UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD TECNICA

CARRERA: ELECTRONICA Y TELECOMUNICACIONES

EXAMEN DE GRADO

TRABAJO DE APLICACIÓN:

“Diseño de una red de área local LAN y WLAN para la Unidad Educativa Región de Murcia “La Primera””

Postulante: Univ. Brayam Boris Zarco Villca

La Paz- Bolivia

Noviembre - 2015

DEDICATORIA

Con mucho cariño principalmente a mis padres que me dieron la vida y han estado conmigo en todo momento. Gracias por todo mama y papa por darme una carrera para mi futuro y por creer en mí, aunque hemos pasado momentos difíciles siempre han estado apoyándome y brindándome todo su amor, por todo esto les agradezco de todo corazón el que estén conmigo a mi lado

AGRADECIMIENTO

Quiero agradecer sinceramente a aquellas personas que compartieron sus conocimientos conmigo para hacer posible la conclusión de este proyecto.

Especialmente agradezco a los docentes de la carrera por su guía y orientación siempre dispuesta , por sus ideas y recomendaciones con respecto a este proyecto.

INDICE GENERAL

INTRODUCCION

Actualmente, el manejo de la información de modo eficiente constituye una de las principales preocupaciones dentro de cualquier organización, sea esta de origen público o privado, por lo que se hace necesario manejarla y emplearla con mucho criterio, ya que de ello podría depender, en gran medida, el éxito o fracaso de las mismas. Son muchas las herramientas que, en la actualidad, facilitan al hombre el manejo del recurso informativo, así como el acceso a este. Una de estas herramientas, que permite utilizar el recurso de la información de manera más eficiente, rápida y confiable, la constituyen las redes de Computadoras, las cuales aparecen enmarcadas dentro del vertiginoso avance tecnológico que ha caracterizado a las últimas décadas del presente siglo.

Hoy en día casi todo el mundo tiene al menos un PC en casa y en muchos casos con conexión a internet, por lo que todos, y especialmente los jóvenes y niños, debemos entender el potencial de esa tecnología e integrarla en nuestras vidas de forma natural. Los estudiantes no deben ver el ordenador como un aparato que solo sirve para jugar o que deben usarlo obligatoriamente cuando tienen alguna investigación, si no como una herramienta viva que les permita acceder a un mundo de información y servicios ahorrando costes en tiempo y mejorando su productividad y calidad de vida, usarlo para su desarrollo vital cotidiano, igual para chatear con compañeros del colegio que para buscar información sobre cualquier tema, estar comunicados con familiares lejanos y amigos, etc. En definitiva tener unos mínimos conocimientos para vislumbrar el potencial de esta tecnología y ser conscientes de que puede haber contenidos dañinos para ellos a nivel digital.

CAPITULO I

ANTECEDENTES DEL PROYECTO

1.1 PLANTEAMIENTO DEL PROBLEMA

- Hoy en día cada vez es mayor la cantidad de información que hay que recibir, procesar y enviar de manera rápida y confiable La Unidad Educativa Región de Murcia “La primera” cuenta con una red LAN pero improvisada con deficiencias de organización

- No cuenta con la red inalámbrica WLAN que brinda el servicio de poder acceder a la red sin necesidad de cables haciendo que el usuario acceda desde dispositivos portátiles, celulares, etc

- En la actualidad los estudiantes quieren estar más y mejor informados, pues quieren disponer de variadas fuentes de información donde puedan satisfacer su curiosidad, por tanto es un problema el no poder tener acceso al servicio de internet ya que es una herramienta primordial en muchas áreas

- Uno de los problemas que se presenta tiene que ver con la calidad del servicio (QoS). Ya que no cuentan con un cableado estructurado

1.2 PLANTAMIENTO DE OBJETIVOS

1.2.1 Objetivo General

- Desarrollar una Red de Área Local (LAN) y WLAN que facilite la comunicación en la Unidad Educativa Región de Murcia “La Primera”

1.2.2 Objetivos Específicos

- Identificar el problema del cableado y de las maquinas ya existentes.

- Determinar los requerimientos de los usuarios que van a componer la red, para obtener opiniones de modificaciones a beneficios de los mismos.

- Contratar el servicio de internet tanto para la red LAN como WLAN dando así la facilidad de acceder a la red de manera cableada e inalámbrica

- Segmentar la red por áreas mediante el uso de las VLANs para así facilitar la organización de la Unidad Educativa

1.3 JUSTIFICACION DE LA INVESTIGACION

1.3.1 Justificación tecnológica

El sistema propuesto se adaptará perfectamente a las operaciones de la Unidad Educativa Región de Murcia “La Primera”, lo que producirá un mejoramiento en cuanto a la calidad y cantidad de información que pasará a través de una red local de datos

1.3.2 Justificación social

Mejorar la gestión académica y el proceso de enseñanza, aprendizaje mediante el uso de las redes LAN Y WLAN

1.3.3 Justificación académica

A lo largo del estudio en la carrera, las materias que ayudaron a realizar este proyecto fueron SISTEMAS DIGITALES I Y SISTEMAS DIGITALES II en los temas de redes, cableado, direccionamiento IP, enrutamiento, etc

1.4 DELIMITACION DEL PROYECTO

1.4.1 Delimitación Temporal

Con respecto al diseño de las redes que son alámbricas (LAN) e inalámbricas (WLAN), se realizaran los cálculos y pruebas por lo que se estima que la implementación se realizara de tres a cuatro meses

1.4.2 Delimitación Espacial

La Unidad Educativa Región de Murcia “La primera” donde se realizara el proyecto está ubicado en la ciudad de EL ALTO

Esta consta de un auditórium para eventos y tres edificios de 2 pisos de los cuales están divididos en Área de Secundaria, Área primaria, Dirección

1.4.3 Delimitación Temática

El objetivo primordial de estas actividades es lograr la actualización tecnológica de la infraestructura para que cuente con una mayor capacidad de crecimiento, manejo de conexiones de alta velocidad, instalación de switches, implantación de políticas de administración y control del tráfico

1.5 METODOLOGIA DE LA INVESTIGACION

1.5.1 Método descriptivo

El propósito de este método es describir situaciones y eventos. Esto decir cómo es y se manifiesta determinado fenómeno. Los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis.

Miden o evalúan diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar

El proyecto describirá el correcto funcionamiento de las redes cableadas LAN que tiene equipos como routers, switches, estaciones de trabajo PC`s, cables, conectores, etc. y las redes inalámbricas WLAN que cuenta con routers inalámbricos, PCI inalámbricos, etc. Así también como la mejoría del desarrollo académico de la Unidad Educativa Región de Murcia “La Primera”

CAPITULO II

MARCO TEORICO

2.1 BASES TEÓRICAS

Esta sección comprende un conjunto de conceptos y proposiciones que permiten fundamentar la investigación

2.1.1. Redes de Comunicaciones y Redes de Comunicación de Datos Un sistema está constituido por un conjunto de elementos los cuales trabajan entre sí con la finalidad de alcanzar un objetivo en común. Si se parte de esto, es posible afirmar que una red es un sistema.

Ejemplo II.1	
Redes de comunicación	En el caso de una red eléctrica de distribución de potencia, todos los elementos interconectados buscan compartir un recurso: la energía eléctrica, para llevarlo desde la fuente hasta la carga.
Ejemplo II.2	
Redes de comunicación de datos	En el caso de una red de vendedores de algún producto, todos sus elementos (los vendedores) se relacionan entre sí con la finalidad de vender su mercancía y, entre ellos, intercambian información sobre técnicas para captar nuevos clientes, etc.

Nótese que en los dos ejemplos, los componentes relacionados comparten algún atributo, ello se debe a que una red es un sistema donde sus elementos se encuentran interconectados con la finalidad de compartir algún recurso. Por ende, si el recurso que se va a compartir es información, se estará hablando de una red de comunicaciones. Si la información viene expresada en señales eléctricas variantes en el tiempo, se hará sobre una red de comunicaciones eléctricas. En el caso que la red tenga la capacidad de interconectar ubicaciones distantes, se disertará acerca de una red de telecomunicaciones. Por último, si la red comparte información en formato digital, se estará refiriendo a una red de datos. Las redes de datos pueden ser redes de comunicaciones eléctricas o redes de telecomunicaciones.
El propósito de un sistema de comunicación de datos es intercambiar información entre dos agentes.

Los sistemas de datos están conformados por tres bloques:

- Sistema fuente, conformado por el dispositivo de entrada y transmisor.
- Sistema destino, conformado por el receptor y dispositivo de salida.
- Medio de telecomunicación.

2.1.2. Ancho de Banda Analógico vs. Ancho de Banda Digital

El ancho de banda originalmente es analógico y se define como el diferencial entre las frecuencias máxima y mínima que se tienen para una transmisión. Si se observa el espectro de frecuencias, se podrá notar que entre la frecuencia mayor y menor de transmisión existen infinitas frecuencias, las cuales al verlas una al lado de otra parece que formaran una faja o banda, la que a su vez tendrá un ancho mayor o menor, dependiendo de qué tan separadas estén sus frecuencias laterales superior e inferior. Es de allí de donde proviene el nombre de ancho de banda, como si se refiriera a la anchura de un cinturón construido en base a frecuencias.

Se sabe que según el tamaño del ancho de banda del canal de transmisión, se podrá transmitir mayor o menor información por unidad de tiempo. Si se intentase pasar por una banda de frecuencias una foto en analógico a mayor ancho de banda, la imagen llegaría más nítida.

Esto se debe a que todos los detalles de esta foto, como lo son el brillo, los colores, etc., lo constituyen los armónicos, con una mayor separación entre las bandas laterales superior e inferior, se filtrarán menos armónicos; pero si estas frecuencias laterales se comienzan a cerrar, cada vez la imagen tendrá menos detalles, porque los armónicos se empezarán a filtrar cada vez más.

En el mundo digital, para transmitir una imagen con altos detalles, ya no se hablará de pasar gran cantidad de armónicos, sino que se necesitará un mayor número de muestras, lo cual implicará una cantidad de códigos mayor. Entonces, para transmitir señales digitales que implique muchos códigos, se tendrá que tener una capacidad de canal grande expresada en algún múltiplo de los bits por segundo (bps). A mayor magnitud de bps, mayor cantidad de información digital se podrá transmitir por unidad de tiempo.

En el trabajo cotidiano se observó que en el *analógico*, a más ancho de banda, mayor cantidad de información podía pasar por el canal por unidad de tiempo y que algo similar sucedía en el ambiente digital, donde a mayor velocidad de transmisión de *bits*, se podía llevar de una ubicación a otra una mayor cantidad de información digital. Por tal motivo se decidió adoptar una convención, llamando a los bps "ancho de banda digital", únicamente por una analogía o semejanza con el comportamiento en canales analógicos.

2.1.3. Estaciones de trabajo (Workstation)

Es un microprocesador que se encuentra conectada físicamente al servidor por medio de algún tipo de cable.

Que en la mayor parte de los casos esta computadora ejecuta su propio sistema operativo y, posteriormente, se añade al ambiente de la red.

2.1.4. Tipos de redes de comunicación

A continuación se presentan los tipos de redes de comunicación que se clasifican utilizando los siguientes criterios: tecnología de transmisión, escala y por servicio de conmutación.

Cuadro 1. Tipos de redes de comunicación

De acuerdo a:	**Tipos**
Tecnología de transmisión	Redes *broadcast* (que significa
	Redes punto a punto
Escala	Redes de área local (LAN o *Local*
	Redes de área extensa o amplia
Servicio de conmutación	Redes de conmutación de circuitos
	Redes de conmutación de paquetes

2.1.4.1. Tipos de redes de acuerdo con su tecnología de transmisión.

Las redes, de acuerdo a su tecnología de transmisión, se clasifican en *broadcast* y de punto a punto, las cuales se explican a continuación.

A) Redes *Broadcast*

El medio de transmisión es compartido por todos los computadores interconectados.
Normalmente, cada mensaje transmitido es para un único destinatario, cuya dirección aparece en el mensaje, pero para saberlo cada máquina de la red ha de recibir o "escuchar" cada mensaje, analizar la dirección de destino y averiguar si va o no dirigido a ella; las normas establecen que un computador debe descartar, sin más análisis, todo mensaje que no vaya dirigido a él; sin embargo, algunos programas llamados *sniffers* se dedican a “cotillear” todo lo que pasa por el cable, independientemente de quién sea su destinatario.

La única protección efectiva en las redes *broadcast* es el encriptado de la información. A veces, en una red *broadcast,* lo que se quiere es precisamente enviar un mensaje a todas las máquinas conectadas. Esto se llama un envío *broadcast.* Así mismo, es posible enviar un mensaje dirigido a un subconjunto de todas las máquinas de la red (subconjunto que ha de estar definido previamente); esto se conoce como envío *multicast* (y el subconjunto se denomina *grupo multicast*). El caso cuando el mensaje va dirigido a una máquina concreta, se denomina envío *unicast*.

Ejemplo

Ejemplo de redes Broadcast: Como ejemplos de estas, se pueden citar casi todas las tecnologías de red local Ethernet (en sus diversos tipos). También son redes *broadcast* las basadas en transmisión vía satélite.

En una red *broadcast* la capacidad o velocidad de transmisión indica la capacidad agregada de todas las máquinas conectadas a la red.

Ejemplo

Por ejemplo la velocidad de Transmisión de *Broadcast:* La red conocida como Ethernet tiene una velocidad de 10 Mbps, lo cual significa que la cantidad máxima de tráfico agregado de todos los equipos conectados no puede superar este valor.

B) Redes punto a punto

Las redes punto a punto se construyen por medio de *conexiones* entre pares de computadores, también llamadas *líneas*, *enlaces*, *circuitos* o *canales*. Una vez que el paquete es depositado en la línea, el destino es conocido de forma unívoca y no es preciso, en principio, que lleve la dirección de destino.

Los enlaces que constituyen una red punto a punto pueden ser de tres tipos, de acuerdo con el sentido de la transmisión:

1. ***Simplex*:** la transmisión se realiza en un sólo sentido.
2. ***Semi-duplex* o *half-duplex*:** la transmisión se puede realizar en ambos sentidos, pero no simultáneamente.
3. ***Dúplex* o *full-dúplex*:** la transmisión puede efectuarse en ambos sentidos a la vez.

En los enlaces *semi-duplex* y *dúplex*, la velocidad de conexión es generalmente la misma en ambos sentidos, por lo que se dice que el enlace es *simétrico*; en caso contrario se dice que es *asimétrico*. La gran mayoría de los enlaces en líneas punto a punto son *dúplex* simétricos. Así, cuando se habla de un enlace de 64 Kbps sin especificar más, se quiere decir 64 Kbps en cada sentido, por lo que la capacidad total del enlace es de 128 Kbps.

Al unir múltiples máquinas con líneas punto a punto, es posible llegar a formar redes de topologías complejas en donde no sea trivial averiguar cuál es la ruta óptima a seguir para ir de un punto a otro, ya que puede haber múltiples caminos posibles con distinto número de computadores intermedios, con enlaces de diversas velocidades y distintos grados de ocupación. Como contraste, en una red *broadcast* el camino a seguir de una máquina a otra es único, no existen computadores intermedios y el grado de ocupación es el mismo para todas ellas.

2.1.4.2. Tipos de redes según su escala

Las redes, según su escala, se clasifican en: Área Local (LAN) y Área Amplia (WAN), las cuales se explican a continuación.

A) Redes de Área Local (LAN)

Son aquellas donde las PC pueden estar a más de 10 metros de separación; pero sin embargo los *hosts* se encuentran relativamente adyacentes. Las LANs tienen generalmente las siguientes características:

1. Tecnología *broadcast*: medio compartido.
2. Cableado específico, instalado normalmente a propósito.
3. Velocidad de 1 a 100 Mbps.
4. Extensión máxima de unos 3 Km (FDDI llega a 200 Km)

Las LANs más conocidas y extendidas son la Ethernet a 10 Mbps, la IEEE 802.5 o Token Ring a 4 y 16 Mbps, y la FDDI a 100 Mbps. Estos tres tipos de LAN han permanecido prácticamente sin cambios desde finales de los '80, por lo que a menudo se les denomina en la literatura como "LANs tradicionales" para distinguirlas de otras más modernas aparecidas en los '90, tales como la Fast Ethernet (100 Mbps).

Las LANs requieren un tipo de cableado específico (de cobre o de fibra); esto no suele ser un problema, ya que al instalarse en una fábrica, *campus* o similar, se tiene un control completo sobre el entorno y las condiciones de instalación.

El alcance limitado de las LANs permite saber el tiempo máximo que un paquete tardará en llegar de un extremo a otro de la red, lo cual permite aplicar diseños que de otro modo no serían posibles y simplifica la gestión de la red. Como consecuencia del alcance limitado y del control en su cableado, las redes locales suelen tener un retardo muy bajo en las transmisiones (decenas de microsegundos) y una tasa de errores muy baja.

La topología básica de las redes locales suele ser de *bus* (Ethernet) o de *anillo* (Token Ring o FDDI). Sin embargo, pueden hacerse topologías más complejas utilizando elementos adicionales, tales como repetidores, puentes y conmutadores, entre otros, tal y como se verá más adelante.

B) Redes de Área Amplia (WAN)

Las redes de amplio alcance se utilizan cuando no es factible tender redes locales, bien porque la distancia no lo permite, por el costo de la infraestructura o simplemente porque es preciso atravesar terrenos públicos en los que no es posible tender infraestructura propia. En todos estos casos, lo normal es utilizar para la transmisión de los datos los servicios de una empresa portadora.

Las redes WAN se implementan casi siempre haciendo uso de enlaces telefónicos que han sido diseñados principalmente para transmitir la voz humana, ya que este es el principal negocio de las compañías telefónicas. Normalmente, la infraestructura está fuera del control del usuario, y supeditado el servicio disponible a la zona geográfica de que se trate. Conseguir capacidad en redes WAN suele ser costoso, por lo que generalmente se solicita el mínimo imprescindible.

Con la paulatina introducción de fibras ópticas y líneas digitales en las infraestructuras de las compañías portadoras, las líneas WAN han reducido apreciablemente su tasa de errores; también se han mejorado las capacidades y reducido los costos. A pesar del inconveniente que en ocasiones pueda suponer el uso de líneas telefónicas, tienen la gran virtud de llegar prácticamente a todas partes, que no es poco.

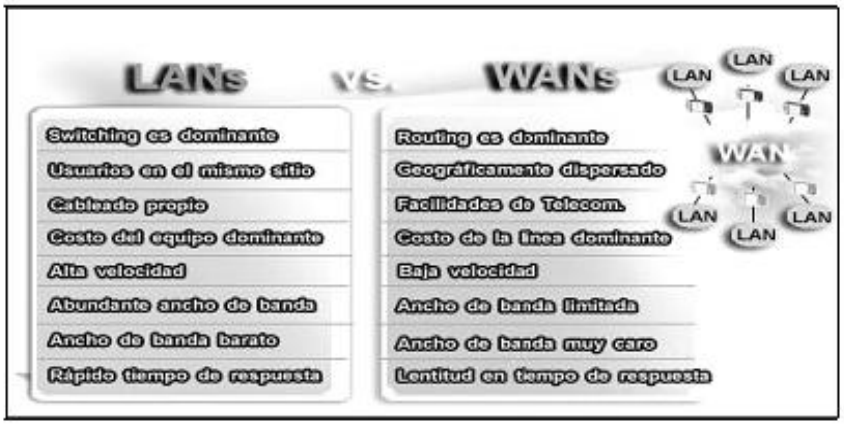


Gráfico 1. Comparación entre LANs y WANs.

2.1.4.3. Tipo de redes según el servicio de conmutación

Las redes, según el tipo de servicio, se clasifican en: de *conmutación de circuitos* y de *conmutación de paquetes*, las cuales se explican a continuación.

A) Redes de conmutación de circuitos

Estas son las características de una red de conmutación de circuitos:

1. Establecimiento de circuito temporal, mientras dura una comunicación.
2. Se establece un canal dedicado con un ancho de banda fijo.
3. Los usuarios pagarán sólo el tiempo que dura la comunicación en el uso del ancho de banda fijo.
4. Principales desventajas: retardo de conexión, ancho de banda fijo (no maneja avalancha de tráfico, requiriendo frecuentes retransmisiones), circuito virtual fijo, sin tener alternativas de caminos (saturación de tráfico).

B) Redes de conmutación de paquetes

Las características de una red de conmutación de paquetes son:

1. La conmutación por paquetes se divide en datagramas y circuitos virtuales.
2. Los *datagramas* son paquetes con información de direccionamiento individual.
3. Los *circuitos virtuales* establecen el camino para la ruta al principio de la sesión y después transmiten los paquetes sin información de direccionamiento de forma secuencial, como en un circuito conmutado. Se les dice *circuitos virtuales*, porque a pesar de que se comportan como un circuito conmutado, a diferencia de éstos, los circuitos virtuales comparten el medio de transmisión de forma simultánea. Existen dos tipos de circuitos virtuales, los circuitos virtuales permanentes (PVC) y los circuitos virtuales conmutados (SVC).
4. Los *circuitos virtuales conmutados* inician la sesión antes de transmitir los paquetes y después liberan el canal.

5. Los *circuitos virtuales permanentes* son iniciados por el administrador de red y se quedan perennemente activos, esperando la transmisión de datos entre ubicaciones, sin necesidad de direccionamiento en los paquetes.
6. Los datos se transmiten paquete a paquete en un entramado de red o nube.
7. Los datagramas pueden tomar caminos alternativos para llegar a su destino, lo que hace un ancho de banda variable (evita líneas colapsadas o congestionadas).

2.1.5. Arquitectura de Redes.

En la telecomunicación, la especificación de una arquitectura de red puede incluir también una descripción detallada de los productos y servicios entregados a través de una red de comunicaciones, y así como la tasa de facturación detallada y estructuras en las que se compensan los servicios.

2.1.5.1 Modelo OSI

Nivel Fisico

Es la primera capa del Modelo OSI. Es la que se encarga de la topología de red y de las conexiones globales de la computadora hacia la red, se refiere tanto al medio físico como a la forma en la que se transmite la información.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), cable coaxial, guías de onda, aire, fibra óptica.
- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

- Transmitir el flujo de bits a través del medio.
- Manejar las señales eléctricas del medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión (aunque no la fiabilidad de dicha conexión).

Nivel de Enlace de Datos

Esta capa se ocupa del direccionamiento físico, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo. Es uno de los aspectos más importantes que revisar en el momento de conectar dos ordenadores, ya que está entre la capa 1 y 3 como parte esencial para la creación de sus protocolos básicos (MAC, IP), para regular la forma de la conexión entre computadoras así determinando el paso de tramas (trama = unidad de medida de la información en esta capa, que no es más que la segmentación de los datos trasladándolos por medio de paquetes), verificando su integridad, y corrigiendo errores, por lo cual es importante mantener una excelente adecuación al medio físico (los más usados son el cable UTP, par trenzado o de 8 hilos), con el medio de red que redirecciona las conexiones mediante un router. Dadas estas situaciones cabe recalcar que el dispositivo que usa la capa de enlace es el Switch que se encarga de recibir los datos del router y enviar cada uno de estos a sus respectivos destinatarios (servidor -> computador cliente o algún otro dispositivo que reciba información como teléfonos móviles, tabletas y diferentes dispositivos, etc.), dada esta situación se determina como el medio que se encarga de la corrección de errores, manejo de tramas, protocolización de datos (se llaman protocolos a las reglas que debe seguir cualquier capa del modelo OSI).

Nivel de Red

Se encarga de identificar el enrutamiento existente entre una o más redes. Las unidades de información se denominan paquetes, y se pueden clasificar en protocolos enrutables y protocolos de enrutamiento.

- Enrutables: viajan con los paquetes (IP, IPX, APPLETALK)
- Enrutamiento: permiten seleccionar las rutas (RIP, IGRP, EIGRP, OSPF, BGP)

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Los dispositivos que facilitan tal tarea se denominan encaminadores o enrutadores, aunque es más frecuente encontrarlo con el nombre en inglés *routers*. Los routers trabajan en esta capa, aunque pueden actuar como switch de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los firewalls actúan sobre esta capa principalmente, para descartar direcciones de máquinas.

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

Nivel de transporte

Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que esté utilizando. La PDU de la capa 4 se llama Segmento o Datagrama, dependiendo de si corresponde a TCP o UDP. Sus protocolos son TCP y UDP; el primero orientado a conexión y el otro sin conexión. Trabajan, por lo tanto, con puertos lógicos y junto con la capa red dan forma a los conocidos como Sockets IP:Puerto (191.16.200.54:80).

Nivel de Sesion

Esta capa es la que se encarga de mantener y controlar el enlace establecido entre dos computadores que están transmitiendo datos de cualquier índole. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

Nivel de Presentación

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

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

Esta capa también permite cifrar los datos y comprimirlos. Por lo tanto, podría decirse que esta capa actúa como un traductor.

Nivel de aplicacion

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

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

2.1.6. Aspectos de las topologías de Red

Una *topología de red* es una representación pictórica de una capa de red. Los tipos de topología de red tienen dos aspectos:

Topologías Físicas.

Topologías Lógicas.

2.1.6.1. Topologías Físicas de Red

Una topología física de red define cómo los dispositivos que están conectados. Para comprender esto, se necesitarán los siguientes conceptos:

a. Especificaciones de hardware para las topologías de red.
b. Topología física bus.
c. Topología física estrella.
d. Topología física anillo.

a) Especificaciones de Hardware para las topologías de red: Los cables, servidores y estaciones son parte de la topología física de una red. Además se necesitará conocer acerca de otros dos componentes usados en una red: *hubs* y repetidores.

- ***Hubs*:** Un *hub* es un simple dispositivo que puede ser usado para conectar múltiples dispositivos a una red, por ejemplo, estaciones de trabajo e impresoras. El *hub* provee un punto común de conexión física para los dispositivos de red

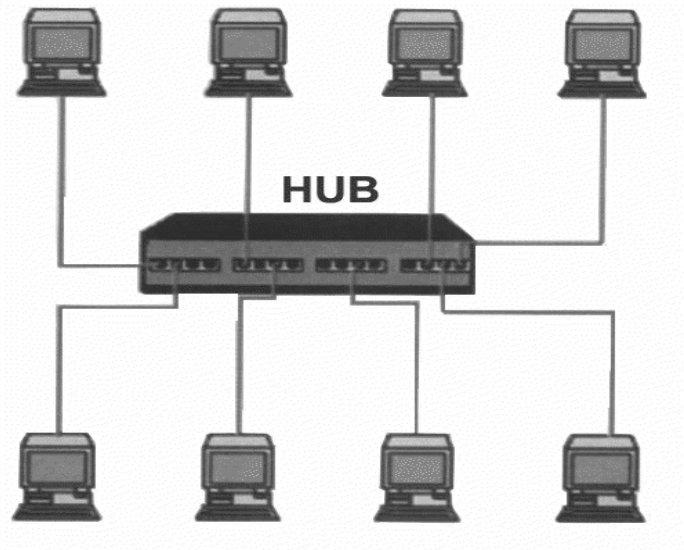


Gráfico 2: Hub.

- Repetidores: Los repetidores incrementan las distancias sobre las cuales las señales de red pueden viajar. Como una señal viaja a través del cable, ésta se debilita dada la resistencia del mismo. Cuando un repetidor recibe una señal débil, éste retransmite a su destino pero manteniendo la señal intacta, esto quiere decir que el repetidor amplifica la señal. La mayoría de los *hubs* tienen un repetidor incluido en el propio dispositivo.

b) Topología bus: El término *bus* es bastante usado en electrónica y tiene que ver con el transporte (*bussing*) de señales desde un punto a otro.

Una topología física de red en *bus* es una simple topología que usa un cable largo llamado *backbone*. Los cables cortos, llamados *drop,* pueden ser conectados al *backbone* usando conectores tipo "T".
El cable *backbone* necesita en los extremos unos elementos que le indiquen el inicio y el fin de la red, así como también evitar que la señal siga buscando otro dispositivo. Este dispositivo se llama *terminador* y está conectado a un punto de tierra. En la topología *bus* se permite que la señal electromagnética viaje en diferentes direcciones.

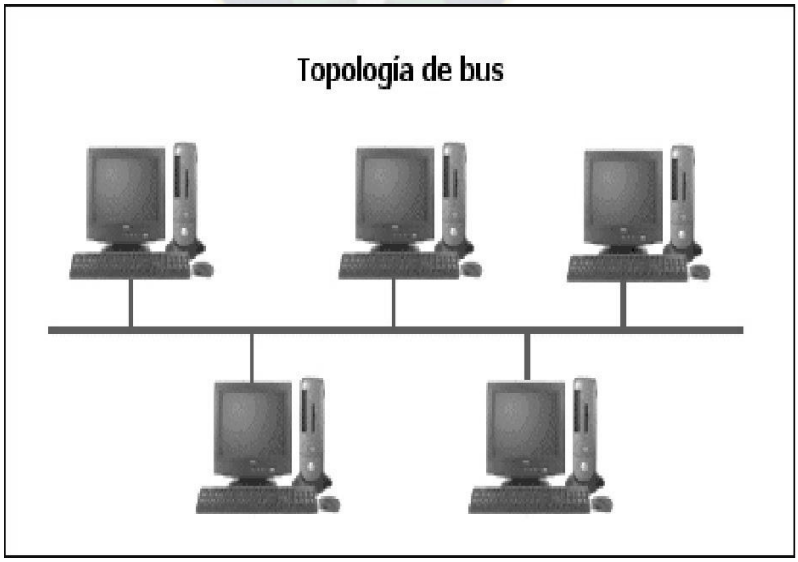


Gráfico 3: Topologia BUS

c) Topología Anillo: Una topología *anillo* es igual a un círculo (un enlace cerrado entre puntos). Cada dispositivo se conecta al anillo a través de un dispositivo similar a un *hub/switch* que también provee un cable de conexión especial.

Gráfico 4: Topologia Anillo

d) Topología Estrella: La topología *estrella* usa un dispositivo central con cables extendiéndose en todas direcciones. Cada dispositivo es conectado al *hub/switch* a través de una conexión punto a punto.

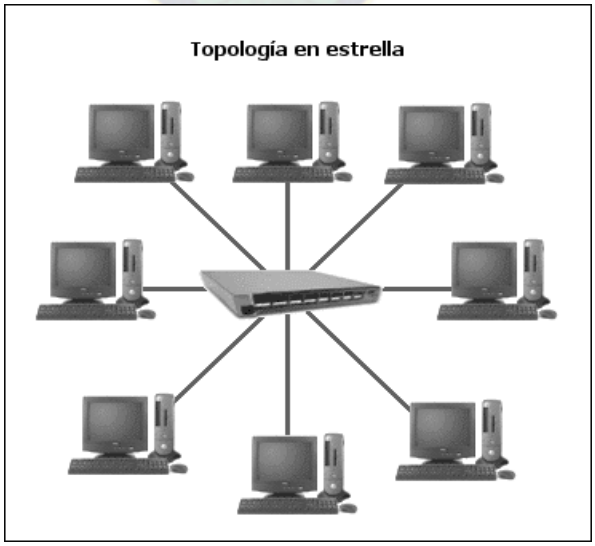


Gráfico 5: Topología estrella.

En la topología estrella, las señales eléctricas y electromagnéticas viajan desde el dispositivo conectado por cable hasta el *hub/switch*. Desde ahí la señal es enviada a los otros dispositivos de red.

2.1.6.2. Topologías Lógicas de Red

Después de planear el esquema físico de la red, se debe considerar el esquema lógico. Hay dos topologías lógicas muy comunes:

Bus Anillo

Las diferentes formas de cómo el tráfico puede fluir en un sistema de calles, es un ejemplo de *topología lógica*. Esta es, en esencia, una estrategia para direccional el flujo de la señal.

Esta metáfora del tráfico es una manera muy válida para entender una topología lógica. Como se puede ver, los términos *tráfico de red y colisiones* son comúnmente usados en la terminología de red.

Las topologías lógicas son una parte fundamental de una red, porque las señales eléctricas deben mantenerse separadas y diferenciadas de las otras, para evitar choques y distorsiones.

Los dispositivos que envían la señal también deben mantener un orden. Estos deben "hablar" para tomar turnos, o "mirar" el tráfico de la red antes de enviar sus mensajes.

a) Topología lógica *bus*: En una topología lógica *bus*, los dispositivos generan señales y las envían a través de la red, independientemente de la ubicación del receptor. Una topología lógica *bus* puede sólo ser usada con las topologías físicas *bus* y *estrella*.

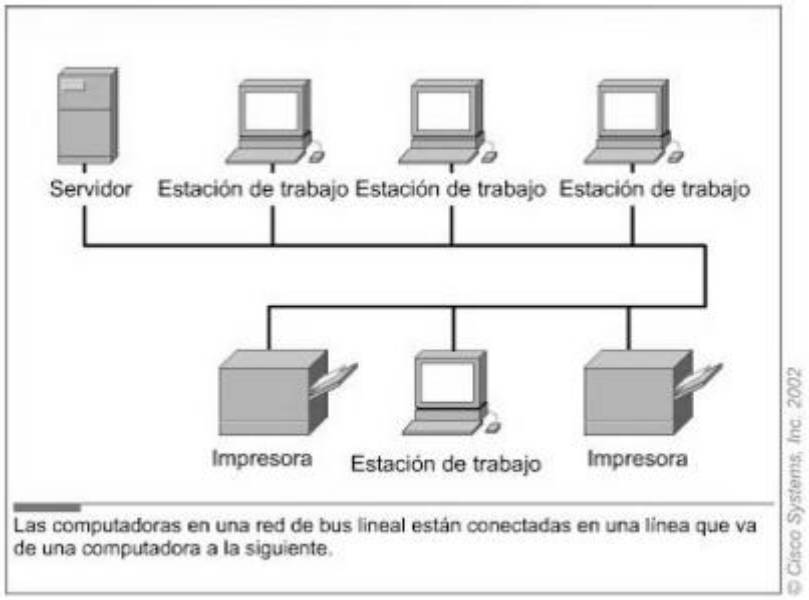


Gráfico 6: Topología bus.

El mensaje enviado a todos los dispositivos, en una topología lógica *bus,* contiene información que dice cuál dispositivo debe de recibir el mensaje. El dispositivo que supuestamente recibió el mensaje, lo recibirá. Otros lo ignorarán.

Una topología bus es recomendable porque los dispositivos de red no están enterados de las ubicaciones físicas de los otros dispositivos.

No se puede dar a un dispositivo instrucciones para enviar mensajes directamente a otro dispositivo. Un dispositivo no puede conocer que otro está localizado a “tres nodos al sur sobre el lado derecho”. Por tanto, un dispositivo debe enviar el mensaje en todas las direcciones. Entonces, cada dispositivo determina si el mensaje fue precisamente para él mismo.

b) Topología lógica anillo: En una topología lógica anillo, la señal es generada y viaja a través de una ruta ya especificada en una simple dirección

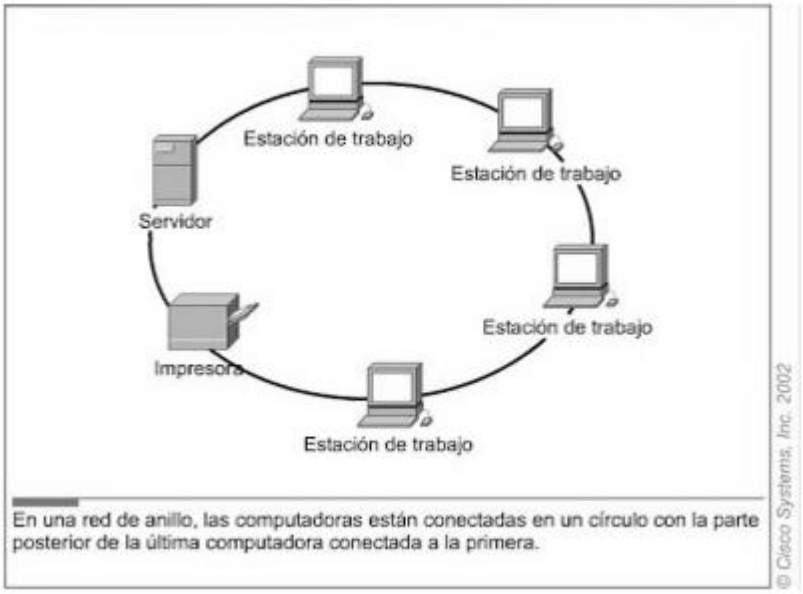


Gráfico 7: Red anillo

La topología lógica anillo puede ser usada con la topología física *anillo* y con la topología física *estrella*.

La diferencia entre el anillo lógico y el *bus* lógico está en que la señal enviada en una lógica *bus* va en todas direcciones. Las señales enviadas en un anillo lógico pueden ir sólo en una dirección. Una topología física *estrella* puede manipular una topología lógica *anillo*, porque las señales entran en el *hub* y son enviadas de regreso a los dispositivos de red en un orden predeterminado.

La topología física puede ser usada con cualquiera de las dos topologías. La estrella física es también relativamente fácil de instalar y fácil de reconfigurar, además de ser muy común.

2.1.7. Dispositivos de Redes de Área Local

Entre los dispositivos de Redes de Área Local (LAN) se pueden nombrar: dispositivos LAN genéricos, tarjetas de red (NIC), repetidores, concentradores (*hubs*), puentes (*bridges*), conmutadores (*switches*), enrutadores (*routers*) y la nube, los cuales se explican a continuación:

2.1.7.1. Dispositivos LAN genéricos.

Los dispositivos que se conectan de forma directa a un segmento de red se denominan *hosts*. Estos *hosts* incluyen computadores, tanto clientes como servidores, impresoras, escáner y varios otros dispositivos de usuario. Estos dispositivos suministran a los usuarios conexión a la red, por medio de la cual los usuarios comparten, crean y obtienen información. Los dispositivos *host* pueden existir sin una red, pero sin la red las capacidades de los *hosts* se ven sumamente limitadas.

Los dispositivos *host* no forman parte de ninguna capa. Tienen una conexión física con los medios de red, ya que poseen una tarjeta de interfaz de red (NIC) y las otras capas OSI se ejecutan en el *software* ubicado dentro del *host*. Esto significa que operan en todas las 7 capas del modelo OSI. Ejecutan todo el proceso de encapsulamiento y desencapsulamiento para realizar la tarea de enviar mensajes de correo electrónico, imprimir informes, escanear gráficos o acceder a las bases de datos.

La función básica de los computadores de una LAN es suministrar al usuario un conjunto de aplicaciones prácticamente ilimitado. El *software* moderno, la microelectrónica y relativamente poco dinero, le permiten ejecutar programas de procesamiento de texto, presentaciones, hojas de cálculo y bases de datos. También le permiten ejecutar un navegador de Web, que le proporciona acceso instantáneo a la información a través de la World Wide Web (WWW). De este modo puede enviar correos electrónicos, editar gráficos, guardar información en bases de datos, jugar y comunicarse con otros computadores ubicados en cualquier lugar del mundo.

2.1.7.2. La tarjeta de red (NIC)

Una tarjeta de interfaz de red (NIC) se conecta a una tarjeta madre y suministra los puertos para la conexión.

Esta tarjeta puede estar diseñada como una tarjeta Ethernet, una tarjeta Token Ring o una tarjeta FDDI. Las tarjetas de red se comunican con la red a través de conexiones seriales y con el computador a través de conexiones en paralelo. Son las conexiones físicas entre las estaciones de trabajo y la red.

Las tarjetas de red requieren una IRQ, una dirección E/S y direcciones de memoria superior para DOS y Windows 95/98. Al seleccionar una tarjeta de red, deben tenerse en cuenta los siguientes factores:

1. El tipo de red (por ejemplo, Ethernet, Token Ring, FDDI u otro)
2. El tipo de medios (por ejemplo, cable de par trenzado, cable coaxial o fibra óptica)
3. El tipo de *bus* del sistema (por ejemplo, PCI e ISA)

Las NIC ejecutan funciones importantes de la capa de enlace de datos (Capa 2) como, por ejemplo, las siguientes:

1. *Control de enlace lógico*: Se comunica con las capas superiores del computador.
2. *Denominación*: Proporciona un identificador exclusivo de dirección MAC.
3. *Entramado*: Parte del proceso de encapsulamiento, empaquetar los *bits* para transportarlos.
4. *Control de acceso al medio (MAC)* : Proporciona un acceso estructurado a los medios de acceso compartido.
5. *Señalización*: Crea señales y realiza interfaz con los medios usando transceptores incorporados.

Ejemplo

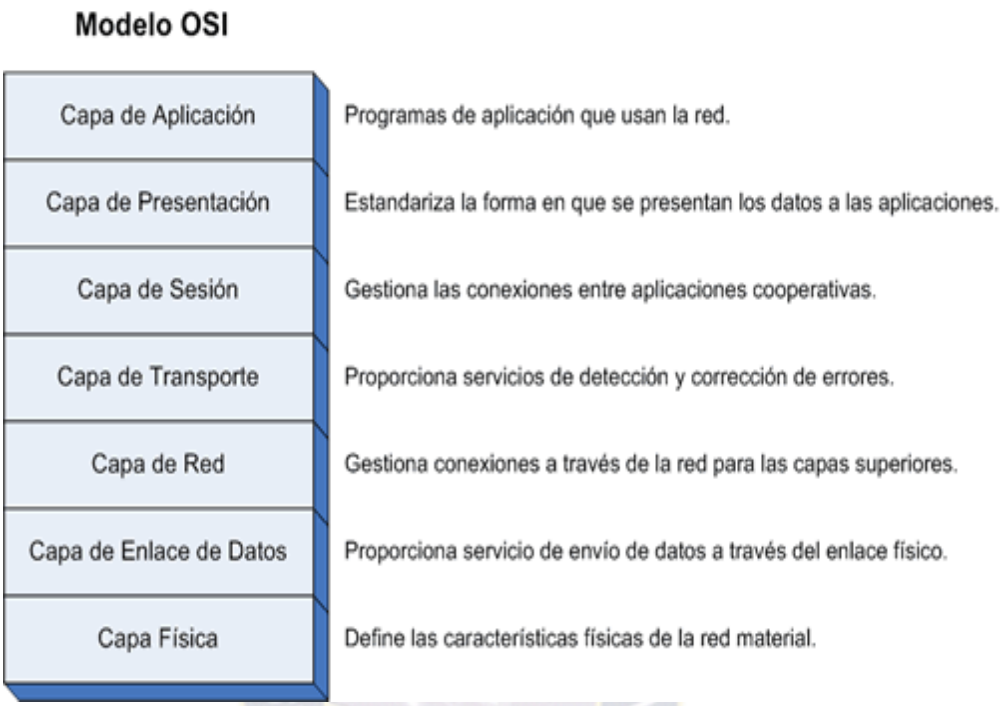


Gráfico 8: Las NIC y el modelo OSI.

Gráfico 9: Ejemplo de una NIC.

2.1.7.3. El repetidor

Hay varios tipos de medios y cada uno de estos tiene sus ventajas y desventajas. Una de las desventajas del tipo de cable que utilizamos principalmente (UTP CAT5) es la longitud del mismo. La longitud máxima para el cableado UTP de una red es de 100 metros. Si es necesario extender la red más allá de este límite, se debe agregar un dispositivo a la red. Este dispositivo se denomina *repetidor*.

Los repetidores son dispositivos con un sólo puerto "de entrada" y un sólo puerto "de salida". En el modelo OSI, los repetidores se clasifican como dispositivos de Capa 1, dado que actúan sólo a nivel de los *bits* y no tienen en cuenta otro tipo de información.

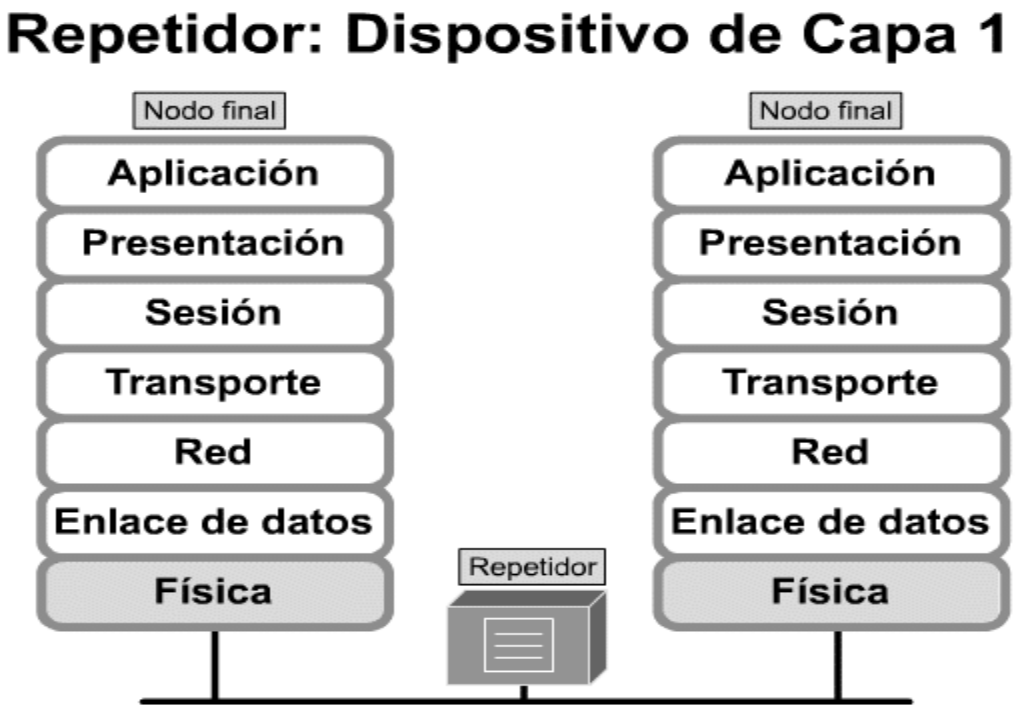


Gráfico10:El repetidor en el modelo OSI.

2.1.7.4. El concentrador (*hub*)

El propósito de un *hub* es regenerar y retemporizar las señales de red. Esto se realiza a nivel de los *bits* para un gran número de *hosts* (por ejemplo, 4, 8 o incluso 24), utilizando un proceso denominado *concentración*.

Podrá observar que esta definición es muy similar a la del repetidor, es por ello que el *hub* también se denomina **repetidor multipuerto**. La diferencia es la cantidad de cables que se conectan al dispositivo. Las razones por las que se usan los *hubs* son crear un punto de conexión central para los medios de cableado y aumentar la confiabilidad de la red.

La confiabilidad de la red se ve aumentada al permitir que cualquier cable falle sin provocar una interrupción en toda la red. Esta es la diferencia con la topología de *bus*, en la que si un cable falla, causa una interrupción en toda la red. Los *hubs* se consideran dispositivos de la Capa 1, dado que sólo regeneran la señal y la envían por medio de un *broadcast* de ella a todos los puertos (conexiones de red)

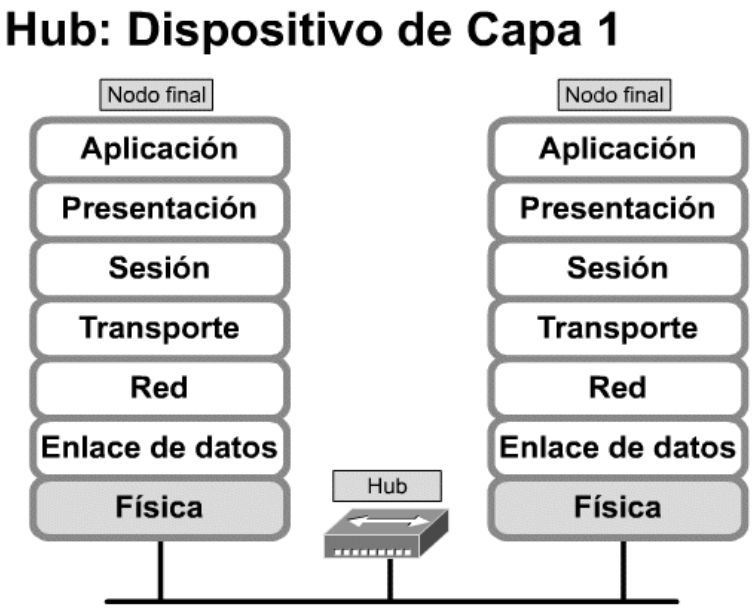


Gráfico 11: El concentrador en el modelo OSI

2.1.7.5. Los puentes (*bridges*)

Un *puente* conecta los segmentos de red y debe tomar decisiones inteligentes con respecto a si debe transferir señales al siguiente segmento. Un puente puede mejorar el desempeño de una red al eliminar el tráfico innecesario y reducir al mínimo las probabilidades de que se produzcan colisiones. El puente divide el tráfico en segmentos y filtra el tráfico basándose en la estación o en la dirección MAC.
Los puentes no son dispositivos complejos. Analizan las tramas entrantes, toman decisiones de envío basándose en la información que contienen las tramas y las envían a su destino. Los puentes sólo se ocupan de pasar los paquetes, o de no pasarlos, basándose en las direcciones MAC destino. A menudo pasan paquetes entre redes que operan bajo distintos protocolos de Capa 2 del modelo referencial OSI.

Las características principales de los puentes son:

- Más inteligentes que un *hub*, analizan los paquetes entrantes y los envían o descartan, según la información de direccionamiento.

- Reúnen y transmiten paquetes entre dos segmentos de red.
  Control de *broadcast* hacia la red.

- Mantenimiento de las tablas de dirección.

- Hay distintos tipos de puentes: Transparente y Ruta Origen (principalmente usado en las LAN Token Ring).

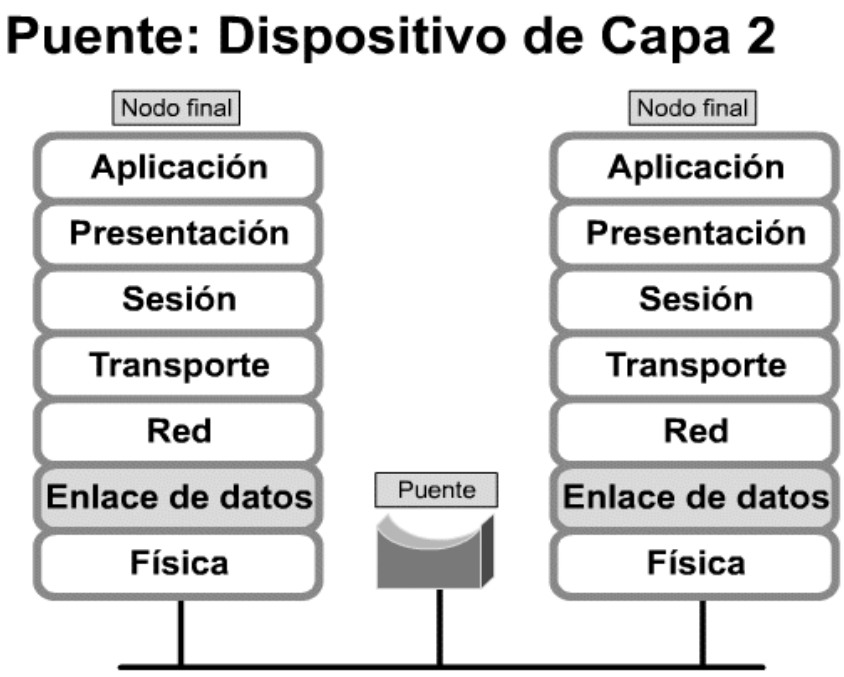


Gráfico 12: El puente.

El *puenteo* se produce en la capa de enlace de datos, que controla el flujo de datos, maneja los errores de transmisión, proporciona direccionamiento físico y administra el acceso hacia el medio físico. Los puentes ofrecen estas funciones mediante diversos protocolos de capa de enlace que imponen control de flujo, manejo de errores, direccionamiento y algoritmos de acceso a los medios específicos. Entre los ejemplos de protocolos de capa de enlace de datos de uso generalizado se incluyen Ethernet, Token Ring y FDDI.

La transparencia del protocolo de capa superior es una de las ventajas principales del puenteo. Como los puentes operan en la capa de enlace de datos, no necesitan examinar la información de capa superior. Esto significa que pueden enviar rápidamente tráfico que represente cualquier protocolo de capa de red. Es habitual que un puente transporte protocolos y otro tipo de tráfico entre dos o más redes.

No es necesario que los puentes examinen la información de capa superior, ya que operan en la capa de enlace de datos, o sea, en la Capa 2 del modelo OSI. Los puentes filtran el tráfico de red observando sólo la dirección MAC, no los protocolos. Es habitual que un puente transporte protocolos y otro tipo de tráfico entre dos o más redes. Como los puentes sólo verifican las direcciones MAC, pueden enviar rápidamente tráfico que represente cualquier protocolo de capa de red. Para filtrar o enviar de forma selectiva el tráfico de red, un puente genera tablas de todas las direcciones MAC ubicadas en sus segmentos de red directamente conectados.

Si los datos se transportan a través del medio de red, el puente compara la dirección MAC destino que contienen los datos con las direcciones MAC de las tablas. Si el puente determina que la dirección MAC destino de los datos pertenece al mismo segmento de red que el origen, no envía los datos hacia los otros segmentos de la red. Por el contrario, si el puente determina que la dirección MAC destino de los datos no está en el mismo segmento de red que la fuente, envía los datos al segmento correspondiente. Al hacer esto, los puentes pueden reducir significativamente la cantidad de tráfico entre segmentos, eliminando el tráfico innecesario.

Los puentes son dispositivos de *internetworking* que se pueden usar para reducir los dominios de colisión de gran tamaño. Los *dominios de colisión* son áreas en las que existe la probabilidad de que los paquetes interfieran entre sí. Logran esto dividiendo la red en segmentos más pequeños y reduciendo la cantidad de tráfico que debe pasar entre los segmentos.

Los puentes operan en la Capa 2 o capa de enlace de datos del modelo OSI, ya que sólo se encargan de las direcciones MAC.

A medida que los datos se transportan a través de la red hacia su destino, cada dispositivo de la red, incluyendo los puentes, los recogen y los examinan. Un puente trabaja mejor cuando no hay demasiado tráfico entre un segmento de la red y los demás segmentos. Cuando el tráfico entre los segmentos de red aumenta, se puede producir un cuello de botella en el puente y la comunicación puede tornarse más lenta.

Existe un problema posible cuando se usa un puente. Éstos siempre difunden y multiplican una clase especial de paquetes de datos. Estos paquetes de datos aparecen cuando un dispositivo de la red desea comunicarse con otro dispositivo, pero no conoce la dirección destino del dispositivo. Cuando esto ocurre, con frecuencia el origen envía un *broadcast* a todos los dispositivos de la red. Como todos los dispositivos de la red tienen que prestar atención a estos *broadcasts*, los puentes siempre los envían. Ahora, si se envían demasiados *broadcasts* a través de la red, se puede provocar una tormenta de *broadcast*. Una tormenta de este tipo puede retrasar la información más allá de los límites de tiempo, causar demoras en el tráfico y hacer que la red no pueda operar a un nivel óptimo.

Las LAN Ethernet que usan un puente para segmentar la LAN, proporcionan mayor ancho de banda por usuario porque hay menos usuarios en los segmentos, en comparación con la LAN completa. El puente permite que sólo las tramas cuyos destinos se ubican fuera del segmento lo atraviesen. Los puentes aprenden cuál es la segmentación de una red creando tablas de direcciones que contienen la dirección de cada dispositivo de la red y el segmento que debe usar para alcanzar ese dispositivo. Los puentes son diferentes de los *routers*, ya que son dispositivos de la Capa 2 y, por lo tanto, son independientes de los protocolos de la Capa 3. Un puente transmite tramas de datos, sin considerar cuál es el protocolo de la Capa 3 que se usa, y es transparente para los demás dispositivos de la red.

Los puentes aumentan la *latencia* (demora) de una red en un 10-30%. Esta latencia se debe a la toma de decisiones que el puente (o los puentes) debe(n) realizar al transmitir datos al segmento correcto. Un puente se considera como un dispositivo de almacenamiento y envío porque debe recibir toda la trama y calcular la verificación por redundancia cíclica (CRC) antes de que pueda tener lugar el envío. El tiempo que tarda en ejecutar estas tareas puede hacer que las transmisiones de red sean más lentas, causando una demora de propagación.

2.1.7.6. El conmutador (*switch*)

La *conmutación* es una tecnología que alivia la congestión en las LAN Ethernet, reduciendo el tráfico y aumentando el ancho de banda. Los *switches*, también denominados *switches de LAN*, a menudo reemplazan los *hubs* compartidos y funcionan con infraestructuras de cable existentes, de manera que su instalación puede realizarse con un mínimo de problemas en las redes existentes.

En la actualidad, y en las comunicaciones de datos, todos los equipos de conmutación y de enrutamiento ejecutan dos operaciones básicas:

Conmutación de tramas de datos: Esta es una operación de "guardar y enviar" en la que una trama llega a un medio de entrada y se transmite a un medio de salida.
Mantenimiento de operaciones de conmutación: Los *switches* crean y mantienen tablas de conmutación y buscan *loops*.

Los *routers* crean y mantienen tanto tablas de enrutamiento como tablas de servicios. Como en el caso de los puentes, los *switches* conectan segmentos de la LAN, usan una tabla de direcciones MAC para determinar el segmento en el que es necesario transmitir un datagrama y reducen el tráfico. Los *switches* operan a velocidades mucho más altas que los puentes y pueden soportar nuevas funcionalidades como, por ejemplo, las LAN virtuales.

Un *switch* Ethernet brinda muchas ventajas como, por ejemplo, permitir que varios usuarios se comuniquen en paralelo a través del uso de circuitos virtuales y segmentos de red dedicados en un entorno libre de colisiones. Esto aumenta al máximo el ancho de banda disponible en el medio compartido. Otra de las ventajas es que desplazarse a un entorno de LAN conmutado es muy económico, ya que el *hardware* y el cableado se pueden volver a utilizar. Por último, los administradores de red tienen mayor flexibilidad para administrar la red a través de la potencia del switch y del *software* para configurar la LAN.

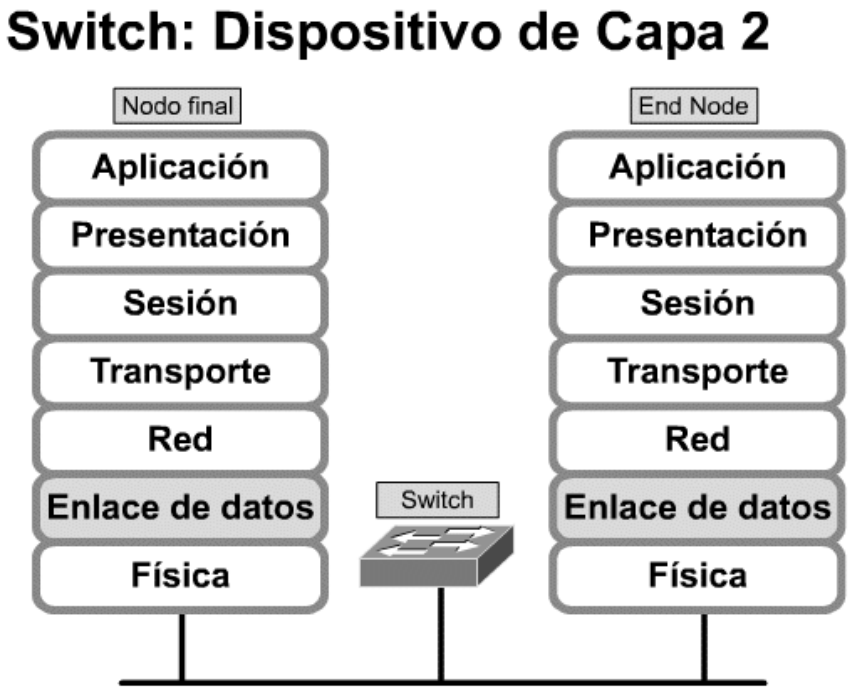


Gráfico 13: El conmutador.

Uno de los principales beneficios de los conmutadores es la *microsegmentación*. Los *switches* de LAN se consideran puentes multipuerto sin dominio de colisión debido a la microsegmentación. Los datos se intercambian a altas velocidades, haciendo la conmutación de paquetes hacia su destino. Al leer la información de Capa 2 de dirección MAC destino, los *switches* pueden realizar transferencias de datos a altas velocidades, de forma similar a los puentes. El paquete se envía al puerto de la estación receptora antes de que la totalidad del paquete ingrese al switch. Esto provoca niveles de latencia bajos y una alta tasa de velocidad para el envío de paquetes.

La conmutación Ethernet aumenta el ancho de banda disponible en una red. Esto se hace creando segmentos de red dedicados, o conexiones punto a punto, y conectando estos segmentos en una red virtual dentro del *switch*. Este circuito de red virtual existe sólo cuando se deben comunicar dos nodos. Esto se denomina *circuito virtual*, ya que existe sólo cuando es necesario y se establece dentro del switch.

Aunque un switch de LAN reduce el tamaño de los dominios de colisión, todos los hosts conectados al mismo se encuentran todavía en el mismo dominio de broadcast, por lo tanto, un broadcast desde un nodo será visto por todos los demás nodos conectados a través del switch de LAN.

Los switches son dispositivos de enlace de datos que, al igual que los puentes, permiten que múltiples segmentos físicos de LAN se interconecten para formar una sola red de mayor tamaño. De forma similar a los puentes, los switches envían e inundan el tráfico con base a las direcciones MAC. Dado que la conmutación se ejecuta en el hardware en lugar del software, es significativamente más veloz. Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina microsegmentación. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada *host*

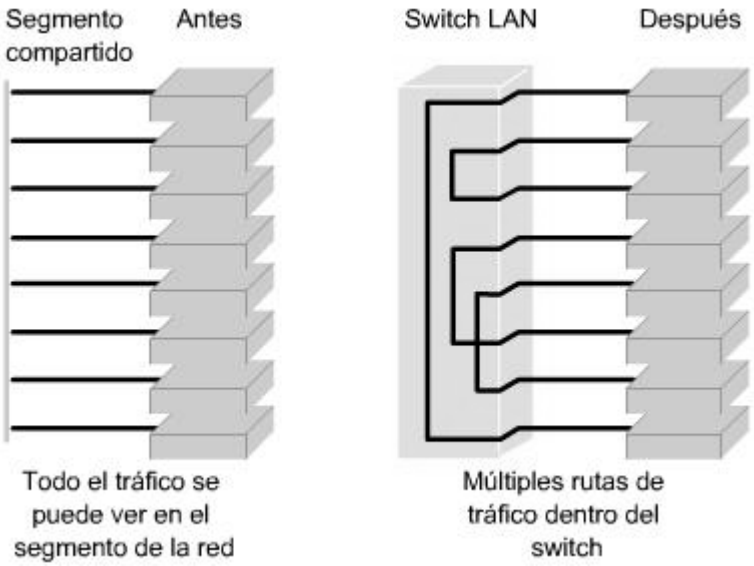


Gráfico 14: Microsegmentación.

Existen dos factores muy importantes a tomar en conmutación, tales como el rendimiento del conmutador (throughput) y la latencia (latency), los cuales se explican a continuación:

El rendimiento del conmutador (*throughput*)

Se refiere a la cantidad de tramas que pueden ser trasladadas con éxito de un puerto a otro en un periodo dado de tiempo; es el único parámetro para evaluar el desempeño de un conmutador e involucra un concepto llamado retardo o latencia (*latency*).

Latencia (latency)

Es el tiempo que tarda una trama dentro del conmutador, creándose de esta forma una relación inversamente proporcional: a mayor retardo, menor desempeño tendrá el conmutador.

Hay dos tipos de conmutación en redes de área local, la simétrica y la asimétrica

Conmutación Simétrica

Esta provee conmutación entre segmentos que poseen anchos de banda similares, es decir, 10/10 Mbps. En estos casos se utiliza el método de conmutación *cut-throught*, en el cual se envía la trama al puerto de la salida tan pronto se ha detectado la dirección de la computadora de destino. Este método introduce la menor cantidad de retardo (*latency*).

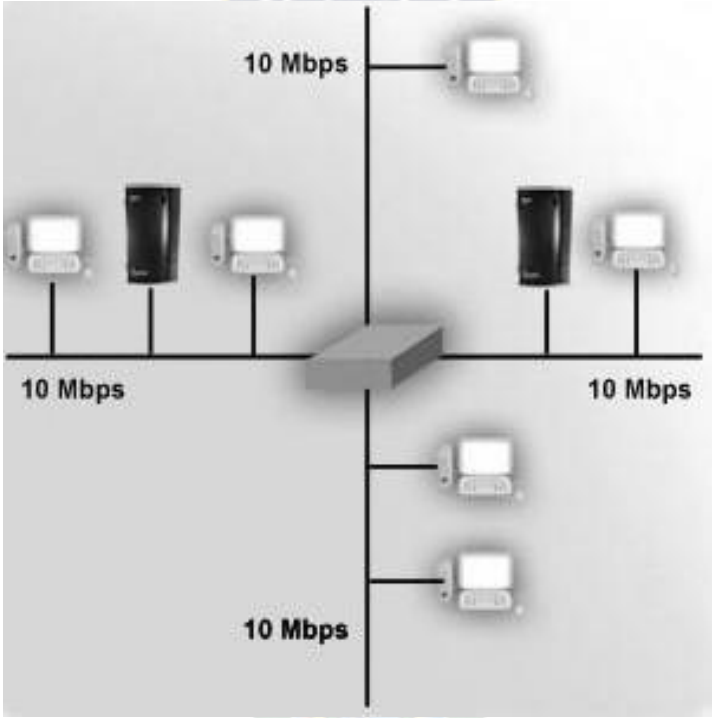


Gráfico 15: Conmutación simétrica.

Conmutación Asimétrica. Este tipo provee conmutación entre segmentos que poseen anchos de banda diferentes, es decir 10/100 Mbps. En estos casos se utiliza el método de conmutación *store and forward*, en el cual se almacena la trama entera, chequea su longitud y ejecuta cálculos de errores, introduciendo retardos apreciables.

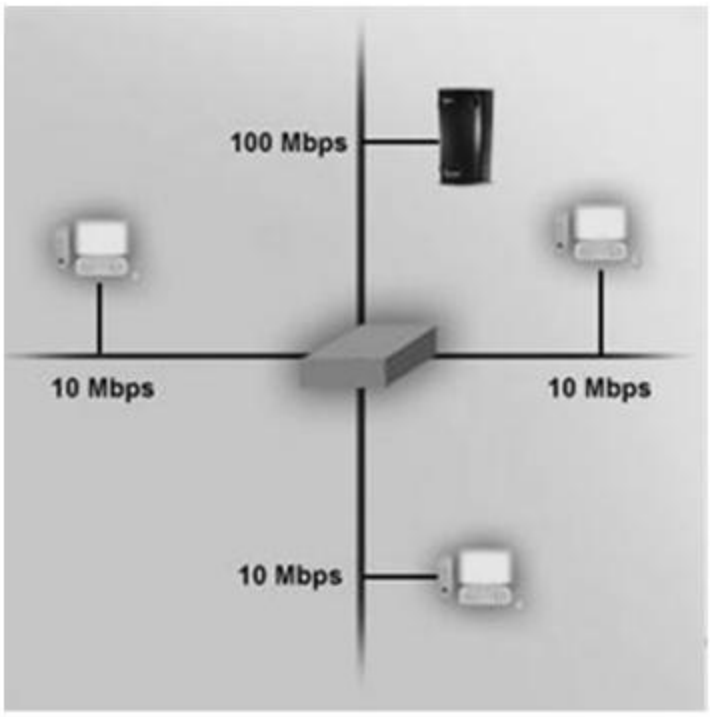


Gráfico 16: Conmutación asimétrica.

2.1.7.8 El enrutador (*router*)

Aunque el *router* es un dispositivo de Capa 3 del nivel OSI, y las redes de área local sólo llegan en norma hasta el nivel de enlace de datos, es conveniente el estudio de los *enrutadores*, ya que éstos permiten interconectar las LAN con otras redes.

El *router* es el primer dispositivo con el que se trabajará que está ubicado en la capa de red del modelo OSI, o Capa 3. Al trabajar en esta capa, permite que el *router* tome decisiones basándose en grupos de direcciones de red (clases), a diferencia de las direcciones MAC individuales, que es lo que se hace en la Capa 2.

Los *routers* también pueden conectar distintas tecnologías de la Capa 2 como, por ejemplo, Ethernet, Token Ring y FDDI. Sin embargo, dada su aptitud para enrutar paquetes basándose en la información de la Capa 3, los *routers* se han transformado en el *backbone* de Internet, ejecutando el protocolo IP.

El propósito de un *router* es examinar los paquetes entrantes (datos de la Capa 3), elegir cuál es la mejor ruta para ellos a través de la red y luego conmutarlos hacia el puerto de salida adecuado. Los *routers* son los dispositivos de regulación de tráfico más importantes en las redes de gran envergadura. Permiten que prácticamente cualquier tipo de computador se pueda comunicar con otro en cualquier parte del mundo. Aunque ejecutan estas funciones básicas, los *routers* también pueden ejecutar muchas otras tareas.

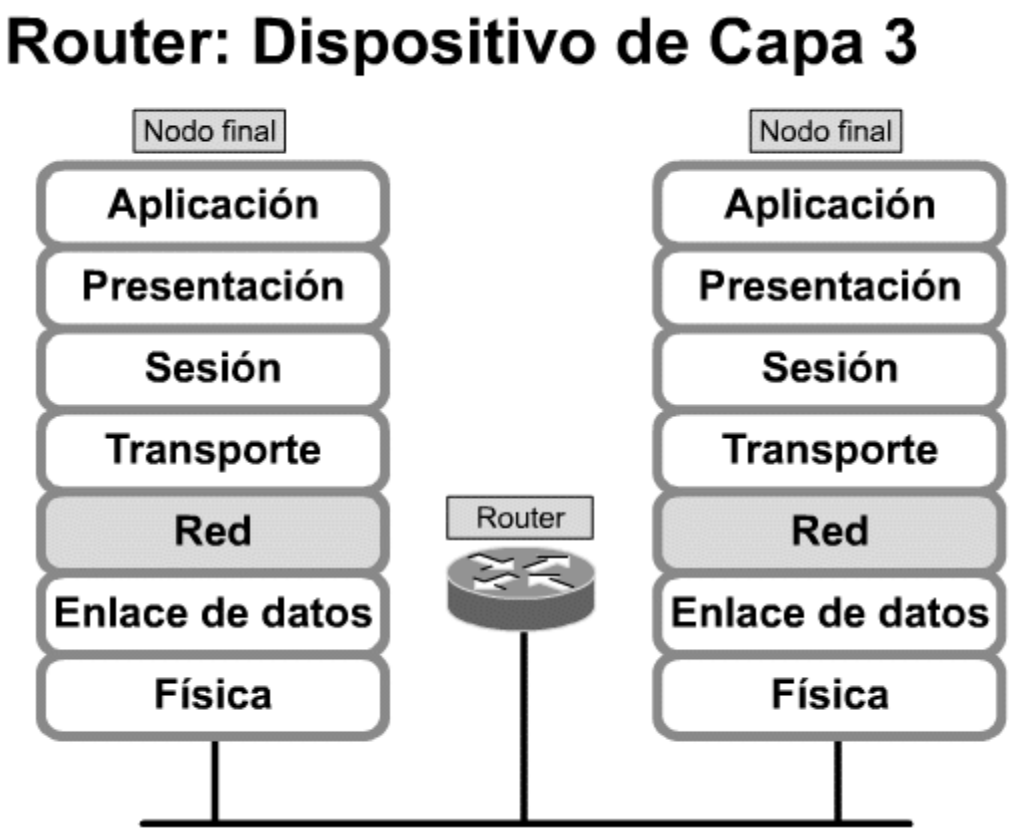


Gráfico 17: El enrutador y el modelo OSI. Fuente:

2.1.8. Cableado estructurado

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

Específicamente, este cableado consiste en el tendido de cables en el interior de un edificio con el propósito de implantar una red de área local.

2.1.8.1. Subsistemas de Cableado Estructurado

El cableado estructurado está compuesto de varios subsistemas:

- Sistema de cableado vertical.
- Sistema de cableado horizontal.
- Salida de área de trabajo.
- Cuarto o espacio de telecomunicaciones.
- Cuarto o espacio de equipo.
- Cuarto o espacio de entrada de servicios.
- Administración, etiquetado y pruebas.
- Sistema de puesta a tierra para telecomunicaciones.

2.1.9. Redes VLAN

Una **VLAN**, acrónimo de *virtual LAN* (**red de área local virtual**), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local

Una VLAN consiste en dos o más redes de computadoras que se comportan como si estuviesen conectados al mismo PCI, aunque se encuentren físicamente conectados a diferentes segmentos de una red de área local (LAN). Los administradores de red configuran las VLAN mediante software en lugar de hardware, lo que las hace extremadamente fuertes.

2.1.9.1. Clasificación

Aunque las más habituales son las **VLAN basadas en puertos** (nivel 1), las redes de área local virtuales se pueden clasificar en cuatro tipos según el nivel de la jerarquía OSI en el que operen:

- **VLAN de nivel 1 (por puerto)**. También conocida como “port switching”. Se especifica qué puertos del switch pertenecen a la VLAN, los miembros de dicha VLAN son los que se conecten a esos puertos. No permite la movilidad de los usuarios, habría que reconfigurar las VLAN si el usuario se mueve físicamente. Es la más común y la que se explica en profundidad en este artículo.
- **VLAN de nivel 2 por direcciones MAC**. Se asignan hosts a una VLAN en función de su dirección MAC. Tiene la ventaja de que no hay que reconfigurar el dispositivo de conmutación si el usuario cambia su localización, es decir, se conecta a otro puerto de ese u otro dispositivo. El principal inconveniente es que si hay cientos de usuarios habría que asignar los miembros uno a uno.
- **VLAN de nivel 2 por tipo de protocolo**. La VLAN queda determinada por el contenido del campo tipo de protocolo de la trama MAC. Por ejemplo, se asociaría VLAN 1 al protocolo IPv4, VLAN 2 al protocolo IPv6, VLAN 3 a AppleTalk, VLAN 4 a IPX...
- **VLAN de nivel 3 por direcciones de subred (subred virtual)**. La cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece. En este tipo de VLAN son los paquetes, y no las estaciones, quienes pertenecen a la VLAN. Estaciones con múltiples protocolos de red (nivel 3) estarán en múltiples VLAN.

- **VLAN de niveles superiores**. Se crea una VLAN para cada aplicación: FTP, flujos multimedia, correo electrónico. La pertenencia a una VLAN puede basarse en una combinación de factores como puertos, direcciones MAC, subred, hora del día, forma de acceso, condiciones de seguridad del equipo.

2.1.9.2. Protocolos

Durante todo el proceso de configuración y funcionamiento de una VLAN es necesaria la participación de una serie de protocolos entre los que destacan el IEEE 802.1Q, STP y VTP (cuyo equivalente IEEE es GVRP). El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN. El cometido principal de Spanning Tree Protocol (STP) es evitar la aparición de bucles lógicos para que haya un sólo camino entre dos nodos. VTP (*VLAN Trunking Protocol*) es un protocolo propietario de Cisco que permite una gestión centralizada de todas las VLAN.

El **protocolo de etiquetado IEEE 802.1Q** es el más común para el etiquetado de las VLAN. Antes de su introducción existían varios protocolos propietarios, como elISL (*Inter-Switch Link*) de Cisco, una variante del IEEE 802.1Q, y el VLT (*Virtual LAN Trunk*) de 3Com. El IEEE 802.1Q se caracteriza por utilizar un formato de trama similar a 802.3 (Ethernet) donde solo cambia el valor del campo Ethertype, que en las tramas 802.1Q vale 0x8100, y se añaden dos bytes para codificar la prioridad, el CFI y el VLAN ID. Este protocolo es un estándar internacional y por lo dicho anteriormente es compatible con *bridges* y *switches* sin capacidad de VLAN.

Las VLAN y Protocolos de Árbol de Expansión. Para evitar la saturación de los *switches* debido a las tormentas *broadcast*, una red con topología redundante tiene que tener habilitado el protocolo STP. Los *switches* intercambian mensajes STP BPDU entre sí, Bridge Protocol Data Units) para lograr que la topología de la red sea un árbol (no tenga enlaces redundantes) y solo haya activo un camino para ir de un nodo a otro. El protocolo STP/RSTP es agnóstico a las VLAN, MSTP (IEEE 802.1Q) permite crear árboles de expansión diferentes y asignarlos a

grupos de las VLAN mediante configuración. Esto permite utilizar enlaces en un árbol que están bloqueados en otro árbol.

En los dispositivos Cisco, VTP (*VLAN trunking protocol*) se encarga de mantener la coherencia de la configuración VLAN por toda la red. VTP utiliza tramas de nivel 2 para gestionar la creación, borrado y renombrado de las VLAN en una red sincronizando todos los dispositivos entre sí y evitar tener que configurarlos uno a uno. Para eso hay que establecer primero un dominio de administración VTP. Un dominio VTP para una red es un conjunto contiguo de *switches* unidos con enlaces *trunk* que tienen el mismo nombre de dominio VTP.

Los *switches* pueden estar en uno de los siguientes modos: servidor, cliente o transparente. «Servidor» es el modo por defecto, anuncia su configuración al resto de equipos y se sincroniza con otros servidores VTP. Un *switch* en modo cliente no puede modificar la configuración VLAN, simplemente sincroniza la configuración sobre la base de la información que le envían los servidores. Por último, un *switch* está en modo transparente cuando solo se puede configurar localmente pues ignora el contenido de los mensajes VTP.

VTP también permite «podar» (función VTP *prunning*), lo que significa dirigir tráfico VLAN específico solo a los conmutadores que tienen puertos en la VLAN destino. Con lo que se ahorra ancho de banda en los posiblemente saturados enlaces *trunk*.

2.1.9.3. Gestion de la pertenencia a una Vlan

Las dos aproximaciones más habituales para la asignación de miembros de una VLAN son las siguientes: VLAN estáticas y VLAN dinámicas.

Las **VLAN estáticas** también se denominan VLAN basadas en el puerto. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un *switch* o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a

la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el *switch*.

En ella se crean unidades virtuales no estáticas en las que se guardan los archivos y componentes del sistema de archivos mundial

En las **VLAN dinámicas**, la asignación se realiza mediante paquetes de *software* tales como el CiscoWorks 2000. Con el VMPS (acrónimo en inglés de *VLAN Management Policy Server* o Servidor de Gestión de Directivas de la VLAN), el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo. En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN. Se puede consultar el *software*FreeNAC para ver un ejemplo de implementación de un servidor VMPS.

2.1.9.4. VLAN basadas en el puerto de conexión

Con las VLAN de nivel 1 (basadas en puertos), el puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la misma VLAN. Habitualmente es el administrador de la red el que realiza las asignaciones a la VLAN. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

Los puertos de un *switch* pueden ser de dos tipos, en lo que respecta a las características VLAN: puertos de acceso y puertos *trunk*. Un **puerto de acceso** (*switchport mode access*) pertenece únicamente a una VLAN asignada de forma estática (VLAN nativa). La configuración predeterminada suele ser que todos los puertos sean de acceso de la VLAN1. En cambio, un **puerto trunk** (*switchport mode trunk*) puede ser miembro de múltiples VLAN. Por defecto es miembro de todas, pero la lista de las VLAN permitidas es configurable.

El dispositivo que se conecta a un puerto, posiblemente no tenga conocimiento de la existencia de la VLAN a la que pertenece dicho puerto. El dispositivo simplemente sabe que es miembro de una subred y que puede ser capaz de hablar con otros miembros de la subred simplemente enviando información al segmento cableado. El switch es responsable de identificar que la información viene de una VLAN determinada y de asegurarse de que esa información llega a todos los demás miembros de la VLAN. El switch también se asegura de que el resto de puertos que no están en dicha VLAN no reciben dicha información.

Este planteamiento es sencillo, rápido y fácil de administrar, dado que no hay complejas tablas en las que mirar para configurar la segmentación de la VLAN. Si la asociación de puerto a VLAN se hace con un ASIC (acrónimo en inglés de Application-Specific Integrated Circuit o Circuito integrado para una aplicación específica), el rendimiento es muy bueno. Un ASIC permite que el mapeo de puerto a VLAN sea hecho a nivel hardware

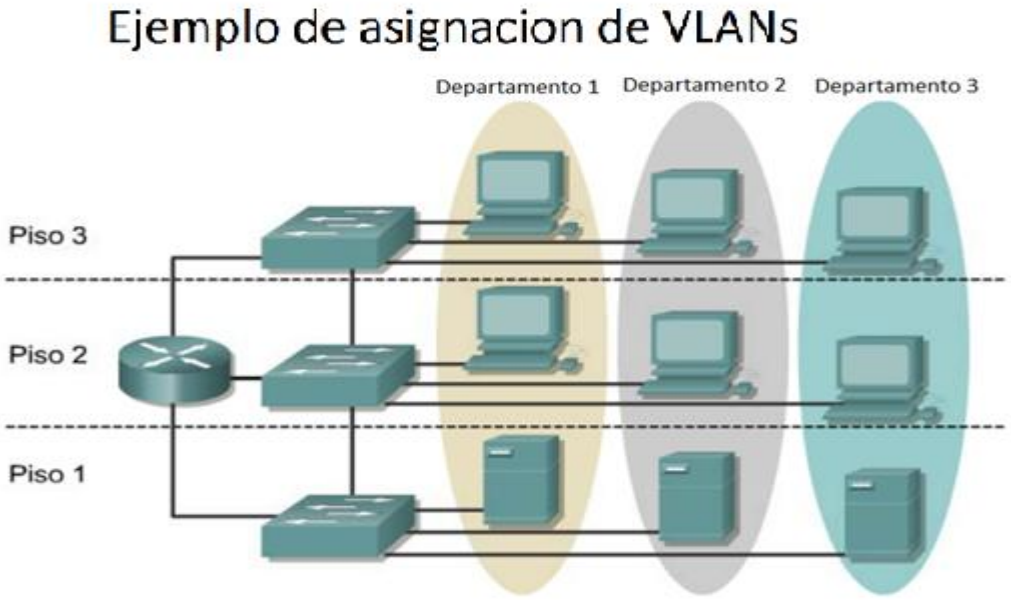


Gráfico 18: VLANs

2.2 REDES WLAN (WIRELESS LAN)

Las redes de área local inalámbricas (WLANs) constituyen en la actualidad una solución tecnológica de gran interés en el sector de las comunicaciones inalámbricas de banda ancha. Estos sistemas se caracterizan por trabajar en bandas de frecuencia exentas de licencia de operación, lo cual dota a la tecnología de un gran potencial de mercado y le permite competir con otro tipo de tecnologías de acceso inalámbrico de última generación como UMTS y LMDS, pues éstas requieren de un importante desembolso económico previo por parte de los operadores del servicio. Ahora bien, ello también obliga al desarrollo de un marco regulatorio adecuado que permita un uso eficiente y compartido del espectro radioeléctrico de dominio público disponible.

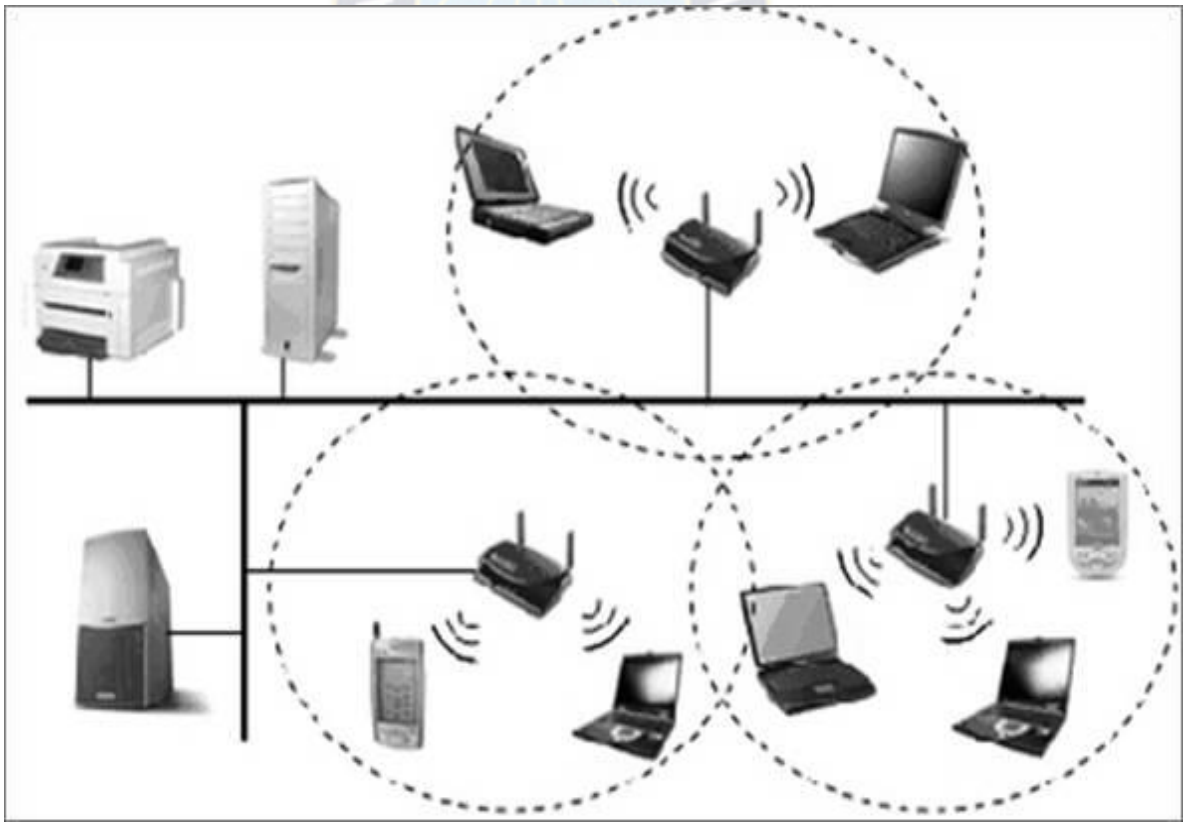


Grafico 19: Red Wireless Lan (WLAN).

Originalmente las redes WLAN fueron diseñadas para el ámbito empresarial. Sin embargo, en la actualidad han encontrado una gran variedad de escenarios de aplicación, tanto públicos como privados: entorno residencial y del hogar, grandes redes corporativas, PYMES, zonas industriales, campus universitarios, entornos hospitalarios, ciber-cafés, hoteles, aeropuertos, medios públicos de transporte, entornos rurales, etc. Incluso son ya varias las ciudades en donde se han instalado redes inalámbricas libres para acceso a Internet.

Básicamente, una red WLAN permite reemplazar por conexiones inalámbricas los cables que conectan a la red los PCs, portátiles u otro tipo de dispositivos, dotando a los usuarios de movilidad en las zonas de cobertura alrededor de cada uno de los puntos de acceso, los cuales se encuentran interconectados entre sí y con otros dispositivos o servidores de la red cableada. Entre los componentes que permiten configurar una WLAN se pueden mencionar los siguientes: terminales de usuario o Clientes (dotados de una tarjeta interfaz de red que integra un transceptor de radiofrecuencia y una antena), puntos de acceso y controladores de puntos de acceso, que incorporan funciones de seguridad, como autorización y autenticación de usuarios, firewall, etc.

El futuro de la tecnología WLAN pasa necesariamente por la resolución de cuestiones muy importantes sobre seguridad e interoperabilidad, en donde se centran actualmente la mayor parte de los esfuerzos. Sin embargo, desde el punto de vista de los usuarios, también es importante reducir la actual confusión motivada por la gran variedad de estándares existentes.

2.2.1 Estándares de Wlan

Los estándares son desarrollados por organismos reconocidos internacionalmente, tal es el caso de la IEEE (Institute of Electrical and Electronics Engineers) y la ETSI (European Telecommunications Standards Institute

Entre los principales estándares se encuentran:

- IEEE 802.11: El estándar original de WLANs que soporta velocidades entre 1 y 2 Mbps.
- IEEE 802.11a: El estándar de alta velocidad que soporta velocidades de hasta 54 Mbps en la banda de 5 GHz.
- IEEE 802.11b: El estándar dominante de WLAN (conocido también como Wi-Fi) que soporta velocidades de hasta 11 Mbps en la banda de 2.4 GHz.
- HiperLAN2: Estándar que compite con IEEE 802.11a al soportar velocidades de hasta 54 Mbps en la banda de 5 GHz.
- HomeRF: Estándar que compite con el IEEE 802.11b que soporta velocidades de hasta 10 Mbps en la banda de 2.4 GHz.

Están	**Velocidad**	**Interfase**	**Ancho de**	**Frecu**
802.11	11 Mbps	DSSS	25 MHz	2.4
802.11	54 Mbps	OFDM	25 MHz	5.0
802.11	54 Mbps	OFDM/DS	25 MHz	2.4
Home	10 Mbps	FHSS	5 MHz	2.4
HiperL	54 Mbps	OFDM	25 MHz	5.0
5-UP	108 Mbps	OFDM	50 MHz	5.0

Tabla 2.1: Principales estándares WLAN.

DSSS: Direct Sequence Spread Spectrum.
OFDM: Orthogonal Frequency Division Multiplexing. FHSS: Frequency Hopping Spread Spectrum.
5-UP: 5-GHz Unified Protocol (5-UP), Protocolo Unificado de 5 GHz propuesto por Atheros Communications.

El gran éxito de las WLANs es que utilizan frecuencias de uso libre, es decir no es necesario pedir autorización o algún permiso para utilizarlas. Aunque hay que tener en mente, que la normatividad acerca de la administración del espectro varía de país a país. La desventaja de utilizar este tipo de bandas de frecuencias es que las comunicaciones son propensas a interferencias y errores de transmisión.
Estos errores ocasionan que sean reenviados una y otra vez los paquetes de información. Una razón de error del 50% ocasiona que se reduzca el caudal eficaz real (throughput) dos terceras partes aproximadamente. Por eso la velocidad máxima especificada teóricamente no es tal en la realidad. Si la especificación IEEE 802.11b nos dice que la velocidad máxima es 11 Mbps, entonces el máximo caudal eficaz será aproximadamente 6 Mbps y menos.

Para reducir errores, el 802.11a y el 802.11b automáticamente reducen la velocidad de información de la capa física. Así por ejemplo, el 802.11b tiene tres velocidades de información (5.5, 2 y 1 Mbps) y el 802.11a tiene 7 (48, 36, 24, 18, 12, 9 y 6 Mbps). La velocidad máxima permisible sólo es disponible en un ambiente libre de interferencia y a muy corta distancia.

La transmisión a mayor velocidad del 802.11a no es la única ventaja con respecto al 802.11b. También utiliza un intervalo de frecuencia más alto de 5 GHz. Esta banda es más ancha y menos atestada que la banda de 2.4 GHz que el 802.11b comparte con teléfonos inalámbricos, hornos de microondas, dispositivos Bluetooth, etc. Una banda más ancha significa que más canales de radio pueden coexistir sin interferencia.

Sin bien, la banda de 5 GHz tiene muchas ventajas, también tiene sus problemas. Las diferentes frecuencias que utilizan ambos sistemas significan que los productos basados en 802.11a no son interoperables con los 802.11b. Esto significa que aunque no se interfieran entre sí, por estar en diferentes bandas de frecuencias, los dispositivos no pueden comunicarse entre ellos. Para evitar esto, la IEEE desarrolló un nuevo estándar conocido como 802.11g, el cual extenderá la velocidad y el intervalo de frecuencias del 802.11b para así hacerlo totalmente compatible con los sistemas anteriores.

Sin embargo, no será más rápido que el estándar 802.11a y según políticas de los fabricantes han retardado el estándar 801.11g.

La demora en la ratificación del 802.11g ha obligado a muchos fabricantes irse directamente por el 802.11a donde existe una gran variedad de fabricantes de chips [circuitos integrados] tales como Atheros, National Semiconductor, Resonext, Envara, inclusive Cisco Systems quien adquirió a Radiata, la primer compañía en desarrollar un prototipo en 802.11a en el 2000.

Como otro intento de permitir la interoperatibilidad entre los dispositivos de bajas y altas velocidades, la compañía Atheros Comunications, Inc. (http://www.atheros.com/) propuso unas mejoras a los estándares de WLANs de la IEEE y la ETSI. Este nuevo estándar conocido como 5-UP (5 GHz Unified Protocol) permite la comunicación entre dispositivos mediante un protocolo unificado a velocidades de hasta 108 Mbps.

Ambas especificaciones, la 802.11a (IEEE) y la HiperLAN2 (ETSI) son para WLANs de alta velocidad que operan en el intervalo de frecuencias de 5.15 a 5.35 GHz. La propuesta de Atheros es para mejorar esos protocolos y proveer compatibilidad hacia atrás para productos que cumplan con las especificaciones existentes, además de permitir nuevas capacidades. El radio espectro asignado para el 802.11a y el HiperLAN2 es dividido en 8 segmentos o canales de 20 MHz cada uno. Cada canal soporta un cierto número de dispositivos; dispositivos individuales pueden transitar a través de segmentos de red como si fueran teléfonos móviles de una estación a otra. Este espectro de 20 MHz para un segmento de red soporta 54 Mbps de caudal eficaz compartido entre los dispositivos en el segmento en un tiempo dado.

2.2.2 Hardware para Wlan

- *Cliente:* cada ordenador que acceda a la red como cliente debe estar equipado con una tarjeta WiFi. Las más comunes son de tipo PC Card (para portátiles) aunque pueden conectarse a una ranura PCI estándar mediante una tarjeta adaptadora.
- *Punto de Acceso:* hace las veces del hub o switch tradicional. Envía cada paquete de información directamente al ordenador indicado con lo que mejora sustancialmente la velocidad y eficiencia de la red. Es normalmente una solución hardware.
- *Antena:* se utilizan solamente para amplificar la señal, así que no siempre son necesarias. Las antenas direccionales emiten en una sola dirección y es preciso orientarlas "a mano". Dentro de este grupo están las de Rejilla, las Yagi, las parabólicas, las "Pringles" y las de Pane. Las antenas omnidireccionales emiten y reciben señal en 360º.
- *Pigtail:* es simplemente el cable que conecta la antena con la tarjeta de red. Es el único cable necesario en una WLAN y hay que vigilar posibles pérdidas de señal.

2.2.3 Topología de las redes Wlan

Depende de la funcionalidad con la que se desee montar este tipo de redes, se puede hacer de 2 modos distintos: Ad-Hoc o lo que es lo mismo, redes punto a punto o bien por infraestructura.

2.2.3.1 Redes Ad-Hoc (punto a punto). El estándar denomina a este modo como un servicio básico independiente (IBSS) con un coste bajo y flexible. Las comunicaciones entre los múltiples nodos se establecen sin el uso de ningún servidor u otro medio como pueden ser los puntos de acceso o Access Point (AP).

Uno de los métodos básicos para encaminar paquetes en este modo, seria tratando a cada uno de los nodos que forman la red como un router y utilizando entre ellos un protocolo convencional (como puede ser los basados en el vector de distancia) para encaminarlos hacia su destino

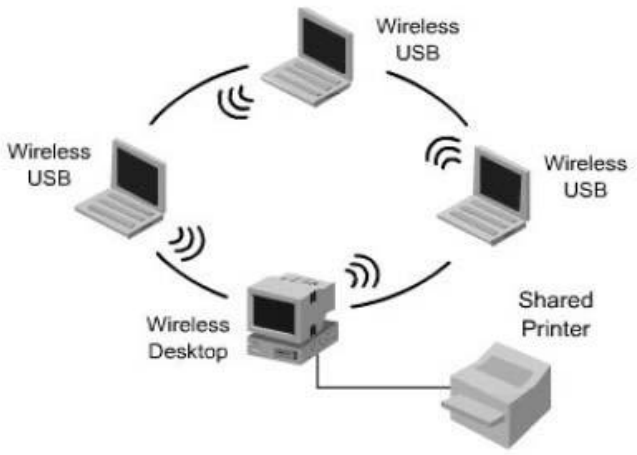


Grafico 20: Redes Punto a Punto.

2.2.3.2 Redes de infraestructura. En este modo, cada cliente de la red envía todas sus comunicaciones a una central o punto de acceso (AP, Access Point). Para efectuar el intercambio de datos, previamente los clientes y los puntos de acceso establecen una relación de confianza.

Los APs, pueden emplearse dentro de la Wireless Lan como:

- Gateway: para redes externas (Internet, intranet, etc.).

- Bridge: hacia otros Access Points para extender los servicios de acceso.

- Router: de datos entre el área de cobertura, abarcando los 100-150mts en un entorno cerrado (dependiendo de la disposición y objetos que bloqueen las ondas de radio) o los 300mts en espacios abiertos.

Estos puntos de acceso tienen un límite de 64 NICs (Network Interface Cards) dentro de su área de actuación. Para paliar este problema se opta por poner en funcionamiento varios APs al mismo tiempo, ampliando así las posibilidades de roaming de un equipo móvil sin perder la conexión.

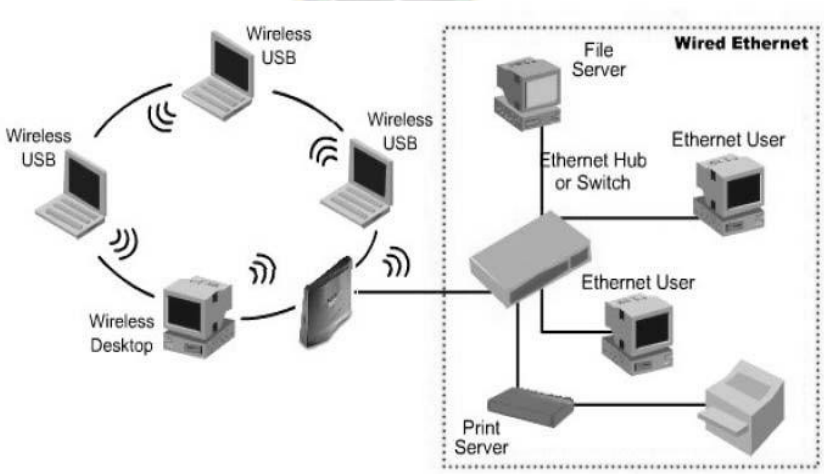


Grafico 21 : Redes WLAN y LAN.

2.2.4 Seguridades de Wlans

2.2.4.1 WEP (Protocolo de equivalencia con red cableada). La seguridad de la red es extremadamente importante, especialmente para las aplicaciones o programas que almacenan información valiosa. WEP cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire.

Cuanto más larga sea la clave, más fuerte será el cifrado. Cualquier dispositivo de recepción deberá conocer dicha clave para descifrar los datos. Las claves se insertan como cadenas de 10 o 26 dígitos hexadecimales y 5 o 13 dígitos alfanuméricos.

La activación del cifrado WEP de 128 bits evitará que el pirata informático ocasional acceda a sus archivos o emplee su conexión a Internet de alta velocidad. Sin embargo, si la clave de seguridad es estática o no cambia, es posible que un intruso motivado irrumpa en su red mediante el empleo de tiempo y esfuerzo.
Por lo tanto, se recomienda cambiar la clave WEP frecuentemente. A pesar de esta limitación, WEP es mejor que no disponer de ningún tipo de seguridad y debería estar activado como nivel de seguridad mínimo.

2.2.4.2 WPA (Wi-Fi Protected Access). WPA emplea el cifrado de clave dinámico, lo que significa que la clave está cambiando constantemente y hacen que las incursiones en la red inalámbrica sean más difíciles que con WEP. WPA está considerado como uno de los más altos niveles de seguridad inalámbrica para su red, es el método recomendado si su dispositivo es compatible con este tipo de cifrado. Las claves se insertan como de dígitos

alfanuméricos, sin restricción de longitud, en la que se recomienda utilizar caracteres especiales, números, mayúsculas y minúsculas, y palabras difíciles de asociar entre ellas o con información personal. Dentro de WPA, hay dos versiones de WPA, que utilizan distintos procesos de autenticación:

Para el uso personal doméstico. El Protocolo de integridad de claves temporales (TKIP) es un tipo de mecanismo empleado para crear el cifrado de clave dinámico y autenticación mutua. TKIP aporta las características de seguridad que corrige las limitaciones de WEP. Debido a que las claves están en constante cambio, ofrecen un alto nivel de seguridad para su red.

Para el uso en empresarial/de negocios. El Protocolo de autenticación extensible (EAP) se emplea para el intercambio de mensajes durante el proceso de autenticación. Emplea la tecnología de servidor 802.1x para autenticar los usuarios a través de un servidor RADIUS (Servicio de usuario de marcado con autenticación remota). Esto aporta una seguridad de fuerza industrial para su red, pero necesita un servidor RADIUS.

WPA2 es la segunda generación de WPA y está actualmente disponible en los AP más modernos del mercado. WPA2 no se creó para afrontar ninguna de las limitaciones de WPA, y es compatible con los productos anteriores que son compatibles con WPA.

La principal diferencia entre WPA original y WPA2 es que la segunda necesita el Estándar avanzado de cifrado (AES) para el cifrado de los datos, mientras que WPA original emplea TKIP. AES aporta la seguridad necesaria para cumplir los máximos estándares de nivel de muchas de las agencias del gobierno federal. Al igual que WPA original, WPA2 es compatible tanto con la versión para la empresa como con la doméstica.

La tecnología SecureEasySetup™ (SES) de Linksys o AirStation OneTouch Secure System™ (AOSS) de Buffalo permite al usuario configurar una red y activar la seguridad de Acceso protegido Wi-Fi (WPA) simplemente pulsando un botón. Una vez activado, SES o AOSS crea una conexión segura entre sus dispositivos inalámbricos, configura automáticamente su red con un Identificador de red inalámbrica (SSID) personalizado y habilita los ajustes de cifrado de la clave dinámico de WPA. No se necesita ningún conocimiento ni experiencia técnica y no es necesario introducir manualmente una contraseña ni clave asociada con una configuración de seguridad tradicional inalámbrica.

CAPITULO III

INGENIERIA DEL PROYECTO

3.1 Fase I: Análisis del Sistema Actual

En esta fase se identifica y se analiza la red actual existente en la Unidad Educativa Region de Murcia “La Primera”. Cabe destacar que aunque tienen una red establecida pero no regida por ningún control o norma la misma no puede monitorearse de manera efectiva y lo que se ve a simple vista es un cableado totalmente desordenado

3.1.1 Infraestructura de la Red

Dentro de la institución no había ningún documento acerca de la infraestructura ni de otras características de la red. Sin embargo como la red existente es pequeña la misma se representó con el diagrama lógico de la Fig. 3.1

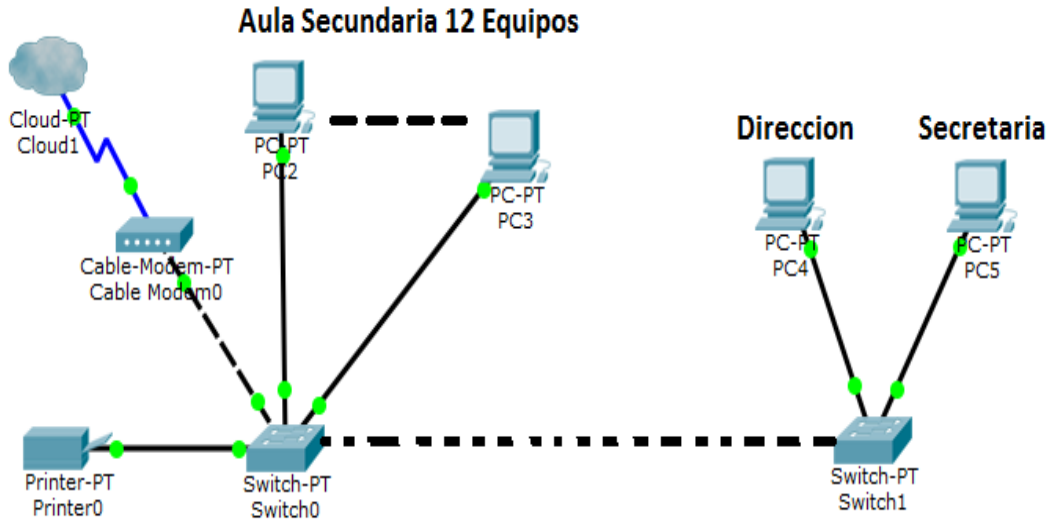


Fig 3.1. Infraestructura lógica de la red Existente

La Unidad Educativa Región de Murcia “La Primera” está constituido por una red en algunos de sus departamentos con conmutadores (Switch) de 8 puertos y 16 puertos. El cableado está conformado por diferentes categorías (3, 4 y 5) en una instalación improvisada.

3.1.2 Identificación y evaluación de los dispositivos de red actuales.

En esta parte se identificaron y evaluaron los dispositivos de red en la institución. En la tabla 1 se muestran los dispositivos de red actuales. Estas especificaciones se obtuvieron directamente de los manuales de usuarios de los dispositivos. Las características de las placas de red se muestran más adelante.

Dispositivo	Características
Switch	8 puertos
Switch	16 puertos
Pc	14 Equipos

Tabla 1. Lista de dispositivos de red actuales

3.1.3 Caracterización del cableado y los medios de transmisión

Para evaluar los cables de red disponibles y corroborar su buen funcionamiento se usara un probador de cables de par trenzado, el cual es un aparato que sirve para medir la continuidad de cada uno de los ocho alambres trenzados que componen el cables.

Esta herramienta permite verificar la correcta disposición de los alambres de acuerdo a la norma con la cual se instaló EIA/TIA 568A y EIA/TIA 568B

Se hizo una inspección visual a las áreas anteriormente expuestas y se pudieron detectar algunas Anomalías.

Además, es sabido que el cable actualmente utilizado, unido a su agotada vida útil, impide llevar bien las señales y pierda tanto la calidad como la cantidad de la información, debido a problemas de diafonía, perturbación e interferencia en su trayecto.

Por esto, es necesario hacer una reestructuración de la infraestructura de red, cambiando el cableado que se encuentre en estado crítico, acondicionando los cuartos de cableado bajo un estándar actualizado, así como los equipos de red basados en concentradores y plantear a corto plazo el cambio de toda la infraestructura de switches por una más avanzada y que pueda soportar velocidades de 1 Gbps a nivel del backbone y puertos a nivel del cliente a 10/100 Mbps.

3.1.4 Análisis de la evaluación de los equipos

Se realizó una exhaustiva revisión de los equipos y se determinó lo siguiente

a) Los equipos tienen todos los requisitos de hardware y software necesarios para conectarse en un ares LAN.

b) Los equipos requieren un mantenimiento a nivel de software como desfragmentación del disco duro, escaneo con antivirus, eliminación de archivos temporales ya que en algunos de ellos se observan ciertas anomalías como el acceso fallido a determinadas carpetas del sistema y ventanas emergentes al iniciar el sistema operativo.

c) Los equipos han sufrido ataque continuos de virus informáticos e instalación de software espía, los puntos que tienen acceso a internet pueden ingresar a cualquier tipo de página web, a la vez descargar música y juegos, obteniendo como resultado la utilización de programas que violenten la seguridad de la red.

d) Con relación a los switchs, estos no están en capacidad de poder soportar una cantidad considerable de clientes accesando a aplicaciones simultáneamente El grado de obsolescencia de estos switchs es del 100%, ya que los equipos están descontinuados por parte del proveedor. Tienen limitaciones en la obtención de repuestos, o dificultades para recibir el soporte técnico adecuado.

Este grupo de requerimientos, conforman el cuadro de necesidades sujetas a ser superadas a traves de la implementación de un servicio de administración de la red.

3.1.5 Verificación del estado de la red

Ya que la equipos conectados a la red son pocos, la verificación de conectividad es sencilla y bien se podrán usar herramientas de testeo que el mismo Windows integra.

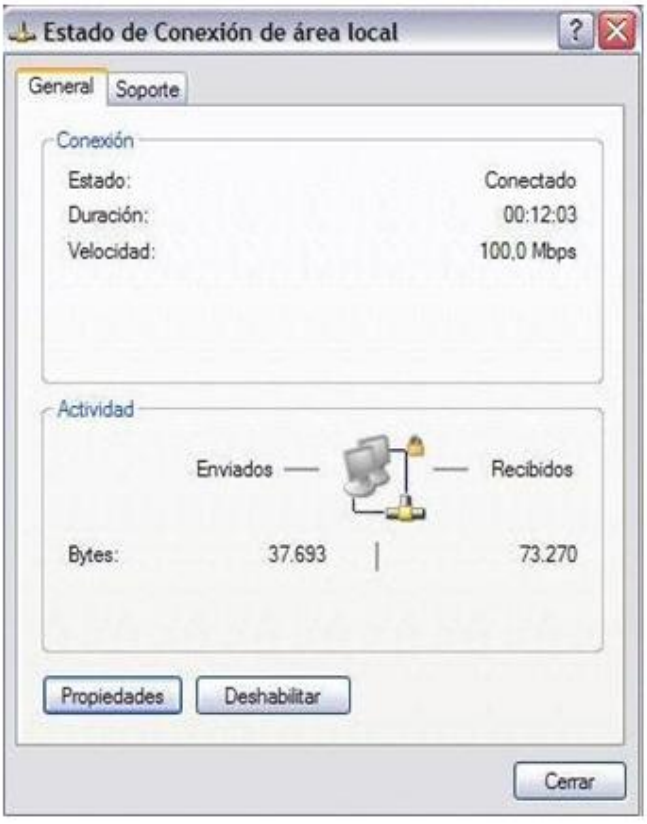


Fig. 3.2 Detalles de la conexión de Red

Fig. 3.3 Detalles del comando *ipconfig/all*

3.2 Fase II: Diseño de la topología y de los servicios de red.

En esta fase se muestran las actividades realizadas con respecto al tipo de red, topología a usar, tecnología de red, medio físico, diseño lógico, diseño físico y el diseño de seguridad.

3.2.1 Selección del tipo de arquitectura de red

De acuerdo a la función de los equipos, existen tres tipos de arquitecturas básicas que determinan como un nodo de una red se comunica con otro dentro de la misma red, estas son: Maestro/Esclavo, punto a punto (peer-to-peer) y cliente/servidor

La mayoría de las respuestas coinciden con la necesidad de implantar una red cliente-servidor, esta arquitectura brindara un nivel alto de seguridad el cual consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo.

3.2.2 Selección de la topología de red y tecnología de red

3.2.2.1 Selección de la topología de red

Existen varias topologías de red básicas topologías de red básicas (bus, estrella, anillo y malla), pero también existen redes hibridas que combinan una o más de las topologías anteriores en una misma red.
Se opto por diseñar la red en topología estrella en la cual las estaciones estarán conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

Dado su transmisión, esta red en estrella tendra un nodo central *activo* que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Se utiliza sobre todo en redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en estas sería el enrutador, el conmutador o el concentrador, por el que pasan todos los paquetes.

Ventajas

- Tiene los medios para prevenir problemas.
- Si una PC se desconecta o se rompe el cable solo queda fuera de la red esa PC.
- Fácil de agregar, reconfigurar arquitectura PC.
  Fácil de prevenir daños o conflictos.
- Permite que todos los nodos se comuniquen entre sí de manera conveniente. El mantenimiento resulta más económico y fácil que la topología bus.

Desventajas

- Si el nodo central falla, toda la red se desconecta.
- Es costosa, ya que requiere más cable que las topologías bus o anillo.
- El cable viaja por separado del switch a cada computadora.

3.2.2.2 Selección de la tecnología de red

Toda la información que se transporta a través de una LAN se hace en BANDABASE, es decir las señales no se modulan. Como NO se modulan, la propagación de las señales a través de una LAN se ve limitada en cobertura, menos de 100 metros.

Si se modularan las señales en una LAN, la cobertura sería mucho mayor, pero los dispositivos de interfaz de red [tarjeta de red] saldrían mas caros, debido a que tienen que implementar un modulador y demodulador.

Por este motivo, se empleara la tecnología **Fast Ethernet** que opera a 100 Mbps sobre par trenzado con la posibilidad de alternarla con la tecnología Gigabit Ethernet que opera a 1000 Mbps (1 Gbps) sobre fibra óptica y cable par trenzado, la selección de esta tecnología se baso en el estándar internacional de la IEEE 802.3, la misma especifica que los estándares Ethernet están denotados por tres partes. Por ejemplo,

10BaseT, **10** se refiere a la velocidad en Mbps; **Base**, debido a que se transmite en banda base (sin modular) y **T** se refiere al medio, en este caso par trenzado.

Velocidades: 10, 100, 1000 Mbps

Medios: 2,5 = coaxial; T = par trenzado y F = fibra óptica

Para este caso en particular seria 100BaseTX, esto es igual a 100Mbps, banda base, utilizando par trenzado UTP Cat5e y 100BaseFX lo que es igual a 100Mbps, banda base, utilizando par de fibra óptica.

3.2.3 Selección del medio de comunicación

Basado en el estándar internacional 802.3 el cual especifica redes Ethernet se hizo la selección del medio de comunicación. El cable de par trenzado sin blindar UTP(Unshielded Twisted Pair) el cual consiste de 4 pares de alambres calibre 24 AWG (0,50mm) forrados con FEP (propileno-etil eno fluorado). La cubierta exterior es de PVC. Ver figura 3.4

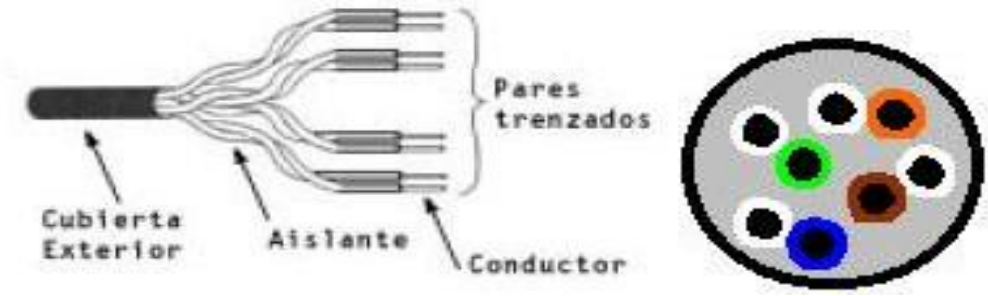


Fig. 3.4 Cable UTP

La categoría 5e, es uno de los grados de cableado UTP descritos en el estándar EIA/TIA 568B el cual se utiliza para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100 Mbps a frecuencias de hasta 100 Mhz.

Está diseñado para señales de alta integridad. Estos cables pueden ser blindados o sin blindar. Este tipo de cables se utiliza a menudo en redes de ordenadores como Ethernet, y también se usa para llevar muchas otras señales como servicios básicos de telefonía, token ring, y ATM.

Descripción

Este cable hara la conexión principal entre el panel de distribución y la roseta del puesto de trabajo, para conectar el switch a otros PCs, y para conectar dichos dispositivos entre sí.

En conclusión y después de haber examinado estándares y normas acerca de este tema el cable a utilizar para la instalación de esta red es **cable de par trenzado UTP Cat 5e** : actualmente definido en TIA/EIA-568- B. Frecuentemente usado en redes fast ethernet (100 Mbit/s) y gigabit ethernet (1000 Mbit/s). Diseñado para transmisión a frecuencias de hasta 100 MHz.

3.2.4 Diseño lógico de la red

El diseño lógico de la red comprendió la selección y especificación de:

Diseño del protocolo de red

Las direcciones IP

La estructura de enrutamiento

Creacion de Areas con VLANs

3.2.4.1 Diseño del protocolo de red

La familia de protocolos de Internet es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se le denomina *conjunto de protocolos TCP/IP*, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

Ventajas e inconvenientes

El conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web. Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

Un inconveniente de TCP/IP es que es más difícil de configurar y de mantener que NetBEUI o IPX/SPX; además es algo más lento en redes con un volumen de tráfico medio bajo. Sin embargo, puede ser más rápido en redes

con un volumen de tráfico grande donde haya que enrutar un gran número de tramas.

El conjunto TCP/IP se utiliza tanto en redes empresariales como por ejemplo en campus universitarios o en complejos empresariales, en donde utilizan muchos enrutadores y conexiones a mainframe o a ordenadores UNIX, así como también en redes pequeñas o domésticas, y hasta en teléfonos móviles y en domótica.

3.2.4.2 Diseño de direcciones lógicas

Es bien sabido que para que dos computadoras puedan comunicarse entre si necesitan estar identificadas en la red a través de direcciones IP. Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualme nte una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar. Esta dirección puede cambiar 2 ó 3 veces al día; y a esta forma de asignación de dirección IP se denomina una *dirección IP dinámica* (normalmente se abrevia como *IP dinámica)*.

Modo de asignación de las direcciones

El modo como se asignara las direcciones IP a los equipos se determinó que sería de forma estatica ya que cuenta con distintas direcciones de red
Se asignara la dirección IP de forma manual en cada equipo

Rango de direcciones para los equipos de la red

Para los equipos se utilizara el rango de direcciones IP de las siguientes redes:

Red 172.16.1.0 255.255.255.0 (172.16.1.1 – 172.16.1.254)

Red 172.16.2.0 255.255.255.0 (172.16.2.1 – 172.16.2.254)

Red 172.16.3.0 255.255.255.0 (172.16.3.1 – 172.16.3.254)

Además de las direcciones de red de los equipos se definieron aquí los nombres que tendrán los equipos en la red, así como sus descripciones. En la tabla 2 se muestran las características y direcciones IP de los equipos separados por áreas.

3.2.5 Determinación de los dispositivos de interface para la red

En esta actividad nos abocamos a determinar los componentes del cableado estructurado señalando ciertas consideraciones a tener presente para los mismos.. Para la determinación de los componentes del cableado estructurado se realiza en dos grupos.

3.2.5.1 Grupo uno. Compuesto por: Cableado Horizontal

El cable usado para el cableado horizontal es el UTP categoría 5ecubierto con PVC. Cuando se está diseñando una instalación es importante conocer donde estarán ubicadas las estaciones de trabajo en relación al cuarto de cableado principal. Se debe planificar la instalación de manera que el cable no exceda de 90 metros. Cuando se tienden cables a través de paredes y cielo raso, estos se deben tener tan lejos como se pueda de las luces fluorescentes, paneles eléctricos, este tipo de cable no debe halarse demasiado ya que si queda muy tenso puede perder rendimiento. Este cable horizontal es el que va desde el wallplate hasta la regleta preconectarizada (Patch Panel).

Regleta Preconectarizada (Patch Panel)

El sistema de parcheo de datos elegida para este proyecto son los "Patch-panels". Los Patch-panels son Dispositivos de interconexión que normalmente vienen para montaje en Rack estándar de 19", pero podrían venir en montaje sobre pared. En su parte posterior presentan un grupo de conectores tipo 110, que mediante circuitos impresos se interconectan con los conectores de la parte frontal, los cuales son del tipo modular de 8 pines (RJ-45). El más pequeño que se obtiene comercialmente es de 12 conectores, pudiéndose obtener de 16, 24, 48 y 96 conectores o puertos. Estos pueden venir de acuerdo a las normas de colores T568A o T568B y últimamente en ambas. Cada conector dentro de un Patch-panel viene claramente numerado tanto en parte posterior como anterior, además en la parte frontal debe tener una sección donde poder escribir información adicional de identificación.

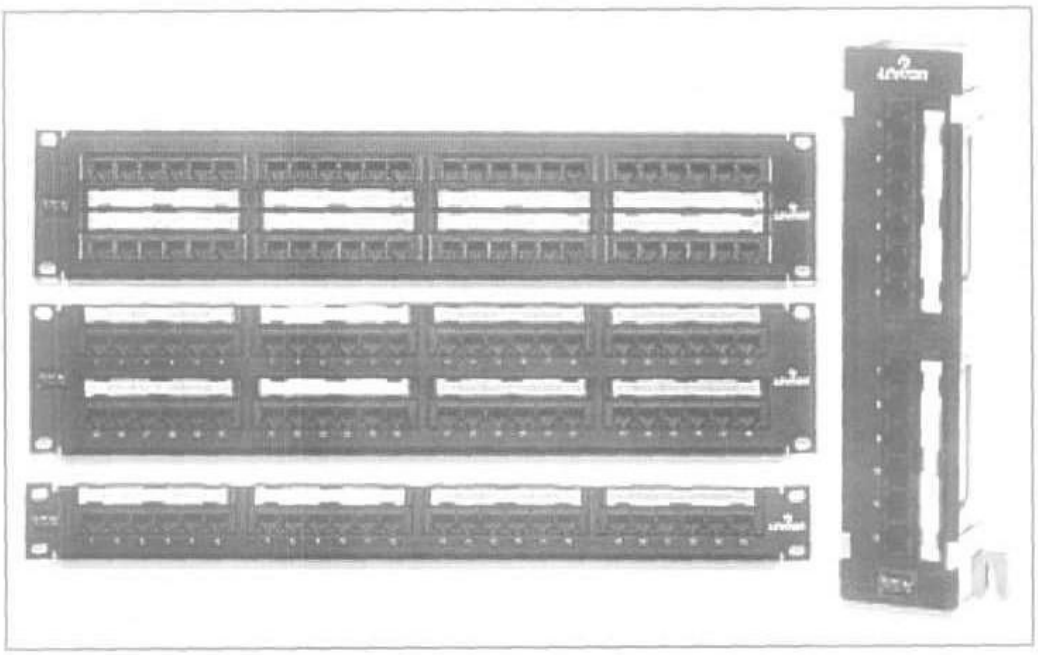


Fig. 3.5 Patch-Panels (Cortesía de Leviton)

Armario de distribución (Rack o gabinete).

En este armario debe converger todo el cableado del piso al cual él sirve y desde él debe partir el cableado (Backbone) al Armario de Telecomunicaciones Principal (MC). El TR debe contener el sistema de conectorización que permita efectuar el parcheo HC ("Horizontal Cross-Connection) y debe tener capacidad para eventuales incorporaciones de equipos activos. La primera decisión es la ubicación, a continuación las dimensiones y finalmente la distribución interna.

Ubicación del TR

Para la elección del lugar óptimo se deben tomar en consideración las siguientes directrices:

- Los TR de todos los pisos deberían ubicarse alineados verticalmente. ?
- Es recomendable ubicar el TR cerca del centro teórico de la Universidad
- Se debe colocar alejado de fuentes de interferencia electromagnética (motores de elevadores, unidades centrales de aire acondicionado y cualquier motor de alta potencia)
- No debe ser comp artido con otras funciones, especialmente la de almacenaje de materiales de limpieza.
- Debe estar incorporado a la climatización del edificio, por ejemplo no se deben usar áreas de las escaleras de emergencia o estacionamientos de vehículos.

Dimensiones de l TR

La tabla 2. indica las dimensiones que deberían tener los TR tomando en consideración el volumen de usuarios potenciales a servir. El cálculo se realiza estimando un potencial usuario cada 10 m2 de espacio efectivo de oficina disponible (se excluyen áreas de circulación, espera, baños, almacenaje, etc.)

Número de potenciales usuarios	Tipo de Armario
10	Gabinete de Pared
11-50 (Opcion 1)	Gabinete empotrado
11-50 (Opcion 2)	Cuarto 3.0 x 2.2 metros
51-80	Cuarto 3.0 x 2.8 metros
81-	Cuarto 3.0 x 3.4 metros

Tabla 2. Dimensiones del TR

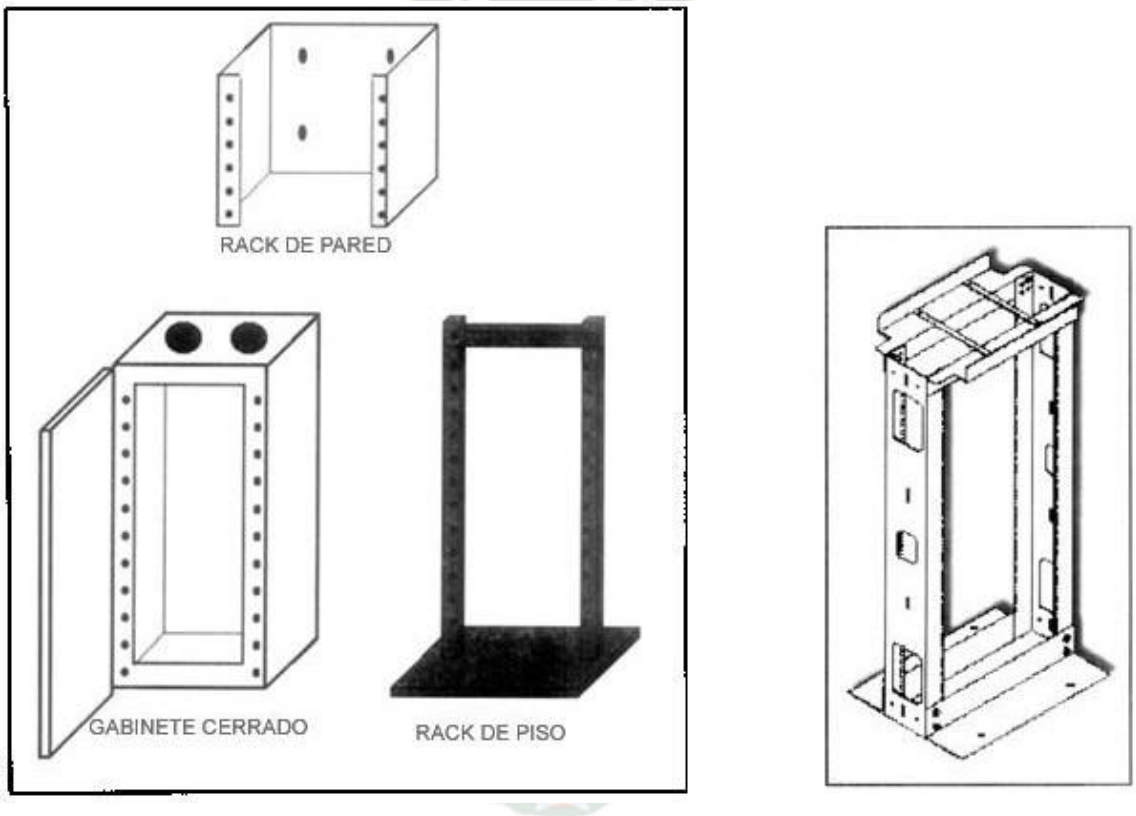


Fig. 3.5 Sistemas de Bastidores

Tubería.

La tubería para el cableado horizontal es de tipo Conduit, la cual es fabricada de plástico resistente o acero galvanizado, todas estas tuberías tendrán un diámetro según la cantidad de cableado que transporten.

Las tuberías deben estar sujetas a la pared con sus propios medios, y deben utilizar componentes como cajas de paso, medios de fijación, éstas no deben pasar a menos de 20 cm. de separación de las líneas de corriente de 120 Voltios.

3.2.5.2 Grupo dos. Compuesto por:

Conectores de hardware.

Los componentes de los conectores de hardware pueden ser fijos o modulares. Los componentes fijos cuentan con un conjunto de puertos Rj-45 que no pueden ser reconfigurados para otras aplicaciones. Este tipo de componentes son usualmente utilizados para sistemas de instalaciones pequeñas y simples con pocos cambios y poco crecimiento.

Los componentes modulares pueden ser configurados y reconfigurados para una variedad de aplicaciones y pueden ofrecer código de colores para identificar fácilmente múltiples sistemas corriendo sobre el mismo sistema de cableado estructurado. Es importante decidir qué tipo de estándar de cable se va a utilizar. El estándar de cableado indica cuales cables de color, del cableado horizontal se va a conectar al conector Rj-45. El estándar preferido es el T5668A, pero el T568B se está volviendo muy popular, éste apunta que no importa usar cualquier cable, pero debe asegurar de utilizar que todos los componentes utilizan el mismo esquema.

Código de Colores

Se debe respetar la norma pues si no se estaría enfrentando a transmitir por pares abiertos. La incorrecta colocación de los pares en los conectores representa la causa más común de deterioro en la velocidad de una red.

Lamentablemente existe una grave inconsistencia en la normativa al existir dos códigos de colores válidos para la conexió n del cableado. En la figura 3.6

se puede observar ambos. Sin entrar en detalle de las razones de luchas corporativas que provocaron este exabrupto, el instalador tiene como objetivo no mezclar en un segmento de cable ambos estándar pues la comunicación será imposible, pues los pares 1-2 y 3-6 estarían cruzados.

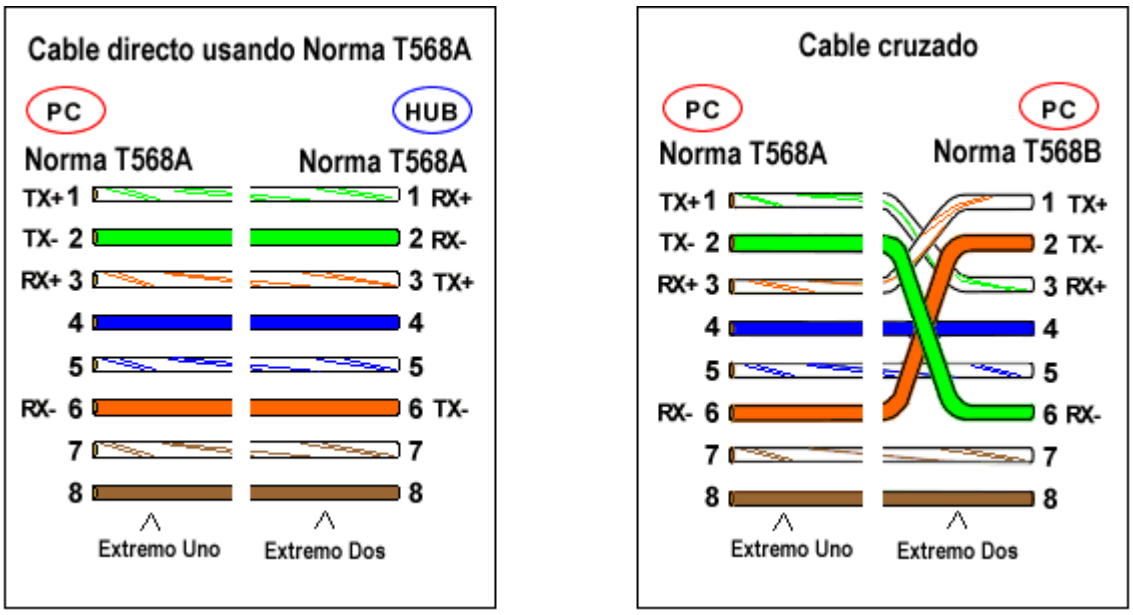


Fig. 3.6 Código de Colores

La norma T568A es la oficial y la T568B se considera opcional, por lo que en nuevas instalaciones es recomendable usar la primera, sin embargo se debe aclarar que por razones de organización, es importante mantener una instalación con un solo estándar de colores, es decir que si se inició por ejemplo con T568B, todas las ampliaciones y remodelaciones mantendrán ese código.

Las hembras (jacks) y los sistemas de parcheo (patch-panels) vienen marcados de fábrica y se debe asegurar que los materiales de parcheo y de las tomas sean de un mismo estándar.

Cables de Interconexión (Patch-Cords)

Aunque el cable de interconexión entre el computador y la toma no está incluida dentro del cableado horizontal, es evidente que forma parte vital

dentro del sistema de cableado y este hecho fue corregido en el boletín TSB75 e incorporado en la norma nueva, que establece que la certificación de un cableado debe incluir este cable, llamando esta prueba "la prueba de canal" (Channel Test). Este cable de interconexión debe ser de la misma categoría del cableado horizontal. El cable es de 4 pares pero no sólido sino multifilar "stranded", para estar preparado al movimiento propio de un cable expuesto al tránsito de oficinas (por ejemplo a la limpieza diaria). Como norma de facto se considera un conector apropiado el que tenga una capa de oro en sus contactos de no menos 50 micrones de espesor, para poder soportar 100 ciclos de conexión-desconexión.

Adicionalmente se considera altamente recomendable que dicho conector esté terminado en la sección del cable en una bota con el objeto de protegerse de los movimientos antes indicados. La longitud máxima de este cable de interconexión será de 5 metros, muchos diseñadores consideran que la mejor opción para este cable de interconexión es la adquisición original de fábrica con la longitud requerida, no menor de dos metros para el cable de interconexión que va en la toma. La bota protectora más recomendada es la que protege el "clip" del conector, comercialmente conocida como
"snagless boot"

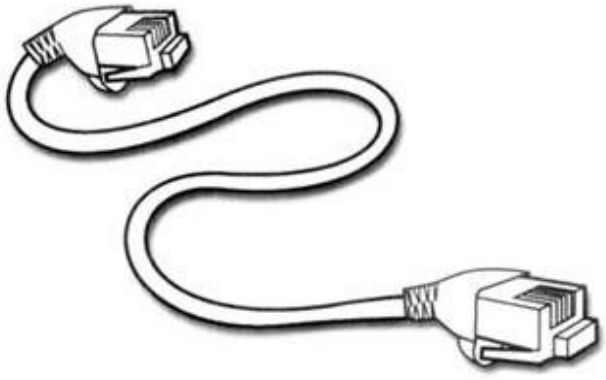


Fig.3.7 Cable de Interconexió n "Patch-Cords"

Toma (Wallplate)

Para cada puesto de trabajo sería recomendable la existencia de una toma doble de conector modular de 8 posiciones (RJ-45), uno de al menos categoría 3 (recomendación categoría 5e) y otro al menos categoría 5e. Una opción muy utilizada es la de dos salidas habilitando inicialmente sólo una, para lo cual se coloca una conector "ciego" (blank panel) en la apertura no usada.

Un inconveniente comercial encontrado es que los cordones telefónicos vienen en conector RJ-11. El Conector RJ-11 "calza" en el RJ-45, pero si las medidas de dicho Conector no son estandarizadas se pueden dañar los pines 1 y 8 del RJ-45, por lo que la toma quedaría inutilizada para futuro uso en datos. Las opciones para resolver este inconveniente son:

1. Cambiar el plug RJ11 por RJ45 en los cordones telefónicos pero para que quede mecánicamente sólido se debe conseguir el plug RJ45 para cable plano .
2. Colocar en la toma un adaptador externo de RJ45 (macho) a RJ11 (hembra), los cuales son extremadamente costosos y sobresalen de la toma.

Lo que hacen muchos instaladores es "violar" la norma y colocan un jack RJ-11 con cable de 2 pares en categoría 3. La consecuencia es la pérdida de flexibilidad en el cableado pues esa salida está condenada a ser telefónica para siempre (no es estructurada). Se debe admitir que baja bastante el costo del cableado (en los armarios se usarían bloques 66) y es práctico, pero se debe aclarar que esta salida de la toma no forma parte del cableado estructurado.

La placa "wallplate" que era más usada era la de color blanco de perfil sobresaliente. Algunos diseños arquitectónicos no comulgaban con dicho tipo de toma y la mayoría de los fabricantes han cambiado y tienen opciones de color y/o bajo perfil (low profile) disponibles, las cuales se están imponiendo rápidamente. La placa debe disponer un sistema de identificación que permita numerar

individualmente cada conector e identificar claramente la toma. Nos encontramos con un inconveniente estético en casi toda Latinoamérica, pues masivamente se utilizan las placas provenientes de Estados Unidos y Asia que son verticales y blancas, y los tomacorrientes de alimentación AC, siguen el estándares europeos: son horizontales y beige. En numerosas instalaciones se solicita a los instaladores que coloquen las placas en posición horizontal para mantener la línea de diseño y debemos aclarar que estas placas no están concebidas para ser ubicadas de esta manera, por lo que se genera un estrés adicional al patch-cord y la lectura de los sistemas de identificación se dificulta.

Concentradores de cableado.

El sistema de administración de la red interna estará constituido por concentradores apilables para redes Ethernet con la capacidad de crecer a medida que surjan nuevas necesidades de puntos activos de conexión. Los concentradores sirven de punto de conexión de todas las estaciones, por lo tanto, deben proveer la información y facilidad necesaria para realizar las funciones de administración. En la práctica, el uso de concentradores se ha desechado puesto que aumentan el riesgo de colisiones, siendo sustituidos por los conmutadores o switches.

3.2.6 Determinar confiabilidad de la red

Básicamente, el presente diseño debe evitar en lo posible las fallas antes de que sucedan, y ser capaz de restituir el servicio en el menos tiempo posible para que los usuarios puedan continuar su trabajo en forma regular.

Prevenir las colisiones, monitorear el tráfico, usar dispositivos que segmenten la red y hacer pruebas de carga máxima son solo algunos de los mecanismos para evaluar y prevenir contingencias.

3.2.7 Determinar la conectividad de la red

La conectividad de la red está diseñada para dar servicio por medios alámbricos e inalámbricos que se han desarrollado notablemente en tiempo reciente, y como están contemplados en el diseño original serán añadidos fácilmente sin modificaciones extensivas a la red, pues solo con la incorporación de Wireless Routers y Access Points se puede alcanzar esa funcionalidad.

3.2.8 Seguridad del Sistema

Para que exista una normativa de seguridad en el sistema propuesto esta debe definirse como la incapacidad de ser usada como medio de acceso de intrusos para obtener información sensible o disponer de recursos o servicios solo autorizado para los usuarios internos. Por esta razón se consideraron 2 aspectos importantes, los cuales fueron siguientes:

* Seguridad lógica.
* Seguridad física.

3.2.8.1 Seguridad Lógica

La seguridad lógica de los sistemas de información, se refiere a las contraseñas, password, claves de acceso o autorizaciones que se encuentran dentro del software de aplicación y que permiten a los usuarios del sistema tener acceso a todas o a una(s) parte(s) del mismo.

Debido a que el sistema propuesto sólo será utilizado por los analistas de redes, para poder accesar a los switches y routers vía consola (directo al equipo) o Telnet (vía remota), se necesitarán nombres de usuarios y sus respectivos passwords. Los equipos Cisco instalados permiten estas características e incluso, pueden guardarse registros de auditoría en los casos de accesos remotos

utilizando un servidor de TACACS (algo así como en ambientes de Windows NT/2000). Las claves son guardadas mediante el uso de técnicas especiales en dicho servidor.

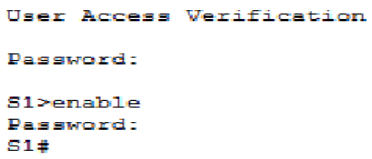


Fig. 3.7 Acceso por Consola

Tanto vía consola o remota, se necesitan dos passwords para accesar al switch y al router; el primero que es el modo ejecutable y el segundo es el modo privilegiado. Este último es el que permite accesar a las partes de configuración confidenciales del equipo y cambiar la configuración del mismo.

Configuracion de contraseñas en cada switch y router

```
Switch>en
Switch#conf t
Switch(config)#enable secret cisco
Switch(config)#line con 0
Switch(config-line)# password cisco
Switch(config-line)# logging synchronous
Switch(config-line)# login
Switch(config-line)#
Switch(config-line)#line vty 0 4
Switch(config-line)# password cisco
Switch(config-line)# logging synchronous
Switch(config-line)# login
Switch(config-line)#exit
```

3.2.8.2. Seguridad Física

Los equipos se instalaran en los cuartos de cableado, ubicados en el Área Técnica, donde el acceso se encuentra restringido a personas no autorizadas.

Con relación al sistema de seguridad del edificio, la seguridad existente en la universidad, debido a su carácter de Institución Educativa y además su condición de edificio administrativo principal en el Estado, donde se encuentran las oficinas de los directivos y coordinación, lo hace más invulnerable a la entrada de sospechosos a cualquier parte.

Los cuartos de cableado cuentan con un sistema de aire acondicionado que mantienen en un ambiente fresco y aislado de las altas temperaturas a los equipos.

Con respecto a dispositivos en caso de ausencia de electricidad, los equipos de redes estarán conectados a líneas preferenciales, las cuales están bajo sistemas de UPS, capaces de controlar las variaciones bruscas de voltaje que pueden afectarlos.

3.3 Fase III: Planificación de la implementación de la red

Esta planificación se refiere al conjunto de actividades y tareas a realizar para el logro de la implementación de la red. Cada actividad incluyó su descripción, recursos materiales, monetarios y humanos necesarios y el intervalo de duración de cada una. La planificación también incluyó el establecimiento de los procedimientos o instrucciones para llevar a cabo cada tarea

Dispositivos	Cantidad
Switch	3
Router	1
Router inalámbrico	1
Impresoras	2
Pc's	39

Dispositivos que van a ser usados en la red

Areas	Nro. de Equipos
Area Secundaria	12
Area Primaria	12
Direccion	2
Secretaria	1
Bibloteca	12

Equipos PC divididas por areas

3.4 Fase IV: Construcción del diseño

Esta fase comprendió la elaboración del diseño de la red conformada por un router, switch y PCs conectados a éste que represento una simulación de lo que realmente haría el sistema, lo que llevo a verificar como se podría dejar de trabajar con el actual e ir reemplazándolo con la propuesta actual. Es decir, la implementación de una pequeña red de 'laboratorio' que simulo la red de datos y que cumplió con el objetivo general del proyecto para así tener una idea amplia que más adelante en gran escala se utilizaría para realizar la y llevar a cabo la propuesta.

El diseño proporcionaría información con relación a la factibilidad del concepto. El sistema diseñado podrá ser modificado con facilidad y en el momento que así lo requiera según sea el caso. La versión modificada se tomará, a su vez, como prueba para obtener información valiosa en el diseño final.
Como se observa en la Fig 3.8 en el sistema propuesto se añadió varios elementos a la red que cuenta con la organización requerida para el sistema, dividida en 3 areas Secundaria, Primaria y Dirección también se añadió la Zona WIFI

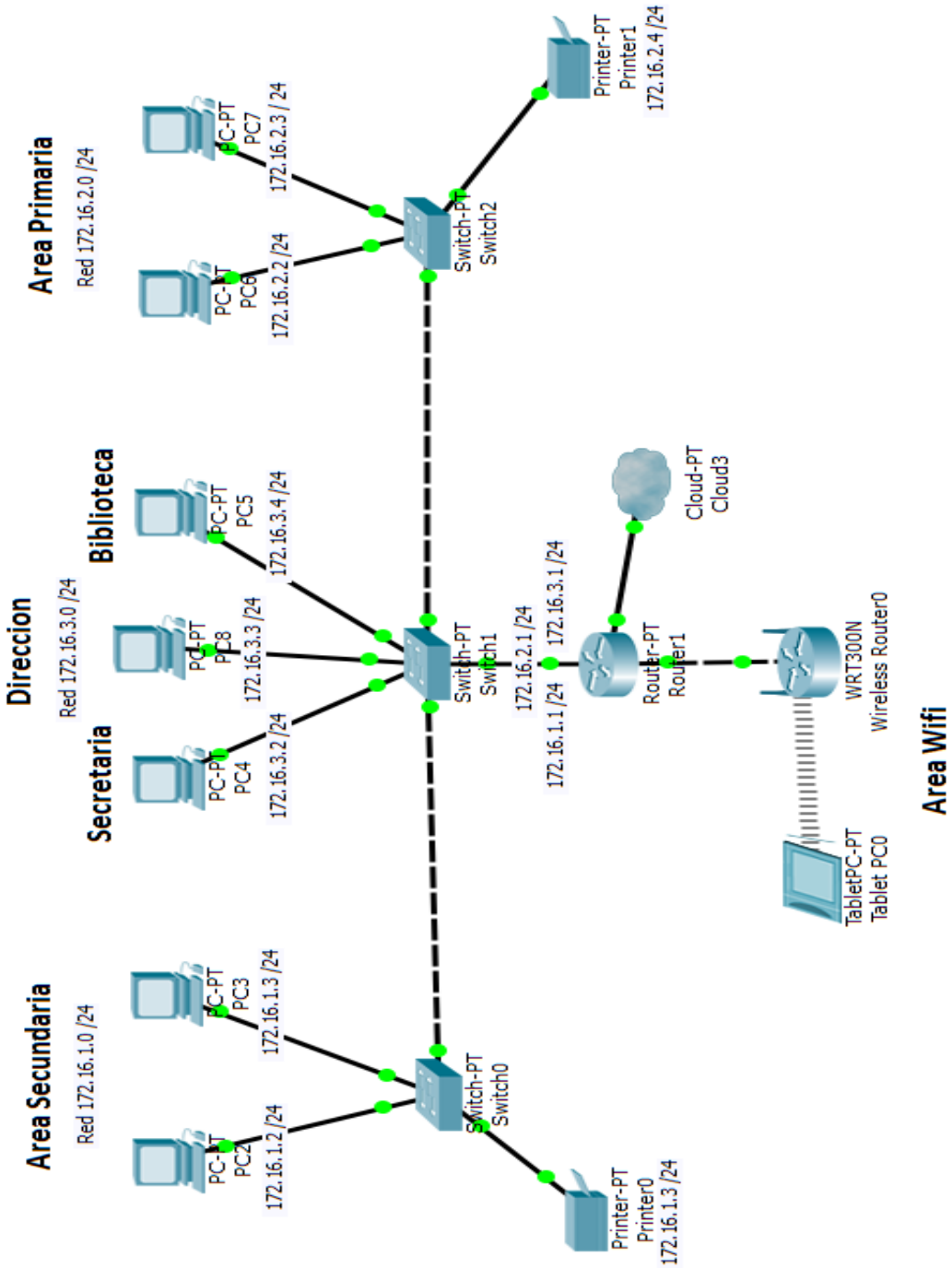


Figura 3.8 Diseño de la red

3.4.1 Características de los equipos de conectividad.

Switch (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Un conmutador en el centro de una red en estrella. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Área Network- Red de Área Local).

Enrutador (en inglés: router), ruteador o encaminador es un dispositivo de hardware para interconexión de red de computadoras que opera en la capa tres (nivel de red). Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. En este diseño se instalará un router en la sede para contener y proteger la red, sin que por ello estén impedidos de transmitir información o recibir información de direcciones autorizadas. Además, así se pueden aplicar políticas de tiempo de uso y contenido de Internet, un tema sensible para la mayoría de los jefes de departamento.

3.4.2 Características del software requerido.

Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. Si no se dispone de ningún sistema operativo de red, los equipos no pueden compartir recursos y los usuarios no pueden utilizar estos recursos.

Dependiendo del fabricante del sistema operativo de red, tenemos que el software de red para un equipo personal se puede añadir al propio sistema operativo del equipo o integrarse con él.

El software del sistema operativo de red se integra en un número importante de sistemas operativos conocidos, incluyendo Windows 2000 Server/Professional, Windows XP profesional SP2 Cada configuración (sistemas operativos de red y del equipo separado, o sistema operativo combinando las funciones de ambos) tiene sus ventajas e inconvenientes. Por tanto nuestro trabajo como investigadores en redes, es determinar la configuración que mejor se adapte a las necesidades de nuestra red.
El sistema operativo elegido es Windows 7

3.4.3 Caracteristicas del hardware requerido

Equipos PC

Se usara los equipos ya existentes con el nuevo sistema operativo Windows 7 y también los nuevos equipos Quipus que esta dando el gobierno asi aprovechando todos los elementos y tratar de ahorrar lo mas que se pueda para que el proyecto sea mas factible.

Switches

Los switches son importantes en la configuración de la red es por eso que se escogió el siguiente con todas sus características:

Cisco Small Business 200 Series Switch SG200-26 - Switch - managed - 24 x 10/100/1000

Precio 350$

Layer 2 Switching	
Spanning Tree Protocol (STP)	Standard 802.1d STP support Fast convergence using 802.1w (Rapid Spanning Tree [RSTP]), enabled by default
Port grouping	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) ● Up to 4 groups ● Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad link aggregation
VLAN	Support for up to 256 VLANs simultaneously (out of 4096 VLAN IDs). 16 VLANs supported in SG200-08 and SG200-08P Port-based and 802.1Q tag-based VLANs
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS
Internet Group Management Protocol (IGMP) versions 1 and 2 snooping	IGMP limits bandwidth-intensive multicast traffic to only the requesters; supports 256 multicast groups
Head-of-line (HOL) blocking	HOL blocking prevention
Security	
IEEE 802.1X (Authenticator role)	802.1X: RADIUS authentication, MD5 hash

Port security	Locks MAC addresses to ports, and limits the number of learned MAC addresses
Storm control	Broadcast, multicast, and unknown unicast
DoS prevention	DoS attack prevention
Quality of Service	
Priority levels	4 hardware queues
Scheduling	Strict priority and weighted round-robin (WRR) Queue assignment based on differentiated services code point (DSCP) and class of service (802.1p/CoS)
Class of service	Port based, 802.1p VLAN priority based, IPv4/v6 IP precedence/type of service (ToS)/DSCP based, Differentiated Services (DiffServ)
Rate limiting	Ingress policer, per VLAN and per port

Router

El router es otro elemento muy importante ya que con el haremos posible la conexión entre todos los dispositivos de la red y además en el futuro se podrá hacer uso de las muchas aplicaciones que este tiene.

Cisco RV320 Dual Gigabit WAN VPN Router Data Sheet

Precio 245$

Figure 1. Cisco RV320 Dual Gigabit WAN VPN Router

Description	Specification
Dual WAN	Dual Gigabit Ethernet Ports Failover Load balancing
Standards	802.3, 802.3u › IPv4 (RFC 791) › IPv6 (RFC 2460)
WAN Connectivity	Dynamic Host Configuration Protocol (DHCP) server, DHCP client, DHCP relay agent › Static IP › Point-to-Point Protocol over Ethernet (PPPoE) › Point-to-Point Tunneling Protocol (PPTP) › Transparent bridge › DNS relay, Dynamic DNS (DynDNS.org, 3322.org), DNS local database › IPv6
Routing protocols	› Routing Information Protocol (RIP) v1 and v2, and RIP for IPv6 (RIPng) Inter-VLAN routing Static routing VLANs supported: 7
Network Address Translation (NAT)	Port Address Translation (PAT) One-to-one NAT NAT traversal
Protocol binding	Protocols can be bound to a specific WAN port for load-balancing purposes
Network edge (DMZ)	DMZ port DMZ host
Dual USB 2.0 ports	Storage and 3G/4G modem support
Security	
Firewall	› SPI firewall Denial-of-service (DoS) prevention: ping of death, SYN flood, IP spoofing, WinNuke
Access rules	› Schedule-based access rules Up to 50 entries
Port forwarding	Up to 30 entries

Description	Specification
Port triggering	Up to 30 entries
Blocking	Java, cookies, ActiveX, HTTP proxy
Content filtering	Static URL blocking or keyword blocking
Secure management	HTTPS web access to device manager Username/password complexity enforcement
VLAN	802.1Q VLAN 7 VLANs supported
VPN	
IP Security (IPsec)	25 IPsec site-to-site tunnels for branch office connectivity 25 IPsec VPN tunnels via Cisco VPN client and third-party clients such as “The GreenBow” for remote-access VPN connectivity
SSL VPN	10 SSL VPN tunnels for remote client access
PPTP	10 PPTP tunnels for remote access
Encryption	Data Encryption Standard (DES) Triple Data Encryption Standard (3DES) Advanced Encryption Standard (AES) encryption: AES-128, AES-192, AES-256
Authentication	MD5/SHA1
IPsec NAT traversal	Supported for gateway-to-gateway and client-to-gateway tunnels
VPN pass-through	PPTP, Layer 2 Tunneling Protocol (L2TP), IPsec
Advanced VPN	Dead peer detection (DPD) Split DNS VPN backup Internet Key Exchange (IKE) with certificate
Quality of Service (QoS)	
Service-based QoS	Rate control or priority
Rate control	Upstream/downstream bandwidth per service
Prioritization types	Application-based priority on WAN port

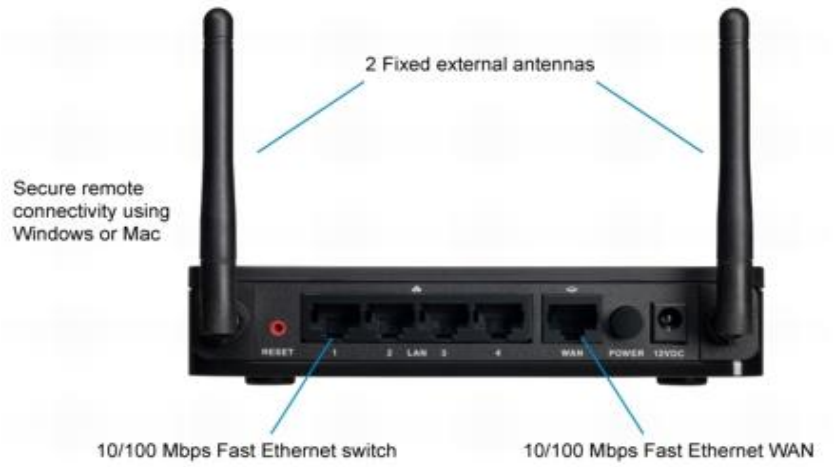
Description	Specification
Priority	Services mapped to one of two priority levels
Performance	
IPsec VPN throughput	100 Mbps
SSL VPN throughput	20 Mbps
Concurrent connections	20,000

Router inalámbrico

Simple, Secure Connectivity for the Small Office/Home Office

Cisco RV110W Wireless-N VPN Firewall **COSTO: 98$**

Back Panel of the Cisco RV110W Wireless-N VPN Firewall



Wireless LAN Specifications

Feature	Description
WLAN hardware	IEEE 802.11n standard-based access point with 802.11b/g compatibility Radio and modulation type: • 802.11b: direct sequence spread spectrum (DSSS) • 802.11g/n: orthogonal frequency division multiplexing (OFDM) • 2 omnidirectional 1.8 dBi gain fixed external antennas Operating channels: • 11 in North America • 13 in most of Europe • Automatic channel selection Transmit power: • 802.11b: 17 dBm +/- 1.5 dBm • 802.11g: 15 dBm +/- 1.5 dBm • 802.11n: 12.5 dBm +/- 1.5 dBm Receiver sensitivity: • -87 dBm at 11 Mbps • -71 dBm at 54 Mbps • -68 dBm at msc15, HT20 / -66dBm at mcs15, HT40
Wireless Domain Services (WDS)	• Allows wireless signals to be repeated by up to 3 compatible devices
Wi-Fi Multimedia (WMM)	• WMM with QoS (802.11e), WMM power save (WMM-PS)
Active WLAN clients	• Up to 32 clients
Service Set Identifiers (SSIDs)	• Up to 4 separate wireless networks

Wireless isolation	• Wireless isolation between clients
WLAN security	• WPS (Wi-Fi Protected Setup), Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) personal and enterprise, WPA2 personal and enterprise

3.4.4 Configuración IP de los equipos de la red

Las direcciones IP para cada equipo se establecerán de forma estática de acuerdo al grafico 3.8

El Area de Secundaria tendrá 12 equipos y los rangos de dirección serán :

172.16.1.2 – 172.16.1.254 de los cuales se usaran las 12 primeras

El Area de Primaria tendrá 12 equipos y los rangos de dirección serán :

172.16.2.2 – 172.16.2.254 de los cuales se usaran las 12 primeras

El Area de Direccion, Secretaria, Biblioteca constara de 15 equipos en total y los rangos de direcciones serán:

172.16.3.2 – 172.16.3.254 de las cuales se usaran las 15 primeras

Areas	Nro. de Equipos	Rango de Direcciones
Area Secundaria	12	172.16.1.2-172.16.1.14
Area Primaria	12	172.16.2.2-172.16.2.14.
Direccion	2	172.16.3.2-172.16.3.17
Secretaria	1	
Bibloteca	12	

Tabla 2 Asignacion de direcciones

3.4.5 Configuracion de los Switches

Primeramente configuraremos el protocolo VTP que facilita la configuración de VLANs en múltiples switches de manera simultanea solo con la configuración del switch denominado como servidor (server).

Para realizar la configuración de VTP, se debe configurar como troncales (trunk), las interfaces que conectan los switches entre si, para esto debemos ingresar al método de configuración global (**S1(config)#**), utilizando el comando "**interface**" seguido la interfaz correspondiente ingresamos al modo de configuración de la interfaz (**S1(config-if)#**) ("**interface range**" si queremos configurar varias interfaces a la vez) y luego utilizando el comando "**switchport mode trunk**" configuramos el puerto como troncal, luego de esto por motivos de seguridad configuramos los demás puertos como acceso ingresando al modo de configuración de interfaces (**S1(config-if-range)#**) y utilizando el comando "**switchport mode access**".

Luego debemos configurar el nombre del dominio VTP desde el modo de configuración global (**S1(config)#**) utilizando el comando "**vtp domain**" seguido del nombre del dominio (el nombre del dominio es sensible al tipo de letra), Luego asignamos una contraseña al dominio con el comando "**vtp password**" seguido de la contraseña que deseamos utilizar, luego debemos especificar el modo en el que el switch funcionara, esto con el comando "**vtp mode**" seguido del modo (**server, client, transparent**).

Luego de haber configurado VTP debemos ingresar las VLANs en el switch que esta en modo servidor para que los que están en modo cliente puedan aprender las VLANs automáticamente, esto lo conseguimos desde el modo de configuración global (**S1(config)#**) utilizando el comando "**vlan**" seguido del numero de la VLAN (**1-1005**), luego en el modo de configuración de VLAN (S1(**config-vlan)#**) asignamos un nombre a la VLAN utilizando el comando "**name**" seguido del nombre que deseamos asignar a la VLAN.
Por ultimo debemos asignar las VLAN a los puertos, esto lo conseguimos desde el modo de configuración global (S1(**config)#**) utilizando el comando "**interface**" o "**interface range**" seguido de la interfaz que deseamos asignar a una VLAN especifica, luego en el modo de configuración de interfaz utilizamos el comando "**switchport access vlan**" seguido del numero de la VLAN correspondiente.

S0

```
S0(config)#vtp domain Escuela
S0(config)#vtp password 12345
S0(config)#vtp mode client
```

S1

```
S0(config)#vtp domain Escuela
S0(config)#vtp password 12345
S0(config)#vtp mode server
```

S2

```
S3(config)#vtp domain Escuela
S3(config)#vtp password 12345
S3(config)#vtp mode client
```

Creamos las Vlans y las asignamos a cada Area en cada switch pero como usamos el protocolo VTP solo creamos las Vlans en el switch server

S0

```
S0(config)#interface fastEthernet 0/1-12
S0(config-if)#switchport mode access
S0(config-if)#switchport access vlan 10
S1(config)#interface fastEthernet 0/13-15
S1(config-if)#switchport mode trunk
```

S1

```
S1(config)#vlan 10
S1(config-vlan)#name Area_Secundaria
S1(config)#vlan 20
S1(config-vlan)#name Area_Primaria
S1(config)#vlan 30
S1(config-vlan)#name Direccion
S1(config)#interface fastEthernet 0/1-12
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config)#interface fastEthernet 0/13
S1(config-if)#switchport mode trunk
```

S2

```
S2(config)#interface fastEthernet 0/1-15
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S1(config)#interface fastEthernet 0/16
S1(config-if)#switchport mode trunk
```

3.4.6 Configuracion del Router

Inter-VLAN Routing (Router on a stick) nos brinda la facilidad de utilizar solo una interfaz para enrrutar los paquetes de varias VLANs que viajan a través del switch conectado a esa interfaz, es decir, podemos configurar varias IP de diferentes redes a varias interfaces virtuales (sub-interfaces) alojadas en una sola interfaz física.

Para realizar la configuración de Router on a stick, debemos ingresar al modo de configuración global del switch (**S1(config)#**), luego utilizando el comando "**interface**" seguido de la interfaz que deseamos configurar entramos al modo de configuracion de la interfaz (**S1(config-if)#**), luego utilizamos el comando "**switchport mode trunk**" para declarar la interfaz como troncal.

Luego en el router (R1) desde el modo de configuración global **(R1(config)#)** utilizamos el comando "**interface**" seguido de la interfaz que albergara las sub-interfaces y aplicamos el comando "**no shutdown**" desde el modo de configuracion de interfaz (**R1(config-if)#**) para encenderla, luego desde el modo de configuración global (**R1(config)#**) ingresamos nuevamente el comando "**interface**" seguido de la sub-interfaz deseada, por ejemeplo: ***fastEthernet 0/0.10****,* ingresamos al modo de configuración de la sub-interfaz (**R1(config-subif)#**), luego ingresando el comando "**encapsulation dot1Q**" seguido del numero de la VLAN que deseamos que utilice esta sub-interfaz y por ultimo utilizamos el comando "**ip address**" seguido de la direccion IP y la mascara de subred que pertenecen al rango de la red de la VLAN asignada a esta sub-interfaz.

R1

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown

R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 172.16.1.1 255.255.255.0
R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 172.16.2.1 255.255.255.0
R1(config)#interface fastEthernet 0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.16.3.1 255.255.255.0
```

3.4.7 Configuracion de la red WLAN

El funcionamiento básico de una red WLAN es utilizar ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) se conecta la red cableada de un lugar fijo mediante cableado normalizado. EL punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

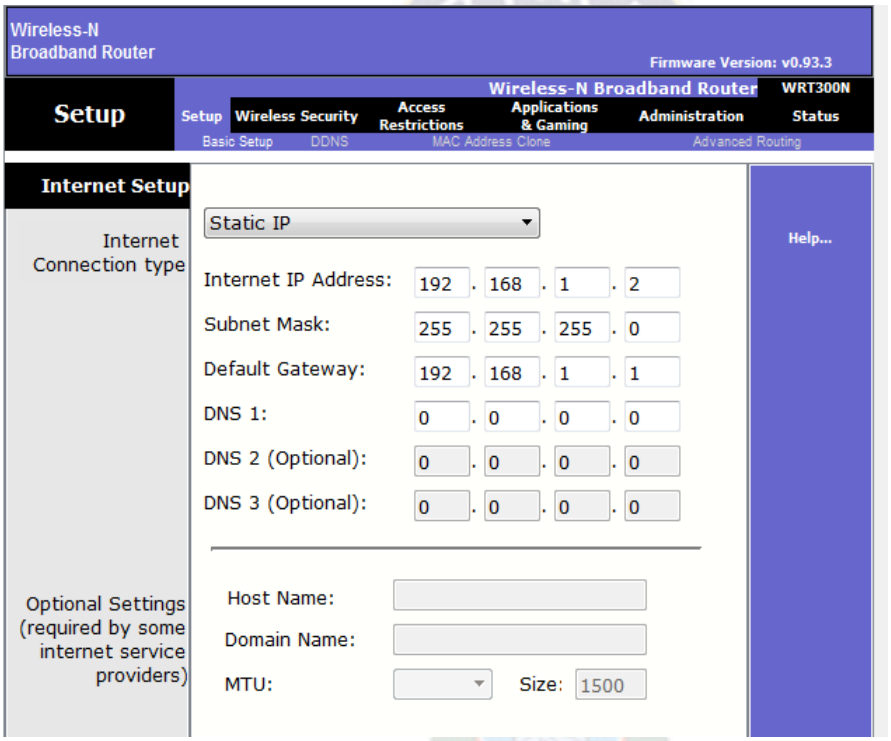
El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero se puede colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena. La naturaleza de la conexión sin cable es transparente al sistema del cliente.

Para este proyecto se procederá como primer paso encontrar un sitio central donde se ubicará el concentrador inalámbrico en este caso el **Cisco RV110W Wireless-N** el cual enviará la señal a los usuarios.

El estándar a utilizar en esta red es el 802.11b y 802.11g por lo que se configura el Router Wireless mediante la página principal del equipo para que sea compatible con ambos estándares, una vez realizadas las pruebas se comprobó que el equipo llegará con su señal hasta una distancia máxima de 85 metros en interiores con esto se verifica el alcance permitido por el fabricante que dice que el alcance de una red WLAN del estándar 802.11 es de 100 metros en interiores y de hasta 300 metros en espacios abiertos, se trabajará además con una velocidad de 54Mbps debido a que se utiliza el estándar 802.11b y 802.11g. Debido a que cada Punto de Acceso puede dar servicio a 20 equipos o más se administrará la red WLAN para evitar incremento de usuarios móviles en la red ya que la cantidad está limitada por el uso que se haga del ancho de banda, es decir, cuantos más equipos estén funcionando simultáneamente, más lenta será la transmisión, se configura el equipo para que utilice una seguridad para establecer conexión al concentrador o a la Red WLAN en este caso se utilizará WPA con algoritmo TKPI para conexión con dispositivos móviles en la cual solo los usuarios que conozcan la contraseña podrán ingresar a la red y podrán obtener los beneficios de la misma, finalmente al concentrador se le asignará una dirección IP fija en el rango de la red interna y los usuarios que se conecten a este se les proporcionará una IP otorgada por el Servidor DHCP de la red.

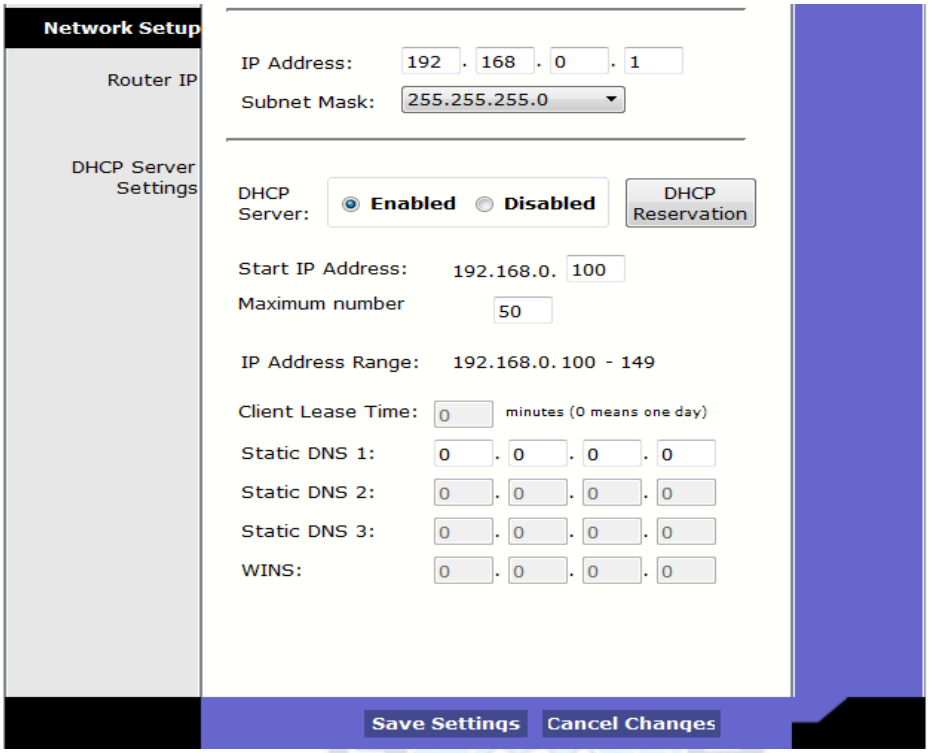
Esta red se implementó para el uso de cualquier usuario sin importar el equipo tales como: Computadores Portátiles, Pocket PC, Computadores de Escritorio, entre otros, con el requerimiento de adaptadores inalámbricos en los equipos como tarjetas PCI o PCMCIA los cuales cumplan con la norma 802.11b o 802.11g para poder ingresar a la red WLAN.

CONFIGURACION



Configuracion de las direcciones de IP Dinamicas

Una **dirección IP dinámica** es una IP asignada mediante un servidor DHCP (**Dynamic Host Configuration Protocol**) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.



3.6 Fase VI Lugar Físico de la red

La Unidad Educativa Región de Murcia “La Primera” en el cual se implementara la red se encuentra en la ciudad de El Alto aquí se mostrara fotografías del sistema que se quiere implementar

Vista del satelite

Areas de funcionamiento

Area de secundaria

Area Primaria

Direccion

3.6 Elaboracion de un Prototipo de red

Este punto comprendió la elaboración de una pequeña red conformada por un switch, router y algunos PCs conectados a éste que represento una especie de maqueta de lo que realmente haría el sistema, lo que llevo a verificar como se podría dejar de trabajar con el actual e ir reemplazándolo con la propuesta actual. Es decir, la implementación de una pequeña red de 'laboratorio' que simulo una parte de la sede y que cumplió con el objetivo general del proyecto para así tener una idea amplia que más adelante en gran escala se utilizaría para realizarla y llevar a cabo la propuesta.

El prototipo proporcionaría información con relación a la factibilidad del concepto. Fue tomado como un plan piloto o prueba del sistema. El prototipo diseñado podrá ser modificado con facilidad y en el momento que así lo requiera según sea el caso. La versión modificada se tomará, a su vez, como prueba para obtener información valiosa en el diseño final.

CAPITULO IV

ANALISIS DE COSTOS

4.1 Estudio económico del proyecto.

El análisis costo/beneficio del sistema propuesto pretende demostrar, de una manera teórica y numérica, la rentabilidad del proyecto por medio de un estudio de los costos tanto de desarrollo como de operación, y los beneficios que acarrea la implementación de la red en la Unidad Educativa Region de Murcia "La primera"

4.1.1 Estudio de Costos

Los costos, como ya se dijo, son de desarrollo y de operación. Los costos de desarrollo están determinados por: El hardware y software adquirido, recursos de procesamiento de datos necesarios para desarrollar el sistema propuesto, salario y beneficios, gastos generales, entre otros.

Los costos de operación surgen a partir de la puesta en marcha del sistema y continúan durante toda la vida útil del mismo. Estos gastos son los que representará la operación del sistema y el mantenimiento.

Los gastos están representados por la plataforma de cableado en sí (bobinas de cables UTP categoría 5e, racks abiertos, ordenadores verticales y horizontales, patch panels, conectores), gastos de personal técnico instalador y analista de redes, y gastos relacionados con la elaboración de la propuesta e informes (papel, impresora, entre otros).

Cisco Small Business 200 Series Switch SG200-26 - Switch - managed - 24 x 10/100/1000

Precio 350$

CANTIDAD 3 (1050$)

Cisco RV320 Dual Gigabit WAN VPN Router

Precio 245$

Figure 1. Cisco RV320 Dual Gigabit WAN VPN Router

CANTIDAD 1 (245$)

Cisco RV110W Wireless-N VPN Firewall

CANTIDAD 1 (98$)

Costo total de los equipos y demás elementos

Dispositivo	Cantidad	Costo/unidad	Costo Total
Cisco Small Business 200 Series Switch SG200-26 - Switch - managed - 24 x 10/100/1000	3	350$	1050$
Cisco RV320 Dual Gigabit WAN VPN Router	1	245$	245$
Cisco RV110W Wireless-N VPN Firewall	1	98$	98$
Bobina de cable UTP cat 5 (300mts)	1	70-150 $	70-150 $
			1493$

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Las redes al igual que las aplicaciones, deben moverse junto con las exigencias de los clientes, por lo cual, ambos deben ir al mismo ritmo de estos últimos. Instituciones Educativas, como es el caso de la Unidad Educativa Region de Murcia “La Primera” donde se toman decisiones importantes y en donde una compleja red LAN los envuelve, deben soportar el tráfico que por ella pasa y el flujo de la información debe ser tan rápido como las exigencias de los mismos usuarios.

El uso de cableado estructurado, plataforma de equipos switcheados y demás componentes que una red involucra, trae consigo a que se esté bien preparado para atender los requerimientos y la LAN soporte tráfico brusco en ciertas ocasiones.

El desarrollo de la infraestructura de cableado representa el punto de partida para que, en un futuro no muy lejano, pueda seguirse con la instalación de equipos más poderosos que puedan soportar velocidades de hasta 1 Gbps.

Gracias al empleo de una efectiva metodología de investigación, se logro alcanzar el mejor desarrollo para realizar el análisis, diseño y se lograra la implementación del sistema de cableado y el reemplazo de los existentes switches por otros nuevos. El análisis hizo posible diagnosticar y proponer una solución factible para satisfacer la problemática que existía en la institución; el diseño permitió elaborar el sistema propuesto de acuerdo a los requerimientos de los usuarios involucrados; y la implementación se convertirá en la solución de todas las debilidades encontradas en el sistema actual y preparación para una posible emigración de toda la plataforma de switches a una de nueva generación y mayor capacidad.

La presente investigación demostró que la estandarización de los procesos de

una organización, conlleva a obtener los mejores resultados una vez procesada la información, ya que además de los importantes beneficios que aportara el cableado y los switches presentara una nueva perspectiva de lo que puede significar una eficiente propuesta de mirar hacia dónde va la tecnología y enfocarse hacia ella.

La propuesta proporcionara a la Unidad Educativa un paso adelante en materia de avances tecnológicos, motivando así a la realización de otros proyectos, que a futuro se implementarán en otras áreas, utilizando el mismo enfoque de aprovechar los equipos existentes en el sistema actual que aún estaban en un estado funcional y que son compatibles con el nuevo cableado instalado, evitar la instalación de equipos no necesarios, para realizar tareas de manera rápida, confiable, precisa, oportuna, actualizada y segura, con el menor esfuerzo posible para obtenerla, contribuyendo así a la toma de decisiones eficiente tanto a nivel del cliente como a nivel del personal de redes.

El nuevo sistema contribuirá a una disminución de costos por horas/hombre invertidas en el mantenimiento de la infraestructura. Además, fue diseñado de una manera flexible que permite facilidad de entendimiento y modificación para los futuros cambios que se hagan en el mismo.

5.2 Recomendaciones

Después de haber implantado el sistema de cableado y la sustitución de los equipos de redes en la Unidad Educativa Region de Murcia “La Primera”, se recomienda lo siguiente:

Una vez migrada la plataforma de cableado estructurado horizontal a categoría 5e, cambiar a mediano plazo, la infraestructura de switches, a fin de poder soportar las exigencias futuras de los servicios de Tecnología de Información (dando prioridad a el tráfico de datos de las aplicaciones calidad de servicio,

conferencia multimedia, plataforma basada en Web, E-learning, E-business, high-end computing, high-end graphics, ambiente de trabajo colaborativo, etc.) y así proveer capacidad de conexión de hasta 1 Gbps a nivel estaciones especializadas y servidores.

Mantener actualizados los planos de la ubicación de los puntos de datos y cualquier modificación de configuración que se haga a los switches, principalmente a nivel de cableado, ya que es donde se encuentra el mayor número de requerimientos por parte de los clientes. Los planos deben estar a disposición de los usuarios (técnicos de cableado) para que consulten en ellos sus dudas y así atiendan los casos eficientemente.

Mantener los cuartos de cableado arreglados y limpios, y no utilizarlos como depósitos de equipos de computación desincorporados ni cualquier otro objeto que obstruya el normal desenvolvimiento de las tareas por parte del equipo de redes.

El diseño plantea a mediano plazo la implantación de enlaces a Gigabit por segundo (Gbps) desde los switches de acceso hacia el backbone de la red, y con esto se incrementaría 10 veces la velocidad de acceso a las aplicaciones web. Para ello se recomienda la adquisición de switches que tengan capacidad de Gbps a nivel de los enlaces tanto para los otros switches como para los clientes.

Ejecutar un mantenimiento preventivo, periódico y continuo, tanto del hardware como del software, al ser implementado el nuevo sistema, a fin de evitar los daños físicos y/o lógicos.

Establecer un control periódico y constante al sistema de cableado y principalmente los cuartos de cableado a través de un proceso de auditoría para verificar el total funcionamiento de los distintos componentes y realizar modificaciones o adiciones al sistema propuesto en caso necesario.

Cuidar que se cumplan con las medidas de seguridad del sistema con la finalidad de impedir la entrada de intrusos, no otorgando las claves a personas no autorizadas para mantener privada y segura la información. Además, nunca utilizar como una clave: nombres, direcciones, marcas, números de cédula, palabras de diccionario, o cualquier otro dato que sea fácil de identificar; por el contrario, usar nombres compuestos que eviten el fácil desciframiento del mismo.

Realizar continuos adiestramientos al personal involucrado como lo son: técnicos de cableado y analistas de redes, en materia de cableado, infraestructura y switches Cisco, para así obtener un mayor aprovechamiento de los equipos y tecnologías existentes en la institución por parte de estos usuarios.

Mantener un respaldo de la configuración de los equipos y del sistema operativo en áreas seguras a fin de evitar fraudes informáticos y garantizar una posible reinstalación en caso de daños lógicos al sistema. También se deben realizar respaldos periódicos de datos cuando se realicen modificaciones mayores a los equipos para garantizar la protección de la información.

Mantener siempre las condiciones ambientales adecuadas para el bienestar del hardware donde opera el sistema propuesto.

BIBLIOGRÁFIA

- Internet y Redes Inalámbricas ARIAS ARAGUEZ 510
- Redes inalámbricas en países de desarrollo
- Redes de comunicaciones
- Cisco System. (2000). Interconnecting Network Cisco Devices V1.1. USA
- Cisco System. (1999). Catalyst 5000 Family: Installation Guide, Module Installation Guide, Supervisor Engine Installation Guide. Quick Software Configuration. USA.
- Dyson, P. (1995) The Network Press Dictionary of Networking. Sybex Incorporated, USA.
- FREEDMAN, A. (1993). Diccionario de Computación. Quinta edición. Editorial Mc Graw Hill. México.
- Hucaby, David. (2001). CCNP Switching. USA.
- INTesa (1997). Cisco Catalyst 5000. Guía de Instalación y configuración. Revisión 3. Caracas, Venezuela
- WHITTEN , Jeffrey. (1997). Analisis y Diseño de Sistemas de Información. Editorial Mc Graw Hill. Madrid.
- HUIDOBRO , José Manuel. (2006). Redes y Servicios de Telecomunicaciones. Thomson Editores. Madrid .
- MENDILLO, Vicenzo. (2004). Redes de Alta Velocidad. Conatel. Venezuela.
- MORERA, Daniel. (2008). Cableado Estructurado y Fibra Óptica. Grupo Ireli. Venezuela.
- TANENBAUM, Andrew. (2003). Redes de Computadoras. Ediciones Pearson Educación. México
- TOMASI, Wayne. (2003). Sistemas de Comunicación Electrónica. Ediciones Prentice Hall. México

Sitios en Internet:

- http://www.cisco.com. Documentación de equipos switches para su configuración y software disponible vía web.
- http://www.belden.com Información acerca del cable UTP nivel 5. Catálogos, características, conectorización y estándares.
- http://www.panduit.com Conectores, patch panels, racks, organizadores, etc.
- http://es.wikipedia.org/wiki/Red_de_área_local_inalámbrica.html.
- http://es.wikipedia.org/wiki/Red_inalámbrica_municipal.html.
- http://dns.bdat.net/seguridad_en_redes_inalambricas/x187.html
- www_34t_com .html.
- http://www.ceditec.etsit.upm.es/dmdocuments/wifi.pdf
- http://www.x-net.es/tecnologia/wireless.pdf
- http://en.wikipedia.org