ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO Y PRUEBAS DE FUNCIONAMIENTO DE LOS ASPECTOS DE SEGURIDAD Y MONITOREOS DE UNA RED DE VIGILANCIA IP USANDO FTP Y SMTP GESTIONADO DESDE UN DISPOSITIVO PORTÁTIL"

TESINA DE SEMINARIO

Previo a la obtención del título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

PRESENTADO POR:

JOSÉ MANUEL COTTO BARDALES

FERNANDO ANDRÉS ORTÍZ BALLESTEROS

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Al Ing. Washington Medina Director de Tesis, por su ayuda y colaboración durante la realización de este trabajo, a nuestros padres por el valioso apoyo que nos han brindado, por las ganas de superación y ejemplo inculcados, y principalmente a Dios por guiarnos por el camino de la vida hacia esta instancia.

DEDICATORIA

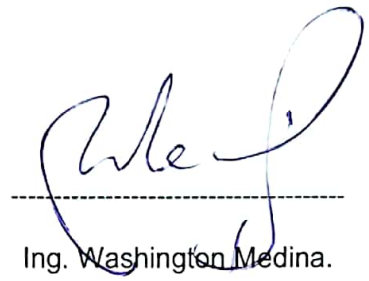
A mis padres y mi hija por el apoyo incondicional que me ha impulsado a lo largo de mi vida a luchar por mis sueños, a todos los profesores que en el transcurso de la carrera supieron brindarme sus valiosos conocimientos y a todas las personas que confiaron en mí y a las que no también, les dedico es este logro.

José Cotto Bardales.

A Dios, mis padres y mi esposa por haber siempre creído en mí de una manera tan especial y por todo lo que hemos pasado juntos les dedico este trabajo.

Fernando Ortiz Ballesteros.

TRIBUNAL DE SUSTENTACIÓN



Ing. Washington Medina.

PROFESOR DEL SEMINARIO DE GRADUACIÓN.

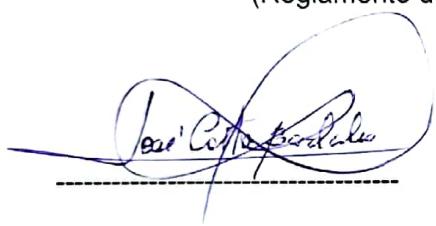
Ing. Sara Ríos.

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA.

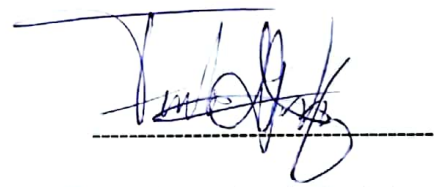
DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesina, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

(Reglamento de Graduación de la ESPOL)



José Manuel Cotto Bardales.



Fernando Andrés Ortiz Ballesteros

RESUMEN

En el presente documento se presenta la información necesaria para la pre-construcción y la verificación del funcionamiento de un sistema de monitoreo remoto de una red de vigilancia de video-cámaras IP a través de los protocolos de comunicación FTP y SMTP, que se gestionará a través de dispositivos portátiles con capacidad de acceso a un portal web. El enfoque del texto tiene como fin presentar un análisis que se extiende desde los basamentos teóricos de los sistemas de vigilancia mediantes cámaras IP, los protocolos de comunicación factibles a emplear en el monitoreo remoto de sistemas de este tipo, el software requerido para el procesamiento de la data proveniente de la red remota en los dispositivos portátiles, hasta la demostración del funcionamiento de un modelo de prueba que se encuentra implementado, que emula una aplicación real del sistema de monitoreo remoto diseñado.

ÍNDICE GENERAL

ÍNDICE DE GRAFICOS

ÍNDICE DE TABLAS

CAPÍTULO 1

DESCRIPCIÓN DEL PROBLEMA

1.1 Introducción

En las grandes empresas, en donde existen sistemas de vigilancia que tienen cámaras, hay vulnerabilidades de estos sistemas de vigilancia. Uno de ellos es la falta de control y monitoreo del sistema en sí debido a los costos que esto representa para tener a una persona que esté 24 horas pendientes del mismo y que sea capaz de resolver algún problema que llegue suceder dentro de las instalaciones que están siendo gestionadas. Otra debilidad de los sistemas de vigilancia es

que al momento de grabar videos y almacenarlos estos pueden llegar ser de gran tamaño y por ende necesitan de muchos medios de almacenamiento de gran capacidad, puesto que el tiempo de almacenamiento fluctúa entre 15 a 30 días como normal y en casos especiales hasta 45 días, lo que resulta relativamente corto para algunas empresas en cuanto a una relación costo-beneficio. Además en el manejo de video resulta muy difícil resolver la función de copia de seguridad ya que esto implicaría que sea transferido a otro servidor resultando a un gran consumo de ancho de banda.

La múltiple ocupación de los encargados para la seguridad y el operador del sistema hacen que se despreocupen de la función de las cámaras y de una óptima calidad en el servicio de video por lo que esto se presta como una debilidad.

1.2 Justificación

Debido a las debilidades que presenta en el aspecto de seguridad y monitoreo, se desea implementar un sistema en empresas y lugares en donde se torne difícil la revisión continúa de video para así

optimizar el servicio que puede prestar una cámara de vigilancia IP de red, en donde sabemos que lo principal que se necesita es la revisión de imágenes en lugares específicos donde se han colocado las cámaras, específicamente en donde más se lo necesite. La cámara de vigilancia ip para red, lo puede ver directamente desde internet o desde la red de su empresa, con visión nocturna (infrarrojo) para el uso de 24 horas.

La optimización del tiempo al mostrar las imágenes y monitoreo de la cámara de vigilancia IP en dispositivos móviles hace que el sistema sea didáctico y atractivo, ya que se podría monitorear desde cualquier lugar al momento del mensaje de advertencia, y podremos observar lo que en ese instante pasa y escuchar lo que las personas hablan cerca de la cámara.

Por estos motivos se justifica la elaboración de este proyecto que permitirá un monitoreo eficaz de nuestra red de vigilancia.

1.3 Objetivo General

Diseñar y probar el funcionamiento de cámaras de seguridad y monitoreo de una red de vigilancia IP usando FTP y SMTP gestionada mediante dispositivos portátiles.

1.4 Objetivos Específicos:

1.- Configurar el software de la cámara IP inalámbrica.

2.- Implementar los protocolos FTP y SMPT.

3.- Instalar ip publica en dispositivos móviles.

4.- Gestionar y Monitorear la vigilancia de la cámara ip desde el dispositivo móvil.

1.5 Metodología:

El gestionamiento y monitoreo del sistema se lo va implementar mediante una configuración de un software de la cámara IP inalámbrica easyn.

La implementación de los protocolos FTP y SMTP nos permitirá tanto la transferencia de Mail y de archivos en este caso imágenes o una advertencia al estar al límite del sensor infrarrojo de la cámara IP, estas imágenes o advertencia podrán ser vistas en el momento o estarán almacenadas para su posterior revisión.

La contratación de nuestra propia dirección de IP publica con el objetivo de gestionar nuestra propia red las 24 horas del día. .

El monitoreo y pruebas de la cámara IP inalámbrica desde nuestro dispositivo móvil, la características de la cámara IP inalámbrica es la sensibilidad al movimiento y el envío de mensajes ya sea de alarma o envió de imágenes que tomara la cámara, en el caso de que este detecte un movimiento en lugares que se requiere algún tipo de autorización para su respectivo ingreso.

La cámara IP inalámbrica al momento de enviar un mensaje de advertencia o imágenes, esta podrá ser monitoreada desde el dispositivo móvil ya sea haciéndole ir de derecha a su izquierda, o de arriba hacia abajo. Esta implementación de esta cámara IP inalámbrica nos ayudara en la seguridad de pymes o en la manera q se asigne su uso.

La cámara de vigilancia ip para red se lo podrá ver directamente desde la red de nuestra empresa las 24 horas, se mueve de un lado a otro lo podremos controlar el movimiento a través del software y desde

nuestra red. Esta cámara de seguridad IP se puede instalar en cualquier lado donde se lo necesite, se podrá escuchar lo que las otra personas hablen cerca de la cámara, se podrá hablar entre ellos desde nuestro dispositivo móvil y podremos grabar en nuestro dispositivo portátil el video de lo que sucede.

CAPÍTULO 2

INTRODUCCIÓN DEL SISTEMA DE VIGILANCIA IP

2.1 Introducción

¿Qué es el Vídeo IP?

El video IP es cuando transmitimos imágenes y sonidos a través de protocolos de comunicaciones IP, el medio de transmisión que utiliza el video IP es por redes de datos y esta transmisión es posible por:

1. Los avances de digitalización de imágenes y compresión de las misma

2. Crecimiento de Redes de datos

3. Desarrollo de equipos de redes digitales (Satélites, TDT, Televisión digital por cable, DVD,etc)

Vigilancia IP

Una grande aplicación del video IP, son los sistemas de seguridad y vigilancia, existen software que han remplazado a los sistemas analógicos tradicionales (CCTV) y los superan ampliamente.[1]

Los Sistemas de Vigilancia IP, son aquellos en que las imágenes y audio son capturados por las cámaras y micrófonos, se comprimen y transmiten por una red de datos Local o Internet (LAN / WAN) y pueden ser acezados desde uno o varios puntos en cualquier lugar del mundo mediante computadoras convencionales (o hardware especialmente diseñado) para descomprimir los datos, visualizarlos, analizarlos, grabarlos y hasta generar acciones de manera automática en respuesta a diferentes eventos pre-definidos o a voluntad de un operador.[8]

Los sistemas de vigilancia IP nos ofrece:

1. Mejora la calidad de video con respecto a los sistemas analógicos CCTV

2. Se puede adaptar a cualquier infraestructura y nos reduce costos por las opciones que estas cámaras nos ofrecen

3. Existen software avanzados para el monitoreo desde una PC o un dispositivo móvil

4. Permite acceder al video desde cualquier lugar de la Red

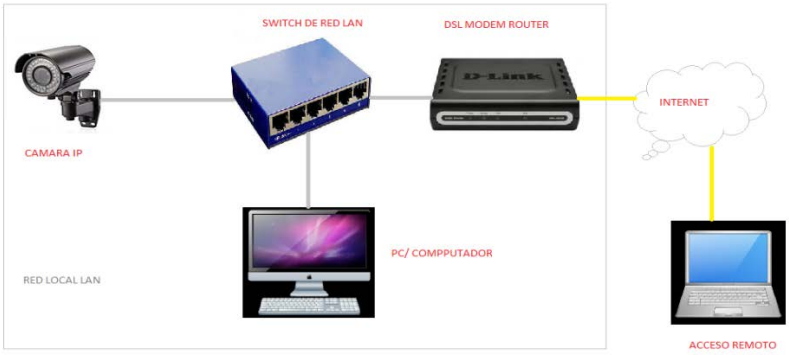


Fig. 2.1 Modelo de vigilancia IP

Un detalle importante dentro de los sistemas de Vigilancia IP es que no solo involucran video sino también audio, y el audio puede ser bi-direccional, es decir: en una Estación de monitoreo se puede escuchar las conversaciones y sonidos generados en los locales donde están las cámaras y micrófonos así como el operador puede hablar a individuos que están en el sitio que se encuentran las cámaras.

Entre los elementos que componen un Sistema de Vigilancia IP merita resaltar:

1. Las Cámaras IP
2. Servidores de Video
3. Decodificadores de Video IP
4. Grabadores Digitales de Red
5. Software Inteligente para Centrales de Monitoreo

Diferencia entre el sistema de vigilancia analógico CCTV y vigilancia IP

En los Sistemas de Vigilancia convencionales (CCTV) el video análogo que sale de las Cámaras viaja por cable coaxial o UTP hasta el dispositivo de grabación, distribución, conmutación o visualización según sea el caso, pero en su “viaje” nunca deja de ser “video analógico”. Esto quiere decir que en cualquier punto entre la cámara y el grabador, podríamos literalmente “cortar el cable” para conectarlo a un monitor análogo y ver el video. [8]

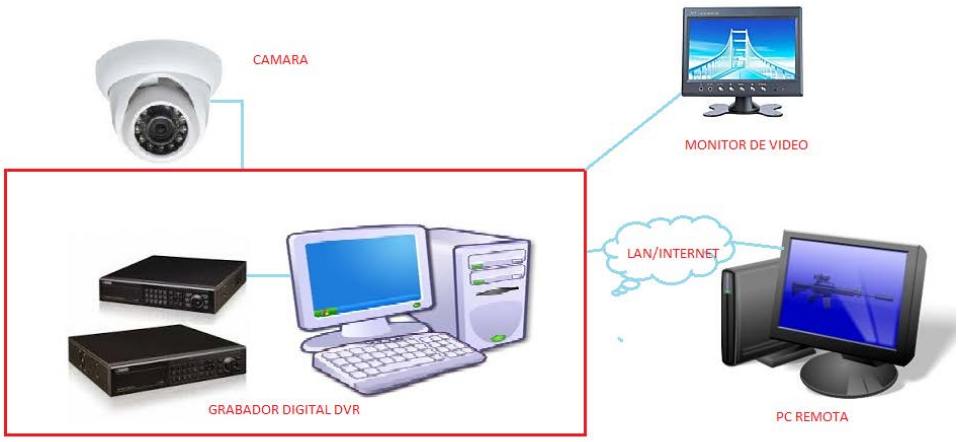


Fig. 2.1.1 Sistema de Vigilancia CCTV

No se debe confundir el uso de cables de red UTP / STP y balun de video (adaptadores de impedancia) para transportar el video analógico con un sistema IP; pues aunque en este caso se utiliza el mismo tipo de cable, la información que viaja por los cables en un sistema IP es completamente digital, o sea: “datos”, y se requiere de Computadoras o algún hardware especialmente preparado para “Decodificar” ese flujo de información y volverlo a convertir en “Video”. [8]

A diferencia de los sistemas de vídeo analógicos convencionales, la Vigilancia IP no requiere de un cableado punto a punto por cada cámara pues las redes de datos que son su medio de transporte, llevan el video, el audio y las señales de control a través de una estructura nódulo-

modular, no solo distinta, sino también más eficiente, conveniente y versátil para las instalaciones y futuras expansiones.[8]

Ejemplo de Sistema IP aplicado al uso Doméstico:

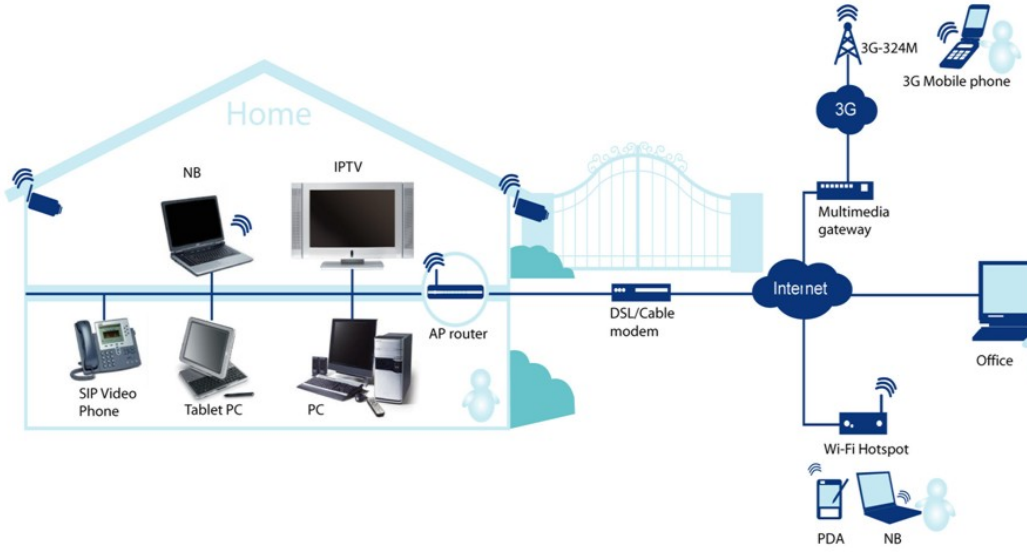


Fig. 2.1.2 Sistema de vigilancia en casas

2.2 Aspectos de la gestión de red enfocada a la seguridad

La gestión de la Red es la acción u operación de técnicas para mantener una red operativa segura y eficiente, que se puede monitorear a todo momento sin ningún problema durante la ejecución ya sea esta una red LAN o WAN. [3]

Las redes definidas por software (SDN), nos permite la programabilidad del control de red y en las estrategias de seguridad SDN nos ofrece un alto nivel de análisis de paquetes, monitoreo de red y control de tráfico que nos ayudara a prevenir ataques en nuestra red.

2.3 Sistemas de vigilancia mediante cámaras.

Son sistemas de vigilancia con cámaras IP, seguridad electrónica, estos sistemas de vigilancia son en tiempo real o pueden ser configurados sus parámetros para grabar dependiendo de la necesidad del usuario, también nos ofrecen componentes de seguridad perimetral, supervisión de controles de acceso y reducción de riesgos de robo esto que puede tener acceso desde una PC o dispositivo móvil.

Estas cámaras vienen con varias opciones como el sensor de movimiento y estas cámaras de vigilancia pueden ser monitoreadas desde un dispositivo móvil.

2.3.1 Las cámaras de seguridad y sus funciones.

Los sistemas de vigilancia IP pueden ser utilizadas en muchas situaciones, desde una residencia local hasta un sistema multinacional. [8]

Mercados donde son utilizados los sistemas de vigilancia IP, estos son:

Educación

Estas son implementadas para la seguridad interna y de áreas desprotegidas tanto en Escuelas, Colegios y Universidades, para dar un valor extra a estas instituciones. [8]

Transporte

Estas son implementadas en los sistemas de tráfico, radares de exceso de velocidad, vigilancia en buses, vigilancia en taxis, estaciones de metro, vigilancia de peajes en carreteras, etc.

Los sistemas IP pueden ser incluso inalámbricos sin dejar de ser efectivos, así como pueden incorporar funciones de inteligencia como reconocimiento de rostro, controles de exceso de velocidad, detección de objetos abandonados, y otras aplicaciones. [8]

Bancos

Se pueden implementar las aplicaciones tradicionales de seguridad en bancos principales y hasta sucursales. Estos sistemas de vigilancia de cámara de seguridad en los bancos también son utilizados para proteger a los clientes, personal del banco y cajeros automáticos (ATM).

También se puede usar tecnología en pantallas HD, dispositivos de almacenamiento de red que estas sean compatibles con cámaras de seguridad IP. [8]

Estos sistemas de cámaras de vigilancia nos ofrece desarrollar Centrales de Monitoreo donde una institución bancaria puede monitorear todas las sucursales.

Esta aplicación es muy importante ya que no solo se puede ver el video “en vivo” de cualquier cámara instalada en cualquier sucursal,

sino que se puede grabar este video, buscar información grabada con anterioridad, hacer backups (copia información total o parcial del disco duro), etc.

Gobierno

Este sistema de vigilancia es utilizado en edificios Gubernamentales, Municipios, Ministerios, Ares Turísticas, etc. Todos estos tienen un servicio por cámaras como por ejemplo en nuestro país tiene el servicio integrado ECU 911, que son las cámaras de video vigilancia.

Comercios minoristas y centros Comerciales

Este sistema de cámaras de vigilancia IP son utilizados en negocios pequeños y Centros Comerciales estos tienes sistemas de monitoreo centralizados de varias sucursales para su seguridad interna. En los centros Comerciales se ponen este sistema de vigilancia por cámara en estacionamientos para la seguridad de los carros y evitar los robos de estos, en los locales también se implementa este sistema de vigilancia para supervisión de las personas que están en el local y evitar robos y en caso de los Súper Mercados ponen más de una cámara para el monitoreo local o remoto de este. [8]

Industrial

Un amplio uso específico en el control de los procesos de fabricación, los sistemas de logística, transporte, control de Calidad, evitar robos internos y supervisar la integridad de los inventarios. Además obviamente se benefician de las funciones complementarias que son integrables a esta tecnología como su posibilidad de monitoreo centralizado de varias sucursales de un mismo negocio a nivel mundial. [8]

2.3.2 Aplicaciones dentro de pequeñas empresas.

El sistema de vigilancia de cámaras IP es muy utilizado en pequeñas empresas, oficinas, hoteles, etc. Estas cámaras de seguridad pueden dar un monitoreo local o remoto, esto ayudara al monitoreo del personal de la empresa, áreas de mayor seguridad y evitar robos. Estas cámaras pueden ser monitoreadas desde una PC o un dispositivo móvil.

Las aplicaciones que este sistema de cámaras de seguridad nos puede ofrecer en pequeñas empresas pueden ser:

1. Video vigilancia IP
2. Una instalación muy flexible para cubrir todos los ángulos

3. Almacenamiento accesible y seguro
4. Monitoreo remoto desde cualquier PC o dispositivo móvil

2.3.4 Vulnerabilidades.

Como todo sistema, siempre presenta debilidades en el sistema de funcionamiento a causa uno o más factores. El objetivo de este proyecto es brindar mediante pruebas optimizar el uso de cámaras de seguridad para reducir costos de mantenimiento y control del mismo.

A continuación nombraremos algunas de las razones por las cuales un sistema de vigilancia podría ser vulnerable:

- Falta de personal que realice monitoreo todo el día: Este problema podría darse debido al alto costo que representa tener un guardia de seguridad o una persona encargada del monitoreo de cámaras debido siendo una empresa pequeña o mediana estos recursos podrían bien usarse en otros temas. [5]
- Falta de almacenamiento de imágenes y videos en un dispositivo: Este problema se da debido a que muchas veces una empresa o negocio no cuenta con un equipo de almacenamiento de

información de gran capacidad debido a su costo de mantenimiento y recuperación de las mismas. [5]

2.3.5 Uso óptimo de recursos del sistema.

Para optimizar y reducir costos al momento de aprovechar el máximo el sistema de cámaras, podría implementarse pequeñas funcionalidades que vienen incluidas en ciertas cámaras con lo cual nos evitaríamos hacer uso de un recurso económico para poder pagar a alguien que nos monitoree las cámaras.

Una de las mejores maneras de hacer uso óptimo es implementar el sensor del movimiento que ahora vienen implementados en la mayorías de las cámaras y este al activarse que empiece a grabar o tomar una foto de donde se lo enfoque y a su vez esta foto pueda enviarse o que se pueda activar una alarma y avisar a un correo electrónico.

Otra función que poseen las cámaras de vigilancia hoy en día es la capacidad de visión nocturna y a su vez proporciona las mismas funciones que con visión normal.

Gracias a los diferentes tipos de software que hay en el mercado ya sea de control o monitoreo, los sistemas de cámaras pueden ser observados y controlados desde la mayoría de dispositivos ya sea una

computadora o cualquier tipo de dispositivos móviles en donde el software de monitoreo pueda ser instalado.

2.4 Protocolo de transferencia de archivos (FTP).

El protocolo FTP (Protocolo de transferencia de archivos) es un protocolo para transferir de manera eficaz archivos. [7]

Actualmente el protocolo de transferencia de archivos (FTP), está definido por RFC 959.

La implementación de FTP se remonta a 1971 cuando se pudo desarrollar un sistema de archivos entre equipos del Instituto Tecnológico de Massachusetts. Desde entonces, varios documentos de RFC han mejorado este protocolo básico, pero las innovaciones con más importancias lo llevaron a cabo en julio de 1973. [9]

El protocolo de transferencia de archivos (FTP), aunque puede ser utilizado por un usuario en un terminal, está diseñado principalmente para ser usado por programas. [7]

Historia

El FTP ha pasado por una larga evolución a través de los años. El FTP. Estos incluyen la primera propuesta de mecanismos para

transferencia de ficheros de 1971, que se desarrolló para su uso en servidores del M.I.T. (RFC 114), más los comentarios y discusiones del RFC 141. [7]

El RFC 172 proporcionó un protocolo orientado al nivel de usuario para transferir ficheros entre ordenadores (incluyendo IMP's terminales). Una revisión de este plasmada en el RFC 265, inició una revisión adicional, mientras que el RFC 281 sugirió más cambios. El uso de una transacción para elegir el tipo de datos se propuso en el RFC 294 en enero de 1982. [7]

El RFC 354 dejó obsoletos los RFCs 264 y 265. El Protocolo de Transferencia de Ficheros se definió en este momento como un protocolo para transferencia de ficheros entre ordenadores conectados a la red ARPANET, señalando como función principal del FTP la transferencia de ficheros fiable y eficiente entre ordenadores y permitiendo el uso adecuado de las características de almacenamiento remotas. El RFC 385 siguió comentando errores, enfatizó algunos puntos y añadió características al protocolo, mientras que el RFC 414 fue un informe sobre los servidores FTP que estaban funcionando. El RFC 430, que salió a la luz en 1973 (entre otros muchos RFCs) presentó más comentarios sobre el FTP.

Finalmente, se publicó un documento "oficial" sobre el FTP como RFC 454. [7]

Hacia julio de 1973, se hicieron considerables cambios a las últimas versiones del FTP, pero la estructura general permaneció igual. El RFC 542 se publicó como una nueva especificación "oficial" para reflejar esos cambios. Sin embargo, muchas implementaciones basadas en anterior especificaciones no se actualizaron. [7]

Las últimas versiones del FTP. El RFC 691 presentó una pequeña revisión del RFC 686, referente al tema de ficheros para imprimir. [7]

Esta edición de la especificación FTP está dirigida a la corrección de pequeños errores en la documentación, a mejorar la explicación de algunas características del protocolo, y a añadir algunas nuevas. [7]

2.4.1 Generalidades

- **La función del protocolo FTP**

El protocolo FTP define la manera en que los datos deben ser transferidos a través de una red TCP/IP. [9]

El objetivo del protocolo FTP es:

- Permitir que equipos remotos puedan compartir archivos
- Permitir la independencia entre los sistemas de archivo del equipo del cliente y del equipo del servidor
- Permitir una transferencia de datos eficaz

El modelo FTP

El protocolo FTP está incluido dentro del modelo cliente-servidor, es decir, un equipo envía órdenes (el cliente) y el otro espera solicitudes para llevar a cabo acciones (el servidor). [9]

Durante una conexión FTP, se encuentran abiertos dos canales de transmisión:

- Un canal de comandos (canal de control)
- Un canal de datos

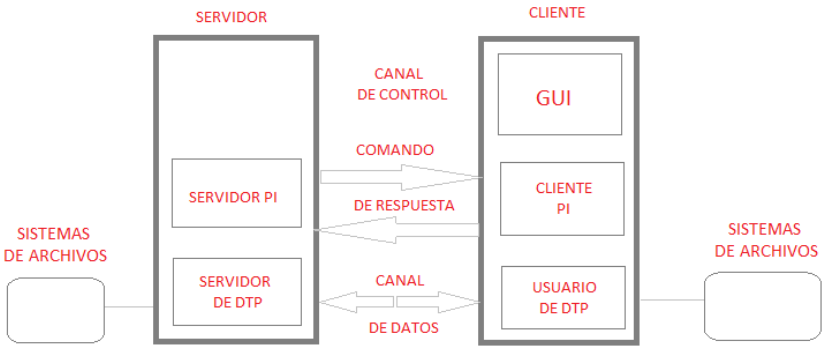


Fig. 2.4.1.1 Conexión FTP

Por lo tanto, el cliente y el servidor cuentan con dos procesos que permiten la administración de estos dos tipos de información:

- DTP (Proceso de transferencia de datos) es el proceso encargado de establecer la conexión y de administrar el canal de datos. El DTP del lado del servidor se denomina SERVIDOR DE DTP y el DTP del lado del cliente se denomina USUARIO DE DTP. [9]
- PI (Intérprete de protocolo) interpreta el protocolo y permite que el DTP pueda ser controlado mediante los comandos recibidos a través del canal de control. Esto es diferente en el cliente y el servidor:
  - El SERVIDOR PI es responsable de escuchar los comandos que provienen de un USUARIO PI a través del canal de control en un

puerto de datos, de establecer la conexión para el canal de control, de recibir los comandos FTP del USUARIO PI a través de éste, de responderles y de ejecutar el SERVIDOR DE DTP. [9]

- El USUARIO PI es responsable de establecer la conexión con el servidor FTP, de enviar los comandos FTP, de recibir respuestas del SERVIDOR PI y de controlar al USUARIO DE DTP, si fuera necesario.

Cuando un cliente FTP se conecta con un servidor FTP, el USUARIO PI inicia la conexión con el servidor de acuerdo con el protocolo Telnet. El cliente envía comandos FTP al servidor, el servidor los interpreta, ejecuta su DTP y después envía una respuesta estándar. Una vez que se establece la conexión, el servidor PI proporciona el puerto por el cual se enviarán los datos al Cliente DTP. El cliente DTP escucha el puerto especificado para los datos provenientes del servidor. [9]

Es importante tener en cuenta que, debido a que los puertos de control y de datos son canales separados, es posible enviar comandos desde un equipo y recibir datos en otro. Entonces, por ejemplo, es posible transferir datos entre dos servidores FTP mediante el paso indirecto por un cliente para enviar instrucciones de control y la

transferencia de información entre dos procesos del servidor conectados en el puerto correcto.

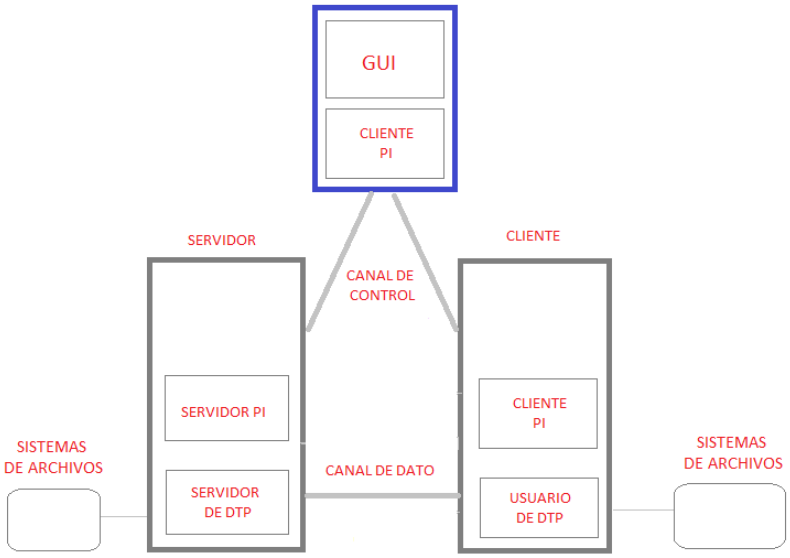


Fig. 2.4.1.2 Conexión FTP canales de control abiertos

En esta configuración, el protocolo indica que los canales de control deben permanecer abiertos durante la transferencia de datos. De este modo, un servidor puede detener una transmisión si el canal de control es interrumpido durante la transmisión.

Los comandos FTP

Toda comunicación que se realice en el canal de control sigue las recomendaciones del protocolo Telnet. Por lo tanto, los comandos FTP son cadenas de caracteres Telnet (en código NVT-ASCII) que

finalizan con el código de final de línea Telnet (es decir, la secuencia <CR>+<LF>, Retorno de carro seguido del carácter Avance de línea indicado como <CRLF>). [9]

Si el comando FTP tiene un parámetro, éste se separa del comando con un espacio (<SP>). [9]

Los comandos FTP hacen posible especificar:

- El puerto utilizado
- El método de transferencia de datos
- La estructura de datos
- La naturaleza de la acción que se va a realizar (Recuperar, Enumerar, Almacenar, etc.)

Existen tres tipos de comandos FTP diferentes:

- Comandos de control de acceso
- Comandos de parámetros de transferencia
- Comandos de servicio FTP

Las respuestas FTP

Las respuestas FTP garantizan la sincronización entre el cliente y el servidor FTP. Por lo tanto, por cada comando enviado por el cliente, el servidor eventualmente llevará a cabo una acción y sistemáticamente enviará una respuesta. [9]

Las respuestas están compuestas por un código de 3 dígitos que indica la manera en la que el comando enviado por el cliente ha sido procesado. Sin embargo, debido a que el código de 3 dígitos resulta difícil de leer para las personas, está acompañado de texto (cadena de caracteres Telnet separada del código numérico por un espacio). [9]

Los códigos de respuesta están compuestos por 3 números, cuyos significados son los siguientes:

- El primer número indica el estatuto de la respuesta (exitosa o fallida)
- El segundo número indica a qué se refiere la respuesta.
- El tercer número brinda un significado más específico (relacionado con cada segundo dígito).

2.4.2 Niveles en los que actúa FTP.

El nivel en el cual actúa FTP es en el nivel de aplicación, aquí se describirá como actúa FTP en la capa de aplicación.

En una sesión de FTP, el usuario está sentado frente a un host local y quiere transferir archivos hacia o desde un host remoto. Para que el usuario acceda a la cuenta remota, el usuario debe proporcionar una identificación de usuario y una contraseña. Después de proporcionar esta información de autorización, el usuario puede transferir archivos desde el sistema de archivos local en el directorio y viceversa. El usuario interactúa con FTP a través de un agente usuario FTP. El primer usuario que proporciona el nombre de host de la máquina remota, haciendo que el proceso de cliente FTP en la máquina local para establecer una conexión TCP con el servidor de FTP en el host remoto. Después, el usuario proporciona la identificación de usuario y contraseña, que una enviada a través de la conexión TCP como parte de los comandos FTP. Una vez que el servidor ha autorizado al usuario, el usuario copia de uno o más archivos almacenados en el sistema de archivos local en el sistema de baldosas remoto (o viceversa). [3]

HTTP y FTP son la transferencia de archivos protocolos que tienen muchas características en común, por ejemplo, ambos se ejecutan en la parte superior de la TCP. Sin embargo, los dos protocolos de la capa de aplicación tienen algunas diferencias importantes. La diferencia más notable es que FTP utiliza dos conexiones TCP paralelas para transferir un archivo, una conexión de control y una conexión de datos. La conexión de control se utiliza para enviar información de control entre los dos ejércitos - la información como la identificación de usuario, contraseña, los comandos para cambiar el directorio remoto, y los comandos de "put" y "get" los archivos. La conexión de datos se utiliza para enviar realmente un archivo, puesto que FTP utiliza una conexión de control independiente, se dice FTP para enviar su información de control fuera de banda. Vamos a ver que el protocolo RTSP, que se utiliza para controlar la transferencia de los medios continuos, como audio y video, también envía su información de control fuera de banda. HTI'P, como se recordará, envía la solicitud y las líneas de encabezado de respuesta en la misma conexión TCP que transporta el archivo transferido en sí. Por esta razón, se dice HTTP para enviar su información de control en banda. En la siguiente sección veremos que SMTP, el protocolo principal de correo electrónico, también se envía información de control en banda. [3]

2.4.3 Principales aplicaciones de FTP.

Las aplicaciones de FTP se basan en varios tipos de software que pueden estar en servidores y computadores en donde el sistema operativo puede que incluya las características para el funcionamiento o de un software adicional que incluya las funcionalidades de FTP. [10]

Puertos múltiples, modos múltiples

A diferencia de la mayoría de los protocolos utilizados en Internet, FTP requiere de múltiples puertos de red para funcionar correctamente. Cuando una aplicación cliente FTP inicia una conexión a un servidor FTP, abre el puerto 21 en el servidor — conocido como el puerto de comandos. Se utiliza este puerto para arrojar todos los comandos al servidor. Cualquier petición de datos desde el servidor se devuelve al cliente a través del puerto de datos. El número de puerto para las conexiones de datos y la forma en la que las conexiones son inicializadas varía dependiendo de si el cliente solicita los datos en modo activo o en modo pasivo. [10]

A continuación se describen estos modos:

Modo activo

El modo activo es el método original utilizado por el protocolo FTP para la transferencia de datos a la aplicación cliente. Cuando el cliente FTP inicia una transferencia de datos, el servidor abre una conexión desde el puerto 20 en el servidor para la dirección IP y un puerto aleatorio sin privilegios (mayor que 1024) especificado por el cliente. Este arreglo implica que la máquina cliente debe poder aceptar conexiones en cualquier puerto superior al 1024. Con el crecimiento de las redes inseguras, tales como Internet, es muy común el uso de cortafuegos para proteger las máquinas cliente. Debido a que estos cortafuegos en el lado del cliente normalmente rechazan las conexiones entrantes desde servidores FTP en modo activo, se creó el modo pasivo. [10]

Modo pasivo

La aplicación FTP cliente es la que inicia el modo pasivo, de la misma forma que el modo activo. El cliente FTP indica que desea acceder a los datos en modo pasivo y el servidor proporciona la dirección IP y el puerto aleatorio, sin privilegios (mayor que 1024) en el servidor.

Luego, el cliente se conecta al puerto en el servidor y descarga la información requerida. [10]

Cortafuegos en el lado del cliente con las conexiones de datos, también puede complicar la administración del cortafuego del lado del servidor. Una de las formas de limitar el número de puertos abiertos en el servidor y de simplificar la tarea de crear reglas para el cortafuegos del lado del servidor, es limitando el rango de puertos sin privilegios ofrecidos para las conexiones pasivas. [10]

Usar un servidor FTP ofrece ventajas propias. Por un lado, un usuario puede utilizar un programa para realizar una carga masiva a un servidor, sin tener que preocuparse por volver a examinar archivos y cargarlos nuevamente usando un formulario. Las descargas también pueden realizarse en masa. Por desgracia, un servidor FTP todavía requiere un cliente FTP para ser usado, y el uso de uno podría ser particularmente incómodo para aquellos que solo desean cargar una imagen o dos. [10]

En el caso de aplicaciones de seguridad que incluyan cámaras de vigilancia, un servidor FTP es ideal para el almacenamiento para imágenes y videos. [10]

2.4.4 Ventajas del uso de FTP

Usar un servidor FTP ofrece ventajas propias. Por un lado, un usuario puede utilizar un programa para realizar una carga masiva a un servidor, sin tener que preocuparse por volver a examinar archivos y cargarlos nuevamente usando un formulario. Las descargas también pueden realizarse en masa. Por desgracia, un servidor FTP todavía requiere un cliente FTP para ser usado, y el uso de uno podría ser particularmente incómodo para aquellos que solo desean cargar una imagen o dos.

En el caso de aplicaciones de seguridad que incluyan cámaras de vigilancia, un servidor FTP es ideal para el almacenamiento para imágenes y videos.

2.5 Protocolo simple de transferencia de correo (SMTP).

Es un protocolo para la transferencia de correo electrónico, que es utilizado para el intercambio de correos electrónicos, desde una PC o cualquier dispositivo móvil.

2.5.1 Generalidades

Con el protocolo SMTP podemos conocer el funcionamiento de transporte de correo electrónico, SMTP tiene muchas ventajas y funciones y están implementadas y dependerán de cada servidor, estas son las llamadas ¨ extensión de servicios ¨.

El protocolo SMTP rige la transferencia de e-mails salientes desde el emisor al servidor de e-mails MDA (Agente de entrega de correo).

Podemos decir que e-mail, es el servicio de red más conocido ya que nos podemos comunicar de una manera simple y con grandes velocidades. Los e-mail requieren servicios y aplicaciones, estos protocolos de capa de aplicaciones pueden ser aplicadas por ejemplo como protocolo de oficina de correos como POP (Protocolo de oficina de correo) y SMTP (Protocolo simple de transferencia de correo), podemos decir que con estos dos protocolos POP y SMTPN junto a HTTP, estos protocolos definen procesos de cliente servidor.

Debemos saber que el protocolo POP, este protocolo es utilizado para la recepción del correo electrónico y el protocolo SMTP en cambio este es utilizado para él envió de correos electrónicos, cada vez que enviamos un correo electrónico estamos utilizando el protocolo SMTP,

2.5.2 Niveles en los que actúa SMTP

Cuando existe una conversación de servicios de correo electrónico para ello debemos disponer de un ISP, que para la explicación del tema podemos dar un ejemplo podría ser un ISP llamado mccartney@hotmail.com y también se conoce el correo del receptor que para nuestro ejemplo puede ser un ISP llamado lennon@gmail.es . Así que uno de estos dos personajes podría comenzar una conversación desde el correo electrónico como se puede mostrar en el siguiente mensaje:

From: mccartney@hotmail.com

To: lennon@gmail.es

Subject: Vamos hacer música

Para este ejemplo lo primero que lo primero que hace el emisor en este caso mccartney al pulsar el botón de envío este se conectara al servidor SMTP de Hotmail, para esto el emisor mccartney debe configurar su cliente de correo, este debe introducir datos como:

La dirección del servidor POP3 (Protocolo de oficina versión tres) de Hotmail y la dirección de servicio SMTP (Protocolo simple de transferencia de correo) de Hotmail, con esto sabemos dónde se deberá conectar. [2]

La conclusión que podemos decir es que nuestro cliente de correo del emisor no debe preocuparse de como localizar el servidor de Gmail, en donde se encuentra la cuenta del correo electrónico del receptor lennon sino que se delega por completo en el servidor de SMTP para lo cual fue configurado el de Hotmail

Envío de correo electrónico

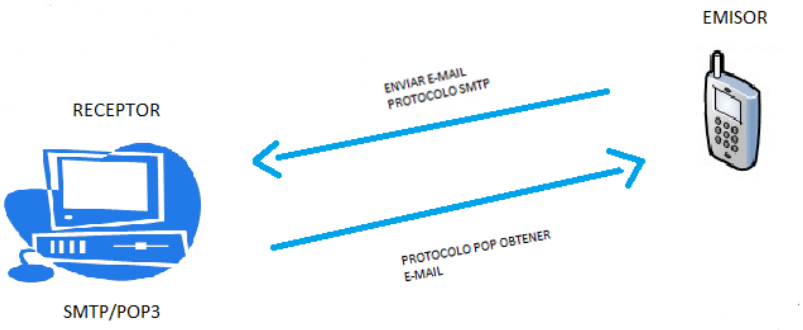


Fig. 2.5.2 Envío de un correo electrónico mediante SMTP y recepción de correo electrónico mediante POP3. [13]

El cliente SMTP estable una conexión TCP con el puerto 25 del servidor SMTP.

SMTP utiliza mensaje en formato ASCII, si el mensaje no tiene caracteres ASCII o binarios, tiene que ser codificados en MIME (Multipur pose Internet extensión). Permite enviar contenido distinto de texto ASCII en mensaje de correo electrónico. [2]

Nivel de aplicación o copa de aplicación es el séptimo nivel del modelo OSI.

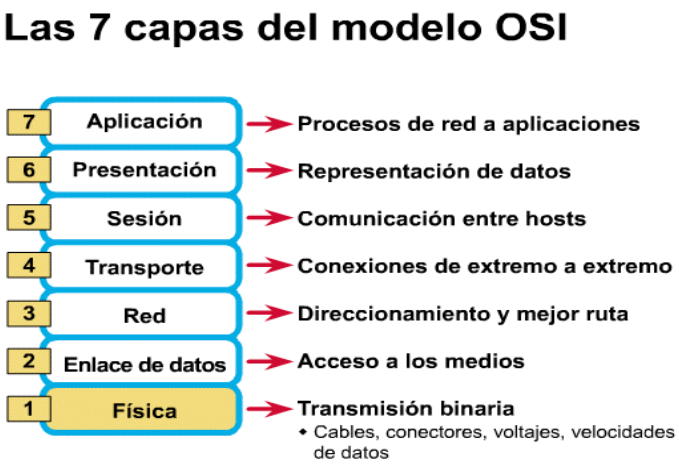


Fig. 2.5.3 Pila OSI [14]

EL NIVEL DE APLICACIÓN (LIBRO RC BLOQUE 2 TEMA 3) REFERENCIA

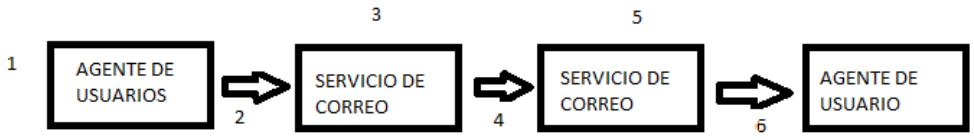


Fig. 2.5.4 Nivel de Aplicación

PROCESO DE ENVÍO DE UN MENSAJE DE CORREO ELECTRÓNICO:

1. El cliente, mediante su lector de correo crea el mensaje.

2. El lector envía el mensaje al servicio de correo del emisor, se almacena en la cola de mensajes.

3. El servidor de correo (actuando como cliente SMTP) se conecta al servidor de correo del remitente.

4. El cliente SMTP envía el mensaje.

5. El servidor SMTP recibe el mensaje y lo almacena en el buzón de destinatario.

6. El destinatario utiliza su lector de correo para obtener el mensaje.

SMTP

COMANDOS BASICOS

HELO: El cliente se identifica mediante este comando. Debe incluir su nombre dominio absoluto.

MAIL: Identifica al remitente del mensaje.

RCPT: Identifica al destinatario del mensaje.

DATA: Se incluye el contenido del mensaje (finalizar con un ¨.¨).

QUIT: Finaliza el intercambio de correo.

MÁS COMANDOS

RESET: Ahora el intercambio de correo y los dos extremos se resetean.

VRFY: El cliente consulta al servidor sobre una dirección de correo.

NOOP: Fuerza al servidor a responder con el código de respuesta 200 (OK).

TURN: Cliente y servidor se intercambian. [2]

2.5.3 Principales aplicaciones de SMTP

Servicio de aplicaciones SMTP

En la interface de correo local siempre existe una cola de entrada y una de salida y las partes de cliente-servidor del SMTP y estas tienen dos funciones:

- El cliente da inicio y va existir una transferencia de correo hacia otro sistema

- El servidor es el que recibe el correo del exterior

En el correo local cada usuario se le asigna una casilla y con esta casilla podremos depositar o recupera los correos.

La casilla consta de dos partes:

- Parte Local: a esta parte se la conoce como el nombre del usuario
- Parte Global: Es la identidad del computador y es única en todo el internet y esta tiene varios campos y formatos depende del tipo de institución como gobierno, militares, empresa de telecomunicaciones, comercial, etc.

La transferencia de correo electrónico tiene dos aspectos importantes:

- El formato del mail: Este formato deberá ser interpretado por todos los sistemas involucrados, de la misma forma tendrá una cabecera y un cuerpo
- El protocolo SMTP: Este protocolo que es usado para el envío de correo de una maquina o dispositivo móvil o a otro ya sea equipo o dispositivo móvil que soporte correos electrónicos (SMART PHONE).

El encabezamiento debe ser:

TO: Nombre del destinatario

FROM: Nombre del remitente

CC: Copias para

SUBJECT: Asunto a tratar

DATE: Fecha

ENCRYTED: Puntero de encriptación

Este encabezamiento incluyendo nombres de destinatarios y asuntos estarán en texto simple, para enviar un correo, el cliente SMTP debe obtener primero la dirección IP del dispositivo móvil o computador. [2]

2.5.4 Ventajas del uso de SMTP

El Protocolo de simple transferencia de correo tiene muchas ventajas de uso aquí especificaremos algunas ventajas de su uso:

1. Es un protocolo servidor a servidor para correo electrónico y no cliente

2. Este protocolo nos permite crear uno o más direcciones de correos electrónicos en nuestro servidor de correo y se puede poner cualquier nombres o alias como por ejemplo jmchoclito@hotmail.com

3. Protocolo para recibir correos electrónicos basados en texto e intercambiar correos

4. Si tenemos un router lo mejor es usar el protocolo SMTP

5. Este protocolo que funciona en línea a través de otro protocolo TCP/IP hace que el mensaje recibido sea siempre satisfactorio al servidor del destinatario.

2.6 Protocolo TCP/IP

Protocolo de Control de Transmisión es también dominado como Internet Model, nos describe un conjunto de guías generales de diseño e implementación de protocolos de red específica, que cualquier equipo se pueda comunicarse en una red.

2.6.1 Generalidades

TCP/IP (Protocolo Control de Transmisión/Protocolo de Internet). Este es un sistema de protocolo que dan posibles servicios FTP, e-mail y otras computadoras que no son de la misma red. [3]

El Protocolo de Transmisión (TCP) este protocolo le permite a dos propietarios establecer una conexión, TCP garantiza la entrega de datos esto quiere decir que los datos no se pierden en la respectiva transmisión y también garantiza que los paquetes sean entregados en el orden que estos fueron enviados. [3]

El Protocolo de internet (IP) utiliza dirección que son series de cuatro números octetos (byte) como por ejemplo: 79.5.153.63. Los protocolo como HTTP y FTP se basan y utilizan TCP/IP. [3]

El TCP / IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. TCP / IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa. [3]

COMO FUNCIONA TCP/IP

Una red TCP/IP transfiere datos mediante el ensamblaje de bloques de datos en paquetes, cada paquete comienza con una cabecera que contiene información de control; tal como la dirección del destino, seguido de los datos. Cuando se envía un archivo por la red TCP/IP,

su contenido se envía utilizando una serie de paquetes diferentes. El Internet protocol (IP), un protocolo de la capa de red, permite a las aplicaciones ejecutarse transparentemente sobre redes interconectadas. Cuando se utiliza IP, no es necesario conocer que hardware se utiliza, por tanto ésta corre en una red de área local. [3]

El Transmisión Control Protocol (TCP); un protocolo de la capa de transporte, asegura que los datos sean entregados, que lo que se recibe, sea lo que se pretendía enviar y que los paquetes que sean recibidos en el orden en que fueron enviados. TCP terminará una conexión si ocurre un error que haga la transmisión fiable imposible.

ARQUITECTURA DEL PROTOCOLO TCP/IP

En la gráfica 2.6.1 podemos observar que los niveles del protocolo TCP/IP no coinciden exactamente con las siete capas del modelo OSI ya que el protocolo TCP/IP fue creado antes que el modelo de capa OSI. [3]

En la arquitectura del Protocolo TCP/IP los datos que son enviados a la red recorren la pila del protocolo desde la capa más alta de

aplicación hasta la capa más baja de acceso a red. Cuando son recibidos, recorren la pila del protocolo en sentido contrario.

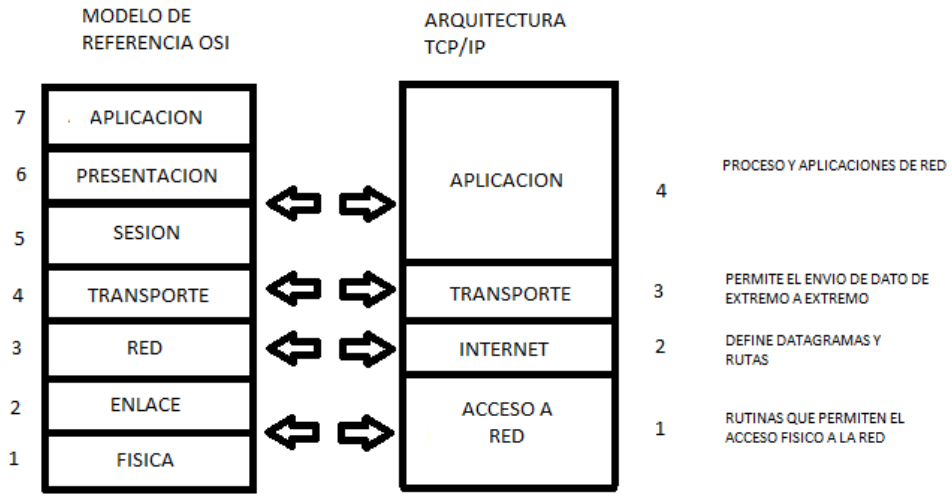


FIG. 2.6.1 CORRESPONDENCIA DEL MODELO OSI CON TCP/IP [15]

ADMINISTRACIÓN TCP/IP

TCP/IP es una de las redes más comunes utilizadas para conectar computadoras con sistema UNIX. Las utilidades de red TCP/IP forman parte de la versión 4, muchas facilidades de red como un sistema UUCP, el sistema de correo, RFS y NFS, pueden utilizar una red TCP/CP para comunicarse con otras máquinas. [3]

Para que la red TCP/IP esté activa y funcionada será necesario:

- Obtener una dirección Internet.
- Instalar las utilidades Internet en el sistema
- Configurar la red para TCP/IP
- Configurar los guiones de arranque TCP/IP
- Identificar otras máquinas ante el sistema
- Configurar la base de datos del o y ente de STREAMS
- Comenzar a ejecutar TCP/IP.

SERVICIOS DE INTERNET A NIVEL DE RED

Un programador que crea programas de aplicación que utilizan protocolos TCP/IP tiene una visión totalmente diferente de una red de redes, con respecto a la visión que tiene un usuario que únicamente ejecuta aplicaciones como el correo electrónico. En el nivel de red, una red de redes proporciona dos grandes tipos de servicios que todos los programas de aplicación utilizan. Aunque no es importante en este momento entender los detalles de estos servicios, no se deben omitir del panorama general del TCP/IP:

- Servicio sin conexión de entrega de paquetes. La entrega sin conexión es una abstracción del servicio que la mayoría de las redes

de conmutación de paquetes ofrece. Simplemente significa que una red de redes TCP/IP rutea mensajes pequeños de una máquina a otra, basándose en la información de dirección que contiene cada mensaje. Debido a que el servicio sin conexión rutea cada paquete por separado, no garantiza una entrega confiable y en orden. Como por lo general se introduce directamente en el hardware subyacente, el servicio sin conexión es muy eficiente. [3]

- Servicio de transporte de flujo confiable. La mayor parte de las aplicaciones necesitan mucho más que sólo la entrega de paquetes, debido a que requieren que el software de comunicaciones se recupere de manera automática de los errores de transmisión, paquetes perdidos o fallas de conmutadores intermedios a lo largo del camino entre el transmisor y el receptor. El servicio de transporte confiable resuelve dichos problemas. Permite que una aplicación en una computadora establezca una "conexión" con una aplicación en otra computadora, para después enviar un gran volumen de datos a través de la conexión como si fuera perramente y directa del hardware. [3]

Muchas redes proporcionan servicios básicos similares a los servicios TCP/IP, pero existen unas características principales que los distingue de los otros servicios:

- Independencia de la tecnología de red. Ya que el TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular. La Internet global incluye una variedad de tecnologías de red que van de redes diseñadas para operar dentro de un solo edificio a las diseñadas para abarcar grandes distancias. Los protocolos TCP/IP definen la unidad de transmisión de datos, llamada datagrama, y especifican cómo transmitir los datagramas en una red en particular.
- Interconexión universal. Una red de redes TCP/IP permite que se comunique cualquier par de computadoras conectadas a ella. Cada computadora tiene asignada una dirección reconocida de manera universal dentro de la red de redes. Cada datagrama lleva en su interior las direcciones de destino para tomar decisiones de ruteo.

- Acuses de recibo punto-a-punto. Los protocolos TCP/IP de una red de redes proporcionan acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aun cuando las dos máquinas no estén conectadas a la misma red física.

- Estándares de protocolo de aplicación. Además de los servicios básicos de nivel de transporte (como las conexiones de flujo

confiable), los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto. Por lo tanto, cuando se diseñan programas de aplicación que utilizan el TCP/IP, los programadores a menudo se encuentran con que el software ya existente proporciona los servicios de comunicación que necesitan. [3]

2.7 Software de configuración y visualización en sistemas de vigilancia.

Fig. 2.7.1 Cámara de vigilancia IP Easyn

DESCRIPCIÓN DEL SOFTWARE DE LA CÁMARA IP DE VIGILANCIA EASYN

El software de la cámara IP de vigilancia easyn tiene una manera muy fácil de ser usada ya que el software fácilmente puede ser instalado en un dispositivo móvil ya sea este una laptop o un androide y a su vez la cámara IP de vigilancia easyn su software puede ser instalada en una PC normal. [11]

El software nos permite configurar varias cámaras con su respectiva dirección IP que esta viene dada en el momento de su instalación, la dirección recomendada de fábrica o la dirección IP que lo vayamos a dar. [11]

El número de cámaras que se puedan configurar en un mismo dispositivo móvil o PC va a depender de donde la cámara IP de vigilancia easyn vaya ser utilizada. [11]

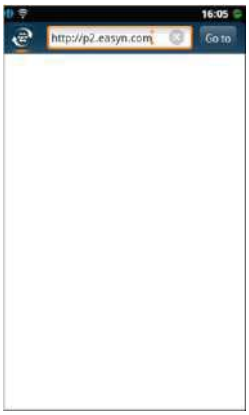
El software de la cámara IP de vigilancia easyn al momento de estar instalada nos da varias opciones ya sea para grabar en todo el tiempo o solo cuando esta detecte un movimiento, que esto es en si lo que hace la cámara IP de vigilancia easyn, el software nos da una opción

para comunicarnos directamente con la persona que esté siendo vigilada por la cámara IP de vigilancia easyn, el software nos permite mover nuestra cámara ya sea de arriba hacia abajo o de izquierda hacia la derecha. Todas estas opciones que nos da el software pueden ser monitoreadas desde nuestra PC o desde el dispositivo móvil que estemos usando. [11]

El software de la cámara IP de vigilancia easyn nos da la facilidad de elegir cualquier navegador para su uso ya sea Explorador de internet, Firefox, Google Chrome y desde un iPhone o androide, y podemos elegir en que navegador vamos usarla si hemos abierto la cámara desde uno de estos navegadores pondremos en la opción que nos da el software el que estemos usando. En el momento de haber escogido la opción de que navegador estamos usando el software de la cámara IP de vigilancia easyn nos pedirá una clave y usuario luego de esto podremos hacer uso de las múltiples opciones ya mencionadas que nos da el software de nuestra cámara IP de vigilancia esyn. [11]

Descargar el software para el dispositivo móvil y su instalación

Buscamos el software para el dispositivo móvil en la dirección http://p2.easyn.com y seleccionamos lo correspondiente. Hay 4 bloques: APP para iPhone, para androide, para PC y el manual.



2.7.2 Fig. Software Para dispositivo móvil

1.- Aquí ponemos App de iPhone como ejemplo

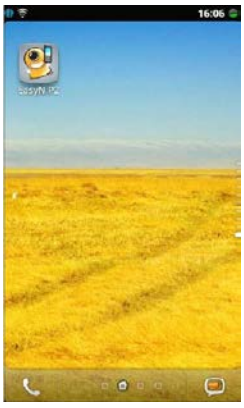


Fig. 2.7.3 App de Iphone

2.- Abrir el App de iPhone después de su instalación

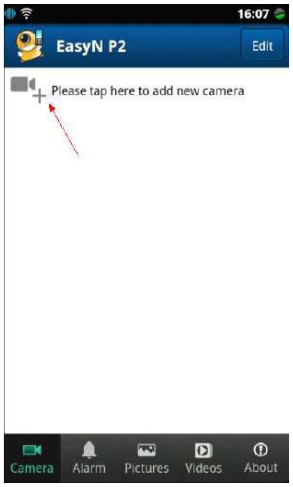


Fig. 2.7.4 App Iphone Instalado

3.- Añadir la cámara IP.

Método 1: El primer paso que se debe hacer es buscar la cámara (el botón buscar). Al salir la ventana de resultados de búsqueda como se indica en la figura de abajo, se debe seleccionar la cámara. Se ponen automáticamente los parámetros de la cámara por defecto. Por ultimo pulsamos el botón de confirmación. [11]

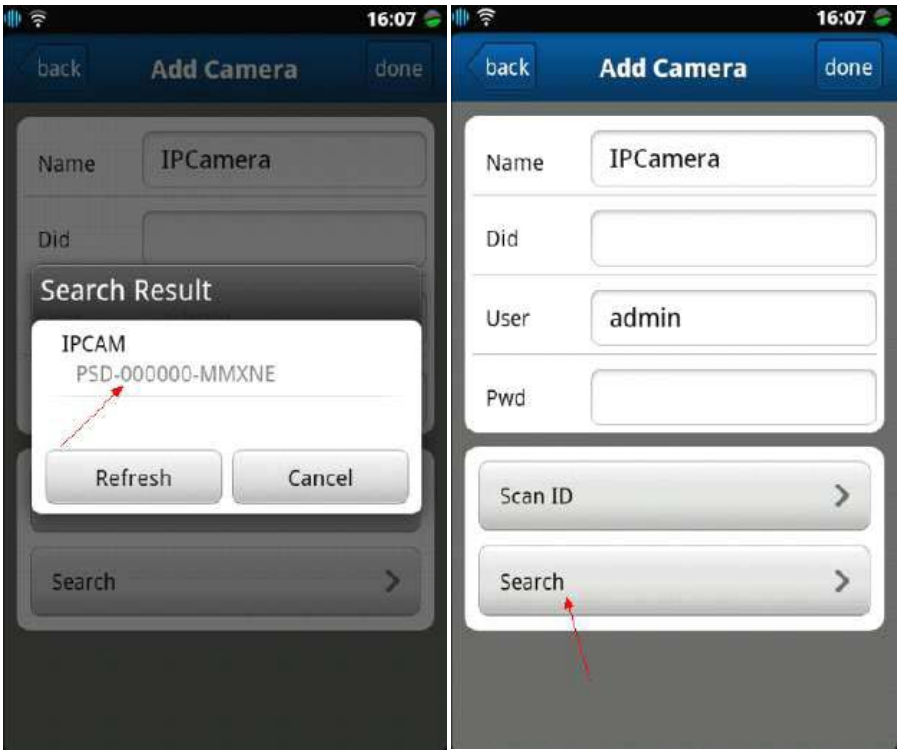


Fig. 2.7.5 Añadir IP cámara en el Iphone

Método 2: Escanear el código de dos dimensiones (Código QR) que viene indicado en la cámara y la de la caja. Pulsar el botón ¨ Scan ID¨ ajustándose el móvil hacia dicho QR. Se lo consigue escanear con éxito se ponen automáticamente los datos de la cámara por defecto en las casillas. Ahora pulsar el botón confirmar. [11]

Fig. 2.7.6 Código QR

Método 3: Con el teclado a mano, poner el número de identificación de las cámaras que vienen indicado en las etiquetas. En este caso, hay que poner en la casilla ¨*Did*¨ dicho número de identificación que también viene indicada en las etiquetas. Poner *admin* en la casilla ¨*User*¨, sin contraseña. Luego pulsar ¨*Done*¨ para confirmarlo. [11]

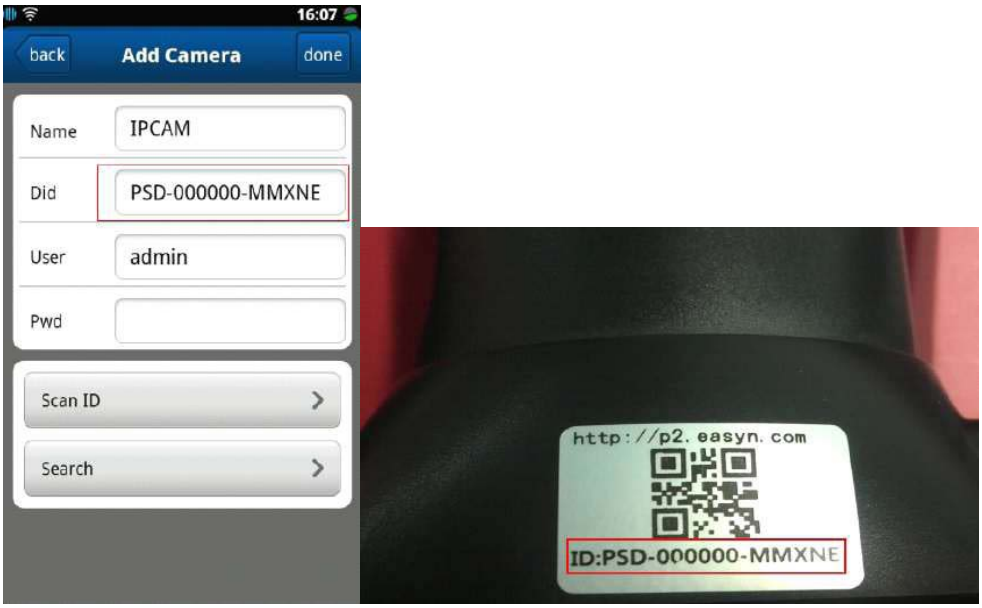


Fig. 2.7.7 Add Camera con ID

Si la cámara se añadió con éxito, debe aparecer lo siguiente:

Fig. 2.7.8 Cámara añadida en el Iphone

4.- Visualizar y controlar la cámara a remoto

Hacer un ¨ click¨ en la opción IPCAM (cámara en línea) para visualizar la imagen.

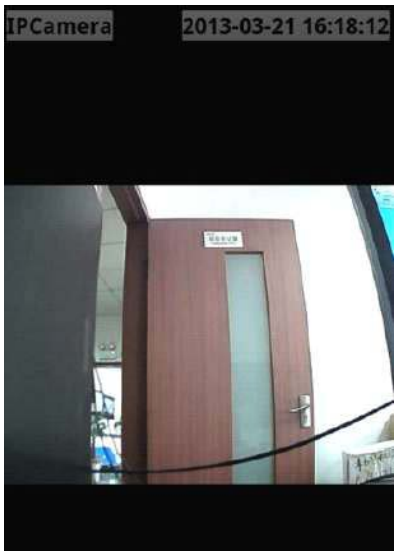


Fig. 2.7.9 Cámara en línea

Al hacer un ¨click¨ en la pantalla nos dará las demás opciones adicionales. En estas opciones se puede grabar, escuchar, sacar fotos, hablar y modificar la calidad visual de las imágenes como su contraste, luminosidad, etc. Para mover la escena basta con deslizar la pantalla. [11]

Fig. 2.7.10 Control de la cámara

2.8 Dispositivos portátiles para control remoto

El software de acceso remoto o también conocido como software de escritorio, este software tiene la capacidad de facilitar la conexión entre dispositivos habilitados para internet múltiple. Esta conexión permite avanzada asistencia técnica de entrega como puede ser las cámaras de seguridad de vigilancia en una casa o empresa.

Este software de acceso remoto puede ser usado en IPhone o en dispositivos androide, el uso de estos programas que permiten al acceso, los usuarios pueden acceder a su derecho de ordenador de

casa desde su Smartphone. Una vez que esté conectado, el usuario va tener un completo control de este sistema y aprovechara su software y la potencia de este software de acceso remoto.

Este acceso puede proporcionar una solución eficaz para resolver los problemas sin tener que comprar una nueva aplicación, y puede ayudar a los usuarios a permanecer activos y seguir siendo productivo. [11]

CAPÍTULO 3

SISTEMA DE VIGILANCIA

3.1 Diseño del sistema de vigilancia

En este capítulo se presentará un diseño de un sistema de vigilancia IP basados en el enfoque que actualmente se le está dando a estos sistemas en pequeños y medianos negocios, lo que nos va a permitir un diseño optimizar el uso de las cámaras para el ahorro de dinero en seguridad de un local. En resumen, se realizará un diseño que dará como resultado el menor gasto posible en función de una buena vigilancia.

3.1.1 Diseño Detallado del Sistema.

Los sistemas de vigilancia IP están compuestos básicamente por cámaras digitales fijas o con movimiento, ocultas o discretas y sus respectivo software de monitoreo y configuración que simula ser lo que en sistemas de cámaras análogas se denomina circuito cerrado. Este software de vigilancia nos provee una mejor gestión o manejo de las cámaras hacia los monitores , ya que utilizan las Matrices de video, que vienen incluidos en las cámaras y son capaces de direccionar a través de microprocesadores las entradas (cámaras) hacia las salidas (software de monitoreo). Con la correcta configuración de este programa se puede obtener una matriz de video para la correcta gestión de la seguridad del local.

A continuación presentamos un diagrama básico de un sistema de vigilancia IP

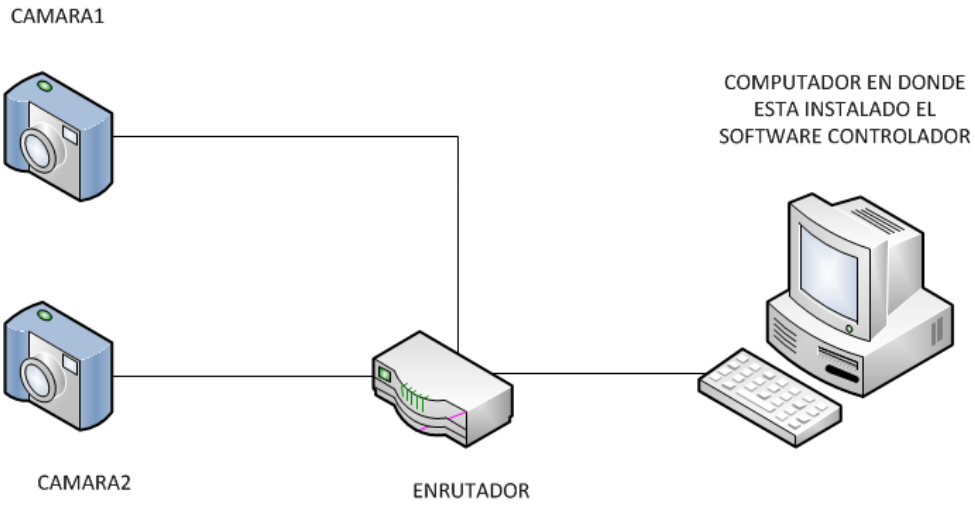


Fig. 3.1.1.1 Diseño del Sistema

Cabe recalcar que estas cámaras están conectadas por puertos Rj45 de cable de cobre de par trenzado de 4 pares, que nos sirve para poder trabajar en red y que simultáneamente este sistema pueda ser monitoreado desde cualquier dispositivo portátil, ya sea una laptop, una Tablet o un teléfono inteligente que tenga previa cargado y configurado un software de visualización para cámaras IP.

En el software a usarse (El cual va a ser descrito más adelante) se puede configurar para capturar video de muchas maneras ya sea de forma permanente, por un tiempo determinado o solamente un cierto tiempo después que detecte movimiento.

Los elementos básicos para este sistema son:

- La cámara IP.
- Un enrutador.
- Un PC.
- Software controlador de la cámara.
- Cableado respectivo o si en otro caso se decide hacerlo de manera inalámbrica.
- Dispositivos de visualización portátiles (Celular, Tablet, laptop, etc.).

Este sistema es el más adecuado a utilizarse en pequeños locales por algunas razones que ya hemos descrito anteriormente.

- **La cámara IP.-**

Es el elemento principal de nuestro diseño del sistema de seguridad. La cantidad a usarse dependerá de los requerimientos y la configuración de la misma.

Una cámara de red incorpora su propio miniordenador, lo que le permite emitir vídeo por sí misma.

Además de comprimir el vídeo y enviarlo, puede tener una gran variedad de funciones:

- Envío de correos electrónicos con imágenes.
- Activación mediante movimiento de la imagen.
- Activación mediante movimiento de sólo una parte de la imagen.
- Creación una máscara en la imagen, para ocultar parte de ella o colocar un logo. O simplemente por adornar.
- Activación a través de otros sensores.
- Control remoto para mover la cámara y apuntar a una zona.
- Programación de una secuencia de movimientos en la propia cámara.
- Posibilidad de guardar y emitir los momentos anteriores a un evento.
- Utilización de diferente cantidad de fotogramas según la importancia de la secuencia. Para conservar ancho de banda.
- Actualización de las funciones por software.

Las cámaras IP permiten ver en tiempo real qué está pasando en un lugar, aunque esté a miles de kilómetros de distancia. Son cámaras de vídeo de gran calidad que tienen incluido un ordenador a través del que se conectan directamente a Internet.

Una cámara IP (o una cámara de red) es un dispositivo que contiene:

- Una cámara de vídeo de gran calidad, que capta las imágenes.
- A diferencia de las cámaras ellas incluyen el paquete completo de configuración, direccionamiento y captura de imagen, a veces hasta visión nocturna.
- Un chip de compresión que prepara las imágenes para ser transmitidas por Internet.

La cámara que vamos a utilizar en nuestro sistema es la EASYN FM166, con las siguientes especificaciones:

Tabla 1. Descripción Modelo Easyn F-M1666 [11]

Modelo : **F-M166**		
Características	Ventajas	Acceso de videovigilancia desde cualquier ordenador y la mayoría de los smartphones en el mercado (tales como Android, Iphone)
	Software para	Ofrecer software especial

	móvil	para iPhone o movil android
	DDNS（gratis）	Sistema de DDNS incorporado gratis, como http://demo.easyn.hk, ‘demo’ es el código de serie
	Software de CMS	Software de gestión de multi-ventanas de EasynN
	Seguridad del sistema	Admite cuenta de tres niveles de jerarquía, contraseña, gestión de autoridad de multi-niveles para usuarios
CPU	Sistema de operación	Embebido Linux OS
	Procesador Microcomputer	32Bit RSIC procesador embebido

Red	Interfaz de red	Interfaz RJ-45 10/100Mb auto-adaptable Ethernet
	Protocolo	Soporte de HTTP, UDP, SMTP, FTP, DHCP, DNS, DDNS, NTP, UPNP
	Inalambrica	Wifi802.11 b/g/n
	Modo IP	Dirección IP dinamica, dirección IP estatica, PPPOE
	Visitor en línea	Corriente (640 * 480) conectado directamente, admite 4 visitores simultáneamente
		Corriente (320*240) conectado directamente, admite 4 visitores

		simultáneamente
		Corriente (160* 120) conectado directamente, admite 4 visitores simultáneamente
Video	Formato de compresión	Motion-JPEG
	Señal del sistema	CMOS 300,000 pixel
	Fotogramas por segundo	1-25fps
	Resolución	VGA (640*480), QVGA (320*240), QQVGA (160*120)
	Ajuste de imágen	Luminosidad, contraste

	WB, BLC	Auto
	LUX	0.3 LUX/F1.2
	SNR	> 48Db
	Lente	Estándar: 3.6mm
Audio	Formato de compresión	G.711/G.726
	Entrada	1 canal lineal/entrada de microphone
	Salida	1 canal lineal de salida
PTZ	Motor	Motor de control incorporado
	Rotación de ángulo de giro	Horizontal: 270°, vertical: 90°
	Preestablecido	Soporte de 15 posiciones preestablecidas

	Protocolo PTZ	No
Visión Nocturna	Interruptor de filtro	Corte de infrarrojos incorporado,con interruptor automatico, sin dominante de color
	Vision nocturna	9Φ5 LED lámparas distancia por infrarrojos: 10m
Alarma	Entrada/salida	Detección de movimiento,entrada de alarma / alarma de PTZ preestablecida, servidor FTP, notificación por email, HTTP
	Detección de alarma	Detector de movimiento; sensibilidad de detector ajustable
	Areas de	Uno

	detección	
	Notificación de alarma	Enlace IO; servidor FTP , notificación por email, HTTP
Otros	Forma material	TIpo robot
	Entorno	Uso interior
	Energía	5V 2ª
	Temperature en operación	-10 ~ 50 °C
	Humedad en operación	10% ~ 90% RH
	Dimensión	Tamaño de artículo : 110mm x 100mm x 125mm (L*W*H)

		Tamaño de embalaje: 170mm x 170mm x 170mm (L*W*H)
	Peso	Peso de artículo： 265g （ Nota: para productos reales）
		Peso de embalaje： 625g
	Accesorios	Adaptador de corriente, CD, manual, tarjeta de garantía, tornillos, soporte, antena
Sistema	Requerimiento del sistema	Microsoft Win98 SE/ME/2000/XP, Vista, Win7, Internet Explorer 8.0
Certificación	Certificado	CE FCC ROHS ISO

- **Un enrutador o router alámbrico e inalámbrico.-**

Un router es un dispositivo que envía datos de paquetes a lo largo de las redes . Un router está conectado a al menos dos redes, comúnmente dos redes LAN o WAN o una LAN y su del ISP red. Los routers se encuentran en pasarelas , los lugares donde dos o más redes se conectan.

Los routers usan encabezados y tablas de reenvío para determinar el mejor camino para la transmisión de los paquetes, y utilizan protocolos como ICMP para comunicarse entre sí y configurar la mejor ruta entre dos hosts.

Muy poco filtrado de los datos se realiza a través de routers.

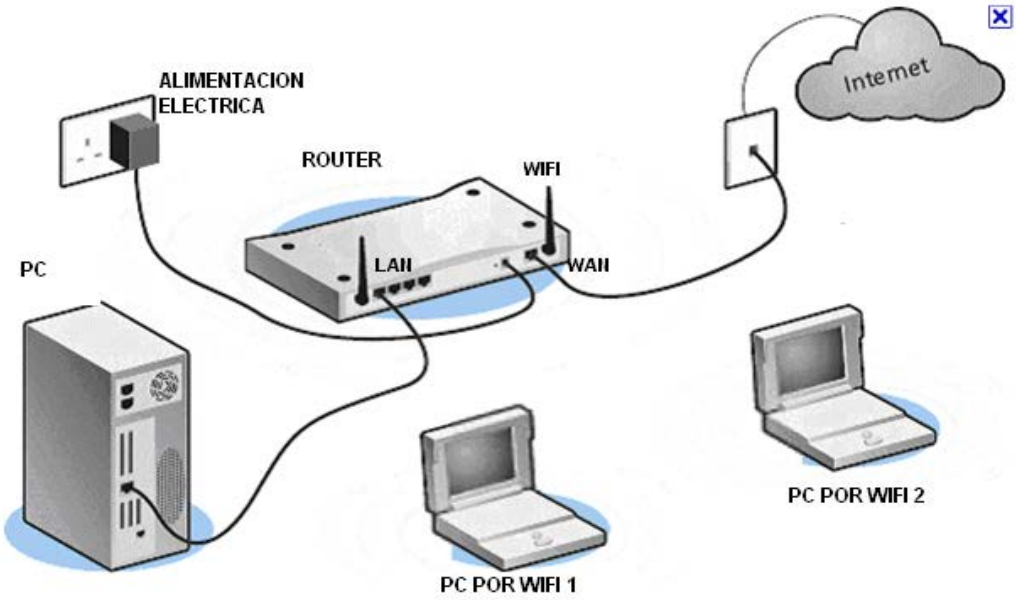


Fig. 3.1.1.2 Router Inalámbrico

El router se divide en dos partes: WAN y LAN.

WAN (Wide Área Network): Hace referencia a un conjunto de redes informáticas que están orientadas a comunicar servidores entre sí, haciendo llegar la conexión a distintos PC. Estas redes WAN son de gran extensión, por lo cual unen numerosas ciudades, países y hasta continentes. Los router que interconectan estas redes WAN son conocidos como: Nodos, Router de Borde enviando la información a de los canales.

LAN (Local Área Network): Hace referencia a lo que sería la red interna dentro de este router. La "red de área local" es a donde conectamos nuestras PC a la red. Dándoles pasó hacia la WAN, para que cumplan con su función de Comunicación. Las computadoras conectadas a la LAN están en "Red" la cual es administrada por el Router en su función de encaminamiento de paquetes.

Básicamente el Router tiene 4 entradas LAN, cualquiera de esas bocas LAN puede ser utilizada como Switch para dar conexión a otro Router o Switch.

En sus inicios el router o Enrutador solo era alámbrico, hoy en día

debido a la gran demanda y la funcionalidad de este aparato contamos en el mercado con una amplia gama de enrutadores inalámbricos, que cuentan con un alcance bastante grande. El router en nuestro caso para efectos de diseño es muy importante para poder establecer conexión entre la cámara y el dispositivo móvil que nos va a servir de monitoreo.

- **Un PC**

Una PC (Personal Computer) o computadora personal el cual es el término que se le da a los computadores ya sean genéricos o de marcas específicas que se utilizan en la actualidad para un número muy grande de funciones.

En este caso la PC va a ser la herramienta para poder realizar la configuración de los dispositivos como la cámara y el enrutador para nuestro diseño, también su uso puede ser para el monitoreo del sistema de cámaras.

En el caso de la configuración de la cámara se va a instalar el software correspondiente de la misma en el ordenador.

La PC a utilizarse debe tener las siguientes características:

- Sistema Operativo compatible con el software de la cámara (Windows XP en adelante).
- Memoria Ram superior a 2Gb.
- Almacenamiento como mínimo 100Gb.
- Capacidad de procesamiento de imágenes en tiempo real o almacenado en el mismo.

Como acotación adicional la PC puede contar con una tarjeta de video que ayudaría a mejora el procesamiento de imágenes, eso queda a criterio de quien vaya a instalarlo.

- **Software controlador de la cámara**

El software controlador de la cámara viene dado con firmware ya instalado en la misma que se va a poder controlar cuando la cámara esté conectada al PC que va a ser configurado y diseñado nuestro sistema.

Otra manera u otro software a utilizarse para la configuración de las cámaras es el software que viene con ella que debe ser instalado previamente (en el siguiente capítulo hablaremos de cómo instalarlo y configurarlo para poner en marcha nuestro sistema) en la PC, el nombre del software es el Central Management.

La compatibilidad de este programa con los sistemas operativos es desde Windows XP en adelante, y los requisitos de la PC son los anteriores ya descritos en la PC

- **Cableado respectivo o si en otro caso se decide hacerlo de manera inalámbrica.**

El cableado de la cámara está dado por un cable de par trenzado de categoría 5e en adelante el cual va desde el router o enrutador hasta la cámara.

El tipo de cableado que se va a utilizar depende de lo que se le haya solicitado al instalador o diseñador del sistema de seguridad. Existe una diferencia significativa en el precio de las diferentes características de cable que pueden ser utilizada así como también lo hay entre las marcas del producto.

En nuestro caso se utilizará categoría 5e en los patchcords utilizados en nuestro diseño.

- **Dispositivos de visualización portátiles (Celular, Tablet, laptop, etc.).**

Ahora gracias a la tecnología y a su evolución en los teléfonos celulares, tablets, laptops, etc… Existe la posibilidad de poder visualizar cámaras IP desde estos dispositivos con mucha facilidad y una gran capacidad de procesamiento de datos.

En este caso vamos a implementar la aplicación para visualización de las cámaras en teléfonos inteligentes con sistema operativo Android.

La aplicación para esto se llama IpCamViewer Pro el cual nos permite ver todo nuestro sistema de cámaras funcionando a la perfección y también permite el control de direccionamiento de la cámara para que pueda ser observado por el usuario o diseñador del sistema.

3.1.2 Parámetros del diseño del sistema.

- **Parámetros de la cámara.-**

Un factor importante al momento de escoger las cámaras es el número de posiciones predeterminadas que pueden ser predefinidas en la cámara. Existen parámetros predeterminados que son una serie de posiciones en las que puede programarse una cámara para que pase automáticamente en el curso de una ronda de vigilancia, un turno o un día para ayudar a garantizar el cubrimiento de un área específica o cuando se integre un sistema de vigilancia con un sistema de alarma

o de control de acceso. La cámara puede programarse para ir a una posición predeterminada apropiada cuando ocurre determinado evento, por ejemplo, cuando se abre una puerta. [12]

En nuestro caso la cámara con la cual vamos a realizar el diseño tiene un una función de zoom digital, en muchos casos magnificar los pixeles no ayuda a obtener mejores resultados para una correcta vigilancia, el zoom digital no añade más información; solo la hace más difusa. En la actualidad, las cámaras disponen de software integrado que sirven para implementar servidor web, de correo electrónico y otras características adicionales muy útiles como el sensor de movimiento o la visión nocturna. En el interior de las cámaras IP existen los componentes necesarios que hacen que la imagen captada se transforme en una señal eléctrica y pueda ser enviada a los diferentes dispositivos de monitoreo que previamente han sido configurados. [12]

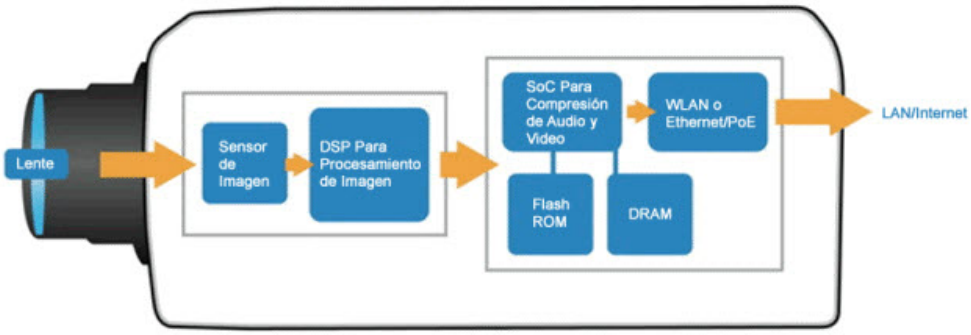


Fig. 3.1.2.1 Sistema de la Cámara [16]

- **Sensor de imagen**

Este sensor tiene como función transformar la luz que recibe en señales eléctricas. Los fabricantes de cámaras tienen a su disposición dos tecnologías de sensor de imagen:

- CCD(dispositivos de acoplamiento de carga)
- CMOS(Semiconductor de óxido metálico complementario)

A.- CCD

Como característica fuerte es que tiene una mejor sensibilidad a la luz, la cual da como resultado una imagen con mejor calidad que la de de

sensores CMOS. Esta característica ayuda en situaciones o lugares en donde la luz es escasa. [12]

Pero al dar una mejor calidad en la sensibilidad en la luz esto representa un alto costo a la hora construir una cámara de vigilancia ya que usan procesos no tan comunes para poderse implementar. Y además cuando el objeto tiene mucha luz, puede tener pérdidas en la imagen, provocando rayas por encima o por debajo del objeto a mostrarse. Esta situación puede resolverse cuando una cámara con este tipo de sensores están en el exterior, colocando a la misma dentro de una carcasa adecuada. [12]

B.- CMOS

Aunque son muy parecidos a los CCD en cuanto a la calidad de la imagen, estos resultan ser en muchos casos inadecuados para una correcta vigilancia en donde se exige una máxima calidad de la imagen posible. [12]

A diferencia de las CCD, esta tecnología presenta muchos problemas en lugares donde hay muy poca luz y resulta ser un problema a la hora de seguridad en lugares específicos; la imagen resultante con

estos sensores en lugares de poca luz es una imagen muy oscura o una imagen con apariencia granular. [12]

En conclusión, la tecnología de CCD resulta ser mejor para el diseño que la tecnología CMOS, pero resulta muy difícil implementar un sistema de cámaras con este tipo de sensores debido a que su costo final resulta ser muy alto en comparación que la otra tecnología que, dándole un buen uso y un diseño correcto se pueden obtener muy buenos resultados. [12]

Con lo enunciado anteriormente, se llegó a determinar que el mejor sensor es el CCD pero con las desventajas que se presentaron, se le suma una que es el alto consumo de energía. Dentro del tipo de sensor que debe escogerse otro parámetro importante es el tamaño del sensor que puede variar según el tipo de cámara y de la calidad de imagen resultante.

Los tamaños más conocidos y comerciales son: 2/3” 1/2” 1/3” 1/4”.

Hay que tener cuenta que existe una relación estrecha entre el tipo de sensor y el lente que tiene la cámara. Por ejemplo si un lente está dispuesto para un sensor más pequeño este mostrará las esquinas

como oscuras. Mientras que si se usa un lente que está dispuesto a trabajar con un sensor mayor al que está trabajando, este terminará perdiendo parte de la imagen que se capta. El lente solo va a trabajar bien con sensores de menor o igual tamaño del sensor para el cual está diseñado. [12]

- **Selección del tipo de lente**

El lente es el encargado de capturar la imagen para que luego sea procesada por los demás componentes de la cámara. Entonces debe existir cierto criterio al momento de elegir la cámara y el tipo de lente según su requerimiento, que además como lo dijimos anteriormente está relacionado con el tipo de sensor.

Los tipos de lentes que existen son:

- Lente fija o estándar: Lente con el foco fijo.
- Lente varifocal: Lente que puede variar el foco manualmente.

En nuestro caso usaremos un lente estándar de 3.6mm.

A continuación en la siguiente tabla sacaremos los lentes y el tipo de sensor apropiado para el mismo.

Tabla 2. Tipos de Sensor

Lentes y tamaño del sensor	1/2”	1/3”	1/4”
Distancia focal	12mm-9mm	8mm-7mm	6mm-3mm

Bajo estas medidas el tipo de sensor de nuestra cámara es de 1/4”.

Para que no se pierda la imagen al momento de transformarla en señal eléctrica.

Como una ley al momento del diseño se tomará en cuenta que para detectar la presencia de alguien en la pantalla se tomará en cuenta por lo menos un porcentaje aceptable de la altura real del objeto. [12]

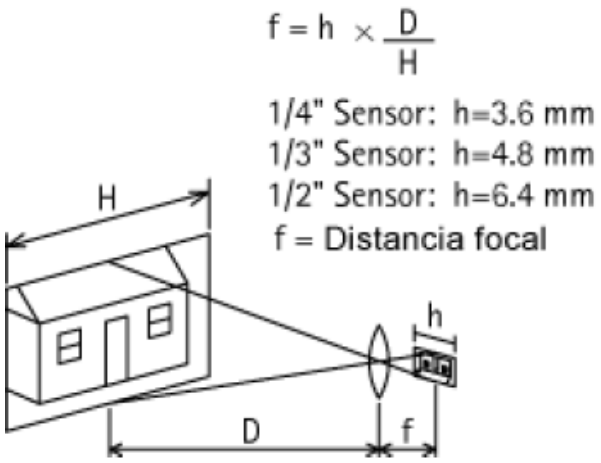


Fig. 3.1.2.2 Distancia Focal de la Cámara

- **Tipo de iris**

El iris es la parte de la cámara que controla la cantidad de luz que que pasa por el lente, por defecto, las cámaras IP controlan la luz a través del iris. Existen dos tipos de iris

- Iris automático: Son los que cambian automáticamente al tipo de luz
- Iris manual: No reaccionan ante cambios de luz.

Tabla 3. Tipos de Iris

Numero F	F1.0	F1.4	F1.7	F1.8	F4.0	F5.6
% de Luz	20	10	7.07	2.5	1.25	0.625

En nuestro caso el tipo iris a utilizarse es automático y tiene un número F1.2 que da como resultado un porcentaje de luz aproximado a 15%.

- **Cálculo de las distancias que puede cubrir la cámara**

Es muy importante tomar esto en cuenta para el diseño de un sistema de vigilancia ya que con este cálculo nos evitaríamos los problemas de tener un exceso de cámaras o lo contrario que no existieran muchas cámaras para poder cubrir correctamente todas las áreas. Por tal razón es que se hace el cálculo de la distancia máxima que puede cubrir la cámara.

La distancia está determinada por:

Distancia= Distancia focal x ancho de imagen / tamaño de sensor.

=6mm x 30 metros /3.6mm = 50 metros

La mayor distancia que puede cubrir nuestra cámara es de 50 metros para obtener una nitidez en la imagen aceptable para la seguridad.

- **Capacidad de almacenamiento**

La capacidad de almacenamiento y su concepto es la cantidad de imágenes y de videos que puede almacenarse en los servidores configurados para nuestro sistema (nuestra PC) de cámaras de vigilancia. Para elegir de manera correcta la capacidad de almacenamiento se deben realizar cálculos de la cantidad de imágenes, videos en función del tiempo que va a ser grabado en el caso de video y la vigencia de esta información en nuestro servidor. [12]

El formato para la compresión de la cámara que vamos a utilizar es de MJPEG, que tal vez no sea el que menos espacio ocupe en nuestro disco duro destinado al almacenamiento pero tiene la ventaja de recibir el empaquetado en imágenes distintas. [12]

Las fórmulas a utilizarse para el cálculo de la capacidad de almacenamiento son:

- Tasa de bits / 8 bits por byte x 3600s = KB por hora / 1000 = MB por hora
- MB por hora x horas de operación por día / 1000 = GB por día
- GB por día x período solicitado de almacenamiento = almacenamiento.

En nuestra cámara obtenemos los siguientes datos:

- Resolución: VGA que equivale a 640 x 480 píxeles (resolución estándar)
- Frecuencia de imágenes: 25 imágenes por segundo (frecuencia apropiada)
- Tasa de bits: 8.44 Mbits por segundo. Esto se calculó en relación a la frecuencia de imagen, resolución, compresión y nivel de movimiento de la escena. Este cálculo se lo hace mediante herramientas en el internet que son proporcionadas por los fabricantes de cámaras. Para este caso se usa compresión con factor 25, donde este parámetro indica que a menor factor mejor calidad pero mayor tasa de bits, y a mayor factor menor calidad pero menor tasa de bits.

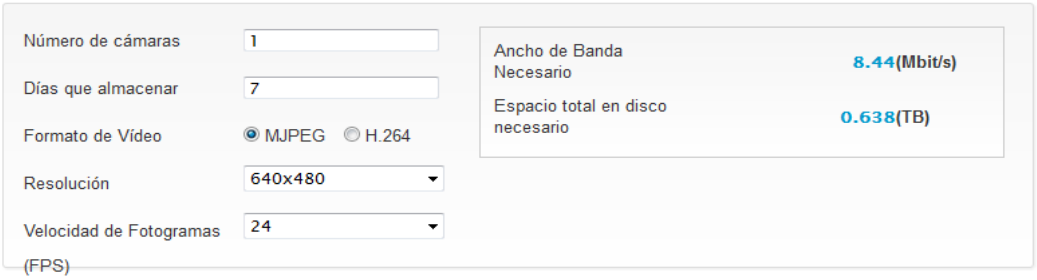


Fig. 3.1.2.3 Grafico para cámaras con compresión MJPEG y para H.264 (mp4).

- Horas de funcionamiento: 17
- Se analizara la capacidad por 7 dias

El cálculo para el almacenamiento con formato de compresión de MJPEG es cuatro veces que el de H.264 que no es más que el formato MPEG-4, dando como resultado una mayor eficiencia en cuanto al uso del ancho de banda y los demás parámetros a ser consideras para el cálculo del almacenamiento. Resulta que para video el MPJEG resulta no ser factible su almacenamiento ya que resultaría muy costoso al momento de implementar una cantidad considerable de cámaras.

3.2 Diagrama principal (arquitectura física del sistema).

En el sistema de cámaras IP lo principal que se requiere es una conexión de banda ancha, debido a la necesidad de transferencia de imagen y video en tiempo real de manera ágil y segura, la maquina en donde se va controlar el software principal (CMS) debe tener una capacidad considerable de almacenamiento para poder guardar toda información que sea considerada importante y además el mismo programa (CMS) debe tener sistemas de compresión y

empaquetamiento de la información esto ayuda mucho para un mejor manejo de la misma. [12]

Nuestro sistema va a contar con almacenamiento directo que no es más que la función de almacenar todo lo capturado por la cámara en la pc que tiene instalado el sistema de manejo y control de la cámara (CMS). [12]

A continuación en el grafico se va a describir todo nuestro sistema.

Uno de los elementos principales en el sistema es el router ya que nos ayuda con algunos beneficios:

- Tiene la función de Port Forwarding que nos ayuda con el enmascaramiento de la dirección IP Local que nos asigna el router y la asocia con la dirección IP o URL del sistema en el internet.
- Es posible tener múltiples PC´s en la misma conexión con la cual podremos ver nuestra cámara de manera simultánea de manera local.
- Facilita mucho la conexión de cámaras de red.

Otro elemento importante es la PC principal la cual debe tener como mínimo una capacidad de almacenamiento de 300Gb lo cual ayudaría

a una cámara a mantener información almacenada por más o menos un mes. [12]

La topología de nuestra red LAN va a ser tipo bus ya que esto nos ayuda mucho a reducir costos de instalación y además que las computadoras conectadas al sistema la mayor parte tienen interfaz Ethernet. El tipo de Ethernet a usarse en nuestro sistema es 10Mbit/s, aunque es muy poco usado por su baja capacidad es satisfactorio para nuestro sistema; el mismo que usa una topología de 10BaseT.

Nuestra cámara usara red inalámbrica debido a la escalabilidad dentro del sistema y la movilidad de la misma, considerando un espacio de operación pequeño esta opción es muy útil y económica, debido que ahora se cuenta con tecnología de alta velocidad en las redes inalámbricas; otra ventaja de la red inalámbrica es que evita que se rompan paredes y se hagan daños dentro de los edificios o salas en donde se instalan cámaras IP. [12]

Nuestro tipo de red inalámbrica es WLAN debido que los estándares en la actualidad están bien definidos y funcionan bien juntos.

Hoy en día el estándar más utilizado es el 802.11n el cual su rendimiento es superior a los 10Mbps.

La mayor parte de los hogares en nuestro entorno cuentan con una pequeña red y un router en donde nuestro trabajo se facilitaría mucho al momento de querer instalar una cámara IP.

Se debe tomar en cuenta la distancia desde el router inalámbrico hasta la cámara para que esta tenga una mejor funcionalidad y evitar que en algún momento la conexión se caiga.

Otra consideración que se debe tener es al momento de implementar los protocolos y las tecnologías de estos puede que la red deje de ser tan aprovechada y ayude de manera negativa a nuestro sistema.

En nuestro sistema vamos a usar dos tipos de protocolos que nos van a ayudar a almacenar imágenes captadas por detección de movimiento. Estos protocolos son:

a) SMTP (Simple Maill Transfer Protocol).

Es el protocolo más utilizado y confiable de Internet para el envió de mensajes de correo electrónico entre distintos dispositivos. En el conjunto de protocolos TCP/IP de la capa de transporte el SMTP está usando normalmente el puerto 25 (en nuestro caso usaremos el 587). Además el modelo cliente-servidor es el utilizado por SMTP. [12]

b) FTP (File Transfer Protocol).

Es un protocolo de transmisión de datos entre un usuario y servidor. El protocolo asegura que los archivos se transmitan sin errores y están sobre los protocolos TCP/IP usados en la capa de transporte. El servidor tiene un sistema de corrección basado en un control por redundancia, por lo tanto, tiene la capacidad de retomar la descarga desde el punto que se perdió la conexión. {12]

Por seguridad es necesario tener claves de acceso a estos servidores para evitar el robo de información y el hackeo de los servidores. [12]

3.3 Diseño interfaz gráfica.

Para que el usuario final o lector del sistema pueda monitorear y controlar bien las cámaras IP se deben contar con una buena interfaz gráfica y muy amigable. Para contar con buen desarrollo del sistema se debe contar con un software de las siguientes características:

- Facilidad de comprensión, aprendizaje y uso.
- Representación fija y permanente de un determinado contexto de acción (fondo).
- El objeto de interés ha de ser de fácil identificación y control.

- Diseño simplificado mediante el establecimiento de menús, barras de acciones e iconos de fácil acceso.
- Las interacciones se basarán en acciones físicas sobre elementos de código visual o auditivo (iconos, botones, imágenes, mensajes de texto o sonoros, barras de desplazamiento y navegación...) y en selecciones de tipo menú con sintaxis y órdenes.
- Las operaciones serán rápidas, incrementales y reversibles, con efectos inmediatos
- Existencia de herramientas de Ayuda y Consulta

La interfaz que tiene el software que utilizamos es muy enfocada en todos los objetivos que se necesitan para la configuración de la cámara, además todas las funcionalidades están en la pantalla principal, situación que facilita mucho el uso por parte del cliente y el control del sistema. [12]

Otra interfaz considerada para control y monitoreo del sistema es mediante el firmware de la cámara que tiene las mismas características del software y con la misma simplicidad ofrecida del software. Una característica adicional de esto es que es administrable desde internet mediante un DDNS (dinamic DNS) que la cámara proporciona. [4]

3.4 Herramientas usadas en el diseño y desarrollo de sistema de monitoreo y vigilancia.

Para el diseño del sistema se utilizó herramientas básicas sin costo que ayudaron al diseño y posteriormente sirvieron de guía para el desarrollo del sistema la cual nos ayudó de manera inicial en varios aspectos como:

- Aumentar la eficiencia de su sistema de seguridad a la vez que reduce los costos encontrando las mejores ubicaciones para la cámara.
- Calcular longitud focal precisa del lente de la cámara y ángulos de visión en segundos.
- Estimar del ancho de banda de red necesaria para crear sistemas de vídeo en red con cualquier número de cámaras IP y servidores de vídeo.
- Calcular el espacio necesario de almacenamiento de disco duro para el archivo de vídeo.

Estos aspectos son varios puntos interesantes que siempre deben ser tomados en cuenta para el diseño de un sistema de vigilancia eficiente y funcional.

Para el desarrollo del sistema la herramienta que se uso es el software de monitoreo, control y grabación de las imágenes de la cámara, anteriormente se debía instalar una serie de programas que ayudaban a la configuración de los protocolos que se pueden implementar pero ahora la mayoría vienen precargados en los sistemas operativos de uso tradicional en nuestro entorno

3.5 Procesos del Sistema de monitoreo y vigilancia

En el sistema de vigilancia de cámara IP, es un proceso de monitoreo por persona o personas, que puede ser monitoreada desde una PC o dispositivo móvil, ya sea el monitoreo de una o más cámaras de vigilancia IP dependiendo la necesidad del usuario, esta va tener una carpeta de captura de imágenes y otra de captura de videos que estas carpetas serán guardadas en la maquina central.

3.5.1 Módulo de Captura de Imagen

La cámara IP de vigilancia easyn captura imágenes de acuerdo a las configuraciones establecidas ya sean capturas de imágenes diurnas o nocturnas, el control de movimiento que tiene la cámara IP para la captura de imágenes. Estos movimientos de la cámara IP pueden ser de lado a lado y de arriba-abajo, si el movimiento de la cámara IP es de lado a lado es de 270 grados y si es de arriba-abajo es de 120 grados, la cámara puede ser configurada para la detección de imágenes cuando la cámara detecta un movimiento en tiempo real es una detección de movimiento inteligente y estas imágenes de captura son enviadas como mensajes de alerta por mail (foto capturada a un email configurado). [11]

Para la captura de imágenes de la cámara IP de vigilancia easyn esta consta de 10 LEDs infrarrojos que estos funcionan de 5 a 10 metros de distancia al detectar algún movimiento la cámara IP hace la captura de las imágenes que estas serán enviadas a un email configurado previamente.[11]

Estas capturas de imágenes en general ya sean diurnas o nocturnas de la cámara ip pueden ser imágenes en redes LAN, WAN e Internet. Con un formato de comprensión de imágenes M-JPEG estándar.

3.5.2 Módulo de Captura de video

La cámara IP de vigilancia easyn en su configuración captura videos estos que se los puede ver directamente desde Internet o desde la red de una empresa y que consta con visión nocturna (infrarrojos) desde el momento que llega un mensaje de aviso en nuestro email configurado, uno puede ver y se puede escuchar lo que las personas hablan cerca de la cámara y a su vez se puede hablarle a ellos también desde una PC o dispositivo móvil, se puede grabar en la PC el video de vigilancia de la cámara IP de lo que sucede todo el día.

La cámara IP de vigilancia easyn captura y grabación de video en tiempo real desde la PC de nuestra casa o de una empresa o cualquier dispositivo móvil, la cámara IP tiene detección de video con movimiento de un lado a otro y de arriba-abajo con un ángulo de vista de 67 grados y audio de dos vías, soporta ajuste automático de claridad. [11]

El video de la cámara IP de vigilancia easyn de cómo opera puede ser visto desde cualquier navegador ya sea Explorador de internet, Firefox, Google Chrome y desde un iPhone o androide.

3.5.3 Modulo de almacenamiento de imágenes y videos mediante FTP.

Para esta parte del sistema de vigilancia se necesita configurar la cámara a un servidor FTP, ya sea de manera local o a nivel de internet en donde este almacenará imágenes y videos capturados, las imágenes que se almacenaran son las imágenes del sistema de alarma de detección de movimiento y los videos son los que se grabaran de acuerdo al requerimiento del usuario final.

Un diagrama que nos puede ayudar a entender cómo funciona el sistema con FTP esta descrito en el grafico a continuación.

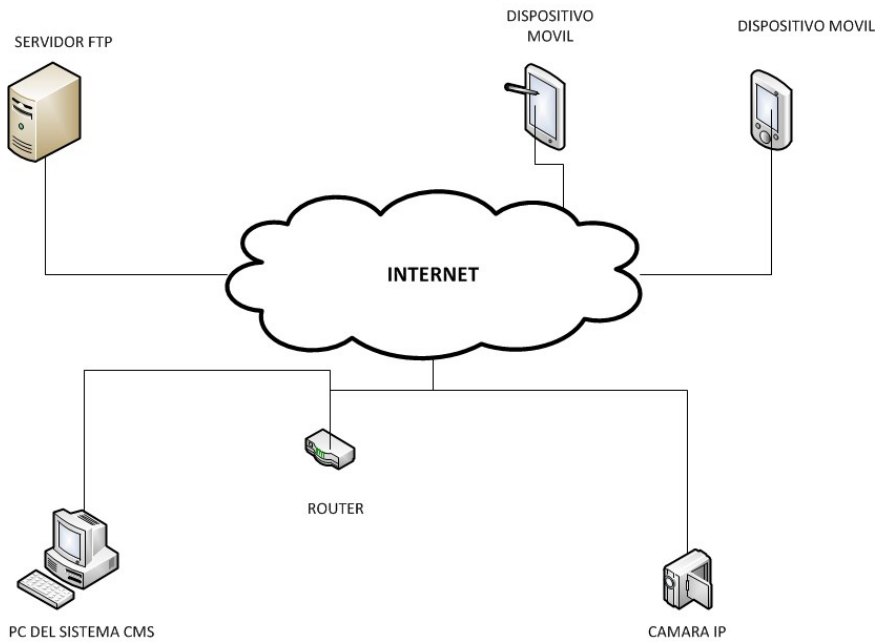


Fig. 3.5.3.1 Modulo de Almacenamientos de imágenes y videos mediante FTP

En este diagrama podemos observar que el sistema puede conectarse a un servidor ftp de manera local (Red LAN) o a través del internet.

Este servidor puede ser una maquina considerada Servidor o en su defecto una pc normal que pueda servir para configurar un servidor FTP en la misma; en la cual se puede acceder y observar y descargar todas las imágenes que le lleguen al mismo por la alarma de detección de movimiento.

3.5.4 Modulo de envío de alarmas mediante SMTP

El sistema de correo electrónico nos ayuda a obtener dos tipos de información: Informe de la dirección URL que usa la cámara y un informe de las imágenes de la alarma de detección de movimiento.

El informe de la dirección de la URL sirve para saber qué dirección IP o URL está siendo usada por el sistema, debido a que hay proveedoras de servicio de internet que suelen cambiar la dirección IP y eso causaría problemas al momento de intentar acceder a la cámara.

La cámara ofrece la opción de configurar alarmas de detección de movimientos, donde se captura imágenes y estas son enviadas a desde un correo electrónico remitente hacia un correo electrónico receptor ambos previamente configurados.

A continuación en el grafico se detalla un diagrama que sirve para implementar el sistema de mensajes de alarma mediante SMTP.

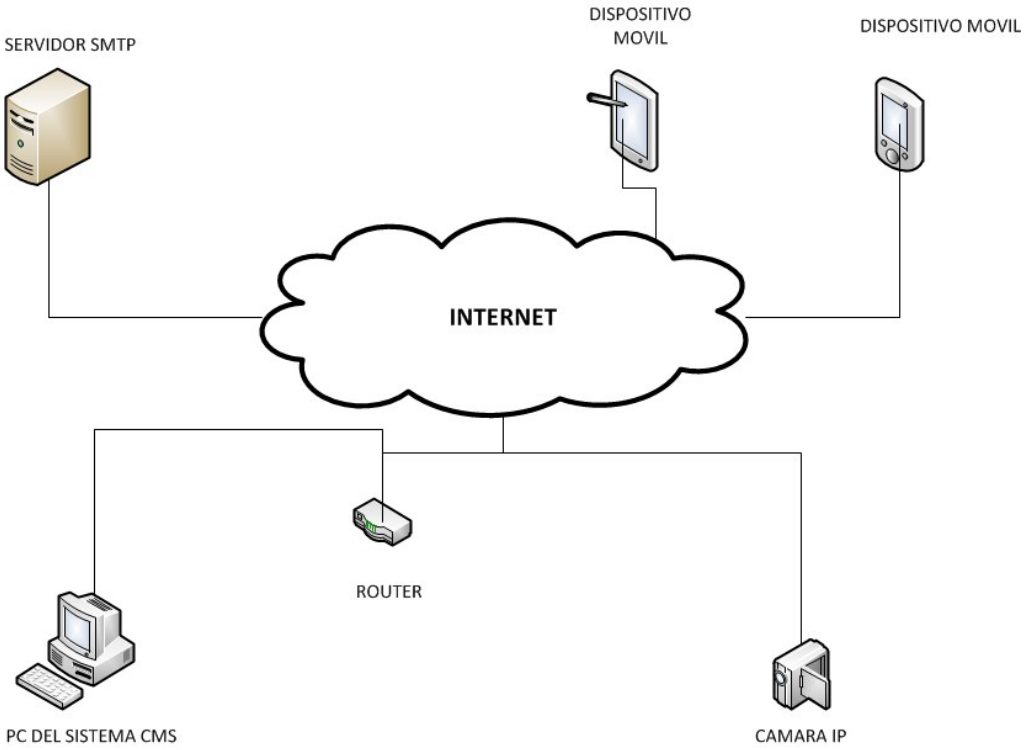


Fig. 3.5.4.1 Modulo de envió mediante SMTP

En el caso del servidor SMTP se puede utilizar uno de los servicios ya conocidos como Gmail, Hotmail, Yahoo, etc. Para configurar la cuenta remitente de correo y cualquier cuenta de correo para las receptoras, se pueden configurar hasta cuatro cuentas receptoras de correo electrónico en nuestro sistema.

3.5.5 Modulo de envió de imágenes mediante SMTP

La cámara IP de vigilancia easyn captura imágenes de acuerdo a las configuraciones establecidas, estas imágenes que pueden ser enviadas por email o FTP a un correo electrónico

Se deben configurar las alarmas de la cámara IP para que nos llegue un correo electrónico cuando se active la alarma de movimiento, en primera instancia se debe configurar el email en la cámara easyn, donde se debe tener un remitente, receptor, servidor SMTP, autentificación, Protocolo de seguridad de capa de transporte, usuario SMTP y la clave SMTP (clave de nuestro correo Gmail).

Al configurar el email se puede hacer una prueba para saber que todo está correctamente y de esta manera está configurado el correo.

Luego se debe configurar la alarma en la cámara de vigilancia, para poder enviar un correo a un SMARTPHONE o PC se debe activar el detector de movimiento y la sensibilidad de movimiento y activa la acción en alarma, cuando la cámara detecta un movimiento llegara un correo de aviso o advertencia y también se puede configurar para poner un lapso de tiempo para que se active la cámara en ciertas horas o días dependiendo el uso que se le vaya a dar.

3.5.6 Modulo de Administración y gestión de Usuario

Para poder entrar a la cámara de vigilancia IP easyn por internet se necesita la dirección DDNS que esta no las da la propia cámara en la parte inferior de ella, que también nos da la clave y usurario que para ambas es ¨admin¨.

La dirección DDNS es **ysax.easyn.hk** con esta dirección se puede entrar a la cámara de vigilancia IP easyn desde cualquier navegador, donde aparecerá una ventana donde se pone la opción Server Push Mode, luego va pedir un usuario y clave, donde nuestro usurario es feran2485@gmail.com y nuestra clave es *paulina20.*

También se debe configurar en la cámara de vigilancia los parámetros SMTP para poder añadir las cuentas de correo electrónico donde se enviaran y recibirán las imágenes que va detectar la cámara de vigilancia IP easyn, que será un remitente feran2485@gmail.com y el receptor pueden ser hasta cuatro correos como por ejemplo jmchoclito@hotmail.com en este correo llegaran las imágenes que la cámara va detectar con la sensibilidad de movimiento.

CAPÍTULO 4

FUNCIONAMIENTO DEL SISTEMA DE VIGILANCIA

4.1 Implementación del sistema

Se debe configurar la cámara de vigilancia IP easyn por medio inalámbrico por la red wifi, conectamos la antena inalámbrica a la cámara y el cable de red al router inalámbrico, la computadora portátil está conectada de forma inalámbrica al router, para su configuración inicial, debemos conectar con el cable de red a la cámara para luego hacer la configuración. Instalamos el CD que viene en nuestra cámara de seguridad para su respectiva configuración de parámetros para el uso ideal de la cámara de vigilancia IP easyn.

4.1.1 Implementación y configuración de parámetros de FTP.

Lo principal en FTP es definir dos parámetros: Cliente y servidor.

Para la implementación del servidor, hablando de un sistemas local, como es un sistema pequeño puede ser usada una PC normal con un sistema operativo Microsoft Windows 7 en el cual se puede proceder a crear la aplicación de servidor y luego la cuenta de usuario que será usada en todo momento para el servidor FTP.

Instalación del servidor de FTP en Windows 7

En primer lugar se debe disponer de un equipo "normal" (no es necesario un equipo con características hardware de servidor), con Microsoft Windows 7 como sistema operativo.

Se pulsa en el botón "Iniciar" - "Panel de control":

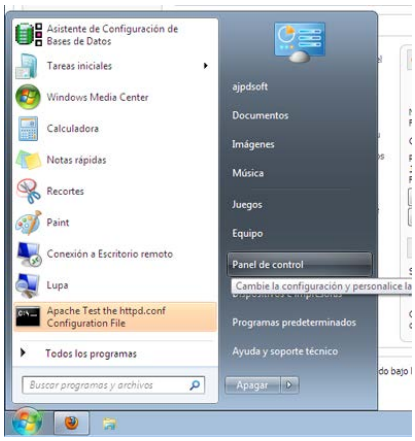


Fig. 4.1.1.1 Instalación Servidor FTP

Se pulsa en "Programas":

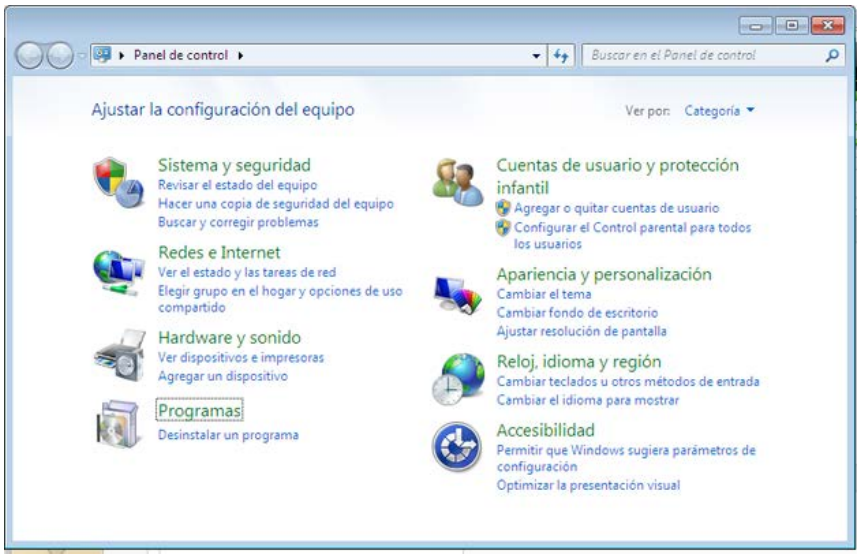


Fig. 4.1.1.2 Configuración en el Equipo

En "Programas y características", se pulsa en "Activar o desactivar las características de Windows":

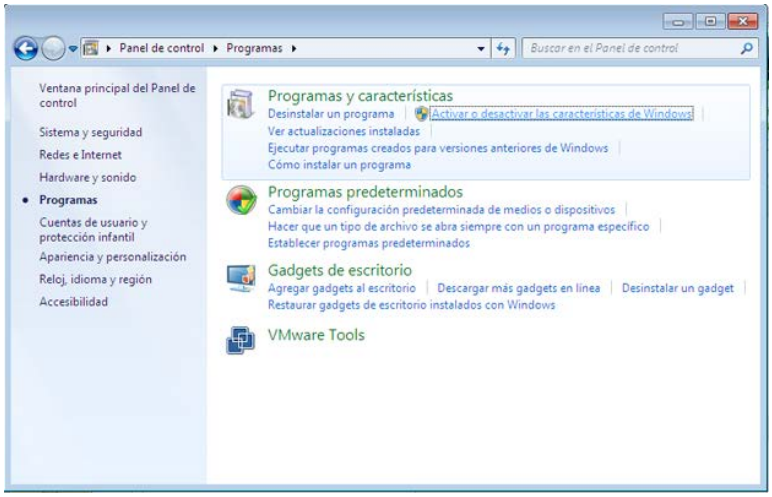


Fig. 4.1.1.3 Instalación del Programas y Características

A lo que se despliega la rama "Internet Information Services" - "Herramientas de administración web" - "Consola de administración de IIS" (complemento necesario para administrar y configurar el Servicio FTP). Se marcara también en "Servidor FTP" la opción "Servicio FTP". Y se pulsa "Aceptar" para iniciar la instalación del servicio de FTP:

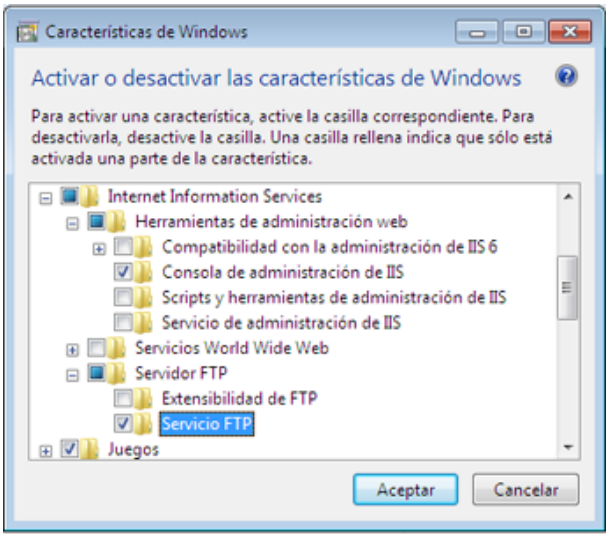


Fig. 4.1.1.4 Instalación del Servicio de FTP

Se iniciará la instalación del software necesario para la utilización de este servicio de FTP:

Configuración y administración del Servicio de FTP en Windows 7

Para administrar y configurar las opciones del servicio de FTP instalado, se debe acceder al panel de control, desde el botón "Iniciar" - "Panel de control":

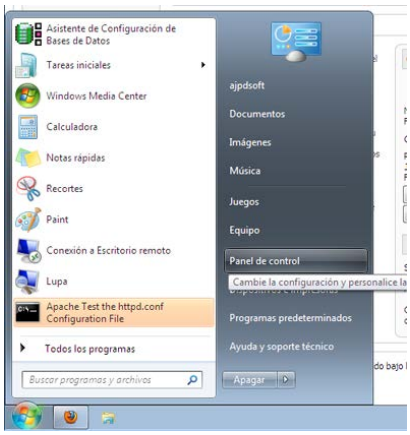


Fig. 4.1.1.5 Configuración y Administración del Servicio de FTP

Para mostrar las "Herramientas administrativas" se debe pulsar en "Ver por" y seleccionaremos "Iconos pequeños":

Fig. 4.1.1.6 Icono ¨Ver Por¨

Pulsaremos en "Herramientas administrativas":

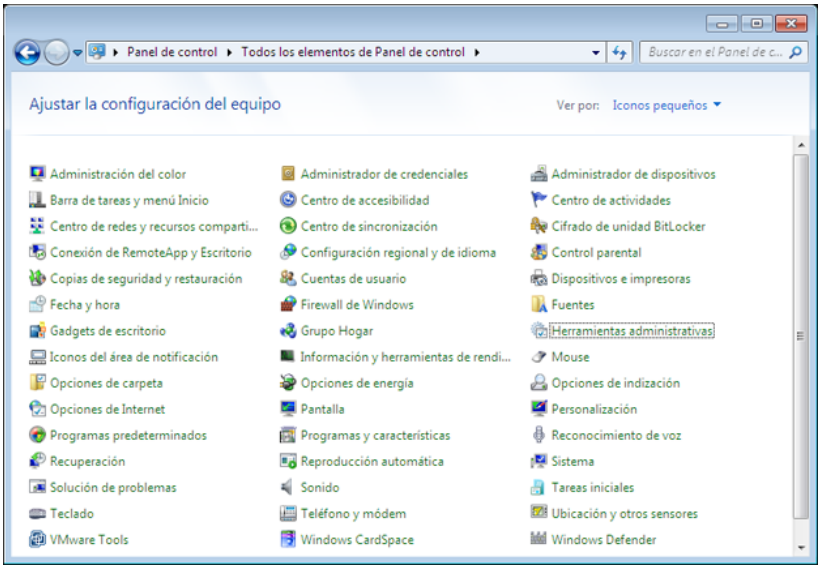


Fig. 4.1.1.7 Herramientas Administrativas

Pulsaremos en "Administrador de Internet Information Services (IIS)":

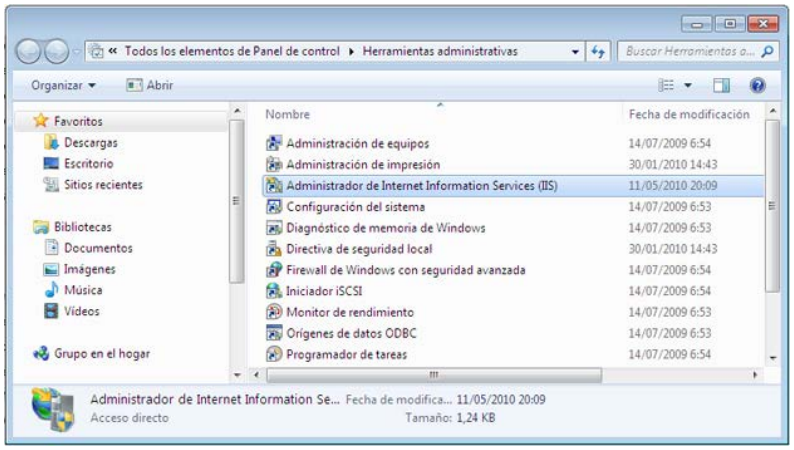


Fig. 4.1.1.8 Administrador de Internet

Una vez en el administrador de Internet Information Services (IIS), se puede administrar y configurar nuestro servidor FTP, en primer lugar se tiene que crear un sitio FTP, para ello se pulsa con el botón

derecho sobre el nombre del equipo (en nuestro caso "PCWSEVEN"), en el menú emergente y se pulsa en "Agregar sitio FTP...":

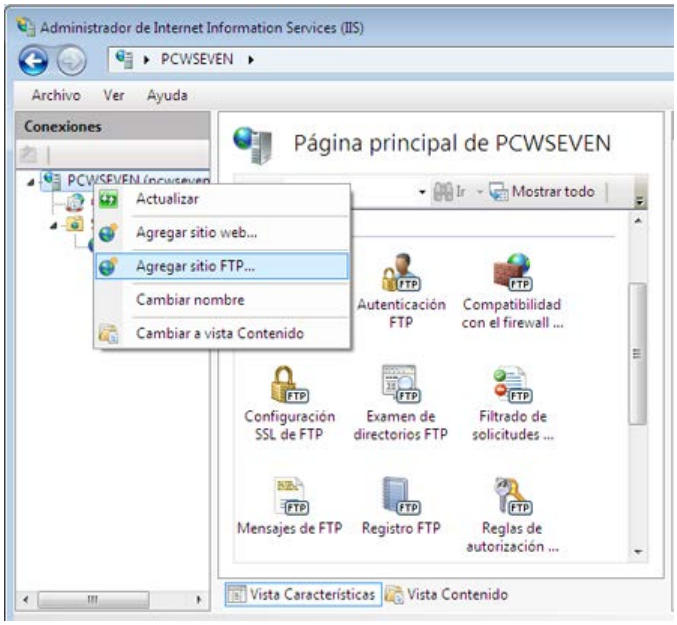


Fig. 4.1.1.9 Agregar sitio FTP

Se tiene que introducir los siguientes datos en "Información del sitio" para nuevo sitio FTP:

Nombre del sitio FTP: introducir aquí el nombre que tendrá el sitio FTP, puesto que podemos varios sitios, lo identificará unívocamente, por ejemplo "ajpdsoft".

Ruta de acceso física: se debe introducir a la unidad y carpeta del equipo con Microsoft Windows 7 donde vamos alojar los ficheros del sitio FTP, en nuestro caso "C:/ftp".

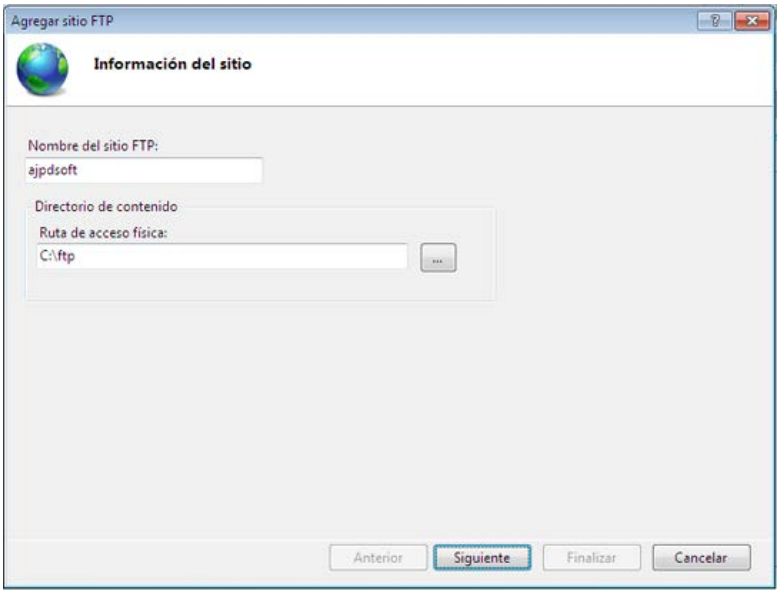


Fig. 4.1.1.10 Información de sitio

A continuación se puede indicar los siguientes datos (en "Configuración de enlaces y SSL"):

Enlace - Dirección IP: en este campo se puede indicar qué dirección IP se le asignará a este sitio FTP, siempre que el equipo tenga varias direcciones IP. Por defecto quedará seleccionada "Todas las no asignadas". Si se tiene varios sitios FTP y se quiere que sean accesibles desde fuera del equipo, se debe indicar qué dirección IP se le asignará a cada sitio FTP.

Puerto: Se puede indicar la dirección IP y el puerto que se asignará al sitio FTP. Por defecto el 21.

Habilitar nombres de host virtuales: si se quiere tener varios sitios FTP en un equipo con una sola dirección IP y que sean accesibles desde fuera del equipo (LAN o Internet) se puede marcar esta opción de "Habilitar nombres de host virtuales" e indicar el nombre del sitio ftp que queramos establecer, por ejemplo: ftp.ajpdsoft.com. Si se quiere que este sitio FTP esté disponible en Internet, introduciremos en "Host virtual" el nombre de dominio del sitio igual que lo escribirían los usuarios en un explorador, por ejemplo, ftp.ajpdsoft.com.

Iniciar sitio FTP automáticamente: se marca esta opción para que el servicio del sitio FTP se inicie automáticamente al arrancar el equipo.

Sin SSL: seleccionando esta opción de Secure Sockets Layer (Protocolo de Capa de Conexión Segura) desactivaremos este protocolo.

Permitir: con esta opción se tiene la posibilidad de conexión SSL o sin SSL.

Requerir SSL: marcando esta opción sólo se podría conectar mediante SSL.

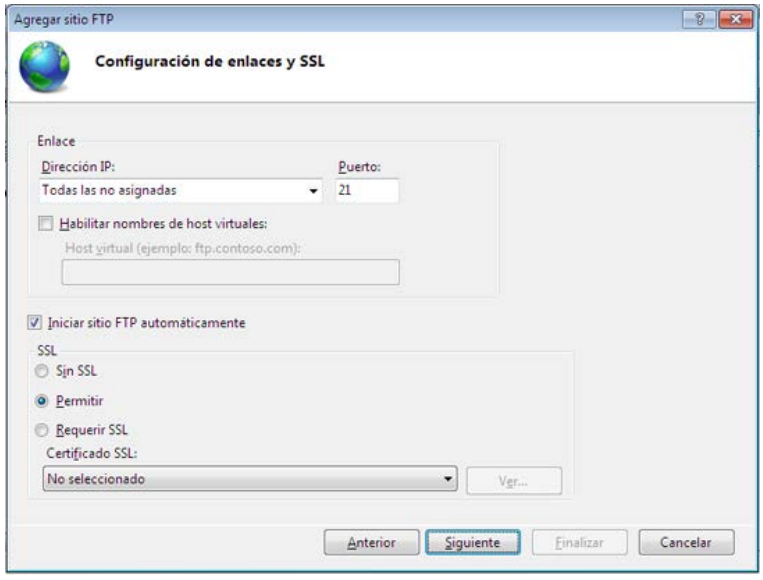


Fig. 4.1.1.11 Configuración de enlace y SSL

En "Información de autenticación y autorización" se puede indicar las siguientes opciones:

Autenticación anónima: es un método de autenticación integrado que permite a los usuarios el acceso a cualquier contenido público proporcionando un nombre de usuario anónimo y una contraseña. De forma predeterminada, la autenticación anónima está deshabilitada. Esta autenticación se usará sólo cuando se desee que todos los clientes que visiten el sitio FTP puedan ver su contenido.

Autenticación básica: es un método de autenticación integrado que requiere que los usuarios proporcionen un nombre de usuario de Windows y una contraseña válidos para obtener acceso al contenido.

La cuenta de usuario puede ser local en el servidor FTP o una cuenta de dominio. La autenticación básica transmite contraseñas no cifradas por la red. Solo se debe utilizar la autenticación básica cuando se tenga la certeza de que la conexión entre el cliente y el servidor está protegida con SSL.

Autorización: podremos indicar los usuarios del equipo Windows que tendrán permisos de acceso a la carpeta del sitio FTP:

En "Permitir el acceso a" podremos indicar:

Todos los usuarios: todos los usuarios del equipo tendrán los permisos indicados (lectura y/o escritura).

Usuarios anónimos: cualquier usuario tendrá los permisos indicados.

Roles o grupos de usuarios especificados: los grupos indicados tendrán los permisos de lectura y/o escritura.

Usuarios especificados: los usuarios indicados tendrán los permisos de lectura y/o escritura.

En "Permisos" indicaremos si queremos que los usuarios o grupos indicados puedan leer o escribir en la carpeta del sitio FTP.

Una vez configurado el servidor en el sistema operativo se debe configurar los permisos en nuestro enrutador para que este se vea a nivel de internet.

En un caso local caso debemos liberar el puerto en el router mediante port forwarding:

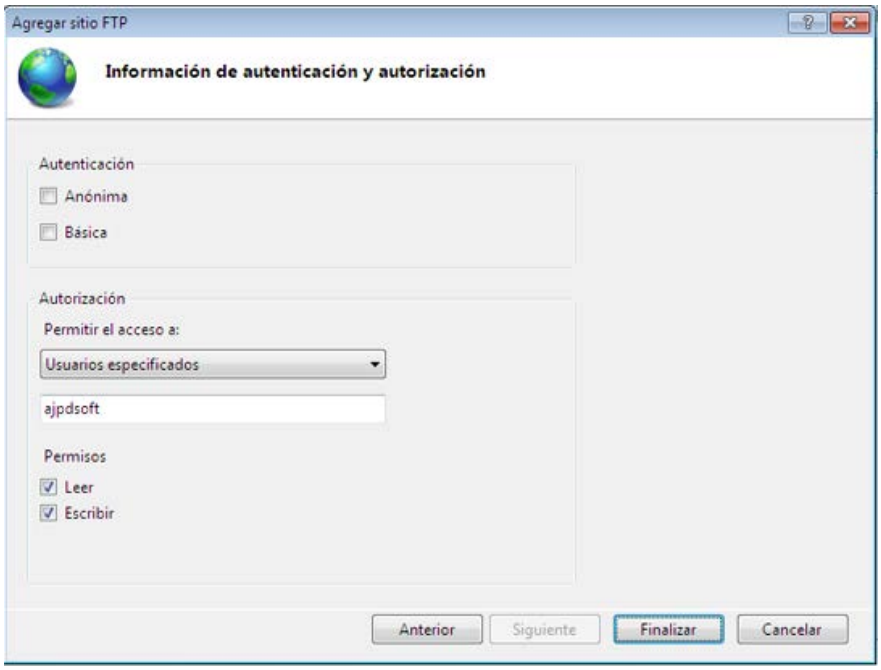


Fig. 4.1.1.12 Información de autenticación y autorización

Una vez creado el sitio FTP se debe administrarlo y configurarlo desde el Administrador de Internet Information Services (IIS):

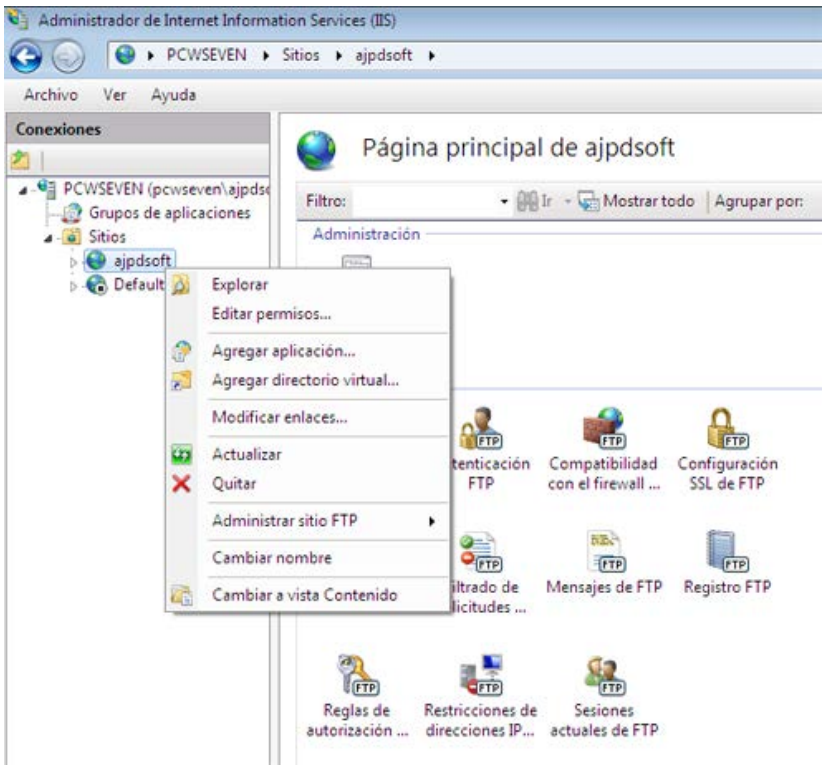


Fig. 4.1.1.13 Administrador de Internet

Luego de se necesita crear la regla para el puerto 21 en el router.

Se accede y configuramos en el router mediante port forwarding y creamos la regla para nuestra dirección ip local obtenida de cmd en nuestro caso es 192.168.0.45 y eso la colocamos en el router.

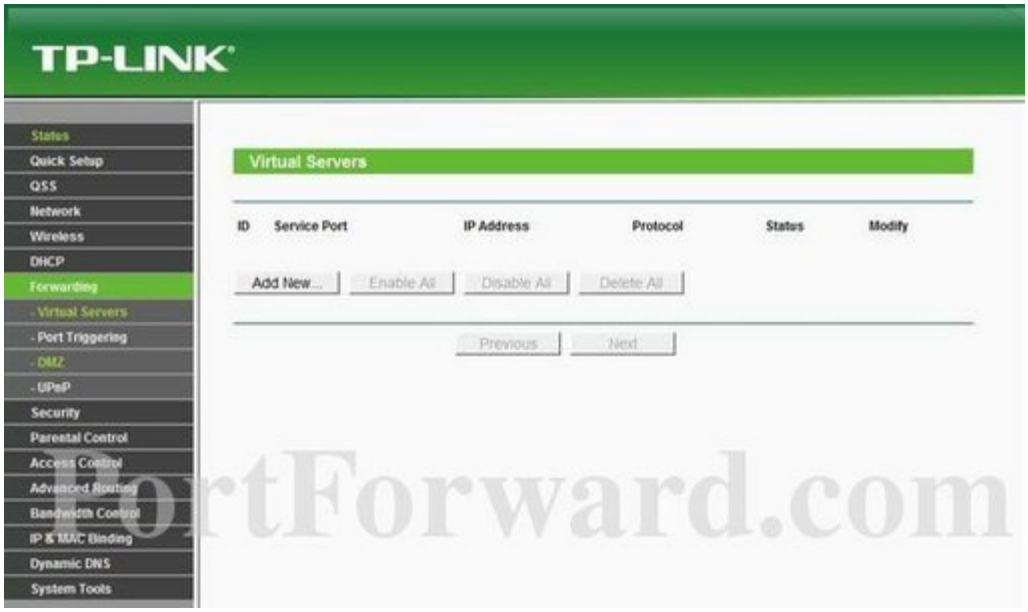


Fig. 4.1.1.14 Virtual Servers

Se debe dar clic en “Add New” y nos sale la siguiente pantalla y llenamos con los datos

Service port: 21

IP Adress: 192.168.0.45

Protocol All

Status: Enabled

Common service port: FTP y Clic en “save”.

Fig. 4.1.1.15 Virtual Server Entry

Con eso nuestro servidor FTP queda levantado y visible a nivel de internet.

Algunos proveedores de internet usan DHCP (Dynamic Host configuración protocol) y esto hace que la red cambie de dirección IP publica cada vez que se cambie o se termine de sesión de conexión. Para evitar esto se crea una cuenta de DDNS y se la asocia con la IP que hemos trabajado en el Router en nuestro caso es www.cottoortiz.ddns.net.

Ahora procedemos a configurar la cámara con nuestras direcciones IP pública en este caso es 190.107.81.85.

Llenamos con los siguientes datos:

Servidor FTP: 190.107.81.85

Puerto: 21

Usuario: CottoOrtizftp

Clave: 12345

Subir carpeta ftp: User/cottoortizftp

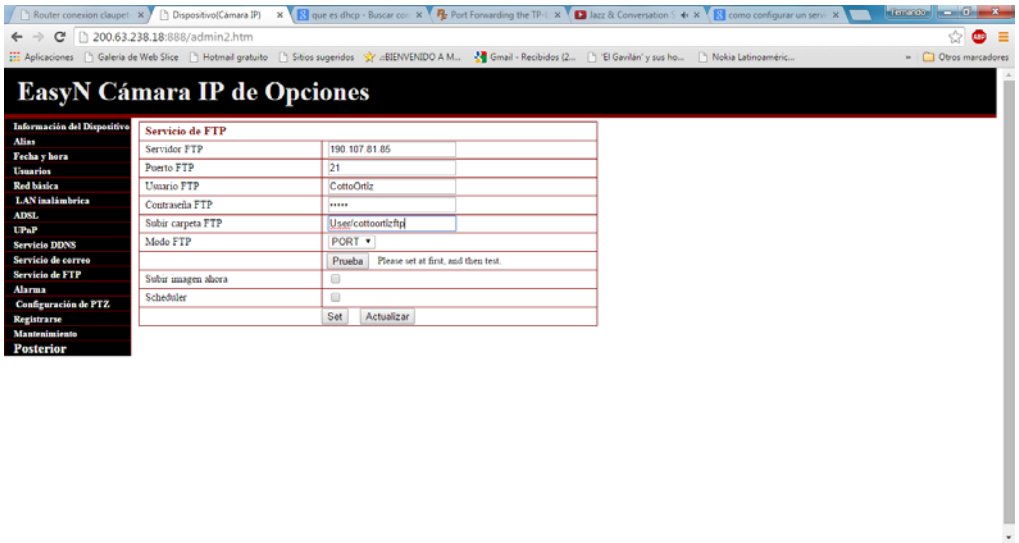


Fig.4.1.1.16 Opciones de la cámara IP EasyN

Una vez configurado las imágenes se subirán al servidor ftp.

4.1.2 Implementación y configuración de parámetros SMTP

La configuración de este parámetro SMTP es para añadir cuentas de correo electrónico que servirán para enviar y recibir imágenes de la alarma de detección de movimientos.

Esta cámara nos permite enviar imágenes desde de un correo electrónico y hasta 4 cuentas de correo pueden recibir simultáneamente imágenes detectadas por la cámara de vigilancia ip.
Los parámetros a configurar son:

- Remitente: Cuenta que se usa para enviar las imágenes feran2485@gmail.com
- Receptor: Pueden ser hasta 4 cuentas de correo diferentes
- Servidor SMTP: Es el servidor de la cuenta remitente smtp@gmail.com en este caso la cuenta remitente es feran2485@gmail.com
- Puerto SMTP: El caso de gmail es 587
- Capa de seguridad utilizada por el servidor de correo remitente: STARTTLS
- Necesidad de autenticación: Le damos un visto
- SMTP del usuario: La cuenta a usarse feran2485@gmail.com

- Contraseña: La clave del correo remitente

Luego de eso hacemos una prueba en donde antes de realizarla, debemos entrar en la cuenta de gmail y autorizamos que la aplicación de la cámara utilice este correo para enviar imágenes, informe de internet ip por correo y enviar la dirección IP de la cual pertenece la cámara.

4.1.3 Configuración de la cámara

1.- Instalar el CD de la cámara de vigilancia IP easyn y damos enter en Search IP camera

Fig. 4.1.3.1 Instalador CD de cámara de vigilancia IP

2.- Ponemos la opción Advance mode y damos enter

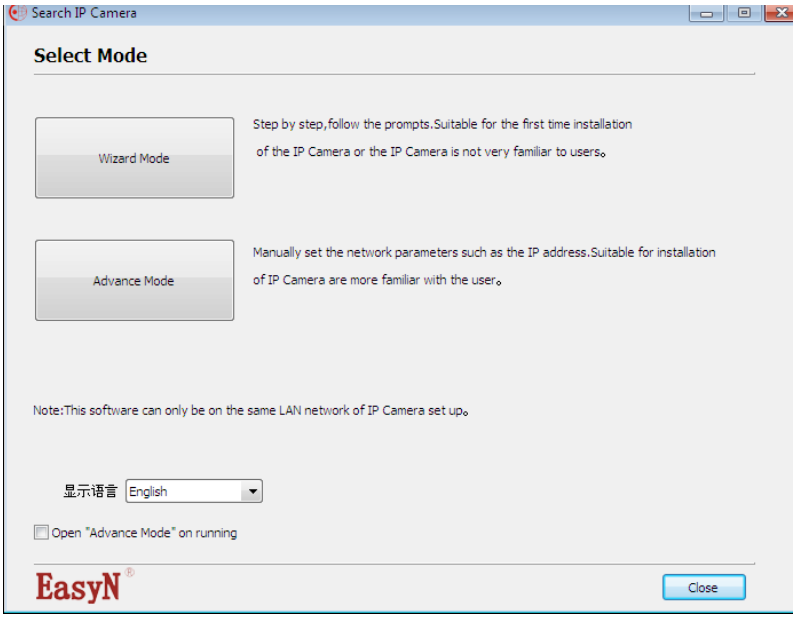


Fig. 4.1.3.2 Modo Avanzado

3.- Después de haber dado enter en Advance Mode hay que darce cuenta que el gateway que usa la cámara para poder configurar en el Inner Access debe ser htpp://192.168.0.3:888 es una configuración interna LAN.

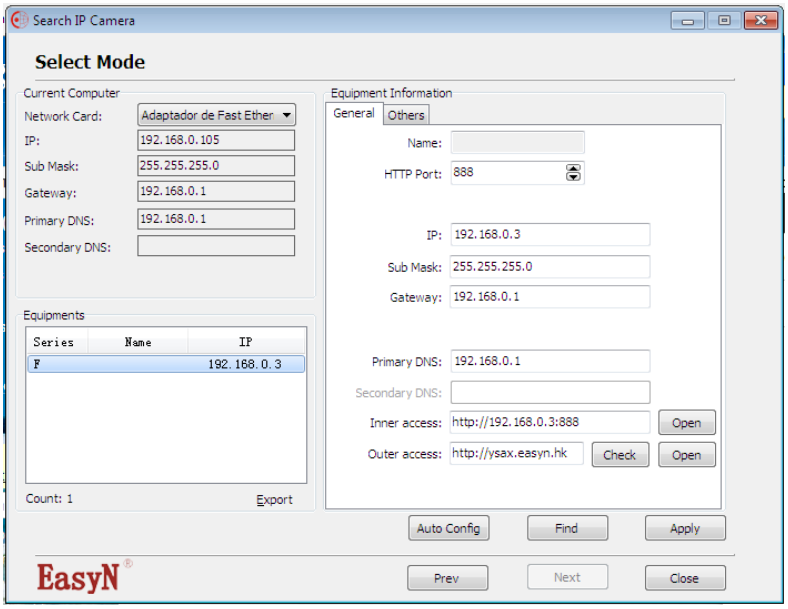


Fig. 4.1.3.3 Equipments

4.- Se copia el Inner Access y lo ponemos en un navegador cualquiera donde luego nos va pedir un usuario y clave

- Usuario: feran2485
- Clave: paulina20

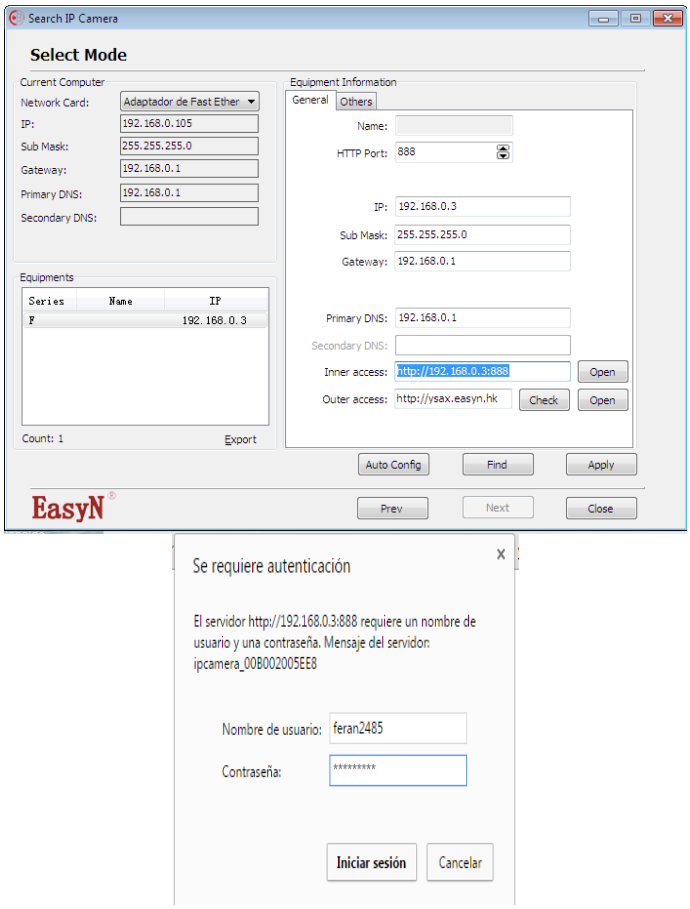


Fig. 4.1.3.4 Ingreso de usuario y contraseña

5.- Luego de poner usuario y clave tiene que aparecer una ventana donde se debe escoger la opción Server Push Mode

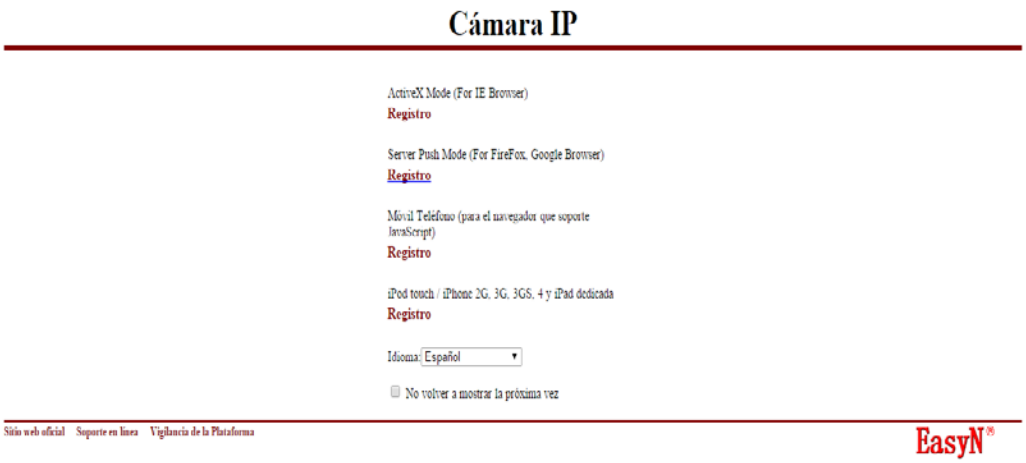


Fig. 4.1.3.5 Selección de monitoreo de cámara

6.- Configuración de la Red Básica

Fig. 4.1.3.6 Cámara de vigilancia IP en función

- Obtener IP de servidor DHCP: Esta opción lo dejamos en blanco
- Agregar IP: Ponemos nuestra IP 192.168.0.3
- Mascara de Subred: Es la que tiene nuestra Red
- Puerta de enlace: Que está dado por el router
- Servidor DNS: El traductor que es para la red LAN
- Puerto Http: El valor de 888

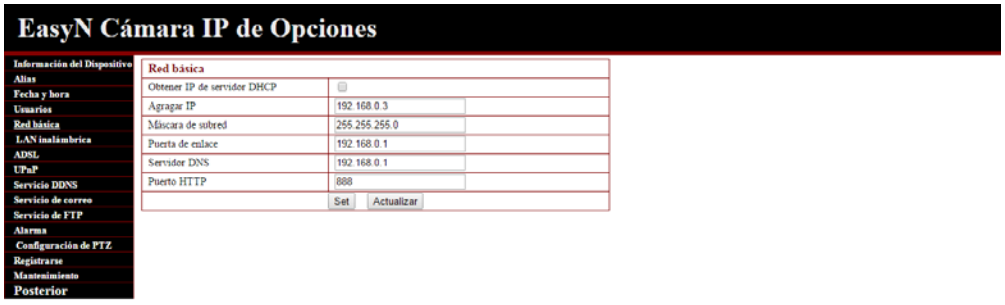


Fig. 4.1.3.7 Red Básica Opciones

7.- Servicio DDNS

Este Servicio DDNS es para la red global donde se puede acceder de cualquier punto del mundo, existen dos opciones:

1. Servidor DDNS
2. Servidor Port Forwarding

Servidor DDNS.- Este servicio se lo debe utilizar para las compañías que tienen IP dinámicas, si se quiere entrar con la dirección IP puede que la compañía la haya cambiado y si es el caso se tiene que volver a configurar.

La configuración de servicio DDNS para la cámara es:

- Servicio DDNS: Ponemos la opción IP cam
- Usuario DDNS: Ponemos ysax
- Contraseña DDNS: Para nuestra camara 316725 (Contraseña previamente configurada de fábrica).
- DDNS o Servidor Proxy: Ponemos ysax.easyn.hk
- DDNS o Puerto Proxy: El puerto que utiliza esta configuración es el 80

Para saber que el servicio DDNS está correctamente configurado al final de este le damos ¨set¨ en donde la condición DDNS debe ser ¨Succedd¨.

Servidor Port Forwarding.- Se debe entrar con la dirección de la puerta de enlace predeterminado o la dirección del router que en nuestro caso es 192.168.0.1 esta dirección IP es la del router.

Se pone en el navegador la dirección IP del router en donde nos va pedir usuario y contraseña, donde el usuario y contraseña es ¨admin¨.

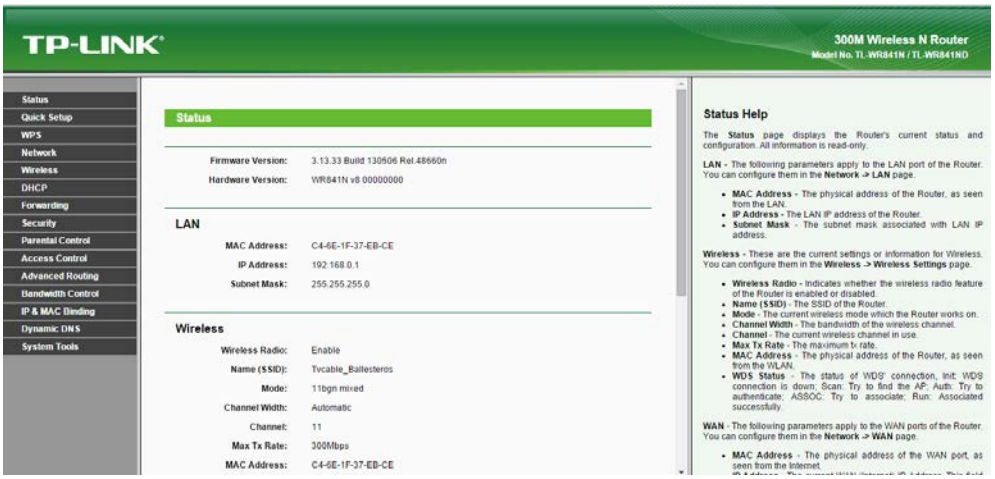


Fig. 4.1.3.8 Servidor Port Forwarding

Vamos a la opción forwarding→Virtual Servers cogemos la opción Add New y llenamos con los siguientes parámetros:

- Service Port: Se pone el puerto 888
- Internal Port: Configurado automáticamente por el router
- IP Adress: Se pone la dirección que nos da la cámara que fue asignado por el router 192.168.0.3
- Protocolo: Existen tres opciones All-TCP-UDP, vamos utilizar ambos protocolos ¨All¨.
- Status: Se pone Enabled (Avilitado).
- Common Service Port: Esta opción lo dejamos en blanco

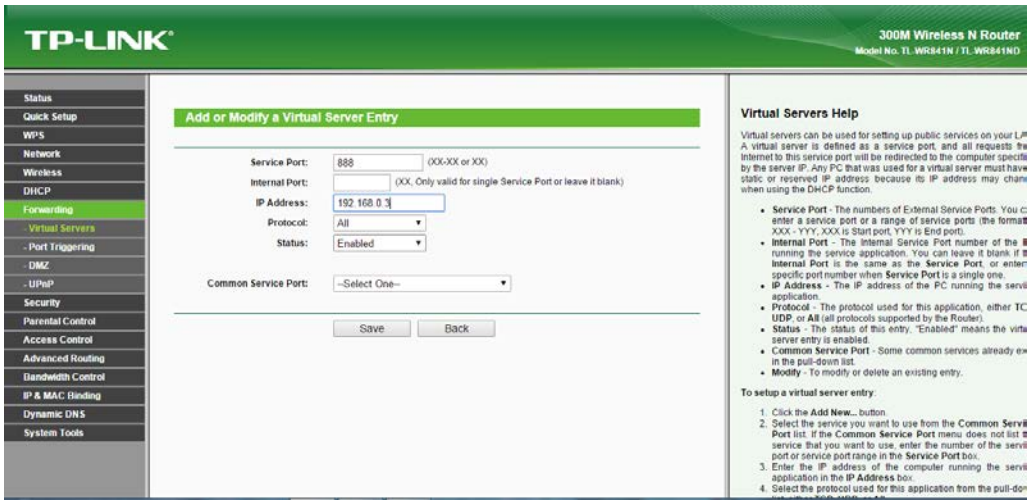


Fig. 4.1.3.9 Forwarding Virtual

8.- Configuración de PTZ

La configuración PTZ es para el movimiento de la cámara en su eje vertical y horizontal y para el zoom, donde se debe definir ciertos parámetros:

- Habilitar Predefinido: Se habilita, para que posteriormente configurar los demás parámetros
- Comienza a correr a la especificada preestablecida: Velocidad para que se mueva la cámara velocidad del 1-15, donde el menor número es la mayor velocidad y el mayor numero la menor velocidad
- Velocidad PT: Velocidad Pan-Till, esta es la velocidad de enfoque vertical y horizontal

- Velocidad de Patrulla hacia arriba: Es la velocidad de la cámara hacia arriba que va del rango del 1-15 donde el menor número es la mayor velocidad y el mayor la menor velocidad
- Velocidad de Patrulla hacia abajo: : Es la velocidad de la cámara hacia abajo que va del rango del 1-15 donde el menor número es la mayor velocidad y el mayor la menor velocidad
- Indicador de Modo de Visualización: Se debe poner que ha extinguido para que el indicador se mantenga apagado por discreción

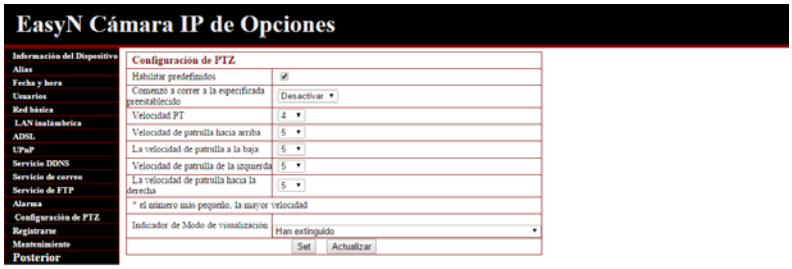


Fig. 4.1.3.10 Configuración PTZ

4.1.4 Software.

Para poder controlar, configurar y monitorear la cámara se necesita la ayuda de software ya sea aplicaciones o programas que nos brinden facilidades para la cámara.

4.1.4.1 Software para controlar cámara.

Existen dos maneras de controlar la cámara:

- Software Central Management System.
- Acceso remoto IP.

El software CMS (Central Management System) es el programa que va instalado en la computadora que va a servir para monitorear, grabar video, hacer capturas de pantalla cuando el sensor de movimiento este activado.

Fig. 4.1.4.1.1 Software CMS

Lo primero que se debe hacer en este software es encontrar la cámara para poder controlarla en los parámetros ya establecidos anteriormente.

Primero lo se lo instala, una vez instalado va a pedir un usuario y clave los cuales son:

Usuario: admin.

Clave: password.

Luego se debe proceder a buscar la cámara, en el símbolo  y nos aparecerá una tabla y le damos clic en “search”

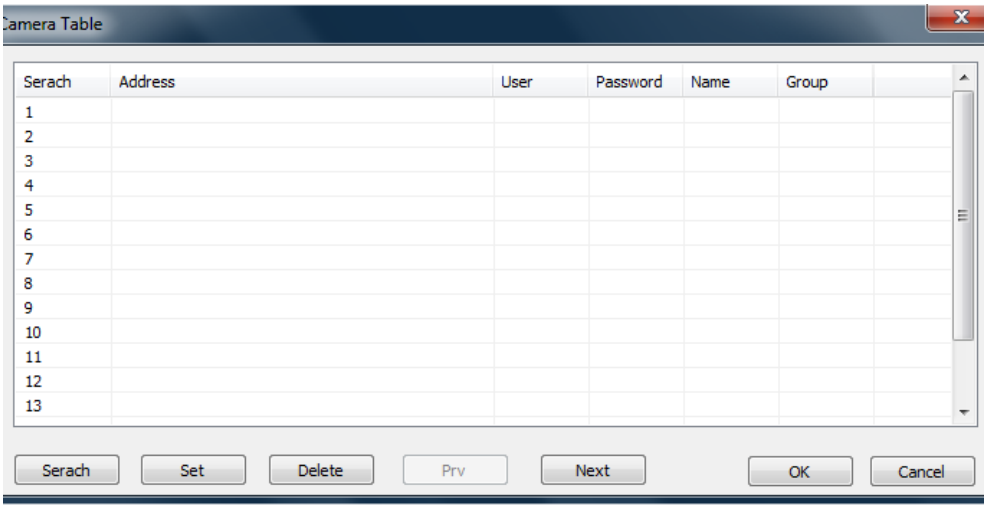


Fig. 4.1.4.1.2 Camera Table

Se nos despliega un menú y la dirección IP de la cámara debe salir en device list le damos clic en la cámara luego en “add”.

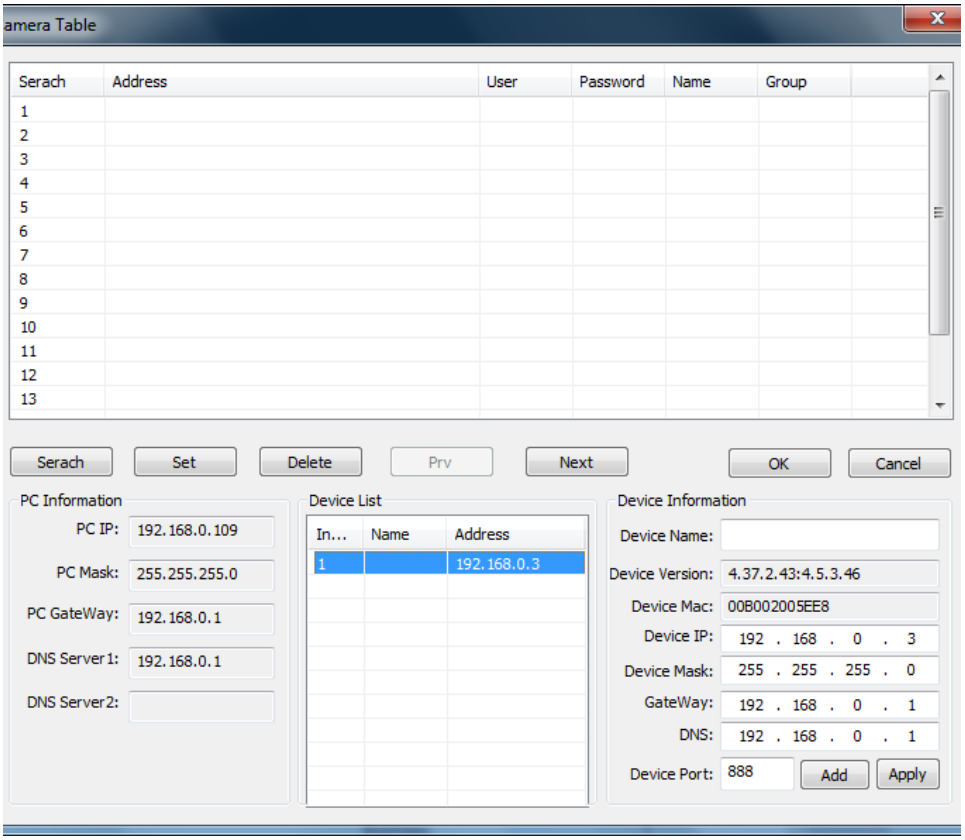


Fig. 4.1.4.1.3 Device List

Se nos va a desplegar una ventana donde nos pide el usuario y clave de acceso remoto de la cámara:

Usuario: feran2485.

Clave: paulina20.

Damos clic en aceptar 2 veces y la cámara debe aparecernos en la pantalla principal del programa.

En la cámara nos muestra la fecha, el canal usado y la hora en esta ventana se puede modificar la frecuencia, resolución, brillo y contraste.

Este programa permite controlar la cámara en tiempo real desde el ordenador sin necesidad de entrar a un navegador para monitorear por acceso remoto.

- Acceso remoto IP.

Este método es utilizado más cuando no tenemos al alcance el PC donde tenemos instalado el software anteriormente descrito y aunque no es tan completo como al anterior, tiene características interesantes:

- Configuración de la cámara.
- Activación de alarmas.

Para poder utilizar esta opción se abre un navegador (recomendamos usar Mozilla, Firefox) e ingresamos la dirección IP de la cámara con el puerto utilizado http://192.168.0.3:888 y nos va a pedir usuario y clave.

Usuario: feran2485.

Clave: paulina20.

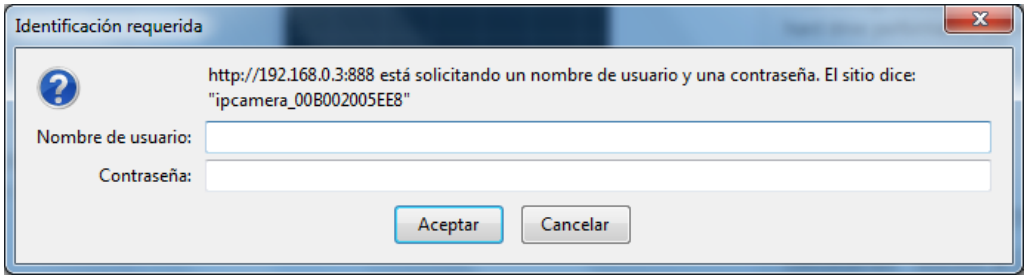


Fig. 4.1.4.1.4 Identificación Requerida

Una vez ingresado tiene que aparecer la ventana de acceso y da 4 opciones para ingresar a controlar la cámara, las opciones se dan para Internet Explorer, Mozilla o Chrome , para ipad o iphone o para dispositivos móviles android u otros. En nuestro caso estamos desde una laptop y usamos mozilla entonces escogemos 2da opción y damos clic donde dice “registro”.

Fig. 4.1.4.1.5 Ventana de Acceso

Tiene que aparecer la ventana para el control de la cámara

Fig. 4.1.4.1.6 Control de la Cámara

Desde esta ventana el firmware va a permite controlar el movimiento de la cámara, la resolución, frecuencia el contraste y el movimiento de PTZ de la misma.

4.1.4.2 Software para visualizar la cámara en tiempo real.

El mismo software de control de la cámara descrito en la parte anterior nos sirve visualizar la cámara en tiempo real el primero (CMS) de manera local y por medio de la IP publica del sistema se puede hacerlo de manera remota desde la Internet.

A continuación se muestra como se accede desde cualquier parte para la visualización del mismo.

Primero se investiga cual es la dirección IP de la red WAN, esto lo hacemos mediante cualquier página que muestre la dirección en nuestro caso usamos la página www.myipadress.com y muestra que la IP de este sistema es 200.25.165.185.

Fig. 4.1.4.2.1 Dirección IP de la red WAN

Luego accedemos desde otro computador o dispositivo móvil que no sea parte de nuestra red LAN y colocamos la dirección IP de arriba más: 888 que es el puerto que usa nuestra cámara.

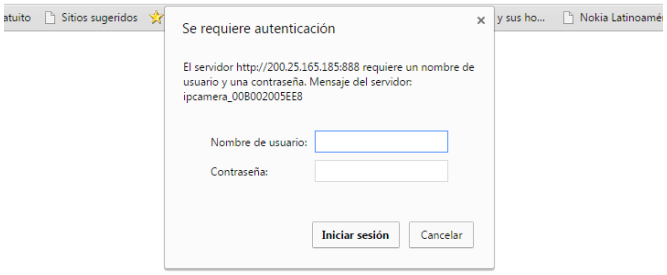


Fig. 4.1.4.2.2 Autenticación

Donde pide usuario y clave y se ingresa.

Y nos da esta pantalla.

Fig. 4.1.4.2.3 Cámara en uso desde la PC

De esta manera se puede monitorear desde cualquier computador en el mundo esta cámara

.

4.1.4.3 Instalación de aplicación en dispositivos móviles.

La aplicación que se tiene que utilizar a utilizar se llama IP cam Viewer pro y la podemos descargar desde cualquier aplicación gestora de descargas en Iphone o Android.

Fig. 4.1.4.3.1 IP Cam Viewer

Una vez descargada se procede a configurarla.

Fig.4.1.1.3.2 Aplicación en dispositivo Móvil

Se toca el símbolo  para añadir la cámara y nos da esta una pantalla y la llenamos con la información de nuestra cámara y luego

nos sale los diferentes tipos de cámaras que pueden ser configurados y escogemos la opción cámara IP, DVR, NVR

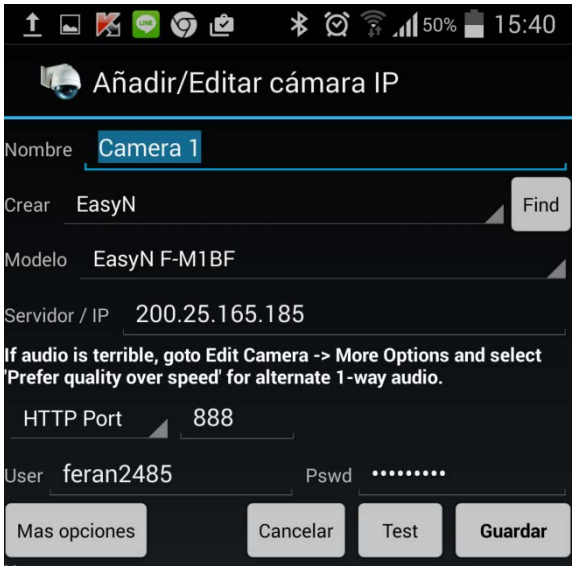


Fig. 4.1.1.3.3 Configuración de Cámara en Dispositivo Móvil

Los datos que debemos ingresar son:

1. Nombre:(colocamos camera 1).
2. Crear: (escogemos la marca de la cámara).
3. Modelo de la cámara.
4. La dirección IP publica asociada a nuestra red WAN , en el caso nuestro es 200.25.265.185
5. Http Port: 888
6. Usuario: feran2485
7. Clave: paulina20

Si los parámetros ingresados están bien al hacer test saldrá una imagen abajo como esta:

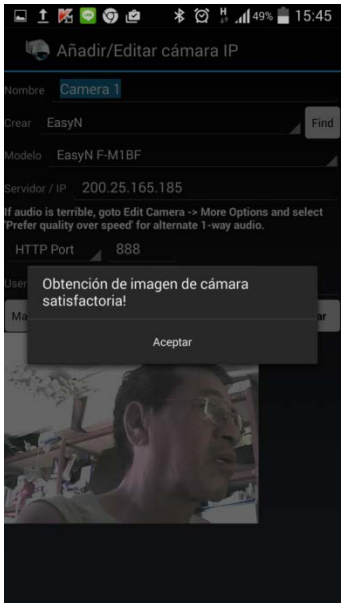


Fig. 4.1.1.3.4 Obtención de Imagen desde Dispositivo Móvil

Una vez ya configurado los parámetros en el dispositivo móvil la cámara puede ser monitoreada y controlada de manera remota desde el dispositivo móvil.

Fig.4.1.1.3.5 Control de Brillo desde el dispositivo Móvil

Con esta aplicación se puede controlar el movimiento, brillo, contraste, control PTZ, sonido y capturas de imagen, además que también permite la visualización de varias cámaras de manera simultánea.

4.2 Pruebas

Se configura la cámara con una alarma para detección de movimientos y que las imágenes capturados por nuestra cámara de vigilancia IP easyn sean enviadas por correo electrónico a los usuarios previamente configurado.

Para configurar la alarma existen más parámetros que pueden ser modificables como la sensibilidad de movimiento.

- Sensibilidad de Movimiento: Va desde un rango de 1-10 donde el menor número es la mayor sensibilidad y el mayor numero la menor sensibilidad
- Entrada de Alarma Armada: La alarma puede ser configurada algún aparato a la cámara detecta un movimiento se activa algún sonido
- Enviar un Mensaje de Alarma: Se configura para enviar un correo
- Subir Imágenes de Alarma: Para guardar o almacenar la imagen en el servidor FTP
- Scheduler: Es un programador de la alarma para configurarla para días y horas para cuando la alarma se va activar

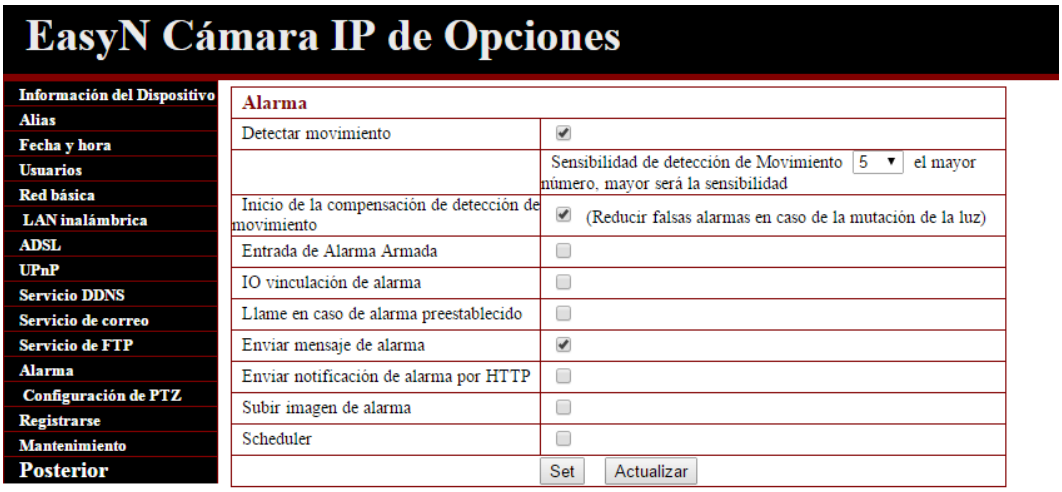


Fig. 4.2.1 Alarma

Fig. 4.2.2 Detección de Movimiento

Prueba de envío de la dirección IP por correo electrónico.

Hay compañías que suelen cambiar la dirección IP que asignan a los usuarios finales, la cámara nos da la opción de mandar una alarma de correo electrónico indicando que dirección URL es la que se está usando en el sistema de la cámara.

En el gráfico se muestra que han sido enviados mensajes desde el correo remitente donde la cámara inicialmente estaba con la dirección IP http://200.25.165.185:888 a las 9:43 am y luego la cámara fue cambiada de lugar físico y por ende de proveedor de servicio de internet y la dirección IP cambio a http://200.63.238.18:888 a las 11.34am.

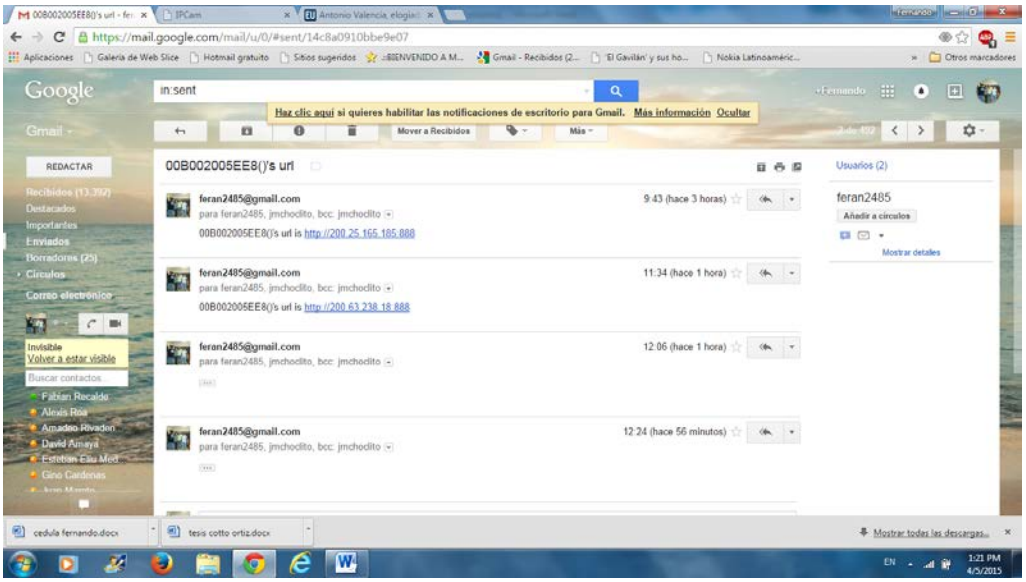


Fig. 4.2.3 Cambio de URL

Otra opción que tiene la cámara de vigilancia es la grabación de video y esa configuración se la puede hacer central management system, se puede programar día, hora y el tiempo que se necesita el video según las necesidades del usuario.

Fig. 4.2.4 Grabación de Video desde la Cámara de Vigilancia

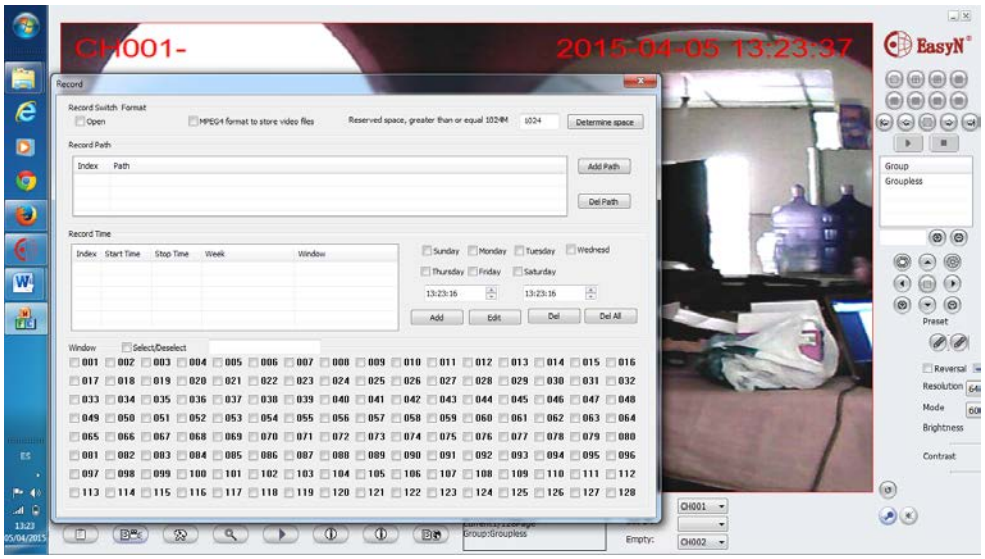


Fig. 4.2.5 Record Time

4.3 Ambiente de Pruebas

En el ambiente de prueba dependerá donde se encuentre nuestra cámara de vigilancia IP, pueden ser en ambientes diurnos y nocturnos, las pruebas las podemos realizar desde cualquier parte del mundo desde una PC o un dispositivo móvil teniendo el software de la cámara de vigilancia easyn.

La cámara de vigilancia tiene varios usos óptimos una de ellas es el sensor del movimiento y este al activarse empieza a grabar o tomar fotos de donde se lo enfoque y a su vez esa foto se puede enviarse o que se activa la alarma y avisa a un correo electrónico receptor de las imágenes.

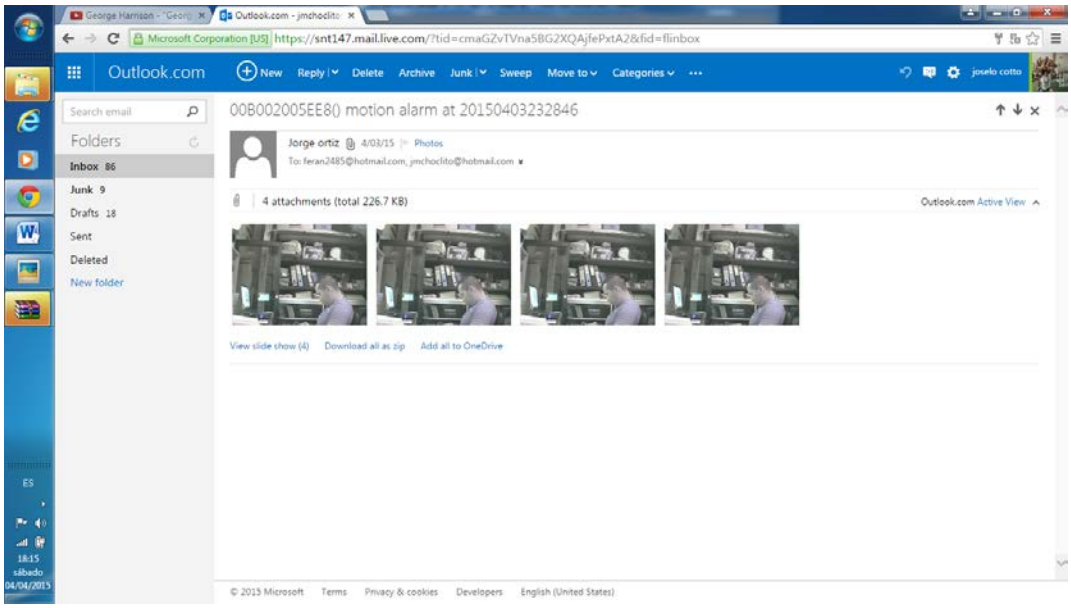


Fig. 4.3.1 Pruebas de envió Sensor de Movimiento

El sensor de la cámara cada que detecta el movimiento, envía simultáneamente correos electrónicos con las fotos enfocadas en un ambiente diurno como en este caso

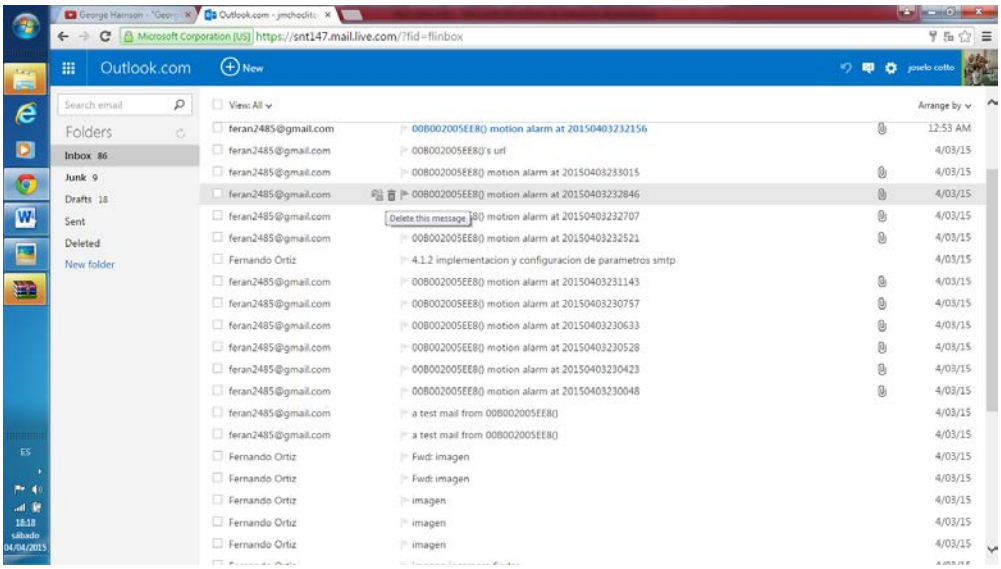


Fig. 4.3.2 Prueba de Envió de Correos

Otra de las funciones que tiene la cámara de vigilancia IP easyn es la capacidad de visión nocturna y que esta proporciona las misma funciones que con visión normal.

Fig. 4.3.3 Prueba Visión Nocturna

Dentro de las demás opciones que tiene esta cámara de vigilancia es el audio bidireccional, es decir se puede escuchar la conversación y el operador puede hablar a él o los individuos que se encuentren donde esta nuestra cámara de vigilancia IP easyn.

4.4 Recursos utilizados para ejecutar las pruebas

Los recursos que tenemos para ejecutar las pruebas son tres:

1. Servidor de correo de gmail
2. Firmware de la cámara
3. Software CMS instalado en la PC principal

Servidor de correo de gmail.- Es un servidor confiable de correo electrónico que está haciendo utilizado en el sistema de cámara IP, nos sirvió para configurar el correo remitente de los mensajes de alarma o de los mensajes de cambio de dirección URL.

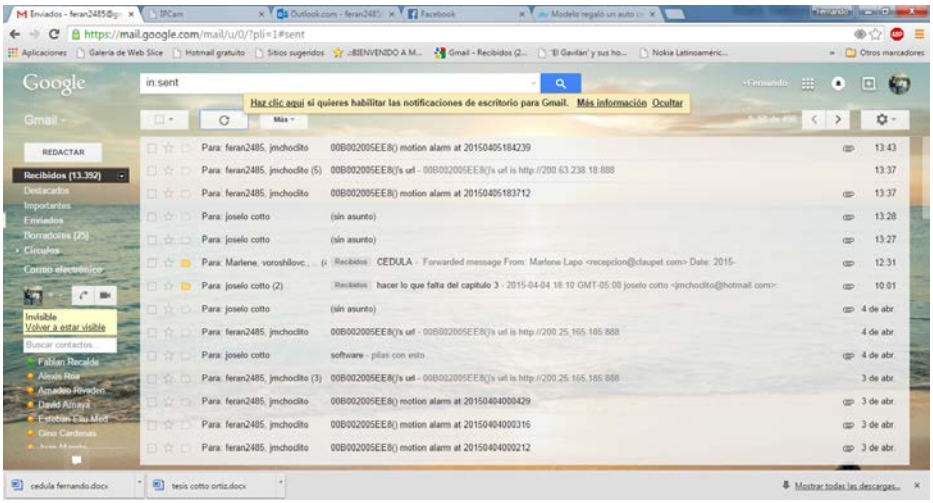


Fig. 4.4.1 Servidor de correo Gmail

Firmware de la cámara.- Sirve para configurar la alarma de detección de movimiento, este software es proporcionado por la propia cámara.

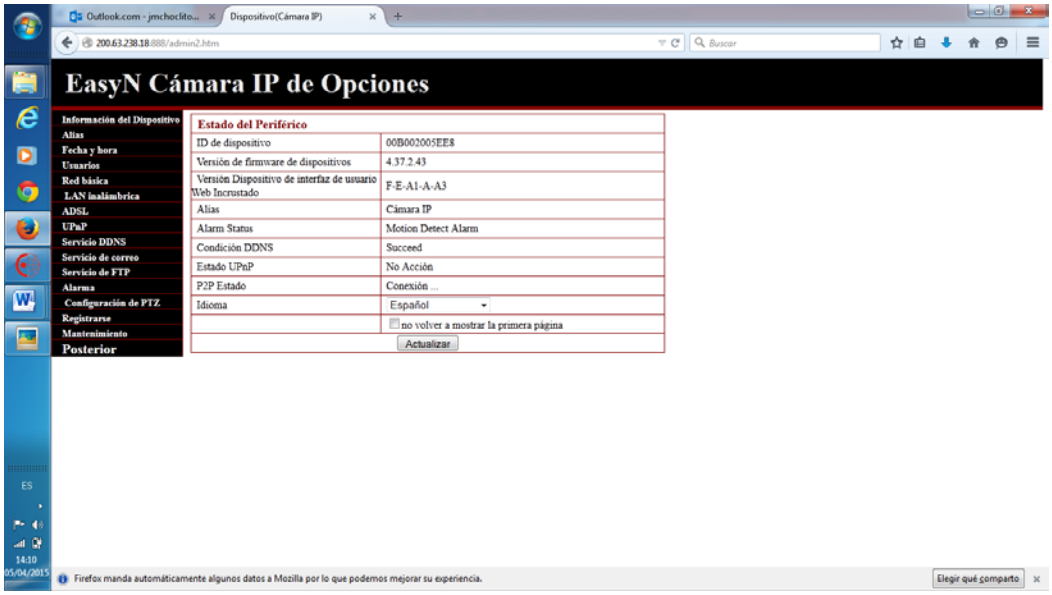


Fig. 4.4.2 Estado del Periférico

Software CMS instalado en la PC principal.- Este software es utilizado para la grabación y configuración de videos.

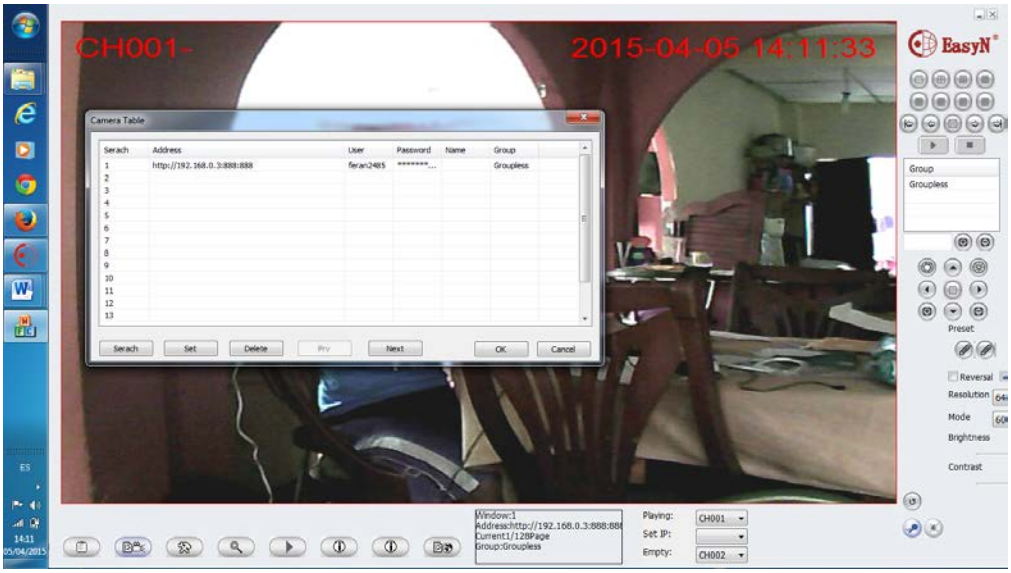


Fig. 4.4.3 Software CMS en maquina Principal

4.5 Verificación de proceso de pruebas

Prueba de alarma de correo electrónico

Para verificar si la cámara está enviando los mensajes de correo con las imágenes de la alarma de detección de movimiento desde el correo remitente, se debe verificar si coincide el asunto del correo enviado con el asunto del correo recibido y su contenido.

A continuación en la imagen de la bandeja de enviados del correo remitente observamos un correo de los que dicen *alarm motion* y el código que tiene.

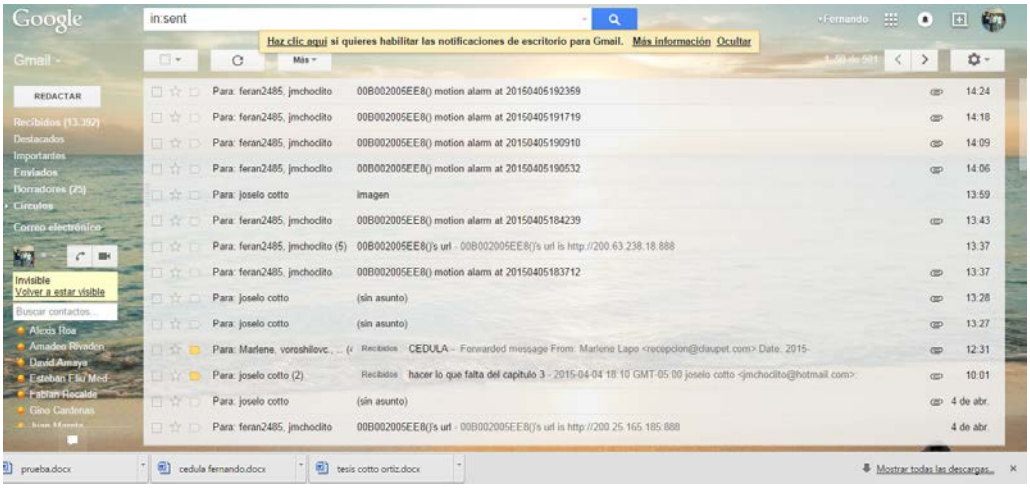


Fig. 4.5.1 Proceso de Prueba

Se puede observar que uno de los correos el código que está en el asunto es 20150405190532.

Ahora verifiquemos el código en una de las cuentas de correo electrónico receptoras.

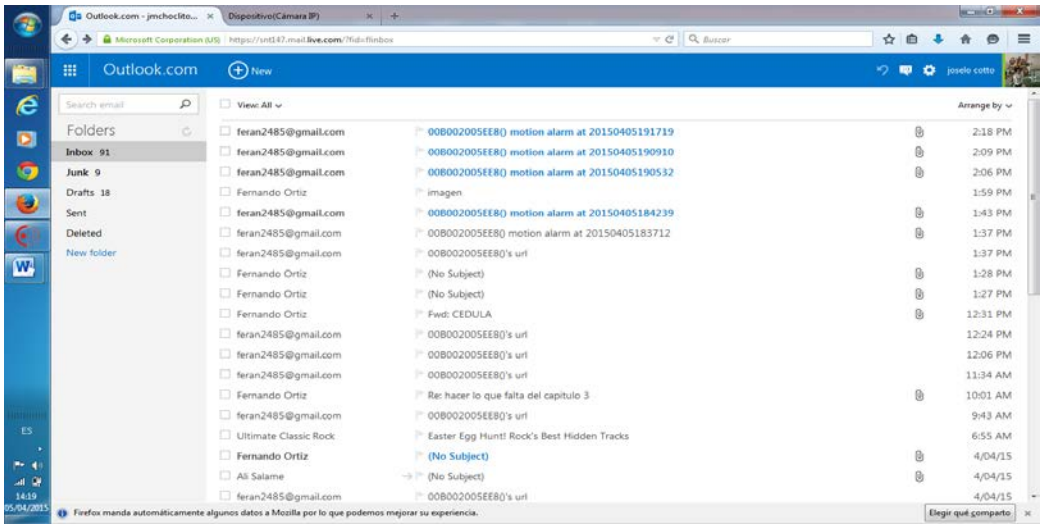


Fig. 4.5.2 Cuenta Receptora

Y el código en uno de los correos en la bandeja de entrada es 20150405190532 que coincide con el código de uno de los correos en la bandeja de entrada.

Prueba de grabación de video.

Para la verificación de la grabación de video lo que vamos es a comprobar si el programa CMS (Central Management System) está grabando video. Lo que vamos a hacer es grabar un pequeño video y luego reproducirlo dentro del mismo programa para verificar las imágenes.

Empezamos grabando el video:

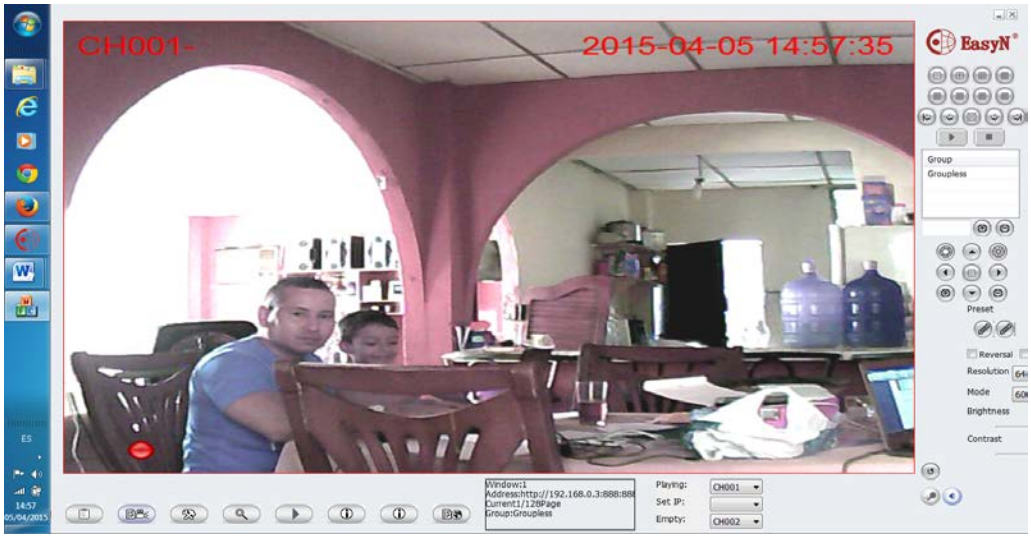


Fig. 4.5.3 Prueba Grabación de Video

El punto rojo en la parte inferior izquierda indica que la cámara está grabando un video dentro del programa. Ahora se procede a observar y de esta manera verificar que graba el video.

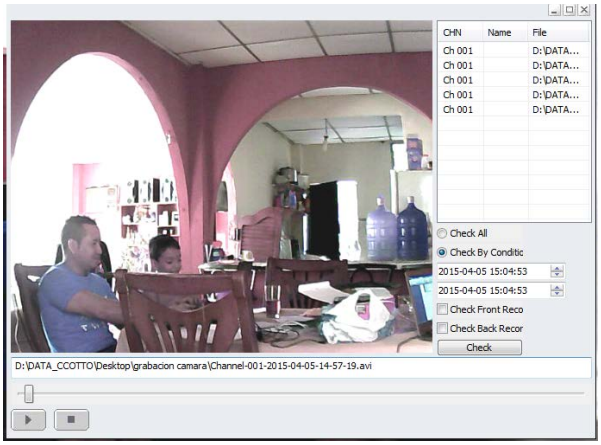


Fig. 4.5.4 Prueba de Video Grabado por la cámara de seguridad IP

En el reproductor se puede ver de manera normal el video con todos los movimientos que se hicieron.

Verificación de mensaje de URL

Esta prueba se la realiza ingresando a una de las cuentas de correo electrónico receptoras y abrimos un correo electrónico con el asunto 00B002005EE8 ()'s url en donde nos aparece un mensaje asi:

00B002005EE8 ()'s url is http://200.63.238.18:888

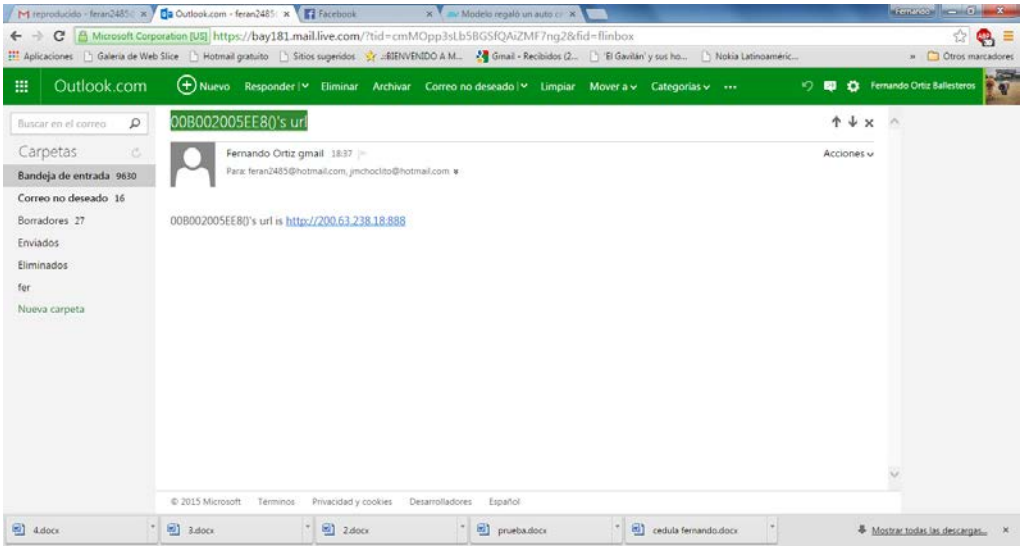


Fig. 4.5.5 Verificación de mensaje URL

Esta es la dirección URL que está usando nuestro sistema, se de hacer clic en la misma ya que es un vínculo y como resultado nos lleva a la cámara IP.

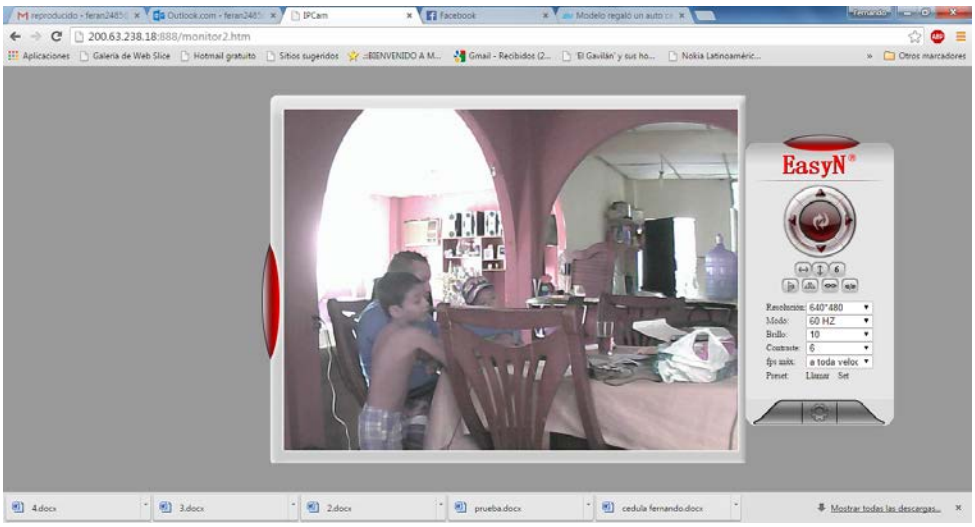


Fig. 4.5.6 Verificación de dirección URL

4.6 Documentación de las Pruebas

Prueba de alarma en la detección de movimientos

Donde dependerá de la sensibilidad con la que ha sido configurada la cámara y del tiempo de movimiento que será detectado y estas imágenes captadas por la cámara de vigilancia serán enviadas al

correo receptor con un mensaje que tiene como asunto ¨motion alarm¨.

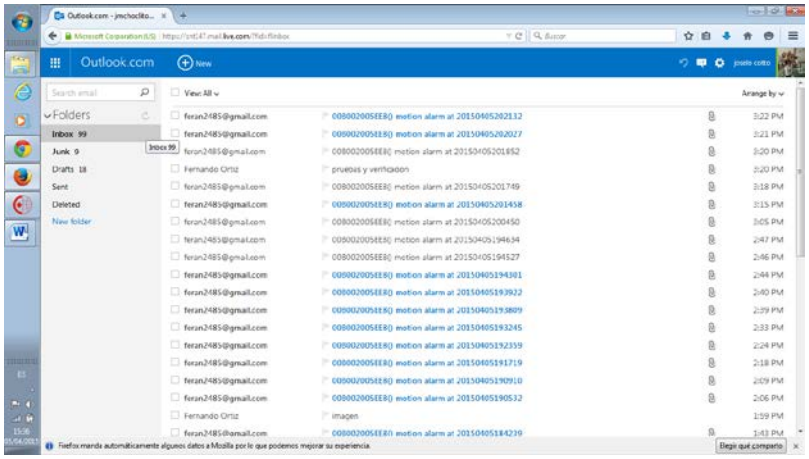


Fig. 4.6.1 Prueba de alarma en la detección de movimientos

Fig. 4.6.2 Imágenes captadas en la detección de movimientos

Prueba de notificación de URL o IP

Cuando la cámara de vigilancia es conectada en otro sitio con una IP diferente o si la dirección IP es cambiada en el mismo sitio, llegara al correo receptor la dirección IP de ese lugar.

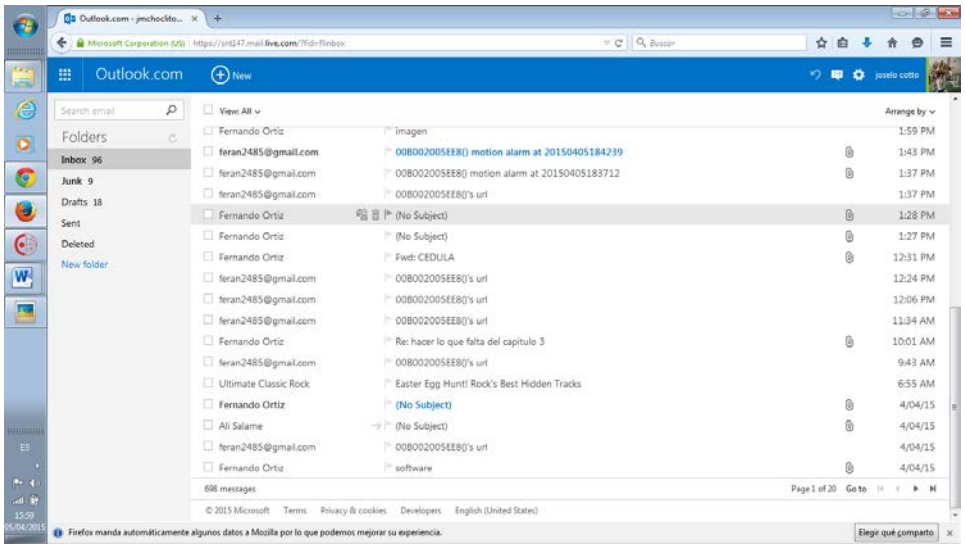


Fig. 4.6.3 Prueba de notificación URL o IP

Prueba de grabación de video.

Para la verificación de la grabación de video lo que vamos es a comprobar si el programa CMS (Central Management System) está grabando el video, este que será grabado dependiendo las necesidades del usuario, desde horas, hasta días de grabación.

Fig. 4.6.4 Prueba de Grabación de Videos desde CMS

4.7 Resultado del Sistema

Con la correcta implementación del sistema de vigilancia da como resultado múltiples ventajas: facilidad en el uso, capacidad de grabación y visualización simultánea sin pérdida de calidad en la imagen, mejora de la compresión y mayor potencial de integración. Además ofrece otras ventajas como son:

a) Accesibilidad remota: el principal beneficio ganado con las cámaras IP es que basados en su configuración y una modificación en el enrutador se puede acceder a la cámara o nuestro sistema desde cualquier parte del mundo en donde se tenga internet. Además se

puede conectar varias cámaras con diferentes IP públicas en un mismo software instalado en una computadora desde cualquier lugar.

b) Almacenamiento seguro e ilimitado: gracias a la capacidad de configuración del sistema podemos incluir o disponer de cualquier carpeta que este dentro de nuestro sistema operativo para poder almacenar información obtenida desde la cámara.

c) Distribución flexible y proactiva de imágenes: se pueden obtener imágenes de algún movimiento inesperado o incidente dentro del rango de observación que tenga nuestra cámara y por ende se envían por correo electrónico o son subidas las imágenes al servidor FTP y se pueden revisar en cualquier momento.

d) DDNS: existe problema cuando se tiene proveedores de servicio con DHCP el cual nos puede causar pérdidas de tiempo al momento de querer encontrar con que IP publica está trabajando nuestra cámara, pero ahora las cámaras IP vienen con una dirección URL que ayuda y puede ser configurada para que accedamos a ella como si fuera una página web.

e) Alertas: En las alertas el cliente final se puede respaldar de movimiento que no espera por parte de desconocidos y además estas pueden ser almacenadas simultáneamente en correos electrónicos o páginas web.

f) Rendimiento y costo total del sistema:

g) En cuestión de rendimiento y mantenimiento ya no se tiene que recurrir a sistemas externos para grabación de videos sino que solo basta configurar el sistema hasta que capacidad necesite guardar y por cuanto tiempo, por lo cual se tiene un alto rendimiento a un bajo costo.

CONCLUSIONES

1. Se cumplió con el objetivo realizar el diseño correcto del sistema de vigilancia dando como resultado que todas las pruebas que se hicieron tuvieron resultados positivos y esto permitió que funcione de manera correcta sin mayor complicación ni imprevisto.

2. En el caso de la transmisión de la información se obtuvo como resultado la instalación de un router inalámbrico que transmitirá la información a través de internet permitiendo el monitoreo remoto. Con el diseño del sistema de vigilancia, se logró usar equipos con la tecnología de red inalámbrica, lo cual permitió cubrir completamente el ambiente de diseño propuesto, de una manera eficiente y moderna. Esto se pudo comprobar, la verificación visual de la cámara de todo el espacio a monitorear, quedando sin puntos ciegos para la vigilancia.

3. Asimismo, se logró el objetivo de evitar la instalación de cableado necesario para estos sistemas al utilizar equipo inalámbrico. Además, con el sistema inalámbrico se logra una mejor recepción en comparación con el cableado donde ocurren perdidas en áreas de gran extensión. De la misma forma, se logró reducir el presupuesto ya que no se necesitó cablear un punto de red para nuestra cámara IP.

4. Con la utilización de la red IP y red inalámbrica se facilita el crecimiento del sistema cuando se requiera, debido a su escalabilidad que permite aumentar un equipo nuevo sin la necesidad de otros equipos adicionales, sino solo con la configuración necesaria.

5. Se concluye que la cámara representa un gran aliado para usuarios o clientes que no cuenten con muchos recursos económicos para contar en su hogar o pequeño negocio sistemas complejos de vigilancia IP que pueden incluir hasta guardias de seguridad.

6. Por otro lado se concluye, que el software mejora la calidad del servicio comparado con un sistema analógico o un sistema DVR en aspectos como la calidad de imagen al utilizarse cámaras de red digitales, en el almacenamiento al usar servidores o PC´s de uso doméstico en contraste con las cintas de video, y en el medio de transmisión inalámbrico que facilita la instalación y elimina el costo de cableado.

7. Finalmente, con los equipos propuestos en este tema de estudio, se logra que el usuario final comprenda el funcionamiento del sistema de una manera fácil y sencilla dando como resultado la operación optima de cada elemento en acción.

RECOMENDACIONES

1. Para realizar las pruebas para un correcto diseño hay que tomar en cuenta el número de cámaras que se requieren en el sistema, en esta caso solo se necesita de una cámara, por lo tanto, no fue necesario el uso de otra herramienta, pero si el sistema, es grande, entonces será necesario el uso de simuladores de cámaras de seguridad para cubrir una mayor área y evitar que queden puntos sin observación.

2. Debe tomarse en cuenta el lugar en donde se va a instalar una cámara para que esta opere de manera correcta y además no vaya a ser destruida por algún factor ajeno al sistema, en el caso de exteriores hay que verificar que la cámara en uso soporte condiciones al exterior.

3. Para obtener una buena calidad de imagen se tomar en cuenta que cámara se va usar y cuanto se cuenta de presupuesto para poder obtener algo equilibrado en función de costo y beneficio, además para la transmisión en tiempo real se debe contar con un servicio de internet de banda ancha alto para tener imágenes sin pixelaje o algún tipo de retardo.

4. Debe tomarse en cuenta al momento de diseñar el sistema que requiere el usuario final o el cliente, en este caso como diseñador de un sistema se aconseja que se debe hacer todo tipo de preguntas para tener información suficiente para poder realizar un correcto desarrollo del mismo.

BIBLIOGRAFÍA

[1] León García Widjaja, Redes de comunicación, España: Mcgrawhill/Interamericano, 2002

[2] Olifer Natalie; & Olifer Víctor , Redes de computadores, España: Mcgrawhill/Interamericano, 2002

[3] Barba Martí Antoni , Gestión de la red, España: Edicions UPC, 1999

[4] Kurose James F. & Ross Keith W., Redes de computadores, España: Pearson Educación, 2005

[5] Video vigilancia IP. Sistema de seguridad http://es.kioskea.net/faq/3415-video-vigilancia-por-IP , fecha de consulta abril 2013

[6] Cámaras de Seguridad (2011.). http://www.voxdata.com.ar/camaras-seguridad.html , fecha de consulta abril del 2013

[7] Postel, Jon, Protocolo de control de transmisión de protocolo de internet, 1981.

[8] Llaramendi, Sistemas de vigilancia IP (2014), Ilaramendi Julio http://camarasde-segurity.blogspot.com/_2014_07_ _01_archive.html , fecha de consulta febrero 2014.

[9] Postel, Protocolos de Seguridad. http://es.kioskea.net/contents/263-protocolo-ftp-protocolo-de-transferencia-de-archivos , fecha de consulta enero 2015

[10] Mit, Red Hat Enterprise Linux 4 (2005). http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-ftp-servers.html, fecha de consulta marzo 2014.

[11] IP camera Easyn, Guía de configuración, http://www.easyn.com/DownLoad.aspx , fecha de consulta junio 2014.

[12] Lacie, Soluciones en almacenamiento de disco duro, http://classic.www.axis.com/es/products/video/about_networkvideo/storage_considerations.htm , fecha de consulta octubre del 2014.

[13] León, Envío de un correo electrónico mediante SMTP y recepción de correo electrónico mediante POP3,http://fundamentos-redes.wikispaces.com/file/view/3.3.3Clientedecorreo_electronico.jpg/255322784/3.3.3_Cliente_de_correo_electronico.jpg, fecha de consulta enero 2014.

[14] Marín, Modelo OSI, http://www.info-ab.uclm.es/labelec/solar/Comunicacion/Redes/images/Modelos/OSI.gif , fecha de consulta diciembre del 2013

[15] León, Correspondencia del modelo OSI. http://www.monografias.com/trabajos30/ redes-de-datos/Image131.gif, fecha de consulta junio 2014

[16] Morales, Sistema de la Cámara. http://www.tecnoseguro.com/images/stories/Tutoriales/650x247xCamara_IP_Diagrama_Flujo.jpg.pagespeed.ic.wuGbRaxvBa.jpg , fecha de consulta septiembre del 2014