

UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE TECNOLOGIA

CARRERA ELECTRONICA Y TELECOMUNICACIONES



NIVEL TECNICO UNIVERSITARIO SUPERIOR

INFORME DE PASANTIA REALIZADO EN LA EMPRESA VERALDA S.R.L.

**INSTALACION Y MANTENIMIENTO DE REDES DE INTERNET PARA EDIFICIOS, OFICINAS Y
VIVIENDAS PARTICULARES**

POSTULANTE: HEMBER ADHEMAR OROZCO BLANCO

TUTOR: LIC. JAVIER YUJRA

La Paz – Bolivia

2016

Informe de pasantía

Instalación y mantenimiento de redes de internet para edificios, oficinas y viviendas particulares.

Empresa VERALDA

Este informe detalla la experiencia adquirida y el trabajo realizado durante el periodo de pasantía realizado en una empresa que va creciendo día a día en el ámbito de la construcción y asesoramiento técnico electrónico.

Hember Adhemar Orozco Blanco

Diciembre 2016

Agradecimientos

Si tendría que agradecer este logro a todas las personas que contribuyeron en mi desarrollo personal y profesional seguro no alcanzaría esta página para mencionarlos, pero quiero nombrar a los que todavía siguen dándome su apoyo incondicional.

Agradecer primero a mi creador Dios Padre por estar conmigo siempre.

Quisiera también mencionar a mi madre “mami Martha” la persona que dio y que aun todavía da todo su amor a sus hijos y nietos preocupándose todos los días por ellos. A mi esposa Esther que confió en mí, gracias por tu amor, comprensión, paciencia y el impulso que me das para seguir adelante y no mirar atrás “te amo flaca”. Y los tres retoños que Dios me dio Israel, Flor y Cielito los cuales son mi inspiración y motivo de superación.

Por último agradecer este logro también a mis hermanos David, Abel, Marleny, Kroscaya y Maribel los cuales están siempre predispuestos a brindarme cualquier tipo de ayuda incondicional y a aquellos amigos verdaderos que no solo están contigo en las buenas sino también en las malas que no los nombro por temor de olvidarme de alguno *gracias a esos más que amigos hermanos.*

INDICE

CAPITULO I	4
DESCRIPCION DE LA INSTITUCION	4
1.1.- ACTIVIDAD DE LA EMPRESA.....	4
1.2.- MISION.....	4
1.3.- VISION.....	4
1.4.- ORGANIGRAMA GENERAL DE LA EMPRESA.....	5
1.5.- ORGANIGRAMA DEL DEPARTAMENTO TECNICO ELECTRONICO	5
1.6.- PROYECTOS DESARROLLADOS	6
1.7.- CARGOS DESEMPEÑADOS	7
CAPITULO II	8
MARCO TEORICO	8
2.1.- REDES DE INTERNET	8
2.2.- CONCEPTO DE UNA RED INFORMATICA	9
2.2.1.- FINALIDAD DE UNA RED INFORMATICA.....	9
2.3.- CONCEPTOS FUNDAMENTALES.....	9
2.3.1.- QUE ES LA IEEE Y SU ESTANDARIZACION	10
2.3.1.1.- LA IEEE 802	10
2.3.1.2.- LA IEEE 802.11.....	11
2.3.2.- QUE ES EL MAC	12
2.3.3.- DIRECCION IP	13
2.3.3.1.- CLASES DE DIRECCIONES IP	14
2.3.4.- MASCARA DE SUB-RED	15
2.3.5.- PUERTA DE ENLACE	15
2.3.6.- SERVIDOR DNS.....	16
2.3.7.- QUE ES LA WWW	17
2.3.8.- QUE ES LA WEB	17
2.3.8.1.- QUE ES LA WEB 2.0.....	18
2.3.9.- LA HTTP	18
2.4.- DISPOSITIVOS DE RED.....	19
2.4.1.- ESTACION DE TRABAJO.....	19
2.4.2.- SERVIDOR	19
2.4.2.1.- SERVIDOR PROXY	20
2.4.2.2.- SERVIDOR DNS	21
2.4.2.3.- SERVIDOR WEB.....	21
2.4.3.- TARJETA DE RED.....	21

2.4.4.- HUB	21
2.4.5.- SWITCH.....	22
2.4.6.- ROUTER	22
2.4.7.- CABLE COAXIAL	24
2.4.8.- PAR TRENZADO	24
2.4.9.- FIBRA OPTICA.....	26
2.5.- CLASIFICACION DE LAS REDES.....	27
2.5.1.- CLASIFICACION DE LAS REDES SEGÚN SU ALCANCE	27
2.5.1.1.- REDES LAN	28
2.5.2.- CLASIFICACION DE LAS REDES POR SU TIPO DE CONEXIÓN	29
2.5.2.1.- MEDIOS GUIADOS	29
2.5.2.2.- MEDIOS NO GUIADOS.....	29
2.5.3.- CLASIFICACION DE LAS REDES POR SU RELACION FUNCIONAL	30
2.5.4.- CLASIFICACION DE LAS REDES POR SU TOPOLOGIA FISICA	30
2.5.5.- CLASIFICACION DE LAS REDES POR LA DIRECCIONALIDAD DE DATOS	31
2.5.6.- CLASIFICACION DE LAS REDES POR SU AUTENTIFICACION.....	31
2.5.7.- CLASIFICACION DE LAS REDES SEGÚN SU GRADO DE DIFUSION	31
2.5.7.1.- REDES INTRANET	31
2.5.7.2.- REDES INTERNET	32
2.5.8.- CLASIFICACION DE LAS REDES POR SU SERVICIO O FUNCION	32
2.6.- PROTOCOLO DE COMUNICACIONES.....	33
2.7.- MODELO OSI Y SUS CARACTERISTICAS	33
2.7.1.- INTRODUCCION A LA CAPA FISICA.....	34
2.7.2.- LA CAPA DE ENLACE DE DATOS	34
2.7.3.- LA CAPA DE RED	35
2.7.3.1.- DIRECCIONAMIENTO	36
2.7.3.2.- ENCAPSULAMIENTO	36
2.7.3.3.- ENRUTAMIENTO.....	37
2.7.3.4.- DESENCAPSULAMIENTO	37
2.7.4.- LA CAPA DE TRANSPORTE	37
2.7.5.- LA CAPA DE SESION	39
2.7.6.- LA CAPA DE PRESENTACION.....	39
2.7.7.- LA CAPA DE APLICACIÓN.....	40
2.7.8.- VENTAJAS DEL MODELO OSI	41
2.7.9.- DESVENTAJAS DEL MODELO OSI	41
2.8.- MODELO TCP / IP	42
2.8.1.- COMO FUNCIONA EL TCP/IP	43
2.8.2.- ENCAPSULACION DE DATOS Y LAS CAPAS DEL MODELO TCP/IP	43
2.8.2.1.- CAPA DE INTERFAZ DE RED	44
2.8.2.2.- LA CAPA DE INTERNET	45

2.8.2.3.- CAPA DE TRANSPORTE.....	46
2.8.2.4.- LA CAPA DE APLICACIÓN.....	46
2.8.3.- VENTAJAS Y DESVENTAJAS DEL MODELO TCP/IP	47
CAPITULO III	49
ACTIVIDADES DESARROLLADAS	49
3.1 MOTIVO DE LA PASANTIA.....	49
3.2.- OBJETIVO DE LA PASANTIA.....	49
3.3.- ASPECTOS LABORALES.....	49
3.4.- SIMBOLOGIA.....	50
3.5.- PLANOS DE DIRECCIONAMIENTO Y DE DISTRIBUCION	51
3.6.- CABLEADO ESTRUCTURADO	54
3.7.- ARMADO DE LAS ROSETAS	55
3.8.- CRIMPADO DE LOS CABLES.....	56
3.9.- INSTALACION DE LOS ENLACES USUARIO INTERNET	57
3.10.- CONFIGURACION	58
3.11.- MUESTRA DE TRABAJOS REALIZADOS	63
CAPITULO IV	69
CONCLUSIONES.....	69
4.1.- CONCLUSIONES.....	69
4.2.- RECOMENDACIONES	69
4.3.- PROPUESTA	70
BIBLIOGRAFIA.....	72

DESCRIPCION DE LA INSTITUCION

1.1.- ACTIVIDAD DE LA EMPRESA

La Empresa VERALDA creada en el año 2000 comenzó como una empresa dedicada netamente a la construcción, con el paso de los años a sugerencia de sus propios clientes, después de haber demostrado responsabilidad y puntualidad en todos sus trabajos, la Gerencia General de la Empresa decide implementar servicios de electricidad, telefonía, redes, alarmas y CATV para brindar un mejor servicio a su clientela. Tal fue la aceptación de la gente que la empresa empezó a crecer y ahora es una de las líderes en su rubro.

VERALDA en la actualidad es una institución que se encarga de entregar a sus clientes casas, edificios, parques, remodelaciones y otros tipos de construcciones con una calidad de terminado impecable, brindando también comodidad y facilidad en el área comunicacional haciendo que el cliente final disfrute de todas las comodidades y seguridad con las que contamos en la actualidad.

En el área técnica la Empresa VERALDA se encarga de realizar todo el cableado estructural y las conexiones respectivas en cada punto donde el cliente lo solicite, en la actualidad no solamente se da el servicio a construcciones nuevas sino que también se brinda asesoramiento a empresas que tienen un servicio defectuoso en sus conexiones y comunicaciones orientándolos para realizar una actualización en sus sistemas electrónicos.

1.2.- MISION

La misión de la Empresa es brindar a sus clientes una mejor calidad de vida y la mayor comodidad posible en cuanto a construcciones e infraestructura se refiere y demostrando confianza, seguridad y profesionalismo en los departamentos técnicos en todos sus trabajos.

1.3.- VISION

Convertirse en una empresa pionera en el rubro de la construcción, las telecomunicaciones y la seguridad no solamente en nuestra ciudad sino también brindando un servicio a nivel nacional.

1.4.- ORGANIGRAMA GENERAL DE LA EMPRESA

La estructura organizacional que forma la empresa fue modificada a medida que esta fue creciendo y todavía se pretende realizar algunos cambios con el paso de los años ya que la empresa promete a su clientela ampliar sus servicios en otras áreas.

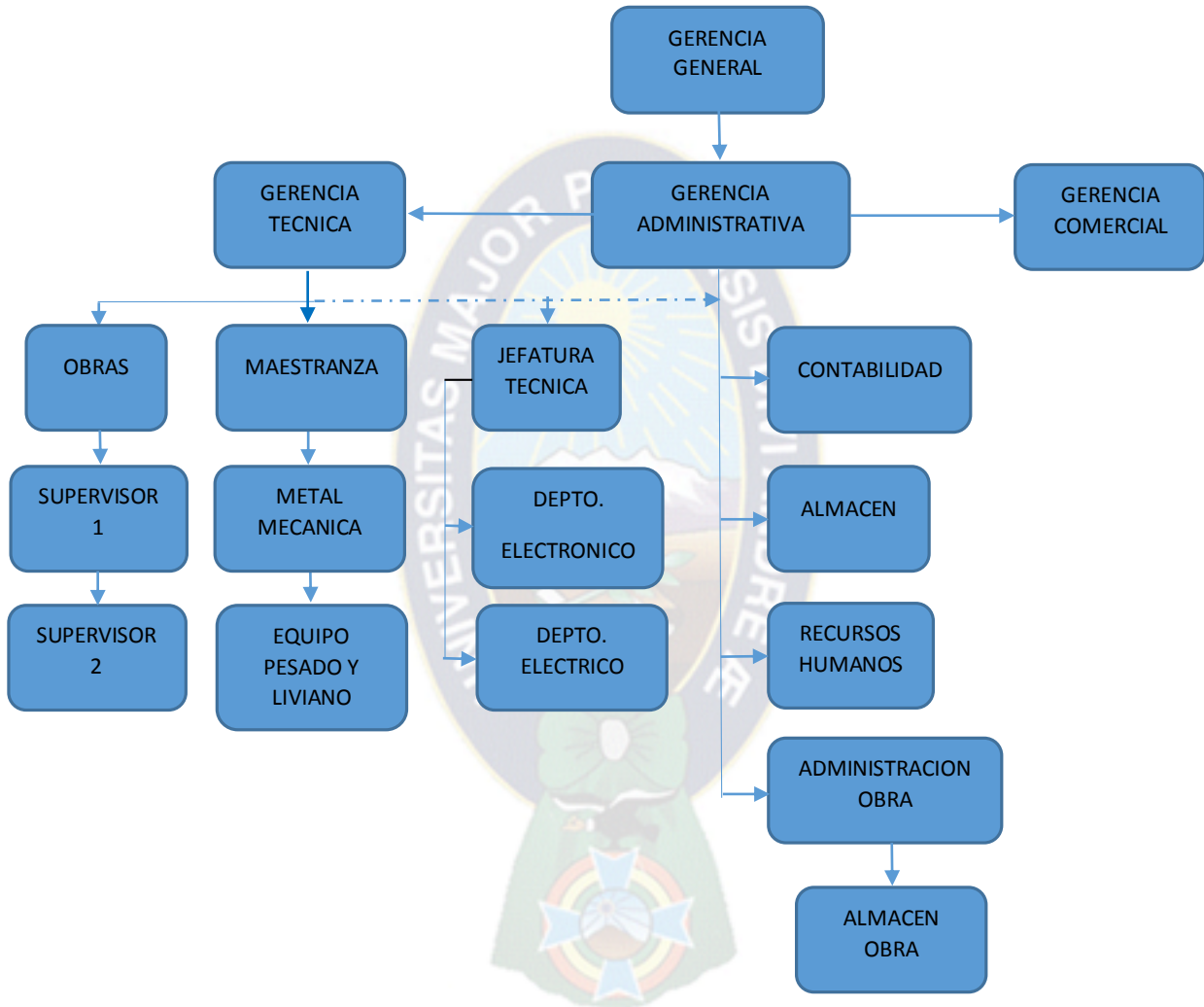


Figura 1.1 Organigrama de la Empresa

1.5.- ORGANIGRAMA DEL DEPARTAMENTO TECNICO ELECTRONICO

El departamento electrónico es uno de los sectores que más contribuye en cuanto a tecnología ya que cuenta con distintas áreas pero que lo realiza el mismo personal como por ejemplo el área de telefonía y redes también contribuye al trabajo que realiza el área

de sistemas de seguridad apoyando en el trabajo cuando les falta personal en esta área y viceversa. Tiene como objetivo mostrar al cliente calidad en cuanto al servicio prestado y estética en cuanto a infraestructura. Tiene sus dependencias independientes y cuenta con todas herramientas necesarias para realizar los trabajos con eficiencia.

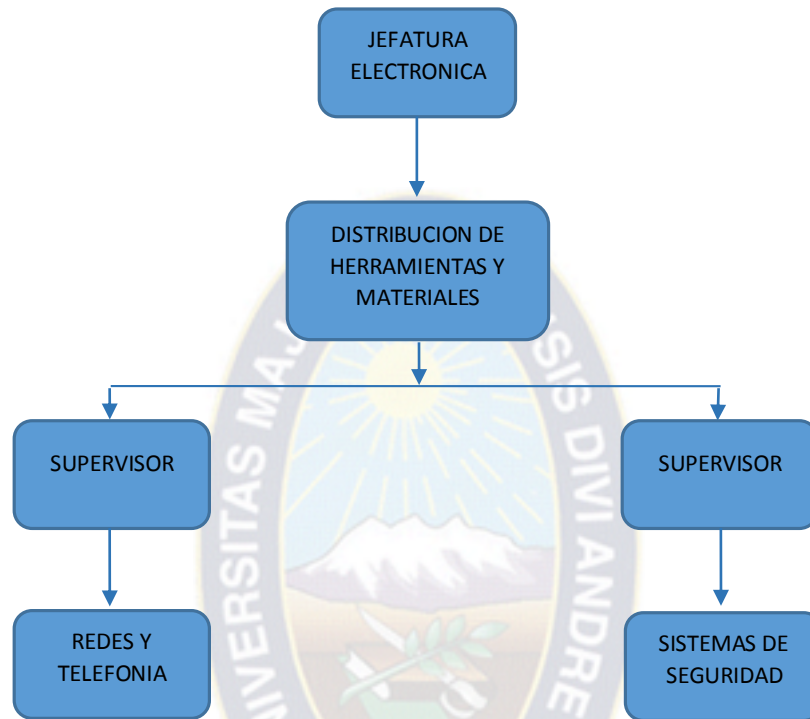


Figura 1.2 Organigrama del departamento técnico

1.6.- PROYECTOS DESARROLLADOS

La Empresa Verda como institución desarrollo muchos proyectos entre los cuales en este periodo de la pasantía se colaboró en:

- la instalación de servicio de Internet al edificio Casanovas
- Instalación de red de Internet y telefonía de voz sobre IP a la fabrica la Estrella
- Instalación de redes de Internet en el Ministerio de Obras Publicas
- Instalación de una Central telefónica en el Ministerio de Desarrollo productivo
- Instalación de red de internet para telefonía de voz sobre IP en el Ministerio de Justicia.

También se realizaron muchos otros trabajos en distintos domicilios particulares en nuestra ciudad y el Alto.

1.7.- CARGOS DESEMPEÑADOS

El puesto de trabajo donde se desarrolló las actividades fue en el departamento de redes y telefonía, ahí se ocupó el cargo de técnico encargado de las instalaciones y cableado estructurado dentro del cual se verifica el correcto funcionamiento de los swiches, routers, estaciones de trabajo, etc. Se colaboró y aprendió mucho en especial en lo que refiere a redes de internet. En los distintos tipos de instalaciones se realiza el cableado estructurado cuidando siempre la estética y asegurándonos de una funcionalidad al 100%. El hecho de trabajar en esta área no significo estar dedicado simplemente en estas dos ramas sino que también se colaboró, cuando nos solicitaron, en la instalación de alarmas, cámaras de seguridad y telefonía de vos sobre IP.



MARCO TEORICO

2.1.- REDES DE INTERNET

Internet ha revolucionado la informática y las comunicaciones como ninguna otra cosa. La invención del telégrafo, el teléfono, la radio y el ordenador sentó las bases para esta integración de funcionalidades sin precedentes. Internet es a la vez una herramienta de emisión mundial, un mecanismo para diseminar información y un medio para la colaboración y la interacción entre personas y sus ordenadores, sin tener en cuenta su ubicación geográfica. Internet representa uno de los ejemplos más exitosos de los beneficios de una inversión y un compromiso continuos en el campo de la investigación y el desarrollo de la infraestructura de la información. Desde las primeras investigaciones en conmutación de paquetes, el Gobierno, la Industria y la Academia se han asociado como artífices de la evolución e implementación de esta apasionante nueva tecnología.

Internet no nació en su forma actual, con un alcance mundial de miles de redes y conexiones. Tuvo un comienzo humilde, pero excitante, como una red denominada ARPANET, la madre de Internet. Arpanet se inició como un experimento del gobierno de los EEUU en un sistema de conmutación por lotes desde 1969. Arpa, cuyas siglas en inglés significan Agencia de Proyectos Avanzados de Investigación del Departamento de Defensa de los EEUU, inicialmente conectaba a los investigadores con centros de cómputo lejanos, permitiéndoles compartir recursos, tanto de los equipos como de los programas; por ejemplo espacio de disco duro, bases de datos y computadoras. En este sentido M. Algora (Comunicación 7/10/1994) sitúa el origen de Internet en la época de la Guerra Fría, con la finalidad de que el Departamento de Estado americano pudiera prever posibles ataques. Más tarde otras redes experimentales que utilizaban paquetes de radio y satélite se conectaron con Arpanet utilizando tecnología interconectada, patrocinada por DARPA (Agencia de Proyectos Avanzados de Investigación en Defensa). A principios de la década de los 80 se dividió Arpanet en dos redes: Arpanet y Milnet (una red militar con información no clasificada) pero las conexiones que se hicieron entre las redes permitieron que continuara la comunicación. Al principio esta interconexión de redes experimentales y de producción se denominó Internet Darpa y posteriormente el nombre se redujo a "Internet"⁽¹⁾.

Varios proyectos que buscaban finalmente un nuevo método de comunicación informatizada y seguro, que resistiese a un ataque nuclear entre otras cosas, fueron desarrollándose en paralelo hasta que finalmente todos fueron reunidos en ARPANET, donde coincidieron en sus esfuerzos. Por fin, en 1968 el proyecto estaba claro y en ejecución. Fue un año después **ARPANET** enviaba su primer mensaje dentro de su nodo de California de modo que el 21 de noviembre de 1969 ARPANET contactaba por primera vez

con un ordenador a cientos de kilómetros de prueba. Y menos de un mes después, el 21 de noviembre de 1969, realizaba su primer contacto a cientos de kilómetros de distancia.

Hoy día Internet está presente en más del 60% del mundo. Prácticamente todos los países europeos, Estados Unidos, Asia, Latinoamérica y más de la mitad del continente Africano tienen fácil acceso a Internet. Algo que supera los mejores deseos de 1969 ¿Y qué ha cambiado desde entonces? Prácticamente todo. No solo el acceso a internet ya no es solo propio de la agencia de seguridad de turno, (y de uso eminentemente público), sino que su formato, su tecnología y hasta su concepto son radicalmente distintos de cómo comenzó todo.

2.2.- CONCEPTO DE UNA RED INFORMATICA

Es el conjunto de computadoras terminales y dispositivos que se comunican entre sí, proporcionando el entorno necesario para que los usuarios, desde diferentes ubicaciones (local o remota), tengan acceso en situaciones similares a la información.

Este tipo de redes implica la interconexión de los equipos a través de ciertos dispositivos que permiten el envío y la recepción de ondas. Estas ondas llevan los datos que son compartidos. En las redes informáticas, por lo tanto, hay emisores y receptores que intercambian mensajes.

De acuerdo al tipo de conexión, a la relación entre los elementos y al alcance, es posible calificar a una red informática de diferentes formas. Internet, de hecho, es una red informática: millones de computadoras están interconectadas a través de servidores y pueden compartir todo tipo de datos.

2.2.1.- FINALIDAD DE UNA RED INFORMATICA

- Compartir archivos y programas.
- Compartir recursos de red.
- Compartir bases de datos.
- Mejorar la comunicación de los usuarios.
- Software de grupos y de flujos de trabajo.
- Gestión centralizada.
- Mejorar la estructura corporativa.

2.3.- CONCEPTOS FUNDAMENTALES

Para toda instalación de una red se debe conocer algunos conceptos y términos que son necesarios aclararlos para poder comprender mejor como trabajan las redes en internet. Estos términos como por ejemplo Dirección IP, máscara de sub red, puerta de enlace. Servidor DNS, la WWW y otros se los utiliza diariamente en la configuración de redes y el

uso de internet aunque muchas veces utilizamos dichos servicios sin darnos cuenta de la importancia que tienen estos.

2.3.1.- QUE ES LA IEEE Y SU ESTANDARIZACION

IEEE corresponde a las siglas de Institute of Electrical and Electronics Engineers que traducido al español sería Instituto de Ingenieros Eléctricos y Electrónicos es una asociación mundial de ingenieros dedicada a la estandarización y el desarrollo en áreas técnicas. Con cerca de 425 000 miembros y voluntarios en 160 países, es la mayor asociación internacional sin ánimo de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en computación, matemáticos aplicados, ingenieros en biomedicina, ingenieros en telecomunicación, ingenieros en mecatrónica, etc.

Según el mismo IEEE, su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales.

Mediante sus actividades de publicación técnica, conferencias y estándares basados en consenso, el IEEE produce más del 30% de la literatura publicada en el mundo sobre ingeniería eléctrica de potencia, electrónica, en computación, telecomunicaciones, telemática, mecatrónica y tecnología de control y robótica, biomédica y biónica, procesamiento digital de señales, sistemas energéticos, entre otras ramas derivadas y correspondientes a la Ingeniería Eléctrica; organiza más de 1000 conferencias al año en todo el mundo, y posee cerca de 900 estándares activos, con otros 700 más bajo desarrollo.

2.3.1.1.- LA IEEE 802

IEEE 802 fue un proyecto creado en febrero de 1980 paralelamente al diseño del Modelo OSI. Se desarrolló con el fin de crear estándares para que diferentes tipos de tecnologías pudieran integrarse y trabajar juntas. El proyecto 802 define aspectos relacionados con el cableado físico y la transmisión de datos.

La IEEE 802 actúa sobre Redes de computadoras, concretamente y según su propia definición sobre redes de área local (RAL, en inglés LAN) y redes de área metropolitana (MAN en inglés). También se usa el nombre IEEE 802 para referirse a los estándares que proponen, algunos de los cuales son muy conocidos: Ethernet (IEEE 802.3), o Wi-Fi (IEEE 802.11). Está, incluso, intentando estandarizar Bluetooth en el 802.15 (IEEE 802.15).

Se centra en definir los niveles más bajos (según el modelo de referencia OSI o sobre cualquier otro modelo). Concretamente subdivide el segundo nivel, el de enlace, en dos subniveles: el de Enlace Lógico (LLC), recogido en 802.2, y el de Control de Acceso al Medio

(MAC), subcapa de la capa de Enlace Lógico. El resto de los estándares actúan tanto en el Nivel Físico, como en el subnivel de Control de Acceso al Medio.

NOMBRE	DESCRIPCION
IEEE 802.1	Normalización de interfaz
802.1d	<i>Spanning Tree Protocol</i>
802.1p	Asignación de Prioridades de tráfico
802.1q	<i>Virtual Local Area Networks (VLAN)</i>
802.1x	Autenticación en redes LAN
802.1aq	<i>Shortest Path Bridging (SPB)</i>
IEEE 802.2	Control de enlace lógico LLC
IEEE 802.3	CSMA / CD (ETHERNET)
IEEE 802.3a	Ethernet delgada 10Base2
IEEE 802.3c	Especificaciones de Repetidor en Ethernet a 10 Mbps
IEEE 802.3i	Ethernet de par trenzado 10BaseT
IEEE 802.3j	Ethernet de fibra óptica 10BaseF
IEEE 802.3u	Fast Ethernet 100BaseT
IEEE 802.3z	Gigabit Ethernet parámetros para 1000 Mbps
IEEE 802.3ab	Gigabit Ethernet sobre 4 pares de cable UTP Cat5e o superior
IEEE 802.3ae	10 Gigabit Ethernet
IEEE 802.4	Token bus LAN
IEEE 802.5	Token ring LAN (topología en anillo)
IEEE 802.6	Redes de Área Metropolitana (MAN) (ciudad) (fibra óptica)
IEEE 802.7	Grupo Asesor en Banda ancha
IEEE 802.8	Grupo Asesor en Fibras Ópticas
IEEE 802.9	Servicios Integrados de red de Área Local (redes con voz y datos integrados)
IEEE 802.10	Seguridad de red
IEEE 802.11	Redes inalámbricas WLAN. (Wi-Fi)
IEEE 802.12	Acceso de Prioridad por demanda 100 Base VG-Any Lan
IEEE 802.13	Se ha evitado su uso por superstición ¹
IEEE 802.14	Módems de cable
IEEE 802.15	WPAN (Bluetooth)
IEEE 802.16	Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX)

Tabla 2.1 Grupos de trabajo de la IEEE 802

2.3.1.2.- LA IEEE 802.11

La especificación IEEE 802.11 es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). **Wi-Fi** (que significa "Fidelidad inalámbrica", a

veces incorrectamente abreviado WiFi) es el nombre de la certificación otorgada por la Wi-Fi Alliance, anteriormente WECA (Wireless Ethernet Compatibility Alliance), grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11. A los dispositivos certificados por la Wi-Fi Alliance se les permite usar este logotipo:



Figura 2.1 Logotipo de la Wire Inhambric Fidelity

Con Wi-Fi se pueden crear redes de área local inalámbricas de alta velocidad siempre y cuando el equipo que se vaya a conectar no esté muy alejado del punto de acceso. En la práctica, Wi-Fi admite ordenadores portátiles, equipos de escritorio, asistentes digitales personales (PDA) o cualquier otro tipo de dispositivo de alta velocidad con propiedades de conexión también de alta velocidad (11 Mbps o superior) dentro de un radio de varias docenas de metros en ambientes cerrados (de 20 a 50 metros en general) o dentro de un radio de cientos de metros al aire libre.

Los proveedores de Wi-Fi están comenzando a cubrir áreas con una gran concentración de usuarios (como estaciones de trenes, aeropuertos y hoteles) con redes inalámbricas. Estas áreas se denominan "zonas locales de cobertura".

2.3.2.- QUE ES EL MAC

Las tarjetas de red tipo Ethernet tienen una pequeña memoria en la que alojan un dato único para cada tarjeta de este tipo. Se trata de la dirección MAC, y está formada por 48 bits que se suelen representar mediante dígitos hexadecimales que se agrupan en seis parejas (cada pareja se separa de otra mediante dos puntos ":" o mediante guiones "-"). Por ejemplo, una dirección MAC podría ser F0:E1:D2:C3:B4:A5.

MAC son las siglas de Media Access Control y se refiere al control de acceso al medio físico. O sea que la dirección MAC es una dirección física (también llamada dirección hardware), porque identifica físicamente a un elemento del hardware, cada tarjeta Ethernet viene de fábrica con un número MAC distinto. Windows la menciona como Dirección del adaptador. Esto es lo que finalmente permite las transmisiones de datos entre ordenadores de la red, puesto que cada ordenador es reconocido mediante esa dirección MAC, de forma inequívoca.

La mitad de los bits de la dirección MAC son usados para identificar al fabricante de la tarjeta, y los otros 24 bits son utilizados para diferenciar cada una de las tarjetas producidas por ese fabricante.

Casi todas las redes de hoy día (y concretamente Internet) utilizan el protocolo IP, que usa otro sistema de direcciones no relacionadas con el hardware. Las direcciones IP responden a un sistema de convencionalismos más abstractos. Cuando un software quiere enviar datos a otro ordenador, normalmente sabe la dirección IP del ordenador destinatario, pero no sabe realmente cómo hacerle llegar los datos (físicamente). Hay otro protocolo llamado ARP (Protocolo de Resolución de Direcciones) que es el encargado de averiguar la dirección MAC correspondiente a una dirección IP, y así se pueden enviar físicamente los datos desde un ordenador a otro. No hay relación alguna entre la dirección IP y la dirección MAC, pero el protocolo ARP y la red cuentan con mecanismos para averiguar en cualquier momento cuál es esa correspondencia.

¿Qué pasa si no tenemos tarjeta de red y conectamos por módem? Pues en ese caso no se usa la dirección MAC ni tampoco funciona el protocolo ARP. La conexión por módem funciona mediante otro protocolo llamado PPP (Point to Point Protocol, protocolo de punto a punto), que actúa como enlace directo entre los dos ordenadores conectados por medio de la línea telefónica. A todos los efectos (visto desde el resto de Internet), nuestro ordenador tiene la misma dirección MAC que el servidor con el que enlazamos mediante módem. Pero hay que tener en cuenta que si tenemos instalada una tarjeta de red, la dirección MAC de esa tarjeta puede resultar visible desde Internet, incluso aunque conectemos por módem y sin usar la tarjeta de red.

¿Cómo puedo saber cuál es mi dirección MAC?:

- En Windows, tenemos que dirigirnos a Inicio-> Ejecutar, y escribir un comando y luego pulsar en Aceptar. Entonces aparecerá nuestra dirección MAC en el apartado Dirección de adaptador. El comando en cuestión es:
 - winipcfg, si nuestro Sistema Operativo es Windows 95/98/Me.
 - ipconfig, si es Windows NT/2.000.
 - Ipconfig -all en Windows xp.
 - Ipconfig /all en win 7 y win 8.
- Para Macintosh, (Mac OS 8.5 y 9) sería .Menú Apple-> Paneles de Control-> TCP/IP. Aquí ya nos aparece la dirección IP, pero para ver la dirección MAC tenemos que ir a Archivo, elegir Obtener Información, y aparecerá en el apartado Dirección del Hardware.

2.3.3.- DIRECCION IP

La dirección IP es una serie de números que identifica un dispositivo en una red local ya sea la computadora, la impresora, etc., o una red de redes que sería el internet. Si tendríamos que hacer comparaciones los números IP son como los números de teléfono para las personas ya sea celular o fijo en ninguna parte del mundo dos personas tienen el mismo

número, de la misma forma ningún dispositivo en el mundo puede tener el mismo número y es necesario conocer ese número para tener acceso a ese dispositivo. Dicho esto toda computadora conectada a internet (o a cualquier red) posee una identificación única, llamada *dirección IP* (en inglés, Internet Protocol), compuesta por cuatro combinaciones de números (p.ej. 187.25.14.190). Cada combinación va desde 0 hasta 255 así que nunca encontraremos un número superior a este.

Estos números, llamados octetos, pueden formar más de cuatro billones de direcciones diferentes. Cada uno de los cuatro octetos tiene una finalidad específica. Los dos primeros grupos se refieren generalmente al país y tipo de red (clases). Este número es un identificador único en el mundo: en conjunto con la hora y la fecha, puede ser utilizado, por ejemplo, por las autoridades, para saber el lugar de origen de una conexión.

Para que entendamos mejor el IP debemos conocer primero el TCP. Un protocolo de red es como un idioma, si dos personas están conversando en idiomas diferentes ninguna entenderá lo que la otra quiere decir. Con las computadoras ocurre una cosa similar, dos computadoras que están conectadas físicamente por una red deben "hablar" el mismo idioma para que una entienda los requisitos de la otra. El protocolo TCP estandariza el cambio de información entre las computadoras y hace posible la comunicación entre ellas. Es el protocolo más conocido actualmente pues es el protocolo estándar de Internet

El protocolo TCP contiene las bases para la comunicación de computadoras dentro de una red, pero así como nosotros cuando queremos hablar con una persona tenemos que encontrarla e identificarla, las computadoras de una red también tienen que ser localizadas e identificadas. En este punto entra la dirección IP. La dirección IP identifica a una computadora en una determinada red. A través de la dirección IP sabemos en qué red está la computadora y cuál es la computadora. Es decir verificado a través de un número único para aquella computadora en aquella red específica.

Existen cuatro tipos de números IP: las IP privadas, las públicas, las estáticas y las dinámicas.

2.3.3.1.- CLASES DE DIRECCIONES IP

Las direcciones IP se dividen en tres clases A, B y C y su objetivo es facilitar la búsqueda de un equipo en la red. De hecho, con esta notación es posible buscar primero la red a la que uno desea tener acceso y luego buscar el equipo dentro de esta red. Por lo tanto, la asignación de una dirección de IP se realiza de acuerdo al tamaño de la red.

Las direcciones de clase A se utilizan en redes muy amplias, mientras que las direcciones de clase C se asignan, por ejemplo, a las pequeñas redes de empresas.

Clase	Cantidad de redes posibles	Cantidad máxima de equipos en cada una
A	126	16777214
B	16384	65534
C	2097152	254

Tabla 2.2 Clasificación de las direcciones IP

2.3.4.- MASCARA DE SUB-RED

En realidad la IP por sí sola no sirve para identificarnos en la red. Tenemos que acompañarla siempre con la máscara de subred, la cual, a efectos prácticos es otra IP pero cuya numeración casi siempre va a estar compuesta por ceros y 255. Por ejemplo imaginemos que en casa tenemos un computador, una Xbox conectada a Internet y un iPad. La IP del primero es 192.168.1.2, la del segundo 192.168.1.3 y la del tercero 192.168.1.4. Como se puede ver, los tres primeros números son iguales mientras que el último cambia. Pues es precisamente con la máscara de subred como identificamos esa parte fija de la IP de la parte variable. ¿Cómo? De una manera muy sencilla, marcando la parte que no varía con 255 y la parte que sí lo hace con 0. Así que, siguiendo el ejemplo anterior, la máscara de subred sería 255.255.255.0.

En Internet, gracias a las máscaras de subred se pueden distinguir direcciones IP que a simple vista parecen iguales pero, al tener una máscara de subred distinta permite que no haya confusión y, lo que es más importante, sigan habiendo IP's disponibles.

2.3.5.- PUERTA DE ENLACE

Conociendo lo anterior, este es el término más sencillo de comprender. Y es que su propio nombre no invita a intuir para que sirve. Efectivamente, la puerta de enlace es la "puerta" por la que saldremos de "casa" hacia Internet. Esta metafórica puerta está más cerca de lo que creemos y es que en realidad es nuestro router, es decir, el que hace el trabajo de comunicarnos con el exterior.

Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

La pasarela es normalmente un equipo informático configurado para dotar a las máquinas de una red de área local (*Local Area Network*, LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red (*Network Address Translation*, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada "enmascaramiento de IP" (*IP Masquerading*), usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

La dirección IP de una pasarela a menudo se parece a 192.168.1.1 o 192.168.0.1 y utiliza algunos rangos predefinidos, 127.x.x.x, 10.x.x.x, 172.x.x.x, 192.x.x.x, que engloban o se reservan a las LAN.

En entornos domésticos, se usan los *routers ADSL* como puertas de enlace para conectar la red local doméstica con Internet; aunque esta puerta de enlace no conecta dos redes con protocolos diferentes, sí que hace posible conectar dos redes independientes haciendo uso de NAT.

2.3.6.- SERVIDOR DNS

DNS son las iniciales de Domain Name System (sistema de nombres de dominio) y es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder. Cuando un ordenador está conectado a una red (ya sea Internet o una red casera) tiene asignada una dirección IP. Si estamos en una red con pocos ordenadores, es fácil tener memorizadas las direcciones IP de cada uno de los ordenadores y así acceder a ellos pero ¿qué ocurre si hay miles de millones de dispositivos y cada uno tiene una IP diferente? Pues que se haría imposible, por eso existen los dominios y las DNS para traducirlos.

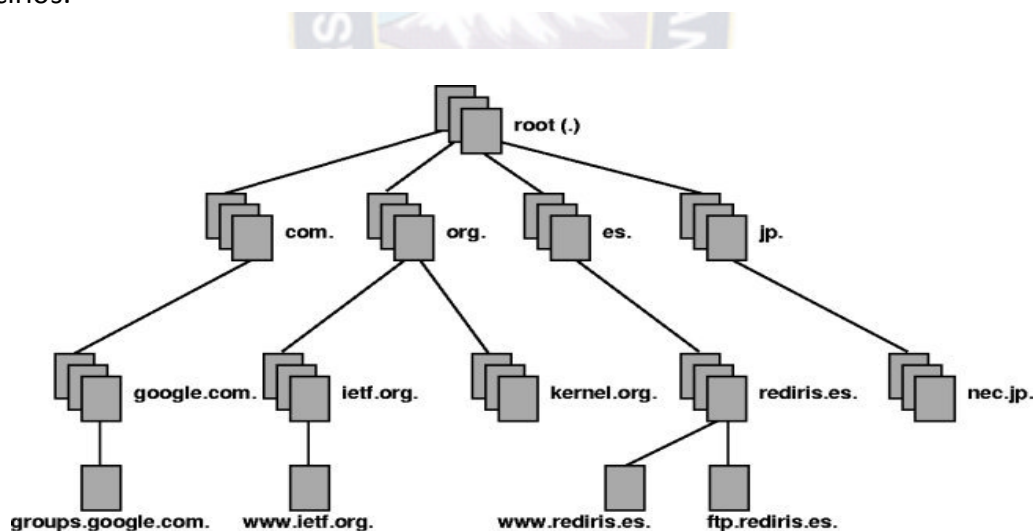


Figura 2.2 Estructura de árbol para petición de DNS

Por lo tanto, el DNS es un sistema que sirve para traducir los nombres en la red, y está compuesto por tres partes con funciones bien diferenciadas.

- **Ciente DNS:** está instalado en el cliente (es decir, nosotros) y realiza peticiones de resolución de nombres a los servidores DNS.

- **Servidor DNS:** son los que contestan las peticiones y resuelven los nombres mediante un sistema estructurado en árbol. Las direcciones DNS que ponemos en la configuración de la conexión, son las direcciones de los Servidores DNS.
- **Zonas de autoridad:** son servidores o grupos de ellos que tienen asignados resolver un conjunto de dominios determinado (como los .es o los .org).

La resolución de nombres utiliza una estructura en árbol, mediante la cual los diferentes servidores DNS de las zonas de autoridad se encargan de resolver las direcciones de su zona, y si no se lo solicitan a otro servidor que creen que conoce la dirección.

En la imagen se puede ver claramente como es la estructura en árbol. Y sí, hay un servidor general que tiene las direcciones de los servidores encargados de las zonas de autoridad. Lo que ocurre es que ese servidor son muchas máquinas repartidas en todos los lugares del mundo, por lo que no hay mucho peligro que nos quedemos sin servidores DNS (a no ser que haya un ataque muy planeado, claro está).

2.3.7.- QUE ES LA WWW

La World Wide Web (WWW) o red informática mundial es un sistema de distribución de documentos de hipertexto o hipermedios interconectados y accesibles vía Internet. Con un navegador web, un usuario visualiza sitios web compuestos de páginas web que pueden contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de esas páginas usando hiperenlaces.

El primer paso consiste en traducir la parte nombre del servidor de la URL (Uniform Resource Locator o en español Localizador Uniforme de Recursos), en una dirección IP usando la base de datos distribuida de Internet conocida como DNS. Esta dirección IP es necesaria para contactar con el servidor web y poder enviarle paquetes de datos.

El siguiente paso es enviar una petición HTTP al servidor web solicitando el recurso. En el caso de una página web típica, primero se solicita el texto HTML y luego es inmediatamente analizado por el navegador, el cual, después, hace peticiones adicionales para los gráficos y otros ficheros que formen parte de la página.

Al recibir los ficheros solicitados desde el servidor web, el navegador representa (renderiza) la página tal y como se describe en el código HTML y otros lenguajes web. Al final se incorporan las imágenes y otros recursos para producir la página que ve el usuario en su pantalla.

2.3.8.- QUE ES LA WEB

Web es un vocablo inglés que significa “red”, “telaraña” o “malla”. El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general, a Internet.

Una página web es un documento que incluye un archivo HTML (formato de lenguaje para hipertextos con texto), imágenes, videos, animaciones Flash, etc. Al conjunto de páginas web que suelen formar parte del mismo dominio o subdominio de Internet se lo conoce como sitio web. Dentro del sitio web, todas las páginas guardan alguna relación entre sí y están vinculadas mediante vínculos (también conocidos como enlaces, hipervínculos, hiperenlaces o links).

2.3.8.1.- QUE ES LA WEB 2.0

La Web 2.0 no es más que la evolución de la Web o Internet en el que los usuarios dejan de ser usuarios pasivos para convertirse en usuarios activos, que participan y contribuyen en el contenido de la red siendo capaces de dar soporte y formar parte de una sociedad que se informa, comunica y genera conocimiento. La Web 2.0 es un concepto que se acuñó en 2003 y que se refiere al fenómeno social surgido a partir del desarrollo de diversas aplicaciones en Internet. El término establece una distinción entre la primera época de la Web (donde el usuario era básicamente un sujeto pasivo que recibía la información o la publicaba, sin que existieran demasiadas posibilidades para que se generara la interacción) y la revolución que supuso el auge de los blogs, las redes sociales y otras herramientas relacionadas. Entre los ejemplos de Web 2.0 pueden nombrarse a las redes sociales (como Facebook), los portales de alojamiento de videos (YouTube) y los servicios wikis (Wikipedia).

2.3.9.- LA HTTP

HTTP de Hyper Text Transfer Protocol (Protocolo de transferencia de hipertexto) es el método más común de intercambio de información en la world wide web, el método mediante el cual se transfieren las páginas web a un ordenador y está ubicado en la capa de Aplicación del modelo OSI.

Todas las páginas web están escritas en lenguaje de hipertexto (HTML), por lo que el hipertexto es el contenido de las páginas web. El protocolo de transferencia es el sistema mediante el cual se transfiere información entre los servidores y los clientes (por ejemplo los navegadores).

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

LA HTTPS, Hypertext Transfer Protocol Secure (*Protocolo seguro de transferencia de hipertexto*), es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales y/o contraseñas.

Muchos navegadores incluyendo Firefox usan un aviso en la barra de direcciones para indicar al usuario que su conexión es segura, coloreando el fondo como el nombre del dueño del sitio web.

Cuando se accede a un sitio web con un certificado común, en la barra de direcciones no se observa al dueño del sitio. En algunos navegadores puede aparecer un candado.

El sistema HTTPS utiliza un cifrado basado en TLS/SSL (Transport Layer Security, seguridad de la capa de transporte y su antecesor Secure Sockets Layer capa de conexión segura, son protocolos criptográficos que proporcionan comunicaciones seguras por una red, (comúnmente Internet) para crear un canal cifrado más apropiado para el tráfico de información sensible que el protocolo HTTP. De este modo se consigue que la información sensible (usuario y claves de paso normalmente) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados que le resultará imposible de descifrar.

2.4.- DISPOSITIVOS DE RED

Son los elementos físicos que hacen posible la comunicación entre emisor y receptor para formar una red entre estos podemos mencionar los más destacados.

2.4.1.- ESTACION DE TRABAJO

Básicamente es una computadora de escritorio, un equipo portátil, una Tablet, un celular, etc., cualquier equipo que facilita a los usuarios el acceso a los servidores y periféricos de red.

2.4.2.- SERVIDOR

Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al “servicio” de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información. A modo de ejemplo, imaginemos que estamos en nuestra casa, y tenemos una despensa, pues bien a la hora de comer necesitamos unos ingredientes por lo cual vamos a la despensa, los cogemos y nos lo llevamos a la cocina para cocinarlos. Así en nuestro ejemplo, nuestra máquina servidor sería la despensa, y los clientes somos nosotros como personas que necesitamos unos ingredientes del servidor o despensa. Pues bien con este ejemplo podemos entender ahora un poco mejor qué es un servidor.

Por tanto básicamente tendremos el siguiente esquema general, en el denominado esquema “cliente-servidor” que es uno de los más usados ya que en él se basa gran parte de internet.

Como vemos, tenemos una máquina servidora que se comunica con variados clientes, todos demandando algún tipo de información. Esta información puede ser desde archivos de texto, video, audio, imágenes, emails, aplicaciones, programas, consultas a base de datos, etc.

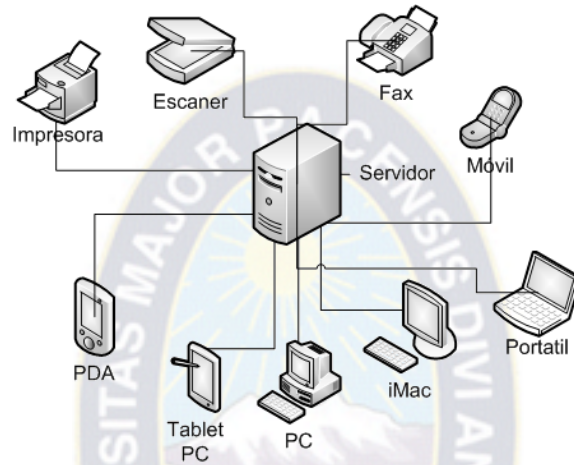


Figura 2.3 Servidor repartiendo distintos servicios

Dentro de la familia de los servidores tenemos varios que nos ayudan para dar un mejor servicio de Internet entre los cuales podemos mencionar a los servidores Proxi, DNS y WEB.

2.4.2.1.- SERVIDOR PROXY

Un servidor proxy es un equipo que actúa de intermediario entre un explorador web (como Internet Explorer) e Internet. Los servidores proxy ayudan a mejorar el rendimiento en Internet ya que almacenan una copia de las páginas web más utilizadas. Cuando un explorador solicita una página web almacenada en la colección (su caché) del servidor proxy, el servidor proxy la proporciona, lo que resulta más rápido que consultar la Web. Los servidores proxy también ayudan a mejorar la seguridad, ya que filtran algunos contenidos web y software malintencionado.

La palabra inglesa proxy significa *procurador* en español, el uso más común es el de servidor proxy, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.

2.4.2.2.- SERVIDOR DNS

Son las siglas de Domain Name System. Es un sistema por el que se asocia una información con un nombre de dominio. El ejemplo más claro es cuando introducimos una ruta URL en nuestro navegador de internet del tipo ***http://www.aprenderde-servidores.com*** una vez que hemos introducido esta ruta, dicha información es enviada a un servidor DNS que lo que hace es determinar en qué lugar se encuentra esa página web alojada y nos conecta con ella.

2.4.2.3.- SERVIDOR WEB

El término web va asociado a internet, donde los usuarios utilizan sus navegadores web para visitar sitios web, que básicamente se componen de páginas web donde los usuarios pueden acceder a informaciones con texto, videos, imágenes, etc. y navegan a través de enlaces o hipervínculos a otras webs.

2.4.3.- TARJETA DE RED

Permite la comunicación entre diferentes equipos conectados entre sí y también permite compartir recursos entre dos o más equipos. Opera en la capa 2 del modelo OSI el más común es del tipo Ethernet utilizando una interfaz o conector RJ45, cada tarjeta de Red tiene un número de identificación único de 48 bits, en hexadecimal llamado dirección MAC.



Figura 2.4 Tarjeta de Red básica

2.4.4.- HUB

El HUB es un concentrador o un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.



Figura 2.5 HUB de 8 puertos

2.4.5.- SWITCH

El switch es uno de los elementos más utilizados en el diseño e implementación de redes informáticas. Este pequeño dispositivo es vital para establecer múltiples conexiones. Un switch es un dispositivo de hardware, que también es conocido como conmutador, utilizado para establecer interconexiones en redes informáticas.

En pocas palabras, es un aparato que se utiliza para filtrar y encaminar paquetes de datos entre segmentos de redes locales y ofrecer conexión a los equipos que conforman una subred LAN.

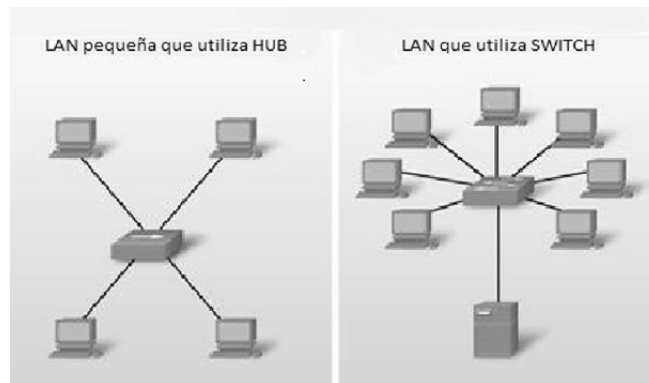


Figura 2.6 Diferencias entre HUB y SWITCH

El switch opera en la “capa de enlace” del modelo OSI, siendo completamente independiente de los protocolos que se ejecutan en las capas superiores de la red. Tiene la capacidad de escuchar todos los puertos y construir tablas para realizar un mapeo de las direcciones MAC, con el puerto a través del cual se pueden alcanzar estas direcciones.



Figura 2.7 Forma física de un Switch

2.4.6.- ROUTER

Un *router*; también conocido como enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador.

El funcionamiento básico de un enrutador o encaminador, como se deduce de su nombre, consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. Con arreglo a esta información reenvía los paquetes a otro encaminador o bien al anfitrión final, en una actividad que se denomina 'encaminamiento'.

Cada encaminador se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto.

Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- Reenvío de paquetes: cuando un paquete llega al enlace de entrada de un encaminador, éste tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los encaminadores es que no difunden tráfico difusivo.
- Encaminamiento de paquetes: mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.

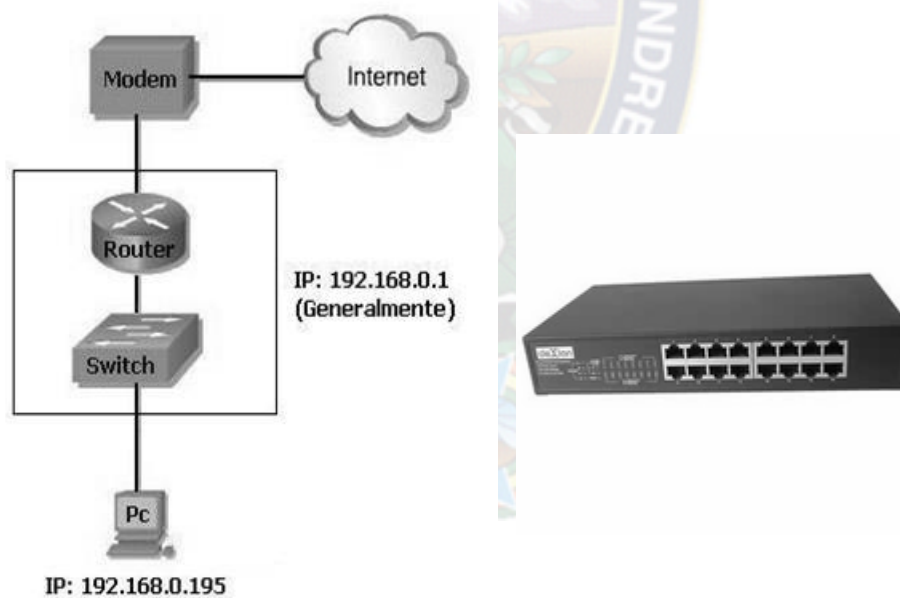


Figura 2.8 Forma lógica de conexión de un router y su esquema físico

Por tanto, debemos distinguir entre reenvío y encaminamiento. Reenvío consiste en coger un paquete en la entrada y enviarlo por la salida que indica la tabla, mientras que por encaminamiento se entiende el proceso de hacer esa tabla

2.4.7.- CABLE COAXIAL

Consiste en un conductor interno (cilíndrico) separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Todo esto se recubre por otra capa aislante (ocasionalmente de acero para darle rigidez mecánica y protegerlo frente a la corrosión y ataques de animales), que es la funda del cable.

Este cable es más caro que el par trenzado, pero se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar más estaciones. Se utiliza para televisión, telefonía a larga distancia, redes de área local, conexión de periféricos a corta distancia, etc., y su instalación y armado suele ser más compleja, además en caso de tener que enterrarse requiere de un permiso de obra civil.



Figura 2.9 Partes de un cable coaxial

2.4.8.- PAR TRENZADO

Es el medio guiado más usado y más barato y con estos cables se pueden transmitir señales analógicas y digitales. Consiste en un par de cables para cada enlace de comunicación, recubiertos para su aislamiento y protección.

Debido a que puede haber acoples entre pares, estos se trenzan con pasos diferentes, ya que la utilización del trenzado disminuye la interferencia electromagnética. Es un medio muy susceptible al ruido y las interferencias, por lo que para utilizarse en aplicaciones se suele recubrir como una malla metálica externa que las evita.

Este tipo de medio es el más utilizado debido a su bajo coste (se utiliza mucho en telefonía y con ADSL se aumenta el ancho de banda nominal), pero su inconveniente principal es su poca velocidad de transmisión y su corta distancia de alcance.

Los pares sin apantallar (UTP) son los más baratos, aunque los menos resistentes frente a las interferencias (aunque se usa con éxito en telefonía y en redes de área local). Los pares

apantallados (STP) son menos susceptibles a interferencias, aunque son más caros y más difíciles de instalar.

- Cable UTP, UTP son las siglas de Unshielded Twisted Pair. Es un cable de par trenzados y sin recubrimiento metálico externo, de modo que es sensible a las interferencias: sin embargo, al estar trenzado compensa las inducciones electromagnéticas producidas por las líneas del mismo cable. Es importante guardar la numeración de los pares ya que por el contrario el efecto del trenzado no sería eficaz, disminuyendo sensiblemente, o incluso impidiendo la capacidad de transmisión. Es un cable barato, flexible y sencillo de instalar, la impedancia de este cable es de 100 ohmios.

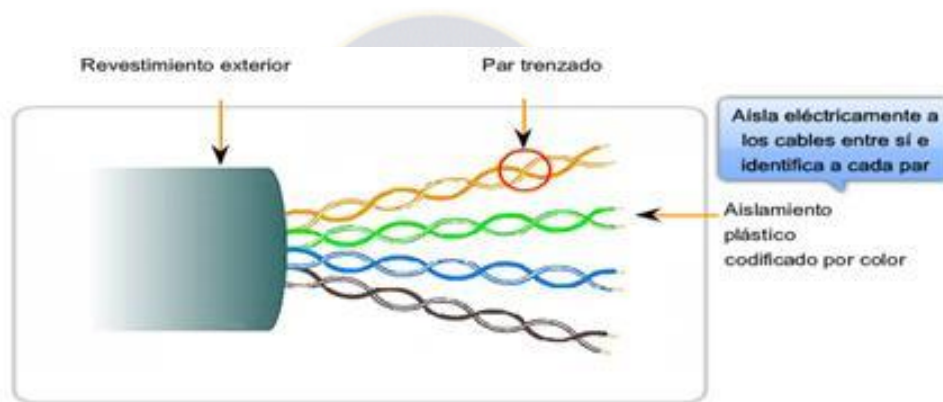


Figura 2.10 Cable UTP sin apantallar

- Cable STP, STP son las siglas de Shielded Twisted Pair, este cable es semejante al UTP, pero se le añade un requerimiento metálico para evitar las interferencias externas. Por tanto es un cable más protegido, pero menos flexible que es primero y su sistema de trenzado es semejante al cable UTP. La impedancia característica de un cable STP es de 150 ohmios.

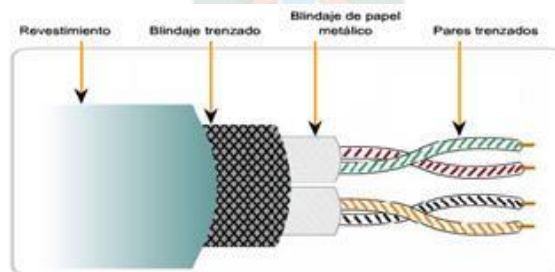


Figura 2.11 Cable UTP apantallado

2.4.9.- FIBRA OPTICA

Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza lumínica (fotones), con muy bajas pérdidas si se utiliza una de las tres ventanas de transmisión.

Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta. El núcleo está formado por una o varias fibras muy finas de cristal o plástico. Cada fibra rodeada por su propio revestimiento con diferentes propiedades ópticas a las del núcleo. Todo este conjunto se recubre para proteger el contenido de aplastamiento, abrasiones, humedad, etc.

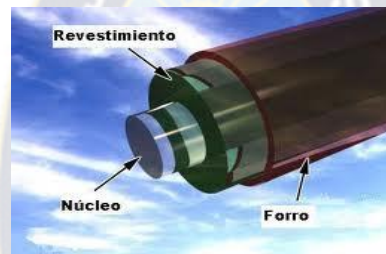


Figura 2.12 Forma física de una fibra óptica

Es un medio muy apropiado para largas distancias e incluso últimamente para redes locales, sus beneficios frente a cables coaxiales y pares trenzados son: permite mayor ancho de banda, menor tamaño y peso, menor atenuación, total aislamiento electromagnético, mayor separación entre repetidores. Los rayos de luz que incide en el núcleo de la fibra con ángulos diferentes, se van reflejando en la capa que lo recubre hasta llegar a su destino, a este tipo de propagación se le llama **multimodal**. Si se reduce el radio del núcleo suficientemente, solo es posible la transmisión de un rayo, el rayo axial, siendo **monomodal**, alcanzándose en este caso el mayor ancho de banda (2Ghz).

El inconveniente del modo multimodal es que dependiendo del ángulo de incidencia de los rayos, estos tomaran caminos diferentes y tardaran más o menos tiempo en llegar al destino, con lo que se puede producir una distorsión en los pulsos (desfase entre modos), con lo que se ve limitada la velocidad de transmisión.

Hay un tercer modo de transmisión que es un paso intermedio entre los anteriormente comentados y que consiste en cambiar el índice de refracción del núcleo. A este modo se le llama multimodo de índice gradual.

Los emisores de luz utilizados son: LED (de bajo coste, con utilización en un amplio rango de temperaturas y con larga vida media) y Laser (más caro, pero más eficaz y que permite mayor velocidad de transmisión). Para aumentar la capacidad de la fibra se utiliza la técnica DWDM (Multiplexación por Longitud de Onda-Densa).

A continuación se muestra una tabla de comparación de anchos de banda y distancias de transmisión entre cable coaxial, UTP y la fibra óptica.

Medios Típicos	Ancho de banda máximo teórico	Distancia máxima teórica
Cable coaxial de 50 ohmios (Ethernet 10Base2, Thinnet)	10 Mbps	185 m
Cable coaxial de 50 ohmios (Ethernet 10Base5, Thinnet)	10 Mbps	500 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 10Base-T)	10 Mbps	100 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 100Base-TX)	100 Mbps	100 m
Cable de par trenzado no blindado de categoría 5 (UTP) (Ethernet 1000Base-TX)	1000 Mbps	100 m
Fibra óptica Multimodo (62.5/125 μ m)(100Base-FX Ethernet)	100 Mbps	2000 m
Fibra óptica Multimodo (62.5/125 μ m)(1000Base-SX Ethernet)	1000 Mbps	220 m
Fibra óptica Multimodo (50/125 μ m)(1000Base-SX Ethernet)	1000 Mbps	550 m
Fibra óptica Multimodo (9/125 μ m)(1000Base-LX Ethernet)	1000 Mbps	5000 m

Tabla 2.3 Comparación entre cable coaxial, par trenzado y fibra óptica

2.5.- CLASIFICACION DE LAS REDES

Una red puede recibir distintos calificativos de clasificación sobre la base de distintas taxonomías: por su alcance, tipo de conexión, por su relación funcional, por su tecnología, por su topología física, por la direccionalidad de datos, por grado de autenticación, por su grado de difusión, por su servicio o función.

2.5.1.- CLASIFICACION DE LAS REDES SEGÚN SU ALCANCE

Las redes según su alcance se pueden dividir en diferentes grupos como ser:

- Redes PAN
- Redes LAN
- Redes MAN
- Redes WLAN
- Redes CAN
- Redes VLAN
- Redes WAN

Una de las redes con las que trabajamos en edificios y viviendas es la red LAN por lo cual es muy importante conocer los pormenores de esta red.

2.5.1.1.- REDES LAN

Las redes de Área local (Local Area Networks) llevan mensajes a velocidades relativamente grande entre computadoras conectados a un único medio de comunicaciones: Un cable de par trenzado, un cable coaxial o una fibra óptica. Las redes de área local mayores están compuestas por varios segmentos interconectados por conmutadores (switches) o concentradores (HUB's). El ancho de banda total del sistema es grande y la Latencia pequeña, salvo cuando el tráfico es muy alto.

Cuando tiene varios equipos, puede ser conveniente conectarlos entre sí para crear una red de área local (LAN). A diferencia de lo que la gente cree, el costo por configurar una red con estas características es muy reducido.

Existen dos clases principales de arquitectura de red local:

- Las redes conectadas, basadas en la tecnología Ethernet, que representan a la mayoría de las conexiones locales. Muchas veces se las denomina redes RJ45 ya que, por lo general, las redes Ethernet usan cables RJ45.
- Las redes inalámbricas, que generalmente usan la tecnología WiFi, corresponden a este tipo.

Para crear una Red LAN o RJ45 necesitamos:

- Varios equipos con el sistema operativo Windows, Linux, Mac u otro instalado (es posible tener dos equipos con diferentes versiones de sistema operativo en la misma red).
- Tarjetas Ethernet conectadas a un puerto ISA o PCI (con un conector RJ45) o integradas a la placa madre. Debemos asegurarnos de que los diodos de la parte posterior de la tarjeta de red, si corresponde, se enciendan cuando el equipo esté encendido y de que el cable esté conectado. También existen adaptadores de red para puertos USB, especialmente en el caso de los adaptadores de red inalámbrica.
- Los cables RJ45 en el caso de las redes conectadas.

- Un HUB, dispositivo al que se pueden conectar los cables RJ45 desde diferentes equipos de la red, un conmutador (Switch), un router o un cable cruzado, si desea conectar sólo dos equipos.

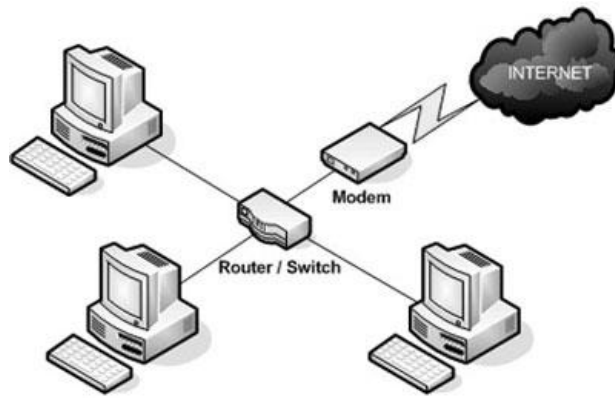


Figura 2.13 Estructura de una red LAN

2.5.2.- CLASIFICACION DE LAS REDES POR SU TIPO DE CONEXIÓN

Se refiere al medio que las redes utilizaras para conectarse ya seas físico o inalámbrico, estos pueden ser medios guiados y no guiados.

2.5.2.1.- MEDIOS GUIADOS

Los medios guiados son:

- Cable de par trenzado, es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes. Dependiendo de la red se pueden utilizar, uno, dos, cuatro o más pares trenzados.
- Cable coaxial, se utiliza para transportar señales electromagnéticas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo y uno exterior denominado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes; los cuales están separados por un material dieléctrico que, en realidad, transporta la señal de información.
- Fibra óptica, es un 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.

2.5.2.2.- MEDIOS NO GUIADOS

Son aquellos que no utilizan medios físicos como ser:

- Red por radio, en aquella que emplea radio frecuencia como medio de unión de las diversas estaciones de la red.
- Red por infrarrojos, (*Infrared Data Association, IrDA*), permiten la comunicación entre dos nodos, usando una serie de led's infrarrojos para ello. Se trata de emisores/receptores de ondas infrarrojas entre ambos dispositivos, cada dispositivo necesita al otro para realizar la comunicación por ello es escasa su utilización a gran escala. No disponen de gran alcance y necesitan de visibilidad entre los dispositivos.
- Red por microondas, es un tipo de red inalámbrica que utiliza microondas como medio de transmisión. Los protocolos más frecuentes son: el IEEE 802.11b y transmite a 2,4 GHz, alcanzando velocidades de 11 Mbps (Megabits por segundo); el rango de 5,4 a 5,7 GHz para el protocolo IEEE 802.11a; el IEEE 802.11n que permite velocidades de hasta 600 Mbps; etc.

2.5.3.- CLASIFICACION DE LAS REDES POR SU RELACION FUNCIONAL

Este tipo de redes se subdividen en dos tipos de arquitecturas:

- Cliente – Servidor.
- Arquitectura P2P.

2.5.4.- CLASIFICACION DE LAS REDES POR SU TOPOLOGIA FISICA

Se llama topología de una Red al patrón de conexión entre sus nodos, es decir, a la forma en que están interconectados los distintos nodos que la forman. Los Criterios a la hora de elegir una topología, en general, buscan que eviten el coste del encaminamiento (necesidad de elegir los caminos más simples entre el nodo y los demás), dejando en segundo plano factores como la renta mínima, el coste mínimo, etc. Otro criterio determinante es la tolerancia a fallos o facilidad de localización de éstos. También tenemos que tener en cuenta la facilidad de instalación y reconfiguración de la Red.

La topología hace referencia a la forma de una red. La topología muestra cómo los diferentes nodos están conectados entre sí, y la forma de cómo se comunican está determinada por la topología de la red. Las topologías pueden ser físicas o lógicas, la primera consiste en la configuración o disposición del cableado y equipos de comunicación. La lógica define como los datos fluyen a través de la red. Este tipo de topologías pueden ser:

- Topología tipo Bus
- Topología tipo Anillo
- Topología tipo Estrella
- Topología tipo Malla
- Topología tipo Árbol
- Topología Híbrida

2.5.5.- CLASIFICACION DE LAS REDES POR LA DIRECCIONALIDAD DE DATOS

Un método de caracterizar líneas, dispositivos terminales, computadoras y modems es por su modo de transmisión o de comunicación. Las tres clases de modos de transmisión son simplex, half-duplex y full-duplex.

La transmisión simplex (sx) o *unidireccional* es aquella que ocurre en una dirección solamente, deshabilitando al receptor de responder al transmisor. Normalmente la transmisión simplex no se utiliza donde se requiere interacción humano-máquina. Ejemplos de transmisión simplex son: La radiodifusión (broadcast), la TV y radio. La transmisión half-duplex (hdx) permite transmitir en ambas direcciones; sin embargo, la transmisión puede ocurrir solamente en una dirección a la vez. Tanto transmisor y receptor comparten una sola frecuencia. Un ejemplo típico de half-duplex es el radio de banda civil (CB) donde el operador puede transmitir o recibir, pero no puede realizar ambas funciones simultáneamente por el mismo canal. Cuando el operador ha completado la transmisión, la otra parte debe ser avisada que puede empezar a transmitir (ejemplo diciendo "cambio"). La transmisión full-duplex (fdx) permite transmitir en ambas direcciones, pero simultáneamente por el mismo canal. Existen dos frecuencias una para transmitir y otra para recibir. Ejemplos de este tipo abundan en el terreno de las telecomunicaciones, el caso más típico es la telefonía, donde el transmisor y el receptor se comunican simultáneamente utilizando el mismo canal, pero usando dos frecuencias.

2.5.6.- CLASIFICACION DE LAS REDES POR SU AUTENTIFICACION

Según el grado de autenticación las redes pueden ser de dos tipos, privadas y de acceso público.

2.5.7.- CLASIFICACION DE LAS REDES SEGÚN SU GRADO DE DIFUSION

Según el grado de difusión las redes se subdividen en redes Intranet y redes de Internet.

2.5.7.1.- REDES INTRANET

Es una red privada de computadoras que utiliza tecnología de Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.

Considerada como un sitio web interno, diseñado para ser utilizado dentro de los límites de la compañía. Lo que distingue una Intranet de un sitio de Internet, es que las intranets son privadas y la información que en ella reside tiene como objetivo asistir a los trabajadores en la generación de valor para la empresa.

El 80% de la información que se utiliza diariamente para realizar el trabajo no está en los sistemas transaccionales de las empresas. Se estima que un empleado promedio consume

entre un 25% y 30% de su tiempo buscando información. Esto significa que las empresas pierden mensualmente un 30% del dinero correspondiente al costo de sus empleados, sumado al lucro cesante derivado de este tiempo improductivo en los que los empleados no generan valor para la empresa.

Una Intranet pone a disposición esta información a lo largo y ancho de la empresa, las 24 horas del día, los 365 días del año, trabajando en la oficina, estando de viaje o desde la casa haciendo trabajo remoto. Todo bajo un esquema de seguridad y control de acceso que asegura que cada persona puede ver únicamente lo que le corresponde

2.5.7.2.- REDES INTERNET

Podemos definir a Internet como una "red de redes" que utiliza el protocolo TCP/IP como su protocolo de comunicación. La Internet es una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos.



Figura 2.14 La red de Internet conecta al mundo entero

De esta manera, Internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una "red global". Esta red global tiene la característica de que utiliza un lenguaje común que garantiza la intercomunicación de los diferentes participantes; este lenguaje común o protocolo (un protocolo es el lenguaje que utilizan las computadoras al compartir recursos) se conoce como TCP/IP.

Internet es un acrónimo de INTERconnected NETworks (Redes interconectadas). Para otros, Internet es un acrónimo del inglés INTERnational NET, que traducido al español sería Red Mundial.

2.5.8.- CLASIFICACION DE LAS REDES POR SU SERVICIO O FUNCION

Por último, según Servicio o Función de las Redes, se pueden clasificar como Redes Comerciales, Educativas o Redes para el Proceso de Datos. Todas estas clasificaciones, nos

permiten identificar la forma en que estamos conectados a una red, qué uso podemos darle y el tipo de información a la cual tendremos acceso. Conocerlas entonces nos servirá para elegir con una base mucho más sólida, qué conexión necesitamos para cubrir las necesidades de nuestro negocio y valorizar los costos que implica cada una de ellas.

2.6.- PROTOCOLO DE COMUNICACIONES

En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física. Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, por software, o por una combinación de ambos.

Los sistemas de comunicación utilizan formatos bien definidos (protocolo) para intercambiar mensajes. Cada mensaje tiene un significado exacto destinado a obtener una respuesta de un rango de posibles respuestas predeterminadas para esa situación en particular. Normalmente, el comportamiento especificado es independiente de cómo se va a implementar. Los protocolos de comunicación tienen que estar acordados por las partes involucradas. Para llegar a dicho acuerdo, un protocolo puede ser desarrollado dentro de un estándar técnico. Un lenguaje de programación describe el mismo para los cálculos, por lo que existe una estrecha analogía entre los protocolos y los lenguajes de programación, (los protocolos son para las comunicaciones como los lenguajes de programación son para las computadoras). Un protocolo de comunicación, también llamado en este caso **protocolo de red**, define la forma en la que los distintos mensajes o tramas de bit circulan en una red de computadoras.

Un protocolo de comunicación se puede definir también como un conjunto de reglas y procedimientos que permite a los sistemas el intercambio de información.

2.7.- MODELO OSI Y SUS CARACTERISTICAS

El **modelo de referencia OSI** (*open system interconnection*, interconexión de sistemas abiertos) lo desarrolló la ISO (*international standard organisation*, organización internacional de normalización) como una guía para definir un conjunto de protocolos abiertos. Su finalidad es proporcionar una base común para la coordinación en el desarrollo de normas destinadas a la interconexión de sistemas, permitiendo a la vez situar las normas existentes en la perspectiva del modelo de referencia global.

El modelo OSI tiene siete capas o niveles, como se muestra en la figura:

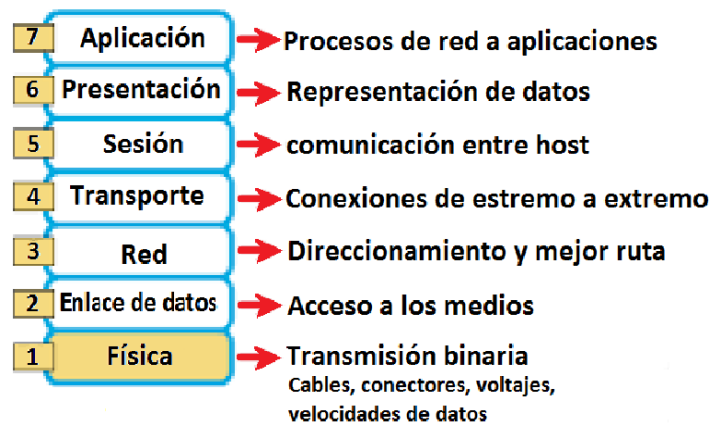


Figura 2.15 Las capas del modelo de referencia OSI

Los siete niveles que configuran el modelo OSI suelen agruparse en dos bloques. Los tres niveles inferiores (físico, de enlace, de red) constituyen el bloque de transmisión. Son niveles dependientes de la red de conmutación utilizada para la comunicación entre los dos sistemas. Por el contrario, los tres niveles superiores (de sesión, de presentación y de aplicación) son niveles orientados a la aplicación y realizan funciones directamente vinculadas con los procesos de comunicación. El nivel intermedio (de transporte) enmascara a los niveles orientados a la aplicación el funcionamiento detallado de los niveles

2.7.1.- INTRODUCCION A LA CAPA FISICA

La capa física comunica directamente con el medio de comunicación; se ocupa de enviar y recibir bits. En esta capa se decide qué voltaje describe un 0 y cuál un 1; los microsegundos que dura un bit; si la transmisión se puede efectuar simultáneamente en ambas direcciones; cómo se establece la conexión inicial y cómo se interrumpe, etc.

En esta capa se ubican los repetidores, amplificadores, estrellas pasivas, multiplexores, concentradores, módems, codecs, CSUs, DSUs, transceivers, transductores, cables, conectores, NICs, etc.

2.7.2.- LA CAPA DE ENLACE DE DATOS

El nivel de enlace de datos detecta y corrige los errores que ocurren en el nivel físico, proporcionando una línea libre de errores de transmisión al nivel de red. Para ello trocea los datos de entrada en marcos de datos, los transmite secuencialmente, y procesa los marcos reconocidos, ofreciendo una comunicación fiable y eficiente entre dos máquinas adyacentes.

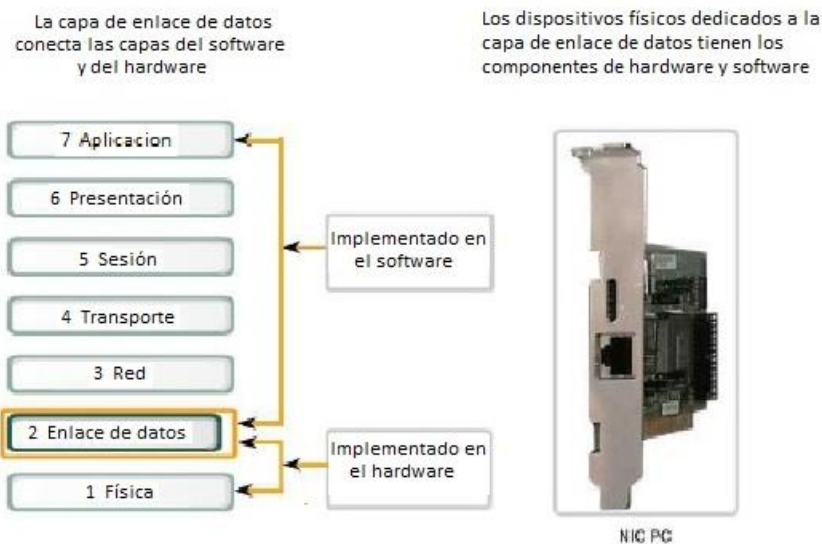


Figura 2.16 Función de la capa de enlace de Datos

El enlace de datos puede definirse como el conjunto de 2 componentes conectados por un circuito de emisión de datos, es decir, un enlace de datos es el conjunto de estaciones terminales con sus circuitos de datos asociados que constituyen un sistema que permite el intercambio de información entre dichos elementos.

Además se encarga también del control de flujo, es decir, de la regulación del ritmo de envío de tramas desde el transmisor con el fin de no abrumar a los receptores lentos. Mientras que la capa física proporciona solamente un servicio bruto de flujo de datos, la capa de enlace de datos intenta hacer el enlace físico seguro y proporciona medios para activar, mantener y desactivar el enlace. Puesto que la capa física se encarga de la transmisión de cadenas de bits no estructuradas, una de las funciones del nivel de enlace será agrupar estos bits en marcos en los que se incluirán además de los bits de información campos de delimitación del marco (para saber cuál es el inicio y el final de dicho marco).

2.7.3.- LA CAPA DE RED

La capa de red se ocupa de controlar el funcionamiento de la subred, proporcionando un mecanismo que dirige los mensajes de una red a otra.

Para entregar mensajes en una red, cada subred debe estar identificada de forma única por una dirección de subred. Al recibir un mensaje de las capas superiores, la capa de red añade una cabecera al mensaje incluyendo las direcciones de subred de origen y destino. Este conjunto de datos sumado a la capa de red se denomina paquete. La información de la dirección de subred se utiliza para entregar el mensaje a la subred correcta; después la capa de enlace de datos puede utilizar la dirección del nodo para entregar el mensaje.

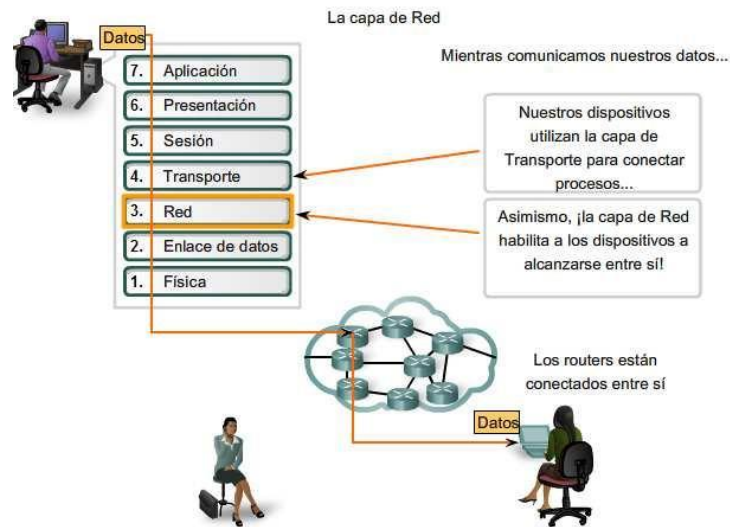


Figura 2.17 La capa de red

La Capa de red o Capa 3 de OSI provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados.

Para realizar este transporte de extremo a extremo la Capa 3 utiliza cuatro procesos básicos: direccionamiento, encapsulamiento, enrutamiento y desencapsulamiento.

2.7.3.1.- DIRECCIONAMIENTO

Primero, la Capa de red debe proveer un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red.

2.7.3.2.- ENCAPSULAMIENTO

Segundo, la capa de Red debe proveer encapsulación. Los dispositivos no deben ser identificados sólo con una dirección las secciones individuales, las PDU (Unidades de Datos de Protocolo), de la capa de red, deben además, contener estas, direcciones. Durante el proceso de encapsulación, la Capa 3 recibe la PDU de la Capa 4 y agrega un encabezado o etiqueta de Capa 3 para crear la PDU de la Capa 3. Cuando nos referimos a la capa de Red, denominamos paquete a esta PDU. Cuando se crea un paquete, el encabezado debe contener, entre otra información, la dirección del host hacia el cual se lo está enviando. A esta dirección se la conoce como dirección de destino. El encabezado de la Capa 3 también contiene la dirección del host de origen. A esta dirección se la llama dirección de origen.

Después de que la Capa de red completa el proceso de encapsulación, el paquete es enviado

a la capa de enlace de datos que ha de prepararse para el transporte a través de los medios.

2.7.3.3.- ENRUTAMIENTO

Luego, la capa de red debe proveer los servicios para dirigir estos paquetes a su host destino. Los host de origen y destino no siempre están conectados a la misma red. En realidad, el paquete podría recorrer muchas redes diferentes. A lo largo de la ruta, cada paquete debe ser guiado a través de la red para que llegue a su destino final. Los dispositivos intermediarios que conectan las redes son los routers. La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. A este proceso se lo conoce como enrutamiento.

La función del router es seleccionar las rutas y dirigir paquetes hacia su destino. A este proceso se lo conoce como enrutamiento.

2.7.3.4.- DEENCAPSULAMIENTO

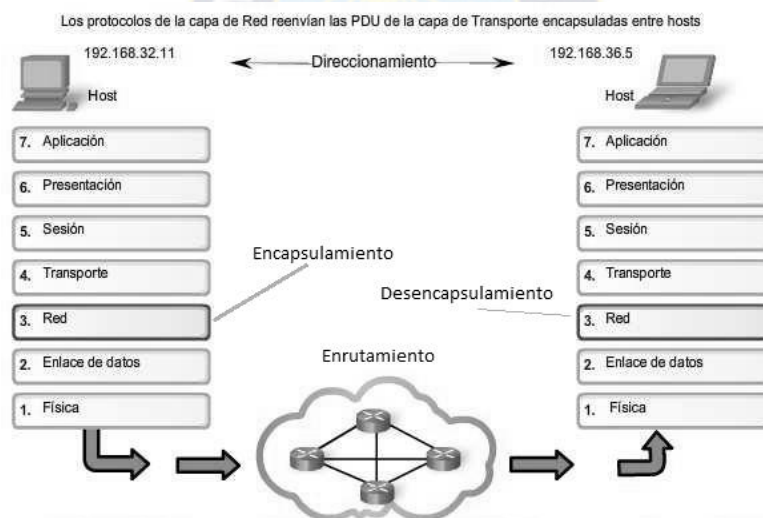


Figura 2.18 Procesos básicos de la capa de red

Finalmente, el paquete llega al host destino y es procesado en la Capa 3. El host examina la dirección de destino para verificar que el paquete fue direccionado a ese dispositivo. Si la dirección es correcta, el paquete es desencapsulado por la capa de Red y la PDU de la Capa 4 contenida en el paquete pasa hasta el servicio adecuado en la capa de Transporte.

2.7.4.- LA CAPA DE TRANSPORTE

La función básica de la capa de transporte es aceptar datos de la capa de red y de sesión, dividirlos en unidades más pequeñas si es necesario, pasarlo al siguiente nivel ya sea de ida o vuelta y asegurar que todas las unidades lleguen correctamente al otro extremo.

La capa de Transporte permite la segmentación de datos y brinda el control necesario para re ensamblar las partes dentro de los distintos streams de comunicación. La capa 4 del modelo OSI tiene cuatro responsabilidades fundamentales que son:

- Seguimiento de conversaciones individuales.
- Segmentación de datos.
- Re ensamblaje de segmentos.
- Identificación de las aplicaciones.



Figura 2.19 Fragmentación de datos en la capa de transporte

Las aplicaciones no necesitan conocer los detalles de operación de la red en uso. Las aplicaciones generan datos que se envían desde una aplicación a otra sin tener en cuenta el tipo de host destino, el tipo de medios sobre los que los datos deben viajar, el paso tomado por los datos, la congestión en un enlace o el tamaño de la red. Además, las capas inferiores no tienen conocimiento de que existen varias aplicaciones que envían datos en la red. Su responsabilidad es entregar los datos al dispositivo adecuado. Luego la capa de Transporte ordena estas secciones antes de entregarlas a la aplicación adecuada.

La división de los datos en partes pequeñas y el envío de estas partes desde el origen hacia el destino permiten que se puedan entrelazar (multiplexar) distintas comunicaciones en la misma red. La segmentación de los datos, que cumple con los protocolos de la capa de Transporte, proporciona los medios para enviar y recibir datos cuando se ejecutan varias aplicaciones de manera concurrente en una computadora. Sin segmentación, sólo una aplicación, la corriente de vídeo por ejemplo, podría recibir datos. No se podrían recibir

correos electrónicos, chats ni mensajes instantáneos ni visualizar páginas Web y ver un vídeo al mismo tiempo.

En la capa de Transporte, cada conjunto de secciones en particular que fluyen desde una aplicación de origen a una de destino se conoce como conversación. Para identificar todos los segmentos de datos, la capa de Transporte agrega un encabezado a la sección que contiene datos binarios. Este encabezado contiene campos de bits. Son los valores de estos campos los que permiten que los distintos protocolos de la capa de Transporte lleven a cabo las diversas funciones.

Por varias razones, es posible que una sección de datos se corrompa o se pierda por completo a medida que se transmite a través de la red. La capa de Transporte puede asegurar que todas las secciones lleguen a destino al contar con el dispositivo de origen para volver a transmitir los datos que se hayan perdido.

Ya que las redes proveen rutas múltiples que pueden poseer distintos tiempos de transmisión, los datos pueden llegar en el orden incorrecto. Al numerar y secuenciar los segmentos, la capa de Transporte puede asegurar que los mismos se re ensamblen en el orden adecuado.

2.7.5.- LA CAPA DE SESION

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos ordenadores que están transmitiendo datos. 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 puede efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción.

La capa de sesión proporciona los siguientes servicios:

- Control del dialogo: este puede ser simultáneo en los sentidos (full-duplex) o alternando en ambos sentidos (half-duplex).
- Agrupamiento: el flujo de datos se puede marcar para definir grupos de datos.
- Recuperación: La capa de sesión puede proporcionar un procedimiento de puntos de comprobación, de forma que si ocurre algún tipo de fallo entre puntos de comprobación, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación y no desde el principio.

2.7.6.- LA CAPA DE PRESENTACION

El nivel de presentación o capa de presentación es el sexto nivel del Modelo OSI que se encarga de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC),

números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que 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. Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

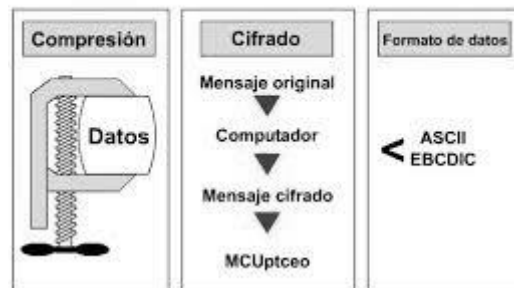


Figura 2.20 Función de la capa de presentación

Esta capa también permite cifrar los datos y comprimirlos. Actúa como traductor.

La Capa 6, o capa de presentación, cumple tres funciones principales. Estas funciones son las siguientes:

- Formateo de datos
- Cifrado de datos
- Compresión de datos

2.7.7.- LA CAPA DE APLICACIÓN

Esta capa ofrece a las aplicaciones (de usuario o no) 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 protocolos de transferencia de archivos (FTP).

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. Así por ejemplo un usuario no manda una petición «GET /index.html HTTP/1.0» para conseguir una página en html, ni lee directamente el código html/xml. O cuando chateamos con el Mensajero Instantáneo, no es necesario que codifiquemos la información y los datos del destinatario para entregarla a la capa de Presentación (capa 6) para que realice el envío del paquete.

Como es la única capa que proporciona servicios directamente a los procesos de aplicación, la capa de aplicación ofrece todos los servicios de OSI directamente utilizables por los procesos de aplicación.

2.7.8.- VENTAJAS DEL MODELO OSI

Las ventajas que ofrecen este modelo son:

- a) Divide la comunicación de la red en partes más pequeñas y sencillas.
- b) Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- c) Permite a los distintos tipos de hardware y software de red comunicarse entre sí, evitando los problemas de compatibilidad.
- d) Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- e) Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.
- f) Detalla las capas para su mejor aprendizaje.

2.7.9.- DESVENTAJAS DEL MODELO OSI

Las principales desventajas de este modelo son:

- a) Mala sincronización: El momento en el que se establece un estándar es crucial para su éxito. Ahora, los protocolos estándar del OSI han quedado aplastados. Los protocolos TCP/IP ya se usaban ampliamente cuando aparecieron los modelos OSI. Esto hizo que la inversión fuera para los protocolos TCP/IP, así cuando OSI llegó, los inversionistas no quisieron apoyar una segunda pila de protocolos por lo que nunca sucedió.
- b) Mala tecnología: La segunda razón por la que OSI nunca prendió, es que tanto el modelo como los protocolos son imperfectos, una explicación errónea acerca de este modelo de siete capas es que estas son el único camino, y que la verdadera razón de que tenga este número de capas es que en el momento en el que lo diseñó IBM tenía un protocolo patentado de siete capas SNA (System Network Architecture), y en esa época IBM dominaba la industria de la computación. Otro problema con OSI, además de ser incomprensible, es que algunas funciones reaparecen una y otra vez en cada capa, además el estándar original ignora por completo los servicios y protocolos carentes de conexión, la relación entre la computación y las comunicaciones apenas si se mencionaban.
- c) Malas instrumentaciones: Dada la enorme complejidad sus implementaciones iniciales fueron enormes, inmanejables y lentas a OSI se le asoció con la mala calidad. Mientras los productos mejoraban con el paso del tiempo, la imagen empeoraba.

- d) Mala política: A OSI se le veía como una invención de los ministerios europeos de telecomunicaciones y más tarde de los EEUU. Esta creencia no era justificada, pero no ayudo mucho la idea de que un montón de burócratas trataran de implementar cierto estándar.

2.8.- MODELO TCP / IP

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas UNIX. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP / IP.

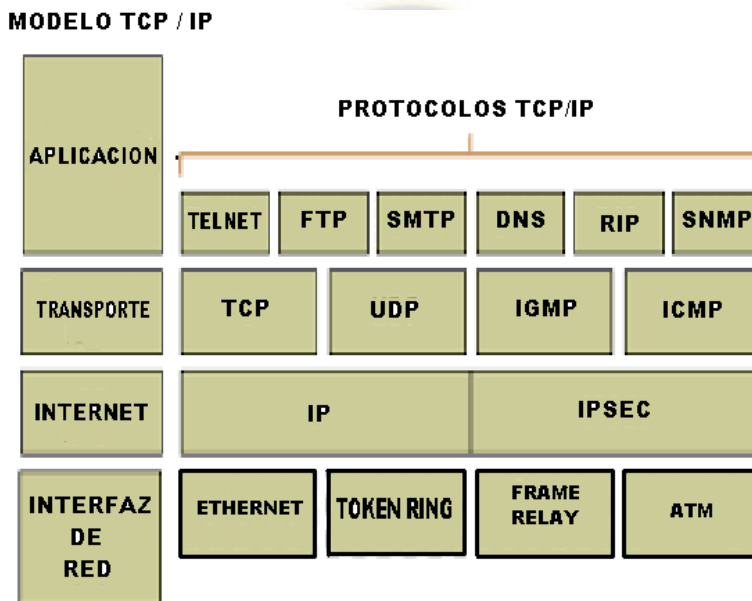


Figura 2.21 Protocolos del modelo TCP/IP

Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP/IP Proviene de dos protocolos importantes de la familia, el Transmission Control Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.

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

2.8.1.- COMO FUNCIONA EL TCP/IP

Una red TCP/IP transfiere datos mediante el ensamblaje de bloques de datos en paquetes, cada paquete comienza con una cabecera que contiene información de control, tal como la dirección del destino, seguido de los datos. Cuando se envía un archivo por la red TCP/IP, su contenido se envía utilizando una serie de paquetes diferentes. El Internet protocol (IP), un protocolo de la capa de red, permite a las aplicaciones ejecutarse transparentemente sobre redes interconectadas. Cuando se utiliza IP, no es necesario conocer que hardware se utiliza, por tanto ésta corre en una red de área local.

Hasta la fecha se han creado 6 versiones diferentes de TCP/IP, siendo la cuarta (IPv4) la implementación más extendida. La quinta versión estuvo basada en el modelo OSI y nunca se implementó. La última (y sexta llamada IPv6 o también IPng - IP Next Generation), el IPv6 incrementa el tamaño de la dirección IP de 32 bits a 128 bits para así soportar más niveles en la jerarquía de direccionamiento y un número mucho mayor de nodos direccionables. El diseño del protocolo agrega múltiples beneficios en seguridad, manejo de calidad de servicio, una mayor capacidad de transmisión y mejora la facilidad de administración, entre otras cosas.

2.8.2.- ENCAPSULACION DE DATOS Y LAS CAPAS DEL MODELO TCP/IP

Durante una transmisión, los datos cruzan cada una de las capas en el nivel del equipo remitente. En cada capa, se le agrega información al paquete de datos. Esto se llama encabezado, es decir, una recopilación de información que garantiza la transmisión. En el nivel del equipo receptor, cuando se atraviesa cada capa, el encabezado se lee y después se elimina. Entonces, cuando se recibe, el mensaje se encuentra en su estado original.

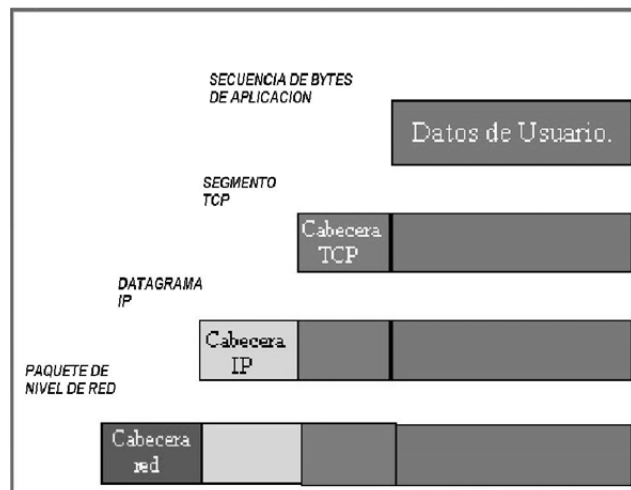


Figura 2.22 Modo de encapsulamiento de datos

En cada nivel, el paquete de datos cambia su aspecto porque se le agrega un encabezado. Por lo tanto, las designaciones cambian según las capas:

- El paquete de datos se denomina mensaje en el nivel de la capa de aplicación.
- El mensaje después se encapsula en forma de segmento en la capa de transporte.
- Una vez que se encapsula el segmento en la capa de Internet, toma el nombre de datagrama.
- Finalmente, se habla de trama en el nivel de capa de acceso a la red.

El modelo TCP/IP a diferencia del modelo OSI consta de cuatro capas que simplifican el trabajo, como se muestra en la siguiente figura.

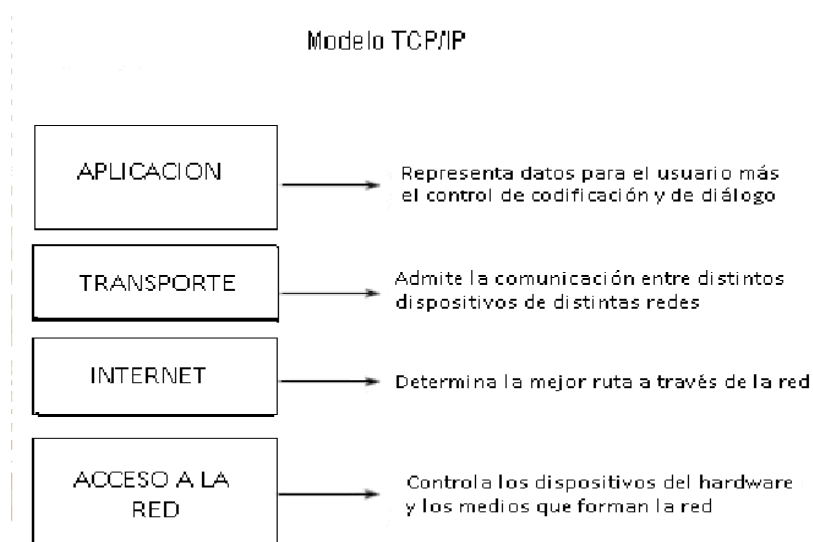


Figura 2.23 Capas del modelo TCP/IP

2.8.2.1.- CAPA DE INTERFAZ DE RED

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).

Otra función importante de esta capa es la de asociar las direcciones IP a direcciones físicas de los dispositivos adaptadores de red (NIC). Por ejemplo: la dirección IP 192.168.1.5 de un ordenador se asocia a la dirección Ethernet 00-0C-6E-2B-49-65. La primera es elegida por el usuario (e, incluso, un mismo ordenador puede trabajar con diferentes direcciones IP). Sin embargo la segunda no puede cambiarse e identifica inequívocamente al adaptador NIC dentro de la red Ethernet.

2.8.2.2.- LA CAPA DE INTERNET

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.

El protocolo IP se ha diseñado para redes de paquetes conmutados no orientadas a conexión, lo cual quiere decir que cuando dos equipos quieren conectarse entre sí no intercambian información para establecer la sesión. IP tampoco se encarga de comprobar si se han producido errores de transmisión, confía esta función a las capas superiores. Todo ello se traduce en que los paquetes de datos contienen información suficiente como para propagarse a través de la red sin que haga falta establecer conexiones permanentes.

Las cinco (o seis) primeras palabras de 32 bits contienen la información necesaria para que el datagrama se propague por la red, y a continuación se adjuntan los datos.

La capa de Internet contiene 5 protocolos siendo los tres primeros los más importantes:

- El protocolo IP, define la unidad básica de transferencia de datos entre el origen y el destino.
- El protocolo ARP, resolución de direcciones.
- El protocolo ICMP, mensajes de control de internet.
- El protocolo RARP, resolución inversa de direcciones
- El protocolo IGMP, mensajes de internet.

2.8.2.3.- CAPA DE TRANSPORTE

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.

En el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo *host*, o puesto de trabajo.

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 la que la detección de errores es obsoleta.

2.8.2.4.- LA CAPA DE APLICACIÓN

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. TCP/IP tiene en esta capa protocolos que soportan servicios de conexión remota, correo electrónico y transferencia de archivos. De todos los protocolos de aplicación los más conocidos son:

- **FTP** (*File Transfer Protocol*). Protocolo orientado a conexión dedicado a la transferencia de archivos. FTP ofrece una gran fiabilidad con este servicio debido a que se basa en el protocolo TCP dentro de la capa de transporte.
- **SMTP** (*Simple Mail Transfer Protocol*). Posibilita el funcionamiento del correo electrónico en las redes de ordenadores. SMTP recurre al protocolo de oficina postal.
- **POP** (*Post Office Protocol*) para almacenar mensajes en los servidores de correo electrónico. Existen dos versiones:

- **POP2**, que necesita la intervención de SMTP para enviar mensajes.
- **POP3**, que funciona de forma independiente.

• **HTTP** (*Hipertext Transfer Protocol*). Es un estándar de Internet que permite la transmisión de gran variedad de archivos de texto, gráficos, sonidos e imágenes. HTTP regula el proceso mediante el cual navegadores como Netscape, Mozilla o Internet Explorer solicitan información a los servidores web.

• **DNS** (*Domain Name Service*). Esta aplicación convierte nombres de dispositivos y de nodos de red en direcciones IP. Por ejemplo, el nombre *www.mcgraw-hill.es*, se convierte en la dirección 198.45.24.91.

Para poder entender un poco mejor el funcionamiento de las capas del modelo TCP/IP se muestra es siguiente resumen el cual describe cómo funciona cada nivel capa del modelo TCP IP, también se indica algunos de los protocolos más utilizados en este modelo:

NIVEL	DESCRIPCION	PROTOCOLOS
APLICACIÓN	Define los protocolos de aplicación TCP/IP y como se conectan los programas de host a los servicios del nivel de transporte para utilizar la red.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows y otros protocolos de aplicación
TRANSPORTE	Permite administrar las sesiones de comunicación entre equipos host. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos	TCP, UDP, RTP
INTERNET	Empaqueta los datos en datagramas IP, que contienen la información de las direcciones de origen y destino utilizada para reenviar los datagramas entre host y a través de redes. Realiza el enrutamiento de los datagramas IP	IP, ICMP, ARP, RARP
INTERFAZ DE RED	Especifica información detallada de cómo se envían físicamente los datos a través de la red, que incluye como se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

Tabla 2.4 Resumen del modelo TCP/IP

2.8.3.- VENTAJAS Y DESVENTAJAS DEL MODELO TCP/IP

Este modelo al ser el más utilizado presenta muchas más ventajas comparado con el modelo OSI ya que debido a las capas que utiliza basado en su mayoría en protocolos facilita el trabajo de envío de información. Entre sus principales ventajas tenemos:

- El conjunto TCP/IP está diseñado para enrutar.

- Tiene un alto grado de fiabilidad.
- Es adecuado para grandes redes y medianas, así como en redes empresariales
- Se utiliza a nivel mundial para conectarse a internet y a los servicios web, es compatible con las herramientas estándar para analizar el funcionamiento de la red.
- Es más rápido en redes con volumen de tráfico grande donde haya que enrutar un gran número de tramas.

A pesar de ser el modelo más utilizado también presenta algunas desventajas pero que pueden ser superadas:

- Es más difícil de configurar y mantener.
- Es algo más lento en redes de tráfico con un volumen de tráfico medio bajo.



ACTIVIDADES DESARROLLADAS

3.1 MOTIVO DE LA PASANTIA

Con el crecimiento de la tecnología en nuestro país y el mundo, cada día nos vemos obligados a mejorar todos los servicios que son necesarios en el diario vivir y es por este motivo que el que una persona particular no esté exento de conocer a través del Internet todo lo que ocurre fuera de nuestras fronteras, conectados a través de una red podemos comunicarnos con el mundo entero y compartir conocimientos entre distintas razas y costumbres.

También a través de las redes de internet podemos realizar transacciones, compras, descargar un sinnúmero de manuales y libros y muchas cosas más que se puede realizar a través de este medio de comunicación.

El hecho de que estemos avanzando en tecnología nos hace desear y pensar en la superación personal y para estar más actualizados todos deberíamos contar con un servicio adecuado a través de las Redes de Internet.

3.2.- OBJETIVO DE LA PASANTIA

El objetivo principal de la pasantía es brindar el apoyo necesario a la Institución con todos los conocimientos adquiridos en la Universidad, tanto física como científicamente y al mismo tiempo aprender el trabajo que se desarrolla en un empresa, ya que es muy distinto realizar una práctica universitaria a una práctica en una institución, porque en la primera se pueden cometer errores que luego el docente los corrige e instruye al estudiante, pero en una empresa tenemos que tener cero por ciento de error para que el cliente final quede satisfecho con nuestro trabajo y así demostrar a la institución que nos contrata nuestra capacidad tecnológica.

3.3.- ASPECTOS LABORALES

Ya que nuestro trabajo es de mayor porcentaje manual no contábamos con un plan semanal de actividades pero esto no exime a que en la empresa realizáramos una vez por semana una reunión grupal para evaluar nuestro trabajo y como mejorar en caso de que alguno de los trabajos nos haya costado más tiempo de lo común al ponerlo en funcionamiento.

También se realizaron reuniones juntamente con los ingenieros a cargo antes de empezar cada trabajo (en construcciones nuevas) para darnos algunos detalles de la instalación y en especial del cableado estructurado para no dañar en lo posible las estructuras de cada institución o domicilio particular donde se realizaba la instalación del servicio de internet.

Cuando se realiza una instalación pequeña no es necesario tener un plano de distribución de cableado sino solamente un poco de criterio para que la instalación se vea lo más estético posible (me refiero a instalaciones de 2 o 5 puntos de internet). Pero ya cuando realizamos la instalación en un edificio por ejemplo, como el edificio Casanovas donde instalamos más de 25 puntos de internet, debemos de contar mínimamente con un plano de direccionamiento para saber el material que emplearemos y la capacidad que tendrá cada switch, la topología que utilizaremos y los lugares donde conectaremos nuestros switch's. También en lo posible deberíamos de contar con el plano eléctrico para conocer si se puede emplear algunos ductos que se dejaron en inicio de la construcción. Y obviamente conocer toda la terminología y simbología que se utiliza para instalar una Red de Internet.

3.4.- SIMBOLOGIA

En toda instalación es importante conocer toda la simbología y la terminología que cubre el campo de las redes de internet, así como en electrónica utilizamos distintos tipos de símbolos para identificar los elementos y componentes, de la misma forma en las Redes de Internet se utilizan términos y símbolos que son necesarios conocerlos al realizar una instalación.

Estos tipos de símbolos, por lo general, vienen en un plano de instalación muy similar al que se utiliza para la conexión eléctrica situado en el plano general de construcción de cualquier entidad. Para esto lo primero que realizamos es la revisión de estos planos, una vez que el cliente haya confirmado que desea que se haga el trabajo en su empresa. Es muy importante la verificación de estos planos para saber la ubicación de los puntos donde se dejaran listos las cajas para el keystone en donde finalizado el trabajo se conectaran los conectores RJ45 de cada host. Cuando tenemos una construcción nueva son los encargados de la parte eléctrica en dejarnos los puntos listos para el cableado y en algunos casos solamente se debe extender un par de cable ductos para llegar a la estación de trabajo.

Los símbolos básicos que debemos identificar en un plano de instalación de una red de internet son:

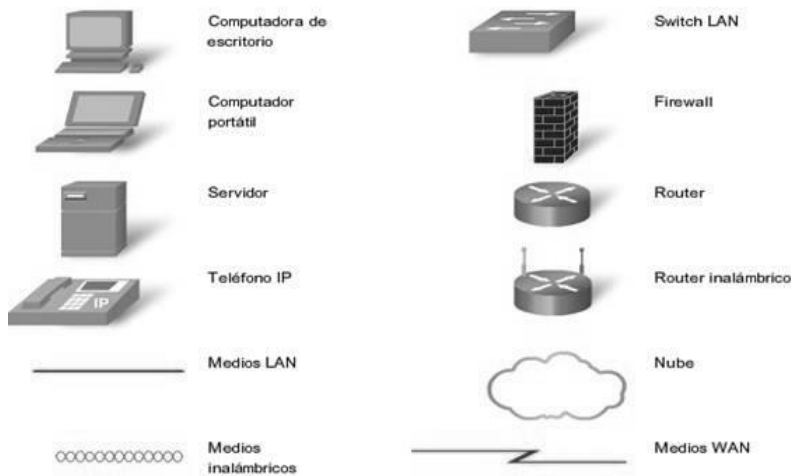


Figura 3.1 Simbología para la instalación de una red de internet

La figura muestra la representación gráfica de los elementos como se los ve en un plano de direccionamiento y esto nos da una idea exacta de cómo debemos realizar el trabajo de instalación de una red con cableado estructurado.

3.5.- PLANOS DE DIRECCIONAMIENTO Y DE DISTRIBUCION

A continuación se muestra como se ve un plano de direccionamiento de datos antes de realizar la instalación.

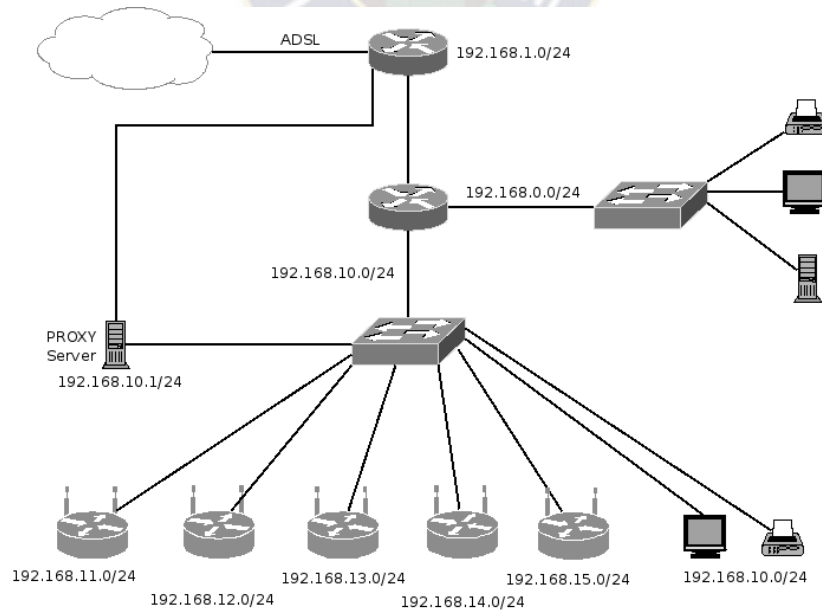


Figura 3.2 Plano general de direccionamiento

Como observamos en este caso en particular sería un diseño que se utilizó para una fábrica en donde deberíamos de instalar más de 70 equipos de computación todos ellos conectados a la red de internet. Este es el primer plano que llega a nuestras manos donde nos indica que utilizaremos 2 routers, 2 switches y 5 routers inalámbricos, también el usuario contara con dos servidores, dos impresoras en red y dos computadoras centrales que estarán monitoreando el tráfico de datos de toda la fábrica, cabe recalcar que este es un plano básico ya que posteriormente a petición del cliente se puede extender a más puntos y brindar más servicios como ser el hecho de tener otros periféricos que quieran compartir como impresoras, escáner, etc.. Los números IP colocados debajo de cada dispositivo nos indica la cantidad de máquinas máximo que deber de conectarse a ese dispositivo por ejemplo el número 192.168.11.0/24 nos indica que los tres primeros números son la dirección a la que responderá ese router y el ultimo 0/24 nos indica la cantidad de segmentos que se pueden derivar de este servidor para obtener buena eficiencia y así evitar pérdidas.

Es muy importante conocer la distribución de los números IP ya que con estos podemos conocer cuántos equipos conectaremos a un switch y de esta manera realizar el pedido a almacenes para la distribución exacta del material sin tener pérdidas en cuanto a material se refiere,

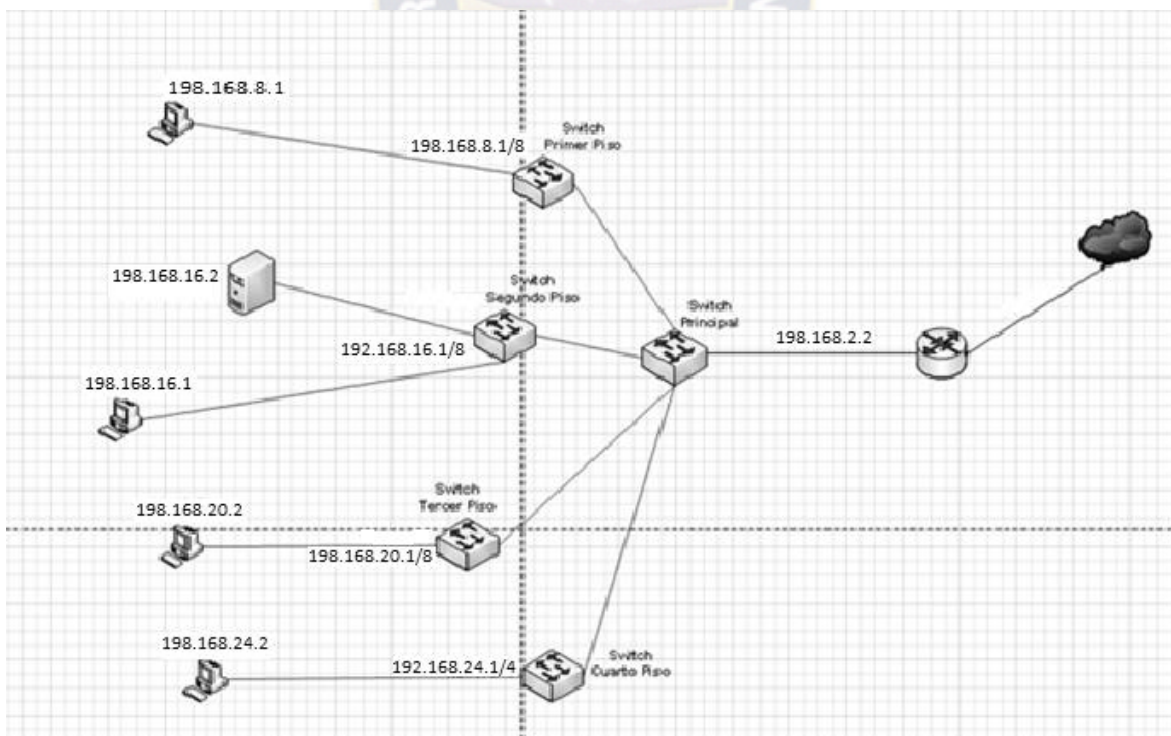


Figura 3.3 Otra forma de ver el plano de direccionamiento

Una vez visto el plano de direccionamiento observamos el tipo de entubado que tendremos en este lugar. Si la instalación es en una construcción nueva el Ingeniero eléctrico es el que se encarga de realizar el diseño del entubado y posicionamiento de los keystone o rosetas RJ45, el entubado es completamente interno (o sea por dentro de las paredes) y nuestro trabajo se reduce solamente a guiar los cables por el entubado que dejaron para la red de internet.

Si la instalación es en una construcción ya acabada entonces el ingeniero eléctrico realiza un nuevo plano indicándonos por donde debemos realizar el empotrado de los ductos. Los planos eléctricos para la conexión de una red de computadoras se ven así.

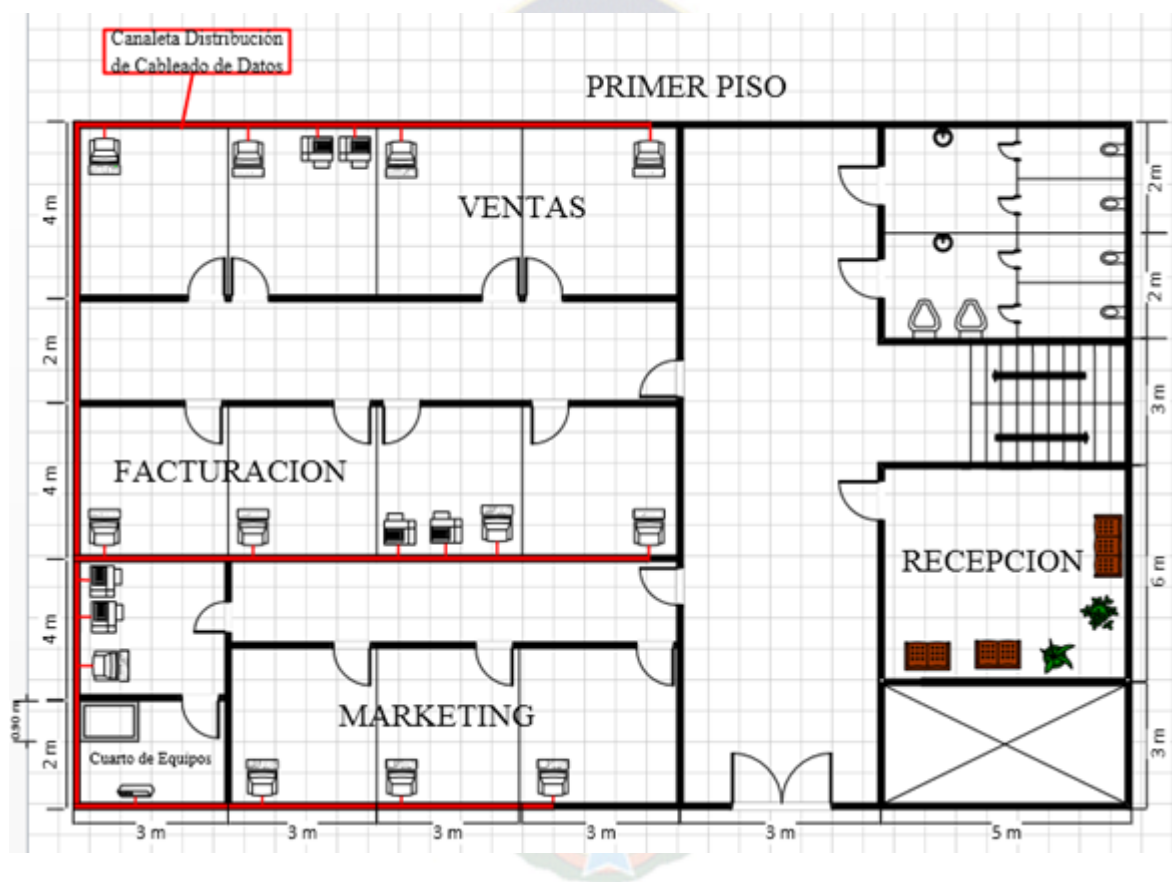


Figura 3.4 Plano de distribución de cableado para una oficina

La figura anterior nos muestra cómo debemos realizar el entubado con cable ductos en caso de que la institución solicitante no cuente con un entubado previo. Para esto si es necesario se debe realizar dicho entubado por el entretecho y en algunos casos se tiene que picar las paredes para colocar un ducto y así no perder la estética de la oficina ya que hay algunos clientes que no les gusta ver cables sueltos o tubos que vayan por sus paredes, también es muy importante cuidar de no ensuciar la oficina cuando se utilice por ejemplo un taladro,

por eso es recomendable realizar los trabajos fuera del horario de oficina ya sea por las noches o en fines de semana. A continuación otro ejemplo de cómo tienen que ir los ductos por el entretecho y las paredes para cuidar la estética.

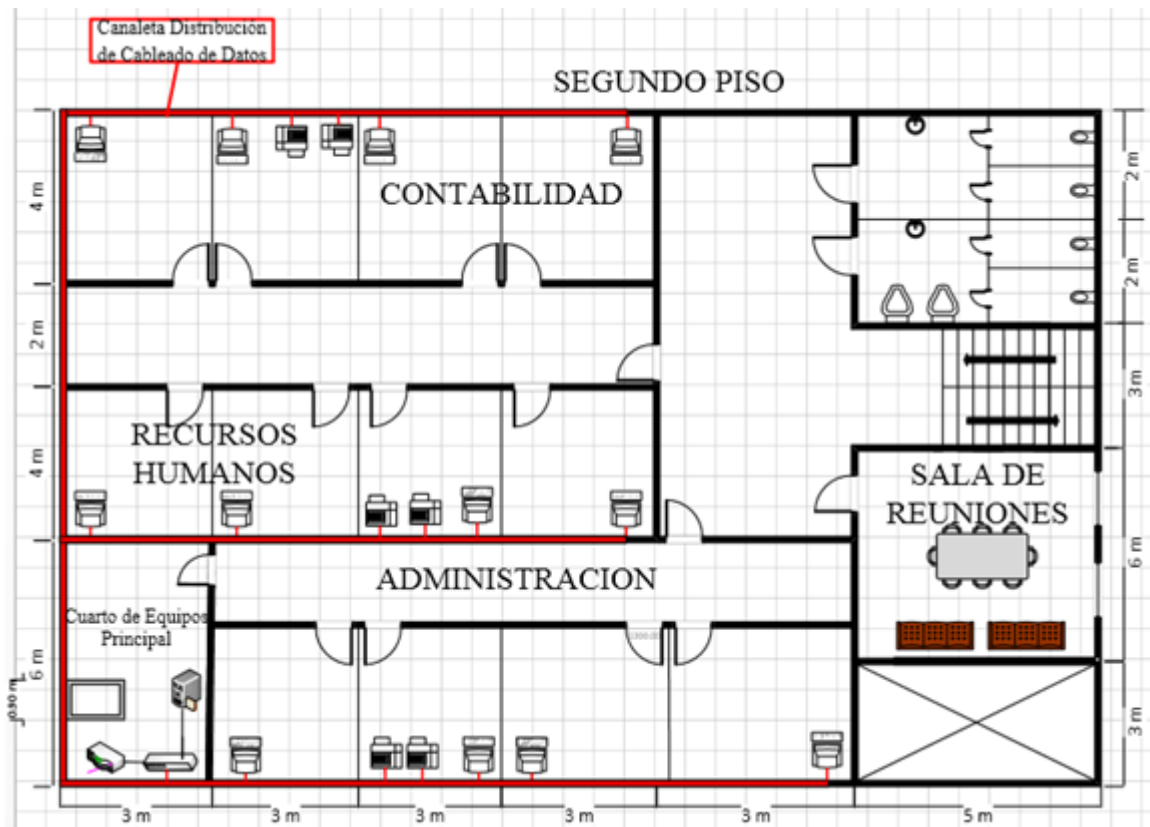


Figura 3.5 Plano del cableado en otro piso

Conociendo ya los lugares en donde se implementaran los equipos entonces procedemos al cableado estructurado de la red.

3.6.- CABLEADO ESTRUCTURADO

Otra de las normas que debemos seguir en toda instalación de una red de internet es la forma en que realizaremos el cableado, en esta parte tomaremos en cuenta los requerimientos del cliente acerca de qué tipo de servicios brindara cada host a la empresa o domicilio particular, en cuanto a seguridad y eficiencia de este. Si bien lo común es que se brinde un servicio de manera convencional existen ocasiones en que el requerimiento es detallado y se debe tomar en cuenta las características de las redes como se vio en los capítulos anteriores.

Hoy en día es muy común ver servicios de internet en buses, restaurantes, y muchos negocios los cuales responden a las normas de instalación que se vio en este informe. Debemos conocer las dimensiones de los cables de punto a punto, el espesor que tiene este, en caso de que varios cables (por lo general UTP) pasen por un mismo ducto, también buscar el mejor lugar para que estéticamente toda la conexión se vea lo más limpia posible.

Cuando el cableado se complica (es decir tiene que pasar por un entretecho, terraza, ductos de ventilación, etc.) se debe tomar en cuenta las distancias y normas de seguridad para evitar pérdidas. A veces cuando el cable tiene que estar expuesto a factores climatológicos o lugares húmedos usamos un cable UTP blindado cat6 que está diseñado especialmente para este tipo de instalaciones el cual cuenta con un recubierto capaz de resistir este tipo de factores.

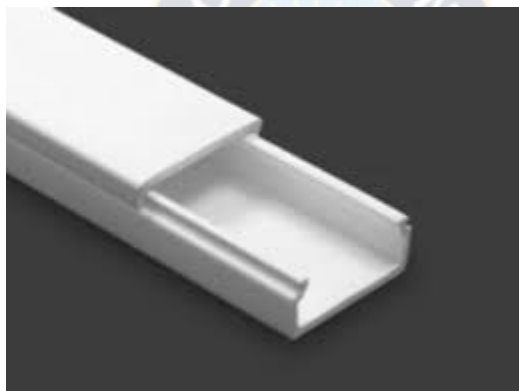


Figura 3.6 Ducto para cableado estructurado de red dentro de un ambiente

En interiores usamos los ductos cuadrados y buscamos los lugares menos visibles en lo posible para no dañar el ambiente y de esta forma también brindar comodidad al cliente. Cuando se trata solamente de compartir información entre distintos host (una intranet por ejemplo), no es necesario instalar equipos muy caros a no ser por requerimiento, con un HUB bastara ya que nuestros equipos no estarán expuestos a que nuestra información sea vista desde las redes y de esta forma también podemos compartir recursos como impresoras, faxes, etc..

3.7.- ARMADO DE LAS ROSETAS

También llamados keystone o cajas de sobreponer, es muy importante tener cuidado con el armado de estas cajas ya que debemos respetar la norma con que lo estamos armando (Norma A o B), estas cajas vienen siempre con indicaciones de cómo debemos realizar la

conexión y para esto utilizamos un ponchador de red el cual es una herramienta de mucha utilidad la que nos ayuda a que los cables estén bien sujetos.

Debemos tomar también en cuenta que en el momento del armado hay que evitar que los cables pierdan el trenzado ya que esto puede significar pérdida de información, colocando cada cable en su lugar con la mayor delicadeza y seguridad posible para evitar futuros reclamos.



Figura 3.7 Ponchador de red



Figura 3.8 instalación de los cables en el keystone



Figura 3.9 Distintos modelos de Keystone's

3.8.- CRIMPADO DE LOS CABLES

Una vez que ya realizamos el cableado estructurado y el armado de los keystone's procedemos a realizar el crimpado de los cables con conectores RJ45 los cuales debemos realizarlos según la norma que hayamos optado por colocar ya sea la norma "A" que sería blanco verde, verde, blanco naranja, azul, blanco azul, naranja, blanco café, café; o la norma "B" que es la más común con los colores blanco naranja, naranja, blanco verde, azul, blanco azul, verde, blanco café, café, y cualquiera que se use también debe de usarse en el Patch Panel y el keystone. Para esto y teniendo cuidado de no malograr los cables y sin tratar de perder el trenzado enfilamos los cables según norma y los colocamos en un conector RJ45,

seguidamente usamos un alicate de red con el que presionaremos con fuerza para que el conector y cable queden totalmente fusionados.



Figura 3.10 Crimpado de un conector RJ45 con norma A o B

3.9.- INSTALACION DE LOS ENLACES USUARIO INTERNET

Como habíamos visto anteriormente, los dispositivos de red que utilizamos para conectarnos a internet y para poder comunicarnos con otros equipos son los Routers, Switch, Hub y las tarjetas de red que debería contar cada equipo necesariamente. Aquí tomamos en cuenta el tipo de servicio requerido por el usuario para instalar el equipo correcto, es importante conocer los conceptos y definiciones de los modelos OSI y TCP IP en la instalación.

También el hecho de colocar el enlace adecuado nos permitirá tener mayor eficiencia el momento de querer compartir o recibir información, por ejemplo si nuestro requerimiento es la conexión de internet para un domicilio particular, en donde se conectaran hasta 5 equipos de computación, nuestro enlace debería de ser un HUB el cual trabaja en la capa 1 del modelo OSI ya que este dispositivo recibe datos procedentes de una computadora y los transmite a las demás compartiendo la información de manera equitativa a los 5 equipos. Pero en la actualidad los HUB`s ya se encuentran extintos así que utilizamos solamente Switch`s para realizar conexiones pequeñas.

Por otra parte si tenemos que brindar servicio a alguna pequeña empresa u oficina en donde tendremos varios host es necesario colocar un switch, el switch es un aparato muy semejante al HUB, pero tiene una gran diferencia: Los datos provenientes de la computadora de origen solamente son enviados a la computadora de destino. Esto se debe

a que los switches crean una especie de canal de comunicación exclusiva entre el origen y el destino. De esta forma, la red no queda "limitada" a una única computadora en el envío de información. Y para edificios o grandes corporaciones debemos de instalar un router, el cual es un dispositivo utilizado en redes de mayor capacidad, más "inteligente" que el switch, pues, además de cumplir la misma función, también tiene la capacidad de escoger la mejor ruta que un determinado paquete de datos debe seguir para llegar a su destino. Es como si la red fuera una ciudad grande y el router elige el camino más corto y menos congestionado, como vimos estos dispositivos trabajan en las capas 1 del modelo TCP/IP, el switch se encargara de enviar la información al host solamente el momento que lo solicite y el Router buscara y designara al host el tipo de información requerida. Otro aspecto que debemos tomar en cuenta es el hecho de la velocidad, actualmente contamos con varios servidores de internet los cuales brindan al usuario diferentes capacidades de transmisión de datos en cuanto a internet se refiere, en esta parte ya dependerá del usuario según su requerimiento y su disposición económica el tipo de servicio que comprara de estos servidores. Una vez que el servicio llega a nuestra entrada principal es importante buscar un lugar adecuado donde podamos tener el control y poder realizar cambios a los dispositivos de comunicación, (un RACK seria lo adecuado cuando tenemos más de 15 puntos interconectados), se debe tomar muy en cuenta la organización de los cables colocando nombres o números que nos indiquen cual es el tipo de usuario que requiere nuestra ayuda y también para realizar un mantenimiento adecuado, rápido y sin complicaciones.

3.10.- CONFIGURACION

Según la compañía que nos brinda el servicio será importante conocer los números IP de configuración los cuales tienen que ser ingresados correctamente a cada host, estos números vienen configurados de la siguiente forma:

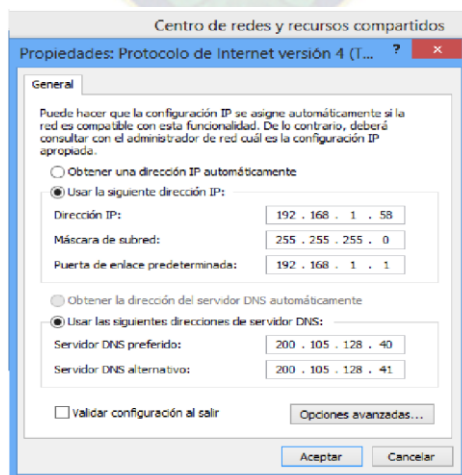


Fig. 3.11 Como ingresar los números IP

En toda pc de escritorio se encuentran las propiedades de la tarjeta de red en donde ingresamos estos números, el primero donde nos indica Dirección IP es por lo general donde designamos un número al host. Los números 192.168.1.X son casi siempre inamovibles, la "X" es el número designado al host que varía desde 2 a 254.

La máscara de subred recibe la configuración 255.255.255.0 el cual nos indica que los 3 primeros números de la dirección IP no varían en toda la red y de esta forma la búsqueda de información y de algún usuario se hace más sencilla.

La puerta de enlace predeterminada siempre va configurada con 1 para el HUB o Switch porque el primer dispositivo con el que tendremos salida al exterior, como en todo lugar donde se haga una instalación de internet el primer dispositivo siempre lleva como número IP el número 1 dependerá del número MAC que es único en todo el mundo para que el dispositivo no tenga conflicto con algún otro por repetición de número.

Los servidores DNS preferido y el alternativo son los que nos brindan los proveedores de servicios de internet ya que cada una cuenta con distintos servidores los cuales almacenan la información de las páginas más solicitadas.

Estos números denominados números IP's nos lo proporciona la empresa que nos brindara el servicio de internet y todos los usuarios deben estar configurados de la misma forma exceptuando la dirección IP la cual variara para cada usuario.

En caso de que tengamos que configurar una red inalámbrica debemos seguir los siguientes pasos

- Abrimos el navegador WEB e ingresamos la dirección IP del dispositivo en la barra de direcciones (por defecto este es 192.168.1.1 , 192.168.0.1 o 192.168.0.0 según el tipo de fabricante)
- Ingresamos el nombre de usuario y contraseña en la página de inicio de sesión, por defecto este viene con el seudónimo de "ADMINISTRADOR".
- Buscamos Wireless (inalámbrico) y configuramos los parámetros básicos en donde también debemos introducir los números IP provistos por nuestro proveedor de servicio.

Cabe recalcar que según el fabricante la configuración puede variar en cuanto a plataforma pero la sintaxis de configuración en un router inalámbrico es el mismo.

Por otra parte también debemos configurar los servicios para poder compartir carpetas, impresoras y otros recursos que se solicite para una oficina o un domicilio particular.

Tomemos como ejemplo que trabajamos con un sistema operativo Windows 7 u 8 estos deberían ser los pasos a seguir.

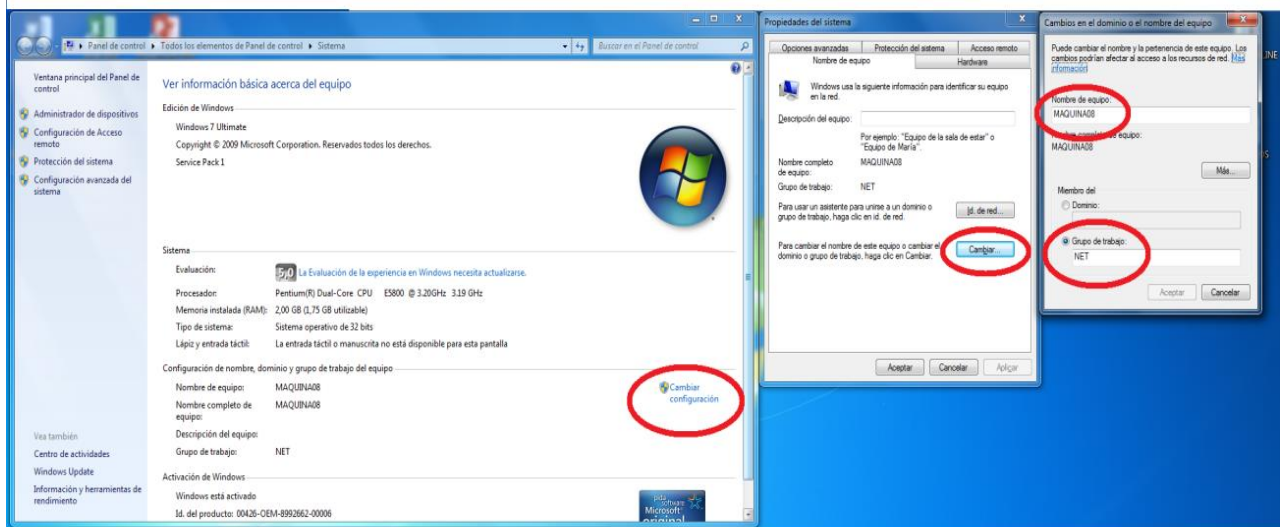


Figura 3.12 Configuración del nombre y grupo de trabajo para la red

Lo primero que debemos hacer es configurar el nombre del equipo y el nombre del grupo de trabajo, esto es muy importante ya que todos los equipos que compartirán recursos en la red deben pertenecer al mismo grupo de trabajo y se debe poder distinguirlos según el lugar o sección donde trabaja, por ejemplo en un domicilio podemos colocar los nombres de los usuarios para poder distinguirlos como Anita, Jorge, mamá, etc., pero si se trata de realizar la configuración en una oficina entonces es importante distinguirlos por sus cargos como Contador, Secretaria, Sistemas, etc.. En algunas instituciones todavía se utilizan equipos de computación un tanto obsoletos es decir equipos Pentium III o Pentium IV de primera generación en los cuales se hace un poco más dificultoso realizar la configuración de usuarios pero no imposible, en este tipo de máquinas es necesario reiniciar el equipo cuantas veces hayamos realizado alguna configuración para que el sistema operativo pueda reconocer y aceptar todos los cambios realizados.

Una vez realizada esta configuración de identificación procedemos a configurar la red para esto nos vamos al menú inicio y escribimos redes en el campo de búsqueda de abajo y pinchamos en el enlace Centro de redes y recursos compartidos.

En la pestaña "cambiar la configuración" elegimos la opción configurar una nueva conexión de red y seguidamente elegimos el tipo de red que vamos a utilizar ya sea doméstica o una red pública y seguimos los pasos de configuración.

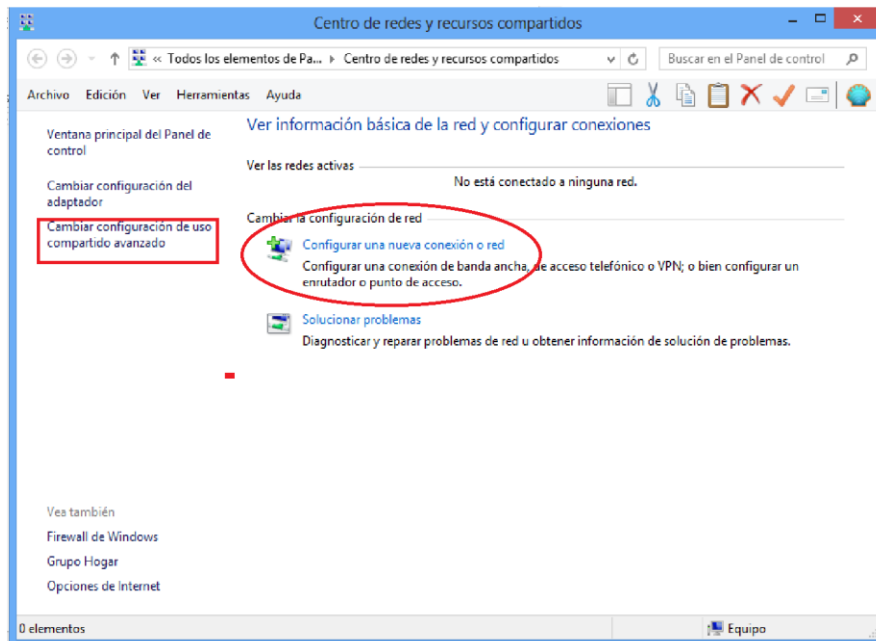


Figura 3.13 Configuración de la red

Esta es la nueva pantalla que aparecerá donde debemos elegir una opción de conexión que en nuestro caso será la primera porque deseamos conectarnos a internet aunque en algunas ocasiones elegimos las otras opciones por ejemplo para conectarse a un nuevo enrutador con un numero de IP distinto o para conectarse a una red inalámbrica.

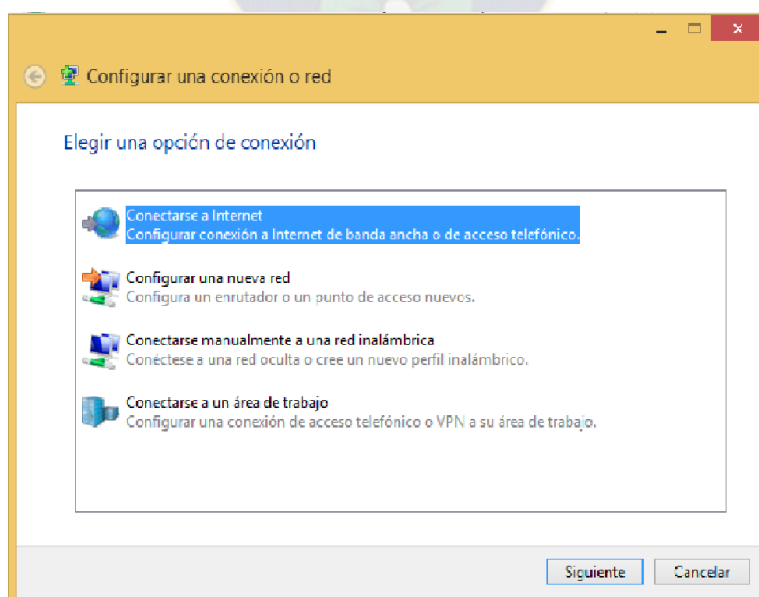


Figura 3.14 Opciones para conexión de red

Seguidamente nos aparece el puerto por el que vamos a conectarnos que en nuestro caso si es una conexión a internet será el puerto PPPoE.

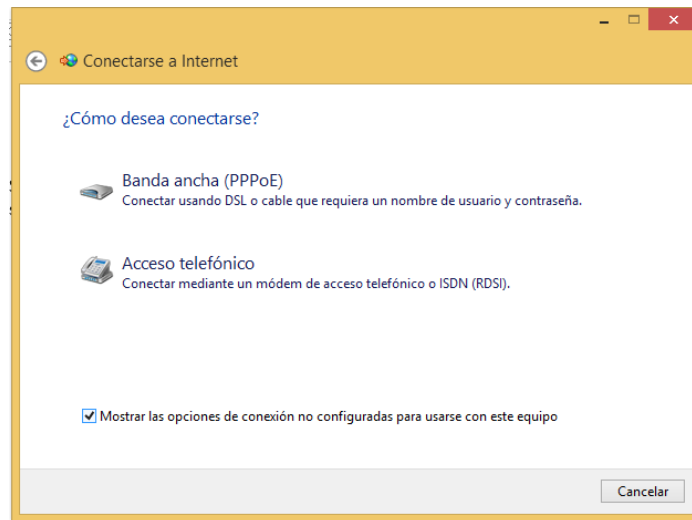


Figura 3.15 Selección de tipo de conexión

Por último nos pide colocar los datos de usuario y una contraseña para tener acceso único a nuestra red de internet.

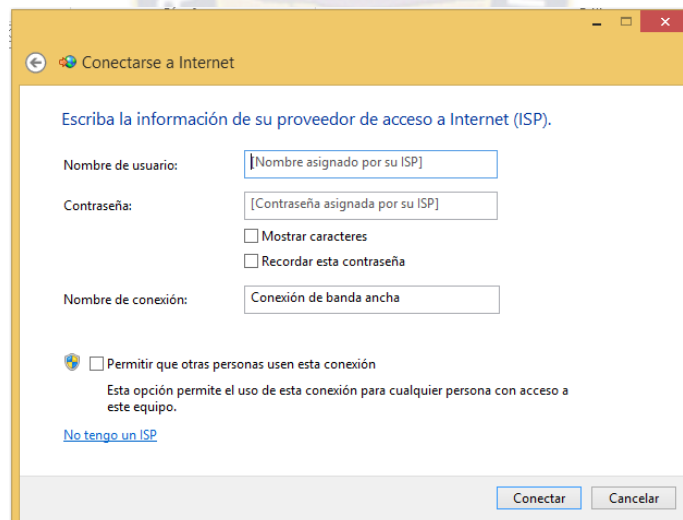


Figura 3.16 Información del usuario

Como observamos estos serían los pasos básicos en un sistema operativo Windows 7 o Windows 8, y aunque Windows XP difiere un poco de los pasos que menciono y muestro en las figuras, la sintaxis de la configuración es muy similar con la única diferencia que si nos equivocamos en algún paso debemos volver a reiniciar el equipo luego de la corrección.

3.11.- MUESTRA DE TRABAJOS REALIZADOS

Las primeras dos semanas fueron de ambientación y conocimiento acerca de cómo se realizaba el trabajo, como se realiza el pedido de materiales y el funcionamiento de la Empresa así también la relación personal con los compañeros y el personal jerárquico. Los primeros trabajos que se realizaron fueron en el Edificio Casanovas instalando una red de internet para 25 copropietarios del edificio, corrigiendo todos los errores que se habían cometido en la anterior conexión. A continuación se muestra algunas fotos tomadas de la instalación de red que se hizo antes que la empresa Verda corrija estos errores.



Figura 3.17 Cables UTP's colgados y ductos rotos sin protección

En la figura se muestra dos errores comunes que se cometen en la instalación de las redes en la primera se puede ver el cableado que se hizo sin ductos y sin tomar en cuenta los factores climatológicos que afectarían a los cables



Figura 3.18 Fotos luego de las correcciones

En la figura anterior se ve que dichos cables ya están dentro del ducto blanco que se ve al fondo, se pudo observar primero que se colocaron ductos pero sin las medidas de seguridad necesarias para este ambiente ya que nuevamente los factores climatológicos se

encargaron de deteriorar totalmente los ductos que duraron aproximadamente 2 años. Cuando nosotros hicimos las correcciones necesarias todo el cableado entro a un solo ducto de alta resistencia al sol y debidamente impermeabilizado para evitar que el agua ocasionado por las lluvias entren en los ductos, una vez realizado este trabajo se pasaron los claves de manera conjunta para luego terminar todo en un pequeño RACK especialmente diseñado para este sitio y que nos ayudó a distribuir los puntos para un mejor control de la red.

En las figuras siguientes observamos cómo se dañaron los cables hasta el punto de verlos totalmente sin sus fundas y partidos y como colocaron acoples provisionales para corregir los cables partidos. La mala estética de este cableado y la falta de seguridad al realizar la conexión anterior fueron los que ocasionaron que los copropietarios del edificio tengan constantes quejas por las fallas en el servicio y los cortes cotidianos.



Figura 3.19 Cables pelados sin protección y enredados

En las siguientes figuras podemos observar los errores ya corregidos de las anteriores fotografías con sus respectivos ductos, y como podemos ver ya no existen más cables de red (UTP) sueltos, pero todavía nos dimos cuenta que otras empresas de renombre como ENTEL y COTEL u otros siguen cometiendo los errores comunes de dejar cables a la intemperie sueltos y sin ninguna protección.



Figura 3.20 Cables puestos en ductos correctamente

En las siguientes figuras observamos el momento en el que estábamos colocando la caja de distribución para el RACK la cual tiene que ser impermeable y totalmente cubierta ya que se encuentra en la parte de la terraza para que las constantes lluvias y el radiante sol no maltrate el RACK y el Patch Panel, también se puede ver el Patch Panel ya implementado en el RACK todo enumerado y con la estética y las condiciones de seguridad necesarias para este tipo de conexión.



Figura 3.21 Colocando caja del Patch Panel y en la derecha la caja ya terminada

También se desarrolló trabajos de telefonía IP con centrales telefónicas, uno de los trabajos importantes que se hizo fue en la fábrica la Estrella. Esta fábrica ya contaba con una central telefónica muy antigua y sus gerentes decidieron cambiar a la tecnología IP adquiriendo equipos de última generación. En la verificación de las instalaciones se comprobó el desorden que tenían en el cuarto de controles, teniendo muchos cables que ni siquiera utilizaban. Uno de los aspectos buenos de esta fábrica es que cuenta con una red de fibra óptica por donde también se pueden conectar con sus otras sucursales.

En esta fábrica se volvió a realizar el cableado estructurado de muchos puntos ya que en anteriores conexiones no se tomó en cuenta la telefonía IP y en otras solo fue necesario instalar un switch aprovechando que había internet es ese punto. Por la complejidad y tamaño de la fábrica se trabajó en distintos horarios incluyendo fines de semana y noches para no perjudicar así la producción de esta gran fábrica que produce para el país muchos productos que consumimos diariamente.

Algunos problemas que se tuvo en la instalación de la nueva central telefónica fue en la ubicación de los puntos que van desde el usuario al panel central ya que la conexión fue realizada en dos partes por la distancia (aprox. 200m) y la cantidad de usuarios (más de 60), los cuales quedaron muy satisfechos luego de ver sus nuevos teléfonos con más funciones que las anteriores, ya que solo podían recibir llamadas transferidas desde un operador, sin embargo ahora pueden transferirse llamadas entre usuarios las veces que quieran, realizar conferencias, múltiples conexiones y hasta incluso video conferencias a larga distancia.

El producto que se utilizó en la Estrella fue de la marca AASTRA de Industria Canadiense y como es un producto nuevo aquí en la ciudad los representantes enviaron a un técnico Colombiano especializado en este producto para que nos brinde el asesoramiento técnico en cuanto a la programación de los teléfonos del cual aprendimos mucho por la amplia experiencia que tenía este técnico, uno de los tropiezos que tuvimos fue en la configuración de la VLAN (redes virtuales), ya que aquí no estamos acostumbrados a trabajar con este tipo de redes.

En las siguientes fotos se muestra un poco del trabajo realizado en la Fábrica la Estrella. Las primeras fotos nos muestran los equipos que instalamos en esta Fábrica una centralita IP PBX de la compañía AASTRA como se puede observar tiene 8 puertos de entrada para línea analógica y 8 puertos de salida para telefonía IP los cuales pueden ser derivados a más canales por medio de Switches, esta centralita facilita mucho el trabajo y economiza los costos en telefonía lo cual significa mucho para esta empresa ya que cuenta con muchos departamentos y sucursales en toda la ciudad.



Figura 3.22 Centralita IP PBX

En las siguientes figuras mostramos los teléfonos IP que utilizamos para reemplazar a los antiguos convencionales, como se observa este teléfono tiene una pantalla donde se visualiza los datos del usuario como su número de identificación, la fecha y su nombre.



Figura 3.23 Teléfono IP para operador y teléfono para usuario

Este teléfono también es capaz de mostrar en su display los datos de las llamadas entrantes o sea que nos visualiza el nombre y el número del usuario que se intenta comunicar con este otro punto y todo mediante el sistema de telefonía de voz sobre IP.

El teléfono IP de la operadora tiene más funciones y un display mucho más amplio en el que se puede visualizar toda la agenda de los usuarios que pertenecen a esta central, entre sus otras funciones este teléfono de operador puede retener las llamadas cuando el operador este ocupado y colocar música de espera o colocar mensajes de derivación de llamadas ingresando números de internos.

A continuación se muestra nuevamente los errores comúnmente cometidos por técnicos con poca experiencia dejando cables colgados en completo desorden haciendo complicado el mantenimiento en caso de que alguno de los puntos llegase a tener algún tipo de problema, y no solamente los cables UTP sino que también los cables de energía que con una mala manipulación hasta puede llegar a ser peligroso si ocasionan algún corte.

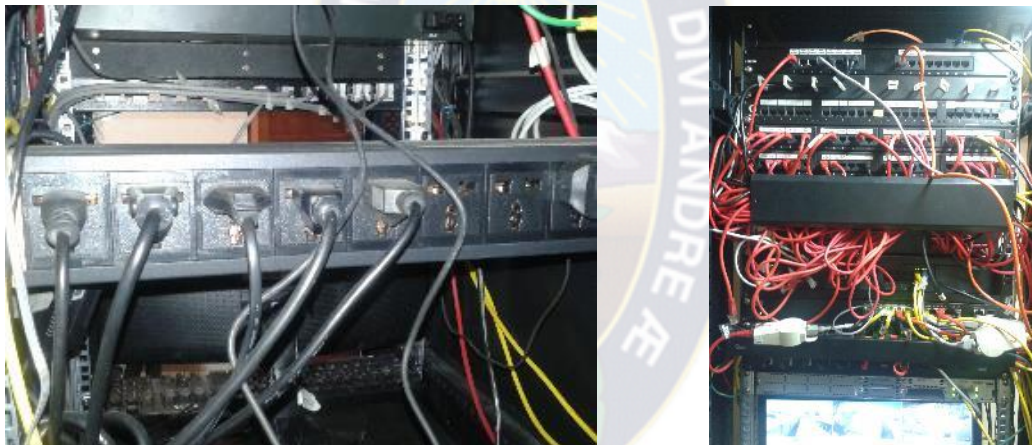


Figura 3.24 Tomas de corriente sin protección y Rack totalmente desorganizado

Y ahora podemos ver las dos anteriores fotografías pero ya corregidas, todos los cables UTP peinados y colocados en regletas y los cables de toma de corriente aislados de todo peligro. En esta parte se tuvo mucho cuidado en la instalación de los cables ya que un error por cruce de cables nos significaría el doble o hasta el triple del trabajo que normalmente se realiza. Es muy importante poder hacer el seguimiento punto a punto, en caso de que las distancias sean muy largas como en esta fábrica es necesario comunicarse mediante woki tokies para poder informar al otro punto de conexión como se va realizando el trabajo y así evitar que haya confusiones. También se debe ir testeando los cables para asegurarse que no haya error en la conexión.



Figura 3.25 Correcciones hechas al cableado de las dos anteriores figuras

Al hacer las correcciones se tomó en cuenta también las conexiones a tierra que no estaban conectadas y se realizó un mantenimiento general en el RACK y luego del orden se pudo liberar muchos puntos que estaban sin ninguna utilidad.

Por último se muestra la foto del personal que trabaja en el departamento de redes y telefonía juntamente con el experto Colombiano en telefonía IP del cual aprendimos mucho por la experiencia que tiene este profesional. Esperamos nuevamente contar con su apoyo y la de otros profesionales ya que la empresa se comprometió a seguir contribuyendo mandando a nuestro país profesionales capacitados para que puedan enseñarnos más todavía.



Figura 3.26 Personal del área de redes de internet y telefonía

CONCLUSIONES

4.1.- CONCLUSIONES

En los más de 4 meses que se realizó la pasantía se logró realizar el objetivo principal que era el de contribuir con los conocimientos adquiridos en la universidad a las instituciones que requieren nuestros servicios, organizándonos contribuimos con muchos conocimientos para poder realizar los trabajos designados en tiempos más cortos de los que eventualmente realizaba la empresa, también se sugirió la compra de materiales e instrumentos que contribuyeron a un mejor desempeño laboral.

Por otra parte también se aprendió bastante acerca de temas administrativos, ya que esta parte aunque parezca irrelevante es muy necesaria en el desarrollo de cualquier actividad, desde el momento en que se solicita materiales en forma escrita hasta cuando se entrega un informe final. La experiencia adquirida en estos meses de trabajo fue memorable y entre las principales es que se debe tener cuidado minucioso en realizar el cableado estructurado y las conexiones, siguiendo y respetando todas las normas técnicas que se tiene al realizar este tipo de instalaciones.

También es importante el uso del material correcto ya que sin este no tendríamos la calidad y el terminado adecuado que deberíamos ver al finalizar nuestro trabajo. También se pudo evidenciar la importancia del trabajo grupal ya que todos contribuyen con distintos conocimientos que adquirieron para que se haga un mejor trabajo. El respeto a nuestros superiores, la coordinación y las sugerencias que puede hacer el personal, para un mejor desarrollo de nuestras actividades, es también de vital importancia ya que son indispensables para facilitarnos el trabajo y de esta manera brindar al usuario final del servicio la comodidad necesaria para poder realizar sus actividades diarias.

4.2.- RECOMENDACIONES

Para todo trabajo es siempre importante tomar en cuenta todos los detalles que hacen que una instalación, no solamente de Internet, cumpla bien con su cometido, se debe seguir siempre las normas establecidas para evitar cualquier tipo de pérdidas en las comunicaciones y también las normas de seguridad industrial para evitar cualquier tipo de accidentes.

En cuanto a lo técnico se deben tomar las siguientes precauciones:

- Evitar que los cables de red estén cerca de los cables de poder (corriente eléctrica) no deben ir en la misma canalización.

- No producir dobleces en los cables mayores a 90 grados
- Si tenemos que atar un grupo de cables juntos, no se los debe ajustar en exceso, está bien atarlos firmemente pero no hacerlo de tal forma que produzca deformaciones en los cables, su cobertura o trenzado
- Mantenga los cables alejados de dispositivos que puedan introducir ruido en los mismos como por ejemplo: fotocopiadoras, equipos de calefacción eléctrica, altavoces, impresoras, equipos de TV, luces fluorescentes, equipos de soldadura, hornos microondas, ventiladores, ascensores, motores, hornos eléctricos, secadoras, lavadoras, etc.
- Evitar halar los cables UTP
- No colocar cableado UTP en los exteriores de los edificios.
- Utilizar el material correcto cuando sea necesario el cableado en exteriores o cableado subterráneo.
- Realizar un estudio del material a utilizar según los requerimientos del cliente ya que podemos ocasionar pérdidas económicas a la empresa si solicitamos el material incorrecto.

En cuanto a lo personal según la experiencia vivida se recomienda:

- Realizar siempre reuniones grupales para evitar trabajos dobles e innecesarios.
- Coordinar con los compañeros de trabajo en cuanto a la designación de las actividades que se realizaran en el día y brindar informes a la finalización de este.
- Utilizar siempre equipos de protección recomendados por seguridad industrial.
- Evitar en lo posible riesgos innecesarios con la excusa de aligerar el trabajo, en especial cuando se trabaja en exteriores y paredes a gran altura, siempre habrá una solución para brindar seguridad al técnico.

4.3.- PROPUESTA

Luego de haber tenido esta grata experiencia en el campo laboral solo me queda dar algunas sugerencias a la Empresa que me brindo su confianza y a la Universidad a la cual le debo mis conocimientos.

A la Empresa Veralda, si bien la Empresa es más dedicada al ámbito de la construcción, le sugerimos poder descentralizar el área de Electrónica con una nueva administración y así de esta manera facilitar los temas burocráticos y poder brindar un servicio en tiempos más cortos, con nuevos ambientes donde el trabajo sea exclusivamente del área técnica. Por otro parte sugerimos también brindar a los departamentos técnicos el material necesario en cuanto a seguridad industrial se refiere esto a fin de evitar cualquier tipo de accidentes.

A la Facultad de Electrónica y Telecomunicaciones, sugerir que el tema “Redes de Internet” no solamente se lo vea como un capítulo de una materia sino como un programa en sí, ya que el estudio de las redes es muy amplio y en el campo laboral me tocó ver conceptos que

nunca los había visto en la Universidad, también sugerir la implementación de un laboratorio con instrumentos y materiales que ayudarían mucho al estudiante a compenetrar el área de las redes y telefonía.



- ARPANET.-** AGENCIA DE PROYECTOS AVANZADOS DE INVESTIGACION DE RED
- BROADCAST.-** EMISION (PAQUETE DE DATOS QUE SE ENVIA A TODOS LOS NODOS DE RED)
- DARPA.-** AGENCIA DE PROYECTOS AVANZADOS DE INVESTIGACION EN DEFENSA
- DNS.-** DOMAIN NAME SYSTEM (SISTEMA DE NOMBRE DE DOMINIO)
- FTP.-** FILE TRANSFER PROTOCOL (PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS)
- HTTP.-** HYPER TEXT TRANSFER PROTOCOL (PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO).
- HTML.-**HYPERTEXT MARKUP LENGUAJE (LENGUAJE DE MARVAS DE HIPERTEXTO)
- HUB.-** CONCENTRADOR
- IEEE.-** INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
- IRC.-** INTERNET RELAY CHAT (PROTOCOLO DE INTERNET PARA CHAT EN TIEMPO REAL)
- MAC.-** MEDIUM ACCESS CONTROL (CONTROL DE ACCESO AL MEDIO)
- NIC.-** NETWORK INTERFACE CARD (TARJETA DE INTERFAZ DE RED)
- NNTP.-** NETWORK NEWS TRANSPORT PROTOCOL (PROTOCOLO PARA LA TRANSFERENCIA DE NOTICIAS)
- OSI.-** OPEN SYSTEM INTERCONNECTION (SISTEMAS ABIERTOS DE INTERCONEXION)
- PDU.-** PROTOCOL DATE OF UNITY (UNIDADES DE DATOS DE PROTOCOLO)
- POP.-** POST OFFICE PROTOCOL (PROTOCOLO DE OFICINA POSTAL)
- PROXY.-** PROCURADOR
- SMTP.-** SIMPLE MAIL TRANSFER PROTOCOL (PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO)
- TCP.-** TRANSMISION CONTROL PROTOCOL (PROTOCOLO DE CONTROL DE TRANSMISION)
- URL.-** UNIFORM RESOURCE LOCATOR (LOCALIZADOR UNIFORME DE RECURSOS)
- UTP.-** UNSHILDED TWISTED PAIR (PAR TRENZADO SIN APANTALLAR O SIN PROTECCION)
- WI – FI.-** WIRELESS FIDELITY (FEDELIDAD INHALAMBRICA)
- WWW.-** WORLD WIDE WEB (RED INFORMATICA MUNDIAL)

LIBROS CONSULTADOS

- Tecnologías avanzadas de telecomunicaciones. Autor: José Manuel Huidobro
- Sistemas de comunicaciones electrónicas. Autor: Wayne Tomasi
- Redes de computadoras. Autor: Andres S. Tanenbaum
- Redes con Ejemplos. Autores: Barry Press – Marcia Press. 1ª Edición

PAGINAS DE INTERNET CONSULTADAS

- <https://www.wikipedia.org>
- <http://clasedeinternetadonay.blogspot.com/2014/09/primera-clase-de-internet.html> (1)
- <http://www.monografias.com>
- <http://www.adrformacion.com/cursos/wserver082/leccion3/tutorial7.html>
- <http://www2.rhernando.net/modules/tutorials>
- <http://es.slideshare.net/Comdat4/modelo-osi>
- <http://es.ccm.net/contents/282-tcp-ip>
- http://es.slideshare.net/b3rmud3z/protocolos-de-las-capas-del-modelo-osi-13386230?next_slideshow=1
- <http://etb2-conceptos-de-redes.blogspot.com/2011/05/>
- http://www.cad.com.mx/que_es_internet.htm
- <http://www.mastermagazine.info/termino/5330.php>
- <http://es.ccm.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi>
- <http://www.internetmania.net/int0/int55.htm>
- <http://www.informatica-hoy.com.ar/aprender-informatica/>
- <http://es.ccm.net/contents/267-direccion-ip>
- <http://www.xatakaon.com/equipos-de-red/>