ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE TECNOLOGÍA

Diseño e Implementación del Sistema de Cableado Estructurado y red inalámbrica para Hormigones del Valle S.A.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ANALISIS DE SISTEMAS INFORMATICOS

JULIAN ALEXANDER LUZCANDO ANDRADE
julianbsc@hotmail.com

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

Quito, Mayo del 2011

DECLARACIÓN

Yo, Julián Alexander Luzcando Andrade, declaro bajo juramento que el trabajo aquí descrito es de mi 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 cedo mis 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.

Julián Luzcando

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Julián Luzcando, bajo mi supervisión.

Ing. Cesar Gallardo
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios que me supo guiar y darme salud para poder culminar mis estudios.

A mis padres que con su apoyo incondicional me dieron fuerzas para alcanzar esta meta y cumplir todos mis objetivos.

A mi director de tesis Ing. Cesar Gallardo por su apoyo constante y su amistad brindada todos estos años.

A la Escuela Politécnica Nacional y a la Escuela de Formación de Tecnólogos donde me brindaron mi formación personal y profesional.

DEDICATORIA

A mis padres ya que gracias a su ejemplo y perseverancia supe que pese a las adversidades de la vida se puede llegar a cumplir los objetivos propuestos.

RESUMEN

El presente proyecto tiene por objetivo el diseño y la implementación de un sistema de cableado estructurado integrado una red inalámbrica en la empresa Hormigones del Valle S.A.

El primer capítulo habla sobre la situación actual de la empresa, identificación del problema, los objetivos y la meta que se quiere alcanzar en dicha empresa.

El segundo capítulo tiene toda la información referente a los conceptos de sistema de cableado estructurado y red inalámbrica como, normas, especificaciones de diseño, topologías de red, alcances protocolos, estándares y factores que debemos considerar para la implementación de la red.

En el tercer capítulo se analizan las diferentes opciones de mercado, tales como precio, limitaciones, durabilidad así como se detalla el diseño físico y lógico de la empresa.

El cuarto capítulo se describe la implementación del proyecto, las instalaciones de los puntos de red, las conexiones, y el funcionamiento del hardware seleccionado.

Por último en el quinto capítulo se llega a las conclusiones y recomendaciones, así como el glosario de términos y las referencias bibliográficas las cuales se usaron en este proyecto.

Índice

Índice de Figuras

Índice de Tablas

CAPITULO 1. I. INTRODUCCION

1.1 ÁMBITO

Hormigones del Valle S.A. es una empresa que se dedica a la producción y a la comercialización del hormigón, su principal objetivo, ahora mismo, es calificar para la certificación ISO9000, que es un estándar en el que la empresa consigue la excelencia en los procesos de producción, para de esta forma ser reconocida como una de las empresas de más prestigio dentro de su rama.
Es una empresa dedicada a la producción y comercialización de Hormigón para la construcción de casas, edificios y estructuras que requieran hormigón.
Tiene en el mercado alrededor de 12 años, tiempo en el cual ha ido creciendo tanto en tamaño de infraestructura como en su crecimiento económico.

1.1.1 MISIÓN

Producir y garantizar en calidad y cantidad el hormigón premezclado con tecnología de punta con personal especializado, generando así la satisfacción de nuestros clientes.

1.1.2 VISIÓN

Mantenernos dentro de las 2 mejores empresas hormigoneras de la provincia de pichincha, solidez, ética y técnica en la producción y entrega de hormigón, cumpliendo normas nacionales e internacionales de calidad y mejorar permanentemente la satisfacción de nuestros clientes

1.2 PROBLEMA ACTUAL

La empresa no tiene implementado un sistema de cableado estructurado acorde a sus necesidades, en estos momentos cuenta un diseño de red poco estable, la cual causa retrasos en acceso a la red, perdida de información y no hay comunicación entre departamentos.

Actualmente funciona bajo la siguiente estructura física:

- Planta 1. Oficinas Administrativas, en una sola casa repartidos en varios departamentos. Gerencia, Marketing, Seguridad Industrial, Departamento Medico, Contabilidad, Ventas, Recepción, Administración, Cuarto de Servidor. Todas las máquinas están conectadas a un switch principal, de donde toman la señal de la red y de internet.

- Planta 2. (Recursos Humanos). separadas a la planta 1 en una distancia de 40m. Tenemos 2 puntos de red. Para una máquina y para un reloj biométrico, un switch de 8 puertos que se enlazan a la oficina principal.

- Planta 3 Planta de Producción. A una distancia de 400m. Tenemos un router inalámbrico, tres Computadoras que están enlazadas a la planta principal (planta 1), via router inalámbrico y por este router se conectan las máquinas de bodega (dos máquinas).

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Optimizar los procesos informáticos y de gestión de recursos compartidos que se encuentran dispersos en la empresa, mediante el diseño e implementación de un Sistema de Cableado Estructurado (SCE) en las áreas físicas independientes e integradas por una red inalámbrica para así incorporar los departamentos aislados a la red de datos de la empresa.

1.3.2 OBJETIVOS ESPECIFICOS

- Analizar los requerimientos de la empresa en cuanto a las aplicaciones informáticas que se ejecutan.
- Investigar las distintas alternativas tecnológicas con su característica, de manera que permitan dar la solución a los problemas presentados.

- Investigar las distintas normas y estándares que rigen a un Sistema de Red Inalámbrica (WLAN) y Sistema de Cableado Estructurado (SCE)
- Diseñar la red integrada (SCE y WLAN) y recomendar la mejor infraestructura del sistema de cableado estructurado e inalámbrico tomando en cuenta eficiencia, rapidez y costos.
- Implementar el Sistema de Cableado Estructurado (SCE) que integre a la red inalámbrica (WLAN).

1.4 ANALISIS DE LA SITUACION ACTUAL

En estos momentos la empresa no cuenta con una infraestructura de red de datos adecuada, como consecuencia se ocasiona pérdida de información, demoras en el uso y acceso a la red, provocando molestias en los usuarios.

La actualización tecnológica para mejorar los procesos de calidad es necesaria, por lo cual la empresa ha previsto la implementación de un sistema de red guiada (cable), que se complementará con una interconexión vía red no guiada (inalámbrica) entre plantas.

Bajo lo mencionado se puede afirmar que la empresa podrá contar con una mejor organización en su estructura de red, teniendo un mejor acceso y uso de sus recursos e información

CAPITULO 2. II. MARCO TEORICO

2.1 REDES DE COMUNICACIÓN

2.1.1 DEFINICION[1]

Las redes o infraestructuras de (tele) comunicaciones proporcionan la capacidad y los elementos necesarios para mantener a distancia un intercambio de información y/o una comunicación, ya sea ésta en forma de voz, datos, vídeo o una mezcla de los anteriores.

Los elementos necesarios comprenden disponer de acceso a la red de comunicaciones, el transporte de la información y los medios y procedimientos (conmutación, señalización, y protocolos para poner en contacto a los extremos (abonados, usuarios, terminales,…) que desean intercambiar información.

Además, numerosas veces los usuarios se encuentran en extremos pertenecientes a diferentes tipos de redes de comunicaciones, o en redes de comunicaciones que aún siendo iguales son de distinta propiedad. En estos casos, hace falta contar con un procedimiento de interconexión.

2.1.2 CATEGORIZACIÓN

En primer lugar las redes de comunicaciones se pueden distinguir en función de si el camino por el que circula la información es posible en ambos sentidos o uno solo. Así, se tienen:

2.1.2.1 REDES DE COMUNICACIONES UNIDIRECCIONALES

En las que la información viaja desde un emisor a un receptor, no existiendo camino de retorno para la comunicación inversa. Este tipo de comunicaciones se suele encontrar en las redes de difusión o distribución.

2.1.2.2 REDES DE COMUNICACIONES BIDIRECCIONALES

La información entre los extremos viaja en los dos sentidos, típicamente por el mismo camino, aunque también existen redes en que no tiene por qué coincidir los caminos de ida y vuelta. Algunos ejemplos son las redes de telefonía y de datos.

2.1.2.3 REDES HÍBRIDAS

En las que se integran tipos diferentes de redes; por ejemplo, una red unidireccional para un sentido de la comunicación es combinada con otra red para el camino de retorno. Estas soluciones fragmentarias permiten tener, por ejemplo, servicios interactivos de televisión, en la que ésta es recibida por la red de difusión terrestre o por satélite, mientras que las selecciones del usuario y sus peticiones de vídeo bajo demanda (VoD), se envían por Internet (sobre la red telefónica).

2.1.3 CLASIFICACION[2]

2.1.3.1 Según el espacio que ocupan

2.1.3.1.1 Red de área local (LAN)

Una LAN es una red de datos de recursos compartidos que permite que dispositivos de computación y comunicación se puedan interconectar entre sí, para permitir la comunicación entre ellos, este tipo de redes están confinadas en áreas geográficas relativamente pequeñas, en áreas departamentales u oficinas. Entre las principales características se tienen que una LAN está ubicada en el rango de 1-10 Km máximo, la velocidad de información desde 300 bps en adelante y actualmente con el uso de Fast-Ethernet hasta 100 Mbps, Toda red local posee características particulares, dependiendo de las exigencias de cada usuario, departamento o institución.

---

[1] http://es.wikitel.info/wiki/Redes_de_comunicaciones
[2] http://www.forest.ula.ve/~mana/cursos/redes/clasifica.html

La necesidad de compartir recursos hacen de este tipo de redes, el sistema de comunicación más apropiado para cualquier tipo de institución, donde se puede compartir desde recursos computacionales hasta los humanos, sobre todo este último, de vital importancia, porque por medio de las redes podemos compartir conocimientos en cualquier campo del trabajo diario.

2.1.3.1.2 Red metropolitana (MAN)

Las redes de área metropolitana (MAN, Metropolitana Área Network) Conectan segmentos de red local de un área específica, como un campus, un polígono industrial o una ciudad, se basa en la conexión de redes locales que expande el servicio en un área metropolitana, el soporte de la conexión de las redes se basa en el servicio de líneas dedicadas o discadas de las compañías telefónicas, en la actualidad crece el interés en redes inalámbricas y redes interconectadas por troncales de Fibra Óptica. La unión a las MANs se realiza mediante el uso de enrutadores o convertidores de protocolos como los Gateways o pasarelas.

2.1.3.1.3 Red de gran alcance (WAN)

Una red de gran área WAN, es una red que interconecta una variedad de nodos de acceso o puntos de presencia geográficamente dispersos, tanto a nivel local como nacional e internacional. En este tipo de red es muy utilizada la conexión por satélite o por fibra óptica.

2.1.4 SEGÚN LA TÉCNICA DE TRANSFERENCIA

2.1.4.1 Redes de difusión:

Aquellas cuando uno de sus componentes envía información, ésta llega al resto de los componentes de la red.

2.1.4.2 Redes conmutadas

Cuando se establece un enlace, como si se tratase de un enlace punto a punto entre el origen y el destino, siendo transparente para los demás dicha comunicación

2.1.5 SEGÚN AL MEDIO DE COMUNICACIÓN

2.1.5.1 Guiados

2.1.5.1.1 Par Trenzado

Los hilos se encuentran trenzados por pares, de forma que cada par forma un circuito. Existen dos categorías de pares trenzados que son: El par trenzado sin pantalla (UTP, unshielder twisted pair) usado en telefonía, y el par trenzado apantallado (STP, shielded twisted pair) proporciona protección frente a la diafonía. El trenzado de los pares permite la eliminación de las interferencias, siendo de esta manera posible la transmisión a velocidades elevadas hasta 100 Mbs.

Figura 2-1: Par Trenzado
Fuente: http://www.forest.ula.ve/~mana/cursos/redes/clasifica.html

2.1.5.1.2 Cable Coaxial

El cable coaxial consta de un núcleo sólido de cobre rodeado por un aislante, una combinación de hilos apantallados y de tierra dispuestos en forma de mallado y un recubrimiento de goma como protector exterior. Con este tipo de cable es posible lograr velocidades altas, pero las técnicas de transmisión más nuevas usan el par trenzado el cual igualan y pasan las velocidades soportadas por el coaxial. Sin embargo las distancias con este cable sobrepasan al par trenzado.

De los cables coaxiales, es más común es el RG-58, el cual es un medio de transmisión que utiliza un cable apantallado de dos conductores similar al cable coaxial usado para transmisión de televisión, este tipo se le conoce como coaxial delgado o fino, tiene una impedancia de 50 Ohmnios.

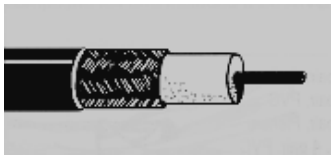

Figura 2-2: Cable Coaxial RG-58

Fuente: http://www.forest.ula.ve/~mana/cursos/redes/clasifica.html

2.1.5.1.3 Fibra Óptica

El cable de fibra óptica consta de un núcleo de vidrio central a través del cual se propagan las ondas luminosas. Este núcleo se rodea por un revestimiento de vidrio que fundamentalmente refleja la luz, este tipo de cable se puede extender sobre distancias mucho más grandes que el cable de cobre, no es susceptible a interferencias electromagnéticas, además no radia señales que puedan interferir a los demás medios de transmisión.

Figura 2-3: Fibra Optica Indoor

Fuente: http://www.forest.ula.ve/~mana/cursos/redes/clasifica.html

2.1.5.2 No Guiados[3]

Se utiliza medios no guiados, principalmente en el aire. Se radia energía electromagnética por medio de una antena y luego se recibe esta energía con otra

[3] http://tutorial.galeon.com/inalambrico.htm

antena. Hay dos configuraciones para la emisión y recepción de esta energía: direccional y omnidireccional.

2.1.5.2.1 Método direccional

Toda la energía se concentra en un haz que es emitida en una cierta dirección, por lo que tanto el emisor como el receptor deben estar alineados.

2.1.5.2.2 Método omnidireccional

La energía es dispersada en múltiples direcciones, por lo que varias antenas pueden captarla. Cuando mayor es la frecuencia de la señal a transmitir, más factible es la transmisión unidireccional.

Por tanto, para enlaces punto a punto se suelen utilizar microondas (altas frecuencias), para enlaces con varios receptores posibles se utilizan las ondas de radio (baja frecuencias)

2.1.5.2.3 Microondas Terrestres

Un radio enlace terrestre o microondas terrestre provee conectividad entre dos sitios (estaciones terrenas) en línea de vista (Line-of-Sight, LOS) usando equipo de radio con frecuencias de portadora por encima de 1 GHz. La forma de onda emitida puede ser analógica (convencionalmente en FM) o digital.
Las principales aplicaciones de un sistema de microondas terrestre son las siguientes:

- Telefonía básica (canales telefónicos)
- Datos
- Telégrafo / Telex / Facsímile
- Canales de Televisión.

- Vídeo
- Telefónica Celular

Las licencias o permisos para operar enlaces de microondas pueden resultar un poco difíciles ya que las autoridades del país donde se encuentren deben de asegurarse que ambos enlaces no causen interferencia a los enlaces ya existentes.

El clima y el terreno son los mayores factores a considerar antes de instalar un sistema de microondas. Como por ejemplo, no se recomienda instalar sistemas en lugares donde no llueva mucho; en este caso deben usarse radios con frecuencias bajas (es decir menores a 10 GHz). Las consideraciones en terreno incluyen la ausencia de montañas o grandes cuerpos de agua las cuales pueden ocasionar reflexiones de multi-trayectorias.

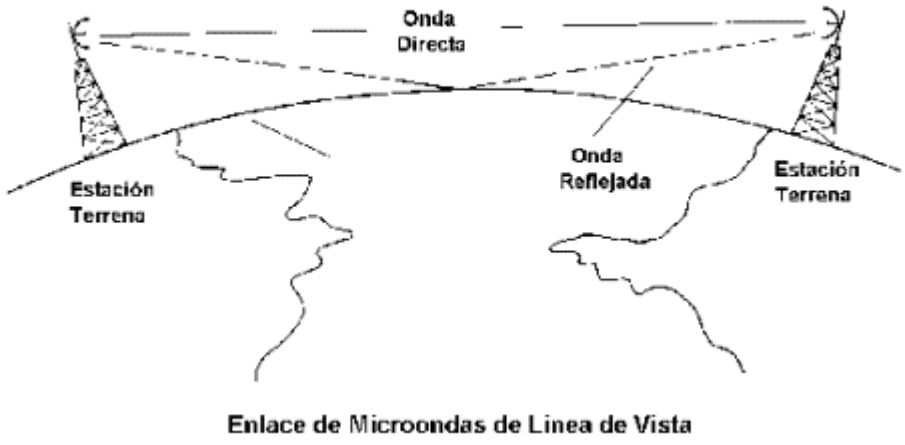

Figura 2-4: Enlace de Microondas de Línea de Vista
Fuente: http://tutorial.galeon.com/inalambrico.htm

2.1.5.2.4 Microondas Satelital

Un satélite actúa como una estación de relevación (relay station) o repetidor. Un transponedor recibe la señal de un transmisor, luego la amplifica y la retransmite hacia la tierra a una frecuencia diferente. Debe notarse que la estación terrena

transmisora envía a un solo satélite. El satélite, sin embargo, envía a cualquiera de las estaciones terrenas receptoras en su área de cobertura o huella (footprint).

La transmisión por satélite ofrece muchas ventajas para una compañía. Los precios de renta de espacio satelital es más estable que los ofrecidos por las compañías telefónicas. Ya que la transmisión por satélite no es sensitiva a la distancia. Y además existe un gran ancho de banda disponible.

Los beneficios de la comunicación por satélite desde el punto de vista de comunicaciones de datos podrían ser los siguientes:

- Transferencia de información a altas velocidades (Kbps, Mbps)
- Ideal para comunicaciones en puntos distantes y no fácilmente accesibles geográficamente.
- Ideal en servicios de acceso múltiple a un gran número de puntos.
- Permite establecer la comunicación entre dos usuarios distantes con la posibilidad de evitar las redes públicas telefónicas.

Entre las desventajas de la comunicación por satélite están las siguientes:

- 1/4 de segundo de tiempo de propagación. (retardo)
- Sensibilidad a efectos atmosféricos
- Sensibles a eclipses
- Falla del satélite (no es muy común)
- Requieren transmitir a mucha potencia
- Posibilidad de interrupción por cuestiones de estrategia militar.

A pesar de las anteriores limitaciones, la transmisión por satélite sigue siendo muy popular.

Los satélites de órbita baja (Low Earth Orbit LEO) ofrecen otras alternativas a los satélites geoestacionarios (Geosynchronous Earth Orbit GEO), los cuales giran alrededor de la tierra a más de 2,000 millas. Los satélites de este tipo proveen

comunicaciones de datos a baja velocidad y no son capaces de manipular voz, señales de video o datos a altas velocidades.

Pero tienen las ventajas que los satélites GEO no tienen. Por ejemplo, no existe retardo en las transmisiones, son menos sensibles a factores atmosféricos, y transmiten a muy poca potencia. Estos satélites operan a frecuencias asignadas entre los 1.545 GHz y los 1.645 GHz (Banda L).

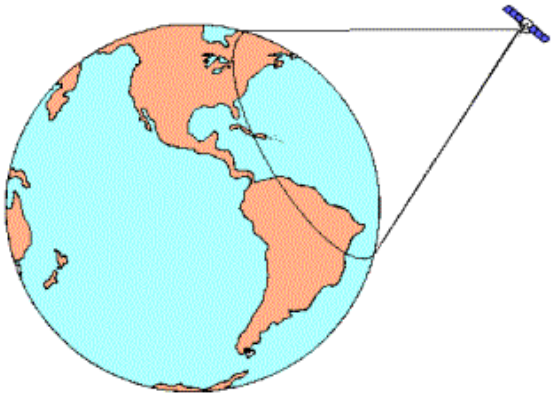

Figura 2-5: Microondas Satelital
Fuente: http://tutorial.galeon.com/inalambrico.htm

2.1.6 POR TOPOLOGIAS[4]

La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cual topología es la más apropiada para una situación dada.

La topología en una rede es la configuración adoptada por las estaciones de trabajo para conectarse entre sí. Entre las más comunes tenemos:

2.1.6.1 Bus

Esta topología permite que todas las estaciones reciban la información que se transmite, una estación transmite y todas las restantes escuchan. Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos

[4] http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml

de una red. Todos los nodos de la red están unidos a este cable: el cual recibe el nombre de "Backbone Cable". Tanto Ethernet como Local Talk pueden utilizar esta topología.

El bus es pasivo, no se produce regeneración de las señales en cada nodo. Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

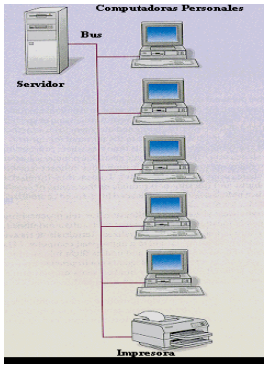

Figura 2-6: Topología "Bus"

Fuente: http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml

2.1.6.2 Anillo

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

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

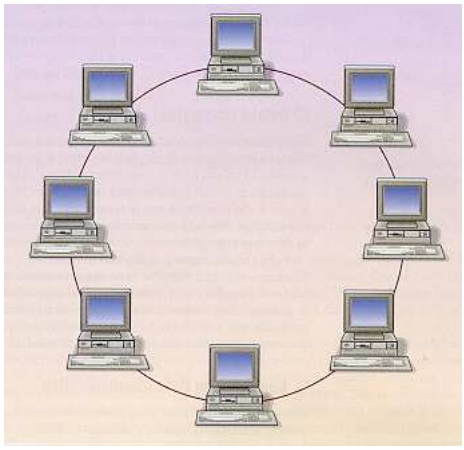

Figura 2-7: Topología Anillo

Fuente: http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml

2.1.6.3 Estrella

Los datos en estas redes fluyen del emisor hasta el concentrador, este realiza todas las funciones de la red, además actúa como amplificador de los datos.

La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

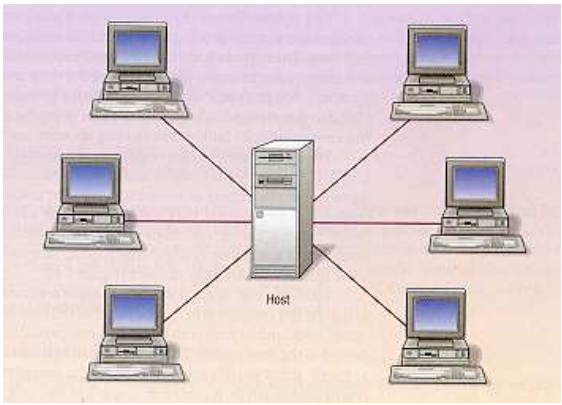

Figura 2-8: Topología Estrella

Fuente: http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml

2.1.7 HIBRIDAS

El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

2.1.7.1 Anillo en Estrella

Esta topología se utiliza con el fin de facilitar la administración de la red.

Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

2.1.7.2 "Bus" en Estrella

El fin es igual a la topología anterior. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

2.1.7.3 Estrella Jerárquica

Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica.

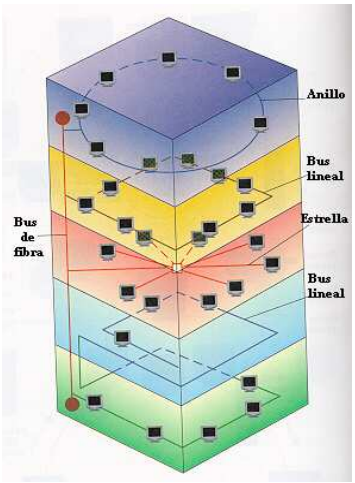

Figura 2-9: Topología Hibrida

Fuente: http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml

2.1.8 ÁRBOL

Esta estructura se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

2.1.9 TRAMA

Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de redes locales (LAN). Las estaciones de trabajo están conectadas cada una con todas las demás.

2.1.10 MECANISMOS PARA LA RESOLUCIÓN DE CONFLICTOS EN LA TRASNMICIÓN DE DATOS

2.1.10.1 CSMA/CD

Son redes con escucha de colisiones. Todas las estaciones son consideradas igual, es por ello que compiten por el uso del canal, cada vez que una de ellas desea transmitir debe escuchar el canal, si alguien está transmitiendo espera a que termine, caso contrario transmite y se queda escuchando posibles colisiones, en este último espera un intervalo de tiempo y reintenta de nuevo.

2.1.11 Token Bus

Se usa un token (una trama de datos) que pasa de estación en estación en forma cíclica, es decir forma un anillo lógico. Cuando una estación tiene el token, tiene el derecho exclusivo del bus para transmitir o recibir datos por un tiempo determinado y luego pasa el token a otra estación, previamente designada. Las otras estaciones no pueden transmitir sin el token, sólo pueden escuchar y esperar su turno. Esto soluciona el problema de colisiones que tiene el mecanismo anterior.

2.1.12 Token Ring

La estación se conecta al anillo por una unidad de interfaz (RIU), cada RIU es responsable de controlar el paso de los datos por ella, así como de regenerar la transmisión y pasarla a la estación siguiente. Si la dirección de la cabecera de una determinada transmisión indica que los datos son para una estación en concreto, la unidad de interfaz los copia y pasa la información a la estación de trabajo conectada a la misma.

Se usa en redes de área local con o sin prioridad, el token pasa de estación en estación en forma cíclica, inicialmente en estado desocupado. Cada estación cundo tiene el token (en este momento la estación controla el anillo), si quiere transmitir cambia su estado a ocupado, agregando los datos atrás y lo pone en la red, caso contrario pasa el token a la estación siguiente. Cuando el token pasa de nuevo por la estación que transmitió, saca los datos, lo pone en desocupado y lo regresa a la red.

2.1.13 PROTOCOLOS[5]

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

Hay 3 puntos a destacar sobre protocolos:

- **Existen muchos protocolos.** A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza

[5] http://fmc.axarnet.es/redes/tema_06_m.htm

distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.

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

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

2.1.13.1 Como Funcionan

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

Los pasos del protocolo se tienen que llevar a cabo en un orden apropiado y que sea el mismo en cada uno de los equipos de la red. En el equipo origen, estos pasos se tienen que llevar a cabo de arriba hacia abajo. En el equipo de destino, estos pasos se tienen que llevar a cabo de abajo hacia arriba.

2.1.13.2 Paquetes de Información[6]

[6] http://www.angelfire.com/mi2/Redes/protocolo.html

La información es embalada en sobres de datos para la transferencia. Cada grupo, a menudo llamados paquetes incluyen las siguientes informaciones:

- **Datos a la carga:** La información que se quiere transferir a través de la red, antes de ser añadida ninguna otra información. El termino carga evoca a la pirotecnia, siendo la pirotecnia una analogía apropiada para describir como los datos son disparados de un lugar a otro de la red.

- **Dirección:** El destino del paquete. Cada segmento de la red tiene una dirección, que solamente es importante en una red que consista en varias LAN conectadas. También hay una dirección de la estación y otra de la aplicación. La dirección de la aplicación se requiere para identificar a que aplicación de cada estación pertenece el paquete de datos.

- **Código de control:** Informa que describe el tipo de paquete y el tamaño. Los códigos de control también códigos de verificación de errores y otra información.

2.1.14 MODELO OSI[7]

El **modelo de referencia de Interconexión de Sistemas Abiertos** (OSI, Open System Interconnection) fue el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, fue un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Siguiendo el esquema de este modelo se crearon numerosos protocolos. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo es muy usado en la enseñanza

[7] http://es.wikipedia.org/wiki/Modelo_OSI

como una manera de mostrar cómo puede estructurarse una "pila" de protocolos de comunicaciones.

El modelo especifica el protocolo que debe ser usado en cada capa, y suele hablarse de modelo de referencia ya que es usado como una gran herramienta para la enseñanza de comunicación de redes. Este modelo está dividido en siete capas:

2.1.14.1 Capa física (Capa 1)

Es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas/electromagnéticas
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de ésta).

2.1.14.2 Capa de enlace de datos (Capa 2)

Esta capa se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Se hace un direccionamiento de los datos en la red ya sea en la distribución adecuada desde un emisor a un receptor, la notificación de errores, de la topología de la red de cualquier tipo.

2.1.14.3 Capa de red (Capa 3)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan encaminadores, aunque es más frecuente encontrar el nombre inglés *routers* y, en ocasiones enrutadores.

Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

2.1.14.4 Capa de transporte (Capa 4)

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmento. Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión.

2.1.14.5 Capa de sesión (Capa 5)

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre los dos computadores que están transmitiendo datos de cualquier índole.

Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

2.1.14.6 Capa de presentación (Capa 6)

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que el cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Esta capa también permite cifrar los datos y comprimirlos. En pocas palabras es un traductor.

2.1.14.7 Capa de aplicación (Capa 7)

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

2.1.14.7.1 Formato de los datos

Estos datos reciben una serie de nombres y formatos específicos en función de la capa en la que se encuentren.

Estos datos reciben una serie de nombres y formatos específicos en función de la capa en la que se encuentren, debido a como se describió anteriormente la adhesión de una serie de encabezados e información final. Los formatos de información son los que muestra el gráfico:

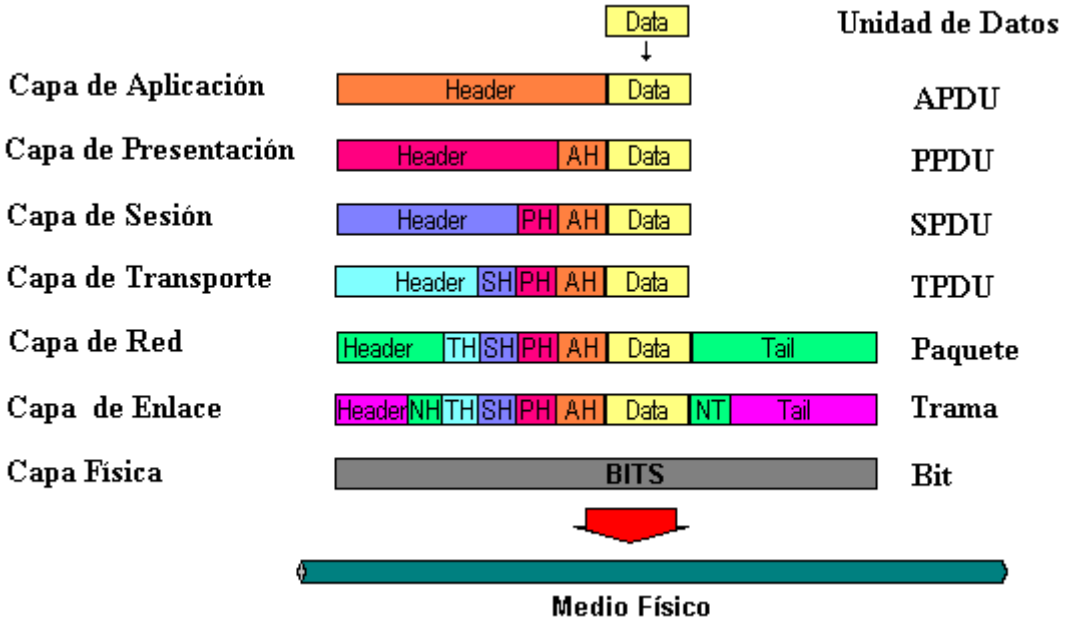

Figura 2-10: Modelo OSI

Fuente: http://es.wikipedia.org/wiki/Modelo_OSI

APDU

Unidad de datos en la capa de aplicación *(Capa 7)*.

PPDU

Unidad de datos en la capa de presentación *(Capa 6)*.

SPDU

Unidad de datos en la capa de sesión *(Capa 5)*.

TPDU

(Segmento)

Unidad de datos en la capa de transporte *(Capa 4)*.

Paquete o Datagrama

Unidad de datos en el nivel de red *(Capa 3)*.

Trama

Unidad de datos en la capa de enlace *(Capa 2)*.

Bits

Unidad de datos en la capa física *(Capa 1)*.

PDU[8]

Protocol Data Units, Unidades de Datos de Protocolo. Se utiliza para el intercambio entre unidades parejas, dentro de una capa del modelo OSI.

2.1.15 MODELO TCP/IP[9]

TCP/IP es un conjunto de protocolos. La sigla TCP/IP significa "Protocolo de control de transmisión/Protocolo de Internet" y se pronuncia "T-C-P-I-P". Proviene de los nombres de dos protocolos importantes del conjunto de protocolos, es decir, del protocolo TCP y del protocolo IP.

En algunos aspectos, TCP/IP representa todas las reglas de comunicación para Internet y se basa en la noción de dirección IP, es decir, en la idea de brindar una dirección IP a cada equipo de la red para poder enrutar paquetes de datos. Debido a que el conjunto de protocolos TCP/IP originalmente se creó con fines militares, está diseñado para cumplir con una cierta cantidad de criterios, entre ellos:

- Dividir mensajes en paquetes;
- Usar un sistema de direcciones;
- Enrutar datos por la red;
- Detectar errores en las transmisiones de datos.

[8] http://es.wikipedia.org/wiki/PDU
[9] http://es.kioskea.net/contents/internet/tcpip.php3

El conocimiento del conjunto de protocolos TCP/IP no es esencial para un simple usuario, de la misma manera que un espectador no necesita saber cómo funciona su red audiovisual o de televisión. Sin embargo, para las personas que desean administrar o brindar soporte técnico a una red TCP/IP, su conocimiento es fundamental.

Para poder aplicar el modelo TCP/IP en cualquier equipo, es decir, independientemente del sistema operativo, el sistema de protocolos TCP/IP se ha dividido en diversos módulos. Cada uno de éstos realiza una tarea específica. Además, estos módulos realizan sus tareas uno después del otro en un orden específico, es decir que existe un sistema estratificado. Ésta es la razón por la cual se habla de modelo de capas.

El término capa se utiliza para reflejar el hecho de que los datos que viajan por la red atraviesan distintos niveles de protocolos. Por lo tanto, cada capa procesa sucesivamente los datos (paquetes de información) que circulan por la red, les agrega un elemento de información (llamado *encabezado*) y los envía a la capa siguiente.

El modelo TCP/IP es muy similar al modelo OSI (modelo de 7 capas) que fue desarrollado por la Organización Internacional para la Estandarización (ISO) para estandarizar las comunicaciones entre equipos.

El modelo TCP/IP, influenciado por el modelo OSI, también utiliza el enfoque modular (utiliza módulos o capas), pero sólo contiene cuatro, las capas del modelo TCP/IP tienen tareas mucho más diversas que las del modelo OSI, considerando que ciertas capas del modelo TCP/IP se corresponden con varios niveles del modelo OSI.

Las funciones de las diferentes capas son las siguientes:

2.1.15.1 Capa de acceso a la red:

Específica la forma en la que los datos deben enrutarse, sea cual sea el tipo de red utilizado.

La capa de acceso a la red es la primera capa de la pila TCP/IP. Ofrece la capacidad de acceder a cualquier red física, es decir, brinda los recursos que se deben implementar para transmitir datos a través de la red.

Por lo tanto, la capa de acceso a la red contiene especificaciones relacionadas con la transmisión de datos por una red física, cuando es una red de área local (Red en anillo, Ethernet, FDDI), conectada mediante línea telefónica u otro tipo de conexión a una red. Trata los siguientes conceptos:

- Enrutamiento de datos por la conexión;
- Coordinación de la transmisión de datos (sincronización);
- Formato de datos;
- Conversión de señal (análoga/digital);
- Detección de errores a su llegada.

Afortunadamente, todas estas especificaciones son invisibles al ojo del usuario, ya que en realidad es el sistema operativo el que realiza estas tareas, mientras los drivers de hardware permiten la conexión a la red (por ejemplo, el driver de la tarjeta de red).

2.1.15.2 Capa de Internet:

Es responsable de proporcionar el paquete de datos (datagrama).

La capa de Internet es la capa "más importante" (si bien todas son importantes a su manera), ya que es la que define los datagramas y administra las nociones de direcciones IP.

Permite el enrutamiento de datagramas (paquetes de datos) a equipos remotos junto con la administración de su división y ensamblaje cuando se reciben.

La capa de Internet contiene 5 protocolos:

- el protocolo IP;
- el protocolo ARP;
- el protocolo ICMP;
- el protocolo RARP;
- el protocolo IGMP.

Los primeros tres protocolos son los más importantes para esta capa.

2.1.15.3 Capa de transporte:

Brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión.

Los protocolos de las capas anteriores permiten enviar información de un equipo a otro. La capa de transporte permite que las aplicaciones que se ejecutan en equipos remotos puedan comunicarse. El problema es identificar estas aplicaciones.

De hecho, según el equipo y su sistema operativo, la aplicación puede ser un programa, una tarea, un proceso, etc. Además, el nombre de la aplicación puede variar de sistema en sistema. Es por ello que se ha implementado un sistema de numeración para poder asociar un tipo de aplicación con un tipo de datos. Estos identificadores se denominan puertos.

La capa de transporte contiene dos protocolos que permiten que dos aplicaciones puedan intercambiar datos independientemente del tipo de red (es decir, independientemente de las capas inferiores). Estos dos protocolos son los siguientes:

TCP, un protocolo orientado a conexión que brinda detección de errores;

UDP, un protocolo no orientado a conexión en el que la detección de errores es obsoleta.

2.1.15.4 Capa de aplicación:

Incorpora aplicaciones de red estándar (Telnet, SMTP, FTP, etc.).
La capa de aplicación se encuentra en la parte superior de las capas del protocolo TCP/IP. Contiene las aplicaciones de red que permiten la comunicación mediante las capas inferiores. Por lo tanto, el software en esta capa se comunica mediante uno o dos protocolos de la capa inferior (la capa de transporte), es decir, TCP o UDP.

Existen diferentes tipos de aplicaciones para esta capa, pero la mayoría son servicios de red o aplicaciones brindadas al usuario para proporcionar la interfaz con el sistema operativo. Se pueden clasificar según los servicios que brindan:

- servicios de administración de archivos e impresión (transferencia).
- servicios de conexión a la red.
- servicios de conexión remota.
- diversas utilidades de Internet.

2.1.16 Comparación Modelo OSI y TCP/IP[10]

Si comparamos los modelos TCP/IP y el modelo OSI, vemos que tienen similitudes y diferencias.

[10] http://www.thehouseofblogs.com/articulo/comparacion_modelo_osi_y_tcpip-4501.html

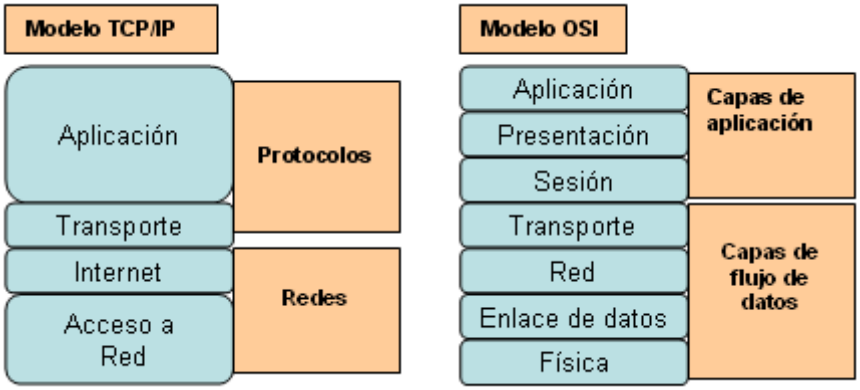

Figura 2-11: Comparación entre Modelo OSI y TCP/IP

Fuente: http://www.thehouseofblogs.com/articulo/comparacion_modelo_osi_y_tcpip-4501.html

Diferencias

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en una sola capa.
- TCP/IP es más simple porque contiene menos capas.
- TCP/IP contiene protocolos sobre los cuales se desarrolló Internet. En comparación, las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque se utilice como guía.

Similitudes

- Ambos modelos se dividen en capas.
- Ambos modelos poseen una capa de aplicación aunque ofrecen servicios muy distintos.
- Ambos modelos poseen una capa de transporte y de red similares.
- Ambos modelos utilizan tecnología de conmutación por paquetes y no de conmutación por circuitos.
- Ambos modelos deben ser conocidos por los profesionales de networking.

2.1.17 ESTANDARES[11]

Un estándar, tal como lo define la ISO "son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito". Por lo tanto un estándar de telecomunicaciones "es un conjunto de normas y recomendaciones técnicas que regulan la transmisión en los sistemas de comunicaciones". Queda bien claro que los estándares deberán estar documentados, es decir escritos en papel, con objeto que sean difundidos y captados de igual manera por las entidades o personas que los vayan a utilizar.

2.1.17.1 Tipos de Estándares

Existen tres tipos de estándares: de facto, de jure y los propietarios. Los estándares de facto son aquellos que tienen una alta penetración y aceptación en el mercado, pero aún no son oficiales.
Un estándar de jure u oficial, en cambio, es definido por grupos u organizaciones oficiales tales como la ITU, ISO, ANSI, entre otras.

La principal diferencia en cómo se generan los estándares de jure y facto, es que los estándares de jure son promulgados por grupos de gente de diferentes áreas del conocimiento que contribuyen con ideas, recursos y otros elementos para ayudar en el desarrollo y definición de un estándar específico. En cambio los estándares de facto son promulgados por comités "guiados" de una entidad o compañía que quiere sacar al mercado un producto o servicio; sí tiene éxito es muy probable que una Organización Oficial lo adopte y se convierta en un estándar de jure.

Por otra parte, también existen los "estándares" propietarios que son propiedad absoluta de una corporación u entidad y su uso todavía no logra una alta penetración en el mercado. Cabe aclarar que existen muchas compañías que

[11] http://www.eveliux.com/mx/estandares-de-telecomunicaciones.php

trabajan con este esquema sólo para ganar clientes y de alguna manera "atarlos" a los productos que fabrica. Si un estándar propietario tiene éxito, al lograr más penetración en el mercado, puede convertirse en un estándar de facto e inclusive convertirse en un estándar de jure al ser adoptado por un organismo oficial.

Un ejemplo clásico del éxito de un estándar propietario es el conector RS-232, concebido en los años 60's por la EIA (Electronics Industries Association) en Estados Unidos. La amplia utilización de la interfase EIA-232 dio como resultado su adopción por la ITU, quién describió las características eléctricas y funcionales de la interfase en las recomendaciones V.28 y V.24 respectivamente. Por otra parte las características mecánicas se describen en la recomendación 2110 de la ISO, conocido comúnmente como ISO 2110.

2.1.17.2 Tipos de Organizaciones de Estándares

Básicamente, existen dos tipos de organizaciones que definen estándares: Las organizaciones oficiales y los consorcios de fabricantes.

El primer tipo de organismo está integrado por consultores independientes, integrantes de departamentos o secretarías de estado de diferentes países u otros individuos. Ejemplos de este tipo de organizaciones son la ITU, ISO, ANSI, IEEE, IETF, IEC, entre otras.

Los consorcios de fabricantes están integrados por compañías fabricantes de equipo de comunicaciones o desarrolladores de software que conjuntamente definen estándares para que sus productos entren al mercado de las telecomunicaciones y redes (e.g. ATM Forum, Frame Relay Forum, Gigabit Ethernet Alliance, ADSL Forum, etc). Una ventaja de los consorcios es que pueden llevar más rápidamente los beneficios de los estándares promulgados al usuario final, mientras que las organizaciones oficiales tardan más tiempo en liberarlos.

Un ejemplo característico es la especificación 100 Mbps (Fast Ethernet 100Base-T). La mayoría de las especificaciones fueron definidas por la Fast Ethernet Alliance, quién transfirió sus recomendaciones a la IEEE. La totalidad de las especificaciones fueron liberadas en dos años y medio. En contraste, a la ANSI le llevó más de 10 años liberar las especificaciones para FDDI (Fiber Distributed Data Interface).

Otro aspecto muy importante de los consorcios de fabricantes es que éstos tienen un contacto más cercano con el mundo real - y productos reales. Esto reduce el riesgo de crear especificaciones que son demasiado ambiciosas, complicadas, y costosas de implementar. El modelo de capas OSI (Open Systems Interconnect) de la organización ISO es el ejemplo clásico de este problema. La ISO empezó a diseñarlas a partir de una hoja de papel en blanco tratando de diseñar estándares para un mundo ideal sin existir un impulso comercial para definirlas. En cambio, los protocolos del conjunto TCP/IP fueron desarrollados por personas que tenían la imperiosa necesidad de comunicarse, ese fue su éxito. Los consorcios de fabricantes promueven la interoperatividad teniendo un amplio conocimiento del mercado.

En Estados Unidos, donde se aglutinan la mayoría de las organizaciones, la mejor manera para saber si una organización de estándares es oficial consiste en conocer si la organización está avalada por la ISO. La ANSI, IEEE y IETF, todas ellas están reconocidas por la ISO y por lo tanto son organismos oficiales. En el resto del mundo, aquellas organizaciones avaladas por la ITU o ISO son organizaciones oficiales.

A continuación se describirán brevemente algunas de las organizaciones de estándares más importantes.

2.1.17.2.1 La Unión Internacional de Telecomunicaciones

La ITU es el organismo oficial más importante en materia de estándares en telecomunicaciones y está integrado por tres sectores o comités: el primero de

ellos es la ITU-T (antes conocido como CCITT, Comité Consultivo Internacional de Telegrafía y Telefonía), cuya función principal es desarrollar bosquejos técnicos y estándares para telefonía, telegrafía, interfases, redes y otros aspectos de las telecomunicaciones. La ITU-T envía sus bosquejos a la ITU y ésta se encarga de aceptar o rechazar los estándares propuestos. El segundo comité es la ITU-R (antes conocido como CCIR, Comité Consultivo Internacional de Radiocomunicaciones), encargado de la promulgación de estándares de comunicaciones que utilizan el espectro electromagnético, como la radio, televisión UHF/VHF, comunicaciones por satélite, microondas, etc. El tercer comité ITU-D, es el sector de desarrollo, encargado de la organización, coordinación técnica y actividades de asistencia

2.1.17.2.2 La IEEE

Fundada en 1884, la IEEE es una sociedad establecida en los Estados Unidos que desarrolla estándares para las industrias eléctricas y electrónicas, particularmente en el área de redes de datos. Los profesionales de redes están particularmente interesados en el trabajo de los comités 802 de la IEEE. El comité 802 (80 porque fue fundado en el año de 1980 y 2 porque fue en el mes de febrero) enfoca sus esfuerzos en desarrollar protocolos de estándares para la interface física de la conexiones de las redes locales de datos, las cuales funcionan en la capa física y enlace de datos del modelo de referencia OSI. Estas especificaciones definen la manera en que se establecen las conexiones de datos entre los dispositivos de red, su control y terminación, así como las conexiones físicas como cableado y conectores.

2.1.17.2.3 La Organización Internacional de Estándares (ISO)

La ISO es una organización no-gubernamental establecida en 1947, tiene representantes de organizaciones importantes de estándares alrededor del mundo y actualmente conglomera a más de 100 países. La misión de la ISO es "promover el desarrollo de la estandarización y actividades relacionadas con el

propósito de facilitar el intercambio internacional de bienes y servicios y para desarrollar la cooperación en la esfera de la actividad intelectual, científica, tecnológica y económica". Los resultados del trabajo de la ISO son acuerdos internacionales publicados como estándares internacionales. Tanto la ISO como la ITU tienen su sede en Suiza.

ALGUNAS ORGANIZACIONES DE ESTANDARES

ORGANISMO	SIGNIFICADO	ENFOQUE	URL
ADSL Forum	Asymmetric Digital Subscriber Line	Tecnología ADSL	www.adsl.com
ANSI	American National Standards Institute	LANs y WANs	www.ansi.org
ATM Forum	Asynchronous Transfer Mode	Tecnología ATM	www.adsl.com
ETSI	European Telecommunications Standards Institute	Telecomunicaciones	www.etsi.org
FR Forum	Frame Relay	Frame Relay	www.frforum.com
GEA	Gigabit Ethernet Alliance	Tecnología Gigabit Ethernet	www.gigabit-ethernet.org
IEEE	Institute of Electrical and Electronics Engineers	LANs y WANs	www.ieee.org
IETF	Internet Engineering Task Force	Internet	www.ietf.org
IMTC	International Multimedia Teleconferencing Consortium	Tele-videoconferencia	www.imtc.org
ISO	International Organization for Standarization	Tecnologías de la Información	www.iso.ch
ITU	International Telecommunications Union	Telecomunicaciones	www.itu.ch
NTIA	National Telecommunications Industry Association	Telecomunicaciones	www.ntia.ch
PCIA	Personal Communications	PCS	www.pcia.com

	Industry Association		
SANS	System Administration Network Security	Seguridad en redes	www.sans.org
TIA	Telecommunications Industry Association	Telecomunicaciones	www.industry.net/tia
W3C	World Wide Web Consortium	Tecnologías Web	www.w3c.org

Tabla 2-1: Organizaciones de Estándares
Fuente: http://www.eveliux.com/mx/estandares-de-telecomunicaciones.php

2.1.17.3 Un nuevo Estándar: IP Próxima Generación[12]

Los aspectos generation IPng son:

En el aspecto del nuevo esquema de Direcciones, este permitiría un mayor número de direcciones, ya que se está ampliando el tamaño de la dirección de 32 bits a 128 bits. Soporte de direcciones Jerárquicas Largas. Uso de Direcciones en *Cluster* que le permiten el enrutamiento de acuerdo con políticas preestablecidas. Tiene previsto además la multiemisión de direcciones (*multicast adresses*), incluyendo una dirección "*anycast address*", la cual permite el envío de un "*packet*" a cualquiera de un número de nodos.

La estructura de direcciones fue también diseñada para soportar el manejo de direcciones de otros conjuntos de protocolos de Internet. El beneficio de este aspecto radicaría en que facilitaría la migración desde otros protocolos al nuevo IPng.

Desde el punto de vista de la Red, habría características incorporadas en la forma de encripción e identificación de usuario. Manejaría además la configuración automática de redes.

En cuanto al manejo de tráfico, se incorporarían características que le permitirían manejar tráfico sensible a los retrasos.

IPng está propuesto como el nuevo Protocolo de Internet que reemplazará la versión de IP actual también conocida como IPv4. El nuevo nombre previsto para la nueva versión del Protocolo IP sería IPv6, en donde el 6 corresponde al número de la nueva versión.

La propuesta del nuevo IPpg proviene de los Directores de Área de la IETF (*Internet Engineering Task Force*), y fué propuesta en la reunión de la IETF de Julio 25 de 1994, llevada a cabo en Toronto, Canadá.

IPpg no se puede considerar como una actualización del actual protocolo IPv4, teniendo en cuenta que su direccionamiento es totalmente diferente, que sus encabezamientos son mucho más especializados y adicionalmente más ligeros, que provee más opciones incluyendo control de flujo y seguridad, que soporta movilidad del Host, auto-configuración, y algunas otras características, por todas estas razones, se puede considerar que efectivamente es un nuevo protocolo.

2.1.17.4 DIRECCIONAMIENTO IPV4 e IPV6[13]

2.1.17.4.1 IPV6

Con un octeto (ocho bits de la forma 00010111) se pueden representar los números de 0 a 255. Por tanto las direcciones IPv4 se componen de cuatro octetos, o 32 bits, lo cual genera los cuatro millones y pico de direcciones.

En IPv6 las direcciones se componen de 16 octetos, es decir 128 bits. Esto daría lugar a 2128 direcciones, más o menos 340 sextillones. No obstante, esta cifra no se alcanza, ya que parte de los dígitos identifican el tipo de dirección, con lo que se quedan en 3800 millones. En cualquier caso se garantiza que no se acabarán en un plazo razonable.

---

[12] http://members.tripod.com/a_pizano/html/cap4.html#Top
[13] http://html.rincondelvago.com/transmision-de-datos_ipv4-e-ipv6_dns.html

Hay tres tipos de direcciones: *unicast*, *anycast* y *multicast*. Las direcciones unicast identifican un solo destino. Un paquete que se envía a una dirección *unicast* llega sólo al ordenador al que corresponda. En el caso de las direcciones *anycast* se trata de un conjunto de ordenadores o dispositivos, que pueden pertenecer a nodos diferentes. Si se envía un paquete a una de estas direcciones lo recibirá el ordenador más cercano de entre las rutas posibles. Las direcciones *multicast* definen un conjunto de direcciones pertenecientes también a nodos diferentes, pero ahora los paquetes llegan a todas las máquinas identificadas por esa dirección.

2.1.17.4.1.1 Representación

Para representar las direcciones IPv6 como cadenas de texto (en lugar de ceros y unos) hay diferentes reglas. La primera se denomina preferred form y consiste en listar la dirección completa como 8 números hexadecimales de cuatro cifras (8 paquetes de 16 bits):

FEDC:2A5F:709C:216:AEBC:97:3154:3D12
1030:2A9C:0:0:0:500:200C:3A4

La otra posibilidad es la forma comprimida o compressed form, en la que las cadenas que sean cero se sustituyen por un par de dos puntos "::" que indican que hay un grupo de ceros.

Por ejemplo:

FF08:0:0:0:0:0:209A:61 queda FF08::209A:61
0:0:0:0:0:0:0:1 queda ::1

Por último se pueden escribir en forma mixta, con las primeras cifras en hexadecimal y las últimas (las correspondientes a IPv4) en decimal:

0:0:0:0:0:0:193.136.239.163
::193.136.239.163

2.1.17.4.2 IPV4

Para identificar cada máquina en el internet, se le asigna un número denominado dirección internet o dirección IP. Este número es asignado de tal forma que se consigue una gran eficiencia al encaminar paquetes, ya que codifica la información de la red en la que está conectado, además de la identificación del *host* en concreto.

Cada dirección internet tiene una longitud fija de 32 bits. Los bits de las direcciones IP de todos los host de una red determinada comparten un prefijo común. Conceptualmente, cada dirección IP es una pareja formada por identidad de red-identidad de host, donde la identidad de red identifica a la red, e identidad de host, a un host determinado dentro de esa red.

Para que exista una flexibilidad en la asignación de direcciones, existen tres formatos básicos de representación de direcciones. La elección de uno de estos formatos dependerá del tamaño de la red. Además de los tres formatos básicos, existe uno para *multicasting*, usado para envío de mensajes a un grupo de hosts, y otro reservado para futuro uso.

La estructura de los diferentes formatos es la que sigue:

Clase A:

1	Identificador de red	Identificador de host
	7 bits	24 bits

Tabla 2-2: Clase A

Fuente: http://html.rincondelvago.com/transmision-de-datos_ipv4-e-ipv6_dns.html

Clase B:

1	0	Identificador de red	Identificador de host
		14 bits	16 bits

Tabla 2-3: Clase B

Fuente: http://html.rincondelvago.com/transmision-de-datos_ipv4-e-ipv6_dns.html

Clase C:

1	1	0	Identificador de red	Identificador de host
			21 bits	8 bits

Tabla 2-4: Clase C

Fuente: http://html.rincondelvago.com/transmision-de-datos_ipv4-e-ipv6_dns.html

Clase D:

1	1	1	0	Dirección multicast
				28 bits

Tabla 2-5: Clase D

Fuente: http://html.rincondelvago.com/transmision-de-datos_ipv4-e-ipv6_dns.html

Clase E:

1	1	1	1	0	Espacio reservado para futuro uso
					27 bits

Tabla 2-6: Clase E

Fuente: http://html.rincondelvago.com/transmision-de-datos_ipv4-e-ipv6_dns.html

Vemos que los primeros bits identifican la clase de dirección IP, que va seguido de un prefijo de identificación de red, y seguido de un identificador de host.
La clase D se usa para transmitir un mismo mensaje a un grupo de hosts determinado.

- La clase A se usa para grandes redes que tengan más de 216 (65536) hosts.

- La clase B se usa para redes de tamaño intermedio, entre 28 (256) y 216 hosts.
- Finalmente, la clase C corresponde a redes con menos de 256 hosts.
- El cuarto tipo, el D, se dedica a tareas de *multicasting*.

Para asegurar que la parte de identificación de red de una dirección internet es única, todas las direcciónes son asignadas por una autoridad central, el Centro de Informacion de Red (NIC, Network Information Center).

Esta autoridad central tan sólo asigna el prefijo de red de la dirección y delega la responsabilidad de asignar las direcciones de host individuales a la organización solicitante. A las redes de área local con pocos ordenadores (menos de 255) se le asignan direcciones de la clase C, pues se espera que surjan un gran número de ellas. A redes muy grandes, como ARPANET, se les asigna la clase A, ya que se espera que no surjan demasiadas.

A la hora de trabajar con direcciones IP, usamos la notación decimal. La dirección expresada de esta forma vendrá dada por cuatro enteros positivos separados por puntos, donde cada entero se corresponde con el valor de un octeto de la dirección IP.

2.2 CABLEADO ESTRUCTURADO[14]

Es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus. Las características e instalación de estos elementos se deben hacer en cumplimiento de estándares para que califiquen como cableado estructurado. El apego de las instalaciones de cableado estructurado a estándares trae consigo los beneficios de independencia de proveedor y protocolo (infraestructura genérica), flexibilidad de instalación, capacidad de crecimiento y facilidad de administración.

El cableado estructurado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local. Suele tratarse de cable de par trenzado de cobre, para redes de tipo IEEE 802.3. No obstante, también puede tratarse de fibra óptica o cable coaxial.

El tendido de cierta complejidad cuando se trata de cubrir áreas extensas tales como un edificio de varias plantas. En este sentido hay que tener en cuenta las limitaciones de diseño que impone la tecnología de red de área local que se desea implantar:

- La segmentación del tráfico de red.
- La longitud máxima de cada segmento de red.
- La presencia de interferencias electromagnéticas.
- La necesidad de redes locales virtuales.
- Etc.

Salvando estas limitaciones, la idea del cableado estructurado es simple:

- Tender cables en cada planta del edificio.
- Interconectar los cables de cada planta.

2.2.1 CARACTERISTICAS[15]

Entre las características generales de un sistema de cableado estructurado destacan las siguientes:

La configuración de nuevos puestos se realiza hacia el exterior desde un nodo central, sin necesidad de variar el resto de los puestos. Sólo se configuran las conexiones del enlace particular.
Con una plataforma de cableado, los ciclos de vida de los elementos que componen una oficina corporativa dejan de ser tan importantes. Las innovaciones

[14] http://es.wikipedia.org/wiki/Cableado_estructurado
[15] http://www.elprisma.com/apuntes/ingenieria_de_sistemas/cableadoestructurado/

de equipo siempre encontrarán una estructura de cableado que -sin grandes problemas- podrá recibirlos. Los ciclos de vida de un edificio corporativo se dividen así:

- Estructura del edificio: 40 años
- Automatización de oficina: 1-3 años
- Telecomunicaciones: 3-5 años
- Administración de edificio: 5-7 años

La localización y corrección de averías se simplifica ya que los problemas se pueden detectar en el ámbito centralizado.

Mediante una topología física en estrella se hace posible configurar distintas topologías lógicas tanto en bus como en anillo, simplemente reconfigurando centralizadamente las conexiones.

2.2.2 NORMAS [16]

Al ser el cableado estructurado un conjunto de cables y conectores, sus componentes, diseño y técnicas de instalación deben de cumplir con una norma que dé servicio a cualquier tipo de red local de datos, voz y otros sistemas de comunicaciones, sin la necesidad de recurrir a un único proveedor de equipos y programas.

De tal manera que los sistemas de cableado estructurado se instalan de acuerdo a la norma para cableado para telecomunicaciones, EIA/TIA/568-A, emitida en Estados Unidos por la Asociación de la industria de telecomunicaciones, junto con la asociación de la industria electrónica.

2.2.2.1 EIA/TIA568-A

[16] http://www.monografias.com/trabajos11/cabes/cabes.shtml

Estándar ANSI/TIA/EIA-568-A de Alambrado de Telecomunicaciones para Edificios Comerciales. El propósito de esta norma es permitir la planeación e instalación de cableado de edificios con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad.

ANSI/EIA/TIA emiten una serie de normas que complementan la 568-A, que es la norma general de cableado:

- Estándar ANSI/TIA/EIA-569-A de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales. Define la infraestructura del cableado de telecomunicaciones, a través de tubería, registros, pozos, trincheras, canal, entre otros, para su buen funcionamiento y desarrollo del futuro.
- EIA/TIA 570, establece el cableado de uso residencial y de pequeños negocios.
- Estándar ANSI/TIA/EIA-606 de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.
- EIA/TIA 607, define al sistema de tierra física y el de alimentación bajo las cuales se deberán de operar y proteger los elementos del sistema estructurado.

Las normas EIA/TIA fueron creadas como norma de industria en un país, pero se ha empleado como norma internacional por ser de las primeras en crearse. ISO/IEC 11801, es otra norma internacional.

Las normas ofrecen muchas recomendaciones y evitan problemas en la instalación del mismo, pero básicamente protegen la inversión del cliente.

2.2.3 ELEMENTOS[17]

2.2.3.1 Cableado Horizontal

[17] http://parla.com.mx/cableadoestructurado.htm

El cableado horizontal incorpora el sistema de cableado que se extiende desde la salida de área de trabajo de telecomunicaciones (Work Area Outlet, WAO) hasta el cuarto de telecomunicaciones.

Es la porción del cableado que se extiende desde el área de trabajo hasta el armario de telecomunicaciones. El término “horizontal” se utiliza porque típicamente este cableado se desplaza de una manera horizontal en el edificio.

El cableado horizontal es típicamente el más difícil de mantener debido a la complejidad de trabajo en una oficina en producción. Es sumamente necesario que se tome en cuenta no solo las necesidades actuales sino las futuras para no causar molestias a los usuarios en el trabajo diario.

El cableado horizontal consiste de dos elementos básicos:

- *Cable Horizontal y Hardware de Conexión. (también llamado "cableado horizontal").* Proporcionan los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones. Estos componentes son los "contenidos" de las rutas y espacios horizontales.
- *Rutas y Espacios horizontales. (también llamado "sistemas de distribución horizontal").* Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "contenedores" del cableado horizontal.

El cableado horizontal incluye:

- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo, "WAO" (Work Area Outlets).
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.

- Paneles de empate (patch) y cables de empate utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

El cableado horizontal típicamente:

- Contiene más cable que el cableado del backbone.
- Es menos accesible que el cableado del backbone.

2.2.3.1.1 Consideraciones de diseño

Los costos en materiales, mano de obra e interrupción de labores al hacer cambios en el cableado horizontal pueden ser muy altos. Para evitar estos costos, el cableado horizontal debe ser capaz de manejar una amplia gama de aplicaciones de usuario. La distribución horizontal debe ser diseñada para facilitar el mantenimiento y la relocalización de áreas de trabajo.

El cableado horizontal deberá diseñarse para ser capaz de manejar diversas aplicaciones de usuario incluyendo:

- Comunicaciones de voz (teléfono).
- Comunicaciones de datos.
- Redes de área local.

2.2.3.1.2 Topología:

- La topología del cableado siempre será de tipo estrella
- Un cable para cada salida en los puestos de trabajo
- Todos los cables de la corrida horizontal deben estar terminados en cajillas y paneles

2.2.3.1.3 Distancia del cable

La distancia horizontal máxima es de 90 metros independiente del cable utilizado.

Esta es la distancia desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones. Al establecer la distancia máxima se hace la previsión de 10 metros adicionales para la distancia combinada de cables de empate (3 metros) y cables utilizados para conectar equipo en el área de trabajo de telecomunicaciones y el cuarto de telecomunicaciones.

2.2.3.1.4 Tipos de cable

Los tres tipos de cable reconocidos por ANSI/TIA/EIA-568-A para distribución horizontal son:

- Par trenzado, cuatro pares, sin blindaje (UTP) de 100 ohmios, 22/24 AWG.
- Par trenzado, dos pares, con blindaje (STP) de 150 ohmios, 22 AWG.
- Fibra óptica fibras multimodo 62.5/125 mm.

El cable a utilizar por excelencia es el par trenzado sin blindaje UTP de cuatro pares categoría 5, 5e o 6. El cable coaxial de 50 ohmios se acepta pero no se recomienda en instalaciones nuevas.

2.2.3.2 Cableado del Backbone (Vertical)

El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios del edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas.

2.2.3.2.1 Funciones

- La función del cableado vertical es la interconexión de los diferentes cuartos de comunicaciones.
- El cableado vertical es típicamente menos costoso de instalar y debe poder ser modificado con más flexibilidad.

2.2.3.2.2 Topología

- La topología del cableado vertical debe ser típicamente una estrella.
- En circunstancias donde los equipos y sistemas solicitados exijan un anillo, este debe ser lógico y no físico.

2.2.3.2.3 Cables Reconocidos

- Cable UTP de 100 . Multipar
- Cable STP de 150 . Multipar
- Cable de múltiples Fibras Opticas 62.5/125 ?m.
- Cable de múltiples Fibras Opticas Monomodo (9/125 ?m).
- Combinaciones

2.2.3.2.4 Distancias

1. Dentro del Edificio

    A. Cobre 90mts
    B. Fibra Optica 500 mts

- Entre Edificios

    - Cobre 800 mts
    - Fibra Optica Multimodo 2Km
    - Fibra Optica Monomodo 3Km.

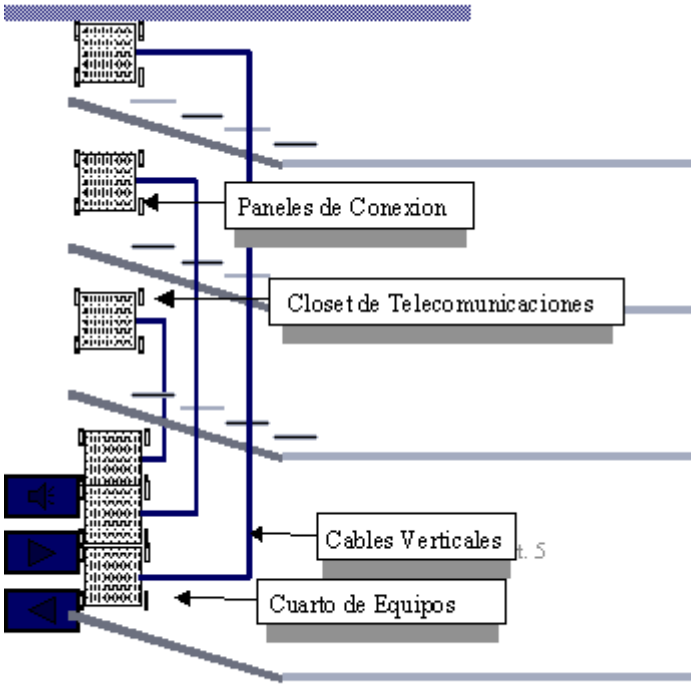

Figura 2-12: Diagrama Cableado Estructurado Vertical

Fuente: http://nuevamericableado.blogspot.com/2008/06/sistema-de-cableado-estructurado_17.html

2.2.3.3 Cuarto de Telecomunicaciones

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones.

El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que pueda haber en un edificio.

2.2.3.4 Cuarto de Equipo

El cuarto de equipo es un espacio centralizado de uso específico para equipo de telecomunicaciones tal como central telefónica, equipo de cómputo y/o conmutador de video. Varias o todas las funciones de un cuarto de telecomunicaciones pueden ser proporcionadas por un cuarto de equipo. Los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen. Los cuartos de equipo incluyen espacio de trabajo para personal de telecomunicaciones. Todo edificio debe contener un cuarto de telecomunicaciones o un cuarto de equipo. Los requerimientos del cuarto de equipo se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

2.2.3.5 Cuarto de Entrada de Servicios

El cuarto de entrada de servicios consiste en la entrada de los servicios de telecomunicaciones al edificio, incluyendo el punto de entrada a través de la pared y continuando hasta el cuarto o espacio de entrada. El cuarto de entrada puede incorporar el "backbone" que conecta a otros edificios en situaciones de campus.

Los requerimientos de los cuartos de entrada se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

2.2.3.6 Sistema de Puesta a Tierra y Puenteado

El sistema de puesta a tierra y puenteado establecido en el estándar ANSI/TIA/EIA-607 es un componente importante de cualquier sistema de cableado estructurado moderno.

2.2.4 CATEGORIAS[18]

Las normas de cableado estructurado especifican topologías genéricas de instalación y diseño que se caracterizan por una "categoría" o "clase" para llevar a

[18] http://portal.cableando.com/index.php/categorias-de-cableados-de-redes-estructuradas

cabo la transmisión. Estas normas de cableado son tomadas posteriormente como referencia en estándares de aplicación, desarrollados por comités como IEEE y ATM, como el nivel mínimo de características necesarias para asegurar la operación de las aplicaciones. Al especificar un cableado estructurado conforme a las normas se obtienen muchas ventajas. Éstas incluyen la garantía de operación de las aplicaciones, la flexibilidad de las elecciones de cables y de conectividad que son interoperables y compatibles con categorías anteriores, y un diseño y topología de cableado estructurado reconocidos universalmente por los profesionales responsables del manejo y las gestión de los sistemas.A continuación hacemos un pequeño resumen explicativo con las características más destacables de las que para nosotros son las categorías de cableado que a día de hoy están funcionando en nuestro mercado.

En orden tecnológico y a la vez, en orden cronológico comentamos la Categoria de Cableado CAT 7 como la más potente y actual y la CAT 5e como una categoría de cableado que ya ha pasado a un segundo nivel tecnológico.

2.2.4.1 Categoría 7

En cableados, la Categoría 7 o Clase F (ISO/IEC 11801:2002) especifica una gama de frecuencias de 1 a 600 Mhz en 100 metros de cableado de par trenzado totalmente apantallado.

Los cables que cumplen la Categoría 7 o Clase F, contienen cuatro pares individualmente apantallados en el interior y un apantallado general, son los llamados Cables de par Trenzado Apantallado/Lamina (S/FTP)o Cable de par Trenzado Lamina/Lamina (F/FTP).

Existe una Clase Fa pendiente, que se basa en el uso de cable S/FTP a 1000Mhz admitiendo así transmisiones a 10GBase-T.

En los dos tipos de cable, cada par trenzado está envuelto en una lámina.

En el cable S/FTP, los cuatro pares están cubiertos con una malla metálica general y en el cable F/FTP, los cuatro pares están recubiertos por una lámina.

El cable de Categoría 7 o Clase F se puede terminar con los conectores especificados en IEC 6063-7-7 e IEC 61076-3-104. Uno es un conector GC-45 compatible con el RJ-45 y el otro es el conector TERA, es un conector más habitual.

Los cables que están totalmente apantallados eliminan prácticamente todas las interferencias entre cables. Además, los cables son resistentes al ruido, por lo que los sistemas de cableado instalados cumpliendo la Categoría 7 o Clase F son idóneos para zonas de alta interferencia electromagnética, como por ejemplo instalaciones industriales o instalaciones para medicina.

2.2.4.2 Categoría 6a

La Categoría 6a es una propuesta 10Gigabit Ethernet (10-GbE) para transmisión por cobre al estándar CAT6.
El IEEE publicó un proyecto de norma (Estándar 803.3an) en octubre de 2004. El proyecto establece la transmisión de datos de 10-Gigabits a través de un cable d cobre de 4 pares hasta una distancia de 100 metros en cableado de cobre de Clase F o Clase E aumentada.

El cableado de Clase E requiere un esquema de codificación de línea y un sistema electrónico para obtener la transmisión de 10-Gpbs hasta 100 metros.
Los sistemas de Cableado CAT6 actuales admiten Ethernet de 10 Gigabits en distancias cortas.

La norma preliminar amplia las especificaciones técnicas del CAT6 de 250Mhz a 500Mhz y también proponen una nueva medición: Power Sum Alien Crosstalk a 500 Mhz.

Alien Crosstalk (ANEXT) es una señal acoplada en un par perturbado que se origina en la señal de un cable adyacente.

Para la eliminación practica del problema ANEXT, se puede utilizar un cable de CAT6a F/UTP.

La F indica recubrimiento exterior de lámina. Es un cable también muy adecuado para situaciones que requieren seguridad, ya que no emite señales.

El cable CAT6a F/UTP funciona bien en entornos con mucho ruido e IEM.

2.2.4.3 Categoría 6

Los Cableados que cumplen la de categoría 6, o Cat 6 o Clase E (ANSI/TIA/EIA-568-B.2-1) son instalaciones de cableado que cumplen lo especificado en el estándar de cables para Gigabit Ethernet y otros protocolos de redes que son compatibles con versiones anteriores, con los estándares de categoría 5/5e y categoría 3.

La categoría 6 posee características y especificaciones para crosstalk y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (*Gigabit Ethernet*) y alcanza frecuencias de hasta 250 MHz en cada par. El cable de categoría 6 contiene 4 pares de cable de cobre trenzado, al igual que estándares de cables de cobre anteriores.

Un canal completo (cable horizontal más cada final) está permitido a llegar a los 100 metros en extensión.

2.2.4.4 Categoría 5e

En nuevas instalaciones no es habitual trabajar con componentes de cableado de Categoría 5e puesto que las categorías superiores son muy competitivas a nivel económico y funcional y podemos decir que las categorías 5 y 5e son categorías que han pasado a una segunda línea tecnológica, aun así en una gran parte de las empresas se dispone de cableados de red en Cat5e que perfectamente pueden soportar aplicaciones a 1Gbits de velocidad.

Los requisitos de cableado de Categoría 5e/Clase D se publicaron por primera vez en 2000 y tenían por objeto normalizar la característica adicional a la CAT5 de transmisión para aplicaciones como 1000BASE-T, que utilizan esquemas de transmisión bidireccionales y enteramente de cuatro pares.

La norma añadió margen de maniobra a los límites del estándar de la Categoría 5 y caracterizó varios criterios nuevos de transmisión que se requerían para el soporte de Ethernet Gigabit en el caso más desfavorable de un canal de cuatro conectores (la aplicación 1000BASE-T fue originalmente destinada a operar con canales de Categoría 5, que sólo tienen dos conectores).

Para asegurar el cumplimiento de los márgenes adicionales del estándar CAT5, las especificaciones de la Categoría 5e/Clase D añadieron margen de maniobra a los parámetros de pérdida NEXT, pérdida ELFEXT y pérdida de retorno, y presentaron la caracterización de la diafonía utilizando suma de potencias, lo que aproxima la diafonía total presente cuando todos los pares están trabajando, como en un esquema de transmisión de cuatro pares.

2.3 REDES INALÁMBRICAS[19]

Una red inalámbrica es, como su nombre lo indica, una red en la que dos o más terminales (por ejemplo, ordenadores portátiles, agendas electrónicas, etc.) se pueden comunicar sin la necesidad de una conexión por cable.

Con las redes inalámbricas, un usuario puede mantenerse conectado cuando se desplaza dentro de una determinada área geográfica. Por esta razón, a veces se utiliza el término "movilidad" cuando se trata este tema.

Las redes inalámbricas se basan en un enlace que utiliza ondas electromagnéticas (radio e infrarrojo) en lugar de cableado estándar. Hay muchas tecnologías diferentes que se diferencian por la frecuencia de transmisión que utilizan, y el alcance y la velocidad de sus transmisiones.

Las redes inalámbricas permiten que los dispositivos remotos se conecten sin dificultad, ya se encuentren a unos metros de distancia como a varios kilómetros.

Asimismo, la instalación de estas redes no requiere de ningún cambio significativo en la infraestructura existente como pasa con las redes cableadas. Tampoco hay necesidad de agujerear las paredes para pasar cables ni de instalar portacables o conectores. Esto ha hecho que el uso de esta tecnología se extienda con rapidez.
Por el otro lado, existen algunas cuestiones relacionadas con la regulación legal del espectro electromagnético. Las ondas electromagnéticas se transmiten a través de muchos dispositivos (de uso militar, científico y de aficionados), pero son propensos a las interferencias. Por esta razón, todos los países necesitan regulaciones que definan los rangos de frecuencia y la potencia de transmisión que se permite a cada categoría de uso.

Además, las ondas hertzianas no se confinan fácilmente a una superficie geográfica restringida. Por este motivo, un hacker puede, con facilidad, escuchar una red si los datos que se transmiten no están codificados. Por lo tanto, se deben tomar medidas para garantizar la privacidad de los datos que se transmiten a través de redes inalámbricas.

2.3.1 VENTAJAS Y DESVENTAJAS[20]

Las principales ventajas que presentan las redes de este tipo son su libertad de movimientos, sencillez en la reubicación de terminales y la rapidez consecuente de instalación. La solución inalámbrica resuelve la instalación de una red en aquellos lugares donde el cableado resulta inviable, por ejemplo en edificios históricos o en grandes naves industriales, donde la realización de canaletas para cableado podría dificultar el paso de transportes, así como en situaciones que impliquen una gran movilidad de los terminales del usuario o la necesidad de disponer de vías alternativas por motivos de seguridad.

---

[19] http://es.kioskea.net/contents/wireless/wlintro.php3
[20] http://www.unincca.edu.co/boletin/indice.htm

Los inconvenientes que tienen las redes de este tipo se derivan fundamentalmente de encontrarnos en un periodo transitorio de introducción, donde faltan estándares, hay dudas que algunos sistemas pueden llegar a afectar a la salud de los usuarios, no está clara la obtención de licencias para las que utilizan el espectro radioeléctrico y son muy pocas las que presentan compatibilidad con los estándares de las redes fijas.

2.3.2 TIPOS DE REDES INALÁMBRICAS[21]

Las redes inalámbricas se pueden clasificar en diferentes tipos en función de las distancias a través de las que se pueden transmitir los datos.

2.3.2.1 Redes de área extensa inalámbricas (WWAN)

Las tecnologías WWAN permiten a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como ciudades o países, mediante el uso de antenas en varias ubicaciones o sistemas satélite que mantienen los proveedores de servicios inalámbricos. Las tecnologías WWAN actuales se conocen como sistemas de segunda generación (2G). Entre los sistemas 2G principales se incluyen Global System for Mobile Communications (GSM), Cellular Digital Packet Data (CDPD) y Code Division Multiple Access (CDMA). Los esfuerzos van encaminados a la transición desde redes 2G, algunas de las cuales tienen capacidades limitadas de movilidad y son incompatibles entre sí, a tecnologías de tercera generación (3G) que seguirían un estándar global y proporcionarían capacidades de movilidad internacional. La UIT está promoviendo activamente el desarrollo de una norma global para 3G.

2.3.2.2 Redes de área metropolitana inalámbricas (WMAN)

Las tecnologías WMAN permiten a los usuarios establecer conexiones inalámbricas entre varias ubicaciones dentro de un área metropolitana (por ejemplo, entre varios edificios de oficinas de una ciudad o en un campus

universitario), sin el alto coste que supone la instalación de cables de fibra o cobre y el alquiler de las líneas. Además, WMAN puede servir como copia de seguridad para las redes con cable, en caso de que las líneas alquiladas principales para las redes con cable no estén disponibles. WMAN utiliza ondas de radio o luz infrarroja para transmitir los datos. Las redes de acceso inalámbrico de banda ancha, que proporcionan a los usuarios acceso de alta velocidad a Internet, tienen cada vez mayor demanda. Aunque se están utilizando diferentes tecnologías, como el servicio de distribución multipunto de canal múltiple (MMDS) y los servicios de distribución multipunto locales (LMDS), el grupo de trabajo de IEEE 802.16 para los estándares de acceso inalámbrico de banda ancha sigue desarrollando especificaciones para normalizar el desarrollo de estas tecnologías.

2.3.2.3 Redes de área local inalámbricas (WLAN)

Las tecnologías WLAN permiten a los usuarios establecer conexiones inalámbricas dentro de un área local (por ejemplo, un edificio corporativo o campus empresarial, o en un espacio público como un aeropuerto). Las WLAN se pueden utilizar en oficinas temporales u otros espacios donde la instalación de extenso cableado sería prohibitivo, o para complementar una LAN existente de modo que los usuarios pueden trabajar en diferentes lugares dentro de un edificio a diferentes horas. Las WLAN pueden operar de dos formas distintas. En las WLAN de infraestructura, las estaciones inalámbricas (dispositivos con radiotarjetas de red o módems externos) se conectan a puntos de acceso inalámbrico que funcionan como puentes entre las estaciones y la red troncal existente. En las WLAN de igual a igual (ad hoc), varios usuarios dentro de un área limitada, como una sala de conferencias, pueden formar una red temporal sin utilizar puntos de acceso, si no necesitan obtener acceso a recursos de red.

En 1997, el IEEE aprobó la norma 802.11 para las WLAN, que especifica una velocidad de transferencia de datos de 1 a 2 megabits por segundo (Mbps). En la 802.11b, que está emergiendo como la nueva norma dominante, los datos se transfieren a una velocidad máxima de 11 Mbps a través de una banda de

[21] http://technet.microsoft.com/es-es/library/cc784756(WS.10).aspx

frecuencia de 2,4 gigahercios (GHz). Otra norma reciente es la 802.11a, que especifica una transferencia de datos a una velocidad máxima de 54 Mbps a través de una banda de frecuencia de 5 GHz.

2.3.2.4 Redes de área personal inalámbricas (WPAN)

Las tecnologías WPAN permiten a los usuarios establecer comunicaciones inalámbricas ad hoc para dispositivos (como PDA, teléfonos celulares y equipos portátiles) que se utilizan dentro de un espacio operativo personal (POS). Un POS es el espacio que rodea a una persona, hasta una distancia de 10 metros.

Actualmente, las dos tecnologías WPAN principales son Bluetooth y la luz infrarroja. Bluetooth es una tecnología de sustitución de cables que utiliza ondas de radio para transmitir datos a una distancia de hasta 30 pies. Los datos de Bluetooth se pueden transferir a través de paredes, bolsillos y maletines. El desarrollo de la tecnología de Bluetooth lo dirige el Grupo de interés general (SIG) de Bluetooth, que publicó la especificación de la versión 1.0 de Bluetooth en 1999. Otra posibilidad que tienen los usuarios para conectar dispositivos en un radio de acción muy cercano (1 metro o menos) es crear vínculos de infrarrojos.

Para normalizar el desarrollo de tecnologías WPAN, el IEEE ha establecido el grupo de trabajo 802.15 para las WPAN. Este grupo de trabajo está desarrollando una norma WPAN, basada en la especificación de la versión 1.0 de Bluetooth. Los objetivos principales en esta norma preliminar son baja complejidad, bajo consumo de energía, interoperabilidad y coexistencia con redes de 802.11.

2.3.3 SEGURIDAD EN LAS REDES INALÁMBRICAS[22]

Son muchos los motivos para preocuparnos por la seguridad de una red inalámbrica. Por ejemplo, queremos evitar compartir nuestro ancho de banda públicamente. A nadie con algo de experiencia se le escapa que las redes inalámbricas utilizan un medio inseguro para sus comunicaciones y esto tiene sus

[22] http://dns.bdat.net/seguridad_en_redes_inalambricas/c14.html

repercusiones en la seguridad. Tendremos situaciones en las que precisamente queramos compartir públicamente el acceso a través de la red inalámbrica, pero también tendremos que poder configurar una red inalámbrica para limitar el acceso en función de unas credenciales. También tenemos que tener en cuenta que las tramas circulan de forma pública y en consecuencia cualquiera que estuviera en el espacio cubierto por la red, y con unos medios simples, podría capturar las tramas y ver el tráfico de la red.

Para resolver los problemas de seguridad que presenta una red inalámbrica se tiene que, por un lado, garantizar el acceso mediante algún tipo de credencial a la red y por otro garantizar la privacidad de las comunicaciones aunque se hagan a través de un medio inseguro.

Una empresa no debería utilizar redes inalámbricas para sus comunicaciones si tiene información valiosa en su red que desea mantener segura y no ha tomado las medidas de protección adecuadas. Cuando utilizamos una página web para enviar un número de tarjeta de crédito deberemos, hacerlo siempre utilizando una web segura porque eso garantiza que se transmite cifrada. Pues en una red inalámbrica tendría que hacerse de una forma parecida para toda la información que circula, para que proporcione al menos la misma seguridad que un cable. Pensemos que en una red inalámbrica abierta se podría llegar a acceder a los recursos de red compartidos.

2.3.3.1 WEP

WEP (Wired Equivalent Privacy), que viene a significar Privacidad Equivalente a Cable, es un sistema que forma parte del estándar 802.11 desde sus orígenes. Es el sistema más simple de cifrado y lo admiten,creo, la totalidad de los adaptadores inalámbricos. El cifrado WEP se realiza en la capa MAC del adaptador de red inalámbrico o en el punto de acceso, utilizando claves compartidas de 64 o 128 bits. Cada clave consta de dos partes, una de las cuales la tiene que configurar el usuario/administrador en cada uno de los adaptadores o puntos de acceso de la red. La otra parte se genera automáticamente y se denomina vector de

inicialización (IV). El objetivo del vector de inicialización es obtener claves distintas para cada trama. Ahora vamos a ver una descripción del funcionamiento del cifrado WEP.

Cuando tenemos activo el cifrado WEP en cualquier dispositivo inalámbrico, bien sea una adaptador de red o un punto de acceso, estamos forzando que el emisor cifre los datos y el CRC de la trama 802.11. El receptor recoge y la descifra. Para no incurrir en errores de concepto, esto es sólo aplicable a comunicaciones estaciones 802.11, cuando el punto de acceso recoge una trama y la envía a través del cable, la envía sin cifrar. El cifrado se lleva a cabo partiendo de la clave compartida entre dispositivos que, como indicamos con anterioridad, previamente hemos tenido que configurar en cada una de las estaciones. En realidad un sistema WEP almacena cuatro contraseñas y mediante un índice indicamos cual de ellas vamos a utilizar en las comunicaciones.

El proceso de cifrado WEP agrega un vector de inicialización (IV) aleatorio de 24 bits concatenándolo con un la clave compartida para generar la llave de cifrado. Observamos como al configurar WEP tenemos que introducir un valor de 40 bits (cinco dígitos hexadecimales), que junto con los 24 bits del IV obtenemos la clave de 64 bits. El vector de inicialización podría cambiar en cada trama trasmitida.

WEP usa la llave de cifrado para generar la salida de datos que serán, los datos cifrados más 32 bits para la comprobación de la integridad, denominada ICV (integrity check value). El valor ICV se utiliza en la estación receptora donde se recalcula y se compara con el del emisor para comprobar si ha habido alguna modificación y tomar una decisión, que puede ser rechazar el paquete.

Para cifrar los datos WEP utiliza el algoritmo RC4, que básicamente consiste en generar un flujo de bits a partir de la clave generada, que utiliza como semilla, y realizar una operación XOR entre este flujo de bits y los datos que tiene que cifrar.

El valor IV garantiza que el flujo de bits no sea siempre el mismo. WEP incluye el IV en la parte no cifrada de la trama, lo que aumenta la inseguridad. La estación

receptora utiliza este IV con la clave compartida para descifrar la parte cifrada de la trama.

Lo más habitual es utilizar IV diferentes para transmitir cada trama aunque esto no es un requisito de 801.11. El cambio del valor IV mejora la seguridad del cifrado WEP dificultando que se pueda averiguar la contraseña capturando tramas, aunque a pesar de todo sigue siendo inseguro.

2.3.3.1.1 Debilidades de WEP

Las debilidades de WEP se basan en que, por un lado, las claves permanecen estáticas y por otro lado los 24 bits de IV son insuficientes y se transmiten sin cifrar. Aunque el algoritmo RC4 no esté considerado de los más seguros, en este caso la debilidad de WEP no es culpa de RC4, sino de su propio diseño.

Si tenemos un vector de inicialización de 24 bits tendremos 2^24 posibles IV distintos y no es difícil encontrar distintos paquetes generados con el mismo IV. Si la red tiene bastante tráfico estas repeticiones se dan con cierta frecuencia. Un atacante puede recopilar suficientes paquetes similares cifrados con el mismo IV y utilizarlos para determinar el valor del flujo de bits y de la clave compartida. El valor del IV se transmite sin cifrar por lo que es público. Esto puede parecer muy complicado, pero hay programas que lo hacen automáticamente y en horas o días averiguan la contraseña compartida. No olvidemos que aunque la red tenga poco tráfico el atacante puede generarlo mediante ciertas aplicaciones.

Una vez que alguien ha conseguido descifrar la contraseña WEP tiene el mismo acceso a la red que si pudiera conectarse a ella mediante cable. Si la red está configurada con un servidor DHCP, entonces el acceso es inmediato, y si no tenemos servidor DHCP pues al atacante le puede llevar cinco minutos más.

Vista la debilidad real de WEP lo ideal es que se utilizaran claves WEP dinámicas, que cambiaran cada cierto tiempo lo que haría materialmente imposible utilizar

este sistema para asaltar una red inalámbrica, pero 802.11 no establece ningún mecanismo que admita el intercambio de claves entre estaciones. En una red puede ser tedioso, simplemente inviable, ir estación por estación cambiando la contraseña y en consecuencia es habitual que no se modifiquen, lo que facilita su descifrado.

Algunos adaptadores sólo admiten cifrado WEP por lo que a pesar de su inseguridad puede ser mejor que nada. Al menos evitaremos conexiones en abierto incluso evitaremos conexiones y desconexiones a la red si hay varias redes inalámbricas disponibles.

2.3.3.2 TKIP

TKIP (Temporary Key Integrity Protocol) es un protocolo de gestión de claves dinámicas admitido por cualquier adaptador que permite utilizar una clave distinta para cada paquete transmitido. La clave se construye a partir de la clave base, la dirección MAC de la estación emisora y del número de serie del paquete como vector de inicialización.

Cada paquete que se transmite utilizando TKIP incluye un número de serie único de 48 bits que se incrementa en cada nueva transmisión para asegurar que todas las claves son distintas. Esto evita "ataques de colisión" que se basan en paquetes cifrados con la misma clave.

Por otro lado al utilizar el número de serie del paquete como vector de inicialización (IV), también evitamos IV duplicados. Además, si se inyectara un paquete con una contraseña temporal que se hubiese podido detectar, el paquete estaría fuera de secuencia y sería descartado.

En cuanto a la clave base, se genera a partir del identificador de asociación, un valor que crea el punto de acceso cada vez que se asocia una estación. Además del identificador de asociación, para generar la clave base se utilizan las

direcciones MAC de la estación y del punto de acceso, la clave de sesión y un valor aleatorio.

Como ve más adelante, la clave de sesión puede ser estática y compartida (PSK) por toda la red o bien, mediante 802.1X, transmitirla por un canal seguro.

2.3.3.3 CCMP

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) es un nuevo protocolo que utiliza AES como algoritmo criptográfico y proporciona integridad y confidencialidad.

CCMP se basa en el modo CCM del algoritmo de cifrado AES y utiliza llaves de 128 bits con vectores de inicialización de 48 bits.

CCMP consta del algoritmo de privacidad que es el "Counter Mode" (CM) y del algoritmo de integridad y autenticidad que es el "Cipher Block Chaining Message Authentication Code" (CBC-MAC).

CCMP es obligatorio sobre RSN (Robust Secure Network).

2.3.3.4 WPA[23]

WPA es la abreviatura de Wifi Protect Access, y consiste en un mecanismo de control de acceso a una red inalámbrica, pensado con la idea de eliminar las debilidades de WEP. También se le conoce con el nombre de TSN (Transition Security Network).

WPA utiliza TKIP (Temporal Key Integrity Protocol) para la gestión de las claves dinámicas mejorando notablemente el cifrado de datos, incluyendo el vector de inicialización. En general WPA es TKIP con 8021X. Por lo demás WPA funciona de una manera parecida a WEP pero utilizando claves dinámicas, utiliza el

[23] http://dns.bdat.net/seguridad_en_redes_inalambricas/x59.html

algoritmo RC4 para generar un flujo de bits que se utilizan para cifrar con XOR y su vector de inicialización (IV) es de 48 bits. La modificación dinámica de claves puede hacer imposible utilizar el mismo sistema que con WEP para abrir una red inalámbrica con seguridad WPA.

Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

2.3.3.5 WPA-PSK

Es el sistema más simple de control de acceso tras WEP, a efectos prácticos tiene la misma dificultad de configuración que WEP, una clave común compartida, sin embargo, la gestión dinámica de claves aumenta notoriamente su nivel de seguridad. PSK se corresponde con las iniciales de PreShared Key y viene a significar clave compartida previamente, es decir, a efectos del cliente basa su seguridad en una contraseña compartida.

WPA-PSK usa una clave de acceso de una longitud entre 8 y 63 caracteres, que es la clave compartida. Al igual que ocurría con WEP, esta clave hay que introducirla en cada una de las estaciones y puntos de acceso de la red inalámbrica. Cualquier estación que se identifique con esta contraseña, tiene acceso a la red.

Las características de WPA-PSK lo definen como el sistema, actualmente, más adecuado para redes de pequeñas oficinas o domésticas, la configuración es muy simple, la seguridad es aceptable y no necesita ningún componente adicional.

2.3.3.5.1 Debilidades de WPA-PSK

La principal debilidad de WPA-PSK es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en un contraseña siempre es susceptible de sufrir un ataque de fuera bruta, es decir ir comprobando contraseñas, aunque

dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas. Debemos pensar que hay un momento de debilidad cuando la estación establece el diálogo de autenticación. Este diálogo va cifrado con las claves compartidas, y si se entienden entonces se garantiza el acceso y se inicia el uso de claves dinámicas. La debilidad consiste en que conocemos el contenido del paquete de autenticación y conocemos su valor cifrado. Ahora lo que queda es, mediante un proceso de ataque de diccionario o de fuerza bruta, intentar determinar la contraseña.

2.3.3.6 WPA empresarial

En redes corporativas resultan imprescindibles otros mecanismos de control de acceso más versátiles y fáciles de mantener como por ejemplo los usuarios de un sistema identificados con nombre/contraseña o la posesión de un certificado digital. Evidentemente el hardware de un punto de acceso no tiene la capacidad para almacenar y procesar toda esta información por lo que es necesario recurrir a otros elementos de la red cableada para que comprueben unas credenciales. Ahora bien, parece complicado que un cliente se pueda validar ante un componente de la red por cable si todavía no tenemos acceso a la red, parece el problema del huevo y la gallina. En este punto es donde entra en juego el IEEE 802.1X, que describimos a continuación, para permitir el tráfico de validación entre un cliente y una máquina de la de local. Una vez que se ha validado a un cliente es cuando WPA inicia TKIP para utilizar claves dinámicas.

Los clientes WPA tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación WPA pueden ser, entre otros, EAP-TLS, PEAP, EAP-TTLS que describimos más adelante.

2.3.3.7 802.1X[24]

[24] http://dns.bdat.net/seguridad_en_redes_inalambricas/x75.html

Debido a las carencias de 802.11 ha sido necesario establecer una nueva normativa estándar que permita tanto la autenticación como el intercambio dinámico de contraseñas, de forma fácil y segura.

El estándar IEEE 802.1X proporciona un sistema de control de dispositivos de red, de admisión, de tráfico y gestión de claves para dispositivos tos en una red inalámbrica. 802.1X se basa en puertos, para cada cliente dispone de un puerto que utiliza para establecer una conexión punto a punto. Mientras el cliente no se ha validado este puerto permanece cerrado. Cada una de estas funcionalidades se puede utilizar por separado, permitiendo a WPA, por ejemplo, utilizar 802.1X para aceptar a una estación cliente.

Para el control de admisión 802.1X utiliza un protocolo de autenticación denominado EAP y para el cifrado de datos CCMP y esto es lo que se conoce como RSN (Robust Secure Network) o también WPA2. No todo el hardware admite CCMP.

2.3.3.8 EAP[25]

Hemos visto que 802.1X utiliza un protocolo de autenticación llamado EAP (Extensible Authentication Protocol) que admite distintos métodos de autenticación como certificados, tarjetas inteligentes, ntlm, Kerberos, ldap, etc. En realidad EAP actúa como intermediario entre un solicitante y un motor de validación permitiendo la comunicación entre ambos.

El proceso de validación está conformado por tres elementos, un solicitante que quiere ser validado mediante unas credenciales, un punto de acceso y un sistema de validación situado en la parte cableada de la red. Para conectarse a la red, el solicitante se identifica mediante una credenciales que pueden ser un certificado digital, una pareja nombre/usuario u otros datos. Junto con las credenciales, el cliente solicitante tiene que añadir también qué sistema de validación tiene que utilizar. Evidentemente no podemos pretender que el punto de acceso disponga

[25] http://dns.bdat.net/seguridad_en_redes_inalambricas/x80.html

del sistema de validación. Por ejemplo, si queremos utilizar como credenciales los usuarios de un sistema, será el punto de acceso el que tendrá que preguntar al sistema si las credenciales son correctas. En general EAP actúa de esta forma, recibe una solicitud de validación y la remite a otro sistema que sepa como resolverla y que formará parte de la red cableada. De esta forma vemos como el sistema EAP permite un cierto tráfico de datos con la red local para permitir la validación de un solicitante. El punto de acceso rechaza todas las tramas que no estén validadas, que provengan de un cliente que no se he identificado, salvo aquéllas que sean una solicitud de validación. Estos paquetes EAP que circulan por la red local se denominan EAPOL (EAP over LAN). Una vez validado, el punto de acceso admite todo el tráfico del cliente.

El sistema de autenticación puede ser un servidor RADIUS situado en la red local.

Los pasos que sigue el sistema de autenticación 802.1X son:

- El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
- El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajena al punto de acceso.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- El servidor pude aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.

- Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

De lo que hemos visto, el protocolo 802.1X tiene un mecanismo de autenticación independiente del sistema de cifrado. Si el servidor de validación 802.1X está configurado adecuadamente, se puede utilizar para gestionar el intercambio dinámico de claves, e incluir la clave de sesión con el mensaje de aceptación. El punto de acceso utiliza las claves de sesión para construir, firmar y cifrar el mensaje de clave EAP que se manda tras el mensaje de aceptación. El cliente puede utilizar el contenido del mensaje de clave para definir las claves de cifrado aplicables. En los casos prácticos de aplicación del protocolo 802.1X, el cliente puede cambiar automáticamente las claves de cifrado con la frecuencia necesaria para evitar que haya tiempo suficiente como para poder averiguarla.

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP podemos citar:

2.3.3.8.1 EAP-TLS

Es un sistema de autenticación fuerte basado en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Public Key Infraestructure) en ambos extremos. TLS (transport Layer Security) es el nuevo estándar que sustituye a SSL (Secure Socket Layer).

2.3.3.8.2 EAP-TTLS

El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor.

2.3.3.8.3 PEAP

El significado de PEAP se corresponde con Protected EAP y consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos.

2.4 METODOLOGÍA SAFE[26]

El uso de la arquitectura SAFE y su respectiva extensión para redes inalámbricas, proporcionará una guía para la elaboración del diseño de la red en una forma modular, considerando varios niveles de seguridad.

SAFE es una arquitectura de seguridad que evita, que la mayor parte de los ataques afecten a los recursos de red más valiosos. La arquitectura SAFE no es una forma revolucionaria de diseñar redes, sino meramente un modelo para asegurarlas. SAFE sirve de guía a los diseñadores de red que están planteándose los requisitos de seguridad de su red. SAFE adopta un enfoque de defensa en profundidad para el diseño de la seguridad de las redes.

SAFE utiliza un enfoque modular que tiene dos ventajas principales. En primer lugar, permite a la arquitectura afrontar la relación de seguridad entre los distintos bloques funcionales de la red, y en segundo lugar, permite a los diseñadores evaluar e implementar la seguridad módulo a módulo, en lugar de intentar completar la arquitectura en una sola fase.

SAFE también es resistente y ampliable. La resistencia de las redes incluye redundancia física que las protege de los fallos de los dispositivos debidos a una configuración errónea, a un fallo físico o a un ataque a la red.

[26] http://bibdigital.epn.edu.ec/bitstream/15000/2402/1/CD-0940.pdf

Esta arquitectura se compone de tres macro módulos: Campus Empresarial, Perímetro de la Empresa y Perímetro del ISP. La figura 2-13 muestra la primera capa de modularidad de SAFE.

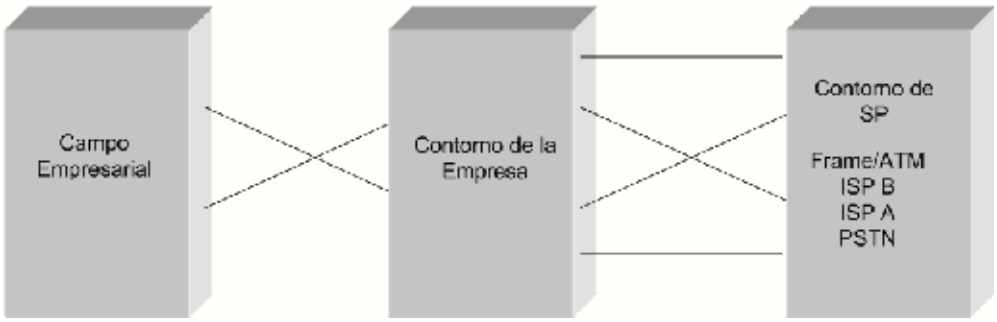

Figura 2-13: Modularidad SAFE

Fuente: http://bibdigital.epn.edu.ec/bitstream/15000/2402/1/CD-0940.pdf

La segunda capa de modularidad se muestra en la figura 2-14, que representa una vista de los módulos de cada área funcional, adaptado a las necesidades para el diseño de la red móvil motivo de este trabajo:

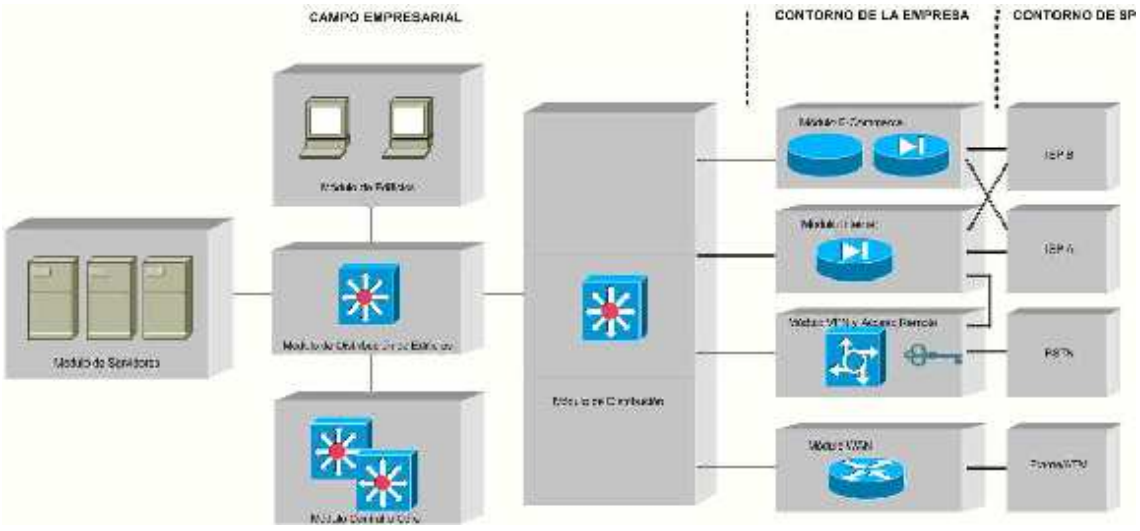

Figura 2-14: Vista de Módulos de cada Área Funcional SAFE

Fuente: http://bibdigital.epn.edu.ec/bitstream/15000/2402/1/CD-0940.pdf

2.4.1 CAMPUS EMPRESARIAL

2.4.1.1 Módulo de edificios

SAFE define el módulo del edificio como la parte amplia de la red, que contiene las estaciones de trabajo de los usuarios finales, los teléfonos y sus puntos de acceso de Capa 2 asociados. Su objetivo principal es ofrecer servicios a los usuarios finales.

2.4.1.2 Módulo de distribución de edificios

El objetivo de este módulo es proporcionar servicios de la capa de distribución a los switches del edificio, entre los que se incluyen el enrutamiento, la calidad de servicio (QoS) y el control de accesos. Las solicitudes de datos entran en estos switches y en el núcleo, mientras que las respuestas siguen el camino inverso

2.4.1.3 Módulo central

El módulo central de la arquitectura SAFE es casi idéntico al de cualquier otra arquitectura de red. Solamente enruta y conmuta el tráfico lo más rápidamente posible de una red a otra.

2.4.1.4 Módulo de servidores

El objetivo principal del módulo de servidores es proporcionar servicios de aplicaciones a los usuarios finales y a los dispositivos. Los flujos de tráfico del módulo de servidores los inspecciona la detección de intrusos a bordo en los switches de Capa 3.

2.4.1.5 Módulo de distribución

El objetivo de este módulo es agregar la conectividad de los distintos elementos al contorno. E l tráfico se filtra y se enruta desde los módulos de contorno al núcleo.

2.4.2 CONTORNO DE LA EMPRESA

2.4.2.1 Módulo de ecommerce

Este módulo está orientado a hacer transacciones de comercio electrónico.

2.4.2.2 Módulo de internet corporativo

El módulo de Internet de la empresa proporciona a los usuarios internos conexión a los servicios de Internet y acceso a los usuarios de Internet a la información de los servidores públicos. El tráfico también fluye de este módulo de VPN y de acceso remoto en que tiene lugar la terminación de la VPN.

2.4.2.3 Módulo de VPN y Acceso Remoto

Como su nombre implica, el objetivo principal de este módulo se divide en tres:

- Terminar el tráfico VPN de los usuarios remotos.
- Proporcionar un switch para terminar el tráfico VPN de los sitios remotos.
- Terminar los usuarios de acceso telefónico tradicionales.

Todo el tráfico que se envía a la distribución del contorno es de los usuarios remotos de la empresa que están autenticados de alguna forma antes de que puedan pasar por el firewall.

2.4.2.4 Módulo WAN

En lugar de incluir todos los diseños potenciales de WAN12, este módulo muestra la resistencia y la seguridad de la terminación de WAN. Utilizando la encapsulación de Frame Relay, el tráfico se enruta entre los sitios remotos y el sitio central.

CAPITULO 3. III. DISEÑO DEL SISTEMA DE CABLEADO ESTRUCTURADO Y RED INALÁMBRICA PARA HORMIGONES DEL VALLE S.A.

En este capítulo se describe el diseño de la solución a las necesidades planteadas en cuanto a sistema de cableado estructurado integrando una red inalámbrica, satisfaciendo los requerimientos actuales y futuros en la empresa.

3.1 DESCRIPCION DE EQUIPOS

3.1.1 Soluciones D-Link[27]

Desde sus inicios en 1986, D-Link se ha desarrollado hacia el mercado global. Para consolidar esta presencia internacional, ha abierto subsidiarias en los mayores mercados y establecido una red extensa de distribuidores en más de 90 países.

Hoy en día la globalización ha llevado a D-Link a ser un “player global” con una rápida estrategia de crecimiento. Este programa consiste en el desarrollo de tres estrategias claves: Investigación y Desarrollo, Producción y Marketing. El objetivo es poder concentrarse en nuevas oportunidades, racionalizando el uso de recursos, los costos y proveyendo un servicio global al cliente.

Con laboratorios de Investigación y Desarrollo en los diferentes continentes, D-Link ha sido capaz de captar nuevas tecnologías trabajarlas en los laboratorios, llevándolas hacia los mercados de forma rápida. Los productos D-Link responden hoy de forma flexible a los requerimientos globales y locales.

Con plantas en Taiwán, China, India y USA, D-Link ha sido capaz de hacer crecer su producción, reducir costos en los componentes y mover de forma rápida los productos desde la fábrica hacia los clientes.

[27] http://www.dlinkla.com/home/corporacion/corporacion.jsp

3.1.1.1 Xtreme N™ Gigabit Router [28]

Figura 3-1: Xtreme N™ Gigabit Router
Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=949

El Xtreme N™ Gigabit Router DIR-655 es un dispositivo basado en la norma estándar 802.11n que ofrece un rendimiento real de hasta un 650 % más rápido que una conexión inalámbrica 802.11g, y también supera de forma inalámbrica a una red Ethernet* cableada de 100 Mbps. Además es compatible con dispositivos de norma 802.11g y 802.11b. Al conectar el Xtreme N™ Gigabit Router a un módem DSL o cable módem, los usuarios podrán compartir su acceso a internet de alta velocidad dentro de la red, compartiendo además inalámbricamente y con avanzadas características de seguridad sus fotos, archivos, música, vídeo, impresoras y almacenamiento de red .

Impulsado por la tecnología Xtreme de N™ y provisto con tres antenas externas, este Router mantiene una cobertura Inalámbrica superior en oficinas y casas de mayor tamaño, y es ideal para usuarios que ejecutan aplicaciones que requieran un gran ancho de banda. El DIR-655 también incorpora un Switch de 4-puertos Gigabit 10/100/1000 que permite unir a la red los dispositivos conectados vía cable, logrando una completa solución de Red con las mejores características tanto en forma inalámbrica como cableada.

Con la Tecnología Intelligent QoS el tráfico a través de cable y vía inalámbrica es analizado y separado en múltiples data streams. El DIR-655 cuenta con el procesador más rápido de la gama Wireless N, que logra incluso un rendimiento más alto entre redes WAN y LAN.

[28] http://www.dlinkla.com/home/productos/producto.jsp?idp=949

Combinado con el galardonado QoS StreamEngine, el DIR-655 permite tener una mejor experiencia en Internet puesto que las llamadas telefónicas por Internet y los juegos en línea se desarrollan perfectamente.

Con la tecnología WISH (Wireless LAN Intelligent Stream Handling), el Xtreme N™ Gigabit Router (DIR-655) incluye calidad de servicio (QoS), tanto inalámbricamente como hacia y desde internet (StreamEngine). Cuenta con WISH, que mejora la experiencia del usuario en los juegos, la televisión de alta definición (HDTV) y otras aplicaciones de medios en una conexión inalámbrica, puesto que minimiza los efectos negativos del tráfico de la red. Automáticamente detecta si en la red inalámbrica se está utilizando contenidos de audio, vídeo o de juegos, y les da prioridad a esas aplicaciones por encima del tráfico menos susceptible al tiempo, como el correo electrónico o la transferencia de archivos. Luego ajusta las prioridades para garantizar que el contenido de medios se transmite sin demoras ni fluctuaciones.
Además, el □úplex□ refuerza una política de «buen vecindario» garantizando que no cree interferencias en las redes vecinas. Esto lo consigue reduciendo el espectro de radio usado cuando detecta una red legacy 802.11g/b la zona.

El DIR-655 es uno de los primeros Routers para el consumidor que pasa las rigurosas pruebas de aprobación de Microsoft® Windows Vista™. Con este Router, los usuarios podrán disfrutar del nuevo sistema operativo, como descubrir y administrar sus dispositivos con Network Explorer y Network Map features in Windows Vista™. Gracias a Wi-Fi Protected Setup / Windows Connect Now (WCN) Config 2.0, podrán configurar redes WiFi de una forma fácil y segura. El □úplex□ también incluye compatibilidad de servicio con Xbox Live®.

El Xtreme N™ Gigabit Router (DIR-655) soporta las últimas características de seguridad inalámbrica para ayudar a prevenir el acceso no autorizado sobre una red inalámbrica o en Internet. Soporta WEP ™, WPA ™, y WPA2 ™ estándares que aseguran la capacidad de usar la mejor encriptación posible. Además, el Xtreme N™ Gigabit Router utiliza Cortafuegos Activos Duales (SPI y NAT) para prevenir ataques potenciales que provengan de Internet.

Entregando el mejor funcionamiento en su clase en cuanto a seguridad de la red y cobertura el Xtreme N™ Gigabit Router DIR-655 es la pieza central ideal, para su red inalámbrica en oficinas y hogares de mayor tamaño.

La velocidad máxima de la señal inalámbrica la definen las especificaciones del estándar IEEE 802.11g y 802.11n. Las velocidades 802.11n se obtienen cuando se opera con los productos Wireless N. El rendimiento real variará. Las condiciones de la red y los factores medioambientales, como el volumen de tráfico por la red, los materiales de construcción, las edificaciones y la sobrecarga de la red, pueden disminuir la velocidad real de los datos. Los productos Wireless N se basan en las especificaciones IEEE 802.11n y no se garantiza que sean compatible con futuras versiones de las especificaciones IEEE 802.11n. Tampoco se garantiza la compatibilidad con dispositivos 802.11n de otros fabricantes. Todas las referencias a velocidades se dan solo a efectos de comparación. Las especificaciones del producto, tamaño y forma están sujetas a cambios sin previo aviso, y el aspecto actual del producto puede ser distinto del que figura aquí. D-Link, el logo D-Link, RangeBooster N 650 y Xtreme NTM son marcas registradas.

CARACTERISTICAS:

- Procesador de alta velocidad, que ofrece en mejor rendimiento.
- Admite la nueva especificación Wi-Fi WPS™ (Wireless Protect Setup).
- Logo «Funciona con Windows Vista™».
- 4 puertos switch Gigabit con soporte para tramas Jumbo.
- QoS: StreamEngine y WISH (Wireless LAN Intelligent Stream Handling).
- Protección con Cortafuegos Activos Duales (SPI y NAT).
- Compatible con dispositivos de norma 802.11g y 802.11b

3.1.1.2 Wireless 150 USB Adapter [29]

Figura 3-2: Wireless 108G USB 2.0 Adapter
Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=1307

Adaptador Inalámbrico USB 2.0 Wireless 150, para Computadoras de escritorio o Laptops. Hasta 150 Mbps de velocidad cliente Wireless 11N.

Conéctese a una red wireless de alta velocidad a través del Adaptador USB Wireless 150 de D-Link y disfrute navegando en la web, revisando su correo electrónico y conversando en línea con su familia y amigos. El DWA-125 usa tecnología Wireless 150, que ofrece mayor velocidad y rango sobre el estándar1 802.11g/b, entregando una conexión wireless más rápida y confiable.

Para proteger sus datos y privacidad, el Adaptador USB Wireless 150 de D-Link soporta cifrado WEP, WPA y WPA2 para una conexión y tráfico de red seguro a través de una red wireless.

El Adaptador USB DWA-125 proporciona una conexión de alta velocidad a otros dispositivos Wireless 150 o 802.11, alcanzando hasta 150 Mbps y es compatible con 802.11b/g, asegurando compatibilidad con una amplia gama de routers y redes wireless.

La Configuración Rápida Wizard de D-Link permite fácil configuración de su red adaptador USB para que pueda obtener una rápida conexión. La Configuración Protegida Wi-Fi (WPS) configura una conexión wireless segura, de modo que todo lo que usted debe hacer es apretar un botón para crear automáticamente una

[29] http://www.dlinkla.com/home/productos/producto.jsp?idp=1307

conexión wireless segura a su red, dejando atrás la necesidad de configurar ajustes complicados para una conexión.

CARACTERISTICAS:

- Adaptador inalámbrico USB 2.0 permite conexiones inalámbricas hasta 150Mbps 802.11n
- Compatible con 802.11b/g/n
- Proporciona hasta 11Mbps para 802.11b, 54Mbps para 802.11g, 150Mbps para 802.11n
- Soporta WEP, WPA-Personal/Empresa, WPA2-Personal /Empresa, WPS
- Instalación Plug and Play. Fácil y segura configuración con WPS y Software Quick Setup Wizard.
- Soporta WiFi WMM & WMM-PS QoS

3.1.1.3 24-Port 10/100Mbps SMB Switch with 2 port Combo Gigabit [30]

Figura 3-3: 24-Port 10/100Mbps SMB Switch with 2 port Combo Gigabit
Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=78

Maximize el rendimiento de su red con este Switch de alto rendimiento y excelentes características. Migre eficientemente su red a la velocidad Gigabit con el Switch no administrable DES-1026G de D-Link. Con 24 puertas de 10/100 Mbps más 2 puertas Gigabit Ethernet, 10/100/1000 Mbps, este switch proporciona una atractiva combinación para soluciones Ethernet, FastEthernet y Gigabit Ethernet, todo de manera compacta. Soluciona los problemas de cuellos de botella hacia los Servidores, extiende el tamaño de la red, y mejora los tiempos de respuesta para todos los usuarios en la red, en una sola movida. La Arquitectura Non-Blocking del DES-1026G habilita un óptimo procesamiento de red a

velocidad wire-speed, mientras el control del flujo de datos filtra los paquetes de salida □úplex□s, minimizando la propagación de ellos. Adicionalmente, los LEDs ubicados en la parte frontal del equipo, proporcionan información fácil de leer, mostrando los diferentes status del equipo, simplificando con ello los posibles diagnósticos de problemas que se presenten.

Las principales características del DES-1026G pueden resumirse en:

- Arquitectura Non-Blocking Wire-Speed
- Capacidad de 8.8Gbps de Backplane (Switching Fabric Capacity)
- Plug & Play
- Configuración y Detección Auto-Sensing
- Soporte de los Estándares de la Industria
- (2) Puertas 10/100/1000 para conectividad High-Speed (Gigabit Ethernet)

El DES-1026G puede ser utilizado para dar una solución de red inmediata, permitiendo la conectividad de 24 usuarios a 10/100Mbps, y de hasta 2 Servidores en GigabitEthernet, sin tener que realizar una gran inversión.

CARACTERISTICAS:

- Arquitectura Non-Blocking Wire-Speed
- 2 puertas 10/100/1000Base-T Gigabit
- 24 puertas 10/100Mbps
- Todas las puertas soportan MDI/MDIX
- Tamaño Rack

3.1.2 Soluciones Linsys[31]

Los routers inalámbricos ofrecen total libertad para trabajar y disfrutar de los juegos en todo el área de trabajo con protección y seguridad. Con los routers de

[30] http://www.dlinkla.com/home/productos/producto.jsp?idp=78
[31] http://www.linksysbycisco.com/LATAM/es/promo/Promotion-Go-Wireless-LAes

Linksys by Cisco, sólo se necesita una conexión de Internet de alta velocidad para comenzar a utilizar la tecnología inalámbrica de inmediato.

3.1.2.1 Router de banda ancha Wireless-N con Storage Link (WRT160NL)[32]

Figura 3-4: Router de banda ancha Wireless-N con Storage Link (WRT160NL)
Fuente: http://www.linksysbycisco.com/LATAM/es/products/WRT160NL?lid=LearnMore

La velocidad y ancho de banda de Wireless-N, la tecnología inalámbrica más avanzada de la actualidad, facilita el acceso compartido de varios usuarios a Internet, archivos e impresiones. Las actividades multimedia intensas como los juegos, videos y llamadas VoIP al mismo tiempo, con menos lentitud y sin afectar el rendimiento. Alcanza una mayor velocidad cuando se utiliza con equipos habilitados con Wireless-N, pero es totalmente compatible con equipos Wireless-G y –B.

La tecnología de “múltiple entrada, múltiple salida” (MIMO) de Wireless-N utiliza las reflexiones de señal que confunden a las tecnologías inalámbricas comunes para mejorar el alcance y reducir los puntos muertos.

La función Storage Link permite conectar un disco duro o un dispositivo de almacenamiento flash USB a la red para agregar fácilmente gigabytes de almacenamiento. Acceder su música, videos o archivos de datos desde cualquier PC de su red, o con seguridad a través de Internet.

[32] http://www.linksysbycisco.com/LATAM/es/products/WRT160NL?lid=LearnMore

Los cuatro puertos Ethernet 10/100 permiten conectar impresoras, unidades de almacenamiento en red y otros equipos Ethernet a la red para acceder y compartirlos desde todas las computadoras al mismo tiempo.

CARACTERISTICAS:

- Internet Explorer 6, Safari 3 o Firefox 2 o superior para configuración con navegador
- Unidad de CD-ROM
- Adaptador de red con cable o inalámbrico con protocolo TCP/IP
- El software EasyLink Advisor y el asistente de configuración requieren contar con una versión actualizada de Windows XP, Vista, o Vista edición 64 bits
- El asistente de configuración también funciona en Mac OS X 10.4 o superior

3.1.2.2 Adaptador USB Wireless-G compactoWUSB54GC[33]

Figura 3-5: Adaptador USB Wireless-G compactoWUSB54GC
Fuente: http://www.linksysbycisco.com/LATAM/es/products/WUSB54GC

La tecnología Wireless-G le ofrece una conexión rápida a la mayoría de las redes inalámbricas para que pueda acceder a Internet o a equipos conectados en red como impresoras, dispositivos de almacenamiento u otras computadoras, esté donde esté: en su casa, en la oficina o en la calle.

[33] http://www.linksysbycisco.com/LATAM/es/products/WUSB54GC

Funciona con computadoras portátiles y de escritorio. Conexión en un puerto USB□o utilice el cable de extensión USB, hasta 1,5 m. de distancia.

La encriptación WPA ayuda a proteger la confidencialidad de las comunicaciones e información.

CARACTERISTICAS:

- PC de 400 MHz o superior
- 128 MB de memoria RAM
- Unidad de CD-ROM
- Puerto USB disponible
- Compatible con Microsoft Windows XP, Vista y Vista edición de 64 bits

3.1.3 Soluciones 3COM[34]

3Com comprende muy bien que la potencia de su negocio depende de la eficiencia y la seguridad de su red. Por eso 3Com Global Services se compromete a asegurar que su empresa se mantenga conectada, proporcionando una combinación integral de herramientas y servicios de soporte, además de paquetes de servicios adaptados para satisfacer sus necesidades particulares de negocios.

3Com adopta un enfoque apasionado en oferta de servicios, que se basa en profundas fuentes de experiencias que emanan de una amplia gama de industrias, modelos de negocios y configuraciones de redes. 3Com ofrece resultados con una infraestructura de servicio organizada para aumentar al máximo el nivel de respuesta y optimizar la resolución de problemas. Para ayudarle a aprovechar a nuestro equipo y conocimientos, ofrecemos varios tipos distintos de servicios, de acuerdo con sus necesidades.

[34] http://lat.3com.com/lat/services/

3.1.3.1 3Com® Wireless 11g Cable/DSL Router[35]

Figura 3-6: 3Com® Wireless 11g Cable/DSL Router
Fuente: http://www.compulogic.com.ar/catalog/images/3CRWER101A_UNIT.jpg

Acceso compartido a Internet asequible, fiable y seguro para usuarios inalámbricos y cableados.
El 3Com® Wireless 11g Cable/DSL Router es una solución asequible y fácil de usar, diseñada para oficinas pequeñas y domésticas, que permite a múltiples usuarios compartir de forma segura una única conexión a Internet por cable o DSL.

CARACTERISTICAS:

- Se conecta a un módem externo de cable o DSL mediante un puerto Ethernet.
- Permite a múltiples usuarios compartir la misma conexión a Internet de cable o DSL.
- El diseño compacto minimiza el uso de espacio de sobremesa.
- El diseño de antena extraíble proporciona flexibilidad con opciones de antenas.
- La tecnología de alcance extendido (XR) proporciona una conectividad con un alcance mayor para usuarios inalámbricos.
- La funcionalidad de ráfagas de paquetes incrementa el caudal al enviar más tramas para un periodo de tiempo dado.
- La encriptación WPA/WPA2 de 128 bits con TKIP/AES protege la privacidad de las transmisiones inalámbricas 11g y 11b.

[35] http://www.3com.com/prod/es_es_emea/detail.jsp?tab=features&sku=3CRWER101A-75

- Encriptación WEP de 40/64 y 128 bits para clientes heredados.
- La certificación Wi-Fi garantiza la interoperabilidad con otros productos con certificación Wi-Fi.
- Cuatro puertos de LAN 10/100 Ethernet con Auto MDI/MDIX proporcionan conectividad de LAN cableada.
- El DNS (Servicio de nombres de dominio) Dinámico permite usar aplicaciones de red como por ejemplo la Web o servidores FTP que requieren normalmente direcciones IP estáticas (se requiere una suscripción con proveedores de DNS Dinámico).
- El filtrado de URL controla el acceso a sitios web inapropiados.
- El routing IP (RIP 1 y 2) y el routing estático favorecen la flexibilidad, ya que permiten usar este router en contextos multi-redes.
- La interfaz basada en navegador, los sencillos asistentes de configuración, y los ajustes por defecto garantizan la facilidad de uso.

3.1.3.2 3Com® Baseline Plus Switch 2928 HPWR[36]

Figura 3-7: 3Com® Baseline Plus Switch 2928 HPWR

Fuente: https://www.paratupc.es/productos/small/3Com/483807_3Com_3CRBSG28HPWR93ME_3Com_Baseline_Plus_S.jpg

El 3Com® Baseline Plus Switch 2928 HPWR “inteligente” preparado para voz es un switch Gigabit Power over Ethernet (PoE) administrable a través de la Web con amplias funcionalidades de Nivel 2 y rutas estáticas de Nivel 3. Ofrece funciones de clase empresarial, personalizables y a un precio especial para pequeñas y medianas empresas.

Con una interfaz fácil de usar y funciones avanzadas (VLAN, autenticación IEEE 802.1X y QoS), este switch es la forma más rentable de proporcionar una red convergente.

[36] http://www.3com.com/prod/es_es_emea/detail.jsp?tab=features&sku=3CRBSG28HPWR93

El Baseline Plus Switch 2928 HPWR proporciona alimentación en línea para los dispositivos conectados— puntos de acceso, teléfonos Voz sobre IP (VoIP), cámaras de seguridad IP, etc.— mediante Power over Ethernet estándar de la industria IEEE 802.3af sobre un único cable Ethernet, lo que redunda en unos ahorros de coste significativos a la hora de implementar estos dispositivos.

El Baseline Plus Switch 2928 HPWR tiene 24 puertos 10/100/1000 Mbps y 4 puertos 1000 Mbps basados en SFP (fibra) para conectar ordenadores de elevado rendimiento, servidores o troncales de núcleo de red.

Este switch “inteligente” dispone de funciones que ayudan a construir una red preparada para voz, compatible con VLAN de voz automática, LLDP, administración basada en SNMP, IGMP snooping, así como IEEE 802.1X y listas de control de acceso (ACL) avanzadas para reforzar la seguridad.

El switch proporciona un rendimiento sin bloqueo— todos los 28 puertos se ejecutan a velocidad de cable que ayuda a eliminar los cuellos de botella de la red. La agregación de enlaces LACP (IEEE 802.3ad) permite agrupar puertos automáticamente para crear una conexión con ancho de banda ultra grande que expande considerablemente la capacidad de ancho de banda con la red troncal.

El Baseline Plus Switch 2928 HPWR también admite Spanning Tree, Rapid Spanning Tree y Multiple Spanning Tree, priorización de tráfico, generación de colas de prioridades y VLAN. Estas funciones de switching aseguran el uso óptimo del ancho de banda disponible a medida que el flujo de tráfico se dirige de acuerdo con las necesidades de la empresa

Este switch Baseline Plus está operativo nada más sacarse del paquete; siempre que se acepten los valores predeterminados, no es preciso configurarlo. Si se desea, el switch se puede configurar usando un navegador Web o software de administración SNMP.

Para aquellas redes que requieren más control, la interfaz de administración Web del switch proporciona un proceso intuitivo y de menús para que incluso los usuarios principiantes puedan configurar de forma rápida y segura el switch durante la instalación y administrarlo durante el funcionamiento normal. Las vistas gráficas del puerto y del switch permiten comprender con claridad el estado y la configuración del switch.

Además, la interfaz Web ofrece el control de tráfico de puertos individuales (duplicación de puertos) y tablas de asignación de puertos de dirección MAC. Una herramienta de diagnóstico de cable permite a los usuarios solucionar los problemas básicos de conectividad a través de la interfaz de administración Web, simplificando aún más la instalación de la red.

Con una sola entidad con una única dirección IP, hasta 32 dispositivos de la misma familia (modelos 3CRBSGxxx) pueden administrarse desde una dirección IP a través de IRF Lite.

Este Baseline Plus Switch también es compatible con el software de administración Intelligent Management Center (IMC), 3Com Network Supervisor (3NS) y 3Com Network Director (3ND).

IMC se puede usar para asignar la topología de la red, indicando qué dispositivos están conectados y en qué puertos. La administración del switch y las actualizaciones de software pueden realizarse fácilmente. También se pueden utilizar otras herramientas de administración basadas en SNMP.

La familia de switches también admite una interfaz de línea de comandos (CLI) compacta que se accede a través del puerto de consola del panel frontal. Usando la CLI, se pueden configurar rápidamente las opciones iniciales de configuración del switch.

CARACTERISTICAS:

- Switch Ethernet Gigabit de Nivel 2 administrable mediante la Web, con 32 rutas estáticas.
- 24 puertos PoE 10/100/1000 y cuatro puertos SFP Gigabit; puerto de consola en panel frontal para administración CLI.
- PoE proporciona suministro eléctrico a teléfonos IP, puntos de acceso de LAN inalámbrica, 3Com Intellijacks y otros dispositivos compatibles sobre el mismo cable que se emplea para datos.
- Administración como una sola entidad con una única dirección IP de hasta 32 dispositivos de la familia Baseline Plus 2900 (modelos 3CRBSGxxx).
- Operativo nada más sacarse del paquete con valores predeterminados o si se desea más control, la interfaz del switch permite incluso a los usuarios principiantes configurarlo de forma rápida y segura.
- Las VLAN permiten segmentar la red, reagrupando los usuarios en función de sus necesidades de intercambio de datos o tráfico para un uso óptimo del ancho de banda disponible.
- La agregación de enlaces LACP permite agrupar puertos automáticamente para crear una conexión troncal con ancho de banda ultra grande con la red troncal, y ayuda a prevenir los cuellos de botella de tráfico.
- El control de acceso a la red IEEE 802.1X proporciona seguridad basada en estándares combinada con autenticación local.
- Las ACL basadas en MAC e IP permiten filtrar el tráfico y mejorar el control de la red.
- VLAN automática de voz que asigna automáticamente el tráfico VoIP (voz sobre IP) a una VLAN de voz dedicada, optimizando así este tráfico sensible al retardo.
- El soporte del protocolo Spanning Tree Protocol (STP/RSTP/MSTP) permite mejorar la compatibilidad, escalabilidad y disponibilidad de la red.
- Soporte de tramas Jumbo para una carga de red reducida.
- El IGMP snooping y el filtrado multicast permiten optimizar el rendimiento de la red.
- El switch puede administrarse con software compatible con SNMP, como por ejemplo 3Com IMC, Network Supervisor y Network Director.

3.2 ANALISIS Y SELECCIÓN DE EQUIPOS

3.2.1 Selección de Equipos

Para realizar la selección de los equipos se debe considerar las características que más se acoplen a las necesidades de la empresa, teniendo en cuenta el costo beneficio.

Tabla comparativa Wireless

Descripción	D-LINK Xtreme N Gigabit Router DIR-655	LINKSYS Wireless-N Broadband Router	3COM ROUTER WIRELESS 11G
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft 2.0	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft)	
Banda de frecuencia	2.4 GHz		2,4 – 2,4835 GHz
Red / Protocolo de transporte	TCP/IP, PPTP, UDP/IP, L2TP, ICMP/IP, IPSec	RIP, direccionamiento IP estático	IPCP para el direccionamiento IP dinámico y estático, Routing IP (RIP 1 y 2), NAT/PAT (con TCP, UDP), PAP, PPCP, PPTP/PPPoE, SNTP
Protocolo de gestión remota	HTTP	HTTP, HTTPS	

Características	Protección firewall, auto-sensor por dispositivo, asignación dirección dinámica IP, soporte de DHCP, soporte de NAT, negociación automática, señal ascendente automática (MDI/MDI-X automático), Stateful Packet Inspection (SPI), servidor DNS dinámico, Alerta de correo electrónico, pasarela VPN, actualizable por firmware, montable en pared, soporte Wi-Fi Multimedia (WMM)	Capacidad □úplex, protección firewall, puerto DMZ, soporte de DHCP, soporte de NAT, conmutador MDI/MDI-X, Stateful Packet Inspection (SPI), filtrado de dirección MAC, pasarela VPN, cifrado de 256 bits, modo operativo Punto de Acceso, actualizable por firmware, tecnología MIMO, Wi-Fi Protected Setup (WPS)	El 3Com OfficeConnect Wireless 11g Cable/DSL Router incluye múltiples características de seguridad y routing IP – routing IP (RIP 1 y 2); routing estático; filtrado de URL o palabras clave y listas de control de acceso de permiso/denegación; más soporte para el servicio de Filtrado de Contenidos 3Com – en un paquete económico. La encriptación WPA de 256 bits y WEP de 40/64 bits protege la privacidad de las transmisiones inalámbricas 11g y 11b. Un intuitivo interfaz web y los sencillos asistentes de configuración simplifican la instalación y la utilización.
Cumplimiento de	IEEE 802.3, IEEE	IEEE 802.3, IEEE	Certificación Wi-Fi,

normas	802.3u, IEEE 802.11b, IEEE 802.11g, Wi-Fi CERTIFIED, IEEE 802.11n (draft 2.0)	802.3u, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft)	certificación WPA, IEEE 802.11b, 802.11g
Precio	Accesible	Accesible	Muy Elevado

Tabla 3-1: Tabla Comparativa D-link, Linksys, 3COM wireless
Fuente: Autor

Tabla Comparativa Interfaces Wireless-USB

Descripción	D-LINK Wireless 150 USB	LINKSYS Compact
Tipo de interfaz (bus)	USB	Hi-Speed USB
Protocolo de interconexión de datos	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (draft 2.0)	IEEE 802.11b, IEEE 802.11g
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.11b, IEEE 802.11g, Wi-Fi CERTIFIED, IEEE 802.11n (draft 2.0	IEEE 802.11b, IEEE 802.11g, Wi-Fi CERTIFIED
Precio	Accesible	Accesible

Tabla 3-2: Tabla comparativa Wireless-USB

Fuente: Autor

Tabla comparativa Switch

Descripción	D-LINK DES 1026G	3Com Baseline Plus Switch 2928
Ports	24 x 10/100 + 2 x 10/100/1000	24 x Ethernet 10Base-T, Ethernet 100Base-TX,

		Ethernet 1000Base-T
Tamaño de tabla de dirección MAC	8K de entradas	8K de entradas
Características	Control de flujo, conmutación Layer 2, auto-sensor por dispositivo, conmutador MDI/MDI-X, negociación automática	Control de flujo, conmutación Layer 3, conmutación Layer 2, soporte de DHCP, negociación automática, soporte ARP, soporte VLAN, snooping IGMP, Weighted Round Robin (WRR) queuing, store and forward, Quality of Service (QoS), compatibilidad con Jumbo Frames
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.3ab, IEEE 802.3x	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x
Interfaces	24 x 10Base-T/100Base-TX – RJ-45 ¦ 2 x 10Base-T/100Base-TX/1000Base-T – RJ-45	24 x red – Ethernet 10Base-T/100Base-TX/1000Base-T – RJ-45 1 x gestión – consola
Precio	Accesible	Muy Elevado

Tabla 3-3: Tabla Comparativa Switches

Fuente: Autor

3.2.2 Selección

Como conclusión se puede decir que la marca que se ajusta a las necesidades de la empresa, es D-link, por su relación de costos, funcionabilidad, y beneficios.
Los equipos a usarse son:

- 2 Router inalámbrico D-LINK 655N
- 2 Switch 24 puertos D-LINK 1026G
- 3 Tarjetas inalámbricas USB D-LINK 150N

3.2.3 Costo Total del Proyecto

Teniendo las características de los equipos y las necesidades de la empresa en claro, se procede a analizar la proforma, y a la compra de los equipos. Teniendo lo siguiente:

Proforma

Ítem	DETALLE	CANTIDAD	V.UNIT	V.TOTAL
1	INSTALACION Y CONFIGURACION ESTRUCTURADO	20	100	2000
	(TENDIDO DE CABLE, INSTALACION DE CANALETAS			
	INSTALACION DE CAJETINES, CONFIGURACION DE			
	ESTACIONES DE RED, MONTAJE DE RACK, PRUEBAS FUNCIONAMIENTO)			
	INCLUYE TODOS LOS MATERIALES			
	LISTADO DE MATERIALES			
1	SOPORTE DE PARED 5 POSICIONES	2		
2	PATCH PANEL 16 CONECTORES CAT6	2		
3	ORGANIZADOR DE CABLES	2		
4	CAJETINES RJ-45 CAT6 VOZ-DATOS DOBLE	10		
5	PATCH CORDS CAT6 1MTS (RACK)	20		
6	PATCH CORD CAT6 3MTS (PUESTO DE TRABAJO)	20		
7	CABLE UTP NIVEL 6 (METROS) DATOS	350		
10	CANALETAS DECORATIVAS 40X25 (10C)	6		
11	CANALETAS DECORATIVAS 32X12 (4C)	8		
12	CANALETAS DECORATIVAS 20X12 (2)	8		

13	BANDEJA METALICA	2		
14	MULTITOMAS POLARIZADOS	2		
	PUNTOS DE RED CONSIDERADOS:			
	PRODUCCION	4		
	CONTABILIDAD	4		
	BODEGA	3		
	VENTAS	3		
	GERENCIA	3		
	IMPRESORAS	**2**		
	INTERNET	**1**		
	TOTAL PUNTOS	**20**		
1	Switch 24 puertos D-Link 1026	2	70	140
2	Router inalámbrico DLynk 655	2	165	330
3	Tarjetas inalámbricas USB 150 N	4	28	112
	TOTAL			**582**
TOTAL GENERAL				**2582**

Tabla 3-4: Lista de Precios

Fuente: JulianLuzcando

3.3 DISEÑO LOGICO

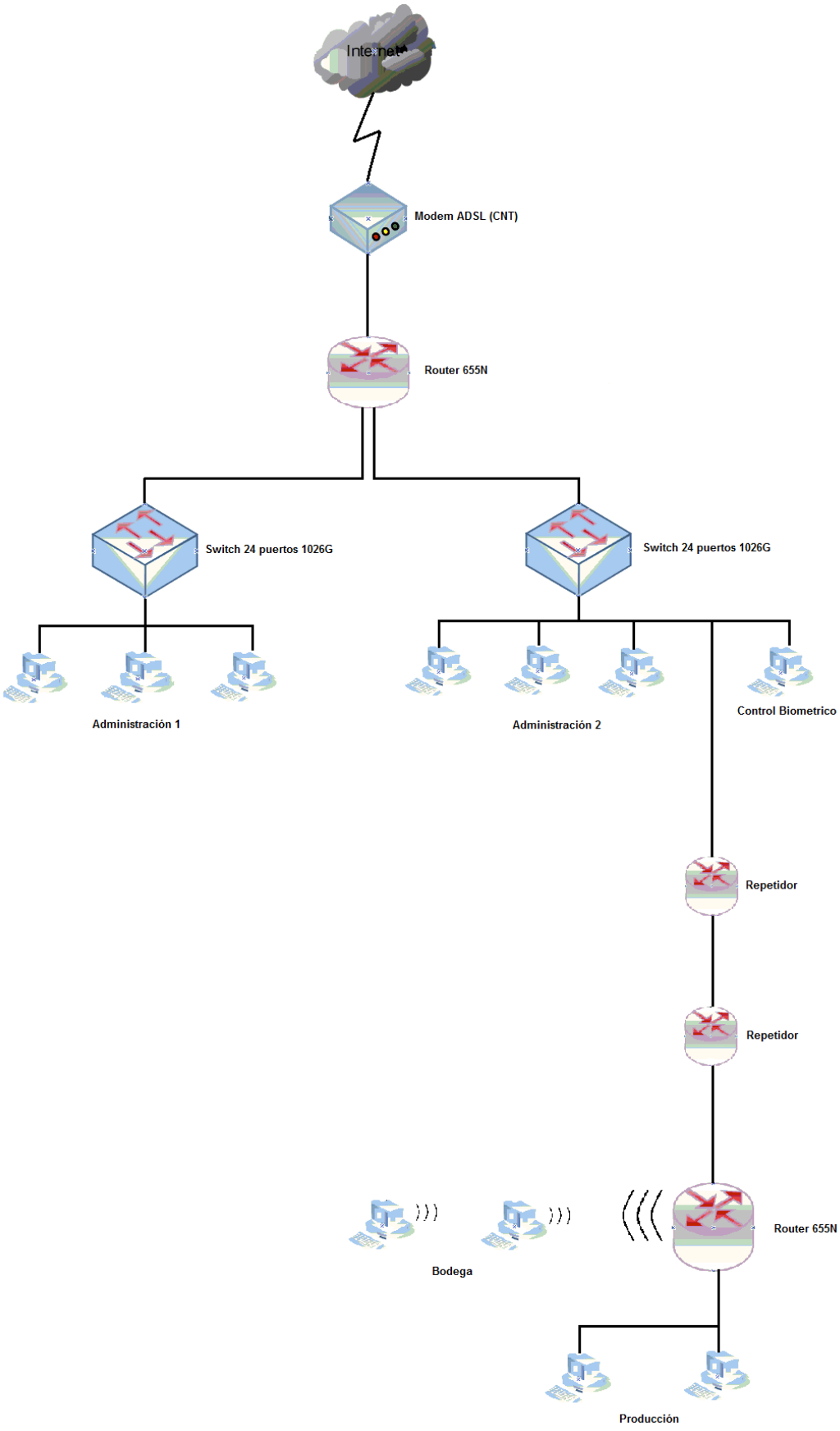

Figura 3-8: Diseño Lógico
Fuente: Autor

3.4 Diseño Físico

Hormigones del Valle S.A., consta de de 3 plantas separadas, la planta Administrativa(P1), la planta de Producción(P2), la planta de Bodega(P3), también consta del control biométrico(B), que se encuentra separada de la planta administrativa.

Para interconectar P1 con B, solo se necesita un tendido de cable utp CAT 5e, ya que la distancia no es grande.

Para interconectar P1 con P2, se necesitan 2 repetidores (R1, R2) suministrados por la empresa, marca D-link 150, ya que P2 se encuentra muy alejada de P1.

Para conectar P2 con P3, se necesita la implementación de wireless, ya que en P3 también se realizan trabajos de mantenimiento y no es posible realizar una red cableada.

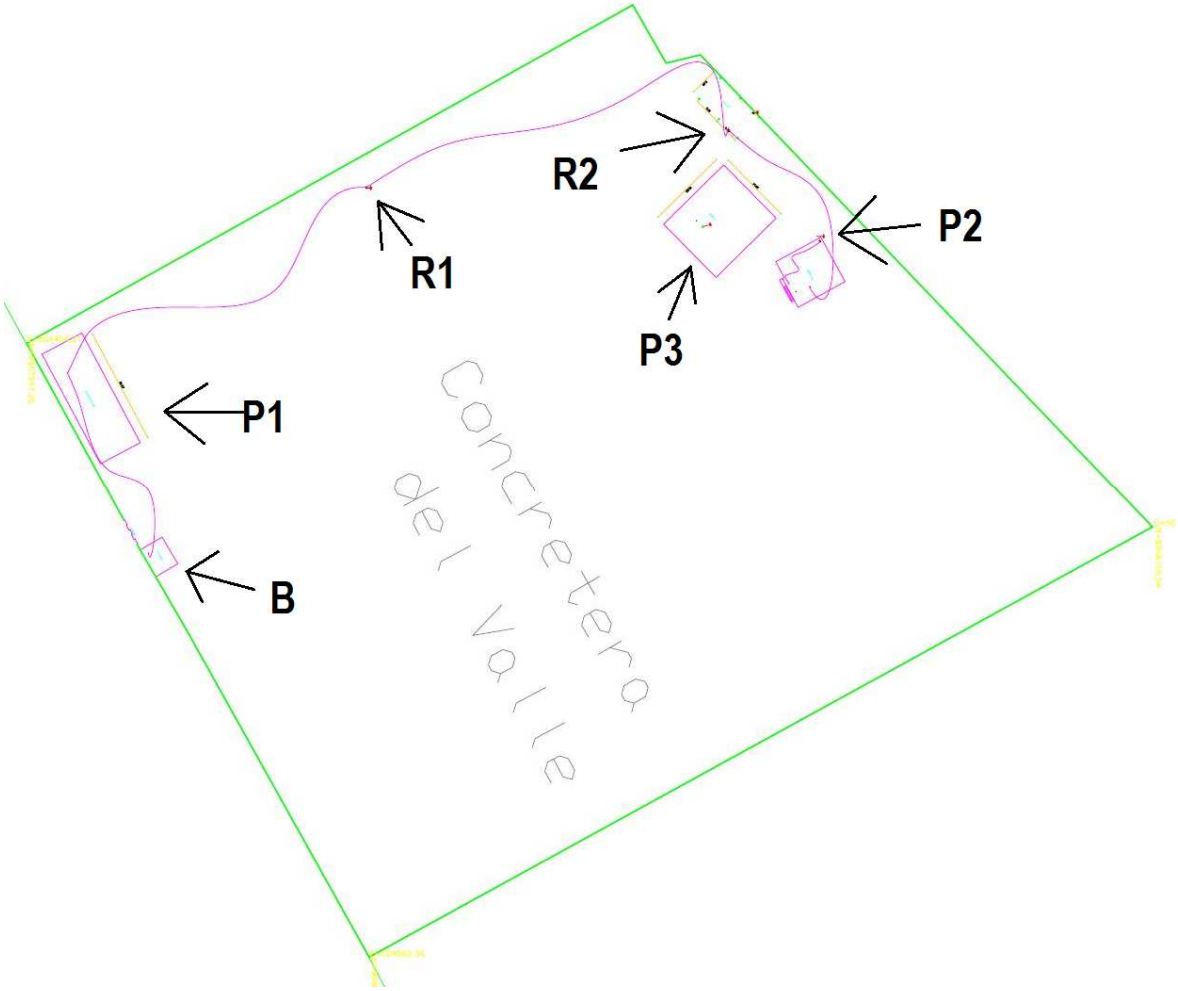

Figura 3-9: Plano General Hormigones del Valle S.A.

Fuente: Autor

La Planta administrativa reparte señal hacia toda la empresa, la señal de internet llega al modem ADSL provisto por CNT, se conecta al rack que está conformado por el router, el switch, patch pannel. De aquí se conecta hacia el servidor y hacia un rack secundario. Las áreas de cobertura están divididas para que cada rack tenga una distancia menor hacia cada estación de trabajo.

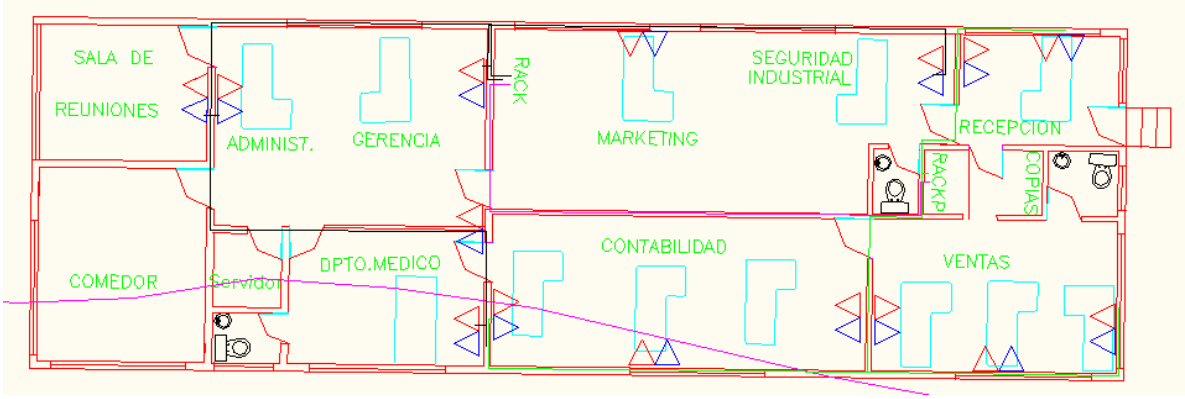

Figura 3-10: Plano Planta Administrativa

Fuente: Autor

Del rack secundario, se alimenta al Control Biométrico (B), en el cual se encuentra una estación de trabajo.

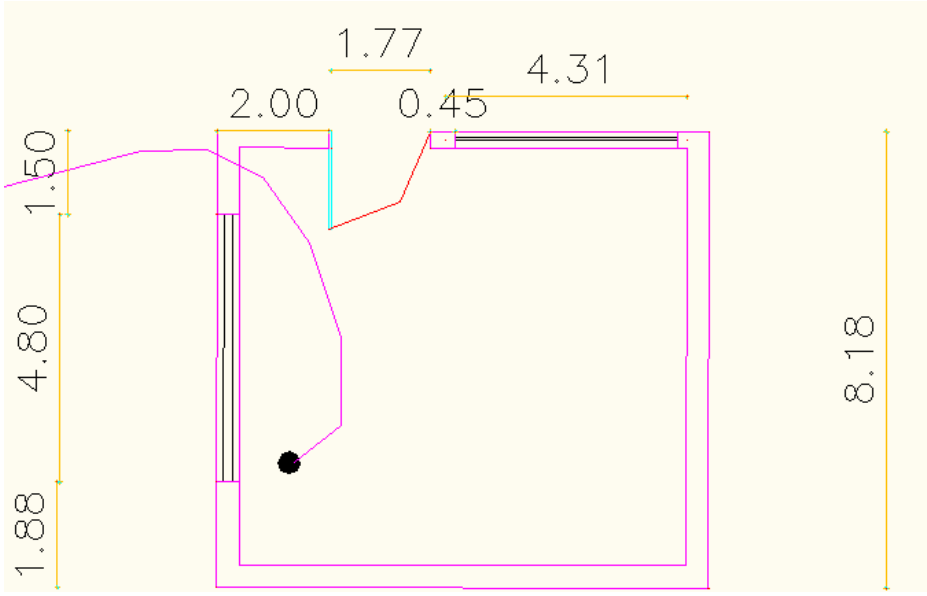

Figura 3-11: Plano Control Biométrico

Fuente: Autor

Así mismo del rack secundario, se conecta de la Planta de Producción (P2), a un router inalámbrico, para repartir la señal vía cable a las estaciones, y vía inalámbrica a Bodega(P3), ya que desde este lugar tiene una línea de vista directa para las antenas ubicadas en bodega.

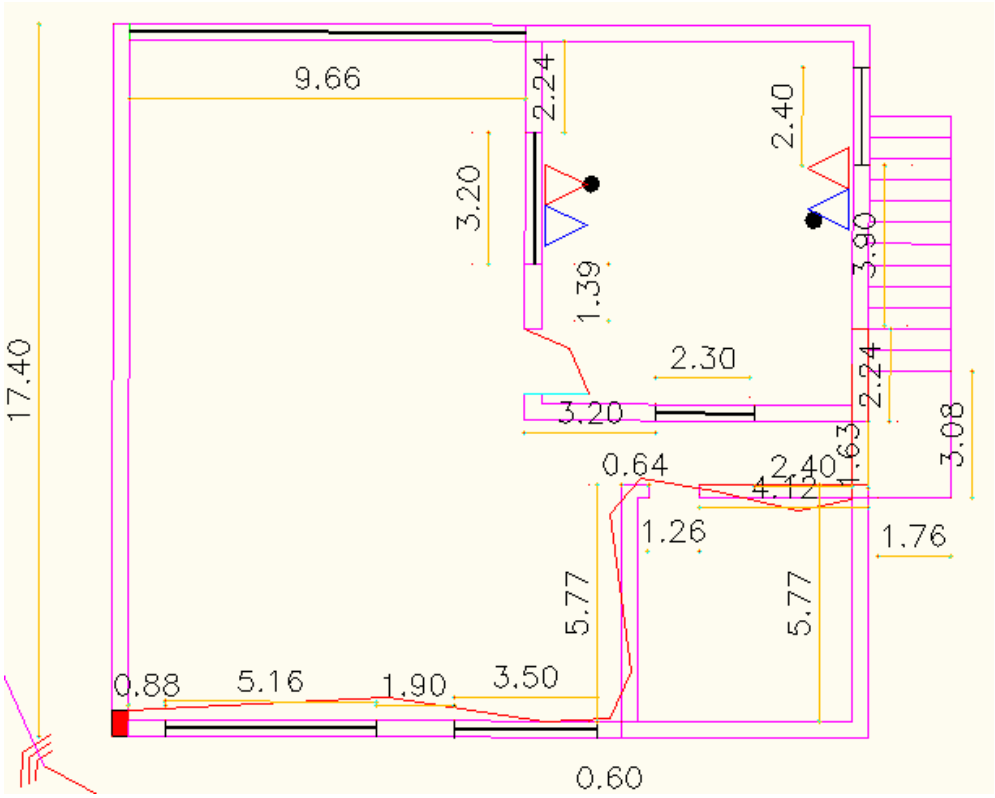

Figura 3-12: Plano Planta Producción

Fuente: Autor

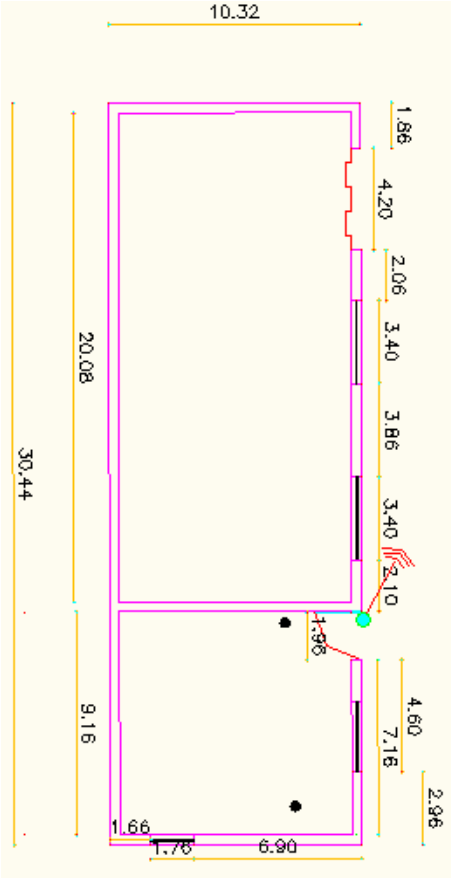

Figura 3-13: Bodega

Fuente: Autor

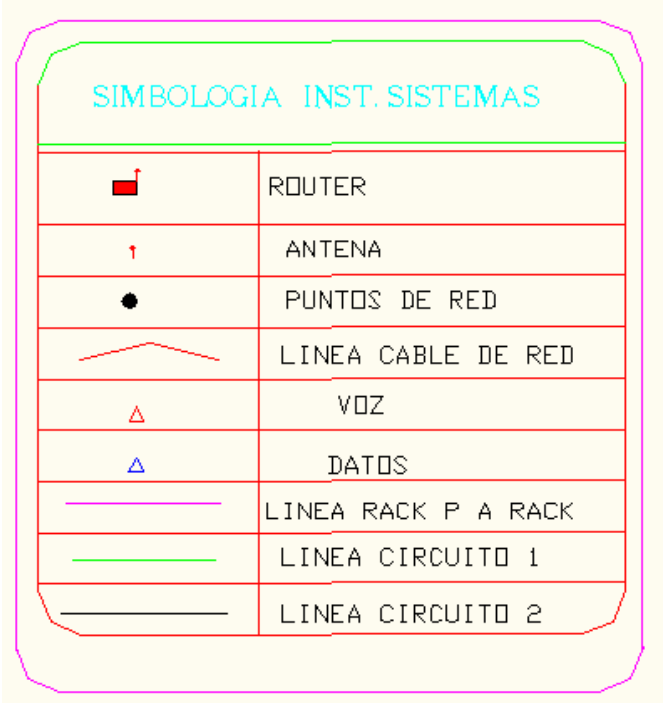

Figura 3-14: Simbología

Fuente: Autor

CAPITULO 4. IV. IMPLEMENTACIÓN DEL SISTEMA DE CABLEADO ESTRUCTURADO Y RED INALÁMBRICA PARA HORMIGONES DEL VALLE S.A.

El problema actual que tiene la empresa es una deficiente red cableada, para lo cual se implementará un diseño de cableado estructurado en las plantas Administrativas, de Producción y Control Biométrico, y una implementación de red wireless a Bodega.

4.1.1 INSTALACIÓN DE LOS PUNTOS DE RED

La empresa Hormigones del Valle S.A., está conformada por 3 plantas, en las cuales está previsto tener, por cada área de trabajo, un punto de red, que consta de un punto de datos y un punto de voz, teniendo un total en toda la empresa 16 puntos de red.

1. La planta administrativa consta de diferentes dependencias, algunas están separadas por paredes o se encuentran en el mismo espacio físico, y aquí se instalará un total de 14 puntos de red.

Figura 4-1: Planta Administrativa
Fuente: Autor

Figura 4-2: Planta Administrativa vista lateral

Fuente: Autor

Las dependencias que existen en esta planta son:

- Recepción:

  Recepción constará de 2 puntos de red, que están destinados a la estación de trabajo y a la impresora en red.

- Ventas:

  Constará de 2 puntos de red, ya que por el volumen de información, se necesitan dos estaciones.

- Contabilidad:

  Por su gran cantidad de ingresos y egresos, este departamento constará de 4 puntos de red.

- Seguridad Industrial

  Como en este departamento está encargada una sola persona, se estima colocar solo 1 punto de red.

- Marketing:

  Se instalará 1 punto de red, ya que este departamento no demanda mucho uso de la red.

- Gerencia:

  Se instalara 1 punto de red, puesto que en gerencia está encargada una sola persona.

- Administración:

  Al igual que en Gerencia, sólo se necesita 1 punto de red.

- Departamento Médico:

  En este departamento se instalará 1 punto de red, para la emisión de certificados respectivos, la cual está encargada una sola persona de emitir dichos documentos.

- Sala de Reuniones:

  Aquí, por petición del administrador, se instalara 1 punto de red, para conectar un equipo para cuando se utilice este espacio.

Figura 4-3: Rack Principal(RACKP)

Figura 4-4: Rack Secundario(RACK)

A unos pocos metros de la planta administrativa se encuentra el control biométrico de la empresa, y aquí se instalará el punto de red necesario para que cumpla su función.

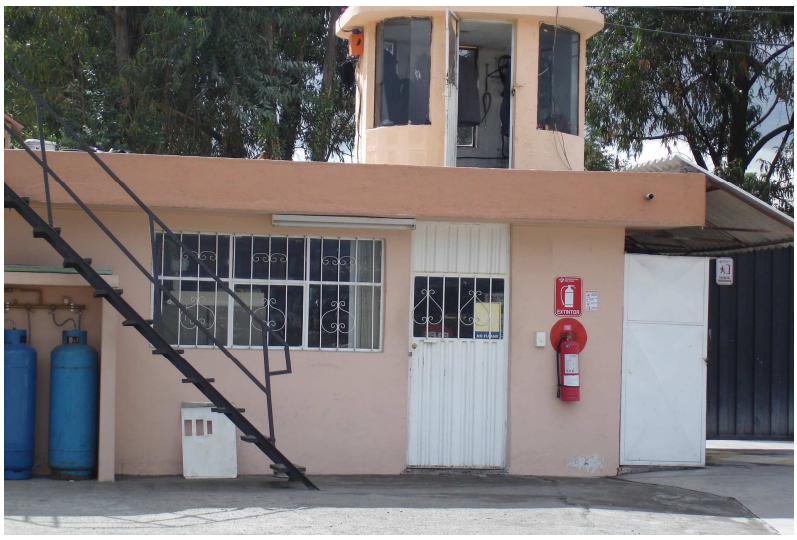

Figura 4-5: Control Biométrico

Figura 4-6: Estación de Trabajo Control Biométrico

2. La segunda planta, de Producción, se encuentra en una estructura de dos pisos, los puntos de red están ubicados en el segundo piso, ya que por el uso de los equipos necesitan monitorear el proceso de producción de su producto, y se instalarán 2 puntos de red.

Figura 4-7: Access Point Producción

Figura 4-8: Estación de Trabajo Producción

Figura 4-9: Estación de Trabajo Producción

3. La segunda planta, es Bodega, esta planta está dividida en dos partes, y por su ubicación, es necesaria la red Wireless

Figura 4-10: Bodega

Figura 4-11: Antenas Wireless Bodega

Se debe tener en cuenta que los puntos de acceso a la red, por el espacio físico y como están distribuidas, necesitarán estar en puntos estratégicos, para mayor facilidad de instalación, conexión e imagen.

4.1.2 TENDIDO DE CABLES

Se procede al tendido de cable UTP, categoría 5, mediante canaletas pegadas en la pared hacia cada estación de trabajo, esto es en el área administrativa.
Aquí tenemos las áreas de recepción, ventas, contabilidad, seguridad industrial, marketing, gerencia, administración, departamento médico, sala de reuniones y el servidor.

La conexión se la hará hacia 2 racks, el principal tendrá la conexión del servidor, departamento médico, gerencia, administración y marketing. También en este sector habrá una impresora en red, y desde este rack saldrá hacia el control biométrico, hacia el segundo rack y hacia dos repetidores para la planta de Producción y esta reparte a Bodega la señal inalámbrica.

El segundo rack abarca lo que es: recepción, ventas, contabilidad, seguridad industrial y una segunda impresora en red.

El primer repetidor antes mencionado, está ubicado a unos 70 metros de la planta administrativa, el segundo repetidor esta a otros 70 metros del primer repetidor conectado por cable UTP categoría 5. Llega hacia un router inalámbrico ubicado en la planta de producción, para de aquí hacer un cableado en esta planta con canaletas hacia las estaciones de trabajo.

Figura 4-12: Tendido cable UTP de Administración hacia Producción

Figura 4-13: Repetidor

4.1.3 IMPLEMENTACIÓN DE WIRELESS

La red inalámbrica se empleará en la planta de bodega, ya que el uso de esta planta también es de mantenimiento de maquinaria, y por la interferencia, ruido y atenuación que producen las máquinas es necesaria la implementación de wireless, la señal recibe del router inalámbrico ubicado en la planta de producción.

4.1.4 INTRODUCCIÓN HARDWARE ROUTER D-LINK DIR-655

Se hará una descripción de las partes del router.

4.1.4.1 Panel Posterior

En este panel se encuentran los puertos Lan, conexión de internet, conector USB, botón reset, y alimentación de poder.

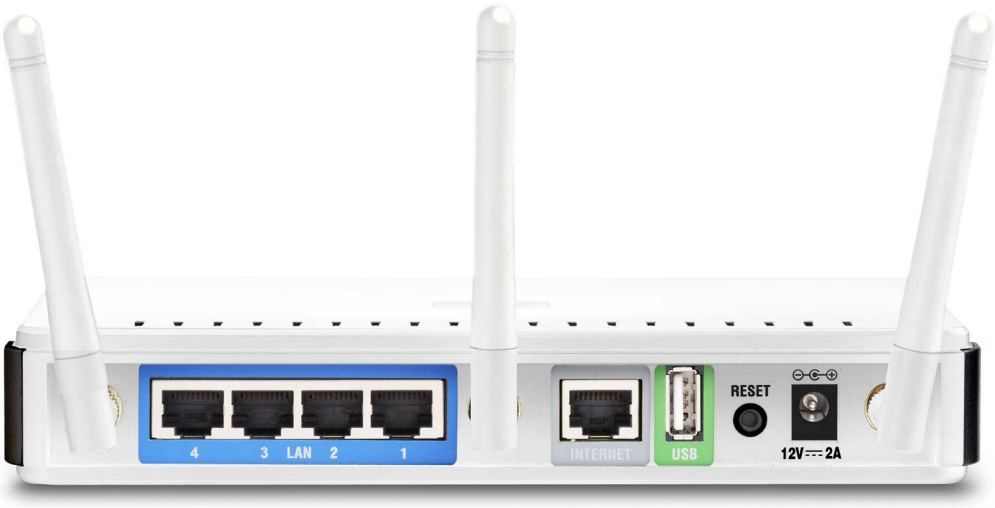

Figura 4-14: Panel posterior router D-link Dir-655
Fuente: Manual

4.1.4.1.1 Puertos LAN

Conectar los dispositivos Ethernet como computadoras, switches y hubs, teniendo 4 puertos disponibles.

4.1.4.1.2 Puerto Internet

Es la conexión desde el cable Ethernet hacia el modem DSL.

4.1.4.1.3 USB

Conectar USB 1.1 o 2.0 “flash drive” para configurar las opciones del wireless usando WCN.

4.1.4.1.4 Reset

Presionando este botón, se restaura el router a su configuración original de fábrica.

4.1.4.1.5 Receptor de Poder

El voltaje con que trabaja el router.

4.1.4.2 Panel Frontal

Indicadores sobre el estado del router, Power Led, Status Led, Internet Led, WLAN Led, WCN Led, Local Network Led.

Figura 4-15: Panel frontal router D-link dir-655

Fuente: Manual

4.1.4.2.1 Power Led.

Esta luz indica la apropiada conexión del cable de poder

4.1.4.2.2 Status Led

La luz parpadeante indica que el router está listo.

4.1.4.2.3 Internet Led

Indica la conexión a internet. La luz parpadea durante la transmisión de datos.

4.1.4.2.4 WLAN Led

Esta luz indica que el segmento de wireless está listo, La luz parpadea durante la transmisión de datos.

4.1.4.2.5 WCN Led

Inserte una memoria USB con información WCN. El led parpadeará 3 veces si las opciones del wireless se transfirieron exitosamente.

4.1.4.2.6 Local Network Leds

Esta luz indica la conexión Ethernet, la luz parpadea durante la transmisión de datos.

4.1.5 INTRODUCCIÓN AL SOFTWARE DEL ROUTER D-LINK DIR-655

Se refiere a la configuración del router.

1. Se conecta el router hacia el PC, en el navegador se escribe la dirección 192.168.0.1

Figura 4-16: Pantalla de Internet Explorer

Fuente: Captura de pantalla

2. Pantalla de login, en password dejar el campo en blanco y pulsar “Log In”.

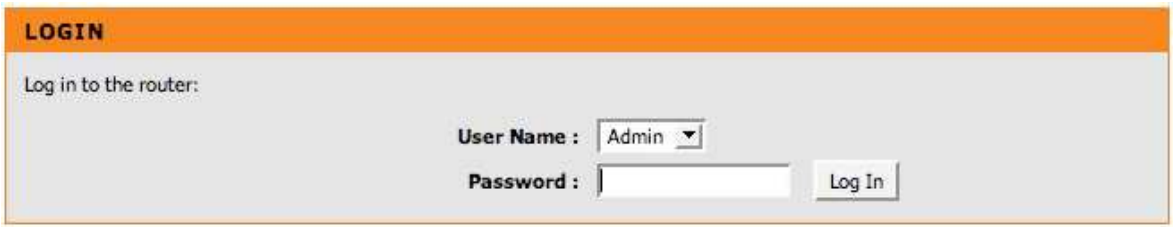

Figura 4-17: Pantalla de Log In

Fuente: Captura de pantalla

3. Click en la opción “Setup Wizard”, para una configuración rápida del router. Configurar las opciones sin la ayuda del wizard, “Manual Configuration”.

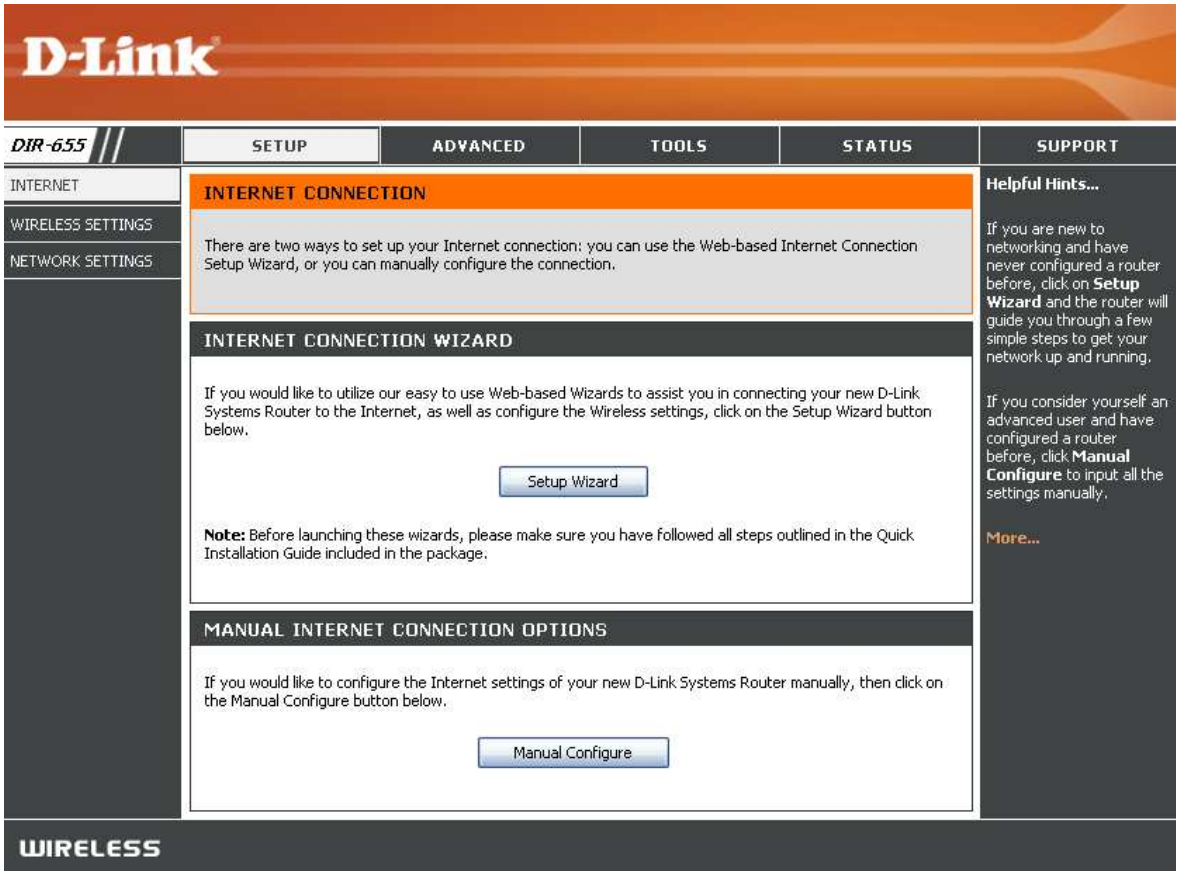

Figura 4-18: Pantalla de Configuración de Internet

Fuente: Captura de pantalla

4. Opción Setup Wizard, y “Launch Internet Connection Setup Wizard para iniciar la configuración.

Configurar las opciones de wireless, “Launch Wireless Security Setup Wizard”.

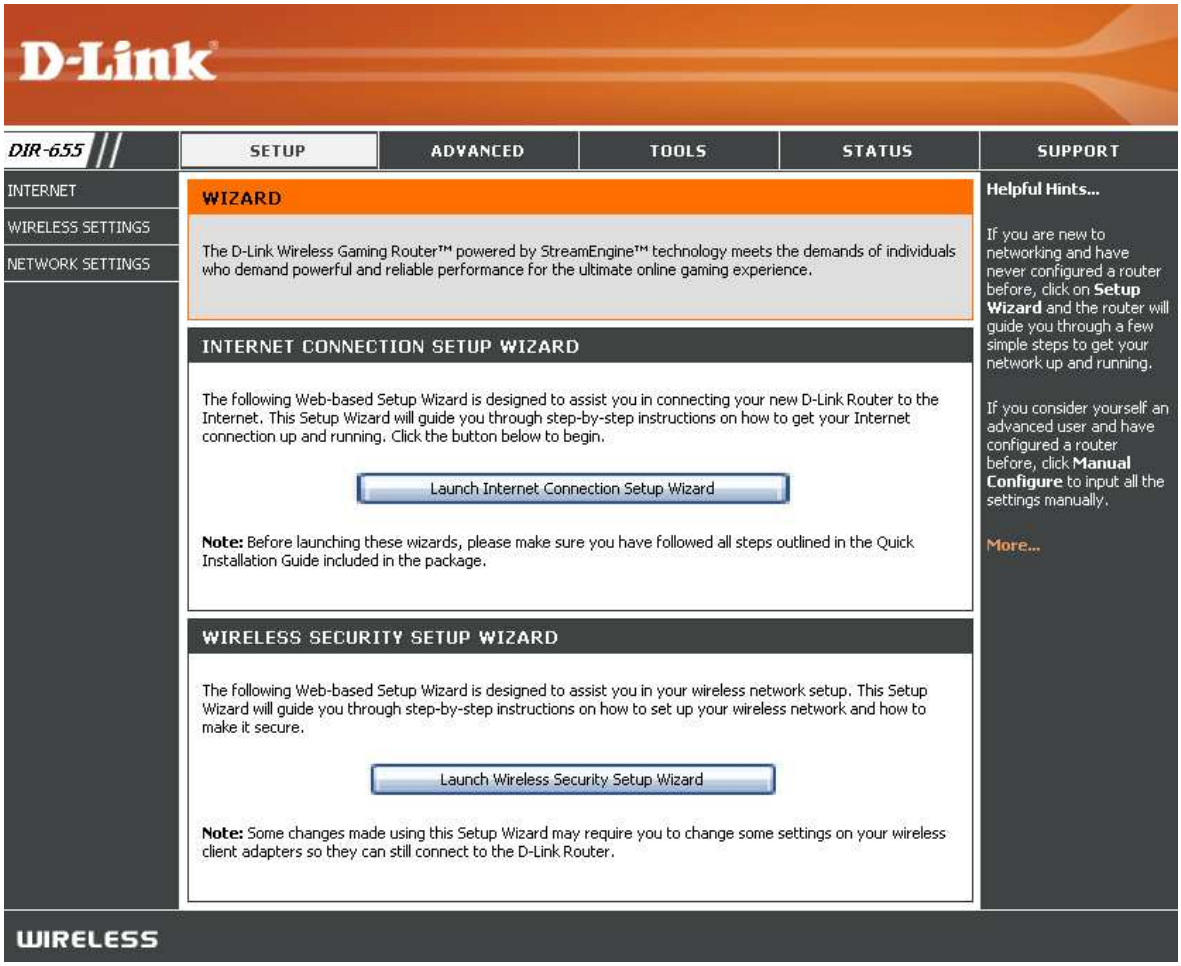

Figura 4-19: Pantalla de configuración básica

Fuente: Captura de pantalla

5. Next.

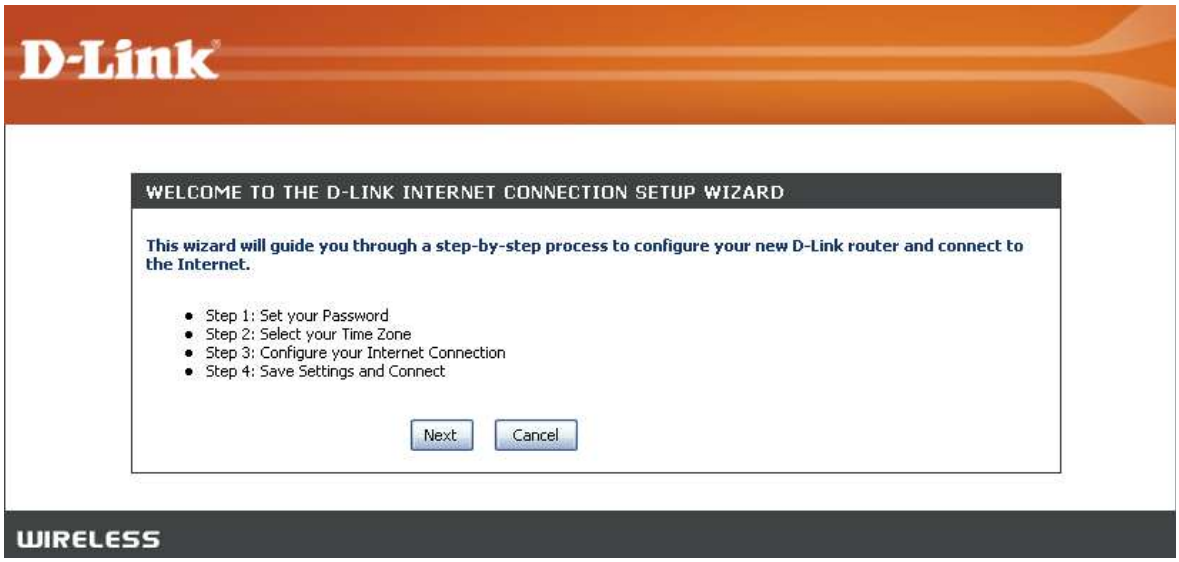

Figura 4-20: Pantalla inicial de configuración a internet.

Fuente: Captura de pantalla

6. Crear una nueva “Password”, confirmar, Next.

Figura 4-21: Configuración de password.

Fuente: Captura de pantalla

7. Zona horaria, Next para continuar.

Figura 4-22: Configuración zona horaria.

Fuente: Captura de pantalla

8. Conexión a internet, en este caso es conexión DHCP, Next.

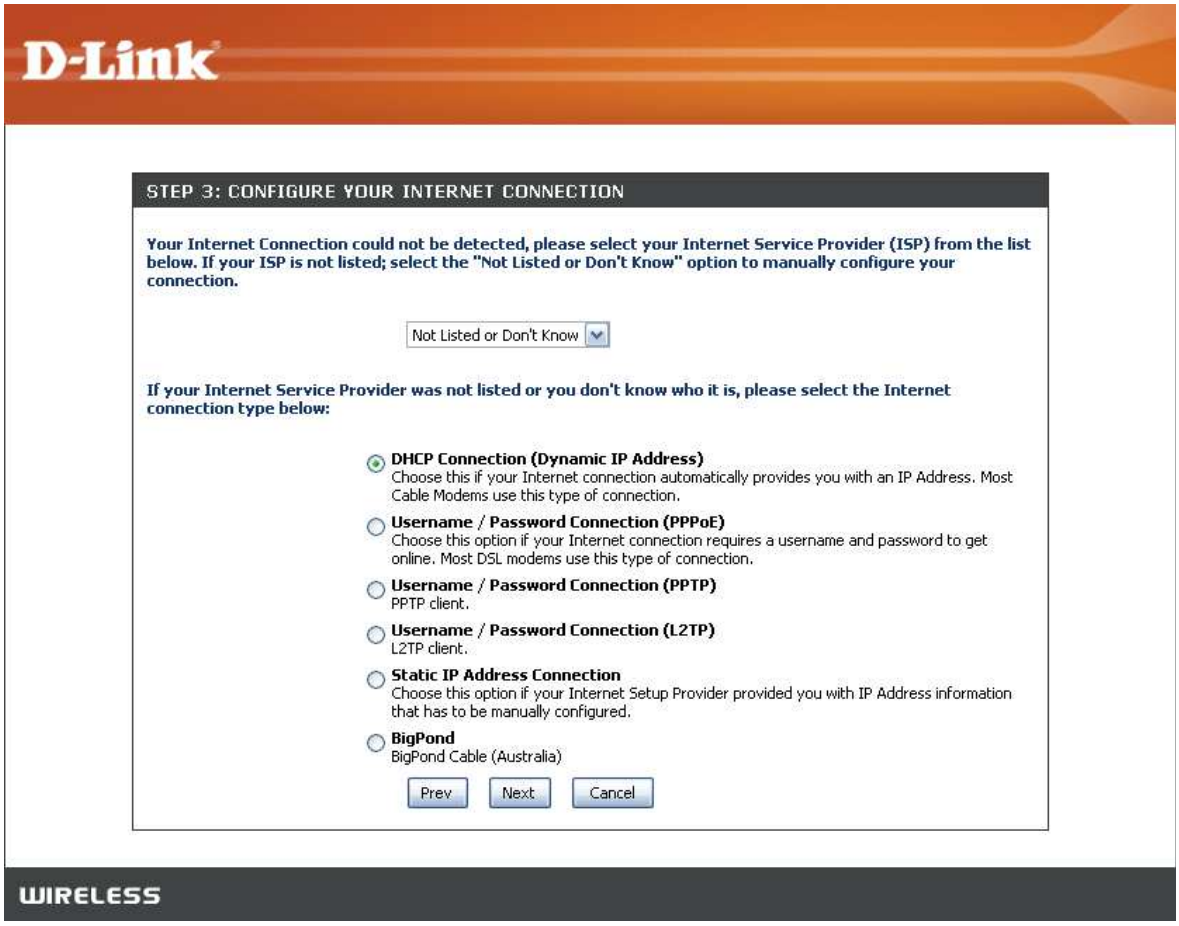

Figura 4-23: Configuración de la conexión a Internet

Fuente: Captura de pantalla

9. En esta pantalla, se necesita la dirección MAC de la computadora que está conectada directamente al moden. En el caso de una computadora, pulsar en “Clone Your PC’s MAC Address” y Next.

El “Host Name” es opcional, en algunos ISPs es requerido. El host name predeterminado es el nombre del router y puede ser cambiado.

- El Host Name aparecerá por default como dlink.

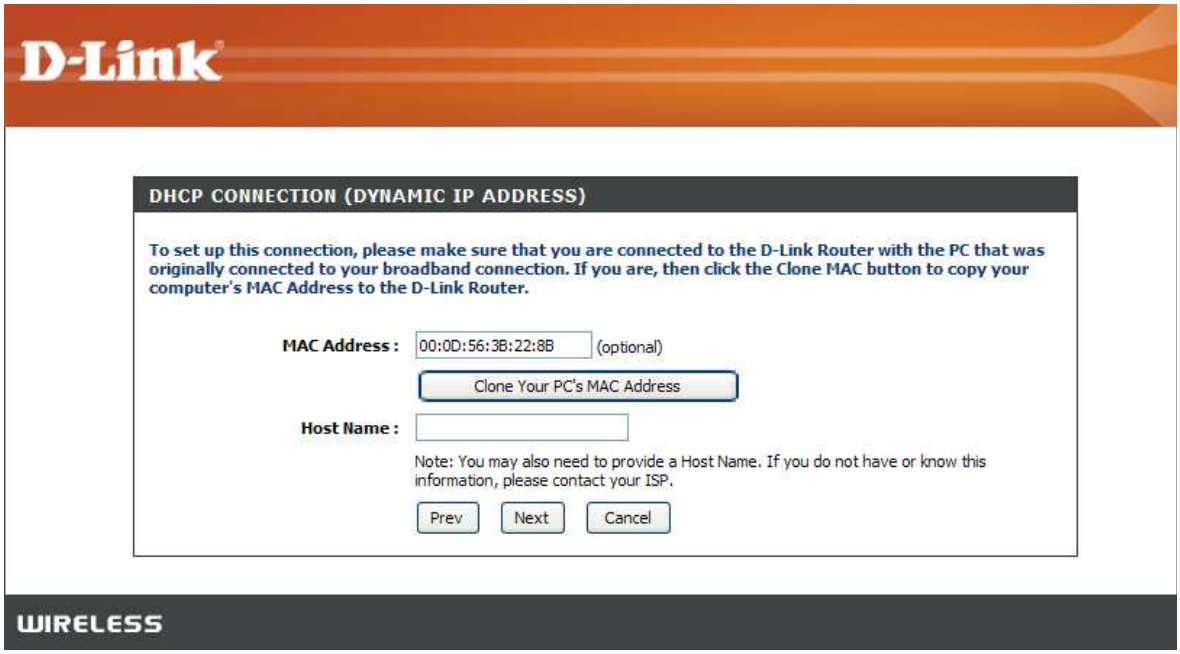

Figura 4-24: Configuración DHCP mediante Wizard

Fuente: Captura de pantalla

Esta opción es la más común.

10. PPPoE, usuario PPPoE y la contraseña, Next.

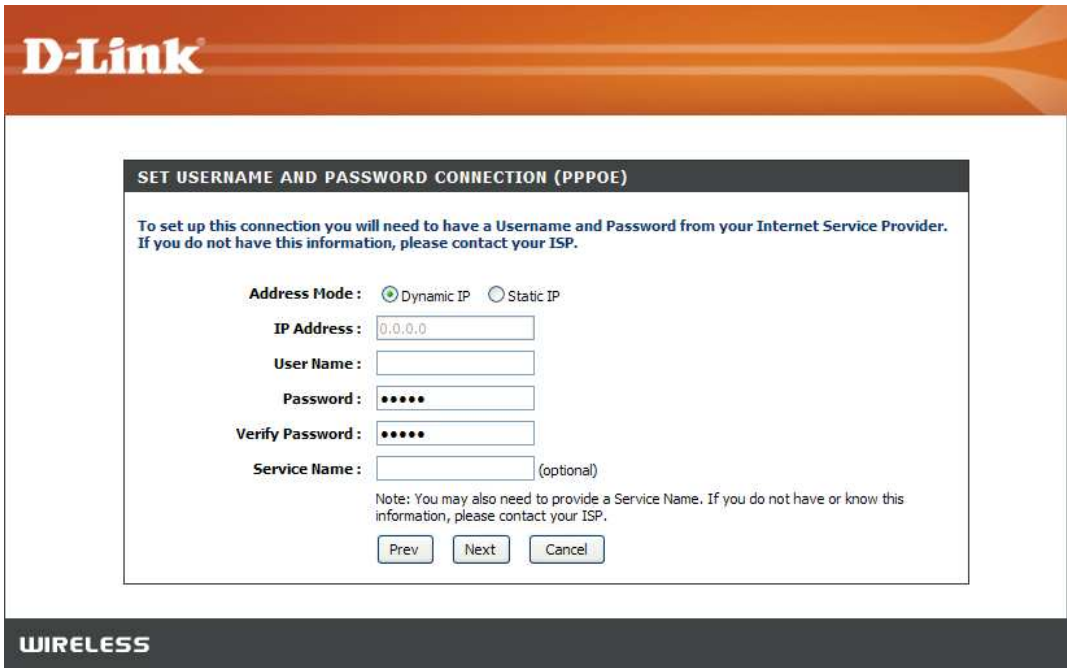

Figura 4-25: Configuración PPPoE mediante Wizard

Fuente: Captura de pantalla

11. PPTP, usuario PPTP y la contraseña, Next.

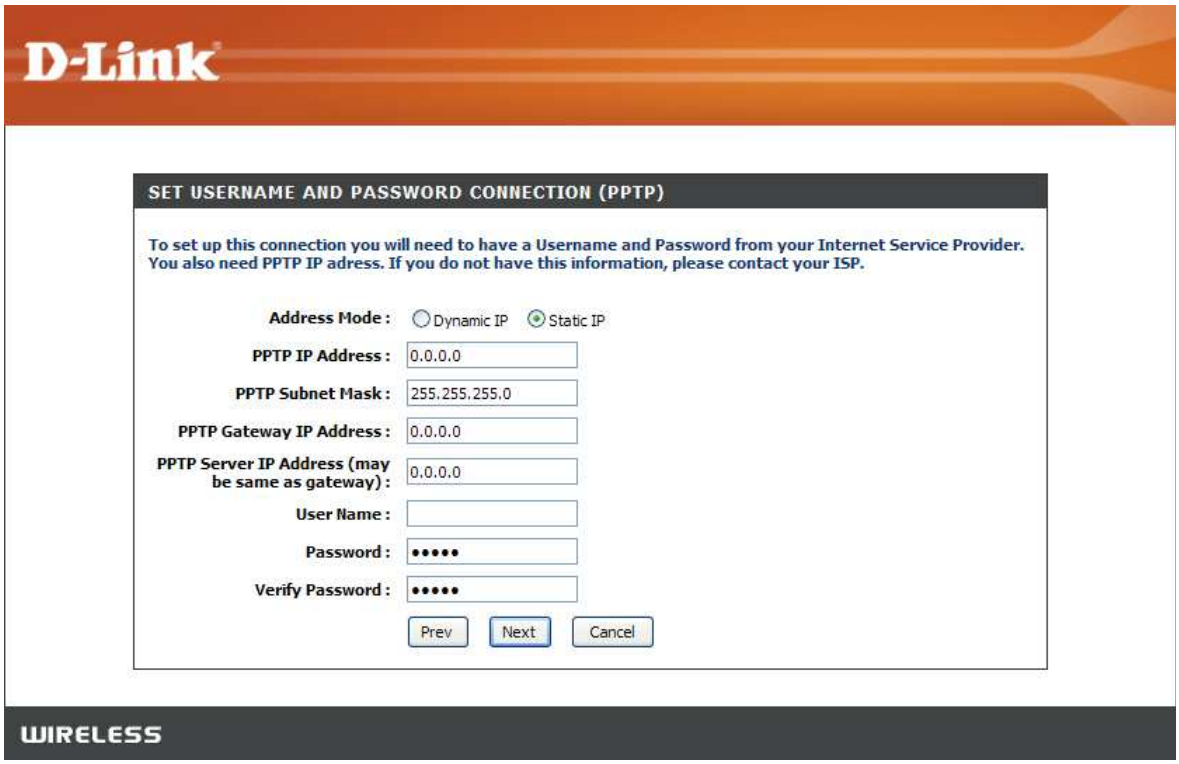

Figura 4-26: Configuración PPTP mediante Wizard

Fuente: Captura de pantalla

12. L2TP, usuario L2TP y la contraseña, Next.

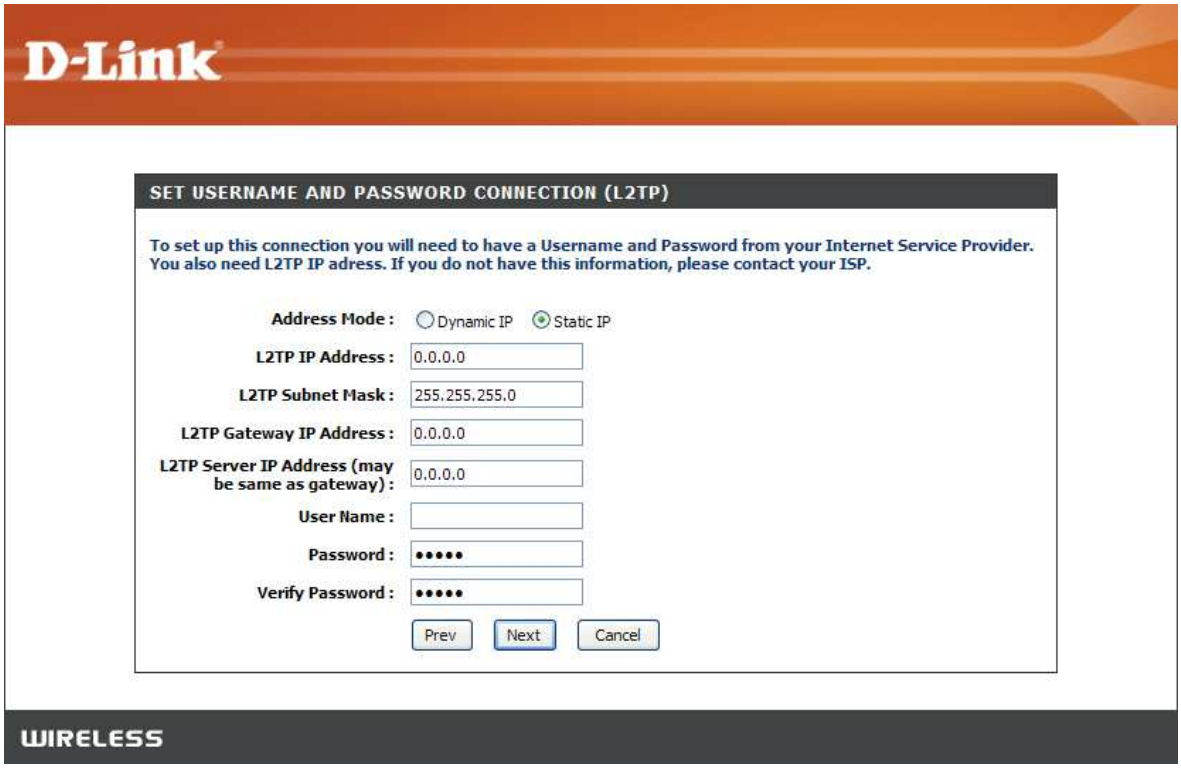

Figura 4-27: Configuración L2TP mediante Wizard

Fuente: Captura de pantalla

13. “Static”, ingresar las opciones de internet provistas por el proveedor de internet, Next.

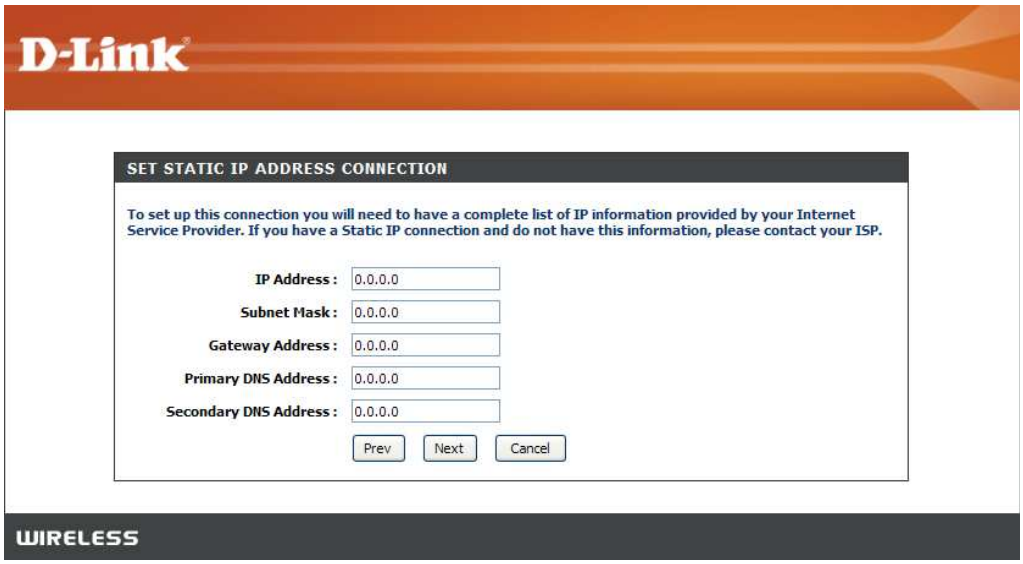

Figura 4-28: Configuración direcciones IP

Fuente: Captura de pantalla

14. “Connect” para guardar cambios. Una vez el router término de reiniciarse, tomara unos pocos segundos para iniciar la conexión a internet.

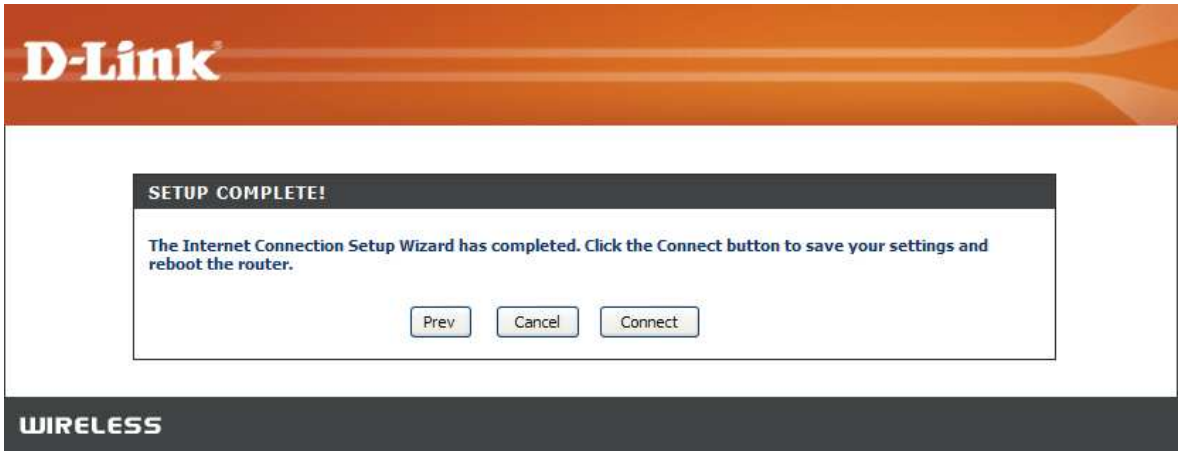

Figura 4-29: Configuración completa mediante Wizard

Fuente: Captura de pantalla

4.1.6 INSTALACIÓN DEL ADAPTADOR USB WIRELESS 150 DWA-125

Este adaptador se instala y se configura mediante el CD de instalación adjunto.

4.1.6.1 Introducción al Hardware del Wireless Adapter DWA-125.

Consta del botón WPS y del puerto USB.

4.1.6.1.1 WPS Button

Presionar el botón WPS para una conexión automática a una red wireless WPS activa.

4.1.6.1.2 Puerto USB

Usado para conectar el dispositivo a la computadora

Figura 4-30: Dispositivo DWA-125

Fuente: Manual

4.1.6.2 Introducción al Software del Wireless Adapter DWA-125

Aquí se explicará la instalación del dispositivo.

1. Para prevenir algún conflicto con otros adaptadores para red wireless deshabilitar los adaptadores wireless.

2. Para deshabilitar, click derecho en Mi PC y seleccionamos Propiedades.

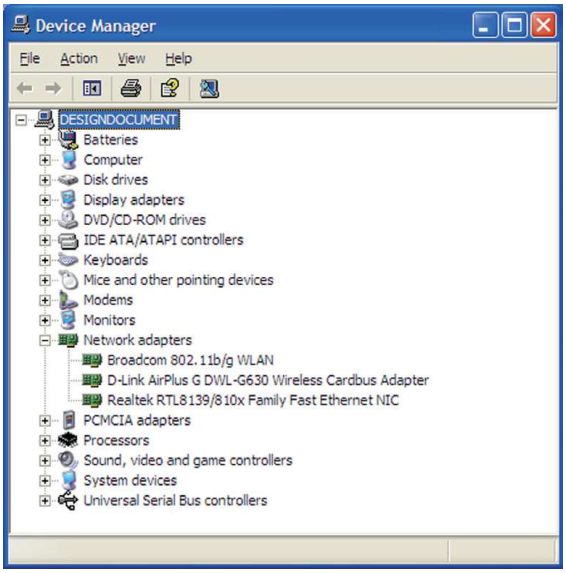

Figura 4-31: Pantalla Dispositivos de la PC

Fuente: Captura de pantalla

3. Click derecho en el adaptador y deshabilitar.

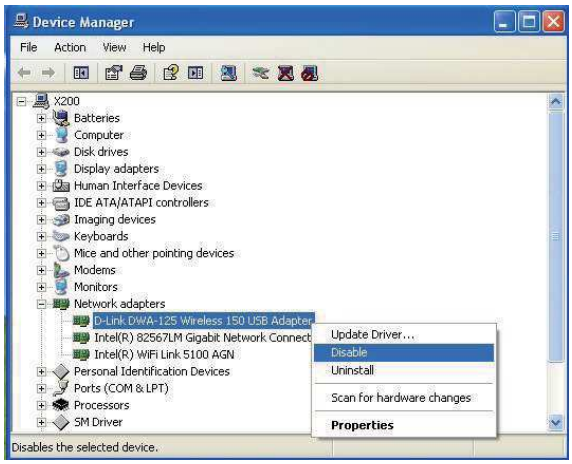

Figura 4-32: Deshabilitar dispositivo de red

Fuente: Captura de pantalla

4. Aceptar.

Figura 4-33: Pantalla confirmación

Fuente: Captura de pantalla

5. El adaptador que puede crear conflicto está ahora deshabilitado, aparecerá una “X” roja.

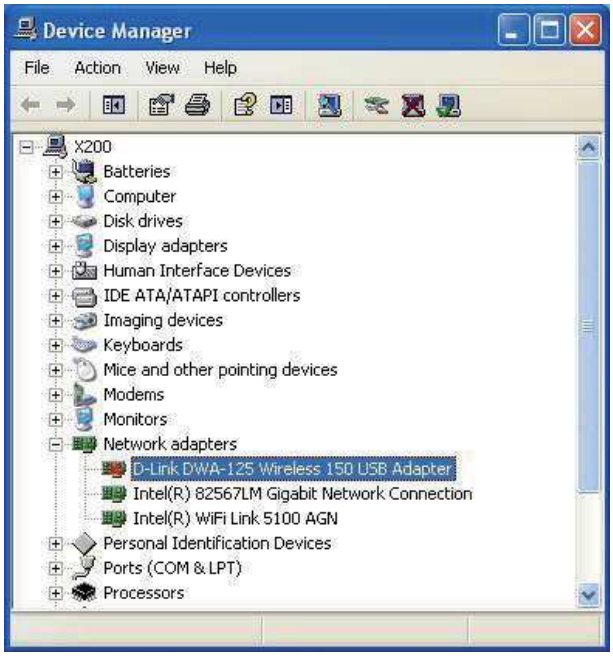

Figura 4-34: Visualización de dispositivo deshabilitado

Fuente: Captura de pantalla

6. CD de instalación y pulsar Install Drivers.

Figura 4-35: Pantalla inicial instalación dispositivo

Fuente: Captura de pantalla

7. Next.

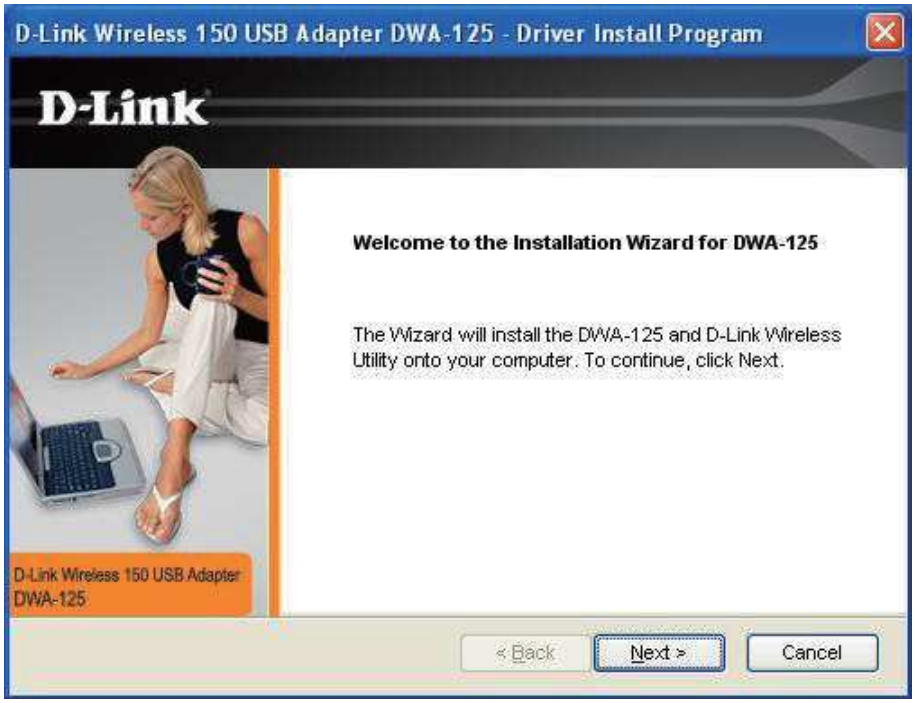

Figura 4-36: Pantalla de Bienvenida

Fuente: Captura de pantalla

8. Por defecto se instalará en la dirección: C:\ProgramFiles\D-Link\DWA-125, Next.

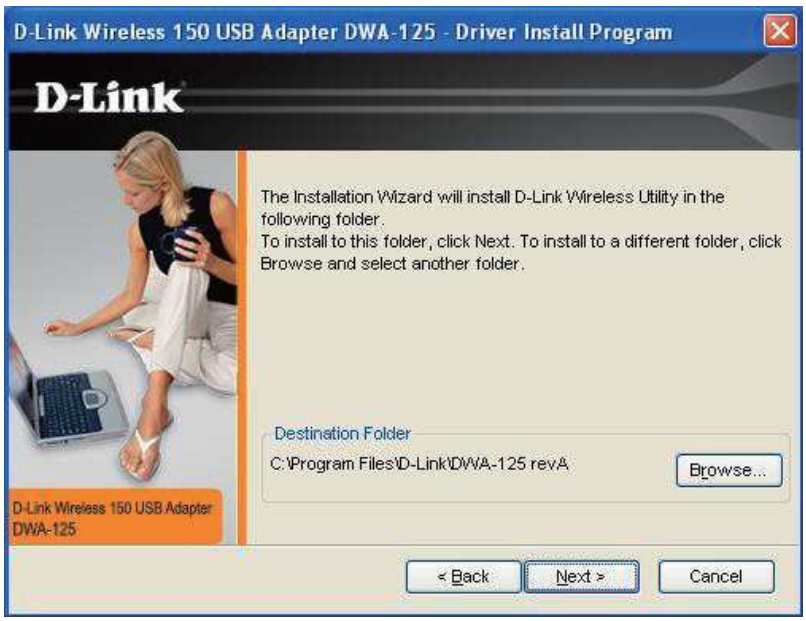

Figura 4-37: Directorio de Instalación

Fuente: Captura de pantalla

9. Next.

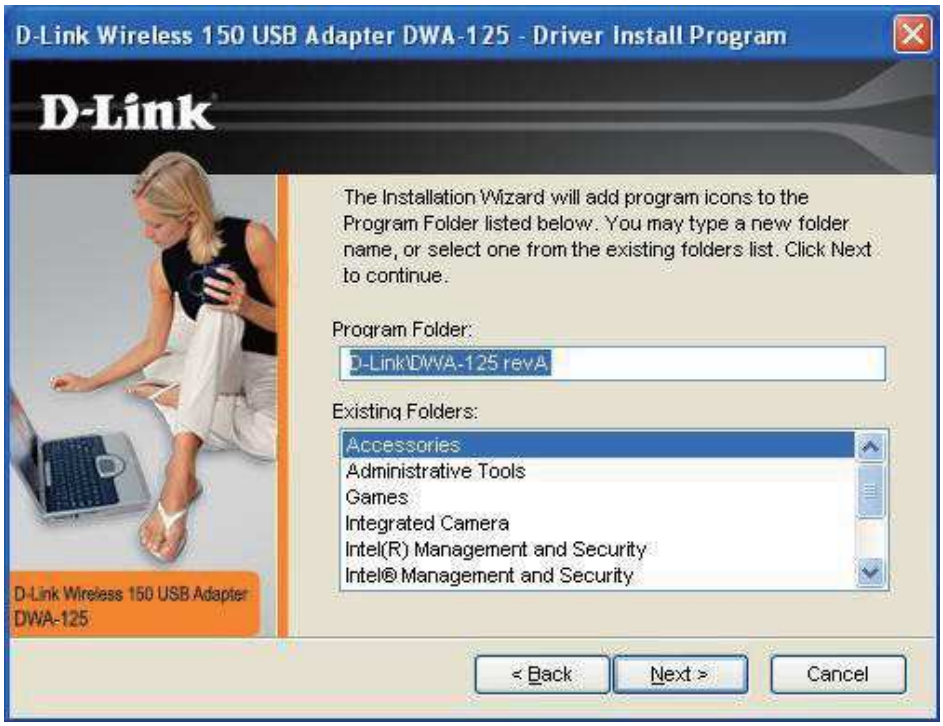

Figura 4-38: Selección de Carpeta

Fuente: Captura de pantalla

10. Insertar USB a la computadora, Next.

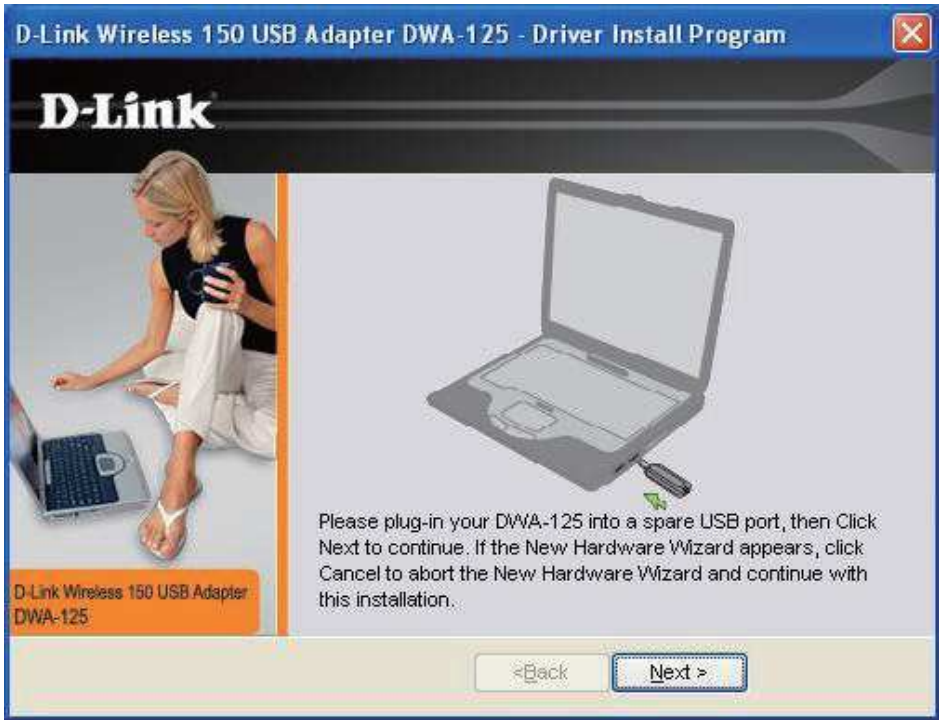

Figura 4-39: Pantalla para conectar dispositivo al PC

Fuente: Captura de pantalla

11. La conección wireless aparecerá, Next.

Conectar manualmente, los siguientes opciones conectaran a una red wireless usando Wi-Fi Protected Setup (WPS).

Figura 4-40: Pantalla selección que método usar

Fuente: Captura de pantalla

12. Para conectar la red usando el método de configuración del botón WPS, presionar en el botón virtual como se muestra en la pantalla.

Figura 4-41: Pantalla de configuración botón WPS

Fuente: Captura de pantalla

13. Presionar el botón WPS del Access point, esperar 2 minutos hasta que establezca la conexión.

Figura 4-42: Pantalla de espera

Fuente: Captura de pantalla

14. Cuando termine ese proceso, una pantalla aparecerá avisando que la conexión fue exitosa. Next para completar la instalación.

Figura 4-43: Pantalla de conexión exitosa

Fuente: Captura de pantalla

15. Para configurar la red, doble click en el icono del software del escritorio.

Figura 4-44: Icono software

Fuente: Captura de pantalla

16. La pantalla, la pestaña de las redes wireless “Wireless Networks” aparecerá con las redes disponibles que están dentro del alcance, para conectar a una red, simplemente seleccionar la red que se va a conectar (SSID) y click en connect.

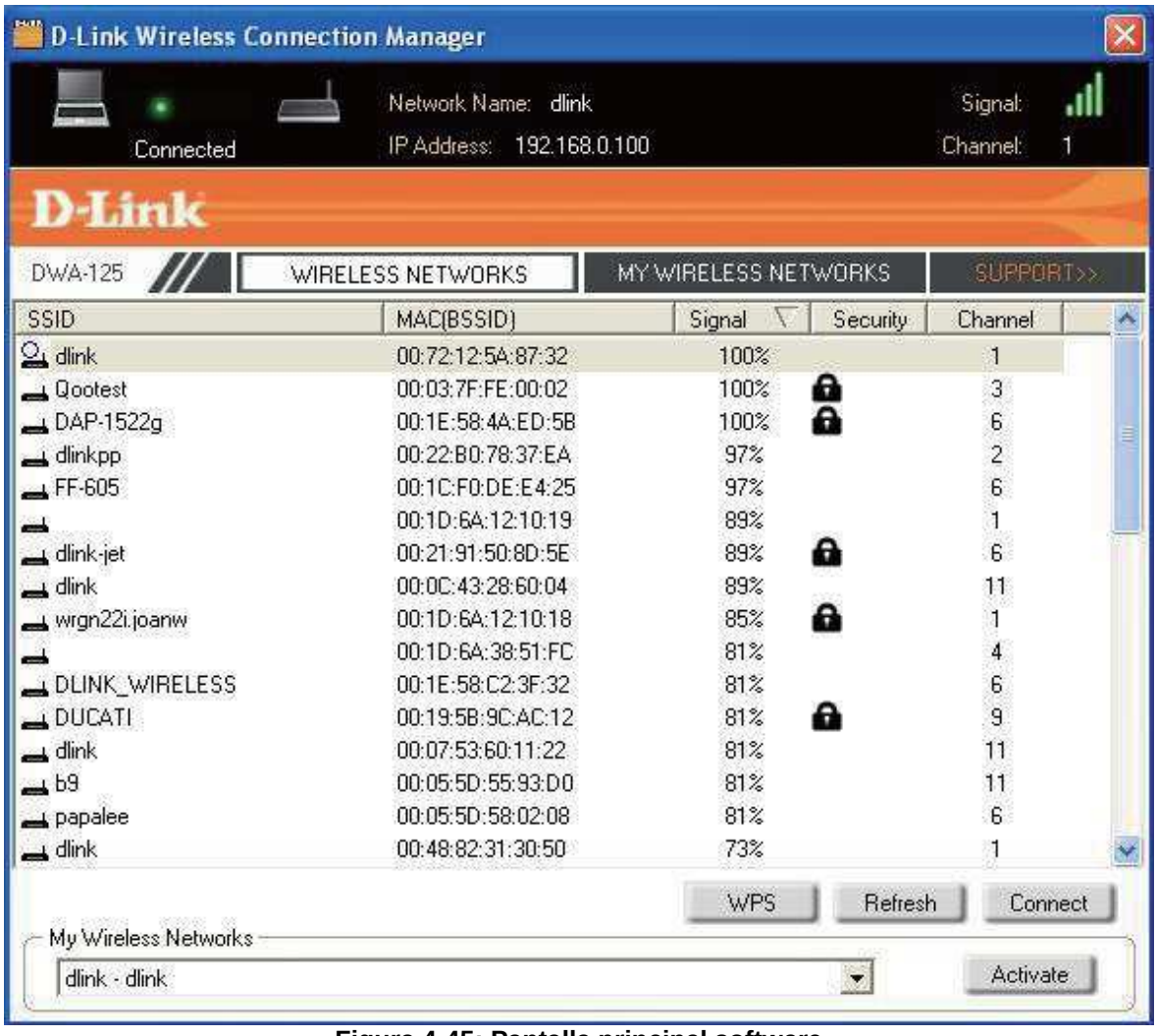

Figura 4-45: Pantalla principal software

Fuente: Captura de pantalla

- SSID: De sus siglas en ingles Service Set Identifier, es el nombre de la red wireless.

- MAC: Despliega la dirección MAC del dispositivo wireless.

- Signal: Despliega la calidad o intensidad de la conexión wireless

- Security: Si esta un icono “look” o un candado, significa que la red es segura, importante saber código de encriptación para poder conectarse.

- Channel: Despliega el canal de la red wireless.

- WPS Button: Para conectarse a una red wireless usando la configuración protegida Wi-Fi.

- Refresh Button: Re-escanea por redes disponibles en nuestra area.

- Connect Button: Seleccionar una red wireless, y presionamos en el botón “Connect”, si la red es segura, una ventana aparecerá. Llenamos la información para conectar referida a la seguridad de la red.

- Activate Button: Seleccionar el perfil de una red wireless del menú ubicado en la parte inferior, presionamos “Activate” para conectar. Esperamos sobre 30 segundos para conectar.

17. En la pestaña “My Wireless Networks”, permite crear, editar y borrar perfiles de las redes wireless. Cada vez que se conecte a una red usando esta pestaña, un perfil automáticamente se creará.

Figura 4-46: Pestaña Wireless Connection Manager

Fuente: Captura de pantalla

- New Button: “New” para crear una red wireless.
- Modify: “Modify” para editar un perfil existente.
- Delete: “Delete” para remover un perfil.
- Activate: “Activate” para usar un perfil, el tiempo de espera es sobre los 30 segundos para conectarse.
- Profile Details: Esta sección muestra información sobre las redes wireless, tales como nombre (SSID), tipo de red (infraestructura) y si la red es segura.

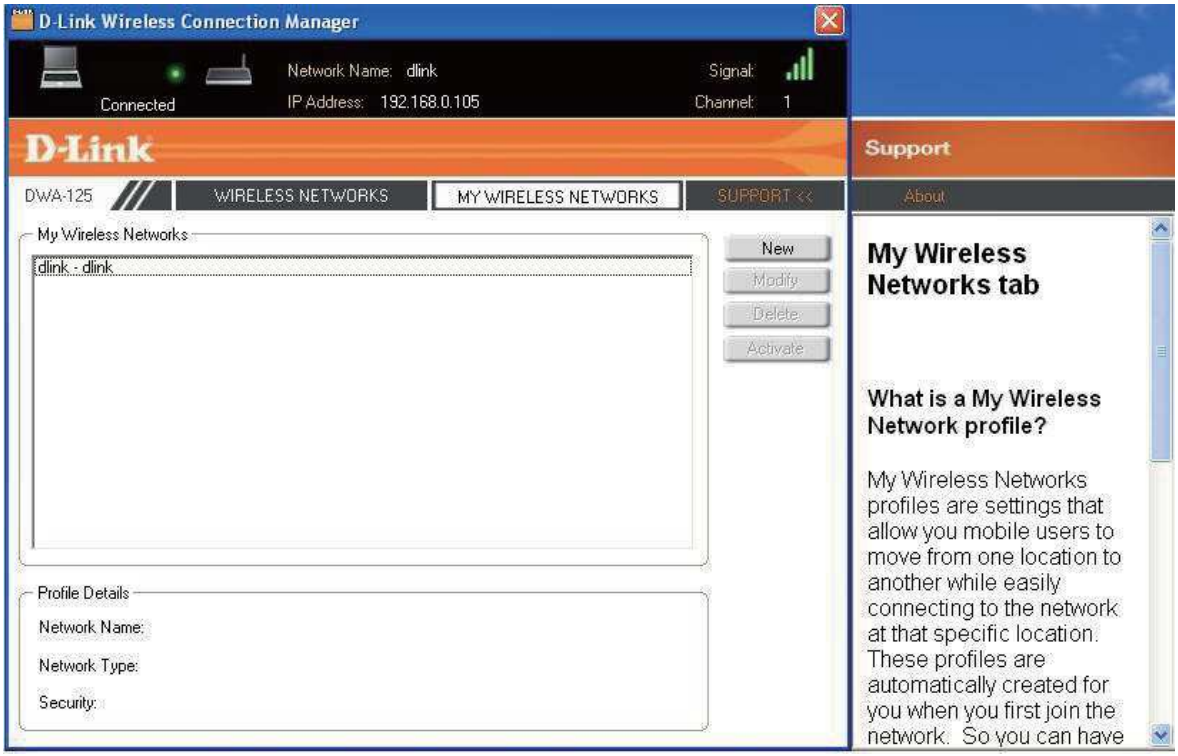

Figura 4-47: Visualización pestaña Support

Fuente: Captura de pantalla

18. La pestaña de “Support”, es para información de ayuda, un panel aparecerá con la información sobre la utilidad.

Figura 4-48: Versión del Software

Fuente: Captura de pantalla

4.1.7 CONEXIÓN DESDE UN PC HACIA LA RED INALAMBRICA CREADA.

El método en Windows es muy simple, en la barra de tareas del escritorio, nos dirigimos al icono de redes disponibles.

1. Doble click a la utilidad para conectarnos.

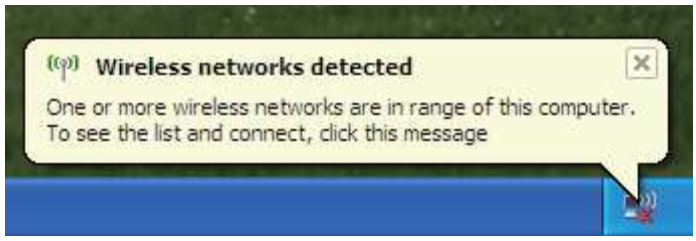

Figura 4-49: Vista de WLAN detectada

Fuente: Captura de pantalla

2. Si no detecta la red, click derecho en el icono de wireless de la computadora, y seleccionar una red.

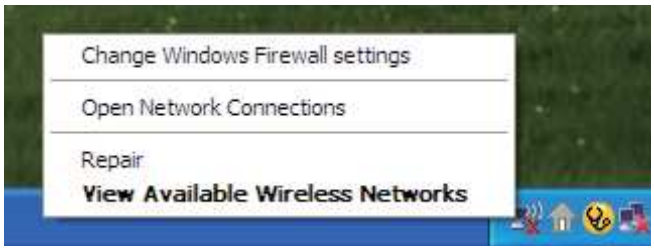

Figura 4-50: Pantalla de vista de redes disponibles

Fuente: Captura de pantalla

3. Aparecerá una pantalla con las redes disponibles, escojer la red que se creo (SSID), en este caso “dlink”, y “conectar”

Si se recibe buena calidad de señal, y no hay conexión, chequear las propiedades de TCP/IP.

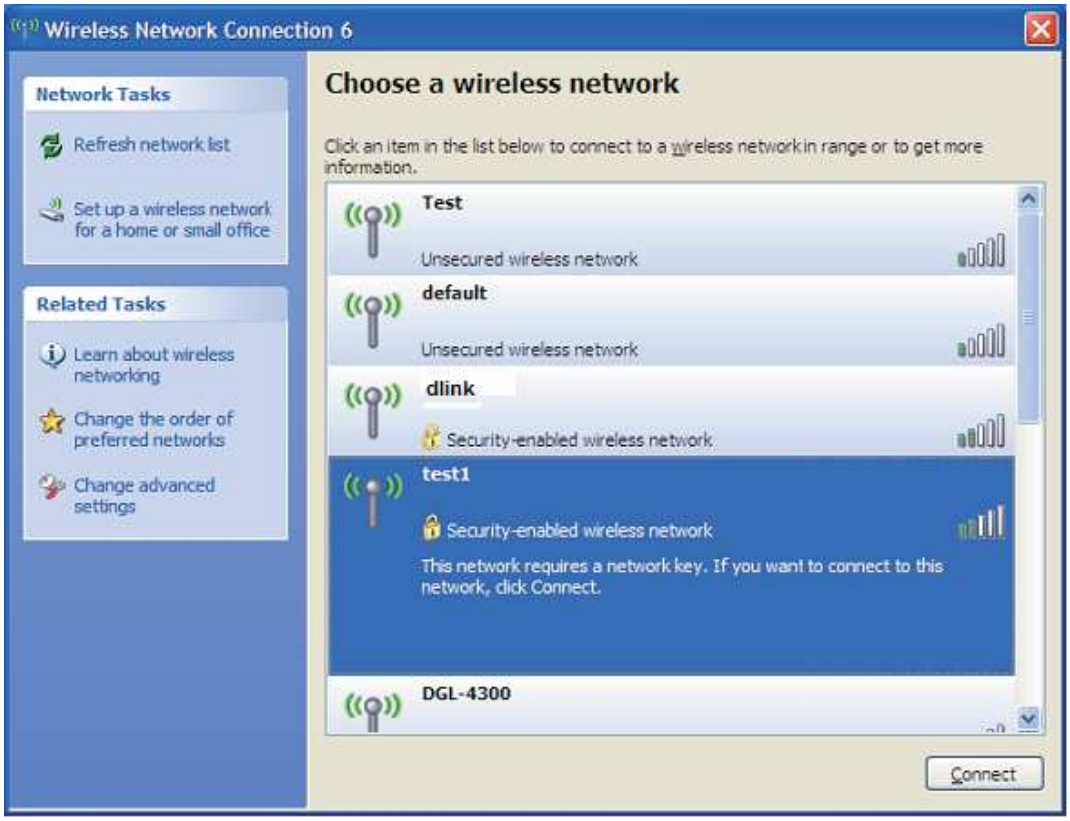

Figura 4-51: Redes disponibles

Fuente: Captura de pantalla

4. Si la red tiene seguridad, escribir la contraseña, caso contrario se conectara automáticamente.

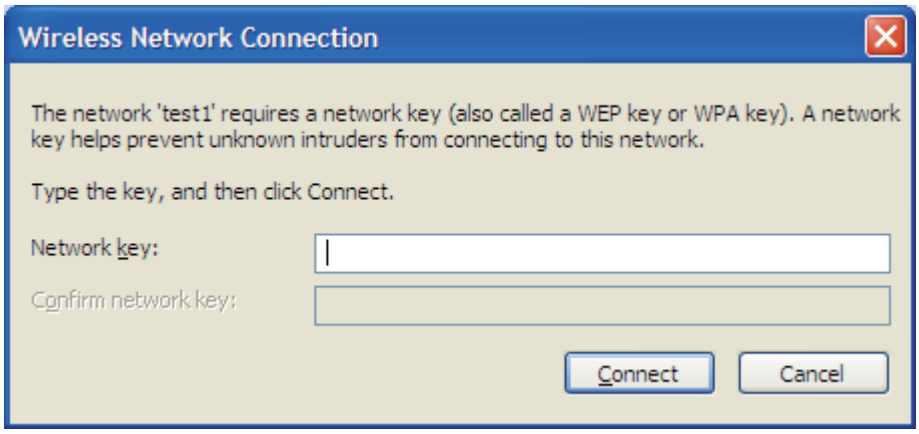

Figura 4-52: Pantalla de contraseña

Fuente: Captura de pantalla

4.1.8 CONFIGURACIÓN DEL PROTOCOLO TCP/IP

En Windows XP, click derecho en Inicio, Panel de control, doble click en Conexiones de red, y hacemos click derecho Propiedades en el adaptador de red inalámbrica.

1. Buscar el protocolo TCP/IP versión 4 (IPv4), propiedades.

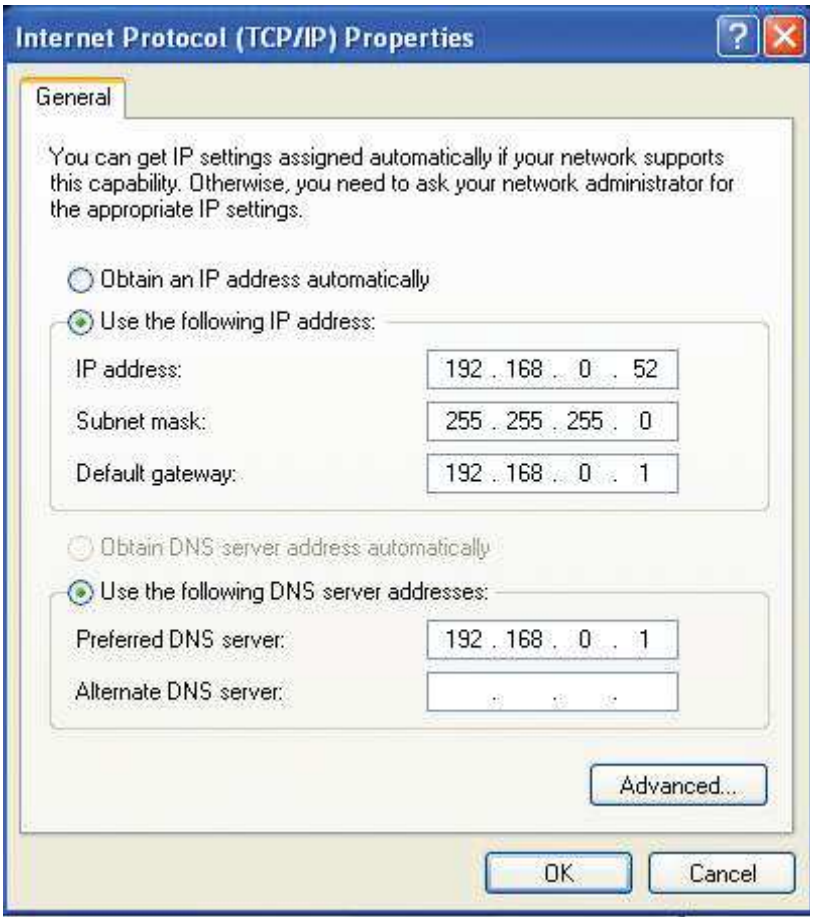

Figura 4-53: Configuración TCP/IP

Fuente: Captura de pantalla

2. Aquí es donde se asigna direcciones IP al PC, la dirección IP será 192.168.0.52, la máscara se asignará automáticamente, será la máscara 255.255.255.0, y el “Default Gateway” será 192.168.0.

- El “Primary DNS” es el mismo de la LAN IP del router.

- EL “Secondary DNS” es opcional, puede ser el servidor DNS del ISP.

3. OK para guardar la configuración.

4. Verificar la dirección de red, seguir los siguientes pasos:

5. Click en Inicio, Ejecutar, “cmd”, Enter.

6. Comando “ipconfig” y Enter

La información aparecerá a continuación.

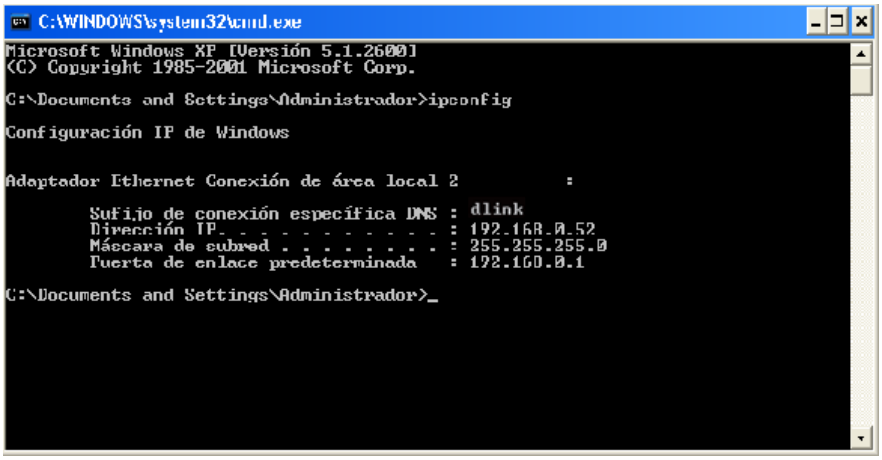

Figura 4-54: Verificación de dirección IP

Fuente: Captura de pantalla

Así se concluye la instalación y configuración, para verificar navegar en internet.

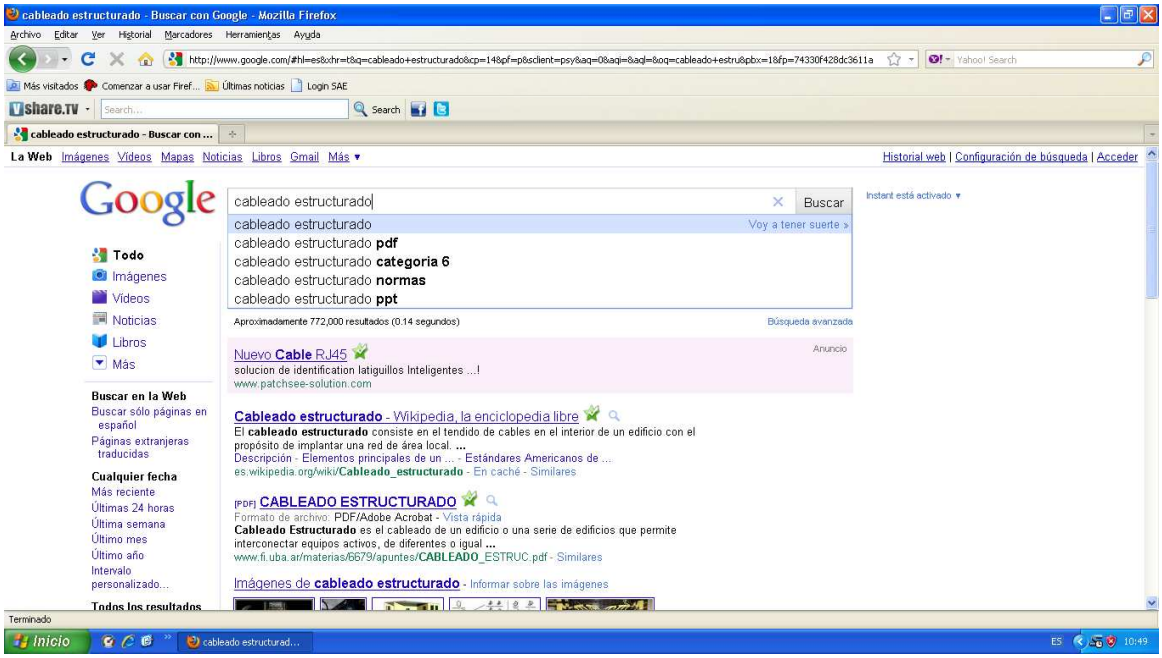

Figura 4-55: Ventana navegador hacia Internet

Fuente: Captura de pantalla

CAPITULO 5. V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Con la ejecución de este proyecto se logró organizar el sistema de comunicación interno y la optimización de tiempo y recursos de la empresa.

- La comunicación que existía entre cada departamento mejoró notablemente, además con la implementación de la red inalámbrica, se logró conectar puntos distantes optimizando de esta forma dinero y recursos físicos y así poder compartir información y dispositivos.

- El departamento de bodega que estaba aislado, tendrá una conexión inalámbrica con el Acess Router ya que éste cuenta con tecnología IEEE 802.11N.

- Todo lo invertido en la implementación de este proyecto es considerado bajo, ya que los beneficios que representan para la empresa son grandes.

- La implementación de la red inalámbrica permitirá determinar su escalabilidad y flexibilidad para futuros cambios en la red interna.

- Los dispositivos inalámbricos permiten la implementación de varias políticas de seguridad, entre ellas tenemos WEP, WPA2.

- La implementación de un sistema cableado estructurado facilita las labores de mantenimiento o reparación de los diferentes puntos de red, por cuanto todos los puntos de voz y datos se encuentran debidamente identificados.

- Con la implementación del cableado estructurado se redujo en un 90% los problemas de conectividad a los que estaba expuesta la empresa antes de la implantación del cableado estructurado.

5.2 RECOMENDACIONES

- Para extender la vida útil de los dispositivos se recomienda apagarlos mientras no estén en uso.

- Se recomienda capacitar a una persona para que se encargada de la red, y solucionar cualquier problema que se presente repentinamente, así como dar soporte a las diferentes dependencias.

- Se recomienda cambiar las claves de acceso al Access point frecuentemente, ya que por seguridad es mandatorio que se lo realice.

- Se recomienda que la clave sea WEP cifrado 128 bits Hexadecimal, esto quiere decir una combinación de números, letras y símbolos para que sea una contraseña segura.

- A las estaciones de trabajo se recomienda hacer mantenimiento preventivo cada cierto tiempo, esto para evitar algún virus en la red, y perdida de información.

- Se recomienda hacer mantenimiento correctivo para así detectar a tiempo cualquier daño en los dispositivos instalados.

- Se recomienda la implementación de redes virtuales (VLAN's), con el objetivo de optimizar el tráfico de la red.

CAPITULO 6. VI. GLOSARIO

2G: Se conoce como telefonía móvil 2G a la segunda generación de telefonía móvil.

3G: Es la abreviación de tercera-generación de transmisión de voz y datos a través de telefonía móvil.

Access Point: Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

Anycast: Es una forma de direccionamiento en la que la información es enrutada al mejor destino desde el punto de vista de la topología de la red.

APDU: Application Protocol Data Unit es la unidad de comunicación entre un lector de tarjetas inteligentes y una tarjeta inteligente.

ARP: Address Resolution Protocol (protocolo de resolución de direcciones) para la resolución de direcciones en informática, es el responsable de encontrar la dirección de hardware que corresponde a una determinada dirección IP.

Backbone: Se refiere al cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.

Bits: Acrónimo de Binary digit, (dígito binario).

Bluetooth: Es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz.

CAT 5e: Estándar de cables que puede transmitir datos a velocidades de hasta 100 Mbps a frecuencias de hasta 100 Mhz.

CAT 6: Estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retrocompatible con los estándares de categoría 5/5e y categoría 3.

CAT 7: Estándar de cable para Ethernet y otras tecnologías de interconexión que puede hacerse compatible hacia atrás con los tradicionales de ethernet actuales Cable de Categoría 5 y Cable de Categoría 6.

Cluster: Se aplica a los conjuntos o conglomerados de computadoras construidos mediante la utilización de componentes de hardware comunes y que se comportan como si fuesen una única computadora.

Code Division Multiple Access: CDMA es un término genérico para varios métodos de multiplexación o control de acceso al medio basados en la tecnología de espectro expandido.

CSMA/CD: (Acceso Múltiple por Detección de Portadora con Detección de Colisiones), es una técnica usada en redes Ethernet para mejorar sus prestaciones.

DHCP: (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

DNS: (en español, sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras.

Enrutadores: (del inglés router), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI.

Ethernet: Estándar de redes de computadoras de área local con acceso al medio.

Fast-Ethernet: Ethernet de alta velocidad es el nombre de una serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo).

FDDI: Fiber Distributed Data Interface) es un conjunto de estándares ISO y ANSI.

Fibra Óptica: Medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

Frame Relay: (Frame-mode Bearer Service) es una técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual.

FTP: (sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos) protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basada en la arquitectura cliente-servidor.

Gateways: Una pasarela o puerta de enlace (del inglés gateway) es un dispositivo, con frecuencia una computadora, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

GSM: Global System for Mobile Communications.

Host: Usado en informática para referirse a las computadoras conectados a una red, que proveen o utilizan servicios a/de ella.

ICMP: Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet.

IGMP: Se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión.

IP: (Internet Protocol), Protocolo usado para la comunicación de datos a través de una red.

IPv4: Internet Protocol version 4 (IPv4) (en español: Protocolo de Internet versión 4) es la cuarta versión del protocolo Internet Protocol (IP).

IPv6: Internet Protocol version 6 (IPv6) (en español: Protocolo de Internet versión 6)
ISO: Organización Internacional de Normalización.

ISO9000: Especifica la manera en que una organización opera, sus estándares de calidad.

LAN: Red de área local, red local o LAN (del inglés local area network) es la interconexión de varias computadoras y periféricos.

LMDS: Sistema de Distribución Local Multipunto o LMDS (del inglés Local Multipoint Distribution Service) es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda.

Local Talk: Es una implementación particular de la capa física del sistema de redes AppleTalk de los ordenadores de la empresa Apple Inc.. LocalTalk se basa en un sistema de cable de par trenzado y un transceptor funcionando todo ello a una velocidad de 230'4 kbit/s.

Luz Infrarroja: Se trata de emisores/receptores de las ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita "ver" al otro para realizar la comunicación.

MAC: media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red.

MAN: Red de área metropolitana (Metropolitan Area Network o MAN, en inglés) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado

Multicast: Envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen.

Patch Panel: Paneles electrónicos utilizados en algún punto de una red informática o sistema de comunicaciones analógico o digital en donde todos los cables de red terminan.

QoS: (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput).

Rack: Es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones.

RARP: Siglas en inglés de Reverse Address Resolution Protocol (Protocolo de resolución de direcciones inverso). Es un protocolo utilizado para resolver la dirección IP de una dirección hardware dada (como una dirección Ethernet).

RJ-45: (registered jack 45) es una interfaz física comúnmente usada para conectar redes de cableado estructurado.

Router Inalámbrico: Dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red) del modelo OSI inalámbricamente.

RS-232: (Recommended Standard 232, también conocido como Electronic Industries Alliance RS-232C) es una interfaz que designa una norma para el intercambio serie de datos binarios entre un DTE (Equipo terminal de datos) y un DCE (Data Communication Equipment, Equipo de Comunicación de datos).

SCE: Sistema de cableado estructurado, Es el sistema colectivo de cables, canalizaciones, conectores, etiquetas, espacios y demás dispositivos que deben ser instalados para establecer una infraestructura de telecomunicaciones genérica en un edificio o campus.

SMTP: Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación.

STP: (Spanning Tree Protocol) (SmmTPr) es un protocolo de red de nivel 2 de la capa OSI.

Switch: Dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI.

TCP: Transmission Control Protocol (en español Protocolo de Control de Transmisión), es uno de los protocolos fundamentales en Internet.

Telnet: (TELecommunication NETwork) es el nombre de un protocolo de red que sirve para acceder mediante una red a otra máquina para manejarla remotamente como se estuviera sentado delante de ella.

UDP: User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Paquete de datos).

Unicast: Envío de información desde un único emisor a un único receptor.

USB: Universal Serial Bus, es un puerto que sirve para conectar periféricos a un ordenador.

UTP: Cable de par trenzado es un medio de conexión usado en telecomunicaciones en el que dos conductores eléctricos aislados son entrelazados para anular las interferencias de fuentes externas y diafonía de los cables adyacentes.

VoD: Televisión a la carta o vídeo bajo demanda, del inglés video on demand (VoD) es un sistema de televisión que permite al usuario el acceso a contenidos multimedia de forma personalizada ofreciéndole, de este modo, la posibilidad de solicitar y visualizar una película o programa concreto en el momento exacto que el telespectador lo desee.

VoIP: (Voice over IP), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet).

VPN: (Virtual Private Network), una tecnología de red que permite extender la red local sobre una red pública relativamente hablando.

WAN: Red de área amplia, con frecuencia denominada WAN, acrónimo de la expresión en idioma inglés wide area network, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente.

WEP: (Wired Equivalent Privacy acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el

estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

Wi-Fi: Organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11 relacionados a redes inalámbricas de área local.

Wireless: La comunicación inalámbrica o sin cables es aquella en la que extremos de la comunicación (emisor/receptor) no se encuentran unidos por un medio de propagación físico, sino que se utiliza la modulación de ondas electromagnéticas a través del espacio.

WLAN: (Wireless Local Area Network), es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de estas.

WMAN: Estándar de comunicación inalámbrica basado en la norma IEEE 802.16.

WPAN: Wireless Personal Area Networks, Red Inalámbrica de Área Personal o Red de área personal o Personal area network es una red de computadoras para la comunicación entre distintos dispositivos (tanto computadoras, puntos de acceso a internet, teléfonos celulares, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso.

WWAN: Wireless Wide Area Network.

6.1 BIBLIOGRAFIA

Internet

- http://es.wikitel.info/wiki/Redes_de_comunicaciones
- http://www.forest.ula.ve/~mana/cursos/redes/clasifica.html
- http://tutorial.galeon.com/inalambrico.htm
- http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml

- http://fmc.axarnet.es/redes/tema_06_m.htm
- http://www.angelfire.com/mi2/Redes/protocolo.html
- http://es.wikipedia.org/wiki/Modelo_OSI
- http://es.wikipedia.org/wiki/PDU
- http://es.kioskea.net/contents/internet/tcpip.php3
- http://www.thehouseofblogs.com/articulo/comparacion_modelo_osi_y_tcpip-4501.html
- http://www.eveliux.com/mx/estandares-de-telecomunicaciones.php
- http://members.tripod.com/a_pizano/html/cap4.html#Top
- http://html.rincondelvago.com/transmision-de-datos_ipv4-e-ipv6_dns.html
- http://es.wikipedia.org/wiki/Cableado_estructurado
- http://www.elprisma.com/apuntes/ingenieria_de_sistemas/cableadoestructurado/
- http://www.monografias.com/trabajos11/cabes/cabes.shtml
- http://parla.com.mx/cableadoestructurado.htm
- http://portal.cableando.com/index.php/categorias-de-cableados-de-redes-estructuradas
- http://es.kioskea.net/contents/wireless/wlintro.php3
- http://www.unincca.edu.co/boletin/indice.htm
- http://technet.microsoft.com/es-es/library/cc784756(WS.10).aspx
- http://dns.bdat.net/seguridad_en_redes_inalambricas/c14.html
- http://dns.bdat.net/seguridad_en_redes_inalambricas/x59.html
- http://dns.bdat.net/seguridad_en_redes_inalambricas/x75.html
- http://dns.bdat.net/seguridad_en_redes_inalambricas/x80.html

Tesis

- Arturo Garces, Juan Pablo Zaldumbide - “Analisis y Diseño de Redes Moviles Ad-Hoc”
  http://bibdigital.epn.edu.ec/bitstream/15000/2402/1/CD-0940.pdf

Otros

- Manual D-link
- Manual de usuario D-link