ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE RED COMBINADA DE VIDEO VIGILANCIA UTILIZANDO TECNOLOGÍA BPL, ETHERNET PARA EL LABORATORIO LTI.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANÁLISIS DE SISTEMAS INFORMÁTICOS

LEONARDO XAVIER MEDRANO CHIMBORAZO
lexmedrano18@hotmail.com

SONIA ELIZABETH RAMOS CÁRDENAS
e2_eli@hotmail.com

DIRECTOR: ING. CÉSAR GALLARDO
cesar.gallardo@epn.edu.ec

Quito, Mayo 2011

DECLARACIÓN

Nosotros Leonardo Xavier Medrano Chimborazo y Sonia Elizabeth Ramos Cárdenas, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Leonardo Xavier	**Sonia Elizabeth**
Medrano Chimborazo	**Ramos Cárdenas**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Leonardo Xavier Medrano Chimborazo y Sonia Elizabeth Ramos Cárdenas, bajo mi supervisión.

Ing. Cesar Gallardo
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco a Dios principalmente por enseñarme cada día, su amor, su fortaleza y bondad.

A mis padres por confiar y estar conmigo en los buenos y malos momentos. Por brindarme su amor y apoyo. Por enseñarme cada día una gran lección “el esfuerzo y dedicación te lleva al éxito y cumplir tus sueños”.

De manera muy especial a mi linda damita que comparte mi vida y sueños, que sin su amor y apoyo incondicional no hubiera podido lograr este tan anhelado sueño.

A mis queridos amigos que con su amistad y cariño me han demostrado cuan valioso son. Gracias por estar allí cuando más los necesitaba, por las alegrías y enseñanzas de la vida.

A todas las personas que me ayudaron de una u otra forma a culminar este proyecto.

DEDICATORIA

Este proyecto te dedico mi Señor, por haberme brindado la oportunidad de ingresar a esta prestigiosa universidad, el cual tanto soñé estar. Eres tu quien me ha dado todo lo mejor y has estado junto a mí en todo momento.

A mi madre por su amor, su ternura y gran corazón me ha enseñado a ser un hombre de bien, respetuoso y responsable.

A mi padre por su cariño y apoyo. Que me ha enseñado a luchar por lo que uno quiere, sin dañar a los demás.
A mi hermana que con sus consejos y cariño me enseño a nunca rendirme ni en las más terribles situaciones de la vida.

A Andreita la damita que se gano mi corazón, con quien comparto esta felicidad tan grande e indescriptible. Gracias mi corazón por brindarme tu amor, ternura y apoyo, sin ti no lo hubiera logrado. Te amo preciosa.

A Elizabeth mi gran amiga y compinche de tesis, te doy gracias por haber emprendido este proyecto conmigo y culminado con éxito.

A mis mejores amigos Mario, Franco y Oscar que con sus ocurrencias y gran amistad siempre puedo contar.

AGRADECIMIENTO

Especialmente a Dios por todo su amor, bendiciones y oportunidades que me ha brindado, como el haberme permitido ingresar a esta gran Universidad otorgándome así el desafío de terminar mi carrera.

A mis padres por su confianza, esfuerzo, amor y apoyo gracias a ellos soy un profesional y un gran ser humano.

Mami gracias por ser a mejor del mundo, por ser mi amiga y por darme la confianza con tus palabras de aliento en todo momento.
Papi muchas gracias por tu amor, tu apoyo y tus consejos eres una parte fundamental en mi vida.

E^2 gracias por haber estado siempre a mi lado dándome ese apoyo para seguir este largo y duro camino y por haber tenido siempre la confianza en mí.

A mi compañero de tesis un gran amigo y confidente, gracias Leito por haber luchado junto a mí en este proyecto para la satisfactoria culminación del mismo.

A mis amigos de la poli, gracias chicos por el apoyo con ustedes hemos sido cómplices de los buenos y malos momentos que hemos pasado en esta etapa gracias por haber estado siempre ahí brindándome una amistad sin condiciones.

Un agradecimiento especial al Ing. César Gallardo quien con paciencia, amistad y sabiduría nos guio para la culminación de este proyecto y en la aulas nos impartió todo su conocimiento en este camino de formación y triunfo.

Elizabeth Ramos Cárdenas

DEDICATORIA

Este trabajo quiero dedicarlo a Dios por darme la vida, salud, bendiciones y una oportunidad, como esta, por haberme dado los mejores padres del mundo y haberme guía dándome la fuerza necesaria para seguir adelante.

A mis padres Ángel y Marlene por ser grandiosos, por haberme inculcado valores y principios, por haberme sabido dar su apoyo, cariño, fe y ánimo haciendo posible este triunfo, a ellos dedico este esfuerzo para terminar esta etapa universitaria.

A mis tíos, primos, tías y abuelita quienes estuvieron aunque indirectamente siempre junto a mí para darme ese impulso a continuar y poder llegar a la satisfactoria culminación de esta etapa.

A la personita que durante toda esta etapa en la poli ha sido mi apoyo, fuerza y empuje para no dejarme abatir por los problemas y obstáculos, por haber sido tan incondicional conmigo y darme su cariño, tú formas una parte fundamental en la culminación de esta etapa… E^2.

"Para empezar un gran proyecto se necesita valentía, para terminar un gran proyecto hace falta perseverancia."

Elizabeth

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN EJECUTIVO

Este documento está dividido en seis capítulos. El primer capítulo hace hincapié en el la definición del problema y la solución planteada al mismo, adicionalmente se presentara los objetivos a alcanzar para satisfacer las necesidades de los usuarios.

El segundo capítulo relacionado con el marco teórico, se realiza un análisis de los aspectos que implica el desarrollo posterior del diseño e implementación de la red. La red y los tipos de redes permitirán la comunicación a distancia entre equipos autónomos. El servidor proxy permitirá el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, es decir, una única dirección IP. El internet dará la facilidad de compartir recursos. Es decir: mediante el ordenador, establecer una comunicación inmediata con cualquier parte del mundo. El host funcionara como el punto de inicio y final de las transferencias de datos. La cámara IP emitirá las imágenes directamente a la red (Intranet o internet) a través del servidor de video. Los adaptadores PLC unirá los dos elementos Ethernet (modem-router – PC, o modem-router – decodificador) a partir del cableado eléctrico existente, evitando tener que tender un nuevo cableado. La tecnología BPL de banda ancha que utiliza las líneas eléctricas de media y baja tensión proveerá servicios de comunicación, transferencia de datos, etc. sobre IP (Protocolo Internet) a través de la red eléctrica, llegando a los usuarios por medio de la instalación eléctrica existente en los hogares, comercios e industria. La seguridad global proveerá de normas y pautas a seguir para que el prototipo implementado esté libre de peligro, daño o riesgo. La video vigilancia servirá para monitorear el lugar que sea implementado (una casa o negocio a distancia) sin necesidad de tener un ordenador instalado en el lugar vigilado, sólo con disponer una conexión a Internet y una toma de corriente eléctrica.

El tercer capítulo corresponderá al diseño de una red Física. En la red física se realizara el diseño y la arquitectura de red usando los equipos mencionados según lo establecido en el capítulo dos.

El cuarto capítulo corresponde a la Implementación y Prueba del Prototipo. En el cual se instala dichos equipos así como también se demuestra el funcionamiento de la red mediante las respectivas pruebas del prototipo.

En el último capítulo se desarrolla las conclusiones y recomendaciones derivadas del desarrollo e implementación del proyecto y de los objetivos aquí planteados.

CAPÍTULO I. 1. INTRODUCCIÓN

1.1 ANTECEDENTES

Este proyecto consiste en el diseño e implementación de un prototipo de red combinada que brinde los servicios de video vigilancia utilizando tecnología BPL (Broadband over PowerLine), Ethernet para el Laboratorio LTI (Laboratorio de Tecnologías de la Información), el mismo que esta a servicio de los alumnos de la carrera de Análisis de Sistemas Informáticos brindando tres salas con más de 50 computadores y equipadas con lo necesario para el aprendizaje de sus estudiantes.

El diseño se realizara a partir de la definición del problema. Con el propósito de que el usuario posea una guía para la implementación del prototipo de red de video vigilancia haciendo de este un prototipo de red útil en cualquier ámbito en que sea requerido tomando en cuenta ciertos parámetros de seguridad.

1.2 ÁMBITO

El Laboratorio de Tecnologías de la Información del DICC de la Escuela Politécnica Nacional da soporte académico a la carrera de Análisis de Sistemas Informáticos de la ESFOT está administrado por un Jefe de Laboratorio, dos Ayudantes y dos Auxiliares de Laboratorio.

1.3 DEFINICIÓN DEL PROBLEMA

El laboratorio LTI – ASI, que es parte de este proyecto, no posee equipamiento tecnológico de video vigilancia y BPL alguno, así como también no existen guías que puedan aportar al uso adecuado de dichos equipos por parte de los estudiantes de la carrera ASI.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Aportar con documentación y guías para que los estudiantes de la carrera ASI apliquen la nueva tecnología BPL, mediante el diseño e implementación de un prototipo de red de video vigilancia, usando tecnologías combinadas como Ethernet, BPL y cámaras IP.

1.4.2 OBJETIVOS ESPECÍFICOS

- Generar documentación de ayuda para los estudiantes de la carrera de Análisis de Sistemas Informáticos sobre la aplicación de la tecnología BPL y video vigilancia con cámaras IP.
- Generar guías prácticas para el uso debido de la tecnología BPL y video vigilancia con cámaras IP.
- Diseñar e implementar un prototipo de red combinada de video vigilancia utilizando tecnología BPL, ETHERNET.

1.5 JUSTIFICACIÓN

Este proyecto está orientado principalmente a proveer guías de aplicación y uso de esta nueva tecnología BPL - Ethernet, para el diseño e implementación de un prototipo de red de video vigilancia que pueda ser implementado en cualquier lugar.

El prototipo propuesto permitirá mejorar los siguientes aspectos:

- Ver las ventajas y desventajas que implica implementar la tecnología BPL.
- Establecer mejoras u optimación de las redes de video vigilancia a través de la tecnología BPL.
- Diseñar e implementar una red de video vigilancia con un presupuesto considerable.
- Formular estrategias y acciones de seguridad preventivas a tomar en lo educacional e institucional en contra de los infractores.
- Aportar conocimiento en el campo de seguridad mediante prácticas de los estudiantes en base al diseño e implementación de este prototipo.

El esquema general de la implementación del prototipo de red de video vigilancia se detalla en el capítulo tres.

CAPÍTULO II. 2. MARCO TEÓRICO

2.1 REDES DE COMPUTADORAS[1]

2.1.1 RED DE COMPUTADORAS

Es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información, recursos y servicios.

2.1.2 CLASIFICACIÓN DE LAS REDES

2.1.2.1 Por su tecnología de transmisión (difusión)

2.1.2.1.1 Redes de Broadcast

Las redes de Broadcast tienen un solo canal de comunicación, el medio de transmisión es compartido y los paquetes se envían a toda la red aunque vaya dirigido a un solo destinatario, cada máquina ignora el paquete si no está dirigida a ella, caso contrario lo procesa. Si envía a un subconjunto de máquinas (Multicast), a todas las máquinas (Broadcast).

2.1.2.1.2 Redes Punto a Punto

Las redes punto a punto consisten en muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más máquinas intermedias.
Como regla general, las redes pequeñas geográficamente localizadas tienden a usar la difusión, mientras que las redes más grandes suelen ser punto a punto.

1 http://es.wikipedia.org/wiki/Red_de_computadoras

2.1.2.2 Por su tamaño

Las redes de ordenadores se pueden clasificar según la escala o el grado del alcance de la red.

2.1.2.2.1 Red de Área Personal (PAN)

Personal Área Network es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora cerca de una persona. El alcance de una PAN es típicamente algunos metros. Las PAN se pueden utilizar para la comunicación entre los dispositivos personales de ellos mismos (comunicación del intrapersonal), o para conectar con una red de alto nivel y el Internet (un up link).

2.1.2.2.2 Red de Área Local (LAN)

Una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de la localización.

2.1.2.2.3 Red de Área de Campus (CAN)[2]

Se deriva a una red que conecta dos o más LAN's los cuales deben estar conectados en un área geográfica específica tal como un campus de universidad, un complejo industrial o una base militar.

2.1.2.2.4 Red de Área metropolitana (MAN)

Es una red que conecta las redes de un área dos o más locales juntos pero no extiende más allá de los límites de la ciudad inmediata, o del área metropolitana. Las rebajadoras múltiples, los interruptores y los cubos están conectados para crear a una MAN

2.1.2.2.5 Red Metro Ethernet [3]

2 Tesis Conza Andrea, Diseño e iimplementación de un prototipo de DMZ y la interconexión segura mediante VPN utilizando el firewall Fortigate 60. Septiembre 2009.

3 http://es.wikipedia.org/wiki/Metro_Ethernet

Es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, a través de UNIs Ethernet. Estas redes denominadas "multiservicio", soportan una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye soporte a tráfico "RTP" (tiempo real), como puede ser Telefonía IP y Video IP, este tipo de tráfico resulta especialmente sensible a retardo y al jitter.

2.1.2.2.6 Red Next Generation Networking (NGN)[4]

Red de Siguiente Generación (Next Generation Networking o NGN en inglés) es un amplio término que se refiere a la evolución de la actual infraestructura de redes de telecomunicación y acceso telefónico con el objetivo de lograr la congruencia de los nuevos servicios multimedia (voz, datos, video...) en los próximos años. La idea principal que se esconde debajo de este tipo de redes es el transporte de paquetes encapsulados de información a través de Internet. Estas nuevas redes serán construidas a partir del protocolo Internet Protocol (IP), siendo el término "all-IP" comúnmente utilizado para describir dicha evolución.

2.1.2.2.7 Red de Área amplia (WAN)

Es una red de comunicaciones de datos que cubre un área geográfica relativamente amplia y que utiliza a menudo las instalaciones de transmisión proporcionadas por los portadores comunes, tales como compañías del teléfono. Las tecnologías WAN funcionan generalmente en las tres capas más bajas del Modelo de referencia OSI: la capa física, la capa de transmisión de datos, y la capa de red.

2.1.2.3 Por método de conexión

Las redes de ordenadores se pueden clasificar según la tecnología que se utiliza para conectar los dispositivos individuales en la red

2.1.2.3.1 Medios guiados [5]

4http://es.wikipedia.org/wiki/Red_de_siguiente_generaci%C3%B3n

5 http://www.monografias.com/trabajos17/medios-de-transmision/medios-de-transmision.shtml

Se conoce como medios guiados a aquellos que utilizan unos componentes físicos y sólidos para la transmisión de datos. También conocidos como medios de transmisión por cable

- Cable coaxial
- Cable par trenzado
- Cable de fibra óptica

2.1.2.3.2 Medios no guiados

Los medios no guiados o sin cable han tenido gran acogida al ser un buen medio de cubrir grandes distancias y hacia cualquier dirección, su mayor logro se dio desde la conquista espacial a través de los satélites y su tecnología no para de cambiar. La transmisión y recepción se realiza por medio de antenas, las cuales deben estar alineadas cuando la transmisión es direccional, o si es omnidireccional la señal se propaga en todas las direcciones. Entre estas tenemos:

- Señales de radio
- Señales de microondas
- Señales de rayo infrarrojo
- Señales de rayo láser

2.1.2.4 Por relación funcional[6]

Las redes de computadoras pueden clasificarse de acuerdo a la relación funcional que existe entre los elementos de una red, Por ejemplo: Redes activas, Cliente/Servidor y Peer to peer

2.1.2.4.1 Redes activas

Este tipo de redes incluyen la transmisión de datos, pero también de programas que pueden ser ejecutados en los diferentes puntos de la red, su propósito es hacer que la red funcione mejor de acuerdo a los requerimientos de la aplicación que la está utilizando.

2.1.2.4.2 Cliente/Servidor

6http://www.mitecnologico.com/Main/DeAcuerdoASuRelacion

Este es un tipo de arquitectura donde pueden existir uno o más servidores con uno o más clientes conectados a ellos, cada cliente y servidor se le llama nodo. Los nodos pueden enviar solicitudes de datos a uno o más de los servidores.
Esta arquitectura es de las más populares ya que se puede aplicar a diferentes tipos de aplicaciones, manteniendo el mismo concepto. Aplicaciones como la navegación web, consultas a bases de datos, manejo de correos electrónicos e inclusive juegos en línea utilizan esta arquitectura para funcionar.
Esta arquitectura es muy versátil, ya que se basa en el envío de mensajes y en la modularidad, destacándose por su uso, flexibilidad, interoperabilidad y escalabilidad.

2.1.2.4.3 Peer to peer

Ese tipo de redes conecta una gran cantidad de nodos de forma “ad hoc”, no hace distinción de nodos tipo servidor o cliente, cada nodo funciona como cliente servidor. Todos los participantes en la red se suman al ancho de banda acumulativo de la red, en lugar de mantener recursos centralizados.
Su uso principal es compartir archivos que contienen video, audio, datos, todo lo que se necesite transmitir en tiempo real, como el tráfico telefónico, por ejemplo.
Las redes peer to peer son más confiables y redundantes en el caso de fallas en alguno de los nodos; además de que ayudan a compartir los recursos de manera compensada entre los participantes y realizan una comunicación multi-punto de una forma eficiente sin depender de la infraestructura multicast de IP

2.1.2.5 Por topología de red

Define cómo están conectadas computadoras, impresoras, dispositivos de red y otros dispositivos. Una topología de red describe la disposición de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos. La topología influye enormemente en el funcionamiento de la red.

2.1.2.5.1 Topología Física

Consiste en la configuración o disposición del cableado y equipos de comunicación. Define cómo están conectadas computadoras, impresoras, dispositivos de red y otros dispositivos. Una topología de red describe la

disposición de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos. La topología influye enormemente en el funcionamiento de la red.

2.1.2.5.2 Red de bus[7]

En esta topología, los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; (el bus). Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzado a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cuál es la que le corresponde, la destinada a él.

Es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red. Por otra parte, una ruptura del bus es difícil de localizar (dependiendo de la longitud del cable y el número de terminales conectados a él) y provoca la inutilidad de todo el sistema.

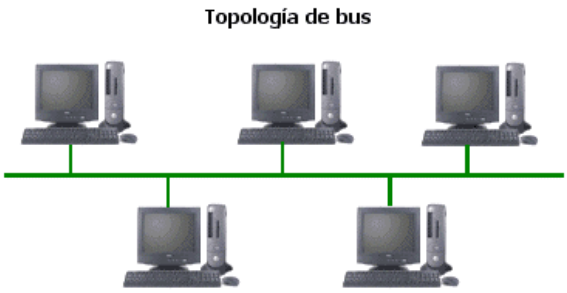


Figura 2.1.- Topología de Bus [8]

2.1.2.5.3 Red de estrella

En la topología en estrella, cada estación tiene una conexión directa a un acoplador (conmutador) central. Una manera de construir esta topología es con conmutadores telefónicos que usan la técnica de conmutación de circuitos.

Otra forma de esta topología es una estación que tiene dos conexiones directas al acoplador de la estrella (nodo central), una de entrada y otra de salida (la cual lógicamente opera como un bus). Cuando una transmisión llega al nodo central, este la retransmite por todas las líneas de salida.

7http://www.geocities.com/timessquare/chasm/7990/topologi.htm

8http://members.fortunecity.es/infokmas/index/memorias/memorias_archivos/image004.gif

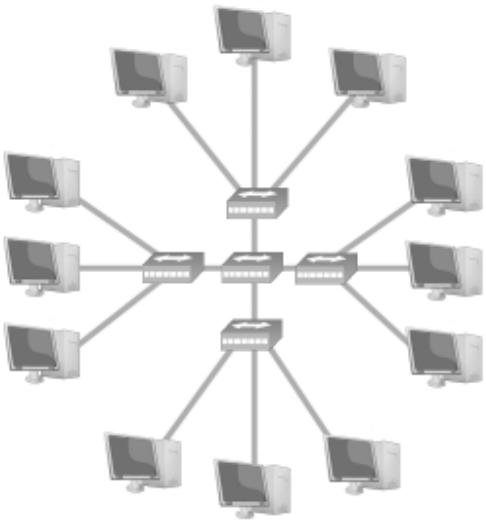
Según su función, los acopladores se catalogan en:

- Acoplador pasivo: cualquier transmisión en una línea de entrada al acoplador es físicamente trasladada a todas las líneas de salida.
- Acoplador activo: existe una lógica digital en el acoplador que lo hace actuar como repetidor. Si llegan bits en cualquier línea de entrada, son automáticamente regenerados y repetidos en todas las líneas de salida. Si llegan simultáneamente varias señales de entrada, una señal de colisión es transmitida en todas las líneas de salida.

Figura 2.2.- Topología en estrella [9]

2.1.2.5.4 Red estrella extendida

Enlaza las estrellas conectadas a los switches de estas en un switch central.



9http://internett.galeon.com/REDES_archivos/image003.gif

Figura 2.3.- Topología en estrella extendida

2.1.2.5.5 Red de anillo (o doble anillo)

En esta topología la red consiste en un conjunto de repetidores unidos por líneas de comunicación punto a punto, que forman un ciclo cerrado.

Cada repetidor participa en dos enlaces, recibe datos de uno y los transmite al otro; su capacidad de almacenamiento, si tiene, es de sólo unos cuantos bits y la velocidad de recepción y de transmisión es igual en todos los repetidores.

Los enlaces (líneas de comunicación) son simplex, por lo tanto la información fluye en un solo sentido en el anillo. Las estaciones se conectan a la red por medio de los repetidores.

Una red con topología de anillo se organiza conectando nodos de la red en un ciclo cerrado con cada nodo enlazado a los nodos contiguos a la derecha y a la izquierda. La ventaja de esta red es que se puede operar a grandes velocidades, y los mecanismos para evitar colisiones son sencillos.

Algunas veces, estas redes utilizan esquemas de transmisión de señales para determinar qué nodo puede tener acceso al sistema de comunicaciones.

Figura 2.4.- Topología en anillo [10]

2.1.2.5.6 Red en malla (o totalmente conexa)

10http://internett.galeon.com/REDES_archivos/image002.gif

En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta.
Por tanto, una red en malla completamente conectada necesita n(n-1)/2 canales físicos para enlazar n dispositivos. Para acomodar tantos enlaces, cada dispositivo de la red debe tener sus puertos de entrada/salida (E/S).

Figura 2.5.- Topología en malla[11]

2.1.2.5.7 Red en árbol

La topología en árbol es una generalización de la topología en bus. Esta topología comienza en un punto denominado cabezal o raíz (head end). Uno ó más cables pueden salir de este punto y cada uno de ellos puede tener ramificaciones en cualquier otro punto. Una ramificación puede volver a ramificarse. En una topología en árbol no se deben formar ciclos.
Una red como ésta representa una red completamente distribuida en la que computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras. Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamientos independientes y recurren a los recursos en niveles superiores o inferiores conforme se requiera.

11http://www.pc-doctor.com.mx/radio%20formula/temas/Redes_archivos/image012.jpg

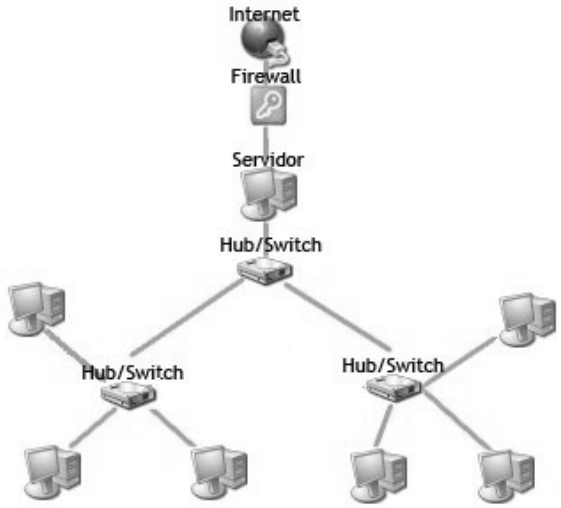


Figura 2.6.- Topología en árbol [12]

2.1.2.5.8 Topología Lógica

Se define cómo los datos fluyen a través de la red.

2.1.2.5.9 Topología Ethernet

Cada host envía sus datos a todos los otros host conectados al medio físico en la red. No hay un orden de trasmisión de datos, el primero en acceder al medio es el primero en transmitir.

2.1.2.5.10 Topología Token Ring

Aquí se controla el acceso al medio utilizando un testigo electrónico que se pasa a cada host. Cuando un host recibe el testigo puede transmitir datos si los tiene. Si no, entonces pasa el testigo al siguiente host.

2.1.2.6 Por el tipo de transmisión

Por el tipo de direccionamiento de datos podemos clasificar las redes de la siguiente forma:

12http://internett.galeon.com/REDES_archivos/image004.gif

2.1.2.6.1 Simplex (unidireccionales)[13]

La transmisión simplex (sx) o unidireccional es aquella que ocurre en una dirección solamente, deshabilitando al receptor de responder al transmisor. Normalmente la transmisión simplex no se utiliza donde se requiere interacción humano-máquina. Ejemplos de transmisión simplex son: La radiodifusión (broadcast) de TV y radio.

2.1.2.6.2 Half-Duplex (bidireccionales)

La transmisión half-duplex (hdx) permite transmitir en ambas direcciones; sin embargo, la transmisión puede ocurrir solamente en una dirección a la vez. Tanto transmisor y receptor comparten una sola frecuencia. Un ejemplo típico de half-duplex es el radio de banda civil (CB) donde el operador puede transmitir o recibir, pero no puede realizar ambas funciones simultáneamente por el mismo canal. Cuando el operador ha completado la transmisión, la otra parte debe ser avisada que puede empezar a transmitir (diciendo “cambio”).

2.1.2.6.3 Full-Duplex (bidireccionales)

La transmisión full-duplex (fdx) permite transmitir en ambas direcciones, pero simultáneamente por el mismo canal. Existen dos frecuencias una para transmitir y otra para recibir. Ejemplos de este tipo abundan en el terreno de las telecomunicaciones, el caso más típico es la telefonía, donde el transmisor y el receptor se comunican simultáneamente utilizando el mismo canal, pero usando dos frecuencias.

2.2 MODELO OSI

2.2.1 INTRODUCCIÓN [14]

En 1977, la Organización Internacional de Estándares (ISO), integrada por industrias representativas del medio, creó un subcomité para desarrollar estándares de comunicación de datos que promovieran la accesibilidad universal y una interoperabilidad entre productos de diferentes fabricantes.

13 http://www.mitecnologico.com/Main/ModosDeTransmisionSimplexHalfDuplexYFullDuplex

14 http://sistemas.itlp.edu.mx/tutoriales/redes/index.htm

El resultado de estos esfuerzos es el Modelo de Referencia Interconexión de Sistemas Abiertos (OSI).

OSI nace de la necesidad de uniformizar los elementos que participan en la solución del problema de comunicación entre equipos de cómputo de diferentes fabricantes.

2.2.2 CONCEPTO DE MODELO OSI[15]

El Modelo OSI es un lineamiento funcional para tareas de comunicaciones y, por consiguiente, no especifica un estándar de comunicación para dichas tareas. Sin embargo, muchos estándares y protocolos cumplen con los lineamientos del Modelo OSI. Así, todo dispositivo de cómputo y telecomunicaciones podrá ser referenciado al modelo y por ende concebido como parte de un sistema interdependiente con características muy precisas en cada nivel.

2.2.3 CAPAS DEL MODELO OSI

Figura 2.7.- Modelo OSI [16]

2.2.3.1 Capa de Aplicación

Es el nivel más cercano al usuario y a diferencia de los demás niveles, por ser el más alto o el último, no proporciona un servicio a ningún otro nivel.

15http://elsitiodetelecomunicaciones.iespana.es/modelo_osi.htm

16http://tbn0.google.com/images?q=tbn:3mTrlL9Q4O5rTM:http://bp0.blogger.com/_GD_DcKMfSls/RdqNw9VVjlI/AAAAAAAAADM/EV5HsVQYyVg/s400/modelo%2Bosi.JPG

En OSI el nivel de aplicación se refiere a las aplicaciones de red que se utilizan para transportar las aplicaciones del usuario.
FTP (File Transfer Protocol), Mail, Telnet, son entre otras las aplicaciones incluidas en el nivel 7 del modelo OSI y sólo cobran vida al momento de requerir una comunicación entre dos entidades.

2.2.3.2 Capa de Presentación

Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformateo de datos de la aplicación del usuario. La información es procesada en forma binaria y en este nivel se llevan a cabo las adaptaciones necesarias para que pueda ser presentada de una manera más accesible. Códigos como ASCII (American Standard Code for Information Interchange) y EBCDIC (Extended Binary Coded Decimal Interchange Code), que permiten interpretar los datos binarios en caracteres que pueden ser fácilmente manejados, tienen su posicionamiento en el nivel de presentación del modelo OSI.
El nivel de Presentación negocia la sintaxis de la transferencia de datos hacia el nivel de aplicación.

2.2.3.3 Capa de Sesión

Este nivel es el encargado de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. Establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas.

2.2.3.4 Capa de Transporte

En este nivel se realiza y se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (del nivel 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.
El nivel de transporte notifica a las capas superiores si se está logrando la calidad requerida. Este nivel utiliza reconocimientos, números de secuencia y control de flujo.

Los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) son característicos del nivel del transporte del modelo OSI, al igual que IPX/SPX (del inglés Internetwork Packet Exchange/Sequenced Packet Exchange), Protocolo Novell o simplemente IPX es una familia de protocolos de red desarrollados por Novell y utilizados por su sistema operativo de red NetWare.

2.2.3.4.1 IPX

El protocolo Intercambio de Paquetes Entre Redes (IPX) es la implementación del protocolo IDP (Internet Datagram Protocol) de Xerox. Es un protocolo de datagramas rápido orientado a comunicaciones sin conexión que se encarga de transmitir datos a través de la red, incluyendo en cada paquete la dirección de destino.

Pertenece a la capa de red (nivel 3 del modelo OSI) y al ser un protocolo de datagramas es similar (aunque más simple y con menor fiabilidad) al protocolo IP del TCP/IP en sus operaciones básicas pero diferente en cuanto al sistema de direccionamiento, formato de los paquetes y el ámbito general. Fue creado por el Ing. Alexis G.Soulle.

2.2.3.4.2 SPX

El protocolo Intercambio de Paquetes en Secuencia (SPX) es la implementación del protocolo SPP (Sequenced Packet Protocol) de Xerox. Es un protocolo fiable basado en comunicaciones con conexión y se encarga de controlar la integridad de los paquetes y confirmar los paquetes recibidos a través de una red.

Actúa sobre IPX para asegurar la entrega de los paquetes (datos), ya que IPX por sí solo no es capaz. Es similar a TCP ya que realiza las mismas funciones. Se utiliza principalmente para aplicaciones cliente/servidor.

Hay dos tipos de servicio dentro de la capa de Transporte:

- Servicios Orientados: Sólo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión. Cuando llega un paquete que no es el primero se identifica a que conexión pertenece y se envía por el enlace de salida adecuado, según la

información que se generó con el primer paquete y que permanece almacenada en cada conmutador o nodo.

Lista de protocolos orientados a la conexión

- ✓ TCP
- ✓ Frame Relay
- ✓ ATM

- Servicios no orientados: Cada paquete debe llevar la dirección destino, y con cada uno, los nodos de la red deciden el camino que se debe seguir. Existen muchas técnicas para realizar esta decisión, como por ejemplo comparar el retardo que sufriría en ese momento el paquete que se pretende transmitir según el enlace que se escoja.

  Lista de protocolos no orientados a la conexión

  - ✓ Protocolo IP
  - ✓ Protocolo UDP
  - ✓ ICMP
  - ✓ IPX
  - ✓ TIPC

2.2.3.5 Capa de Red [17]

La capa de red, según la normalización OSI, es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones.

Para la consecución de su tarea, puede asignar direcciones de red únicas, interconectar subredes distintas, encaminar paquetes y utilizar un control de congestión.

17http://es.wikipedia.org/wiki/Capa_de_red

2.2.3.6 Capa de Enlace de datos

Conocido también como nivel de Trama (Frame) o Marco, es el encargado de preparar la información codificada en forma binaria en formatos previamente definidos por el protocolo a utilizar.

Tiene su aplicación en el contexto de redes WAN y LAN ya que como se estableció previamente la transmisión de datos no es más que el envió en forma ordenada de bits de información. Este nivel ensambla los datos en tramas y las transmite a través del medio (LAN o WAN). Es el encargado de ofrecer un control de flujo entre tramas, así como un sencillo mecanismo para detectar errores. Es en este nivel y mediante algoritmos como CRC (Cyclic Redundancy Check), donde se podrá validar la integridad física de la trama; mas no será corregida a este nivel sino que se le notificará al transmisor para su retransmisión.

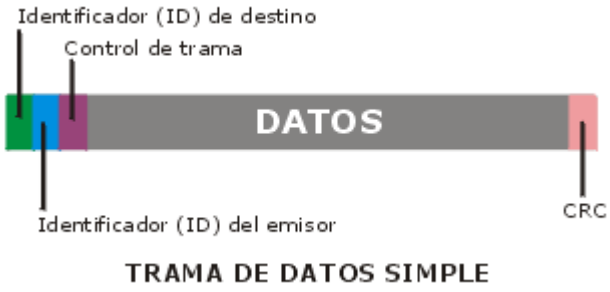


Figura 2.8.- Capa de Enlace de datos[18]

2.2.3.7 Capa Física

Es el primer nivel del modelo OSI y en él se definen y reglamentan todas las características físicas-mecánicas y eléctricas que debe cumplir el sistema para poder operar. Como es el nivel más bajo, es el que se va a encargar de las comunicaciones físicas entre dispositivos y de cuidar su correcta operación. La información computarizada es procesada y transmitida en forma digital siendo esta de bits: 1 y 0, por lo que, toda aplicación que se desee enviar, será transmitida en forma serial mediante la representación de unos y ceros.

En este nivel se ubican también todos los medios de transmisión como los sistemas de telecomunicaciones para el mundo WAN (Wide Área Network), tales como sistemas satelitales, microondas, radio enlaces, canales digitales y líneas

18http://fmc.axarnet.es/images/redes/paquete_simple.gif

privadas, así como los medios de transmisión para redes de área locales (LAN: Local Área Network), cables de cobre (UTP,STP) y fibra óptica. Además, en este nivel se ubican todos aquellos dispositivos pasivos y activos que permiten la conexión de los medios de comunicación como repetidores de redes LAN, repetidores de microondas y fibra óptica, concentradores de cableado (HUBs), conmutadores de circuitos físicos de telefonía o datos, equipos de modulación y demodulación (módems) y hasta los aparatos receptores telefónicos convencionales o de células que operan a nivel hardware como sistemas terminales.

2.3 MODELO TCP/IP

2.3.1 INTRODUCCIÓN [19]

Internet se desarrolló para brindar una red de comunicación que pudiera continuar funcionando en tiempos de guerra. Aunque la Internet ha evolucionado en formas muy diferentes a las imaginadas por sus arquitectos, todavía se basa en un conjunto de protocolos TCP/IP. El diseño de TCP/IP es ideal para la poderosa y descentralizada red que es Internet.

Todo dispositivo conectado a Internet que desee comunicarse con otros dispositivos en línea debe tener un identificador exclusivo. El identificador se denomina dirección IP. Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.

El TCP/IP es la base de Internet, y sirve para comunicar todo tipo de dispositivos, computadoras que utilizan diferentes sistemas operativos, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

19 http://www.alfinal.com/Temas/tcpip.shtml

2.3.2 CONCEPTO MODELO TCP /IP [20]

TCP/IP es junto con OSI una arquitectura de protocolos que ha sido determinante y básica en el desarrollo de los estándares de comunicación. Es la arquitectura más adoptada para la interconexión de sistemas. Al contrario de lo que ocurre con OSI, el modelo TCP/IP es software, es decir, es un modelo para ser implementado en cualquier tipo de red. Facilita el intercambio de información independientemente de la tecnología y el tipo de subredes a atravesar, proporcionando una comunicación transparente a través de sistemas heterogéneos.

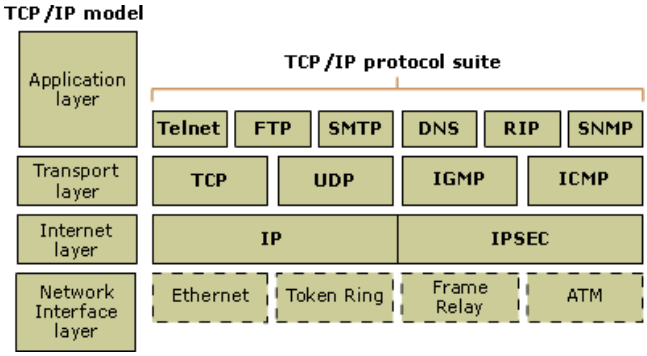


Figura 2.9.- Modelo TCP/IP [21]

Este modelo está compuesto por cuatro capas o niveles que a continuación se indican:

2.3.2.1 Capa de Aplicación [22]

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

20http://ceres.ugr.es/~alumnos/redrs232/tcpip.htm

21 http://i.technet.microsoft.com/cc786900.4aade787-d5e9-45b4-b779-7475d9b77d98(es-es,WS.10).gif

22 http://www.alfinal.com/Temas/tcpip.shtml

2.3.2.2 Capa de Transporte

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

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

2.3.2.3 Capa de Internet

Esta capa tiene como propósito seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el Protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes ocurren en esta capa.

2.3.2.4 Capa de Acceso de Red

También denominada capa de host de red. Esta es la capa que maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red. Esta capa incluye los detalles de la tecnología LAN y WAN y todos los detalles de las capas; física y de enlace de datos del modelo OSI.

Los controladores para las aplicaciones de software, las tarjetas de módem y otros dispositivos operan en la capa de acceso de red. La capa de acceso de red define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión.

Son funciones de esta capa: la asignación de direcciones IP a las direcciones físicas, el encapsulamiento de los paquetes IP en tramas. Basándose en el tipo de

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

2.4 DIRECCIONAMIENTO IP [23]

Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, existen tres clases de dirección que se utilizan para asignar direcciones IP a los equipos. El tamaño y tipo de la red determinará la clase de dirección IP que se aplicara cuando se proporcione direcciones IP a los equipos y otros hosts de nuestra red.

La dirección IP es el único identificador que diferencia un equipo de otro en una red y ayuda a localizar dónde reside ese equipo. Se necesita una dirección IP para cada equipo y componente de red, como un router, que se comunique mediante TCP/IP.

2.4.1 DIRECCIONAMIENTO IPV4

Un Router envía los paquetes desde la red origen a la red destino utilizando el protocolo IP. Los paquetes deben incluir un identificador tanto para la red origen como para la red destino.

Utilizando la dirección IP de una red destino, un Router puede enviar un paquete a la red correcta. Cuando un paquete llega a un Router conectado a la red destino, este utiliza la dirección IP para localizar el computador en particular conectado a la red.

Cada dirección IP consta de dos partes. Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red.

2.4.1.1 Componentes de una dirección IP

Una dirección IP está formada por dos partes:

ID de host y el ID de red.

- ID de red: La primera parte de una dirección IP es el ID de red, que identifica el segmento de red en el que está ubicado el equipo. Todos los equipos del mismo segmento deben tener el mismo ID de red.

23 http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

- ID de host: La segunda parte de una dirección IP es el ID de host, que identifica un equipo, un router u otro dispositivo de un segmento.

El ID de cada host debe ser exclusivo en el ID de red. La combinación del ID de red y el ID de host debe ser exclusivo para todos los equipos que se comuniquen entre sí.

2.4.1.2 Clases de direcciones de Internet IPV4

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande.

2.4.1.2.1 Clase A

Las direcciones de clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer número para el ID de red. Los tres números restantes se utilizan para el ID de host, permitiendo 16.777.214 hosts por red.

La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.

2.4.1.2.2 Clase B

Las direcciones de clase B se asignan a redes de tamaño mediano a grande. Esta clase permite 16.384 redes, utilizando los dos primeros números para el ID de red. Los dos números restantes se utilizan para el ID de host, permitiendo 65.534 hosts por red.

2.4.1.2.3 Clase C

Las direcciones de clase C se utilizan para redes de área local (LANs) pequeñas. Esta clase permite aproximadamente 2.097.152 redes utilizando los tres primeros números para el ID de red. El número restante se utiliza para el ID de host, permitiendo 254 hosts por red.

2.4.1.2.4 Clase D Y E

Las clases D y E no se asignan a hosts. Las direcciones de clase D se utilizan para la multidifusión, y las direcciones de clase E se reservan para uso futuro.

Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

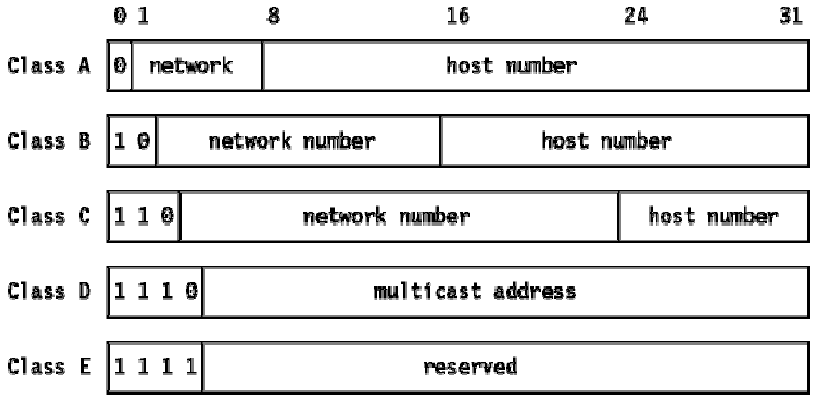


Figura 2.10.- Clases asignadas de direcciones de Internet [24]

2.4.1.3 Cabecera IPV4 [25]

La cabecera IP tiene un tamaño de 160 bits (20 bytes) y está formada por varios campos de distinto significado. Estos campos son:

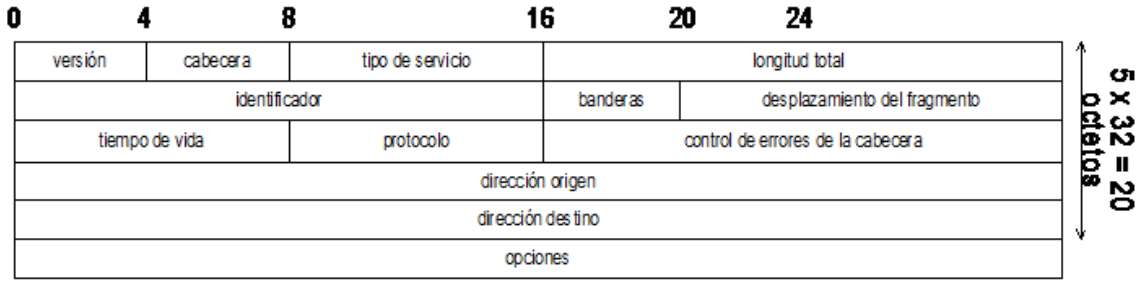


Figura 2.11.- Cabecera IPV4 [26]

Donde:

- Versión: Número de versión del protocolo IP utilizado. Tendrá que tener el valor 4. Tamaño: 4 bit..
- Longitud de la cabecera: (Internet Header Length, IHL) Especifica la longitud de la cabecera expresada en el número de grupos de 32 bit que contiene. Tamaño: 4 bit.

24 http://ditec.um.es/laso/docs/tut-tcpip/3376f2.gif

25 http://www.wikilearning.com/tutorial/tutorial_tcp_ip-ip_internet_protocol_version_4/159-3

26 http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

- Tipo de servicio: o calidad de servicio se utiliza para indicar la prioridad o importancia de los datos que se envían, lo que condicionará la forma en que éstos serán tratados durante la transmisión. Tamaño: 8 bit.
- Longitud total: Es la longitud en bytes del datagrama completo, incluyendo la cabecera y los datos. Como este campo utiliza 16 bit, el tamaño máximo del datagrama no podrá superar los 65.535 bytes, aunque en la práctica este valor será mucho más pequeño. Tamaño: 16 bit.
- Identificación: Valor de identificación que se utiliza para facilitar el ensamblaje de los fragmentos del datagrama. Tamaño: 16 bit.
- Flags: Indicadores utilizados en la fragmentación. Tamaño: 3 bit.
- Fragmentación: Contiene un valor (offset) para poder ensamblar los datagramas que se hayan fragmentado. Está expresado en número de grupos de 8 bytes (64 bit), comenzando con el valor cero para el primer fragmento. Tamaño: 16 bit.
- Tiempo de existencia: Contiene un número que disminuye cada vez que el paquete pasa por un sistema. Si este número llega a cero, el paquete será descartado. Esto es necesario por razones de seguridad para evitar un bucle infinito, ya que aunque es bastante improbable que esto suceda en una red correctamente diseñada, no debe descuidarse esta posibilidad. Tamaño: 8 bit.
- Protocolo: El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Tamaño: 8 bit.
- Suma Comprobación: El campo de comprobación (checksum) es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del campo de comprobación de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el límite de existencia. Tamaño: 16 bit.
- Dirección de origen: Contiene la dirección del host que envía el paquete.

Tamaño: 32 bit.

- Dirección de destino: Esta dirección es la del host que recibirá la información. Los routers o gateways intermedios deben conocerla para dirigir correctamente el paquete. Tamaño: 32 bit.
- Opciones IP: Permite que IP soporte varias opciones, como la seguridad (longitud variable)
- Relleno: se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits

2.4.2 DIRECCIONAMIENTO IPV6 [27]

El cambio más grande de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6, como se describe en la siguiente sección.

El número de direcciones IPv6 posibles es de $2^{128} \approx 3.4 \times 10^{38}$. Este número puede también representarse como 16^{32}, con 32 dígitos hexadecimales, cada uno de los cuales puede tomar 16 valores.

En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

2.4.2.1 Tipos de direcciones en IPV6

2.4.2.1.1 Unicast[28]

Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPV4 actuales.

2.4.2.1.2 Anycast

Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos.) Un paquete enviado a una dirección anycast es entregado en una

27 http://es.wikipedia.org/wiki/IPv6

28 http://bjcu.uca.edu.ni/LibrosIsti/Tutorial_de_IPV6.pdf

(cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing).

2.4.2.1.3 Multicast

Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

2.4.2.2 Representación de las direcciones

La representación de las direcciones tiene la siguiente representación:

- x:x:x:x:x:x:x:x, donde “x” es un valor hexadecimal de 16 bits de la porción correspondiente a la dirección IPV6. No es preciso escribir los ceros a la izquierda de cada campo
- Dado que por el direccionamiento que se ha definido, podrán existir largas cadenas de bits “cero”, se permite la escritura de su abreviación, mediante el uso de “::”, que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo sólo puede aparecer una vez en la dirección IPV6.
- Una forma alternativa y muy conveniente, cuando se encuentra en un entorno mixto IPV4 e IPV6, es x:x:x:x:x:x:d:d:d:d, donde “x” representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y “d” representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPV4).

  A continuación, se incluye un ejemplo de una dirección con un prefijo de 64 bits.

  3FFE:FFFF:0:CD30:0:0:0:0/64.

  El prefijo de este ejemplo es 3FFE:FFFF:0:CD30. La dirección también puede escribirse en formato comprimido, como 3FFE:FFFF:0:CD30::/64.

2.4.2.3 Cabecera IPv6

La cabecera principal de IPv6 tiene, al contrario que la cabecera de IPv4, un tamaño fijo de 40 octetos. Y esta es su estructura:

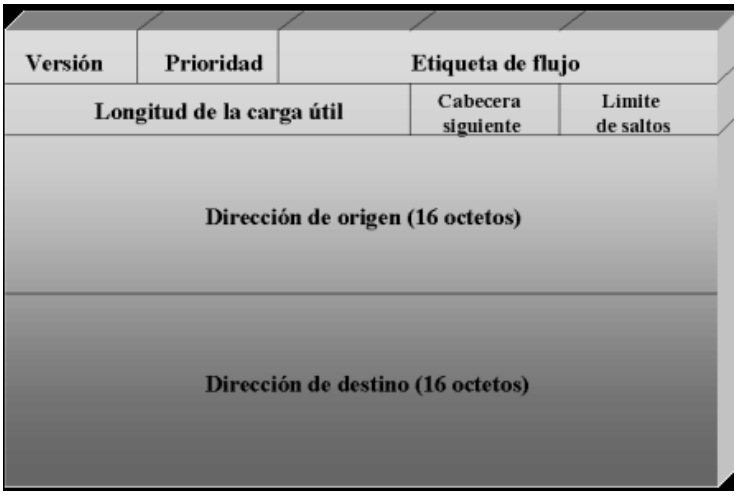


Figura 2.12.- Cabecera Fija IPV6 [29]

Dónde:

- Versión deberá valer 6, en formato de 4 bits.
- Prioridad indicará el tipo de tráfico (se pretende asignar prioridades al trafico según sus necesidades).
- Etiqueta de flujo permitirá tratar de manera más eficiente los flujos de información como los que se generan en aplicaciones multimedia.
- Longitud de la carga útil indica el tamaño de los datos enviados en la trama.
- Cabecera siguiente avisa de la existencia de cabeceras adicionales (o de extensión).
- Límite de saltos viene a sustituir al antiguo TTL, dándole un nombre adecuado al uso que de ese campo se hacía.
- Dirección de origen y dirección de destino Los dos campos de dirección son de 16 bytes.

29 http://www.dei.uc.edu.py/tai2003/ipv6/imagenes/cabeipv4.gif

2.5 COMPARACIÓN ENTRE MODELOS OSI Y TCP/IP

2.5.1 SIMILITUD ENTRE EL MODELO OSI Y EL MODELO TCP/IP

Ambos se dividen en capas o niveles.

Se supone que la tecnología es de conmutación de paquetes (no de conmutación de circuitos).

Los profesionales de networking deben conocer ambos: OSI como modelo; TCP/IP como arquitectura real.

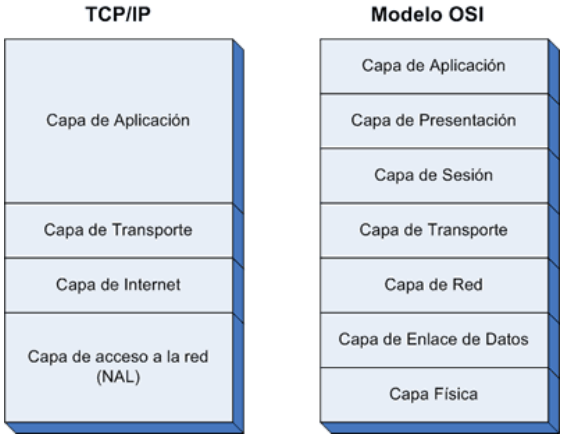


Figura 2.13.- Comparación modelos TCP/IP OSI [30]

2.5.2 DIFERENCIA ENTRE EL MODELO OSI Y EL MODELO TCP/IP

- OSI distingue de forma clara los servicios, las interfaces y los protocolos. TCP/IP no lo hace así, no dejando de forma clara esta separación.
- OSI fue definido antes de implementar los protocolos, por lo que algunas funcionalidades necesarias fallan o no existen. En cambio, TCP/IP se creó después que los protocolos, por lo que se amolda a ellos perfectamente.
- TCP/IP parece ser más simple porque tiene menos capas.

2.6 PROTOCOLOS DE TCP /IP [31]

TCP/IP es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de

30 http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

31 http://elsitiodetelecomunicaciones.iespana.es/protocolo_tcp_ip.htm

todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware.

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. En Internet se diferencian cuatro niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

- Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET) y otros más recientes como el protocolo HTTP (Hypertext Transfer Protocol).
- Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.
- Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.
- Enlace: Los niveles OSI correspondientes son el de enlace y el nivel físico. Los protocolos que pertenecen a este nivel son los encargados de la transmisión a través del medio físico al que se encuentra conectado cada host, como puede ser una línea punto a punto o una red Ethernet.

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el

intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

2.7 REDES BPL

2.7.1 INTRODUCCIÓN

BPL es una tecnología que permite el envío y recepción de señales de telecomunicaciones, con altas velocidades de transmisión y comunicaciones de banda ancha a través de las redes eléctricas y los sistemas de distribución de bajo y medio voltaje.

2.7.2 BREVE HISTORIA

La idea de utilizar el cable eléctrico para transmisión de información no es nueva. El uso de BPL en sus orígenes se limitaba al control de líneas eléctricas y a la transmisión a baja velocidad de las lecturas de los contadores.

Más adelante, las propias empresas eléctricas empezaron a utilizar sus propias redes eléctricas, para la transmisión de datos de modo interno, pero hubo intentos de implantación fallidos en Inglaterra y Alemania.

Durante finales de los noventa los avances tecnológicos realizados permiten alcanzar velocidades de transmisión de Megabits.

La Banda Ancha sobre línea de energía (abreviada BPL por Broadband over PowerLine) representa el uso de tecnologías PLC o “Power Line Communication” definiéndola como la tecnología de banda ancha que utiliza las líneas eléctricas de media y baja tensión, para proveer servicios de comunicación, datos, etc. sobre IP (Protocolo Internet) a través de la red eléctrica, llegando a los usuarios por medio de la instalación eléctrica existente en hogares, comercios e industria. En este caso, una computadora (o cualquier otro dispositivo) necesitaría solo conectarse a un "modem" PLC enchufado en cualquier toma de energía en una edificación equipada para tener acceso de alta velocidad a Internet.

Esta tecnología resulta ser hoy en día una nueva oportunidad de servicios para las empresas de energía y cooperativas eléctricas, pudiendo brindar a los usuarios soluciones, para las demandas de conectividad y uso eficiente de la energía.

Para comprender la ubicación del PLC dentro del sistema de comunicaciones se desarrollan los siguientes puntos:

2.7.2.1 BPL en términos de prestación de servicios:

Es una innovadora oferta de tecnología que permite nuevas oportunidades de servicios para Empresas Distribuidoras de Energía y Cooperativas Eléctricas. En la actualidad es factible convertir las redes eléctricas y tomacorrientes de una casa, oficina o industria en puntos de entrada y salida de información, ya sea voz, video, datos, etc.

2.7.2.2 BPL en términos de competencia:

Es la tecnología que viene a completar el escenario de soluciones al dilema de última milla, así también como el de última cuadra, permitiendo llegar a todos los usuarios conectados a la red eléctrica.

Además se puede decir que la tecnología BPL ofrece ventajas con respecto a las conexiones regulares de banda ancha basadas en cable coaxial o DSL. La amplia infraestructura disponible permitiría que la gente en lugares remotos tenga acceso a Internet con una inversión de equipo relativamente pequeña para la compañía de electricidad.

La banda ancha es entendida como la conexión permanente de alta velocidad proporcionada por un amplio espectro de tecnologías: Cable Modem, DSL, Wireless, Satelital, Fibra, BPL, etc.

La banda ancha es un concepto relativo que varía en el tiempo y para cada realidad.

El sistema BPL se basa en la capa 2 del modelo OSI. Es decir se forma una LAN desde el equipo GW y el CPE.

Usa el CHIP DS2 para la trasmisión de datos a través del cableado eléctrico.

2.7.3 CARACTERÍSTICAS DE LA RED BPL

- No es necesario ningún tipo de obra adicional para poder disfrutar es esta tecnología de Banda Ancha, al utilizar la propia red eléctrica para la transmisión de datos y voz.

- No sufre de los inconvenientes de ADSL o cable que no llega en muchos casos al usuario final. Al estar ya implantada la red eléctrica permite llegar a cualquier punto geográfico.
- Se dispone de una única toma a la cual se conecta un módem con tecnología PLC.
- La conexión es permanente durante las 24 horas del día.
- Su instalación por parte del cliente, es sencilla y rápida.
- El ancho de banda es de 45 Mbps, aunque actualmente ya se alcanzan velocidades de 135 Mbps y en breve se llegará a 200 Mbps, permitiendo la distribución de datos, voz y vídeo de manera rápida y confiable.
- Posibilidad de implementar servicios como Internet a altas velocidades, telefonía VoIP (Voz sobre IP), Videoconferencias, VPN's, Redes LAN, Juegos en línea, teletrabajo y comercio electrónico.

2.7.4 COMPONENTES DE LA RED BPL

La red BPL se compone de:

1. Cableado de Media Tensión.
2. Subestación de Electricidad.
3. Transformadores de Media a Baja Tensión.
4. Cableado de Baja Tensión.
5. Acometida Eléctrica.
6. Medidores.
7. Cableado Eléctrico, Interno en Casa.

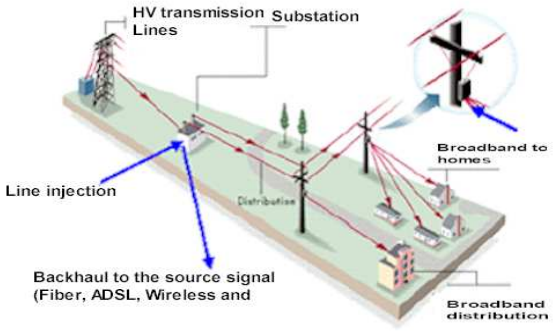


Figura 2.14.- Componentes de un sistema BPL [32]

32 Tesis Cerón Erick, Gómez Boris Diseño de una red de datos TCP/ IP basada en PLC (Power Line Communication) 2009.

2.7.5 ACCESO

La tecnología BPL utiliza como medio de acceso a las líneas de medio y bajo voltaje cuya infraestructura ya es existente.

Esta tecnología utiliza las líneas de medio voltaje para la distribución de la señal, mientras que las líneas de bajo voltaje las utiliza para dar acceso.

2.7.6 ACCESO A LA RED INTERNA O LAN

Es la Red de distribución doméstica que comprende el cableado de energía y las tomas dentro de los locales del usuario final.

2.7.7 APLICACIONES

Entre las aplicaciones de la tecnología BPL se tiene:

- Acceso a Internet
- VoIP
- Video Streaming
- Gaming
- Vigilancia
- Entre otras

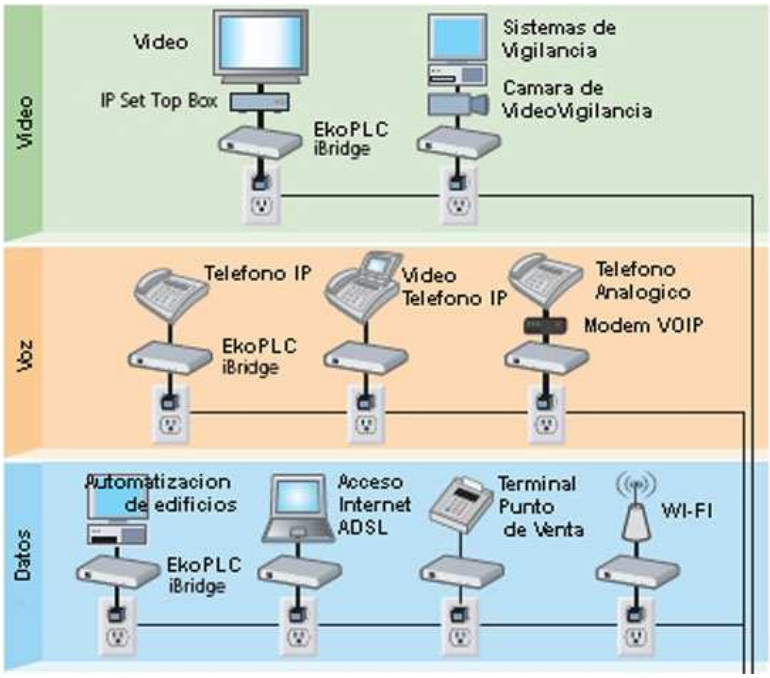


Figura 2.15.- Aplicación de la Tecnología BPL [33]

33 http://www.ekoplc.net/aplicaciones/index.htm

2.7.8 FUNCIONAMIENTO

Su funcionamiento es similar a la tecnología ADSL, en el caso de la Tecnología BPL hace convivir en un mismo medio al servicio eléctrico que trabaja a 60 Hz y al servicio de comunicaciones (datos, voz, video) en el rango de frecuencias de 2 MHz a 34 MHz.

Maneja canales de frecuencia denominados “Modo” los cuales son un conjunto de frecuencias que trabajan utilizando Multiplexación por División de Frecuencia (FDM), los que permiten su operación.

2.7.9 FACTORES QUE AFECTAN LA SEÑAL BPL

2.7.9.1 Atenuación

Es la reducción de la potencia de la señal con la distancia.

Motivos:

- Resistencia del cable (calor)
- Emisión electromagnética al ambiente.

La atenuación es el principal factor limitante de la capacidad de transmisión de datos.

A mayor distancia mayor atenuación:

- Inducción generada por equipos que contiene motores como son el caso de balastros, secadores, aspiradores entre otros.
- Desacoplamiento de impedancias por utilizar cables de diferentes diámetros, por los empalmes realizados su afectación es impredecible.

2.7.9.2 Ruido

- Ruido Ambiental, por ejemplo: RF radio, este es incorregible.
- Ruido Incidental, este ocurre por limitado tiempo y afecta a limitado rango de frecuencias. Técnicamente este tipo de ruido es corregible.

2.7.10 VENTAJAS BPL

- Utiliza la infraestructura existente (red eléctrica interna).
- Los servicios ofertados son competitivos en calidad y en precio.
- Complemento válido a las conexiones ADSL.

- Economía de instalación. Sin obra civil.
- Emisiones electromagnéticas. Equiparables a ADSL y muy inferiores a la telefonía móvil.
- Anchos de banda muy superiores a ADSL. El límite de velocidad para ADSL es 2Mb. PLC puede llegar a ofrecer velocidades superiores a los 10Mb.
- Monopolio en el bucle local. No existen alternativas a ADSL y el operador dominante tiene más del 90% de cuota de mercado. Cualquier enchufe en casa se convertirá en un acceso a los servicios.

2.7.11 DESVENTAJAS BPL

- Si las redes eléctricas están deterioradas o los cables se encuentran en mal estado o tienen empalmes mal hechos no es posible utilizar esta tecnología.
- La distancia también puede ser una limitación, la medida óptima de transmisión es de 100 metros por lo que, a mayores distancias, se hace necesario instalar repetidores.
- El cable eléctrico es una línea metálica recubierta de un aislante. Esto genera a su alrededor unas ondas electromagnéticas que pueden interferir en las frecuencias de otra ondas de radio.
- El 'ruido' en las líneas que impide mantener la calidad de la comunicación. Para evitarlo, es necesario localizar los equipos que los causan y aislarlos mediante un filtro.
- Otro problema es la estandarización de la tecnología PLC, ya que en el mundo existen alrededor de 40 empresas desarrollando dicha tecnología. Para solventar este problema, la organización internacional PLC Forum intenta conseguir un sistema estándar, para lo cual está negociando una especificación para la coexistencia de distintos sistemas PLC. Otro protocolo para líneas PLC fue creado por empresa israelí Nisko que desarrollo el NISCOM.

2.8 ADAPTADORES PLC

Figura 2.16.- Adaptador PLC [34]

Es un equipo que aprovecha el cableado eléctrico existente, para conectar dos elementos Ethernet por ejemplo: El Router y el ordenador, ó, el Router y el Decodificador.

Se enchufa a una toma eléctrica convencional y dispone de un conector Ethernet, para conectar cualquiera de los equipos Ethernet antes indicados.

Se instalaran tantos adaptadores PLC-Ethernet como equipos se vayan a conectar al router ADSL. Por tanto, han de instalarse como mínimo dos adaptadores PLC-Ethernet (uno para el router y otro para el ordenador o el decodificador).

Se pueden instalar hasta un máximo de 7-8 adaptadores PLC-Ethernet, si bien hay que tener en cuenta, que entre todos ellos comparten el ancho de banda disponible.

34 http://articulo.mercadolibre.cl/MLC-32382617-adaptado

2.8.1 CUADRO DE COMPARACIÓN BPL FRENTE A OTROS SISTEMAS

Comparación BPL frente a otros sistemas

	Cableado habitual	Inalámbrico	Sistema de EkoPLC
Instalación	Gran pérdida de tiempo en la instalación, tomando de 2 semanas a los meses para instalar los cables; sistema costoso de instalación.	Gran pérdida de tiempo en la instalación, Debe instalar los cables para conectar puntos de acceso sin cables con la red. Las ediciones físicas o ambientales pueden limitar el despliegue eficaz.	Simple - instalado dentro de horas/ días con equipo mínimo, cableado mínimo y con mínima interrupción a los inquilinos del edificio. Bajo costo.
Coste	Altos costes iniciales para unir con cables un edificio; costes en curso mínimos.	Altos costes iniciales, costes en curso mínimos. Puede costar más que con cableado con la necesidad de funcionar los cables y de instalar puntos de acceso sin cables adicionales.	Gastos bajos de la instalación y de explotación.
Confiabilidad	Extremadamente confiable.	Interferencia de varias fuentes y los tipos de construcción reducen confiabilidad.	Extremadamente confiable.
Funcionamiento	Rendimiento de procesamiento hasta 100 Mbps.	Rendimiento de procesamiento hasta 11 Mbps para 802.11b. Los obstáculos y la distancia físicos degradan perceptiblemente el funcionamiento.	Rendimiento de procesamiento hasta 7 Mbps en la versión actual del producto. El funcionamiento del usuario final es dictado por la velocidad de la conexión de banda ancha.
Seguridad	Seguridad física solamente.	Pobre - bastante campo común para que usuarios puedan tener acceso redes y cuentas de otros usuarios'.	Seguridad física. Asegurar el estándar de cifrado de 56 datos del pedacito (DES) y el estándar avanzado 256 pedacitos del cifrado (AES) para los usos del gobierno.
Movilidad	Limitado al área mantenida por las tomas de la pared.	Muy bueno; la señal se puede atravesar las paredes densas u otros materiales.	Muy bueno - Internet y datos tienen acceso en cada enchufe eléctrico.
EkoPLC proporciona la solución	NO	SÍ	SÍ

Figura 2.17.- Comparación BPL frente a otros sistemas [35]

2.8.2 CLASIFICACIÓN DE LAS REDES BPL

- Red de alto voltaje: transporta la energía desde los centros de generación hasta las grandes áreas de consumo. Las distancias de transporte son grandes, lo que implica altos voltajes para minimizar las pérdidas (una región, un país, entre países).

35 http://www.ekoplc.net/tabla-comparativa/index.htm

- Red de medio voltaje: distribuye la energía dentro de un área de consumo determinada (una ciudad, una comarca).
- Red de bajo voltaje: distribuye la energía a los locales de usuario final, a los voltajes de utilización final (110V-220V-380V).
- Red de distribución doméstica: comprende el cableado de energía y las tomas dentro de los locales del usuario final.

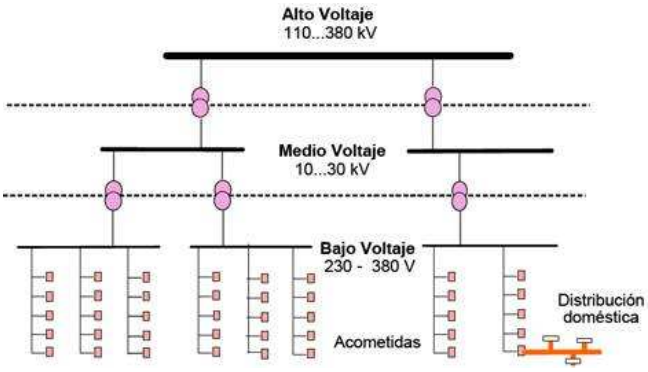


Figura 2.18.- Modelo de Referencia de la Red de Distribución Eléctrica[36]

2.8.3 ANÁLISIS DE SEGMENTOS DE REDES BPL

El papel de las comunicaciones de Banda Ancha sobre la Red Eléctrica o comunicaciones BPL se puede analizar en cada uno de estos segmentos:

- Comenzando por la red de distribución doméstica, que es donde más despliegue real de telecomunicaciones sobre líneas de energía existe actualmente, el objetivo es convertir el cableado de distribución doméstico en una red de área local, siendo cada enchufe un punto de acceso a esta red. Al considerar las soluciones BPL totales, la distribución, utilizando la red interna de los usuarios, constituye una gran ventaja competitiva en comparación con soluciones alternativas.
- Las redes de bajo y medio voltaje pueden considerarse conjuntamente, ya que las soluciones adoptadas abarcan ambas redes. La red de bajo voltaje constituye lo que en el dominio de las telecomunicaciones se ha dado en llamar “la última milla”; se extiende desde el transformador de media a baja tensión hasta los contadores de los abonados.

36 Tesis Cerón Erick, Gómez Boris Diseño de una red de datos TCP/ IP basada en PLC (Power Line Communication) para una urbanización residencial Febrero 2009.

Cabe señalar aquí características importantes de este tramo de la red:

- Varios abonados están conectados a la misma fase; es decir, la red eléctrica desde un punto de vista de transmisión de la información es un medio compartido.
- El número de abonados que son servidos desde un transformador de media a baja, y que constituye un punto candidato para inyectar las señales de telecomunicaciones, varía ampliamente de país a país.
- La red eléctrica no ha sido diseñada para transportar información que requiera cierto ancho de banda; de hecho constituye un medio muy hostil: un canal con una respuesta en frecuencia muy variable, tanto de lugar a lugar como en el tiempo, y muy ruidoso. La banda de frecuencias actualmente aprovechable ("the sweet spot") se extiende desde 1 MHz hasta los 30 MHz.

- Las primeras aplicaciones de PLC se remontan a hace más de veinte años en aplicaciones de banda estrecha, con velocidades de transmisión de unos pocos kbps, siendo su aplicación objetivo la lectura automática de contadores, detección y localización de averías y, en algunos casos, control de carga. La PLC de banda ancha o BPL, tiene entre sus aplicaciones no sólo dar servicios de telecomunicaciones a los usuarios finales, sino también soportar este tipo de aplicaciones de operación de la red de energía.
- Las líneas de la red de alto voltaje se utilizan para transportar señales de telemetría, información de supervisión y órdenes de reconfiguración de la red. También es frecuente que las compañías eléctricas desplieguen una infraestructura de telecomunicación para cubrir sus propias necesidades de comunicaciones entre subestaciones.

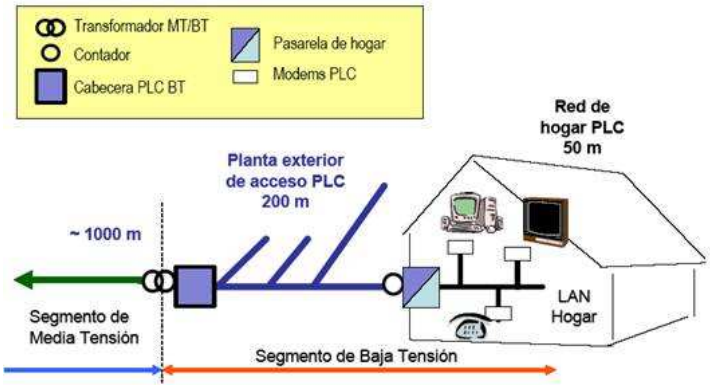


Figura 2.19.- Características de los Segmentos de Baja Tensión y Red Doméstica [37]

- En el segmento de bajo voltaje las distancias del orden de 200 metros desde el transformador al usuario son las más comunes, siendo un medio compartido, con numerosas ramificaciones para servir a los usuarios. Esto hace que el medio sea tremendamente hostil, debido a:
  - La atenuación a las frecuencias de interés con la distancia.
  - Las reflexiones que se producen en las ramificaciones, lo que hace que la función de transferencia del canal presente desvanecimientos selectivos.
  - Las diversas fuentes de ruido de fondo (-120dBm/Hz), impulsivo e interferencias selectivas (por ejemplo emisiones de radio), que hacen necesarias técnicas de codificación contra errores (Reed-Solomon), entrelazado y adaptación a las características de señal/ruido del canal (OFDM).

2.9 SEGURIDAD

2.9.1 SEGURIDAD INFORMÁTICA

En la actualidad, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que

37 Tesis Cerón Erick, Gómez Boris Diseño de una red de datos TCP/ IP basada en PLC (Power Line Communication) para una urbanización residencial Febrero 2009.

permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados.

Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones, con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Toda organización debe estar a la vanguardia de los procesos de cambio. Disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental. Donde la información se reconoce como:

- Crítica, indispensable para garantizar la continuidad operativa de la organización.
- Valiosa, es un activo corporativo que tiene valor en sí mismo.
- Sensitiva, debe ser conocida por las personas que necesitan los datos.
- Donde identificar los riesgos de la información es de vital importancia.

La seguridad informática debe garantizar:

- Disponibilidad, integridad y confidencialidad de los sistemas de información.
- Recupero rápido y completo de los sistemas de información

2.9.1.1 Políticas de seguridad informática (PSI)

Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización.

No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que se desea proteger y el porqué de ello.

Cada PSI es consciente y vigilante del personal por el uso y limitaciones de los recursos así como los servicios informáticos críticos de la compañía.

2.9.1.2 Elementos de una política de seguridad

Como se mencionó en el apartado anterior, una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las PSI deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las PSI deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

De igual forma, las PSI establecen las expectativas de la organización en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan en la compañía. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasará o cuándo algo sucederá; no es una sentencia obligatoria de la ley.

Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros.

2.9.2 SEGURIDAD EN REDES

El objetivo principal de la seguridad en redes es mantener la provisión de información libre de riesgo y brindar servicios para un determinado fin. Es decir, mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

2.9.3 SEGURIDAD GLOBAL

2.9.3.1 Red Global

El concepto de red global incluye todos los recursos informáticos de una organización, aun cuando estos no estén interconectados:

- Redes de área local (LAN),
- Redes de área metropolitana (MAN),
- Redes nacionales y supranacionales (WAN),
- Computadoras personales, mini y grandes sistemas.

De manera que, seguridad global es mantener bajo protección todos los componentes de una red global. Ya que los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar. Siempre hay que tener en cuenta que la seguridad comienza y termina con personas.

Obtener de los usuarios la concientización de los conceptos, usos y costumbres referentes a la seguridad, requiere tiempo y esfuerzo. Que los usuarios se concienticen de la necesidad y, más que nada, de las ganancias que se obtienen

implementando planes de seguridad, exige trabajar directamente con ellos, de tal manera que sea poder en de los beneficios de tener un buen plan de seguridad. (Por ejemplo: permite que se determine exactamente lo que debe hacer cada uno y cómo debe hacerlo, y, también las desviaciones que se pueden producir). De esta forma, ante cualquier problema, es muy fácil determinar dónde se produjo o de dónde proviene.

Para realizar esto, lo más usado, y que da muy buenos resultados es hacer "grupos de trabajo" en los cuales se informen los fines, objetivos y ganancias de establecer medidas de seguridad, de tal manera que los destinatarios finales se sientan informados y tomen para sí los conceptos. Este tipo de acciones favorece, la adhesión a estas medidas.

2.10 FIREWALL

Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

2.10.1 TIPOS DE CORTAFUEGOS

2.10.1.1 Cortafuegos de capa de red o de filtrado de paquetes [38]

Se utilizan Routers con filtros y reglas basadas en políticas de control de acceso. El Router es el encargado de filtrar los paquetes (unChoke) basados en cualquiera de los siguientes criterios:

Protocolos utilizados.

- Dirección IP de origen y de destino.

38 http://www.segu-info.com.ar/firewall/filtradopaquetes.htm

- Puerto TCP-UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida.

El filtrado de paquetes mediante puertos y protocolos permite establecer qué servicios estarán disponibles al usuario y por cuales puertos. Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado).

Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red.

Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta debilidades como:

- No protege las capas superiores a nivel OSI.
- Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
- No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
- Sus capacidades de auditoria suelen ser limitadas, al igual que su capacidad de registro de actividades.
- No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

2.10.1.2 Proxy Gateways de Aplicaciones[39]

Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación o Bastion Host.

El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes.

39http://www.segu-info.com.ar/firewall/proxygateways.htm

Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real y devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.

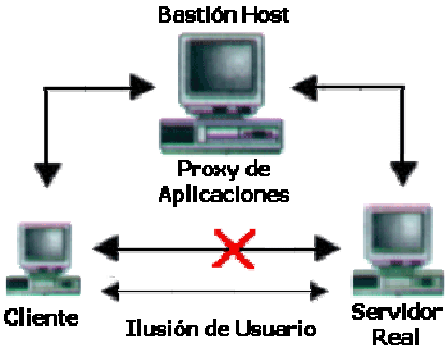


Figura 2.20.- Proxy de aplicaciones [40]

2.11 VIDEOVIGILANCIA

El video vigilancia es un sistema que sirve para supervisar una casa o negocio a distancia sin necesidad de tener un ordenador instalado en el lugar vigilado, sólo con disponer de una conexión a Internet y una toma de corriente eléctrica. La Video vigilancia permite conectarse a un dispositivo (servidor web de vídeo) provisto de cámaras desde cualquier lugar para visualizar lugares diversos como empresas, comercios, hogares, etc.… proporcionando además acceso para gestionar el equipo y poder realizar cambios en su configuración, recuperar imágenes grabadas o en tiempo real.

La captura de estas imágenes se realiza mediante servidores web de vídeo o cámaras IP que son los dispositivos encargados de transmitir, a través de ADSL, toda la información de vídeo que estén captando las cámaras en ese momento, o incluso las imágenes almacenadas en el disco duro, si se trata de un servidor web de vídeo con grabador incorporado.

Además, estos dispositivos ponen a su disposición multitud de funciones como envío de correos electrónicos por detección de movimiento y entrada de alarma, soporte de IP dinámica, visionado de las cámaras en teléfonos móviles o

40 http://www.segu-info.com.ar/firewall/proxygateways.htm

dispositivos portátiles como PDAs, entre otras, y todo ello sin ningún coste adicional para usted.

2.11.1 BENEFICIOS

- Simplicidad. La utilización de la plataforma es simple, intuitiva y amigable para cualquier tipo de usuario. Desde operadores de seguridad tradicionales hasta gerentes generales interesados en mantener un seguimiento de sus instalaciones.
- Seguridad. El manejo de diferentes perfiles de usuario permite diferenciar los niveles de acceso.
- Flexibilidad. La solución se adapta a las necesidades puntuales de cada empresa.
- Respaldo. La infraestructura empleada para el despliegue de la solución se encuentra íntegramente compuesta por los operadores más reconocidos del mercado.
- Economía. La infraestructura de Video Vigilancia que se propone permite la incorporación de sistemas legados sin la necesidad de grandes inversiones iníciales.

2.12 CÁMARAS IP

Es un dispositivo autónomo que cuenta con un servidor web de video incorporado, también conocidas como cámaras Web o de Red, videocámaras especialmente diseñadas para enviar las señales (video, y en algunos casos audio) pudiendo estar conectadas directamente a un Router ADSL o bien a través de redes IP como redes LAN, WAN a través de concentrador (un HUB o un SWITCH) e INTERNET desde un explorador (por ejemplo el Internet Explorer).

En las cámaras IP pueden integrarse aplicaciones como detección de presencia (incluso el envío de mail si detectan presencia), grabación de imágenes o secuencias en equipos informáticos (tanto en una red local o en una red externa (WAN), de manera que se pueda comprobar por qué ha saltado la detección de presencia y se graben imágenes de lo sucedido.

Las imágenes se pueden visualizar utilizando un navegador Web estándar y pueden almacenarse en cualquier disco duro. Tanto si necesita una solución de

vigilancia IP para garantizar la seguridad de personas y lugares, como para supervisar propiedades e instalaciones de modo remoto o retransmitir eventos en la Web con imágenes y sonidos reales.

Si un edificio o una casa poseen una red ya sea alámbrica o inalámbrica ya cuenta con la infraestructura necesaria para incorporar cámaras de red. Una cámara de red realiza la mayoría de las funciones que lleva a cabo una cámara análoga estándar de circuito cerrado, pero proporciona más funcionalidades a un precio notablemente inferior.

2.12.1 CARACTERÍSTICAS

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

Además de comprimir el video 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.
- Una cámara IP tiene incorporado un ordenador pequeño y especializado en ejecutar aplicaciones de red. Por lo tanto, la cámara IP no necesita estar conectada a un PC para funcionar. Esta es una de sus diferencias con las denominadas cámaras web.
- Una cámara IP tiene su propia dirección IP y se conecta a la red como cualquier otro dispositivo; incorpora el software necesario de servidor de web, servidor o cliente FTP, de correo electrónico... y tiene la capacidad de

ejecutar pequeños programas personalizados (denominados scripts).

- Las cámaras de red más avanzadas pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de vídeo analógico.
- Las cámaras IP incorporan todas las funciones de una cámara de vídeo y añaden más prestaciones.
- La lente de la cámara enfoca la imagen en el sensor de imagen (CCD). Antes de llegar al sensor, la imagen pasa por el filtro óptico que elimina cualquier luz infrarroja y muestra los colores correctos.
- Actualmente están apareciendo cámaras día/noche que disponen de un filtro de infrarrojos automático, este filtro se coloca delante del (CCD) sólo cuando las condiciones de luz son adecuadas proporcionándonos de esta manera imágenes en color, cuando las condiciones de luz bajan este filtro se desplaza y la cámara emite la señal en blanco y negro produciendo más luminosidad y de esta manera se podrá iluminar la escena con luz infrarroja y ver en total oscuridad.
- El sensor de imagen convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas señales eléctricas se encuentran ya en un formato que puede ser comprimido y transferido a través de redes.
- Como las cámaras de vídeo convencionales, las cámaras IP gestionan la exposición (el nivel de luz de la imagen), el equilibrio de blancos (el ajuste de los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen. Estas funciones las lleva a cabo el controlador de cámara y el chip de compresión de vídeo.
- Las cámaras IP comprimen la imagen digital en una imagen que contiene menos datos para permitir una transferencia más eficiente a través de la Red, cámaras MPEG4.

2.12.2 COMPONENTES

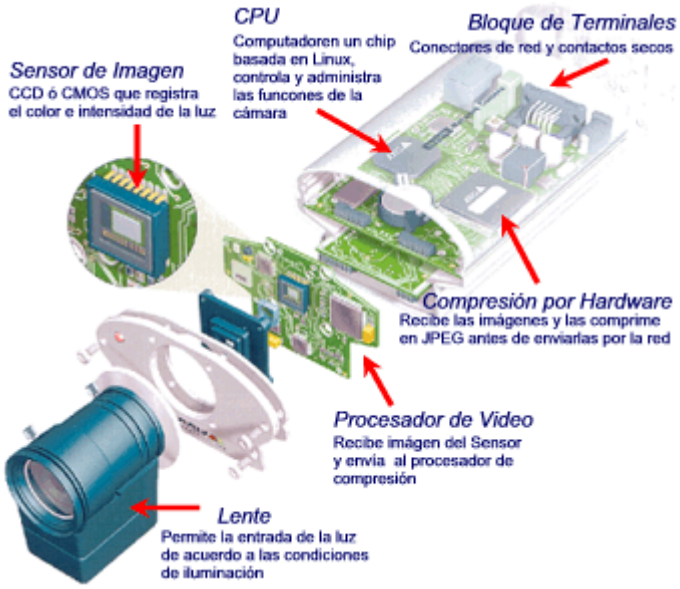


Figura 2.21.- Componentes de la cámara IP[41]

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

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

El procesador ARTPEC (Axis Real Time Picture EnCoder) desarrollado y patentado por Axis realiza las funciones de administración y control de la exposición (Niveles de Luz), balance de blancos (Ajuste de Colores), brillo de la imágen y otros aspectos relacionados con la calidad de la imágen, también este

41 http://3.bp.blogspot.com/_jOq9Ar1JN8Q/SvyqKpsiDVI/AAAAAAAAAuo/rj66HgBmzSc/s400/camaraip3d.gif

procesador incluye un componente de compresión el cual comprime las imágenes digitales a un formato que contiene menos datos y que puede ser transmitido por la red de forma eficiente.

El conector de red Ethernet es habilitado por el chip ETRAX también desarrollador por Axis, el cual es una solución optimizada para conectar periféricos en la red. El chip ETRAX incluye un CPU de 32 bits, conectividad Ethernet de 10/100 MBits, funciones avanzadas para el manejo de memoria directa (DMA) y un amplio rango de interfaces de entrada/salids (I/O).

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

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

2.12.3 VENTAJAS

Entre las ventajas de las cámaras IP:

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

de la cámara.

2.12.4 CONEXIÓN DE UNA CÁMARA IP

Figura 2.22.- Conexión de una cámara IP [42]

2.12.5 SOFTWARE DE VIDEOVIGILANCIA

En el mercado se podrá encontrar Software para video vigilancia. Aquí se mencionara algunos de estos:

- Geovision GV 800
- ZoneMinder
- Vitamin d
- uWatchIt 5.0

2.12.6 APLICACIONES

Algunas de las aplicaciones más frecuentes de las cámaras IP son la vigilancia de:

- Viviendas, permitiendo visionar la propia vivienda desde la oficina, desde un hotel, cuando estamos de vacaciones.

42 http://www.infokrause.com/que_es_una_camara_ip.htm

- Negocios, permitiendo controlar por ejemplo varias sucursales de una cadena de tiendas, gasolineras.
- Instalaciones industriales, almacenes, zonas de aparcamiento, Muelles de descarga, accesos, incluso determinados procesos de maquinaria o medidores.
- Hostelería, Restauración, Instalaciones deportivas.
- Lugares Turísticos, cada día es más frecuente que Organismos oficiales, como: Comunidades Autónomas, Ayuntamientos, promocionen sus zonas turísticas, o lugares emblemáticos de las ciudades, instalaciones deportivas, implementado en sus páginas Web las imágenes procedentes de cámaras IP estratégicamente situadas en esos lugares.

Estas son algunas de las aplicaciones cámaras IP con más demanda.

Además las cámaras IP proporcionan un enorme abanico de posibilidades de costo efectivo para el monitoreo y vigilancia remota de personas, propiedades, lugares, activos, maquinaria y equipo, zonas turísticas, aseguramiento de bienes y personas con ayuda de información de alarmas y detección de movimiento. Prácticamente las posibilidades son ilimitadas y tienen la ventaja de que el video al ser transmitido por la red puede ser consultado en cualquier lugar del mundo.
Algunas de las aplicaciones de monitoreo y vigilancia que actualmente están utilizando esta tecnología son:

- Monitoreo y vigilancia Urbana y lugares públicos,
- Monitoreo y vigilancia residencial con o sin manejo de alarmas,
- Monitoreo y vigilancia de oficinas, fábricas y negocios,
- Monitoreo y vigilancia de escuelas y hospitales,
- Monitoreo y vigilancia de casinos,
- Monitoreo y vigilancia de Bancos, Casas de Bolsa, Aseguradoras, Casas de Cambio,
- Monitoreo y vigilancia de Obras de Construcción,
- Monitoreo y vigilancia de Museos,
- Monitoreo y vigilancia de Carreteras y vías de comunicación,
- Monitoreo y vigilancia de Equipo y Maquinaria,
- Monitoreo y vigilancia de enfermos, niños, ancianos y mascotas,

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

2.13 SERVIDORES

2.13.1 SERVIDOR DE DHCP[43]

El protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de una red. El estándar DHCP permite el uso de servidores DHCP para administrar la asignación dinámica, a los clientes DHCP de la red, de direcciones IP y otros detalles de configuración relacionados, siempre que los clientes estén configurados para utilizar un servidor DHCP.

Cada equipo de una red TCP/IP debe tener un nombre y una dirección IP únicos. La dirección IP (junto con su máscara de subred relacionada) identifica al equipo host y a la subred a la que está conectado. Al mover un equipo a una subred diferente, se debe cambiar la dirección IP; DHCP permite asignar dinámicamente una dirección IP a un cliente, a partir de una base de datos de direcciones IP de servidor DHCP de la red local. En las redes TCP/IP, DHCP reducen la complejidad y cantidad de trabajo que debe realizar el administrador para reconfigurar los equipos.

DHCP es el protocolo de servicio TCP/IP que "alquila" o asigna dinámicamente direcciones IP durante un tiempo (duración del alquiler) a las estaciones de trabajo, distribuyendo además otros parámetros de configuración entre clientes de red autorizados, tales como la puerta de enlace o el servidor DNS. DHCP proporciona una configuración de red TCP/IP segura, confiable y sencilla, evita conflictos de direcciones y ayuda a conservar el uso de las direcciones IP de clientes en la red. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP utilizadas en la

43http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-dhcp

red. Los clientes compatibles con DHCP podrán solicitar a un servidor DHCP una dirección IP y obtener la concesión como parte del proceso de inicio de red.

Las estaciones de trabajo "piden" su dirección IP (y demás configuraciones para este protocolo) al servidor, y éste les va asignando direcciones del rango que sirve, de entre aquellas que le quedan libres; si se desea que a determinados equipos el servidor les sirva siempre la misma, se puede llegar a "forzar" la asignación de la dirección IP deseada a equipos concretos. Además también pueden excluirse del rango de direcciones IP que va a servir nuestro servidor, aquellas que desea que estén asociadas de forma estática a determinados equipos o periféricos de red.

Si por error se dejáse algún equipo de la red configurado con un direccionamiento IP estático del rango gestionado por nuestro servidor DHCP, podría ocurrir que cuando nuestro servidor "alquilase" una IP a la estación de trabajo solicitante, dicha dirección IP fuera la que estuviera siendo utilizada por el equipo con direccionamiento estático, provocándose un conflicto de IP; en ese caso el cliente selecciona otra dirección IP y la prueba, hasta que obtenga una dirección IP que no esté asignada actualmente a ningún otro equipo de nuestra red. Por cada conflicto de direcciones, el cliente volverá a intentar configurarse automáticamente hasta con 10 direcciones IP.

2.13.1.1 Beneficios de Servidor DHCP Linux frente a otros Sistemas Operativos

- Se puede administrar de manera centralizada toda la información de configuración de IP. De esta forma se elimina la necesidad de configurar manualmente los clientes individualmente cuando se implanta por primera vez TCP/IP o cuando se necesitan cambios en la infraestructura de IP.
- Se asegura que los clientes de DHCP, obtienen parámetros de configuración de IP precisos y en tiempo, sin intervención del usuario. Como la configuración es automática se elimina gran parte de los problemas.
- Flexibilidad. Utilizando DHCP, el administrador aumenta su flexibilidad para el cambio de la información de configuración de IP, lo que permite que el administrador cambie la configuración de IP de manera sencilla cuando

se necesitan los cambios.

2.13.2 SERVIDOR DE VIDEO

2.13.2.1 Introducción

Un Servidor web de Vídeo permite ver las imágenes procedentes de una casa o negocio en todo momento esté donde esté, ya que no necesita ningún programa auxiliar para poder visionar o gestionar el equipo.

Un Servidor web de Vídeo se puede instalar en una red local de ordenadores, ya existente (en una oficina) o directamente a una conexión ADSL (en una casa particular o empresa).

Si se dispone de una antigua instalación analógica de circuito cerrado de televisión se puede convertir en una moderna instalación digital adquiriendo un servidor web de vídeo en sustitución de los elementos que se utilizara anteriormente para el visionado de sus instalaciones. No se tiene que realizar grandes inversiones, ya que se puede conservar las cámaras analógicas y el cableado de su anterior instalación.

2.13.3 SERVIDOR PROXY (SQUID)

2.13.3.1 Introducción

Squid es un popular programa de software libre que implementa un servidor proxy y un dominio para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

Squid ha sido desarrollado durante muchos años y se le considera muy completo y robusto. Aunque orientado a principalmente a HTTP y FTP es compatible con otros protocolos como Internet Gopher. Implementa varias modalidades de cifrado como TLS, SSL, y HTTPS.

2.13.3.2 Características

Posee las siguientes características:

- Proxy y Caché de HTTP, FTP, y otras URL.
- Squid proporciona un servicio de proxy que soporta peticiones HTTP, HTTPS y FTP a equipos que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentra fuera de la red interna.

2.13.3.3 Proxy para SSL

Squid también es compatible con SSL (Secure Socket Layer) con lo que también acelera las transacciones cifradas, y es capaz de ser configurado con amplios controles de acceso sobre las peticiones de usuarios.

2.13.3.4 Jerarquías de caché

Squid puede formar parte de una jerarquía de caches. Diversos proxys trabajan conjuntamente sirviendo las peticiones de las páginas. Un navegador solicita siempre las páginas a un sólo proxy, si este no tiene la página en la caché hace peticiones a sus hermanos, que si tampoco las tienen las hacen a sus padres. Estas peticiones se pueden hacer mediante dos protocolos:

- HTTP e ICMP.
- ICP, HTCP, CARP, caché digests.

Squid sigue los protocolos ICP, HTCP, CARP y caché digests que tienen como objetivo permitir a un proxy "preguntarle" a otros proxys caché si poseen almacenado un recurso determinado.

2.13.3.5 Caché transparente

Squid puede ser configurado para ser usado como proxy transparente de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. De modo predefinido Squid utiliza el puerto 3128 para atender peticiones, sin

embargo se puede especificar que lo haga en cualquier otro puerto disponible o bien que lo haga en varios puertos disponibles a la vez.

2.13.3.6 WCCP

A partir de la versión 2.3 Squid implementa WCCP (Web Cache Control Protocol). Permite interceptar y redirigir el tráfico que recibe un router hacia uno o más proxys caché, haciendo control de la conectividad de los mismos. Además permite que uno de los proxys caché designado pueda determinar cómo distribuir el tráfico redirigido a lo largo de todo el array de proxys caché.

2.13.3.7 Control de acceso

Ofrece la posibilidad de establecer reglas de control de acceso. Esto permite establecer políticas de acceso en forma centralizada, simplificando la administración de una red.

2.13.3.8 Aceleración de servidores HTTP

Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el caché, si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el caché en lugar de volver a descargarlo desde Internet. Esta función permite navegar rápidamente cuando los objetos ya están en el caché y además optimiza enormemente la utilización del ancho de banda.

2.13.3.9 SNMP

Squid permite activar el protocolo SNMP, este proporciona un método simple de administración de red, que permite supervisar, analizar y comunicar información de estado entre una gran variedad de máquinas, pudiendo detectar problemas y proporcionar mensajes de estados.

2.13.3.10 Caché de resolución DNS

Squid está compuesto también por el programa dns server, que se encarga de la búsqueda de nombres de dominio. Cuando Squid se ejecuta, produce un número configurable de procesos dns server, y cada uno de ellos realiza su propia

búsqueda en DNS. De este modo, se reduce la cantidad de tiempo que la caché debe esperar a estas búsquedas DNS.

En el contexto de las redes informáticas, el término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es el de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

2.13.3.11 Funcionamiento

- El cliente realiza una petición (p. ej. mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.
- Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, contrasta la fecha y hora de la versión de la página demanda con el servidor remoto. Si la página no ha cambiado desde que se cargó en caché la devuelve inmediatamente, ahorrándose de esta manera mucho tráfico pues sólo intercambia un paquete para comprobar la versión. Si la versión es antigua o simplemente no se encuentra en la caché, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda o actualiza una copia en su caché para futuras peticiones.
- El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").
- Los proxies web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen proxies para

interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

- Un cliente de un ISP manda una petición a Google la cual llega en un inicio al servidor Proxy que tiene este ISP, no va directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta en mucho menor tiempo. Cuando el usuario crea una búsqueda en Google el servidor Proxy ya no es utilizado; el ISP envía su petición y el cliente recibe su respuesta ahora sí desde Google.

2.14 WORLD WIDE WEB.

2.14.1 INTRODUCCIÓN

World Wide Web permite acceder a toda la información y a todas las herramientas de Internet de un modo sencillo. Desde Web se puede establecer una conexión Telnet, se puede acceder a archivos vía FTP, mandar un e-mail etc. Y todo esto con un sistema mucho más rápido, cómodo y atractivo.

2.14.2 INCONVENIENTES

- Es necesario tener un ordenador potente, un modem de gran velocidad, y un programa que permita visualizar gráficos (Windows, Macintosh). Hay, de todas formas, una posibilidad de acceder a la información ofrecida por Web sin este tipo de programas, ejemplo Lynx.
- Puede haber tantas páginas Web (se llama página a la información aparecida o publicada en Web) como personas o usuarios de la red existan. Los organismos oficiales y las grandes empresas internacionales tienen una página Web (la Casa Blanca, Para mount Pictures, IBM, Apple, Sony, Disney, etc.). Y cada usuario individual puede crear una propia.

2.14.3 VENTAJAS

- La característica fundamental de Web es la posibilidad de ir de un sitio a otro, gracias al hipertexto, sin conocer la dirección. Si se accede a la

página de Yahoo, ésta nos ofrece un repertorio de temas, muy variados, y podemos entrar a otras páginas sin saber la dirección.

- Otra de las ventajas de Web es la de poder acceder directamente a una página, siempre que se sepa la dirección de ésta. En la parte "location" se podrá escribir la dirección a la que se quiere ir, y evitar el ir "navegando" de un sitio a otro.
- WWW facilita la conexión con otros ordenadores, "host" (un "host" es todo aquel ordenador con una dirección IP que contenga cualquier tipo de información) o "máquinas". No solamente para acceder a páginas Web, sino para acceder a cualquier otro tipo de conexión en red. Antes existía una cantidad de comandos que había que memorizar para establecer una conexión Telnet, conseguir un fichero FTP o mandar un correo electrónico. Web permite hacer todas estas cosas simplemente con el "ratón", con apuntar y pulsar el botón del ratón.

2.15 HTTP

2.15.1 INTRODUCCIÓN

Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web. HTTP fue desarrollado por el World Wide Web Consortium y la Internet Engineering Task Force, colaboración que culminó en 1999 con la publicación de una serie de RFC, el más importante de ellos es el RFC 2616 que especifica la versión 1.1. HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL). Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

2.15.2 TRANSACCIONES HTTP

Una transacción HTTP está formada por un encabezado seguido, opcionalmente, por una línea en blanco y algún dato. El encabezado especificará cosas como la acción requerida del servidor, o el tipo de dato retornado, o el código de estado.

El uso de campos de encabezados enviados en las trames HTTP le dan gran flexibilidad al protocolo. Estos campos permiten que se envíe información descriptiva en la transacción, permitiendo así la autenticación, cifrado e identificación de usuario.

Un encabezado es un bloque de datos que precede a la información propiamente dicha, por lo que muchas veces se hace referencia a él como metadato porque tiene datos sobre los datos.

Si se reciben líneas de encabezado del cliente, el servidor las coloca en las variables de ambiente de CGI con el prefijo HTTP_ seguido del nombre del encabezado. Cualquier carácter guión (-) del nombre del encabezado se convierte a caracteres "_".

El servidor puede excluir cualquier encabezado que ya esté procesado, como Authorization, Content-type y Content-length. El servidor puede elegir excluir alguno o todos los encabezados si incluirlos exceden algún límite del ambiente de sistema. Ejemplos de esto son las variables HTP_ACPT y HTP_R_AEN.

HT_AEP'. Los tipos MIME que el cliente aceptará, dado los encabezados HTTP. Otros protocolos quizás necesiten obtener esta información de otro lugar. Los elementos de esta lista deben estar separados por una coma, como lo dice la especificación HTTP: tipo, tipo.

HTT_USR_AET. El navegador que utiliza el cliente para realizar la petición. El formato general para esta variable es: software/versión biblioteca/versión.

El servidor envía al cliente, un código de estado que indica si la petición fue correcta o no. Los códigos de error típicos indican que el archivo solicitado no se encontró, que la petición no se realizó de forma correcta o que se requiere autenticación para acceder al archivo.

La información propiamente dicha. Como HTTP permite enviar documentos de todo tipo y formato, es ideal para transmitir multimedia, como gráficos, audio y video. Esta libertad es una de las mayores ventajas de HTTP.

Información sobre el objeto que se retorna.

Hay que tener en cuenta que la lista no es una lista completa de los campos de encabezado y que algunos de ellos sólo tienen sentido en una dirección.

2.15.3 VERSIONES

HTTP ha pasado por múltiples versiones del protocolo, muchas de las cuales son compatibles con las anteriores. El RFC 2145 describe el uso de los números de versión de HTTP. El cliente le dice al servidor al principio de la petición la versión que usa, y el servidor usa la misma o una anterior en su respuesta.

2.15.3.1 HTTP/0.9

Obsoleta. Soporta sólo un comando, GET, y además no especifica el número de versión HTTP. No soporta cabeceras. Como esta versión no soporta POST, el cliente no puede enviarle mucha información al servidor.

2.15.3.2 HTTP/1.0 (mayo 1996)

Esta es la primera revisión del protocolo que especifica su versión en las comunicaciones, y todavía se usa ampliamente, sobre todo en servidores proxy.

2.15.3.3 HTTP/1.1 (junio 1999)

Versión actual; las conexiones persistentes están activadas por defecto y funcionan bien con los proxies. También permite al cliente enviar múltiples peticiones a la vez (pipelining) lo que hace posible eliminar el tiempo de Round-Tripdelay por cada petición.

2.15.3.4 HTTP/1.2

Los primeros borradores de 1995 del documento PEP — an Extension Mechanism for HTTP (el cuál propone el Protocolo de Extensión de Protocolo, abreviado PEP) los hizo el World Wide Web Consortium y se envió al Internet Engineering Task Force. El PEP inicialmente estaba destinado a convertirse en un rango distintivo de HTTP/1.2. En borradores posteriores, sin embargo, se eliminó la referencia a HTTP/1.2. El RFC 2774 (experimental), HTTP Extension Framework, incluye en gran medida a PEP. Se publicó en febrero de 2000.

2.16 INTERNET

2.16.1 INTRODUCCIÓN

Internet es una gran red internacional de ordenadores. Permite, como todas las redes, compartir recursos. Es decir: mediante el ordenador, establecer una comunicación inmediata con cualquier parte del mundo para obtener información sobre un tema que nos interesa, ver los fondos de la Biblioteca del Congreso de los Estados Unidos, o conseguir un programa o un juego determinado para nuestro ordenador. En definitiva: establecer vínculos comunicativos con millones de personas de todo el mundo, bien sea para fines académicos o de investigación, o personales.

2.16.2 BREVE HISTORIA

2.16.2.1 ARPANET.

El Ministerio de Defensa de Estados Unidos estableció una red interestatal en los años 60, de modo que toda la defensa del país dependiera de la misma red y compartiera los recursos de ésta. Así nació ARPANet (Advanced Projects Agency Net, llamada también DARPANet, por Defensa), con tres requisitos fundamentales:

- La red debía estar protegida en caso de que un desastre natural o una guerra, especialmente un ataque nuclear, afectase al país, de modo no debilitase a la totalidad de la red, aunque una parte estuviera dañada.
- La red, al igual que no debía ser afectada por la eliminación de una parte,

debía permitir la incorporación de nuevos elementos con facilidad.

- Debía usar un lenguaje (códigos informáticos), un protocolo, que pudiera ser entendido por cualquier ordenador, independientemente del sistema empleado.

ARPANet emplea ya el sistema de envío de Internet: por "paquetes", es decir: cada archivo es dividido en partes, y se le da a cada una el equivalente a una dirección y un sello. Cuando llegan a su destino (puede llegar por diferentes "medios de transporte") se unen y forman el archivo original. El protocolo que ya se usa (y que es el utilizado por Internet desde entonces) es el TCP/IP (Transmission Control Protocol / Internet Protocol). Es el protocolo necesario para que se dé la comunicación entre todos los ordenadores conectados a la red, sea cual sea su sistema operativo o sus características.

En 1983 nace Internet, con un gran número de usuarios y un crecimiento vertiginoso. Al unirse otros países y otras organizaciones, el DNS debe modificarse. A los nombres anteriormente existentes, se le añaden los identificadores del país en cuestión.

2.16.3 OTRAS REDES DENTRO Y FUERA DE INTERNET.

Internet es una red de redes. Muchas pequeñas redes locales forman parte de ella, así como grandes redes internacionales, en un principio independientes, pero que ofreces pasarelas "gateways", para conectar con internet. Algunas de estas redes importantes son:

- ***BITNet:*** *son las siglas de "Because It's Time to Network". La red se formó por los ordenadores principales de instituciones académicas. Tiene su origen en 1981, cuando crea un enlace entre la Universidad de Yale y la de Nueva York. En dos años se extendió hasta California. La red se basa en tecnología IBM.*
- ***FIDONet:*** *es una agrupación de BBS's con capacidad de intercambiar mensajes. Se crea en mayo de 1984 con tan sólo dos operadores de sistema ("sysops"). Basada en FIDONet se crea en 1990 la red K-12Net: una red de BBS's internacionales para intercambiar experiencias académicas.*

- ***Compuserve, AmericaOnLine, IBMNet:*** *grandes compañías que tienen su red particular, en la que permiten abonados a los que ofrecen los servicios de Internet a cambio de una cuota de alta y una cantidad al mes.*
- ***FrEdMail:*** *Free Education Mail: se crea con el objetivo de comunicar a profesores y alumnos de los institutos estadounidenses.*
- ***Free Nets:*** *BBS's sobre sanidad.*
- ***USENet o UUNet:*** *utilidad que proporciona las News en Internet.*

2.16.4 APLICACIONES.

Internet ofrece muchas posibilidades, pero se podrían agrupar en tres herramientas básicas. Se verá otras muchas, pero son variaciones de estas tres posibilidades.

2.16.4.1 Correo Electrónico

La ventaja del Correo Electrónico frente al correo ordinario es fundamentalmente la rapidez. El e-mail llega a su destino en pocos segundos, en lugar de tardar varios días. La ventaja frente al teléfono y el fax es que es mucho más económico (por el tiempo que tarda en mandar el mensaje, no por la tarifa). Es mucho más fiable que el correo ordinario: un correo electrónico no puede "perderse": si por cualquier razón no ha llegado a su destino, se devuelve a quien lo envió con las causas que ocasionaron el error.

En el correo electrónico no es necesario que los dos ordenadores (emisor y receptor) estén en funcionamiento simultáneamente. Al llegar el mensaje a su destino, si no está conectado el ordenador, el correo se almacena, como en un buzón, hasta que el ordenador se conecta y el buzón se vacía.

En el correo electrónico, al igual que en el resto de las herramientas de Internet, existe la posibilidad de trabajar desde una terminal en modo texto o desde una terminal con posibilidad de entornos gráficos. En la UCM cuando trabaja conectados al Alpha, trabaja en modo texto. Sin embargo, en los ordenadores que lo permitan, se puede trabajar con entornos gráficos.

2.16.4.2 TELNET (Conexión remota).

Al estilo de una llamada telefónica a información, podemos entrar en un ordenador que no es el nuestro, y mirar los datos que tiene. No se puede hacer más que mirar. No se podrá traer ningún. Es el sistema empleado, por ejemplo, para ver los fondos de una biblioteca (podemos saber qué libros tiene, pero no podemos ver el libro en cuestión), para saber la previsión del tiempo o para encontrar una dirección de correo electrónico. En resumen: para consultar una base de datos.

Los recursos accesibles vía Telnet podemos encontrarlos en Hytelnet: una base de datos sobre empresas o universidades con posible conexión Telnet. Con Telnet se lograra encontrar a una gran cantidad de usuarios. La base de datos mantenida por Internic es bastante completa.

2.16.4.3 FTP. (File Transfer Protocol).

Esta herramienta posibilita acceder a documentos y ficheros de un ordenador remoto, y traerlos a nuestro ordenador. Un programa, un texto, una foto,... cualquier cosa que esté en el ordenador con el que hemos conectado, mediante unos comandos, se instala en nuestro ordenador (es lo que los Internautas llaman "bajar" de la red).

FTP Anónimo. Las posibilidades de encontrar un programa en un ordenador que no es el nuestro son escasas. Lógicamente, no todas las empresas dejan que cualquier usuario entre en su sistema. Si es una empresa en la que tenemos cuenta (cuenta: suscripción a una determinada empresa o centro de investigación que nos proporcione los servicios de Internet), pedirá un UserName (nombre de usuario) y un Password o PWD (clave) previamente acordados, para reconocernos. Si no se toma en cuenta, se deberá hacer un FTP anónimo. En este caso, como UserName escribiremos Anonymous y como Password dando nuestra dirección de Correo Electrónico. (es una simple cuestión de "netiquette": ya que no se está suscritos, no nos "conocen", por lo menos debemos identificarnos).

2.17 HOST

Son las interfaces de red, que proveen y/o utilizan servicios a/de ella. Los usuarios deben utilizar hosts para tener acceso a la red. En general, los hosts son computadores mono o multiusuario que ofrecen servicios de transferencia de archivos, conexión remota, servidores de base de datos, servidores WWW, etc. Los usuarios que hacen uso de los hosts pueden a su vez pedir los mismos servicios a otras máquinas conectadas a la red.

Un host o anfitrión es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web. Un host de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de host.

El término host también se utiliza para referirse a una compañía que ofrece servicios de alojamiento para sitios web.

CAPÍTULO III. 3. DISEÑO

El diseño de la infraestructura de la red estará basado en el prototipo propuesto para este Proyecto, en el que se implementará la red de video vigilancia combinando la tecnología Ethernet y BPL, con el propósito de dar a conocer las ventajas de la fusión de estas dos.

Según el diagrama propuesto de la Figura 3.1 se plantea el diseño, que tendrá dos estaciones de red: BPL y Ethernet.

La red BPL constará de dos adaptadores PLC (máster y esclavo). Esta red brindará al usuario final los servicios de video vigilancia e internet.

La red Ethernet constará de los servidores de video vigilancia, DHCP y proxy.

La transmisión de datos entre la estación de red Ethernet y BPL se realizará por medio de los adaptadores PLC que estarán conectados a la red de tendido eléctrico.

Para un mejor entendimiento y de acuerdo con el diseño de este prototipo, se lo ha divido en módulos, los mismo que se irán detallando en este capítulo.

3.1 DISEÑO FÍSICO DE LA RED

Según el prototipo de la Figura 3.1, la ESTACIÓN DE RED ETHERNET comenzará tomando como servicio ISP a la red global del laboratorio ASI, luego pasará por el switch que conecta a los servidores configurados para la red Ethernet, mientras que la ESTACIÓN DE RED BPL comenzará en el switch que se conecta desde el servidor DHCP hacia los adaptadores PLC, los mismos que transmitirán los servicios de video vigilancia e internet a cada uno de los usuarios BPL finales mediante el tendido eléctrico.

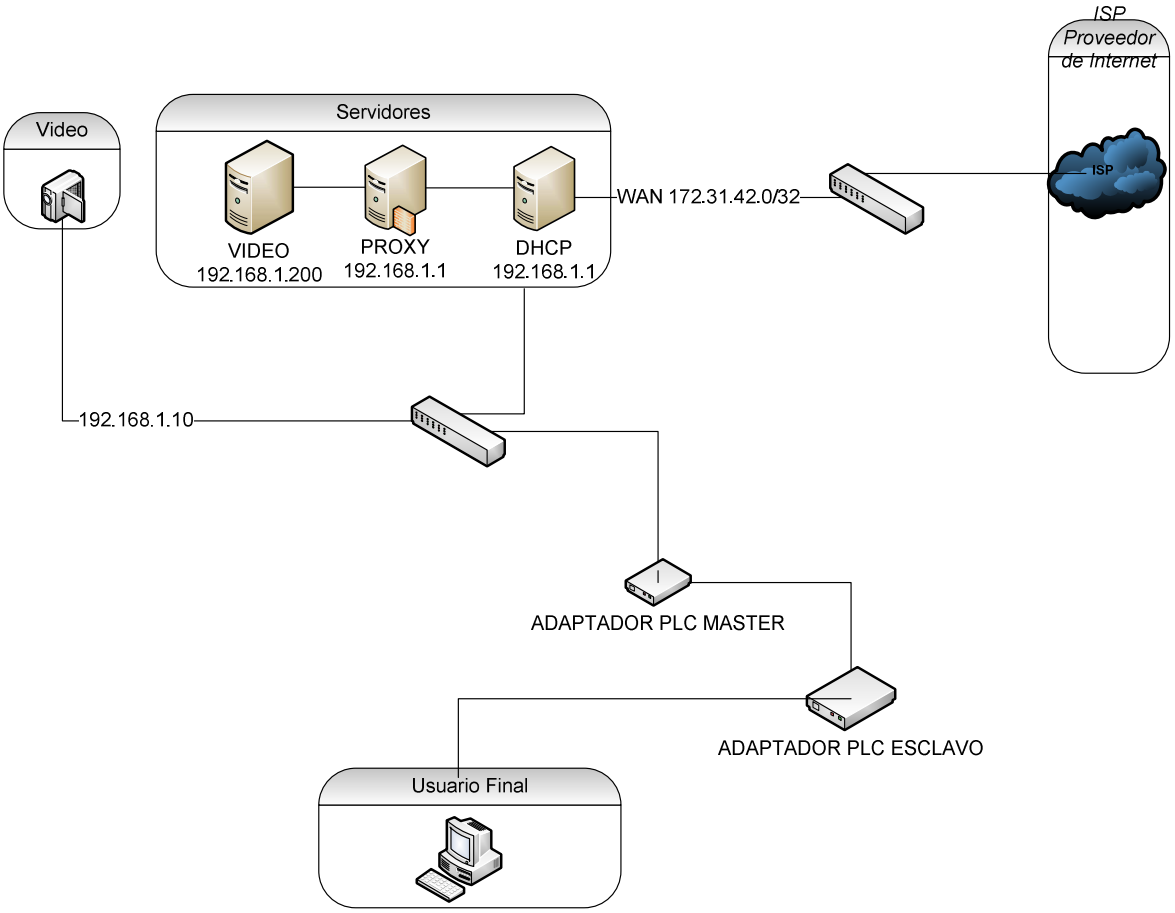


Figura 3.1.- Arquitectura de la Red Física

Elaborado por: Leonardo Medrano y Elizabeth Ramos

3.1.1 MÓDULO DE INTERNET

El principal objetivo de este módulo es brindar internet a todos los equipos de la sala.

Las medidas de seguridad que se han tomado en cuenta en el diseño, de acuerdo a la necesidad de la empresa (en este caso será el laboratorio ASI) será proporcionar restricciones de sitios pero no en tiempos de navegación, esto es debido a que el servicio de internet va a ser filtrado por el servidor proxy para todos los usuarios que no tengan permisos de administrador.

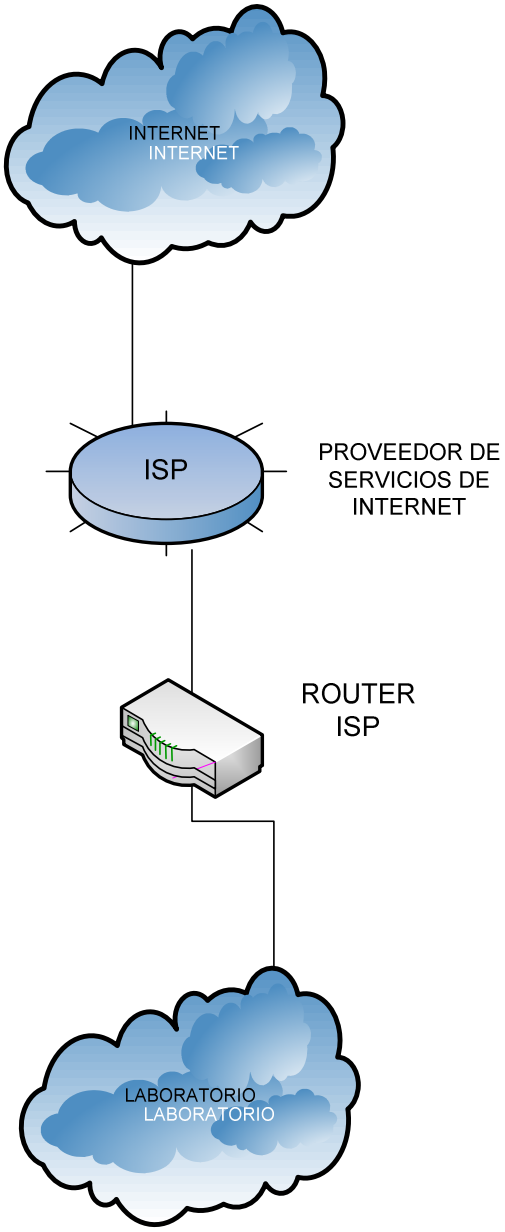


Figura 3.2.- Internet

Elaborado por: Leonardo Medrano y Elizabeth Ramos

Este diseño no consta de ningún sistema de backup para dar el servicio de internet, debido a que no es un sistema crítico dentro del laboratorio.

3.1.2 MÓDULO DE SERVIDORES

Este módulo provee servicios de aplicaciones a los usuarios finales de la red y facilita la gestión segura de todos los componentes usados en el Diseño Físico de

la Red. El servicio SNMP que nos provee el laboratorio a través de su servidor de internet permitirá a los administradores buscar, resolver problemas y supervisar el desempeño de la red.

Los componentes que se van a colocar en este módulo según las necesidades de este proyecto son: Servidor de Video Vigilancia, Servidor de DHCP y Servidor Proxy.

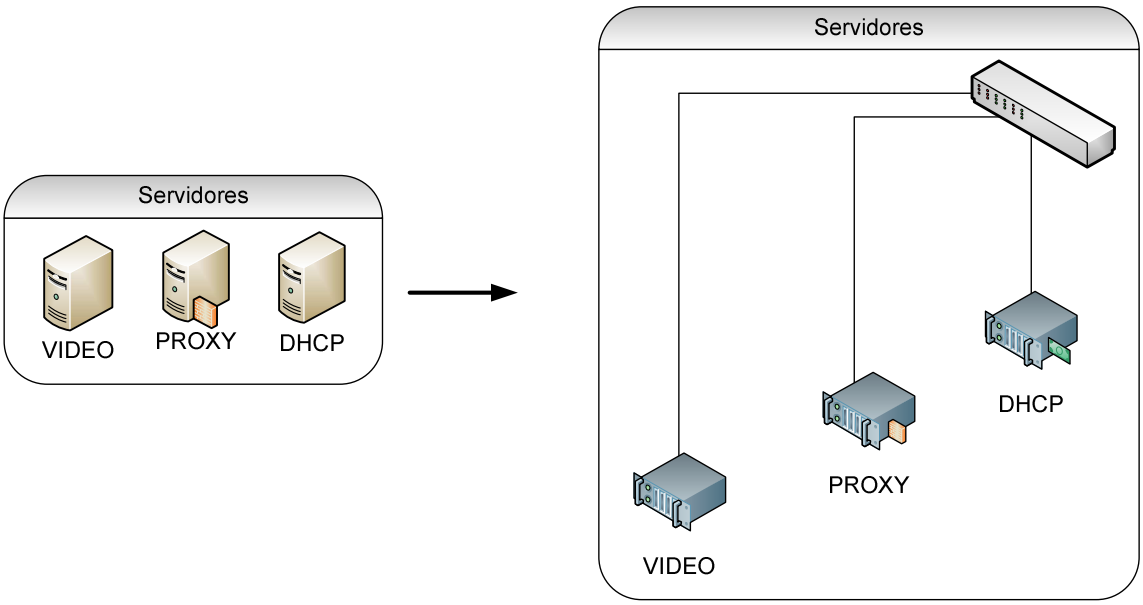


Figura 3.3.- Estructura Ethernet

Elaborado por: Leonardo Medrano y Elizabeth Ramos

Este módulo está conformado por los siguientes dispositivos que van ayudar al manejo y control de la red, brindando seguridad necesaria a los usuarios.

- ***Switch de capa 3.-*** *proporciona los servicios de capa 3 a los servidores e inspecciona los datos que cruzan el módulo de servidores con NIDS.*
- ***Servidor de Video vigilancia.-*** *se encarga de monitorear las cámaras IP por medio del software provisto por el equipo.*
- ***Servidor Proxy.-*** *se encarga de filtrar el acceso a ciertos sitios sin afectar los tiempos de navegación.*
- ***Servidor DHCP.-*** *proporciona direcciones dinámicas a los equipos que integran la estación de red BPL.*

3.1.3 MÓDULO DE RED BPL

En la red BPL, los adaptadores (máster y esclavo) PLC se enchufarán desde la red de media tensión a la red de bajo voltaje (tomacorriente) que se encuentra en el laboratorio ASI; a su vez los adaptadores PLC se conectarán al equipo computacional, logrando así la comunicación entre adaptador máster y esclavo.

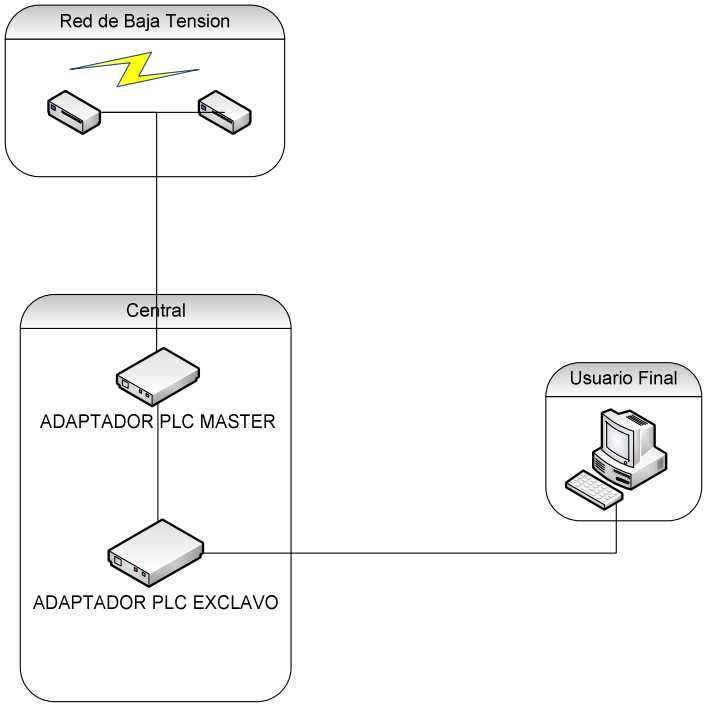


Figura 3.4.- Estructura PLC

Elaborado por: Leonardo Medrano y Elizabeth Ramos

3.2 EQUIPOS Y CARACTERÍSTICAS

A continuación se muestra un cuadro de detalles generales de los equipos candidatos a ser usados en el desarrollo de este proyecto, con el propósito de escoger el más óptimo e integrar en nuestro prototipo.

3.2.1 CÁMARAS IP

3.2.1.1 Network Cam

Cámara	Características	Precio
Network Cam	➢ Sistema operativo integrado - Elimina dependencia en servidores adicionales. ➢ Detección de movimiento integrada y reconocimiento de software. ➢ Notificación de e-mail instantánea. ➢ EEE-802.11b 2.4Ghz Wireless LAN ➢ Plug & Play - Instalación rápida y fácil en tres pasos ➢ Incluye Servidor Web ➢ Sensor de movimiento (Notificación vía e-mail y grabación de imágenes) ➢ Hasta 25 cuadros por segundo - PAL ➢ Hasta 100 usuarios simultáneos ➢ Acceso de usuarios protegido por nombre y contraseña ➢ Soporta también Sistema operativo Linux ➢ Firmware actualizable vía internet ➢ Soporta encriptación de 64 y 128 bits (WLAN) ➢ Resolución: 640 x 480, 320 x 240, 160 x 120 ➢ Registro múltiple - Soporta hasta 100 usuarios de forma simultánea.	➢ $80.00

	➢ Poderosa compresión de video - Acumula un mes de video en una PC típica ➢ Protocols soportado: TCP/IP, UDP, FTP, HTTP, PING (Option) POP3, SMTP, SNMP, MIBII, Proxy Agent, BOOTP, DHCP, DNS, Telnet, etc. ➢ 10 niveles de compresión de imagen JPEG. ➢ Video buffer de 384 Kbytes. ➢ Lentes CMOS 1/3". ➢ Serie de elementos 664 x 492 pixeles. ➢ IEEE 802.11b. ➢ Compensación de luz negra	

Tabla 3.2.1.1-1.- Especificaciones Técnicas Cámara Network Cam

3.2.1.2 Pan-Tilt-Zoom

Cámara	Características	Precio
Pan-Tilt-Zoom	➢ 10 niveles de compresión de imagen JPEG. ➢ Compresión: Alta 80:1, Baja 3:1 Hardware. ➢ Riesgo de CPU de 32 bits con mejora de red. ➢ Video buffer de 384 Kbytes. ➢ Memoria flash de 4 Mbytes. ➢ SDRAM de 8 Mbytes. ➢ Serial port for direct access. ➢ 12 V Power supply included. ➢ Output of 12 V to signal external devices, max 50 mA. ➢ 5.8 x 3.4 x 1.6" Sensor de imagen y especificacioón de lentes.	➢ $147.69

	➢ Lentes CMOS 1/3". ➢ 326,668 pixeles, 24 bits de color, salida YUV digital. ➢ Exposición automática / control de equilibrio blanco. ➢ Control de imagen, brillo, contraste, saturación, matiz Exposición, nitidez. ➢ Serie de elementos 664 x 492 pixeles. ➢ Tiempo de exposición electrónico: 1 / 30 s ~ 1 / 15734 . ➢ Compensación de luz negra. ➢ Lentes de montaje CS estándar reemplazables. ➢ Longitud focal de 6.0 mm, campo angular de vista de 54°, distancia de objetos 0.1 m al infinito. ➢ Lentes CMOS 1/3". ➢ Serie de elementos 664 x 492 pixeles. ➢ Compensación de luz negra.	

Tabla 3.2.1.2-2.- Especificaciones Técnicas Cámara Pan-Tilt-Zoom

3.2.1.3 Wi – fi

Cámara	Características	Precio
Wi – fi	➢ Plug & Play. ➢ Procesador integrado - No requiere de una PC dedicada. ➢ Apta para cualquier lugar con una conexión de Internet. ➢ Soporta hasta cinco usuarios viendo la cámara simultáneamente. ➢ Video en tiempo real hasta 30 cuadros por segundo.	➢ $239.99

	➢ Compresión de imagen basada en hardware de alta velocidad. ➢ Serial port for direct access. ➢ Incluye software fácil de utilizar para vista de 4 cámaras y grabación. ➢ Sistema operativo integrado. ➢ Conexión a una red en cualquier lugar, sin necesidad de un PC dedicado. ➢ Codificador JPEG & RISC. ➢ Sensor CMOS de 1/4", 300,000 píxeles. ➢ Lentes con enfoque manual, F=1.8. ➢ Puerto LAN 10/100 UTP RJ-45 l Soporta Windows 98/Me/XP/NT/2000 l Garantía de 99 años.	

T**abla 3.2.1.3-3.-** Especificaciones Técnicas Cámara Wi-Fi

La cámara a ser usada es **Network Cam** puesto que tiene mejores especificaciones a nivel técnico y de almacenamiento de usuarios, esta cámara nos brinda un mejor servicio a nivel de acceso.

3.2.2 ADAPTADORES PLC

3.2.2.1 Corinex

Adaptador	Características	Precio
CORINEX	➢ Interfaz rápida de Ethernet 10/100BaseT ➢ Filtro anti-ruido integrado de Powerline	➢ $200.00

	➢ Toma eléctrico integrado ➢ Transferencia de datos en la red powerline de hasta 200Mbps con alcance de 300 m. ➢ Protocolos de CSMA/CARP ➢ Puente Ethernet 802.1D integrado con árbol de protocolo optimizado ➢ Bridge Forwarding Table para 32 MAC Addresses ➢ 802.1Q VLAN & VLAN Optimizados ➢ VLAN Tagging en la fuente ➢ Poderosa encriptación DES/3DES (168 BIT) ➢ Tecnología OFDM con sistema de corrección de errores para un fuerte rendimiento bajo severas condiciones en la red eléctrica ➢ 8-niveles de colas de espera con prioridad programable ➢ Clasificación de prioridades según la etiqueta 802.1P, codificación IP (IPv4 o IPv6) o puerto de origen/destino ➢ Soporte optimizado para transmisión y tráfico de difusión múltiple ➢ Filtración MAC - pueden descartar estructuras de Ethernet que provengan de una dirección MAC no presente en la lista de direcciones MAC permitidas ➢ Administración (TR-069 o interfaz del web) ➢ IP Fijo o DHCP	

	➢ Conecta y Juega / Manual de configuración.	

Tabla 3.2.2.1-1.- Especificaciones Técnicas Adaptador Corinex

3.2.2.2 Panasonic

Adaptador	Características	Precio
PANASONIC HD-PLC	➢ Descripción: HD-PLC Adaptador Ethernet ➢ Fabricante: Panasonic ➢ Red: Ethernet - 10 Mbps Twisted Pair(10BaseT)Ethernet - 100 Mbps Two-Pair (100BaseTX) ➢ Adaptador de Red: Powerline Network Adapter ➢ Tipo de Producto: Powerline Network Adapter ➢ Tipo Sistema: PC ➢ Estándares de Conexión de Red Arquitectura de Red: Ethernet - 10 Mbps Twisted Pair (10BaseT), Ethernet - 100 Mbps Two-Pair (100BaseTX) ➢ Indicadores de Estado de Red ➢ Puertos Interface Connection: 1 x RJ-45 10/100Base-TX Network ➢ Dimensiones: 2.80" alto x 4.80" ancho x 1.60" profundidad ➢ Peso: 8.50 oz	➢ $150.00

Tabla 3.2.2.2-2.- Especificaciones Técnicas Adaptador Panasonic

3.2.2.3 Mitsubishi

Adaptador	Características	Precios
MITSUBISHI *3.2.2.*	➢ La memoria interna de la RAM puede alcanzar alta capacidad 64K ➢ Escala del control: 16~38 (contiene CC-LINK) ➢ En la función de localización interno es triaxial y 100khz (el transistor hecho salir) ➢ El lado izquierdo del área se puede conectar el adaptador y es fácil uso y de gran alcance.	➢ $100.00

Tabla 3.2.2.3-3.- Especificaciones Técnicas Adaptador Mitsubishi

El adaptador que se usara es **Panasonic HD-PLC** puesto que tiene mejores especificaciones a nivel técnico, es de fácil instalación y usabilidad. Así como también su precio conveniente.

CAPÍTULO IV. 4. IMPLEMENTACIÓN Y PRUEBA DEL PROTOTIPO.

Después de haber realizado el análisis de costo, el tamaño de empresa en el que se ubica el laboratorio, en éste capítulo se efectúa la implementación y prueba de las tecnologías BPL y Ethernet. Se trata a profundidad los servicios tales como DHCP, Proxy y Video Vigilancia de la red interna, con la finalidad de permitir el acceso a los recursos de video vigilancia a usuarios autorizados de la intranet, así como desde el internet mediante autentificación (cuentas), brindando de esta forma seguridad en la conectividad.

Los servicios DHCP y Proxy se los realiza en un mismo servidor, en este caso se ha instalado Centos 5.

La instalación, configuración de la Cámara IP y el servicio de Video Vigilancia es sobre Windows XP.

4.1 CONFIGURACIÓN DE LAS INTERFACES DE RED DEL SERVIDOR

Configuración de la tarjeta Eth0. Interfaz de red que permitirá tener acceso a internet.

1. Establecer la dirección IP en la tarjeta de red ***(172.31.42.183)***, máscara ***255.255.255.0,*** puerta de enlace ***172.31.4.1***

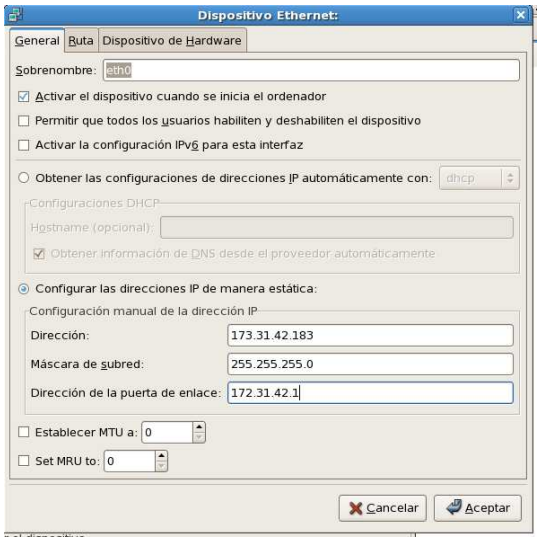


Figura 4.1.- Configuración de tarjeta de red eth0

2. Marcar la opción ***Activar el dispositivo cuando se inicia el ordenador***.
3. Hacer clic en ***Aceptar*** para guardar la configuración de la tarjeta.

Configuración de la tarjeta Eth1. Interfaz de red que estará configurada para la red interna.

1. Establecer la dirección IP en la tarjeta, en este caso ***(192.168.1.1)***, máscara ***255.255.255.0,*** puerta de enlace ***192.168.1.1***

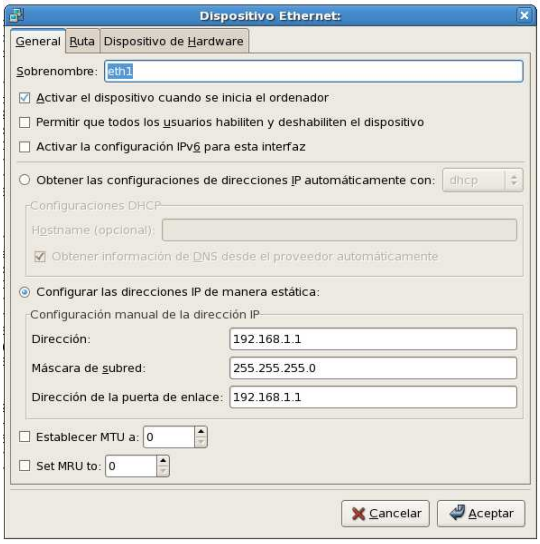


Figura 4.2.- Configuración de tarjeta de red eth1

2. Marcar la opción ***Activar el dispositivo cuando se inicia el ordenador***.
3. Hacer clic en ***Aceptar*** para guardar la configuración de la tarjeta.

Activación de las interfaces de red

1. Abrir una Terminal y escribir:

   #service network start.

2. Verificar que las tarjetas eth0 y eth1 se encuentre activadas. En el terminal digitamos *ipconfig* donde verificamos que las dos interfaces de red estén con la configuración definida.

4.2 INSTALACIÓN DEL SERVIDOR DHCP

Después de haber configurado las tarjetas de red se empieza a configurar el servicio DHCP.

Configuración del servicio

1. Abrir una nueva Terminal
2. Verificar si el paquete dhcp está instalado utilizando el comando

   #rpm –q dhcp

Si el paquete no se encuentra instalado se emplea el comando:

#yum –y install dhcp.

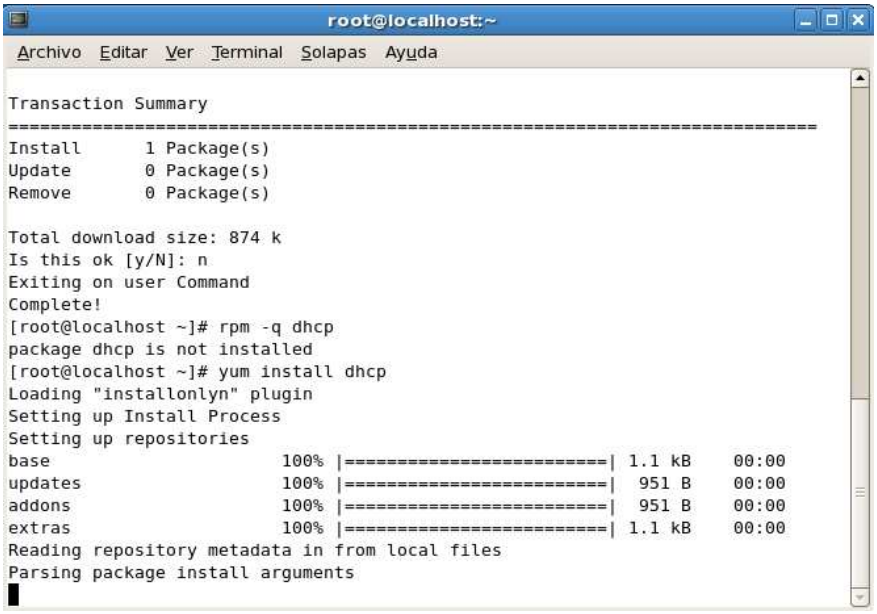


Figura 4.3.- Instalacion de servicio DHCP

3. Copiar el ejemplo de configuración del fichero /etc/dhcp/document
4. Editar el fichero **/etc/dhcp.conf**

   #vim /etc/dhcp.conf.
5. Cambiar los siguientes parámetros:

   subnet 192.168.1.0 netmask 255.255.255.0

   optiondomain-name-servers 172.31.4.2 <dominio LTI>

   range 192.168.1.100 192.168.1.200 <rango de dir ips>
6. Guardar los cambios en el fichero y salir del editor con el comando ***:wq***
7. Inicializar el servicio DHCP mediante el comando:

   #service dhcp start.

8. Añadir el servicio al arranque del sistema:

   #chkconfig dhcpd on.

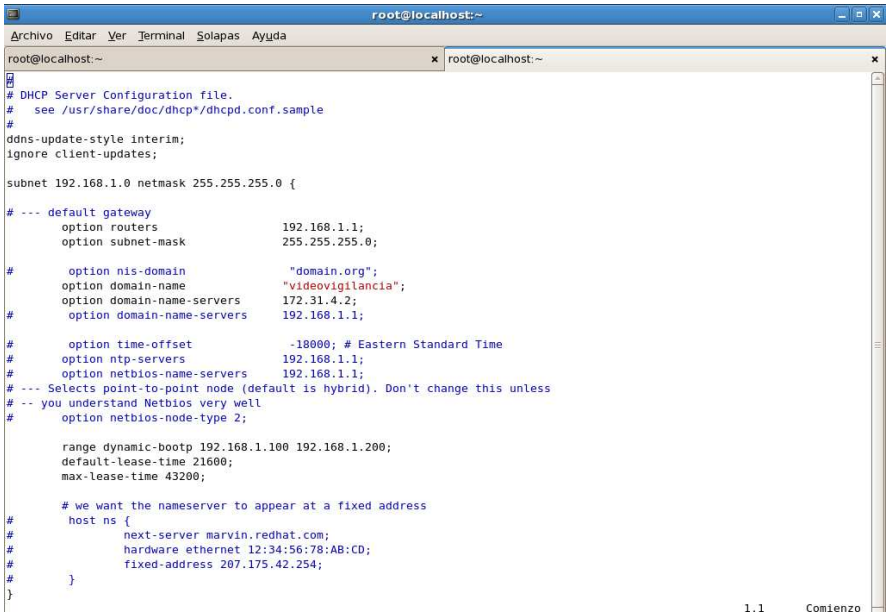


Figura 4.4.- Configuración del fichero dhcp.conf

4.3 SERVIDOR SQUID PROXY

Instalación del servicio

1. Abrir una nueva Terminal
2. Verificar si el paquete squid está instalado utilizando el comando

   #rpm –q squid

Si el paquete no se encuentra instalado se emplea el comando:

#yum –y install squid

3. Editar el fichero ***/etc/squid/squid.conf*** mediante el editor vim. El comando es**: *vim /etc/squid/squid.conf.***
4. Modificar los siguientes parámetros:

   http_port:3128 *< Descomentar>*

   cache_mem 16MB *<Cambiar de 8MB a 16MB>*

   acl video src 192.168.1.0/255.255.255.0

   acl negado url regex “/etc/squid/negado.txt” <insertar nuevos acl>

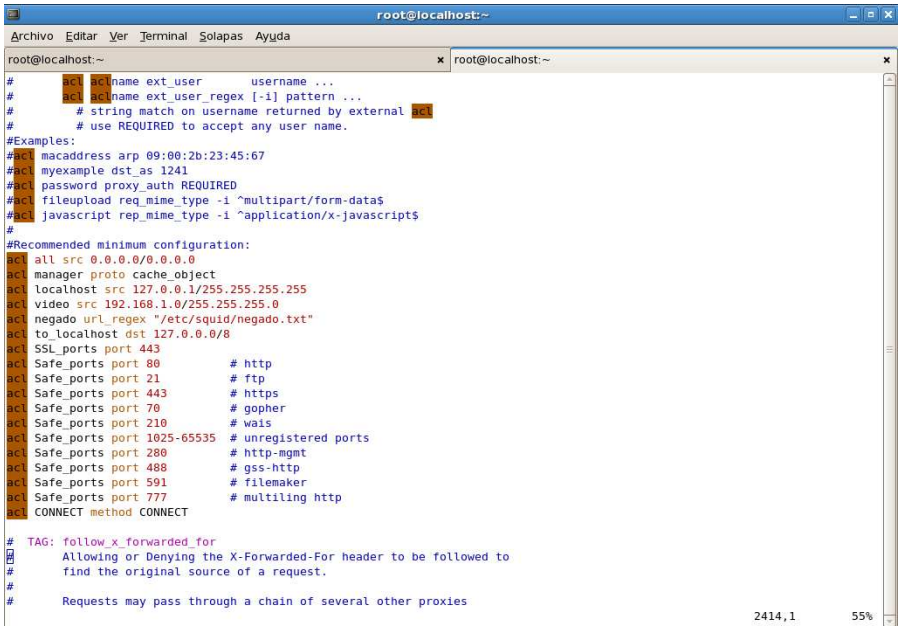


Figura 4.5.- Configuración de archivo squid.conf

http_access allow video

http_access deny negado

*<permitir o denegar el acceso basado en las lista de acceso **acl**>.*

En los permisos se debe ir de lo general a lo específico para hacer uso de las políticas.

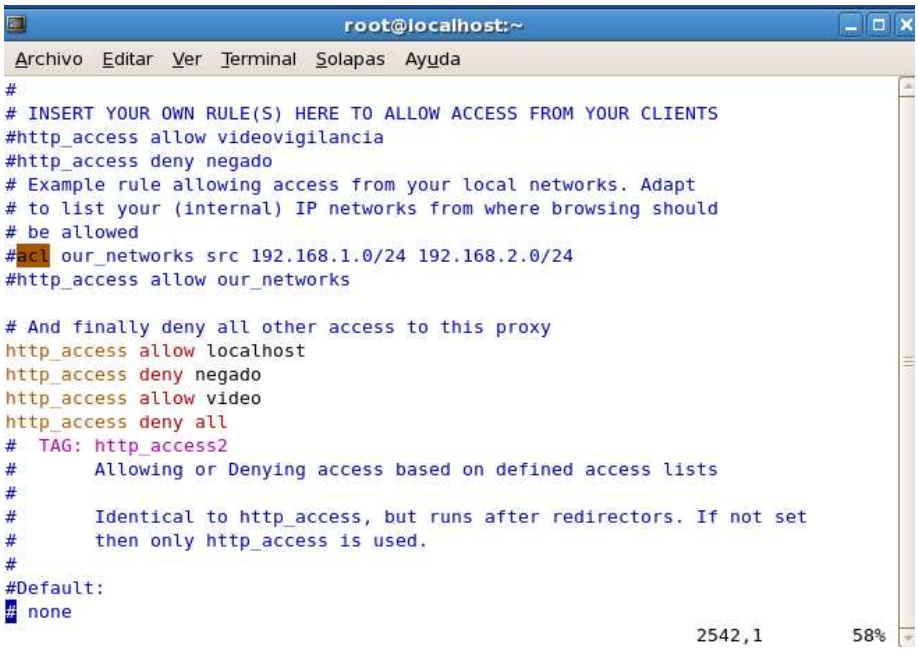


Figura 4.6.- Configuración de archivo squid.conf sección http_access

5. Guardar los cambios **:wq**

6. Inicializar el servicio SQUID mediante el comando:

   #service squid start.

7. Añadir el servicio al arranque del sistema:

   #chkconfig squid on

4.4 SERVIDOR DE VIDEOVIGILANCIA

Para implementar un servidor de video vigilancia se debe considerar los siguientes aspectos:

	Descripción	**Tamaño / Programa**
Tamaño en disco duro	Mejor rendimiento y gran capacidad de almacenamiento de imágenes y video.	Al servidor se le ha asignado al 40GB.
Administración de cámara de video	Mejor administración. Local y Web	Video Viewer es fácil de administrar y es el software que utiliza la Cámara IP (Cámara Network).
***Antivirus**	Protección para prevenir ataques internos externos.	Para este servidor se utilizó, Avast Internet Security 5.
Tarjetas de Red	Para administrar la cámara IP y el servidor Video Vigilancia	Dos tarjetas de red

Tabla 4.4-1.- Aspectos generales para implementar un servidor de video vigilancia

4.4.1 CONFIGURACIÓN DE LA CAMARA IP.

4.4.1.1 Configuración inicial de la Cámara IP

Para la configuración basada en web del equipo se necesita lo siguiente:

- Navegador sea Internet Explorer, o Firefox
- Quick Time la última versión,

- Adobe Flash Player 10.1.2.

Para la integración física de la Cámara IP a la red se debe usar un concentrador (switch) ya la red del LTI.

4.4.1.2 Configuración mediante la conexión de la cámara a la computadora

La administración gráfica con ***Video Viewer***, permite realizar una administración fácil e intuitiva en la configuracion de la Camara IP y el servidor de Video Vigilancia.

Para realizar la configuración es necesario colocar una dirección IP que se encuentre dentro de la subred y sea una dirección IP reservada (fuera del rango de las direcciones asignadas por el servidor DHCP).

Conexión de la cámara IP a la computadora

1. Hacer clic en ***Inicio***, escoger ***Panel de control***
1. Pulsar doble clic sobre ***Conexiones de red***.
2. Escoger la tarjeta de red.
3. Hacer clic derecho sobre la tarjeta y seleccionar ***Propiedades***
4. Escoger ***Protocolo TCP/IP >> Propiedades***
5. Marcar ***Usar la siguiente dirección IP***

Dirección IP:	192.168.1.10
Máscara de subred	255.255.255.0
Puerta de enlace predeterminada:	192168.1.1

6. Instalar el programa Video Viewer, ver anexo.
7. Abrir el programa Video Viewer
8. Agregar la direccion IP de la camara utilizada, a la lista de cámaras.

   IP: 192.168.1.10 Puerto 80
9. Hacer doble clic en el visor izquierdo, para conectar la camara.

Figura 4.7.- Configuración de Cámara IP

4.4.2 CONFIGURACIÓN DEL SERVIDOR DE VIDEO VIGILANCIA.

Después de haber configurado la Cámara IP, se procede a realizar la configuración del servidor de Video Vigilancia.

1. Instalar el programa ***Video Viewer***
2. Abrir el programa ***Video Viewer***
3. Seleccionar la opción  ***Control miscelaneo***, hacer clic sobre  ***configuracion de servidor de video vigilancia***.

Figura 4.8.- Configuración de Servidor de video vigilancia.

Al seleccionar esta opción se desplegará un cuadro informativo, con la siguiente información:

General: Información general de la cámara IP

- Ingresar el nombre de la cámar IP

  TITULO: *Camera1*

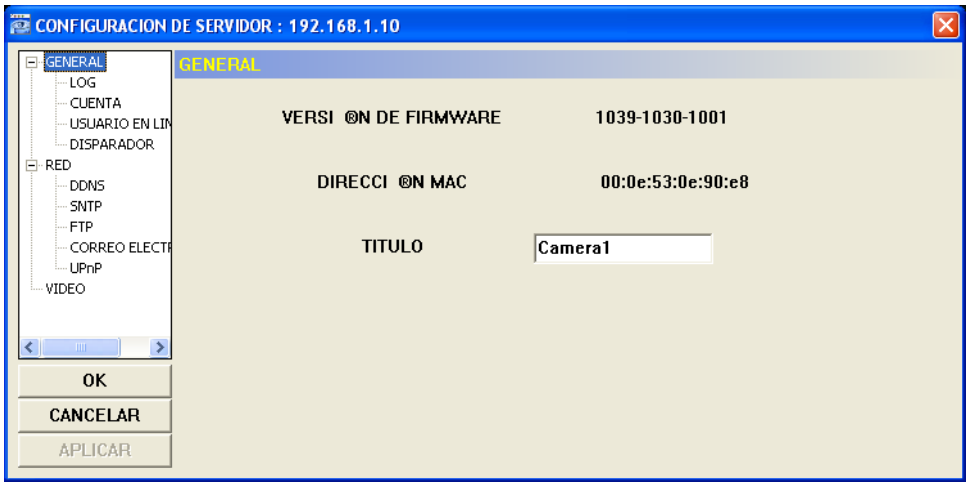


Figura 4.9.- Cuadro de descripción de la versión de la cámara IP.

- Visualizar los LOGS o registro de sucesos ocurridos y acciones realizadas en el servidor de videovigilancia.

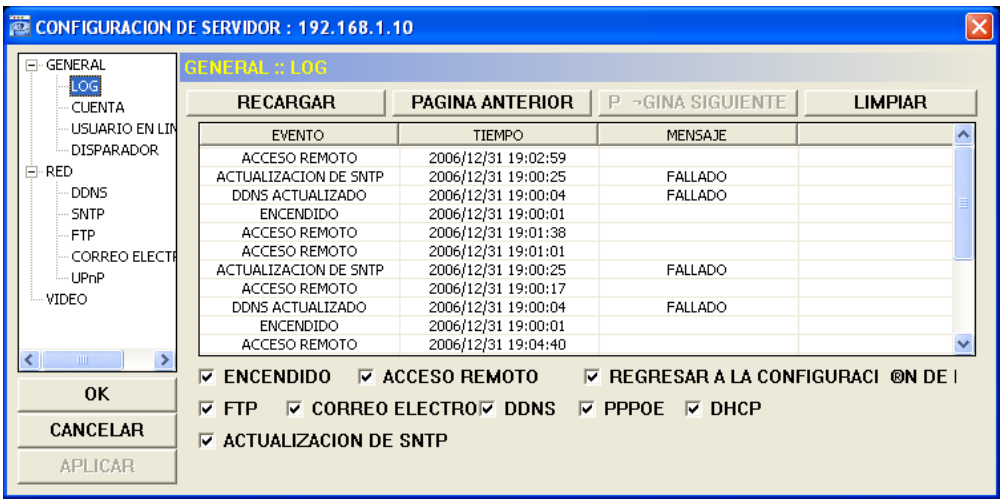


Figura 4.10.- Registro de acciones realizadas en el Servidor de Video vigilancia.

- Cuenta. Permite crear cuentas para uso y administración de la cámara IP. Para la creación de cuentas de usuario hay que considerar los roles que los usuarios desempeñaran y en base a esto otorgar los permisos o restricciones necesarios.

Crear usuarios para administrar la Cámara IP:

1. Hacer clic en ***Nuevo.***
2. Ingresar los siguientes datos:

   Nombre de usuario: Eli

   Contraseña: **********

   Nivel de usuario: *Supervisor*

   **Tiempo de conexión. (Este campo es opcional)*

3. Hacer clic en ***Aplicar***, visualizar la tabla con el nuevo usuario creado.

Figura 4.11.- Creación de usuarios para el uso de la cámara IP.

- Usuarios en Línea, permite observar los usuarios que se encuentran conectados a la cámara IP.

Figura 4.12.- Lista de usuarios conectados a la cámara IP**.**

- Disparador o activacion de disparador de cámara IP, graba el movimiento de una manera automatica en una zona previamente determinada, del

lugar donde se esta filmando. En este caso se ha desactivado.

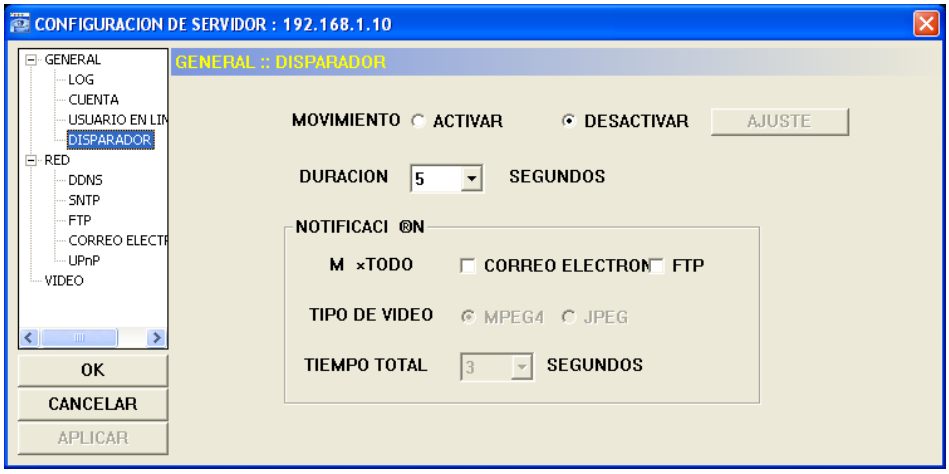


Figura 4.13.- Configuración de activación de disparador de la cámara IP**.**

Red: Configuración de la red

- DDNS, configuración de DNS

  Servidor DNS 1: 172.31.4.2

  nombre de usuario, contraseña, dominio y nombre del sistema, <mayor seguridad>

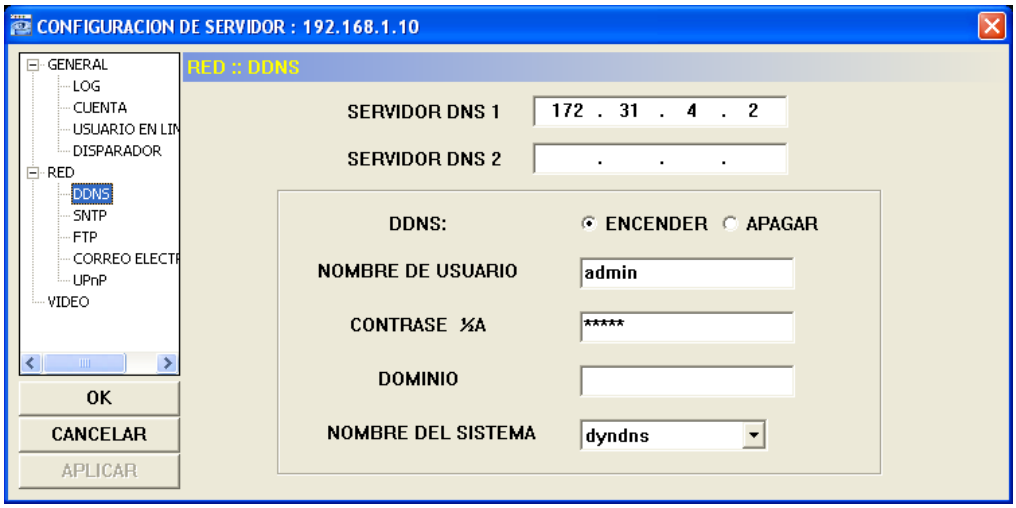


Figura 4.14.- Configuración de la red de la cámara IP.

- SNTP, sincroniza el tiempo del servidor, segun huso horario del pais.

  GMT: (GMT-05:00) BOGOTA, Lima, Quito

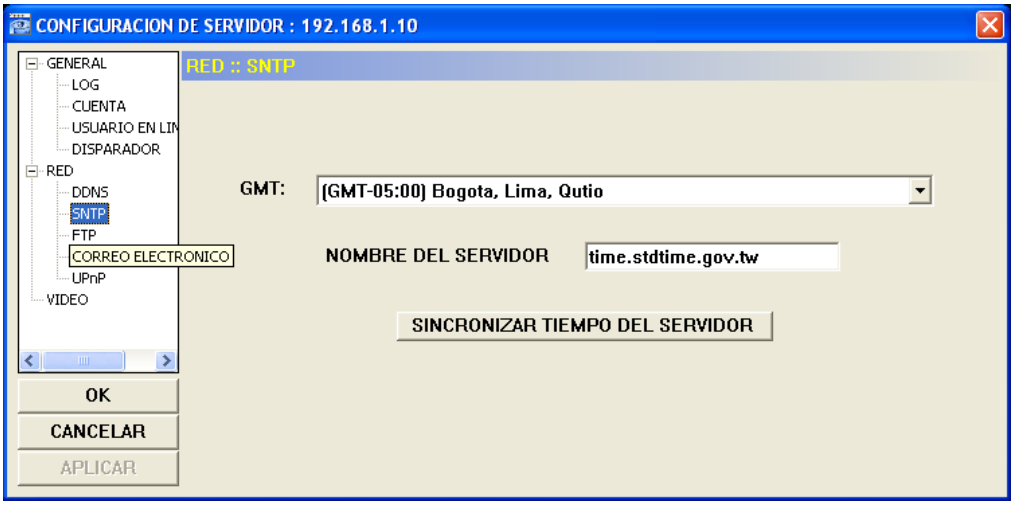


Figura 4.15.- Configuración de uso horario de la cámara IP.

- FTP, permite al usuario del equipo subir los videos y fotografías al servidor de videovigilancia, en este caso no se utilizara.

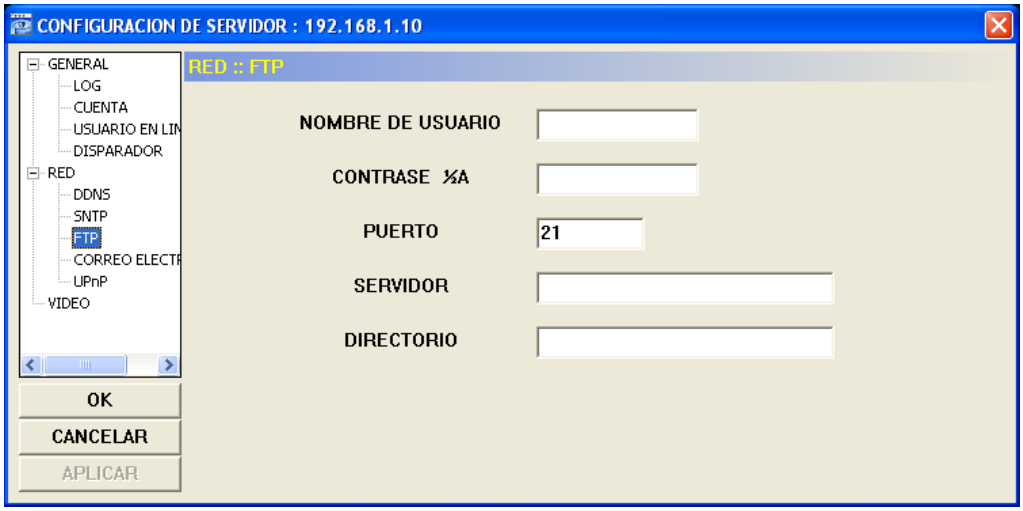


Figura 4.16.- Configuración de Servicio FTP.

- Correo electronico, para envio de video y fotografías a traves del servidor de videovigilancia. Permite enviar al correo electrónico de un usuario los videos y fotografias tomadas automaticamente. No se utilizara está opción.

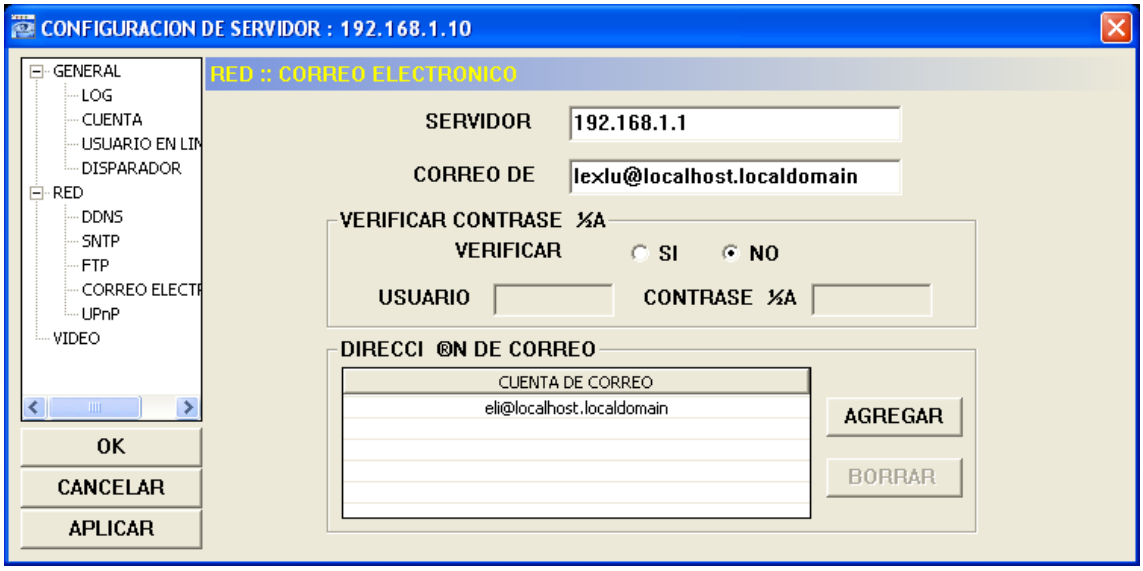


Figura 4.17.- Configuración de correo electrónico para el usuario receptor.

Video: Configuración del formato y calidad de Video.

Formato de la imagen: *MPEG: VGA* *ALTO*

Formato de stream: *MPEG-4*

Velocidad en Frame: *COMPLETO*

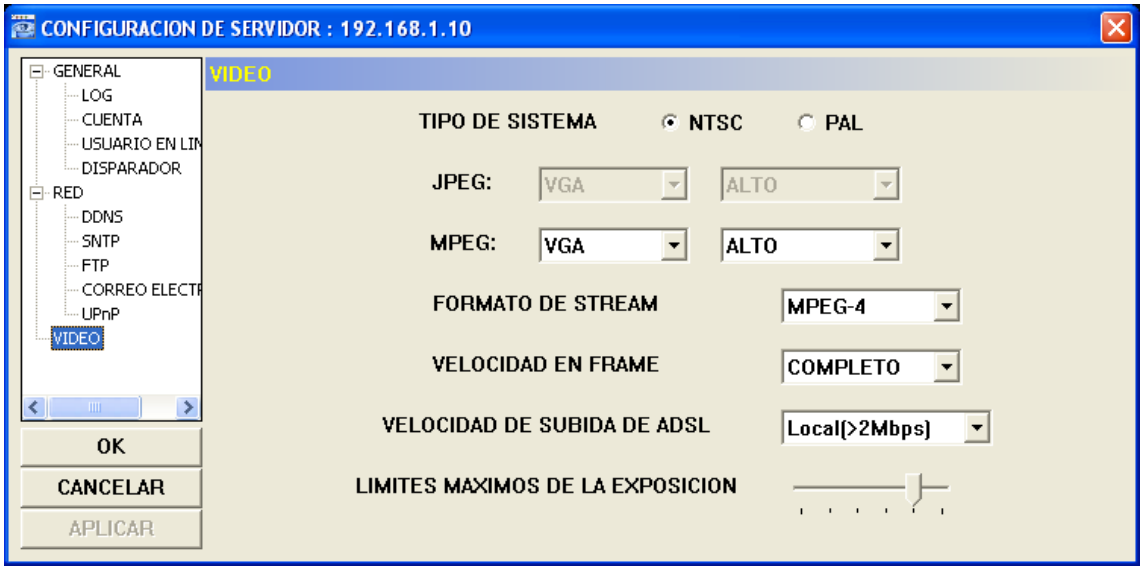


Figura 4.18.- Configuración de calidad de video**.**

4.5 CONEXIÓN DE RED ETHERNET Y RED BPL

Una vez terminada la configuración de los servidores que forman una parte importante en la conexión de la red, se procede a conectar los equipos, para

realizar las respectivas pruebas y comprobar así la fusión entre las tecnologías BPL y Ethernet.

4.5.1 ELEMENTOS QUE INTERVIENEN EN LA RED ETHERNET Y BPL.

Según la Figura 3.1 del Diseño Físico de la red propuesto anteriormente, para una mejor comprensión se lo ha segmentado de la siguiente manera:

Red Ethernet

- ISP: la red global del laboratorio ASI.
- Switchs, utilizando en:

  Tarjeta de red eth0 para la conexión de internet (Squid/Proxy).

  Administración de la cámara IP vía Web en la subred 192.168.1.0.
- Servidores DHCP, Proxy, Video.
- Cables de red directos

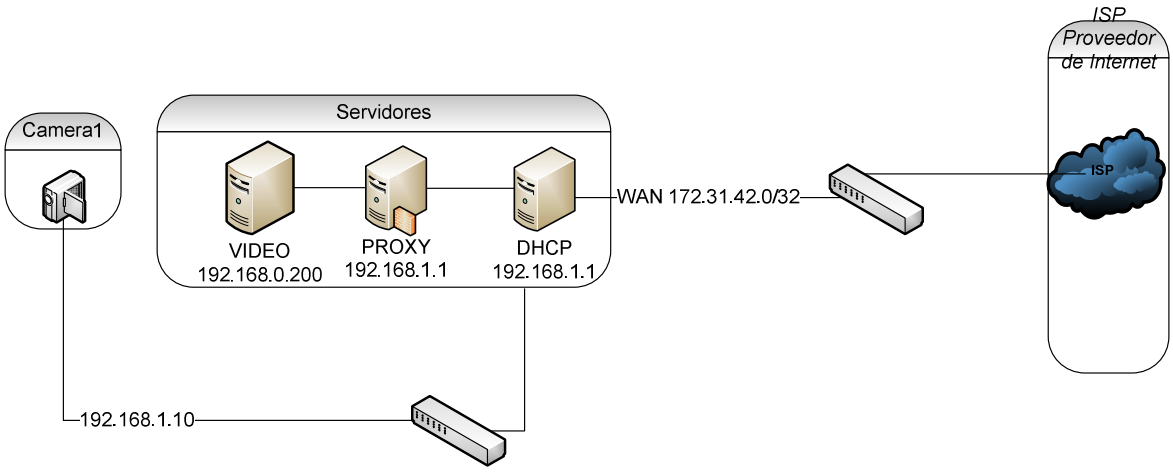


Figura 4.19.- Segmento de red Ethernet**.**

Red BPL

- Switch, utilizando en:

  Conexión desde el servidor DHCP hacia los adaptadores PLC.
- Adaptadores PLC: máster y esclavo, Figura 4.22 que transmiten los servicios de video vigilancia e internet a cada uno de los usuarios BPL
- Energía eléctrica

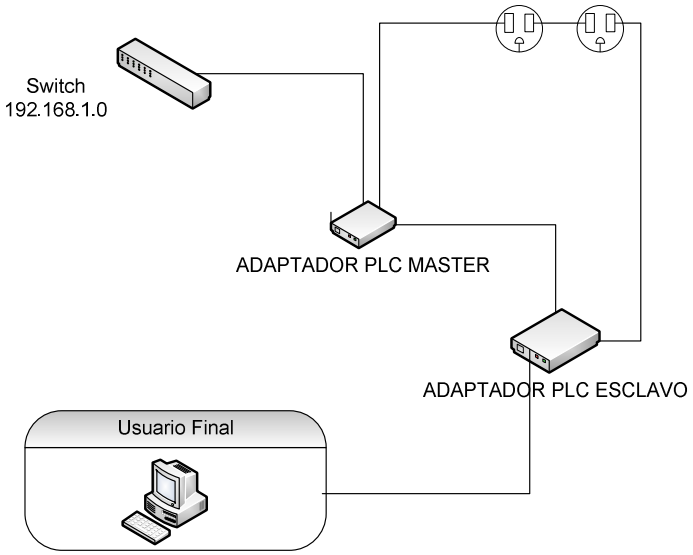


Figura 4.20.- Segmento de red BPL**.**

Conexión de los adaptadores PLC

Máster

1. Conectar un cable directo desde el switch hacia el puerto ethernet del adapatador master.
2. Enchufar el cable de alimentación de energía del adaptador máster en un toma corriente.

Esclavo

3. Conectar un cable directo desde el la tarjeta de red de la computadora hacia el puerto ethernet del adapatador esclavo
4. Enchufar el cable de alimentación de energía del adaptador esclavo en un toma corriente.

Ver anexos 1,2,3 para mayor informacion sobre la conexión de los adaptadores.

4.5.2 USUARIOS DE LA RED ETHERNET Y BPL

Configuración de los servicios en un cliente Windows XP.

Servicio DHCP

1. Hacer clic en ***Inicio***, escoger ***Panel de control***
2. Pulsar doble clic sobre ***Conexiones de red***.
3. Escoger la tarjeta de red.

4. Hacer clic derecho sobre la tarjeta y seleccionar ***Propiedades***
5. Escoger ***Protocolo TCP/IP.***
6. Marcar ***Obtener una dirección de IP automáticamente.***
7. Abrir una terminal de Windows a través del comando ***cmd.***
8. Ejecutar el comando ***ipconfig/release***, para reiniciar la dirección IP a 0.0.0.0.
9. Ejecutar el comando ***ipconfig/renew,*** para que el servidor le una dirección IP.

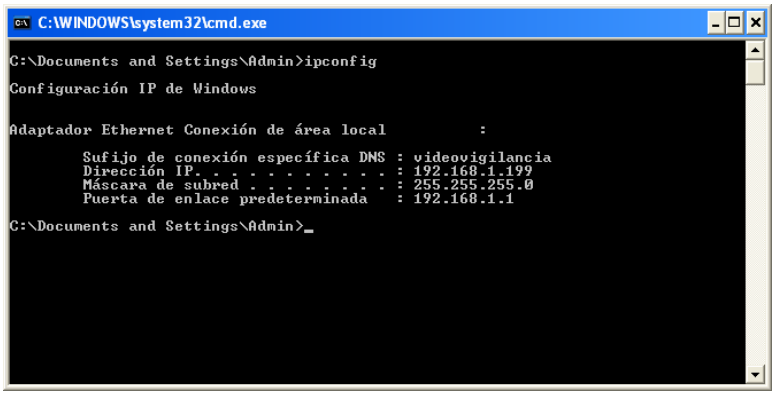


Figura 4.21.- Dirección IP del cliente que recibió el servicio DHCP.

SQUID PROXY.

1. Abrir un navegador de su preferencia este caso Mozilla Firefox 3.0.
2. Escoger la pestaña ***Herramientas*** de la barra de herramientas.
3. Seleccionar ***Opciones*** >> ***Avanzado*** >>***Red*** >> ***Configuración.***
4. Ingresar/ marcar los siguientes datos:

   Proxy HTTP 192.168.1.1 Puerto 3128

   Usar el mismo proxy para todo.
5. Hacer clic en ***Aceptar*** para guardar los cambios

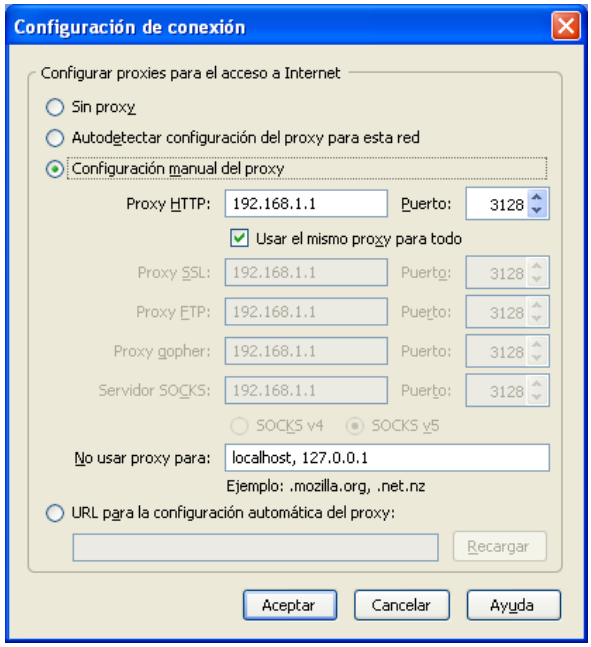


Figura 4.22.- Configuración manual del proxy.

6. Abrir el navegador para comprobar que tiene acceso a internet

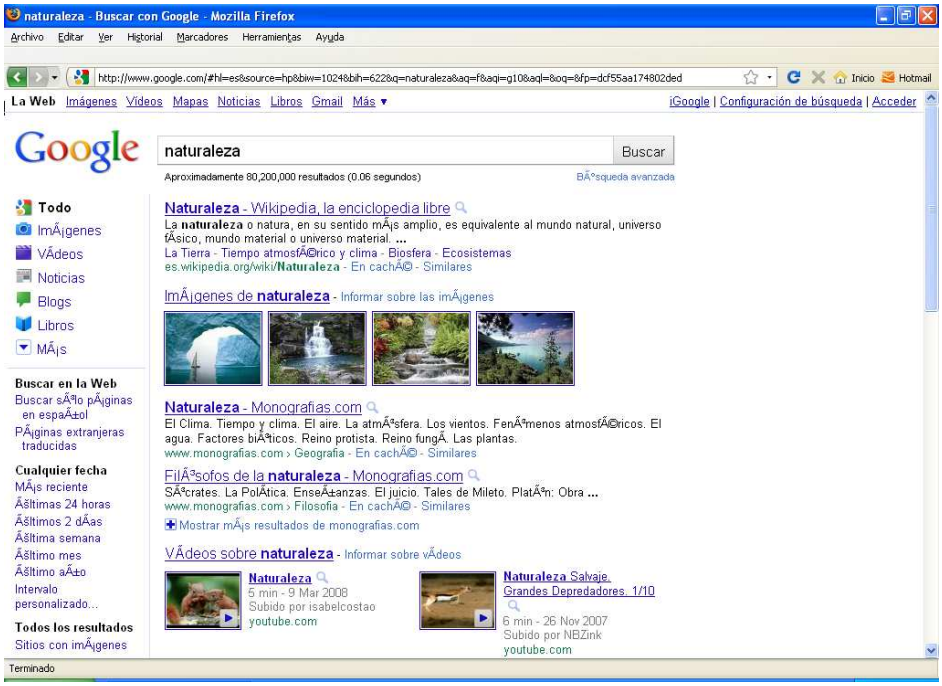


Figura 4.23.- Ingresando a internet

7. Para verificar que el servidor proxy funciona se digita en nuestro navegador una de las palabras que están negadas en el archivo de

configuración.

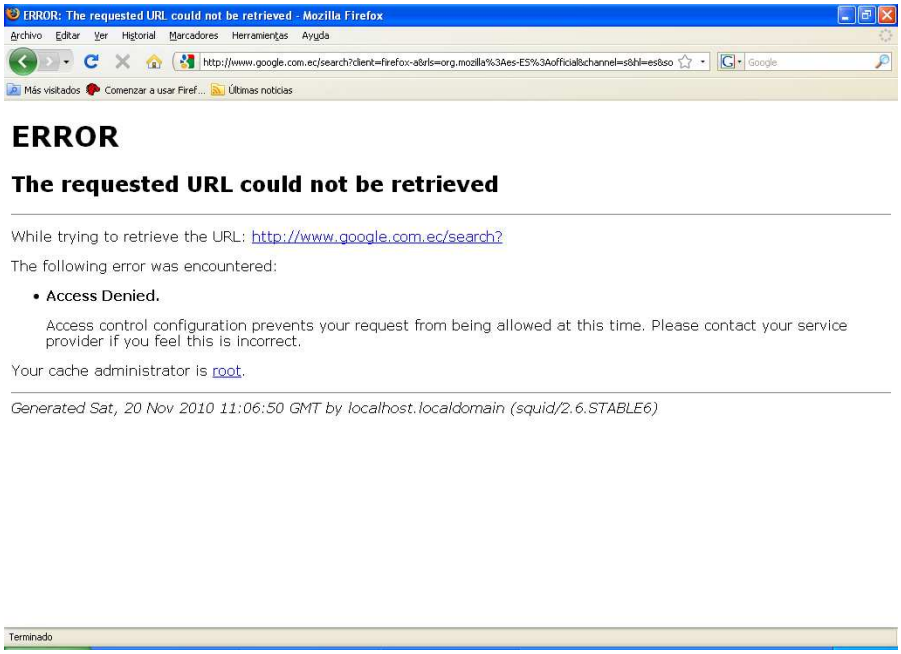


Figura 4.24.- Ingresando a internet

4.6 PRUEBAS DE CONEXIÓN ENTRE LAS REDES ETHERNET Y BPL

Para realizar las pruebas de conexión se dividirá a cada usuario según la red.

4.6.1 PRUEBA DE CONEXIÓN COMPARTIENDO UN ARCHIVO

Usuario Ethernet

- Obtener una dirección IP.

Dirección IP 192.168.1.125

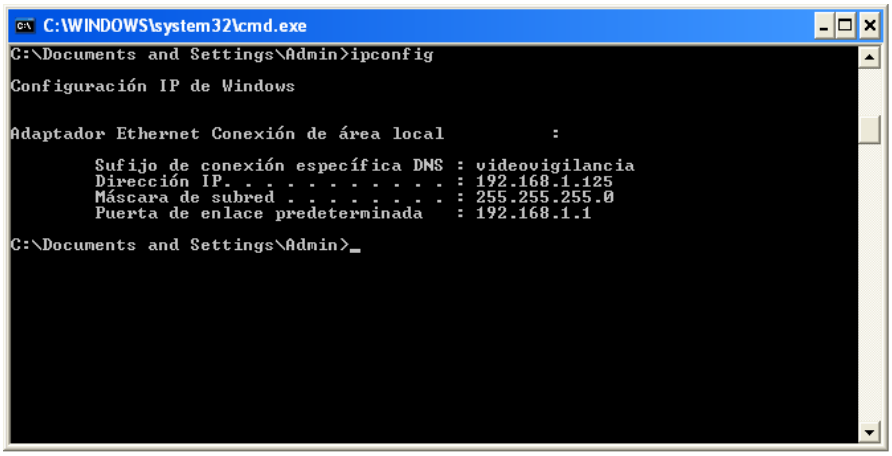


Figura 4.25.- Dirección IP, usuario Ethernet

- Compartir una carpeta con el usuario BPL.

  C:\prueba_plc

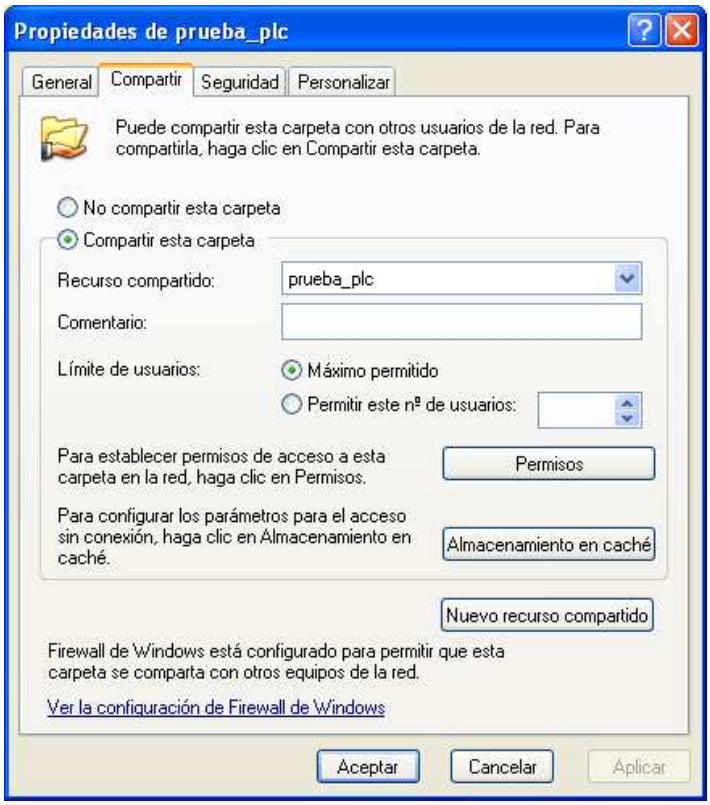


Figura 4.26.- Compartir un archivo con el usuario BPL

- Asignar los permisos necesarios para que pueda leer y modificar el archivo.

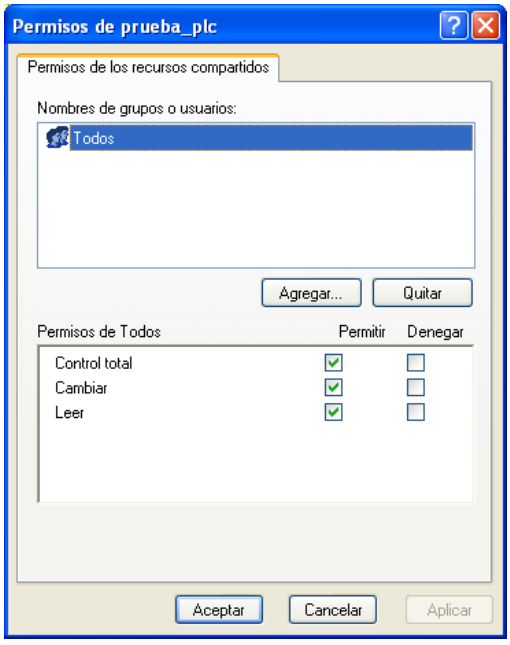


Figura 4.27.- Asignar permisos al archivo.

- Colocar un archivo en la carpeta compartida

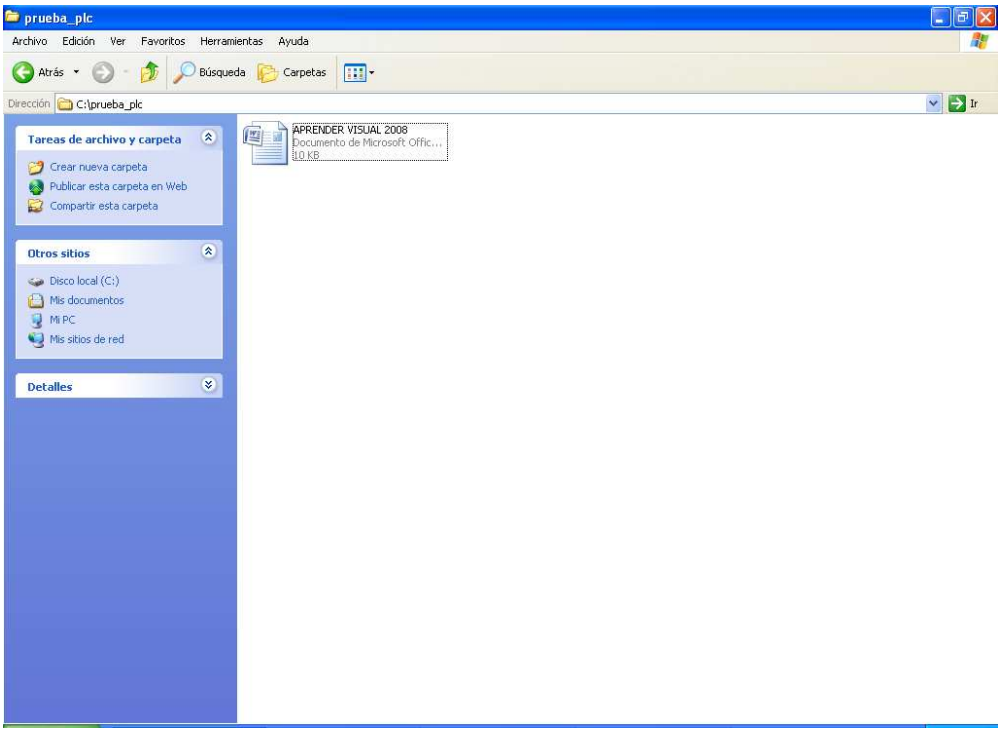


Figura 4.28.- Colocar un documento.

- Observar la carpeta compartida.

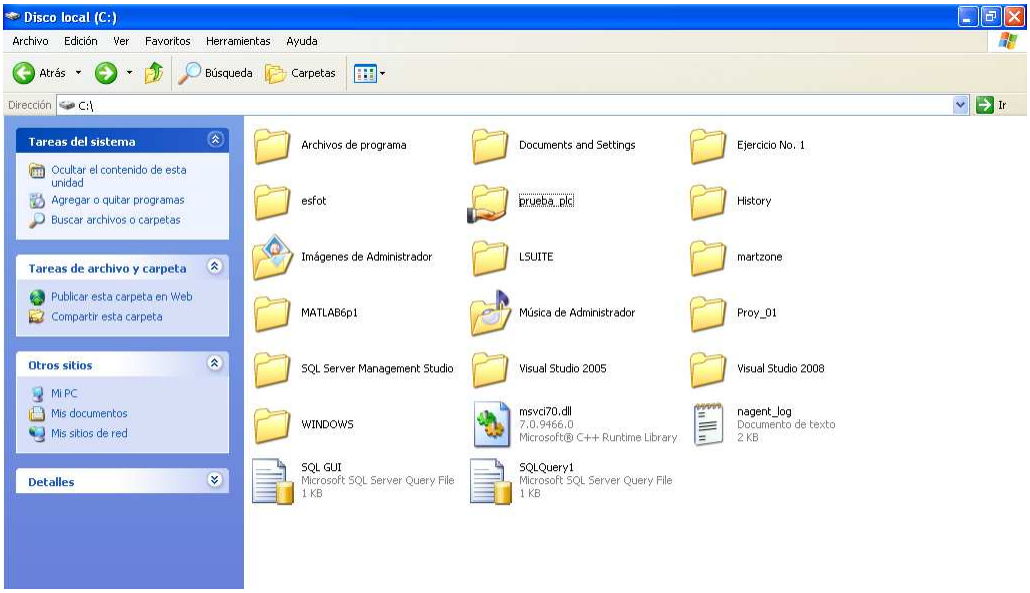


Figura 4.29.- Carpeta compartida.

Usuario BPL

- Obtener una dirección IP.

Direccion IP: 192.168.1.198

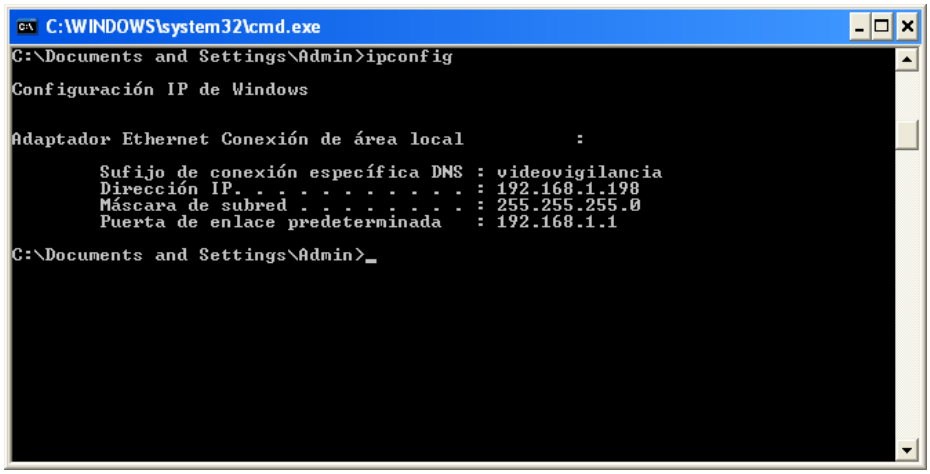


Figura 4.30.- Dirección IP, usuario BPL

- Acceso al equipo de usuario Ethernet

Digitar la dirección IP del usuario Ethernet

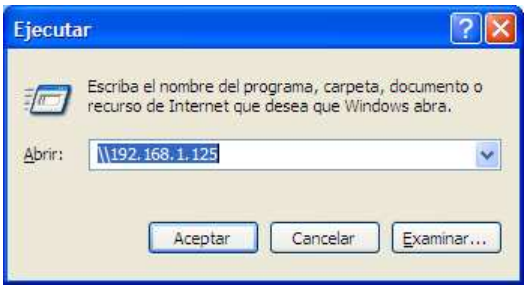


Figura 4.31.- Acceso usuario Ethernet

- Observar los documentos compartidos

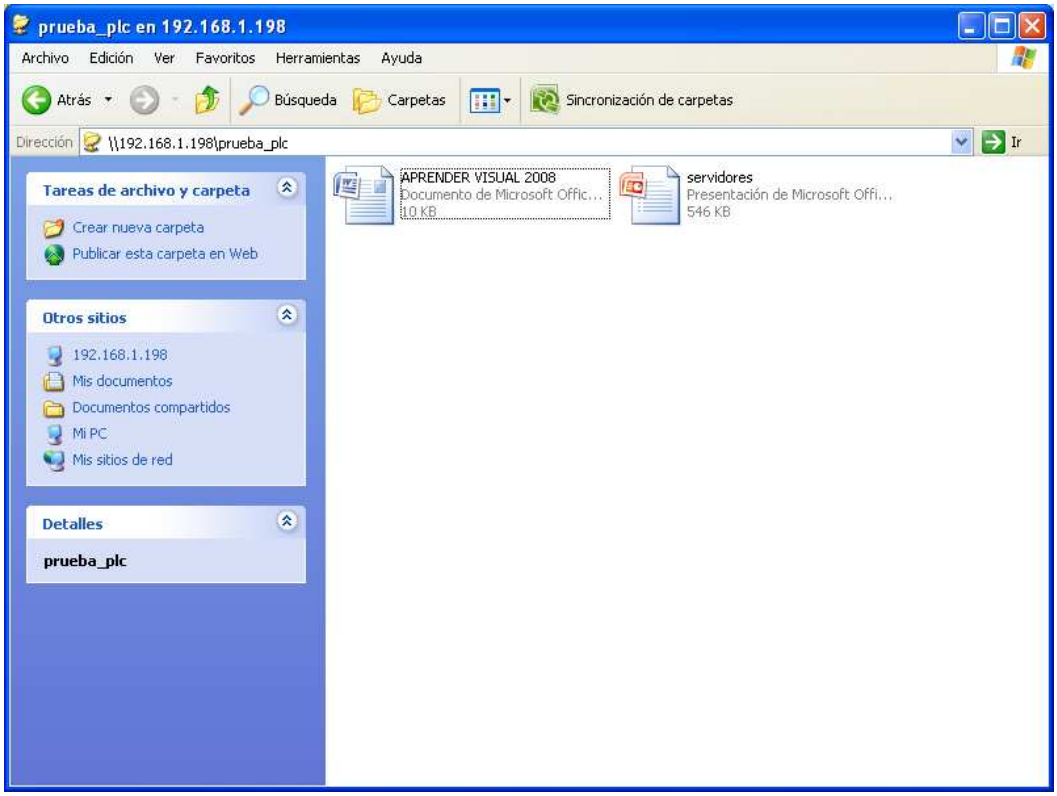


Figura 4.32.- Archivos compartidos desde la red Ethernet

4.6.2 PRUEBA DE CONEXIÓN, CONFIGURANDO VIA WEB EL SERVIDOR DE VIDEOVIGILANCIA

Usuario BPL

- Abrir un navegador, en este caso se utiliza Mozilla Firefox.
- Digitar la dirección IP del servidor de Video Vigilancia.

  http://192.168.1.10

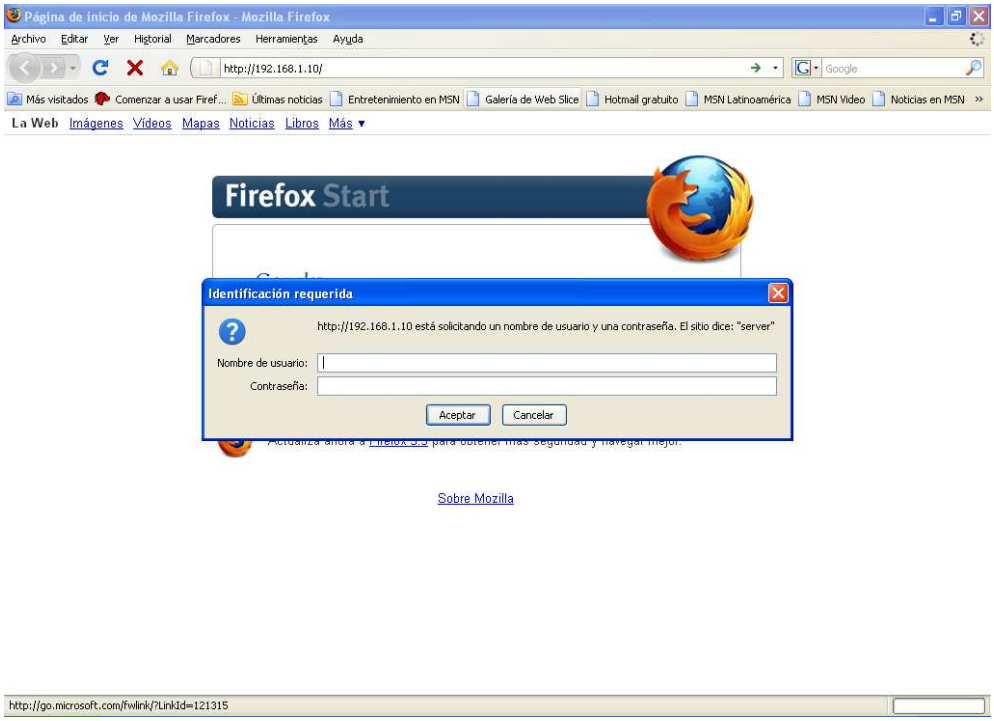


Figura 4.33.- Autentificación de usuario.

- Ingresar el nombre y contraseña para autentificarse, <usuario previamente creado sección 4.3.2>

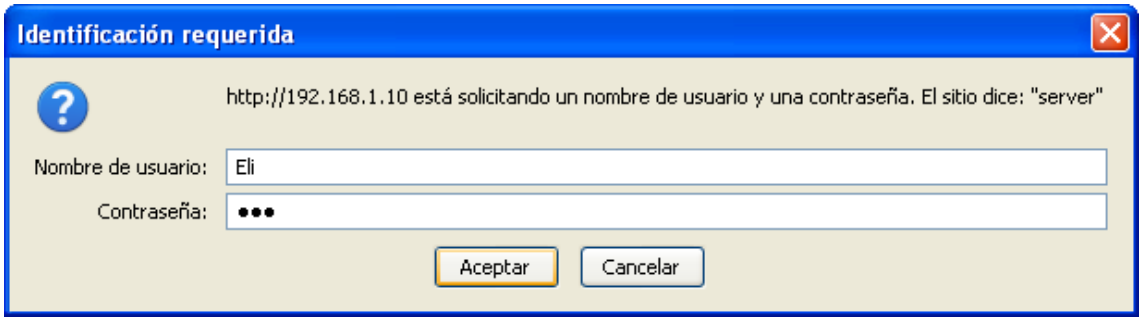


Figura 4.34.- Usuario creado servidor Video Vigilancia.

Según los permisos otorgados al usuario se podrá acceder a la configuración del servidor.

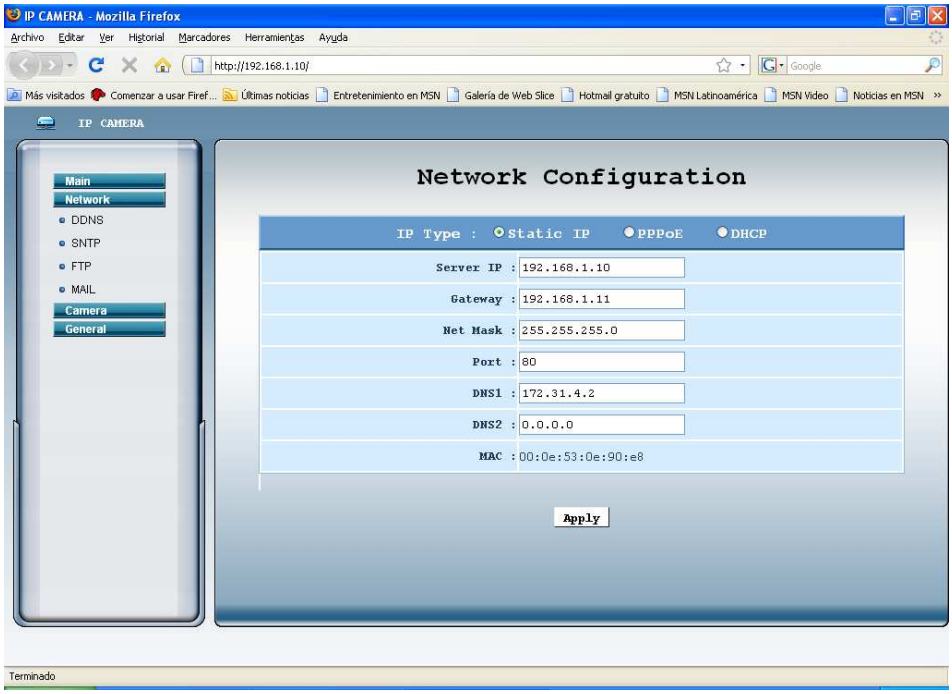


Figura 4.35.- Acceso al servidor a través del usuario Eli.

CAPÍTULO V. **5.CONCLUSIONES Y RECOMENDACIONES**

5.1 CONCLUSIONES

- De acuerdo a lo analizado en capítulos anteriores se puede decir que existe factibilidad técnica para la futura implementación del proyecto BPL en el caso de estudio, debido a que se ha identificado la mejor opción de topología y los equipos necesarios están disponibles en el mercado.

- La tecnología PLC ofrece:
  - ✓ Simplicidad. Ubicuidad de la red eléctrica
  - ✓ Progresividad. Se instalan sólo los equipos necesarios
  - ✓ Movilidad.
  - ✓ Ausencia de obras
  - ✓ Ahorro y rapidez del despliegue
  - ✓ Coexistencia con otras tecnologías

- El PLC es una buena tecnología tanto para usuarios domésticos como para usuarios profesionales por ser de mayor calidad técnica (fácil despliegue, velocidades elevadas, costo reducido) en relación a las existentes, sin embargo necesita una nueva y mejor política de marketing para poder implantarse a un mejor nivel. Es cierto que en la actualidad muchos usuarios ya conocen de su existencia pero debido a que la red Ethernet aun está lejos del máximo de velocidades a las que puede llegar, no se está dejando espacio para esta nueva tecnología.

- La tecnología PLC es una buena competencia en el sector de las telecomunicaciones y en un plazo no muy lejano, podrán ocupar una cuota de mercado muy grande debido a los grandes servicios que pueden ofrecer a un coste tolerado por la mayoría de los actuales internautas, lo cual significará un gran éxito de dicha tecnología.

5.2 RECOMENDACIONES

- Se recomienda tomar en cuenta el estado de las líneas eléctricas en la red de acceso (corrosión, malos empalmes o extremado número de derivaciones) ya que esto genera reflexiones, y atenuaciones que disminuyen significativamente la calidad de la señal de datos transmitida.

- Se recomienda verificar el grado de cobertura de la señal de datos para comprobar la calidad de la transmisión en los diferentes puntos y la evaluación de la instalación de Unidades Repetidoras en la red PLC como la posible ubicación de los mismos.

- Es importante destinar un toma corriente exclusivamente para conectar un modem PLC, esta recomendación se debe a que si se conecta otro dispositivo eléctrico en el mismo toma corriente puede producir una alta posibilidad de interferencia en el artefacto eléctrico.

- Si la tecnología PLC quiere abrirse mercado, deberá o bien ofrecer la misma capacidad que el resto de compañías, pero bajando significativamente el precio (algo muy demandado por los internautas, debido a que los actuales anchos de banda ya son bastante aceptables) o bien, romper el mercado ofertando por el mismo precio o similar que existe en las compañías de ADSL, fibra óptica o cable, pero dotando de un nuevo universo de velocidades subiendo la calidad y velocidad de estas de forma significativa (cosa que pueden realizar debido a las velocidades que ellos si pueden llegar a alcanzar).

- No se debe confundir el PLC In-House, con el PLC access que es la tecnología que intentaron implementar las compañías eléctricas. La diferencia está en que, la in-house usa el cableado eléctrico de baja tensión de cualquier edificio y lo transforma en una red de datos normal y corriente, mientras el PLC de las eléctricas es usar la red de media tensión

para hacer lo mismo. El problema de las eléctricas reside precisamente allí, la red de media tensión complica el uso del PLC debido a los altos niveles de interferencias que se generan en la media tensión, mientras ese problema es inexistente en la baja tensión.

BIBLIOGRAFIA

Redes de computadores

Tesis

CONZA, Andrea. Diseño e Implementación de un Prototipo de DMZ y la Interconexión segura mediante VPN utilizando el Firewall Fortigate 60. Ing Cesar Gallardo. Septiembre 2009.

Web

http://es.wikipedia.org/wiki/Red_de_computadoras

http://www.thehouseofblogs.com/articulo/clasificacion_de_redes-475.html

Cámaras IP

Web

http://es.wikipedia.org/wiki/C%C3%A1mara_de_red

http://www.camarasip.cl/que_es_una_camara_ip.htm

http://www.gscssoftware.com/teccamaraip.htm

http://www.monografias.com/trabajos-ppt/camaras-ip/camaras-ip.shtml

http://valetron.eresmas.net/CamarasIP.htm

http://www.symde.com.co/Productos/SeguridadF%C3%ADsica/C%C3%A1marasIP/tabid/101/language/es-CO/Default.aspx

http://www.visualnetcam.com/

Tecnología BPL

Web

http://es.wikipedia.org/wiki/Power_Line_Communications

http://www.electronet.net.ec/Electronet/Tecnolog%C3%ADaBPL/tabid/110/Default.aspx

http://www.plt.citic.org.ec/index.php?option=com_content&view=article&id=19&Itemid=27

http://www.fcc.gov/cgb/broadband_spanish.html

http://www.labplan.ufsc.br/congressos/XIII%20Eriac/D2/D2-02.pdf

http://www.deltaasesores.com/terminos/a-c/2529-plc-o-bpl
http://grupos.emagister.com/documento/introduccion_para_bpl/1090-58480
https://www.underground.org.mx/index.php?topic=22456.0
http://www.afinidadelectrica.com.ar/articulo.php?IdArticulo=114
http://www.ikasugroup.com/sitio/BPL.pdf
http://www.plc.com.ve/ajax/bpl.html#

Adaptadores PLC

Tesis

CERON, Erick; GOMEZ, Boris. Diseño de una Red de Datos TCP/IP basada en PLC (POWER LINE COMMUNICATION) para una Urbanización Residencial. PH. D Enrique Mafla. Febrero 2009.

Web

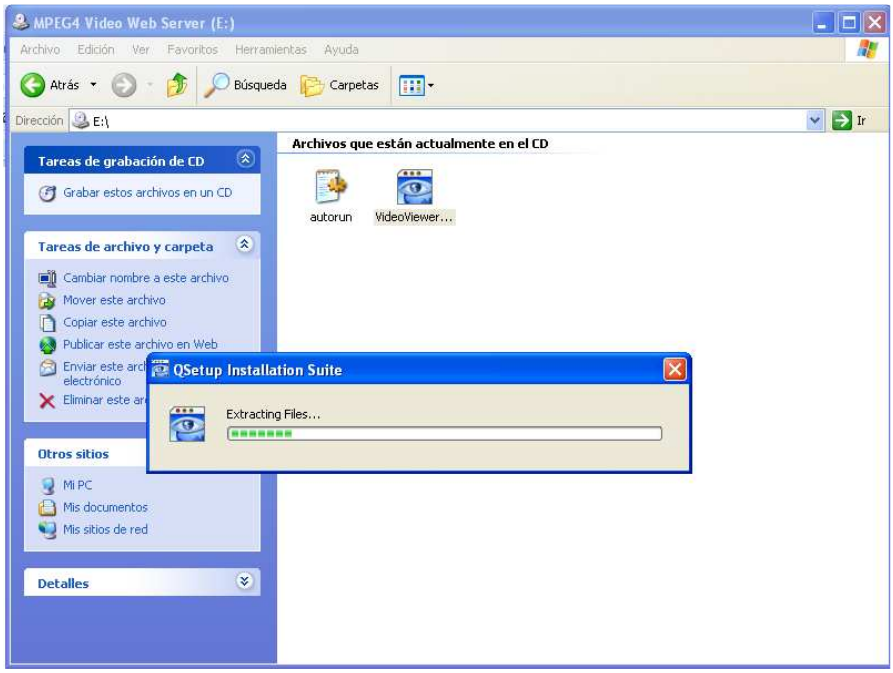
http://www.mewdevenezuela.com/productos/plc/PLCSerieFX3U.htm
http://www.mundodvd.com/showthread.php?t=46223
http://www.adslzone.net/imagenio-14.html
http://www.hispatienda.es/adaptador-plc-zyxel-pl100-p29795.html
http://www.casadomo.com/productosDetalle.aspx?id=286&idm=121&pat=121&cat=5&emp=&cert=
http://plc-net.com/7601.html?*session*id*key*=*session*id*val*
http://www.mundoanuncio.com/anuncio/adaptador_plc_de_red_1178991443.html
http://www.informatica-hoy.com.ar/redes/PLC-Internet-por-la-red-electrica.php
http://www.gratisprogramas.org/descargar/noticias-muy-interesantes/
http://administradorderedes.blogia.com/

ANEXOS

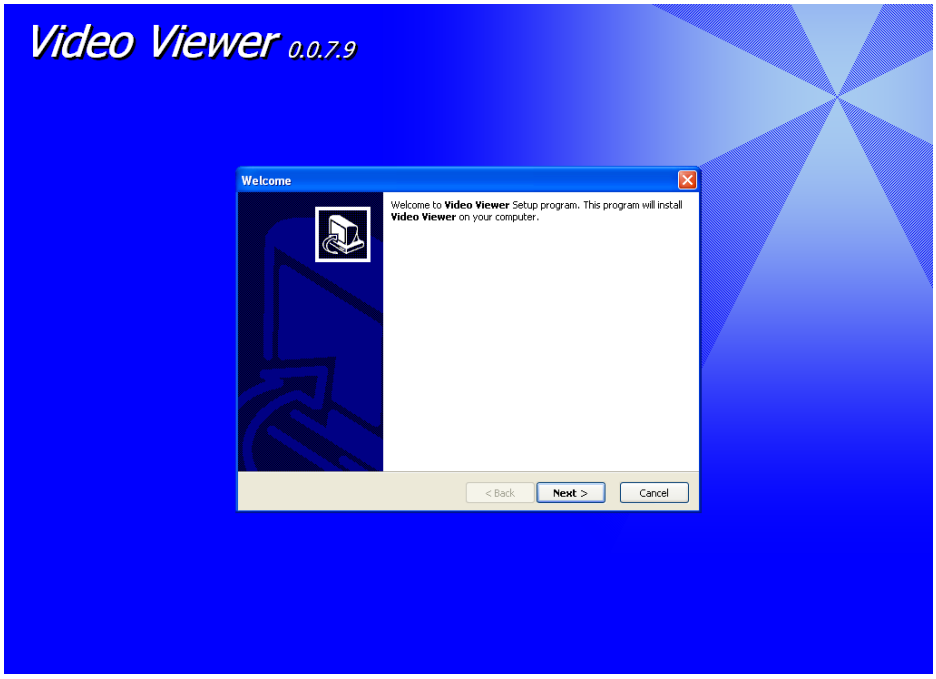
CAMARA IP

ANEXO 1. Instalación Programa Video Viewer

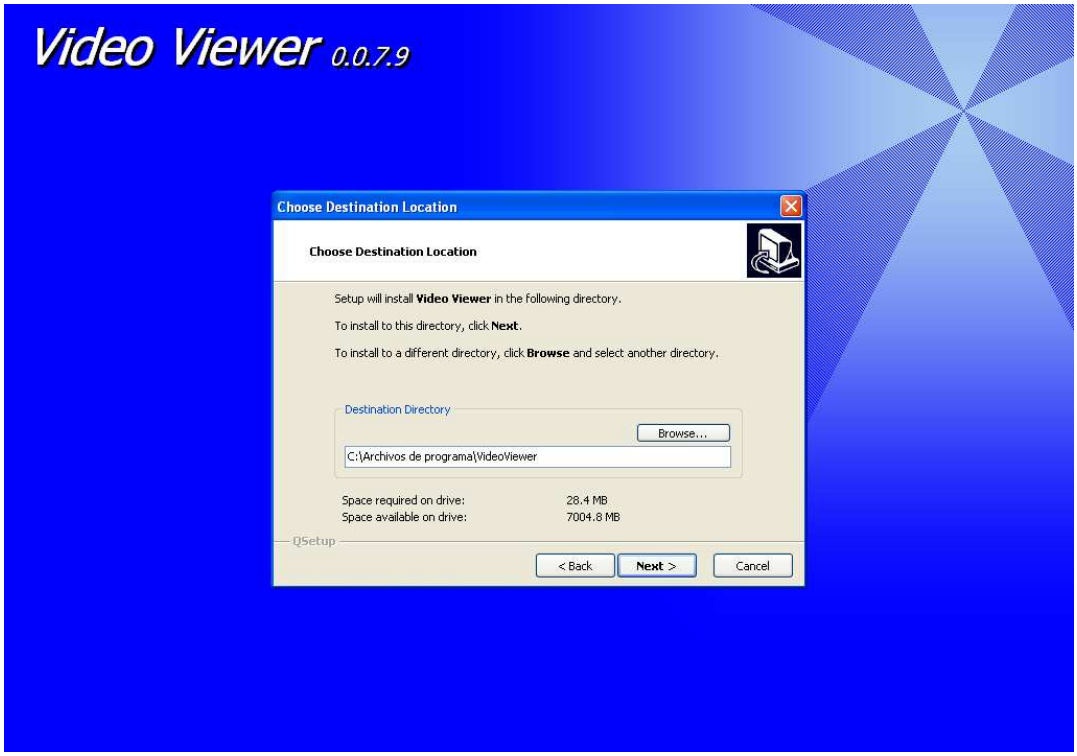
Se ejecuta el archivo ejecutable del CD para la instalación del programa



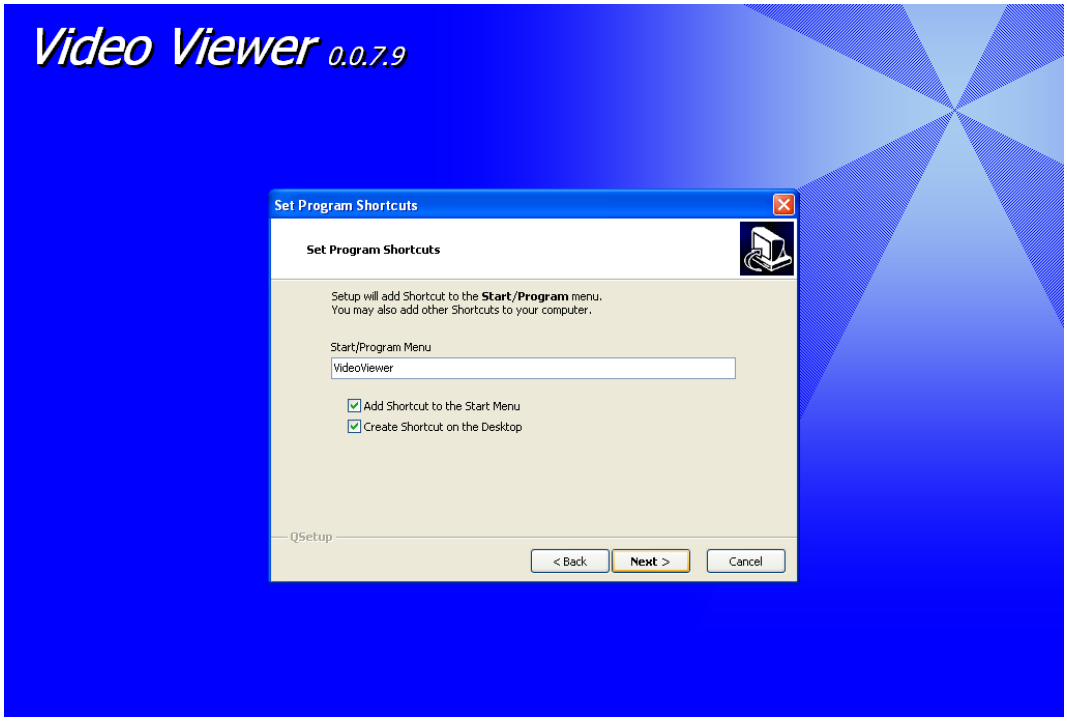
Se inicia la instalación del programa Video Viewer



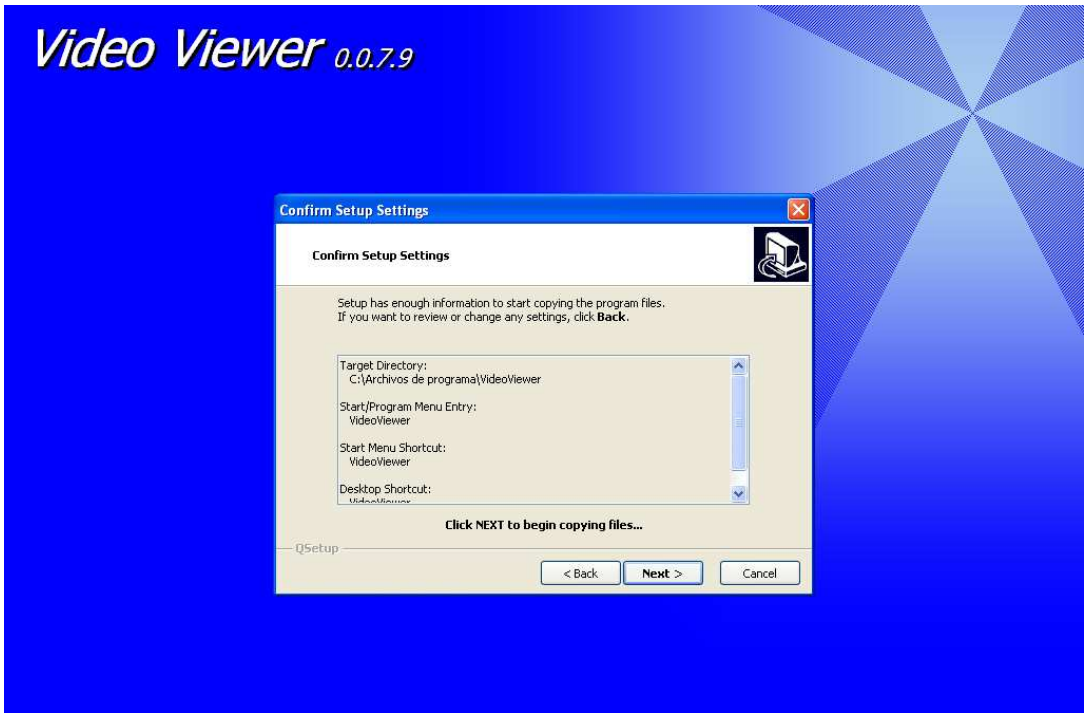
Al pulsar siguiente presenta la ruta donde se instalara el programa.



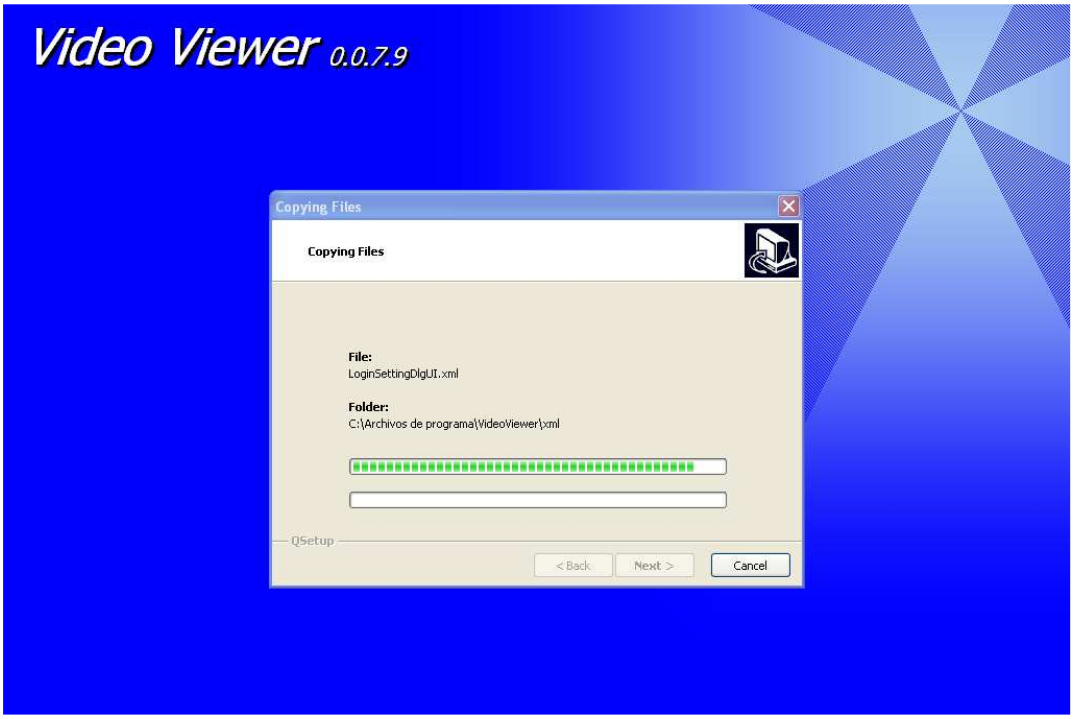
Confirmación de inicio de instalación del programa.



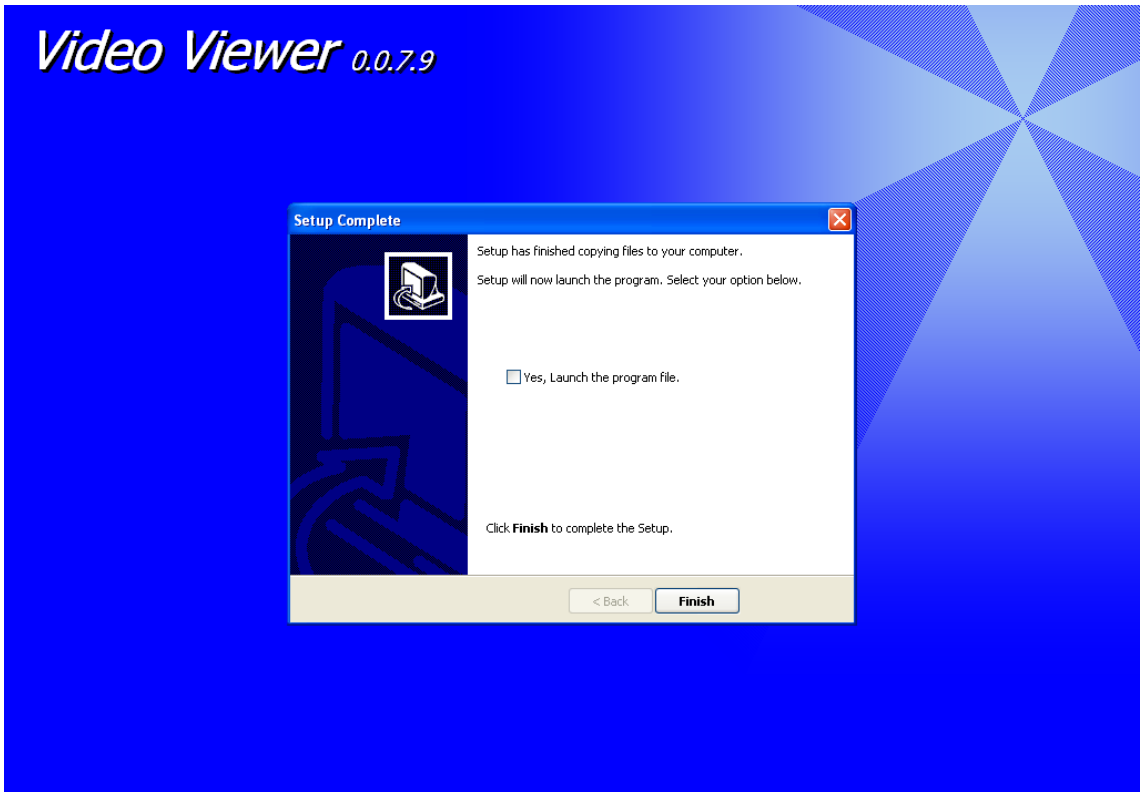
Confirmación de datos para la instalación.



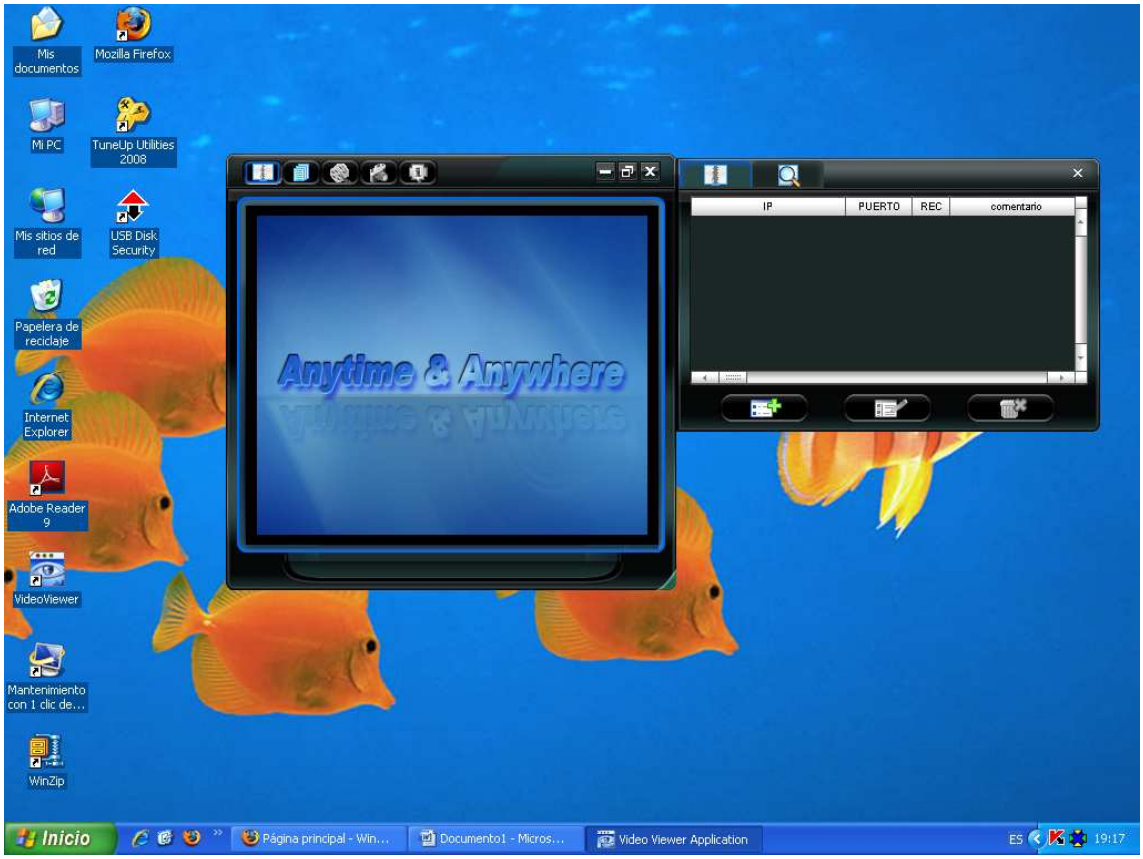
Progreso de instalación



Finalizar la instalación

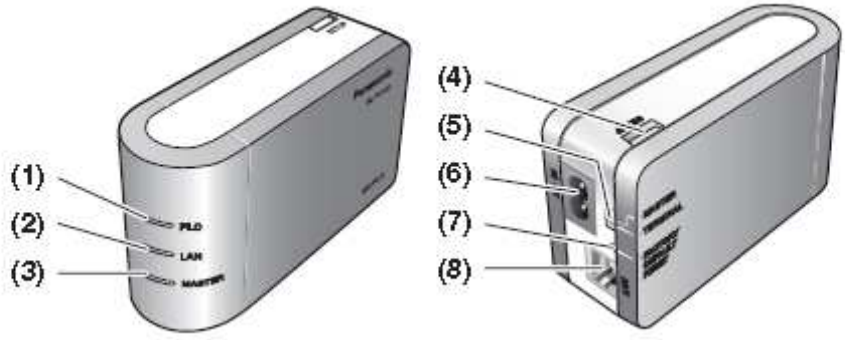


Una vez terminada la instalación se crea una acceso directo en el escritorio



Adaptadores PLC

ANEXO 2. Unidad principal



(1) Indicador PLC

Se enciende para indicar que el adaptador está conectado a la red HD-PLC.

(2) Indicador LAN

Se enciende cuando hay un cable de LAN conectado al adaptador y parpadea cuando se envían o reciben datos.

(3) Indicador MASTER

Se enciende cuando el adaptador está configurado como maestro.

(4) Botón SETUP

Utilizado para registrar el adaptador o para probar la velocidad de red del terminal.

(5) Selector de modo

La posición de este selector durante el registro determina si el adaptador se configurará como maestro o terminal.

(6) AC IN

Conecta el adaptador a la alimentación de CA, así como a la red HD-PLC.

(7) Botón FACTORY DEFAULT RESET

Se utiliza para reiniciar el adaptador y eliminar su registro.

(8) Puerto LAN

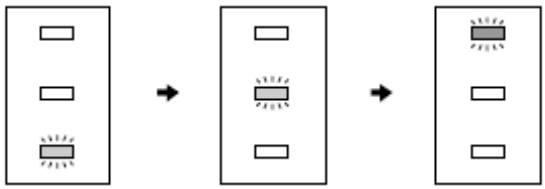
Conecta el adaptador a un dispositivo de red, como un enrutador de banda ancha, concentrador, ordenador, etc.

ANEXO 3. Prueba de la velocidad de red de un terminal

Cuando haya conectado los adaptadores en los puntos donde desee utilizarlos, siga el procedimiento que se describe a continuación para probar la velocidad de la conexión de red de cada terminal con el maestro. Asegúrese de que el adaptador terminal ya se ha registrado en un maestro.

1. Pulse y mantenga presionado el botón SETUP del terminal durante aproximadamente 1 segundo.

• Los indicadores se encienden uno a uno.



2. Tras algunos segundos aparecerá el resultado de la prueba de velocidad de red.

3. Consulte la siguiente tabla para determinar la velocidad de red.

PLC				
LAN				
MASTER				
Velocidad de red	Sin conexión	Buena Menos de 10 Mbps*1	Mejor De 10 Mbps a 30 Mbps*1	Óptima Más de 30 Mbps*1

*1 Velocidad de transmisión de datos aproximada al transmitir datos con el protocolo UDP.

4. Si el resultado de la prueba de velocidad no le satisface, conecte el terminal a una toma de corriente distinta y repita la prueba.

Nota

• Para poder utilizar el adaptador terminal, debe encenderse al menos un indicador (velocidad de red “Buena”).

• Si el resultado de la prueba de velocidad no le satisface y ha probado a conectar el adaptador terminal a distintas tomas de corriente, consulte la sección de solución de problemas.

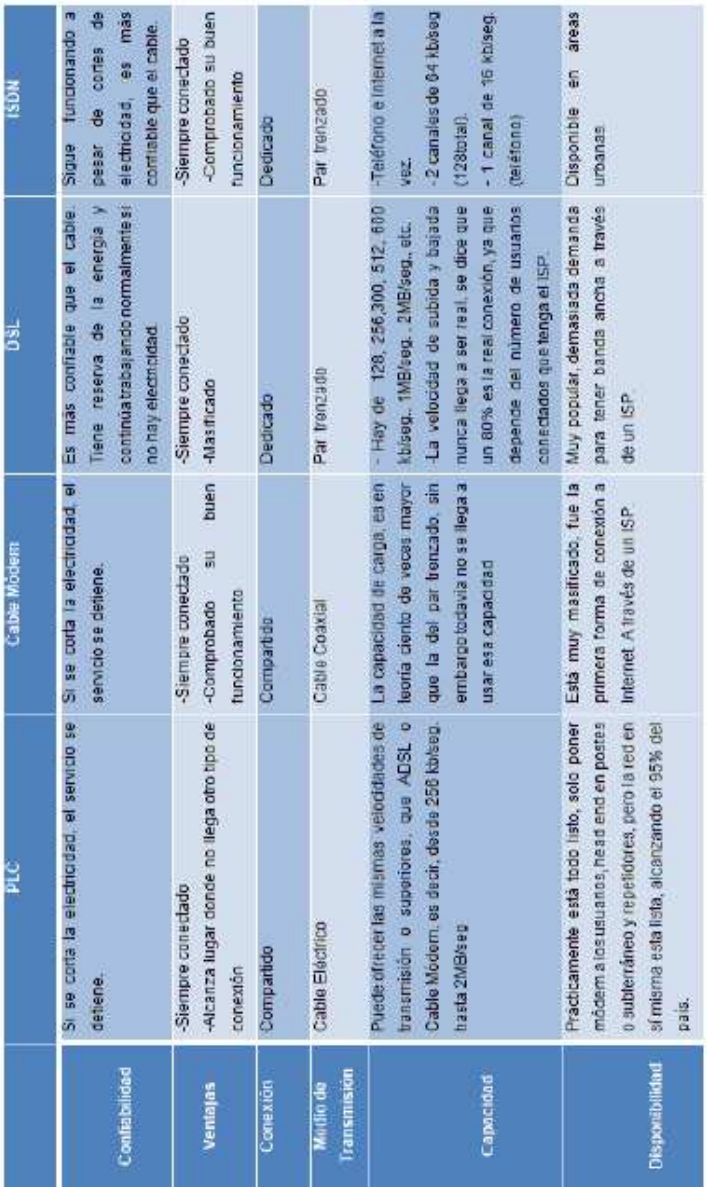
• Si las condiciones eléctricas de su hogar cambian, es posible que la velocidad de red también cambie.

Una vez satisfecho con el resultado de la prueba de velocidad del terminal, podrá conectar cada adaptador a un dispositivo de red (enrutador de banda ancha, concentrador, ordenador, impresora de red, cámara de red, etc.

ANEXO 4. Descripción de los indicadores

PLC	Azul, encendido	El adaptador está conectado correctamente a la red HD-PLC.
	Azul, intermitente	El terminal está registrándose en el maestro.
	Azul, se enciende cada 5 segundos	El adaptador está registrándose en el maestro, pero no está conectado a la red HD-PLC.
	Azul, se apaga cada 10 segundos	El maestro ha detectado otro adaptador maestro. En este caso, el funcionamiento se verá afectado por la presencia del otro adaptador maestro.
	Rojo, se ilumina durante 5 segundos	Error durante el registro. Vuelva a intentarlo.
	Rojo, encendido	El adaptador no funciona correctamente y no puede comunicarse a través de la red HD-PLC. Póngase en contacto con un centro de servicio Panasonic autorizado.
	Apagado	El adaptador no está enchufado. El adaptador no está conectado a la red HD-PLC (no se han encontrado, configurado, etc. otros adaptadores).
LAN	Verde, encendido	Hay un cable de LAN conectado al adaptador.
	Verde, intermitente	Se están enviando/recibiendo datos.
	Naranja, encendido	No hay ningún dispositivo de red conectado al adaptador a través del cable de LAN o el dispositivo de red no está encendido.
	Apagado	El adaptador no está enchufado.
MASTER	Verde, encendido	El adaptador está configurado como maestro.
	Verde, se enciende durante 10 segundos	Un terminal se ha registrado correctamente en el maestro.
	Apagado	El adaptador no está configurado como maestro.

ANEXO 5. Cuadro comparativo entre tecnologías



	PLC	Cable Módem	DSL	ISDN
Confiabilidad	Si se corta la electricidad, el servicio se detiene.	Si se corta la electricidad, el servicio se detiene.	Es más confiable que el cable. Tiene reserva de la energía y continúa trabajando normalmente si no hay electricidad.	Sigue funcionando a pesar de cortes de electricidad, es más confiable que el cable.
Ventajas	-Siempre conectado -Alcanza lugar donde no llega otro tipo de conexión	-Siempre conectado -Comprobado su buen funcionamiento	-Siempre conectado -Elasticado	-Siempre conectado -Comprobado su buen funcionamiento
Conexión	Compartido	Compartido	Dedicado	Dedicado
Medio de Transmisión	Cable Eléctrico	Cable Coaxial	Par trenzado	Par trenzado
Capacidad	Puede ofrecer las mismas velocidades de transmisión o superiores, que ADSL o Cable Módem, es decir, desde 256 kbit/seg. hasta 2MB/seg	La capacidad de carga, es en teoría ciento de veces mayor que la del par trenzado, sin embargo todavía no se llega a usar esa capacidad	- Hay de 128, 256,300, 512, 600 kbit/seg., 1MB/seg., 2MB/seg., etc. -La velocidad de subida y bajada nunca llega a ser real, se dice que un 80% es la real conexión, ya que depende del número de usuarios conectados que tenga el ISP.	-Teléfono e Internet a la vez. -2 canales de 64 kbit/seg (128total). - 1 canal de 16 kbit/seg. (teléfono)
Disponibilidad	Prácticamente está todo listo, solo poner módem a los usuarios, head end en postes o subterráneo y repetidores, pero la red en sí misma esta lista, alcanzando el 95% del país.	Está muy masificado, fue la primera forma de conexión a Internet. A través de un ISP.	Muy popular, demasiada demanda para tener banda ancha a través de un ISP.	Disponible en áreas urbanas.

GLOSARIO

ADSL

Son las siglas de asymmetric digital subscriber line ("línea de abonado digital asimétrica"). adsl es un tipo de línea dsl. consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado,1 siempre y cuando la longitud de línea no supere los 5,5 km medidos desde la central telefónica, o no haya otros servicios por el mismo cable que puedan interferir.

BANDA ESTRECHA

Las conexiones de banda estrecha hacen referencia a un tipo de conexión que utiliza un ancho de banda muy reducido. La conexión más típica de banda estrecha que existe es la conexión por módem telefónico (Dial-up). Un módem adapta las señales informáticas producidas por la computadora a otro tipo de señal que se puede introducir por la línea telefónica; así mismo, convierte la señal que llega a través de la línea telefónica en información comprensible para el ordenador.

BPL

La Banda ancha sobre líneas eléctricas (abreviada BPL por su denominación en inglés Broadband over Power Lines) representa el uso de tecnologías PLC que proporcionan acceso de banda ancha a Internet a través de líneas de energía ordinarias. En este caso, una computadora (o cualquier otro dispositivo) necesitaría solo conectarse a un módem BPL enchufado en cualquier toma de energía en una edificación equipada para tener acceso de alta velocidad a Internet.

CABLE MODEM

Un cablemódem o cable módem es un tipo especial de módem diseñado para modular la señal de datos sobre una infraestructura de televisión por cable. El término Internet por cable (o simplemente cable) se refiere a la distribución de un

servicio de conectividad a Internet sobre esta infraestructura de telecomunicaciones.

CANAL (OFDM)

a multiplexación por división de frecuencias ortogonales, en inglés *orthogonal frequency division multiplexing* (ofdm), es una multiplexación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información.

CHIP DS2

DS2 empezó en el 98 con esta tecnología de 200mbps pensando inicialmente en ser una alternativa para el ADSL. La tecnología de DS2 ha evolucionado muchísimo, ofreciendo dispositivos plug in play para conectividad en el hogar. se venden dispositivos tanto en retail como a operadoras(telefónica, bt, pt,etc) para el servicio de iptv(conectar el router ADSL con el STB de imagenio y ofrecer más de 20 mbps fiables para transmitir video HD).

CIRCUITO CERRADO

Es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades. Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

DSL

(Digital Subscriber Line) Línea de Abonado Digital. Tecnología que permite una conexión a una red con más velocidad a través de las líneas telefónicas. Alternativa al RDSI. Engloba tecnologías que proveen conexión digital sobre red telefónica como ADSL, SDSL, IDSL, HDSL, VDSL, etc. La diferencia entre ADSL y otras DSL es que la velocidad de bajada y la de subida no son iguales, por lo general permiten una mayor bajada que subida.

EQUIPOS CPE

El CPE (Equipo Local del Cliente) es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación. El equipo puede proveer una combinación de servicios incluyendo datos, voz, video y un host de aplicaciones multimedia interactivos.

EQUIPOS GW

Un Gateway (GW) es un equipo que permite interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos.

FIBRA OPTICA

Las redes de fibra óptica se emplean cada vez más en telecomunicación, debido a que las ondas de luz tienen una frecuencia alta y la capacidad de una señal para transportar información aumenta con la frecuencia. En las redes de comunicaciones por fibra óptica se emplean sistemas de emisión láser.

MULTIPLEXACIÓN POR DIVISIÓN DE FRECUENCIA (FDM)

La multiplexación por división de frecuencia o FDM (Frequency-division multiplexing) y su equivalente para medios ópticos, por división de longitud de onda es la combinación de dos o más canales de información en un solo medio de transmisión usando un dispositivo llamado multiplexor.

NIDS

Sistema de detección de intrusos en una Red. Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneadores de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real. Para ello, analiza todos los paquetes, buscando en ellos patrones sospechosos.

PLC

Power Line Communications, es un término inglés que puede traducirse por comunicaciones mediante cable eléctrico. La tecnología PLC aprovecha la red eléctrica para convertirla en una línea digital de alta velocidad de transmisión de datos, permitiendo, entre otras cosas, el acceso a Internet mediante banda ancha.

PLC In-House

PLC in-house usa el cableado eléctrico de baja tensión de cualquier edificio y lo transforma en una red de datos normal y corriente.

PLC access

Es usar la red de media tensión para hacer lo mismo para transformar la corriente en un rede de datos. La red de media tensión complica el uso del PLC debido a los altos niveles de interferencias que se generan en la media tensión, mientras ese problema es inexistente en la baja tensión.

REED-SOLOMON

Reed-Solomon es un código cíclico no binario y constituye una subclase de los códigos BCH. Los códigos cíclicos son una subclase de los códigos de bloque estándar de detección y corrección de errores que protege la información contra errores en los datos transmitidos sobre un canal de comunicaciones.

RF

Una red de área local por radio frecuencia puede definirse como una red local que utiliza tecnología de radio frecuencia para enlazar los equipos conectados a la red en lugar de los medios utilizados en las LAN convencionales cableadas.

RED SATELITAL

Un satélite puede definirse como un repetidor radioeléctrico ubicado en el espacio, que recibe señales generadas en la tierra, las amplifica y las vuelve a enviar a la tierra, ya sea al mismo punto donde se origino la señal u otro punto distinto.

SSL

SSL o Secure Socket Layer por sus siglas en inglés, es un sistema que permite que la información viaje encriptada evitándose que puede ser leída por sniffers u otros recursos.

TELEMETRÍA

La telemetría es una tecnología que permite la medición remota de magnitudes físicas y el posterior envío de la información hacia el operador del sistema. La palabra telemetría procede de las palabras griegas τ□λε (tele), que quiere decir a distancia, y la palabra μετρον (metron), que quiere decir medida.

ULTIMA MILLA

Las redes de acceso, mejor conocidas como de última milla, tienen como propósito enlazar las redes de los operadores con sus usuarios, sean residenciales o corporativos.

WIRELESS

Wireless (inalámbrico o sin cables) es un término usado para describir las telecomunicaciones en las cuales las ondas electromagnéticas (en vez de cables) llevan la señal sobre parte o toda la trayectoria de la comunicación.