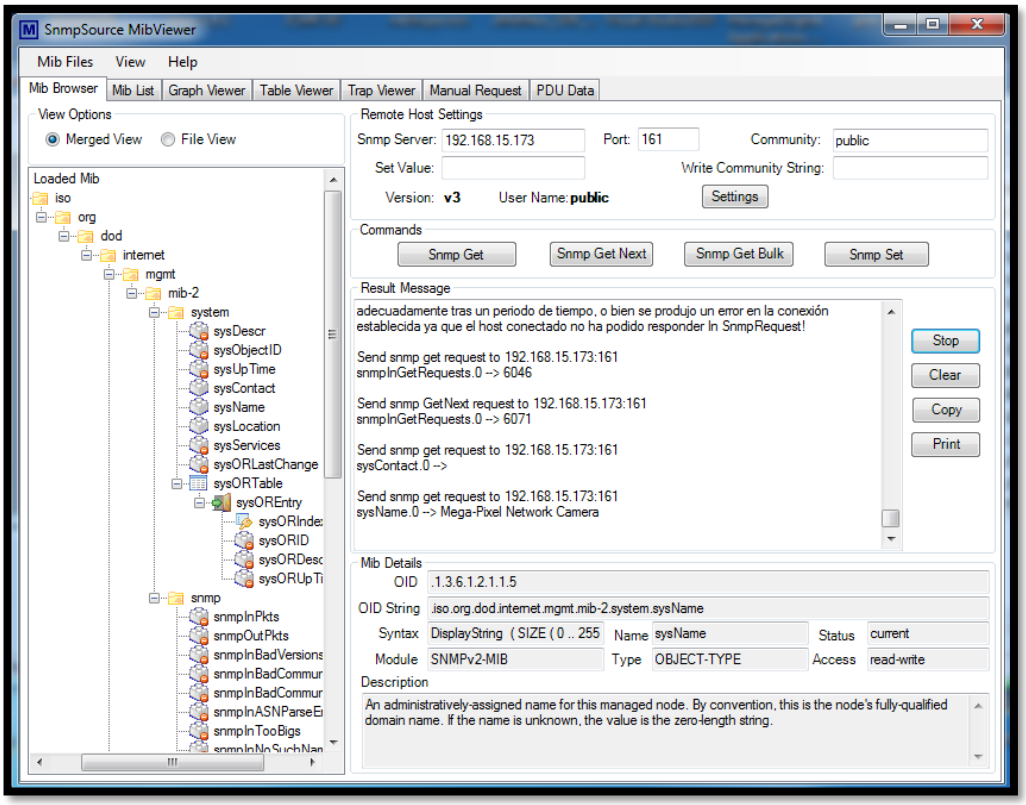

**Elaborado por: Paúl Orta**

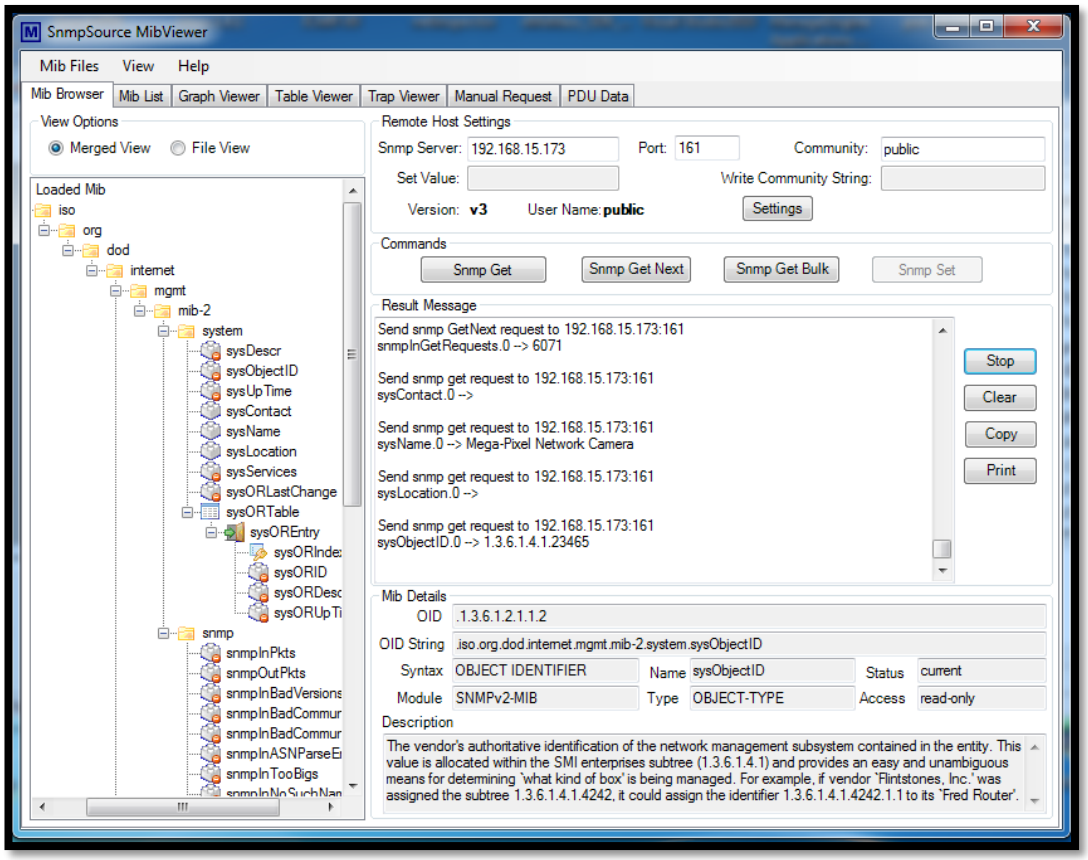
## Error por Falla de Autenticación




**Elaborado por:** Paúl Orta

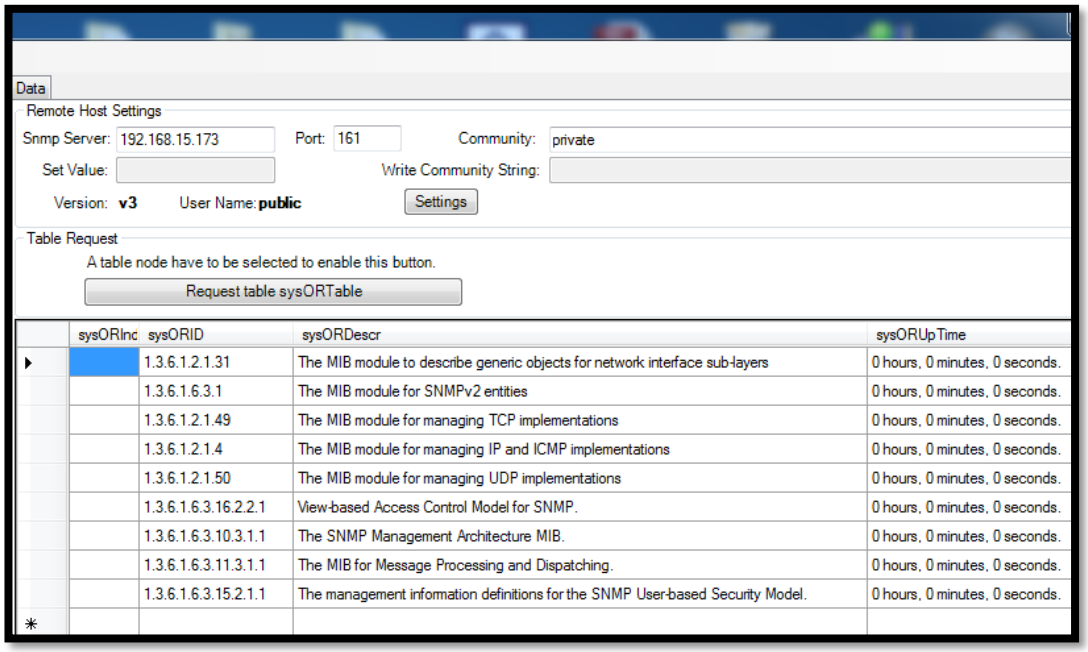
## Verificación exitosa de Autenticación de SNMP V3




**Elaborado por:** Paúl Orta

**Tabla Mib**




| sysORInc | sysORID | sysORDescr | sysORUpTime |
|---|---|---|---|
| | 1.3.6.1.2.1.31 | The MIB module to describe generic objects for network interface sub-layers | 0 hours, 0 minutes, 0 seconds. |
| | 1.3.6.1.6.3.1 | The MIB module for SNMPv2 entities | 0 hours, 0 minutes, 0 seconds. |
| | 1.3.6.1.2.1.49 | The MIB module for managing TCP implementations | 0 hours, 0 minutes, 0 seconds. |
| | 1.3.6.1.2.1.4 | The MIB module for managing IP and ICMP implementations | 0 hours, 0 minutes, 0 seconds. |
| | 1.3.6.1.2.1.50 | The MIB module for managing UDP implementations | 0 hours, 0 minutes, 0 seconds. |
| | 1.3.6.1.6.3.16.2.2.1 | View-based Access Control Model for SNMP. | 0 hours, 0 minutes, 0 seconds. |
| | 1.3.6.1.6.3.10.3.1.1 | The SNMP Management Architecture MIB. | 0 hours, 0 minutes, 0 seconds. |
| | 1.3.6.1.6.3.11.3.1.1 | The MIB for Message Processing and Dispatching. | 0 hours, 0 minutes, 0 seconds. |
| | 1.3.6.1.6.3.15.2.1.1 | The management information definitions for the SNMP User-based Security Model. | 0 hours, 0 minutes, 0 seconds. |

**Elaborado por:** Paúl Orta

**Camara Agasio A603W**

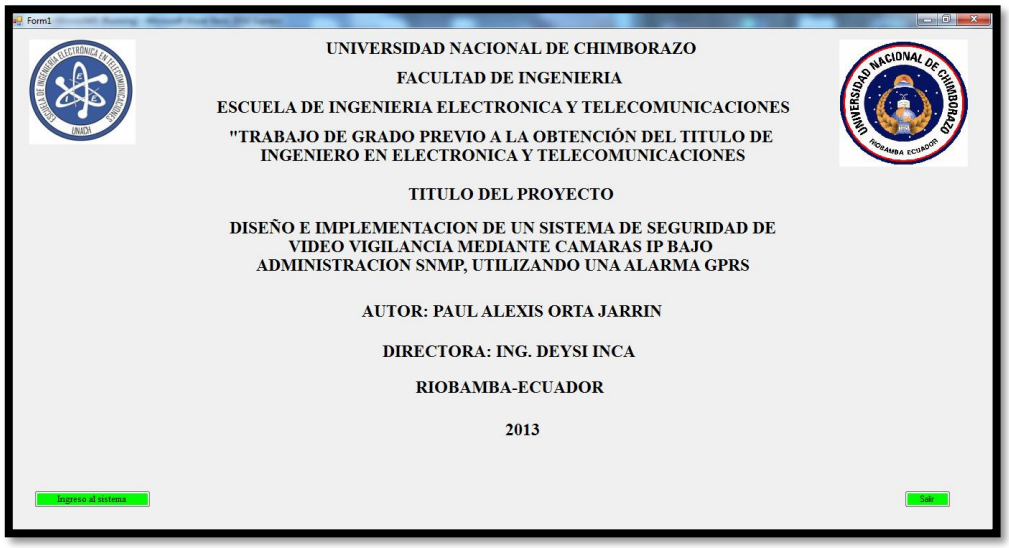
Ubicado con vista hacia el patio central de la institución


Ubicado con vista hacia la entrada principal de la institución

**Elaborado por:** Paúl Orta

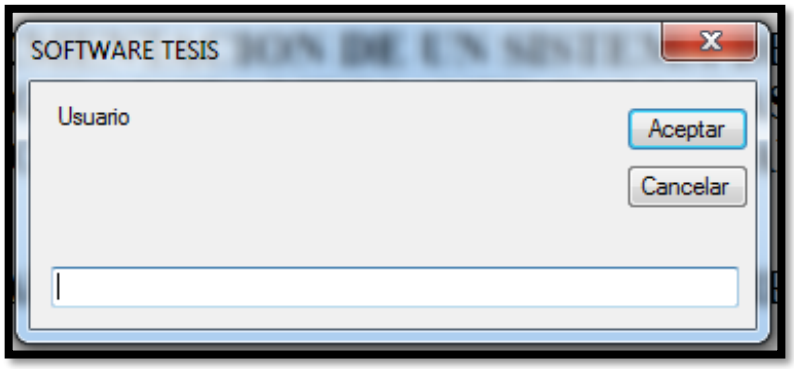
## 8.5 ANEXO E: SOFTWARE DESARROLLANDO EN VISUAL BASIC 2010 PARA ENVIO DE SMS

### Pagina Principal



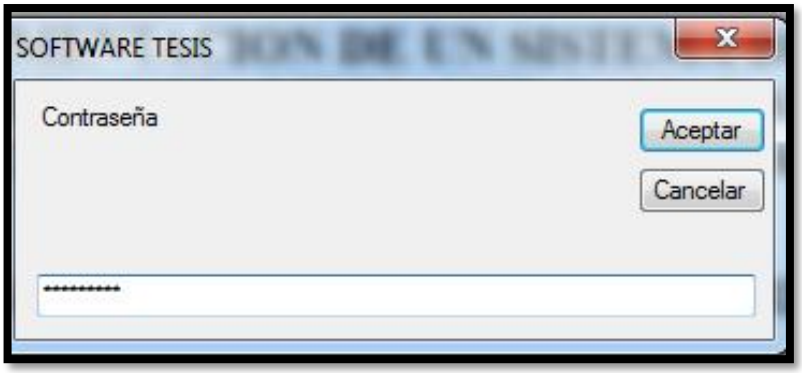

**Elaborado por:** Paúl Orta.

**Ingreso al Sistema SMS**



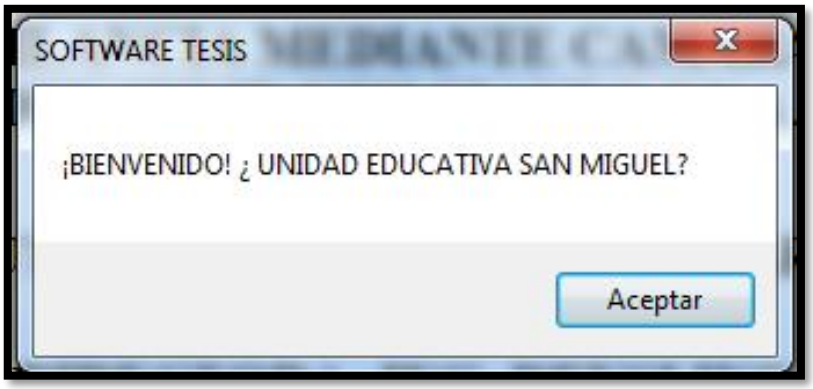

**Elaborado por:** Paúl Orta.

**Ingreso de Contraseña**



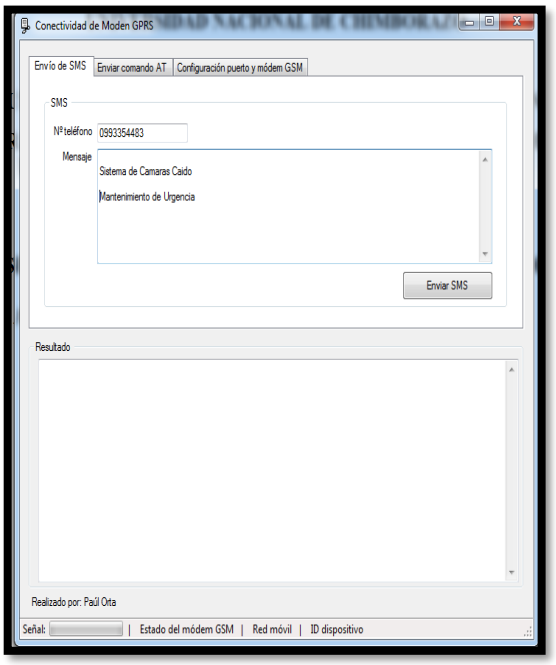

**Elaborado por:** Paúl Orta.

**Anuncio de Ingreso al Sistema**



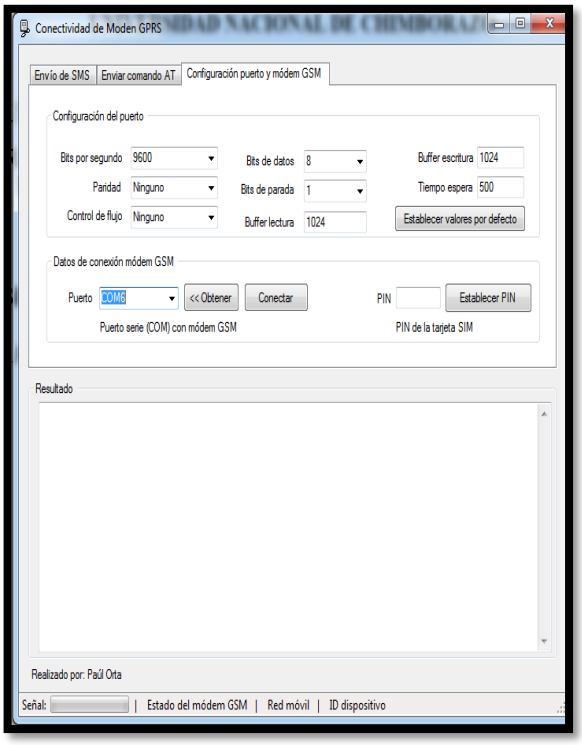

**Elaborado por:** Paúl Orta.

**Configuración del Número de Celular Destinatario y Mensaje de Envió**




**Elaborado por:** Paúl Orta.

**Configuración de Parametros de Moden GPRS**



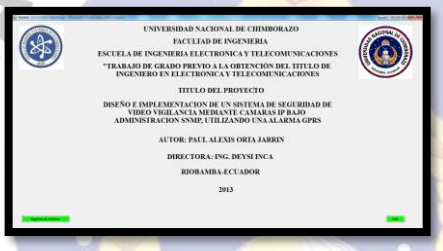

**Elaborado por:** Paúl Orta.

## 8.6. ANEXO F: MANUAL DE USUARIO FINAL.

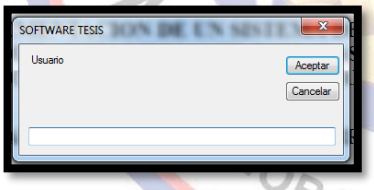
# MANUAL DE USUARIO PARA SISTEMA DE VIDEO VIGILANCIA EN LA "UNIDAD EDUCATIVA SAN MIGUEL DE BOLÍVAR"

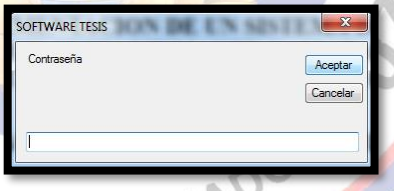
### 1.- Abrir el programa de video vigilancia


### 2.- Se abre la ventana principal y luego ingresar al sistema dando clic en "Ingresar al sistema"




### 3.- Poner usuario y contraseña correspondientes

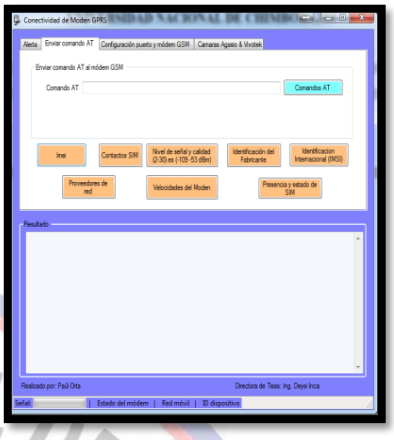



### 4.- Configuración del puerto y modem GPRS

- Dar clic en "Establecer valores por defecto" para asignar los datos para el modem
- Clic en "Obtener" puertos (recomendable poner en el último puerto)
- Luego dar clic en "Conectar"

**5.- Consultas de estado del modem y tarjeta SIM**

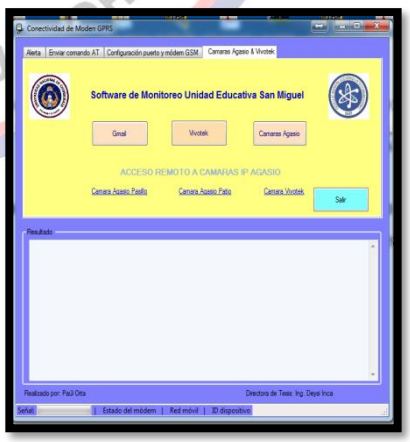


**6.- Activación de alerta GPRS mediante mensaje de texto**.

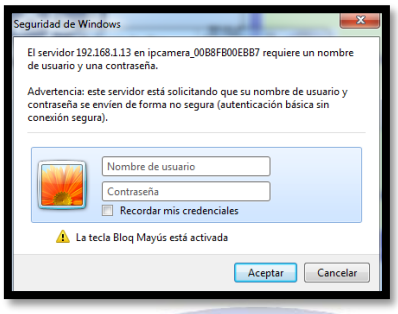
- Asignar el número a la autoridad correspondiente
- Definir el texto de la alarma dando clic en el botón “Alertar”
- Por ultimo dar clic en “Ejecutar Alerta SMS”

**7.- Acceso a Monitorear cámaras agasio y cámara vivotek**.

- Dar clic en la pestaña “Camara Agsio & Vivotek”
- Dar clic en el botón de las Camaras correspondientes (Agasio & Vivotek.), sea para el acceso local o acceso remoto.



**8.- Una vez dando clic en el botón de la "Cámaras Agasio" nos aparecerá una ventana pidiendo un usuario y contraseña correspondiente a la cámara agasio**.



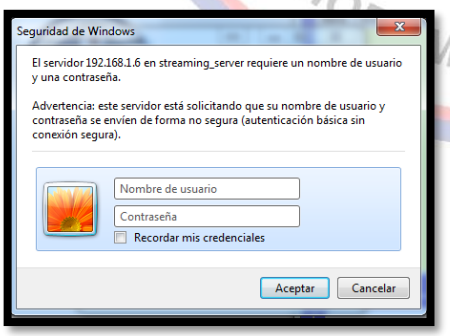

**9.- Una vez accedido a la cámara Ip.**

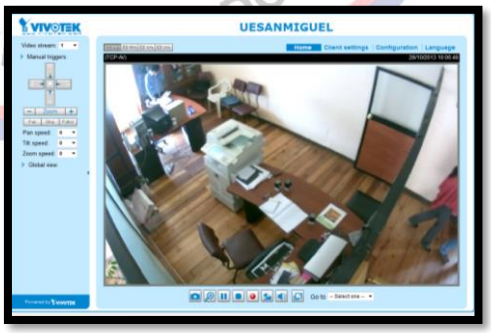
- Dar clic en la primera opción de la cámara agasio (Sign In)
- Para poder observar una sola cámara dar clic en la parte inferior del menú principal en la opción de indicadora de 4 cuadrados.



**10.- Acceso a cámara vivotek**

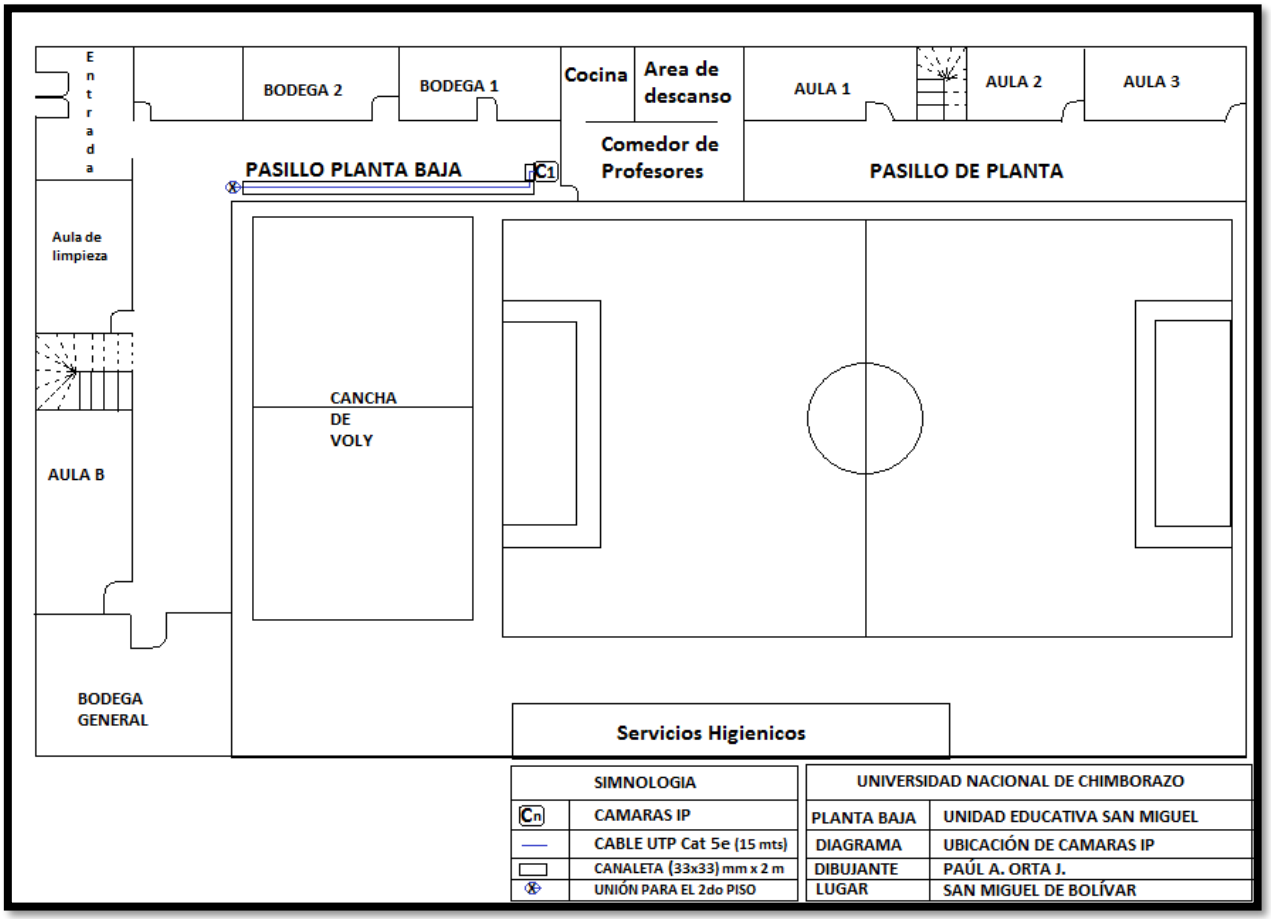
- Ingresar Usuario y Contraseña de la cámara Ip
- Acceso a monitorear Cámara Vivotek.



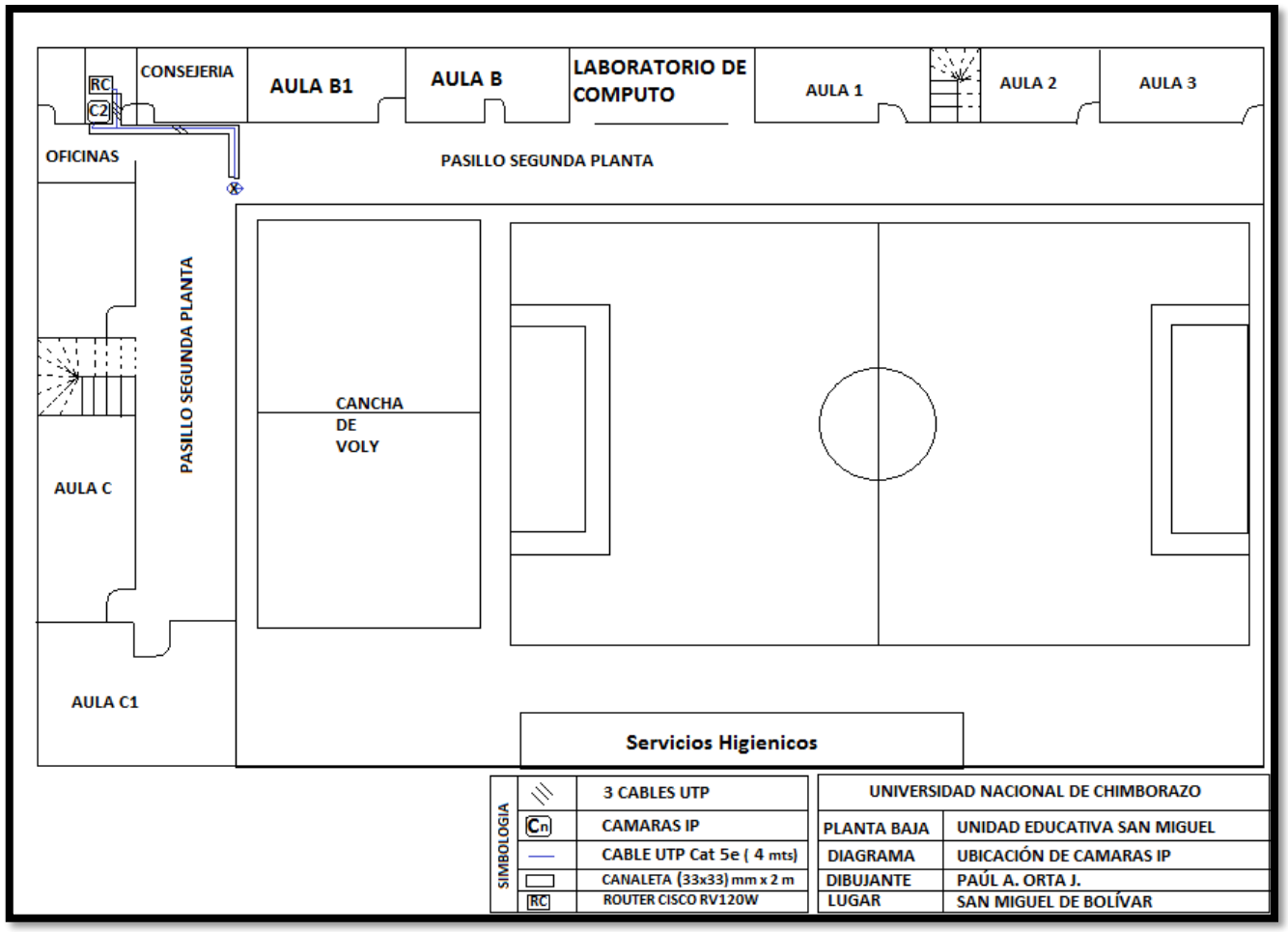



## 8.6. ANEXO G: BOSQUEJOS DE UBICACIONES DE LAS CAMÁRAS IP

### PLANTA BAJA



## SEGUNDA PLANTA



## TERCERA PLANTA