



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

ANÁLISIS Y PROPUESTA DE REESTRUCTURACIÓN
PARA LA OPTIMIZACIÓN DE LA RED DE CÓMPUTO
ACADÉMICO Y ADMINISTRATIVO DEL COLEGIO
ASESORÍA EDUCATIVA QUEEN MARY SCHOOL S.C.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

PRESENTA:
OSCAR ARTURO RAMÍREZ VÁSQUEZ

ASESOR DE TESIS:
ING. ENRIQUE GARCÍA GUZMÁN



MÉXICO 2008



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

A DIOS por dirigir mi vida a cada momento.

A mis Padres, y a ti mamá especialmente por todo tu apoyo y dedicación a mí esfuerzo.

A mis hermanas Ana y Erika por su apoyo incondicional.

A Miss Gena por darme la oportunidad de colaborar en el Colegio.

A mi Asesor Ing. Enrique García por su tiempo y orientación.

A mis revisores:

Ing. Martín Hernández; Ing. Hugo Portilla; M. en C. Marcelo Pérez e
Ing. Oscar Estrada. Por su tiempo y aportación en la elaboración de esta Tesis.

A todos aquéllos por su apoyo en la elaboración de esta Tesis y a la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México por darme los conocimientos y calidad académica por parte de los profesores que la integran, para el desarrollo de mi México, a fin de dar una aportación como egresado de esta gran Universidad.

Oscar Arturo

ÍNDICE

	Página
I.- INTRODUCCIÓN	3
II.-FUNDAMENTOS TEÓRICOS	5
2.1 Conceptos generales de redes y telecomunicaciones	5
2.2 Modelo de Referencia ISO-OSI	11
2.3 Protocolos de Comunicaciones	14
2.4 Cableado Estructurado	30
2.5 Redes Inalámbricas	37
2.5.1 Tecnología de operación de las redes inalámbricas	40
2.5.2 Seguridad	44
2.6 Servidores, plataformas y servicios	47
2.6.1 Servidor de Archivos	47
2.6.2 Servidor de correo electrónico	49
2.6.3 Servidores de nombres DNS (Domain Name Service)	52
2.6.4 Servidor DHCP (Dynamic Host Configuration Protocol)	57
III. DEFINICIÓN DEL PROBLEMA	61
3.1 Diagnóstico actual de la red de cómputo del Colegio	
Asesoría Educativa Queen Mary School S.C.	61
3.2 Análisis de cada una de las áreas que conforman al Colegio	66
3.3 Objetivo	84

IV.- DESARROLLO: PROPUESTA DE REESTRUCTURACIÓN Y OPTIMIZACIÓN DE LA RED	85
4.1 Cableado e implementación de la red inalámbrica para las diferentes áreas del Colegio	85
4.2 Equipo de conectividad	113
4.3 Direccionamiento	129
4.4 Configuración de servidores, plataformas y servicios	133
CONCLUSIONES	142
GLOSARIO	145
ÍNDICE GRÁFICO	152
BIBLIOGRAFÍA	156

I. INTRODUCCIÓN

Las redes convergentes de alto desempeño en México no son solo una realidad al día de hoy, sino que se han convertido en una necesidad para cualquier institución, dependencia o empresa (grande, mediana o pequeña).

El desempeño de una red de este tipo está íntimamente ligado con la calidad de sus conexiones y del medio de comunicación que se elija.

El presente trabajo es una propuesta de optimización de la infraestructura del Colegio Asesoría Educativa Queen Mary School S.C. (QMS), con la finalidad de lograr una red convergente de alto desempeño, apegándose lo más posible a las normas establecidas y tomando como base el modelo de referencia ISO-OSI de telecomunicaciones.

Inicialmente, se realizará un diagnóstico para ubicar la problemática actual y los factores en los que hay que poner énfasis para la obtención de la propuesta de solución. Se revisará a detalle la infraestructura instalada, las carencias en cuanto a nodos y la distribución física de cada uno de ellos de acuerdo con los planos del Colegio.

Con el fin de mantener una clara idea acerca de los conceptos que se deben tener en consideración para la comprensión de un sistema de redes informáticas, de la referencia sobre la cual se hará la propuesta que es el modelo ISO-OSI, de los estándares y protocolos que se aplicarán a lo largo de este trabajo así como de conceptos inherentes al diseño de una red de alto desempeño, se plantea los fundamentos teóricos en donde se expondrá descriptivamente cada uno de estos elementos.

Dentro del capítulo denominado desarrollo y en función de los resultados obtenidos en el diagnóstico que arrojaron los aspectos que determinan la situación y problemática actual, se propondrá una solución siguiendo el modelo de referencia ISO-OSI, en las capas que se ven involucradas en el diseño de las propuestas aplicadas a cada una de las áreas del Colegio.

Dentro de este desarrollo se cubre inicialmente el aspecto del medio de comunicación con sus características funcionales y mecánicas (capa 1 ISO-OSI), en concreto se hará énfasis en el cableado estructurado siguiendo la premisa que dicta que “a mayor inversión en el medio de transmisión de la información, mejor desempeño en la red”.

Posteriormente se describirá el equipo de conectividad sugerido para optimizar el aspecto de la interconexión de los elementos de la red (capa 2). Se continuará con el direccionamiento lógico el cual funge como una parte muy importante en el alto desempeño de una red en tanto a que teniéndolo bien definido se establecen divisiones lógicas en la red (subredes) mismas que minimizan dominios de colisión entre la información que viaja dentro del medio y se definen espacios de trabajo optimizados.

Como punto culminante de esta sección, se definen las plataformas sobre las que actuarán las aplicaciones y servicios que se proporcionarán al usuario en donde se aplican las capas superiores del modelo de referencia.

Al terminar el desarrollo, se presentarán las conclusiones en donde se verán los resultados de la propuesta y se agregará un glosario de los términos técnicos que se empleen dentro del cuerpo del trabajo para evitar ambigüedades conceptuales.

II. FUNDAMENTOS TEÓRICOS

2.1 Conceptos generales de redes y telecomunicaciones

Un proceso de comunicación entre dos o más entes, cuando se ve involucrada una determinada distancia y en donde se necesita hacer uso de un medio de transmisión para realizar el intercambio de información, se entiende como una telecomunicación.

Este concepto se aplica para los sistemas de cómputo que requieren establecer un intercambio de información a través de distancias en tiempos muy cortos.

Las telecomunicaciones en el ámbito informático implican la interconexión de computadoras para la transmisión eficiente de información entre dos o más puntos llamados nodos, que cumplen alternativamente los papeles de emisor y receptor.

“Un conjunto de dos o más computadoras interconectadas que intercambian información se denomina Red de computadoras y el proceso de comunicación entre ellas requiere de diversos “mecanismos” que hacen coherente esta comunicación. Para comprender este proceso, es necesario tener en consideración algunos conceptos inherentes a las telecomunicaciones (en particular de sistemas de información).”¹

El objetivo de una red de computadoras es compartir y explotar recursos tanto físicos como lógicos y se puede entender como la resultante positiva en el manejo de información en tanto a ambiente de trabajo, comprendido desde cualquiera por pequeña que esta sea, hasta grupos departamentales o corporativos.

¹ HERRERA Pérez Enrique. Introducción a las telecomunicaciones modernas. México: Limusa. 2001. 65 p.

Inicialmente para poder establecer la interconexión de equipos (estaciones de trabajo), se requiere tener, por una parte, dispositivos que realicen físicamente la interconexión llamados dispositivos de red, y por otra, elementos lógicos o software que ayude a establecer la comunicación.

Dentro de los dispositivos de red, podemos encontrar los medios de transmisión como pueden ser el par trenzado de cobre, cables coaxiales, fibras ópticas o el espectro electromagnético. Aunado a estos se encuentran las interfases de conexión, que son físicamente las tarjetas de red NIC (Network Interface Card, de sus siglas en inglés) y del mismo modo los dispositivos de interconectividad que unen a los medios de transmisión en las redes que pueden ser concentradores (hubs) o dispositivos de conmutación (switches), entre otros.

La parte del software de redes está actualmente altamente estructurado y lleva implícitas las normas que se tienen que seguir para el establecimiento y manutención del proceso de comunicación. La normatividad que se sigue para que los procesos de comunicaciones se establezcan dentro de los mismos términos, se denomina Protocolos de Red y están regulados a nivel internacional por diversos organismos establecidos con este propósito específico como pueden ser:

- **ITU** (International Telecommunication Union, de sus siglas en inglés) Unión Internacional de Telecomunicaciones. Organismo dependiente de la ONU que se encarga de realizar recomendaciones técnicas sobre comunicaciones que muy a menudo se reconocen como estándares.
- **ISO** (International Organization for Standardization, de sus siglas en inglés) Organización Internacional de Normalización. Agrupa a 89 países y se trata de una organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Desarrolló el modelo conocido como OSI (Open Systems Interconnection, de sus siglas en inglés) Interconexión de Sistemas Abiertos.

- **ANSI** (American National Standards Institute, de sus siglas en inglés) Instituto Americano de Normas Nacionales. Asociación con fines no lucrativos, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación. Representa a Estados Unidos ante ISO.
- **IEEE** (Institute of Electrical and Electronics Engineers, de sus siglas en inglés) Instituto de Ingenieros Eléctricos y Electrónicos. Además de publicar artículos y conferencias, se encarga de la elaboración de estándares en las áreas que involucran la ingeniería eléctrica y electrónica.

En México se cuenta con las Normas Oficiales Mexicanas NOM que establece la Secretaría de Economía y que sirven para regular la normatividad de los procesos que se desarrollen dentro del territorio nacional.

El adecuado uso de las normas que emiten estas instancias, permite un proceso eficiente de comunicación entre dos o más redes informáticas.

Cada red de computadoras tiene una distribución particular, sin embargo se pueden clasificar de acuerdo con diversos aspectos particulares.

De acuerdo con la cobertura geográfica, se pueden clasificar como:

- **Redes de área local, LAN** (Local Area Network, de sus siglas en inglés). Son las redes en las que el medio de transmisión de la información pertenece al mismo administrador de la red y no requiere de la contratación de servicios de terceros.
- **Redes de área abierta, WAN** (Wide Area Network, de sus siglas en inglés). Son las redes que para poderse interconectar requieren de la contratación de un proveedor de medios de transmisión.

Dentro estas redes se pueden ubicar las redes llamadas MAN (Metropolitan Area Network, de sus siglas en inglés), son aquellas que cubren áreas geográficas dentro de una misma región y finalmente se encuentran las redes GAN (Global Area Network) que se refieren a redes que cubren diversas regiones que pueden ir desde dos ciudades contiguas hasta la totalidad del globo terráqueo.

En el presente trabajo, nos enfocaremos hacia las redes de área local, por ser está la necesidad que se tiene que satisfacer para lograr el objetivo.

De acuerdo con la topología (distribución de sus nodos), se pueden clasificar como:

BUS: Utiliza un único cable para conectar equipos en cada uno de los extremos, si un enlace falla, toda la red queda sin conexión. (*Ver figura 11.1*).

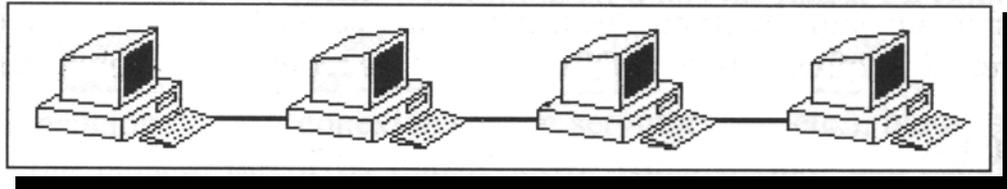


Figura 11.1 Topología de redes en Bus.

Anillo: Todos los nodos están conectados a una única vía con sus dos extremos unidos. Si un enlace falla, la red deja de operar completamente. (*Ver figura 11.2*).

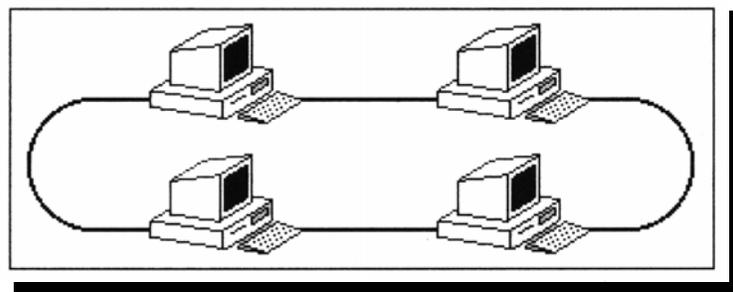


Figura 11.2. Topología de redes en anillo.

Estrella: Los equipos se conectan a un nodo central con funciones de distribución, conmutación y control. Si un nodo de los brazos de la estrella fallara, no afectaría al desempeño del resto de la red. (*Ver figura 11.3*).

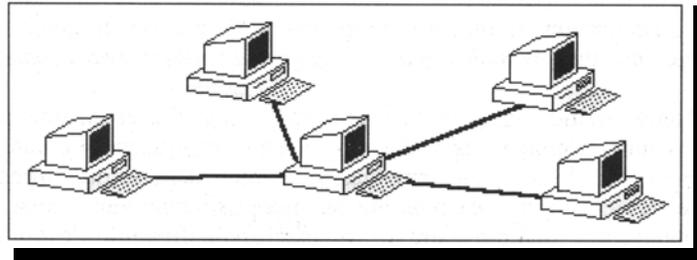


Figura 11.3. Topología de redes en estrella.

Malla: Es una interconexión total de todos los nodos, con la ventaja de que si una ruta falla, se pueden seleccionar rutas alternativas. (*Ver figura 11.4*).

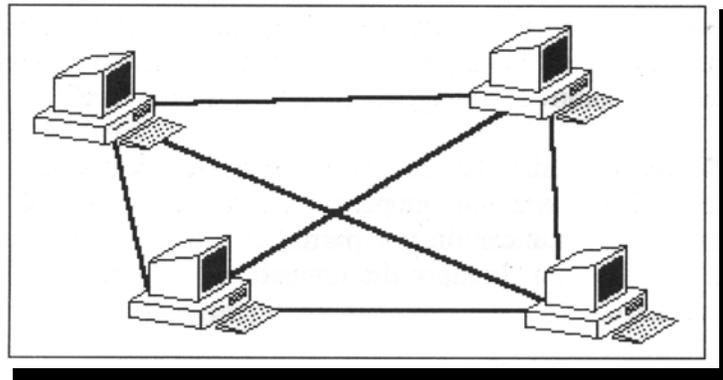


Figura 11.4. Topología de redes en malla.

Híbridas: Pueden ser combinaciones de las antes mencionadas de acuerdo con la necesidad específica. En el desarrollo de esta propuesta, se utilizará la topología de estrella por ser la más adecuada para la propuesta. Dentro de una red, la información viaja en un determinado medio, como se ha mencionado anteriormente. La adecuada selección de este, va a determinar una muy importante parte de la eficiencia de la misma.

La premisa que dice “a mayor inversión en el medio de transmisión, mejor desempeño de la red”, implica que en el diseño de la red, este factor se debe considerar como de vital importancia para el desempeño, buscando la mejor relación costo-beneficio. Dependiendo del tipo de medio de transmisión, varía el ó los protocolos de comunicaciones que se utilizan, lo cual implica la señalización (características intrínsecas de la señal), tiempos de envío-respuesta, modulación-desmodulación.

Actualmente se destaca la utilización de los siguientes medios de transmisión:

Par trenzado de cobre consiste en dos cables de cobre aislados, enlazados en pares. La forma trenzada del par de cables se utiliza para minimizar la interferencia eléctrica con respecto a los pares cercanos y otras interferencias procedentes del exterior denominadas ruido, estos suelen agruparse en cables de mayor grosor, recubiertos de material aislante.

Dependiendo de la forma en que se agrupan estos cables, se pueden encontrar diversos tipos, entre los que se destacan:

- **UTP** (Unshielded Twisted Pair, de sus siglas en inglés) Par trenzado sin blindaje. Es el medio de transmisión más simple, no cuenta con ningún tipo de pantalla conductora y está cubierto de una aislante. Está clasificado en diversas categorías de acuerdo con el ancho de banda que soporta, siendo la más reciente la Categoría 6 que soporta hasta 250Mhz.
- **STP** (Shieled Twisted Pair, de sus siglas en inglés), Par Trenzado Blindado. Este tipo de cable cuenta con una maya conductora que rodea a cada par que se conecta a diversas conexiones de tierra del sistema. Poseen una mayor inmunidad al ruido.
- **FTP** (Foil Twisted Pair, de sus siglas en inglés), Par trenzado con pantalla. Este cuenta con una malla de alambres de aluminio trenzados que cubre a todos los pares de manera global. Mejora la protección contra interferencias.

- **Cable coaxial.** Consta de un alambre rígido de cobre en la parte central, mismo que conduce la señal, rodeado de un material aislante que a su vez está recubierto de una malla de alambres de cobre trenzados que se conecta a tierra. Finalmente esta malla está revestida de un aislante. Esta conformación de permite un gran ancho de banda y un alto nivel de aislamiento al ruido.
- **Fibra óptica.** Está basada en la utilización de las ondas de luz para transmitir información binaria. Se trata de un cilindro de pequeña sección flexible por el que viaja la luz, recubierto de un material con un índice de refracción menor al del núcleo con el fin de mantener toda la luz en el interior de él. Este material está recubierto a su vez de una cubierta plástica delgada para proteger el revestimiento e impedir que cualquier rayo de luz proveniente del exterior penetre en la fibra. Finalmente varias fibras suelen agruparse en haces protegidos por una funda exterior.
- **Espectro electromagnético.** La comunicación inalámbrica resulta indispensable para los usuarios móviles o para las ubicaciones cuyas condiciones geográficas hagan poco accesible el tendido de un medio alámbrico. Consisten en el envío ó recepción de señales electromagnéticas que viajan por el aire. Varían en función de la frecuencia y la potencia de la señal.

2.2 Modelo de Referencia ISO-OSI

“En el año 1983, la ISO realizó la propuesta de un modelo de avance hacia la normalización a nivel mundial de protocolos. Este modelo se llama “Modelo de Referencia OSI de la ISO” debido a que se ocupa de la conexión de sistemas abiertos, es decir, sistemas que están preparados para la comunicación con otros diferentes.”²

² MOLINA Francisco Javier. Instalación y mantenimiento de servicios de redes locales. España: alfa-omega, 2004. 56 p.

Para acortar el nombre se llamará en adelante *Modelo OSI*. Este modelo emplea una arquitectura en niveles con la finalidad de dividir los problemas de interconexión en partes manejables, definiendo las implementaciones en cada nivel para asegurar una completa compatibilidad entre ellos. Este modelo se basa en las siguientes características:

- Cada nivel está pensado para realizar una función bien definida.
- El número de niveles debe ser suficiente para que no se agrupen funciones distintas, pero no tan grande que haga la arquitectura inmanejable.
- Debe crearse una nueva capa siempre que se necesite realizar una función bien diferenciada del resto.
- Las divisiones entre las capas deben establecerse de forma que se minimice el flujo de información entre ellas, es decir, que la interfaz sea más sencilla.
- Permitir que las modificaciones de funciones o protocolos que se realicen en una capa no afecte a los niveles contiguos.

La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.

El modelo consta de siete niveles o capas en donde cada uno de ellos tiene una función perfectamente definida:

- **Nivel Físico.** Se refiere a las características del medio de transmisión y de la transmisión de información binaria en sí. Esto es, asegurarse que cuando sea enviado un dígito binario por el medio, sea recibido el mismo dígito en el otro extremo. Tiene implicaciones sobre el esquema de codificación, sincronización, modulación, ancho de banda (en donde va implícita la tasa de bits por segundo) y todas las cuestiones mecánicas y eléctricas de las señales.

- **Nivel de Enlace de Datos.** Este nivel se encarga de empaquetar la información en tramas llamadas frames así como de verificar posibles errores en la transmisión de datos a nivel de frame y en su caso, notificar a niveles superiores. Define métodos de acceso al medio físico, sincronización entre emisores y receptores (evita que un emisor rápido sature a un receptor lento) y proporciona un direccionamiento físico a los dispositivos. En él se definen protocolos físicos como son CSMA, ATM, Frame Relay y también realiza el acoplamiento entre ellos. Consta de dos subcapas llamadas MAC (Medium Access Control) que define quién puede utilizar la red cuando múltiples dispositivos están intentando acceder simultáneamente y LLC (Logical Link Control) que define la manera en que los datos son transferidos por el medio y provee servicios de enlace de datos a las capas superiores.
- **Nivel de Red.** Agrupa la información en paquetes y se encarga de definir la ruta o camino que seguirá cada uno de ellos a través de la red para alcanzar su destino. La búsqueda de la mejor ruta se basa sobre preguntar cuál es el trayecto más directo, más rápido en el menor número de saltos. En esta capa se define el direccionamiento lógico que implica protocolos de enrutamiento y enrutables (IP, IPX, NetBeui). Dentro de esta se engloban los enrutadores (routers) y los switches nivel 3.
- **Nivel de Transporte.** Este nivel se encarga del ordenamiento secuencial de los paquetes, el control de flujo de la información. Tiene también como función el establecimiento, manutención y terminación de circuitos virtuales. Una de sus funciones más importantes es la detección de errores en los paquetes y la solicitud de reenvío en su caso. Opera a través de protocolos llamados end-to-end como son UDP, TCP o IPX.
- **Nivel de Sesión.** En este nivel se establecen las sesiones (conexiones) de comunicación entre los dos extremos para el transporte ordinario de datos.

Tiene la función de ser una especie de moderador de la comunicación en tanto que establece la sesión, define el inicio y el término de la misma. Facilita la sincronización y el control de diálogo. Maneja protocolos como DAP (Lightweight Directory Access).

- **Nivel de Presentación.** Este nivel es el encargado de realizar las transformaciones que sean requeridas por la capa de aplicación para la correcta interpretación de la información, es decir, se asegura que la información enviada por la capa de aplicación de un sistema sea legible por la misma capa de otro sistema (traducción). También se llevan a cabo los procesos de cifrado de mensajes.
- **Nivel de Aplicación.** Este nivel es el que se ubican las interfases que interactúan directamente con el usuario. Determina la disponibilidad de recursos y la sincronización de servicios tales como el correo electrónico, almacenamiento y recuperación archivos, servicios de directorio, etc.

Un proceso de comunicación entre dos puntos distantes se realiza, de acuerdo con este modelo, partiendo de la capa 7 de manera descendente en el emisor y al llegar a la capa 1, esta se comunica directamente con su análoga en el extremo receptor y el proceso se realiza de manera inversa, es decir, de la capa 1 a la 7.

2.3 Protocolos de Comunicaciones

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

Cuando se piense en protocolos de red se debe recordar estos tres puntos:

1. Existen muchos protocolos. A pesar de que cada protocolo facilita la comunicación básica, cada uno tiene un propósito diferente y realiza distintas tareas. Cada protocolo tiene sus propias ventajas y sus limitaciones.
2. Algunos protocolos sólo trabajan en ciertos niveles OSI. El nivel al que trabaja un protocolo describe su función. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red (NIC) y salgan al cable de la red.
3. Los protocolos también pueden trabajar juntos en una jerarquía o conjunto de protocolos. Al igual que una red incorpora funciones a cada uno de los niveles del modelo OSI, distintos protocolos también trabajan juntos a distintos niveles en la jerarquía de protocolos. Los niveles de la jerarquía de protocolos se corresponden con los niveles del modelo OSI. Por ejemplo, el nivel de aplicación del protocolo TCP/IP se corresponde con el nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones.

Servicios y Protocolos

“Los servicios de comunicaciones proporcionados por una red de transmisión de datos siguen unos protocolos bien establecidos y estandarizados. Si a una red en particular se le desea añadir una funcionalidad concreta, se deberá comprobar si ya posee el protocolo adecuado o hay que añadirsele. Un protocolo de red define unas normas a seguir a la hora de transmitir la información, normas que pueden ser: velocidad de transmisión, tipo de información, formato de los mensajes, etc.”³

³ TANENBAUM, Andrew S. Computer Networks. 4th. New Jersey: Prentice-Hall, 2003. 87 p.

Funcionamiento de los protocolos

La operación técnica en la que los datos son transmitidos a través de la red se puede dividir en dos pasos discretos y sistemáticos. A cada paso se realizan ciertas acciones que no se pueden realizar en otro paso. Cada paso incluye sus propias reglas y procedimientos, o protocolo. Los pasos del protocolo se tienen que llevar a cabo en un orden apropiado y que sea el mismo en cada uno de los equipos de la red. En el equipo origen, estos pasos se tienen que llevar a cabo de arriba hacia abajo. En el equipo de destino, estos pasos se tienen que llevar a cabo de abajo hacia arriba.

Los protocolos en el equipo origen:

- Se dividen en secciones más pequeñas, denominadas paquetes.
- Se añade a los paquetes, información sobre la dirección, de forma que el equipo destino pueda determinar si los datos le pertenecen.
- Prepara los datos para transmitirlos a través de la NIC y enviarlos a través del cable de la red.

Los protocolos en el equipo de destino constan de la misma serie de pasos, pero en sentido inverso:

- Toma los paquetes de datos del cable y los introduce en el equipo, a través del NIC.
- Extrae de los paquetes de datos toda la información transmitida eliminando la información añadida por el equipo origen.
- Copia los datos de los paquetes en un búfer, para reorganizarlos y enviarlos a la aplicación.
- Los equipos origen y destino necesitan realizar cada paso de la misma forma para que los datos tengan la misma estructura, al recibirse, que cuando se enviaron.

a) Protocolos encaminables

Hasta mediados de los ochenta, la mayoría de las redes de área local (LAN) estaban aisladas. Una LAN servía a un departamento o a una compañía y rara vez se conectaba a entornos más grandes.

Sin embargo, a medida que maduraba la tecnología LAN, y la comunicación de los datos necesitaba la expansión de los negocios, las LAN evolucionaron, haciéndose componentes de redes de comunicaciones más grandes en las que las LAN podían hablar entre sí.

Los datos se envían de una LAN a otra a lo largo de varios caminos disponibles, es decir, se encaminan. A los protocolos que permiten la comunicación LAN a LAN se les conoce como protocolos encaminables. Y estas se pueden utilizar para unir varias LAN y crear entornos de red de área extensa, mismas que han tomado gran importancia.

b) Protocolos en una arquitectura multi-nivel

En una red, tienen que trabajar juntos varios protocolos. Al trabajar juntos, aseguran que los datos se preparan correctamente, se transfieran al destino correspondiente y se reciban de forma apropiada.

El trabajo de los distintos protocolos tiene que estar coordinado de forma que no se produzcan conflictos o se realicen tareas incompletas. Los resultados de esta coordinación se conocen como trabajo en niveles.

Jerarquías de protocolos

Una jerarquía de protocolos es una combinación de protocolos. Cada nivel de la jerarquía especifica un protocolo diferente para la gestión de una función o de un subsistema del proceso de comunicación.

Los niveles inferiores en el modelo OSI especifican cómo pueden conectar los fabricantes sus productos a los productos de otros fabricantes, por ejemplo, utilizando NIC de varios fabricantes en la misma LAN.

Cuando utilicen los mismos protocolos, pueden enviar y recibir datos entre sí. Los niveles superiores especifican las reglas para dirigir las sesiones de comunicación (el tiempo en el que dos equipos mantienen una conexión) y la interpretación de aplicaciones.

A medida que aumenta el nivel de la jerarquía, aumenta la sofisticación de las tareas asociadas a los protocolos.

c) El proceso de ligadura

Proceso con el que se conectan los protocolos entre sí y con la NIC, permite una gran flexibilidad a la hora de configurar una red.

Por ejemplo, se pueden ligar dos jerarquías de protocolos a una NIC, como Intercambio de paquetes entre redes e Intercambio de paquetes en secuencia (IPX/SPX). Si hay más de una NIC en el equipo, cada jerarquía de protocolos puede estar en una NIC o en ambas.

El orden de ligadura determina la secuencia en la que el sistema operativo ejecuta el protocolo. Cuando se ligan varios protocolos a una NIC, el orden de ligadura es la secuencia en que se utilizarán los protocolos para intentar una comunicación correcta. Normalmente, el proceso de ligadura se inicia cuando se instala o se inicia el sistema operativo o el protocolo.

Por ejemplo, si el primer protocolo ligado es TCP/IP, el sistema operativo de red intentará la conexión con TCP/IP antes de utilizar otro protocolo. Si falla esta conexión, el equipo tratará de realizar una conexión utilizando el siguiente protocolo en el orden de ligadura.

d) Jerarquías estándar

La industria informática ha diseñado varios tipos de protocolos como modelos estándar de protocolo. Los fabricantes de hardware y software pueden desarrollar sus productos para ajustarse a cada una de las combinaciones de estos protocolos.

Los modelos más importantes incluyen:

- La familia de protocolos ISO/OSI.
- La arquitectura de sistemas en red de IBM (SNA).
- Digital DECnet.
- Novell NetWare.
- Apple Talk de Apple.
- El conjunto de protocolos de Internet, TCP/IP.

Los protocolos existen en cada nivel de estas jerarquías, realizando las tareas especificadas por el nivel. Sin embargo, las tareas de comunicación que tienen que realizar las redes se agrupan en un tipo de protocolo. Cada tipo está compuesto por uno o más niveles del modelo OSI.

Antes del modelo de referencia OSI se escribieron muchos protocolos. Por tanto, no es extraño encontrar jerarquías de protocolos que no correspondan directamente con el modelo OSI.

Cada nivel tiene su propio conjunto de reglas. Los protocolos definen las reglas para cada nivel en el modelo OSI:

- **Nivel de aplicación:** Inicia o acepta una petición.
- **Nivel de presentación:** Añade información de formato, presentación y cifrado al paquete de datos.
- **Nivel de sesión:** Añade información del flujo de tráfico para determinar cuándo se envía el paquete.

- **Nivel de transporte:** Añade información para el control de errores.
- **Nivel de red:** Se añade información de dirección y secuencia al paquete.
- **Nivel de enlace de datos:** Añade información de comprobación de envío y prepara los datos para que vayan a la conexión física.
- **Nivel físico:** El paquete se envía como una secuencia de bits.

e) Protocolos de aplicación

Los protocolos de aplicación trabajan en el nivel superior del modelo de referencia OSI y proporcionan interacción entre aplicaciones e intercambio de datos. Estos protocolos son:

- **X.400:** Un protocolo CCITT para las transmisiones internacionales de correo electrónico.
- **SMTP** (Protocolo básico para la transferencia de correo): Un protocolo Internet para **las transferencias de correo electrónico.**
- **FTP** (Protocolo de transferencia de archivos): Un protocolo para la transferencia de archivos en Internet.
- **SNMP** (Protocolo básico de gestión de red): Un protocolo Internet para el control de redes y componentes.
- **Telnet:** Un protocolo Internet para la conexión a máquinas remotas y procesar los datos localmente.
- **AppleTalk y AppleShare:** Conjunto de protocolos de red de Apple.
- **DAP** (Protocolo de acceso a datos): Un protocolo de DECnet para el acceso a archivos.

f) Protocolos de transporte

Los protocolos de transporte facilitan las sesiones de comunicación entre equipos y aseguran que los datos se pueden mover con seguridad entre equipos.

- **TCP:** El protocolo de TCP/IP para la entrega garantizada de datos en forma de paquetes secuenciados.
- **SPX:** Parte del conjunto de protocolos IPX/SPX de Novell para datos en forma de paquetes secuenciados.
- **NWLink:** La implementación de Microsoft del protocolo IPX/SPX.
- **NetBEUI** (Interfaz de usuario ampliada NetBIOS): Establece sesiones de comunicación entre equipos.
- **(NetBIOS)** proporciona los servicios de transporte de datos subyacentes.

g) Protocolos de red

Los protocolos de red proporcionan lo que se denominan «servicios de enlace». Estos protocolos gestionan información sobre direccionamiento y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es Ethernet o Token Ring.

- **IP:** El protocolo de TCP/IP para el encaminamiento de paquetes.
- **IPX:** El protocolo de Novell para el encaminamiento de paquetes.
- **NWLink:** La implementación de Microsoft del protocolo IPX/SPX.
- **NetBEUI:** Un protocolo de transporte que proporciona servicios de transporte de datos para sesiones y aplicaciones NetBIOS.

h) Estándares de protocolo

El modelo OSI se utiliza para definir los protocolos que se tienen que utilizar en cada nivel. Los productos de distintos fabricantes que se ajustan a este modelo se pueden comunicar entre sí.

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), ANSI (Instituto de Estandarización Nacional Americano), CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía), ahora llamado ITU (Unión Internacional de Telecomunicaciones) y otros organismos de estandarización han desarrollado protocolos que corresponden con algunos de los niveles del modelo OSI.

Los protocolos de IEEE a nivel de enlace de datos son:

- **802.3 (Ethernet).** Es una red lógica en bus que puede transmitir datos a 10 Mbps. Los datos se transmiten en la red a todos los equipos. Sólo los equipos que tenían que recibir los datos informan de la transmisión.
- El protocolo de acceso múltiple con detección de portadora y colisiones (**CSMA/CD**) regula el tráfico de la red permitiendo la transmisión sólo cuando la red esté despejada y no haya otro equipo transmitiendo.
- Para redes inalámbricas se **utiliza CSMA / CA** (Carrier Sense Multiple Access) un nuevo estándar, denominado IEEE 802.11b, y un consorcio de fabricación, el Wireless Ethernet Compatibility Alliance (WECA), Carrier Sensing: Escucha el medio para determinar si está libre. Collision Avoidance: Minimiza el riesgo de colisión por medio de un retardo aleatorio usado antes de sensar el medio y transmitir la información.
- **802.4 (Token Bus).** Es una red en bus que utiliza un esquema de paso de testigo. Cada equipo recibe todos los datos, pero sólo los equipos en los que coincida la dirección responderán. Un testigo que viaja por la red determina quién es el equipo que tiene que informar.
- **802.5 (Token Ring).** Es un anillo lógico que transmite a 4 ó 16 Mbps. Aunque se le llama en anillo, está montada como una estrella ya que cada equipo está conectado a un hub. Realmente, el anillo está dentro del hub. Un token a través del anillo determina qué equipo puede enviar datos.

El IEEE definió estos protocolos para facilitar la comunicación en el subnivel de Control de acceso al medio (MAC). Un controlador MAC está situado en el subnivel de Control de acceso al medio; este controlador de dispositivo es conocido como controlador de la NIC.

Proporciona acceso a bajo nivel a los adaptadores de red para proporcionar soporte en la transmisión de datos y algunas funciones básicas de control del adaptador.

Un protocolo MAC determina qué equipo puede utilizar el cable de red cuando varios equipos intenten utilizarlo simultáneamente. CSMA/ CD, el protocolo 802.3, permite a los equipos transmitir datos cuando no hay otro equipo transmitiendo.

Si dos máquinas transmiten simultáneamente se produce una colisión. El protocolo detecta la colisión y detiene toda transmisión hasta que se libera el cable. Entonces, cada equipo puede volver a tratar de transmitir después de esperar un período de tiempo aleatorio.

i) TCP/IP

El Protocolo de control de transmisión/Protocolo Internet (TCP/IP) es un conjunto de Protocolos aceptados por la industria que permiten la comunicación en un entorno heterogéneo (formado por elementos diferentes).

Además, TCP/IP proporciona un protocolo de red encaminable y permite acceder a Internet y a sus recursos. Debido a su popularidad, TCP/IP se ha convertido en el estándar de hecho en lo que se conoce como interconexión de redes, la intercomunicación en una red que está formada por redes más pequeñas. TCP/IP se ha convertido en el protocolo estándar para la interoperabilidad entre distintos tipos de equipos. La interoperabilidad es la principal ventaja de TCP/IP.

La mayoría de las redes permiten TCP/IP como protocolo. TCP/IP también permite el encaminamiento y se suele utilizar como un protocolo de interconexión de redes. Entre otros protocolos escritos específicamente para el conjunto TCP/IP se incluyen:

- **SMTP** (Protocolo básico de transferencia de correo). Correo electrónico.
- **FTP** (Protocolo de transferencia de archivos). Para la interconexión de archivos entre equipos que ejecutan TCP/IP.
- **SNMP** (Protocolo básico de gestión de red). Para la gestión de redes.

“Diseñado para ser encaminable, robusto y funcionalmente eficiente, TCP/IP fue desarrollado por el Departamento de Defensa de Estados Unidos como un conjunto de protocolos para redes de área extensa (WAN). Su propósito era el de mantener enlaces de comunicación entre sitios en el caso de una guerra nuclear. Actualmente, la responsabilidad del desarrollo de TCP/IP reside en la propia comunidad de Internet.”⁴

La utilización de TCP/IP ofrece varias ventajas:

- Es un estándar en la industria. Como un estándar de la industria, es un protocolo abierto. Esto quiere decir que no está controlado por una única compañía, y está menos sujeto a cuestiones de compatibilidad.
- Es el protocolo, de hecho, de Internet.
- Contiene un conjunto de utilidades para la conexión de sistemas operativos diferentes. La conectividad entre un equipo y otro no depende del sistema operativo de red que esté utilizando cada equipo.
- Utiliza una arquitectura escalable, cliente/servidor. TCP/IP puede ampliarse (o reducirse) para ajustarse a las necesidades y circunstancias futuras. Utiliza sockets para hacer que el sistema operativo sea algo transparente.
- Un socket es un identificador para un servicio concreto en un nodo concreto de la red. El socket consta de una dirección de nodo y de un número de puerto que identifica al servicio.

⁴ MAIWALD Eric. Fundamentos de Seguridad de redes. Madrid: McGraw-Hill, 2004. 18 p.

Estándares TCP/IP

El desarrollo de Internet está basado en el concepto de estándares abiertos. Es decir, cualquiera que lo desee, puede utilizar o participar en el desarrollo de estándares para Internet. La Plataforma de arquitectura Internet (IAB) es el comité responsable para la gestión y publicación de los estándares. La IAB permite a cualquier persona o a cualquier compañía que envíe o que evalúe un estándar.

Arquitectura TCP/IP

TCP/IP se suele confundir muchas veces con un protocolo de comunicaciones concreto, cuando, en realidad, es una compleja arquitectura de red que incluye varios de ellos, apilados por capas. Es, sin lugar a dudas, la más utilizada del mundo, ya que es la base de comunicación de Internet y también se utiliza ampliamente en las distintas versiones de los sistemas operativos Unix y Linux (aunque debido a su gran utilización ha sido también implantado en otros sistemas como Windows).

Algunos de los motivos de la popularidad alcanzada por esta arquitectura son:

- Es independiente de los fabricantes y las marcas comerciales.
- Soporta múltiples tecnologías de redes.
- Es capaz de interconectar redes de diferentes tecnologías y fabricantes.
- Puede funcionar en máquinas de cualquier tamaño, desde las computadoras personales a grandes supercomputadoras. Se ha convertido en estándar de comunicación en EE.UU. desde 1983.

La arquitectura de TCP/IP se construyó diseñando inicialmente los protocolos para, posteriormente, integrarlos por capas en la arquitectura. Por esta razón, a TCP/IP muchas veces se le califica como pila de protocolos.

Su modelo por niveles es algo diferente a OSI de ISO.

TCP/IP sólo tiene definida cuatro capas, mientras que OSI tiene siete. (*Ver tabla II.1*).

	<i>OSI</i>	<i>TCP/IP</i>
7	Aplicación	Aplicación
6	Presentación	
5	Sesión	
4	Transporte	Transporte
3	Red	Interred
2	Enlace de datos	Subred
1	Físico	

Tabla II.1 Comparación entre el Modelo OSI y TCP/IP.

Las funciones que realizan cada una de ellas son las siguientes:

- **Capa de subred:** El modelo no da mucha información de esta capa, y solamente se especifica que debe existir algún protocolo que conecte la estación con la red. La razón fundamental es que, como TCP/IP se diseñó para su funcionamiento sobre redes diferentes, esta capa depende de la tecnología utilizada y no se especifica de antemano.

- **Capa de interred:** Esta capa es la más importante de la arquitectura y su misión consiste en permitir que las estaciones envíen información (paquetes) a la red y los hagan viajar de forma independiente hacia su destino. Durante ese viaje, los paquetes pueden atravesar redes diferentes y llegar desordenados. Esta capa no se responsabiliza de la tarea de ordenar de nuevo los mensajes en el destino. El protocolo más importante de esta capa se llama IP (Internet Protocol o Protocolo de Interred), aunque también existen otros protocolos.

- **Capa de transporte:** Ésta cumple la función de establecer una conversación entre el origen y el destino, de igual forma que hace la capa de transporte en el modelo OSI. Puesto que las capas inferiores no se responsabilizan del control de errores ni de la ordenación de los mensajes, ésta debe realizar todo ese trabajo. Aquí también se han definido varios protocolos, entre los que destacan TCP (Transmisión Control Protocol o Protocolo de Control de la Transmisión), orientado a la conexión y fiable, y UDP (User Datagram Protocol o Protocolo de Datagrama de Usuario), no orientado a la conexión y no fiable.
- **Capa de aplicación:** Esta capa contiene, el igual que la capa de aplicación de OSI, todos los protocolos de alto nivel que utilizan los programas para comunicarse. Aquí se encuentra el protocolo de terminal virtual (TELNET), el de transferencia de archivos (FTP), el protocolo HTTP, que usan los navegadores para recuperar páginas en la World Wide Web, los protocolos de gestión del correo electrónico, etc.

Las capas de sesión y presentación no existen en la arquitectura TCP/IP, ya que los diseñadores pensaron que no se necesitaban. La experiencia obtenida con los trabajos realizados en el modelo OSI ha comprobado que esta visión fue correcta: se utilizan muy poco en la mayoría de las aplicaciones de comunicación.

En caso de que alguna aplicación desee utilizar un servicio de cifrado de datos o recuperación ante caídas, será necesario incluirlos dentro del propio programa de aplicación.

El modelo TCP/IP original no distinguía los conceptos de capa, servicio, interfaz y protocolo, aunque revisiones posteriores han incluido parte de esta nomenclatura. Por esta razón, el modelo OSI es más flexible a los cambios, ya que la interacción y encapsulación entre capas es más estricta.

Protocolo Internet (IP)

El Protocolo Internet (IP) es un protocolo de conmutación de paquetes que realiza direccionamiento y encaminamiento. Cuando se transmite un paquete, este protocolo añade una cabecera al paquete, de forma que pueda enviarse a través de la red utilizando las tablas de encaminamiento dinámico.

IP es un protocolo no orientado a la conexión y envía paquetes sin esperar la señal de confirmación por parte del receptor. Además, IP es el responsable del empaquetado y división de los paquetes requerido por los niveles físicos y de enlace de datos del modelo OSI.

Cada paquete IP está compuesto por una dirección de origen y una de destino, un identificador de protocolo, un checksum (un valor calculado) y un TTL (tiempo de vida, del inglés time to live). El TTL indica a cada uno de los routers de la red entre el origen y destino cuánto tiempo le queda al paquete por estar en la red. Esto funciona como un contador o reloj de cuenta atrás. Cuando el paquete pasa por el router, éste reduce el valor en una unidad (un segundo) o el tiempo que llevaba esperando para ser entregado.

El propósito del TTL es prevenir que los paquetes perdidos o dañados (como correos electrónicos con una dirección equivocada) estén vagando en la red. Cuando la cuenta TTL llega a cero, se retira al paquete de la red.

Otro método utilizado por IP para incrementar la velocidad de transmisión es el conocido como «AND». La idea del AND es determinar si la dirección es de un sitio local o remoto. Si la dirección es local, IP preguntará al Protocolo de resolución de direcciones (ARP) por la dirección hardware de la máquina de destino.

Si la dirección es remota, el IP comprueba su tabla de direccionamiento local para enviarlo al destino. Si existe un camino, el paquete se envía por ahí. Si no existe el direccionamiento cambia, el paquete se envía a través del gateway a su destino.

Un AND es una operación lógica que combina los valores de dos bits (0, 1) o dos valores lógicos (verdadero, falso) y devuelve un 1 (verdadero) si los valores de ambas entradas son 1 (verdadero) y devuelve 0 (falso) en caso contrario.

Protocolo de resolución de direcciones (ARP)

- Antes de enviar un paquete IP a otro host se tiene que conocer la dirección hardware de la máquina receptora. El ARP determina la dirección hardware (dirección MAC) que corresponde a una dirección IP.
- Si ARP no contiene la dirección en su propia caché, envía una petición por toda la red solicitando la dirección. Todos los hosts de la red procesan la petición y, si contienen un valor para esa dirección, lo devuelven al solicitante.
- A continuación se envía el paquete a su destino y se guarda la información de la nueva dirección en la caché del router.

Protocolo inverso de resolución de direcciones (RARP)

- Un servidor RARP mantiene una base de datos de números de máquina en la forma de una tabla (o caché) ARP que está creada por el administrador del sistema.
- A diferencia de ARP, el protocolo RARP proporciona una dirección IP a una petición con dirección de hardware.
- Cuando el servidor RARP recibe una petición de un número IP desde un nodo de la red, responde comprobando su tabla de encaminamiento para el número de máquina del nodo que realiza la petición y devuelve la dirección IP al nodo que realizó la petición.

Protocolo de mensajes de control de Internet (ICMP)

El ICMP es utilizado por los protocolos IP y superiores para enviar y recibir informes de estado sobre la información que se está transmitiendo.

Los routers suelen utilizar ICMP para controlar el flujo, o velocidad, de datos entre ellos. Si el flujo de datos es demasiado rápido para un router, pide a los otros routers que reduzcan la velocidad de transmisión.

Los dos tipos básicos de mensajes ICMP son el de informar de errores y el de enviar preguntas.

Protocolo de datagramas de usuario (UDP)

- **UDP** es un protocolo no orientado a la conexión y es el responsable de la comunicación de datos extremo a extremo. En cambio, a diferencia de TCP, UDP no establece una conexión. Intenta enviar los datos e intenta comprobar que el host de destino recibe los datos. También se utiliza para enviar pequeñas cantidades de datos que no necesitan una entrega garantizada. Aunque UDP utiliza puertos, son distintos de los puertos TCP; así pues, pueden utilizar los mismos números sin interferirse.

2.4 Cableado Estructurado

La norma mexicana NMX-I-248-1998NYCE en el diseño de sistemas de cableado estructurado establece los requisitos mínimos aplicables al cableado de telecomunicaciones dentro de un edificio, hasta la salida/conector de telecomunicaciones y entre edificios en un ambiente de campus. El cableado estructurado especificado por esta norma aplica a una amplia variedad de localidades para edificios comerciales por ejemplo, voz, datos, texto, video e imágenes.

Esta norma consiste de 7 subsistemas funcionales:

- 1. El cableado horizontal.** Es la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones. El cableado horizontal incluye los cables horizontales, las tomas/conectores de telecomunicaciones en el área de trabajo, la terminación mecánica y las interconexiones horizontales localizadas en el cuarto de telecomunicaciones.
- 2. Cableado de backbone.** El propósito es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos.
- 3. El área de trabajo.** Se extiende de la toma/conector de telecomunicaciones o el final del sistema de cableado horizontal, hasta el equipo de la estación. Esta puede incluir, pero no se limita a, teléfonos, terminales de datos y computadoras.
- 4. Instalación de entrada o acometida.** Es el punto donde la instalación exterior y dispositivos asociados entran al edificio. Este punto puede estar utilizado por servicios de redes públicas, redes privadas del cliente, o ambas. Están ubicados los dispositivos de protección para sobrecargas de voltaje.
- 5. Sala de máquinas o equipos.** Es un espacio centralizado para el equipo de telecomunicaciones que da servicio a los usuarios en el edificio.
- 6. Cuarto de Telecomunicaciones.** Debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable, alarmas, seguridad, audio y otros sistemas de telecomunicaciones.
- 7. Administración.** Incluye la documentación de los cables, terminaciones de los mismos, paneles de parcheo, armarios de telecomunicaciones y otros espacios ocupados por los sistemas.

Como complemento a los presentes criterios normativos, debe consultarse las siguiente Norma Oficial Mexicana:

NMX-I-248-1998NYCE “Telecomunicaciones, cableado, cableado estructurado, cableado de telecomunicaciones para edificios comerciales, especificaciones y métodos de prueba”
Especificaciones de un cableado estructurado de telecomunicaciones genérico.

La Descripción del cableado estructurado genérico establece los elementos funcionales de un cableado estructurado genérico y describe la forma de conectarlos para formar redes de cableado estructurado de telecomunicaciones.

Elementos funcionales

Los elementos funcionales de un cableado estructurado de telecomunicaciones genérico son los siguientes:

- Distribuidor de cables de Campus. [DCC]
 - Cableado principal de Campus.
- Distribuidor de cables de edificio. [DCE]
 - Cableado principal de edificio.
- Distribuidor de cables de piso. [DCP]
 - Cableado horizontal en piso.

Subsistemas de cableado

El cableado genérico está conformado por tres subsistemas de cableado: cableado principal de campus, cableado principal de edificio y cableado horizontal, los cuales se interconectan entre sí, para formar la estructura de un cableado genérico de telecomunicaciones.

(Ver figura II.5).

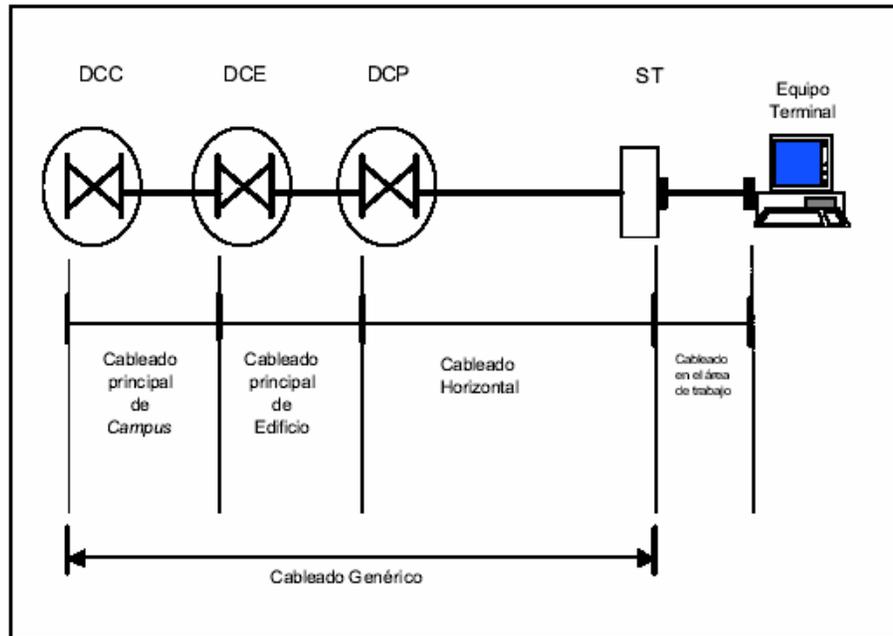


Figura 11.5 Cableado Genérico.

- **Cableado principal de Campus.** Este se extiende desde el distribuidor de cables de campus hasta los distribuidores de cables de edificio.
- **Cableado principal de Edificio.** Este se extiende desde los distribuidores de cables de edificio (DCE) hasta los distribuidores de cables de piso (DCP), e incluye los cables principales de edificio.
- **Cableado horizontal.** Este cableado se extiende desde el distribuidor de cables de piso hasta las salidas de telecomunicaciones. El término “Horizontal” se emplea ya que típicamente el cable en esta parte del cableado genérico se instala horizontalmente a lo largo de los pisos o plafones de un edificio. El cableado horizontal no debe contener más de un punto de transición o punto de consolidación, entre el distribuidor de cables de piso y la salida/conector de telecomunicaciones.

Topología del cableado genérico

El cableado estructurado genérico de un edificio, campus o área industrial debe tener una estructura en estrella jerárquica, donde la cantidad y tipo de subsistemas de cableado que están incluidos en un diseño, depende de la geografía y tamaño de éstos.

La topología de un cableado genérico debe tomar la forma mostrada (*Ver figura 11.6*) Los cables se deben instalar entre los niveles jerárquicos adyacentes de la topología de un cableado genérico.

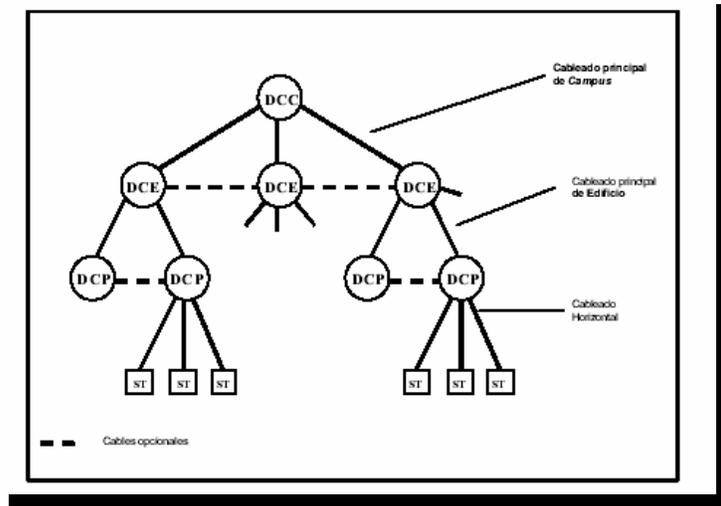


Figura 11.6 Topología del cableado genérico.

El cableado principal de un edificio se puede utilizar para interconectar los distribuidores de cables de piso, no obstante, estas conexiones directas serán adicionales a las requeridas para la topología básica de estrella jerárquica.

En la *Figura 11.7*. Se muestra un ejemplo de un cableado genérico para un campus formado por 2 edificios, en la cual el edificio que aparece en primer plano contempla los distribuidores de cables de edificio y de piso de la planta baja del edificio, en forma separada, mientras que el edificio que aparece en segundo plano, muestra que las funciones de los mismos distribuidores de cables han sido combinadas en un mismo distribuidor. Generalmente, las funciones de los distribuidores DCC, DCE y DCP se agrupan en un solo distribuidor.

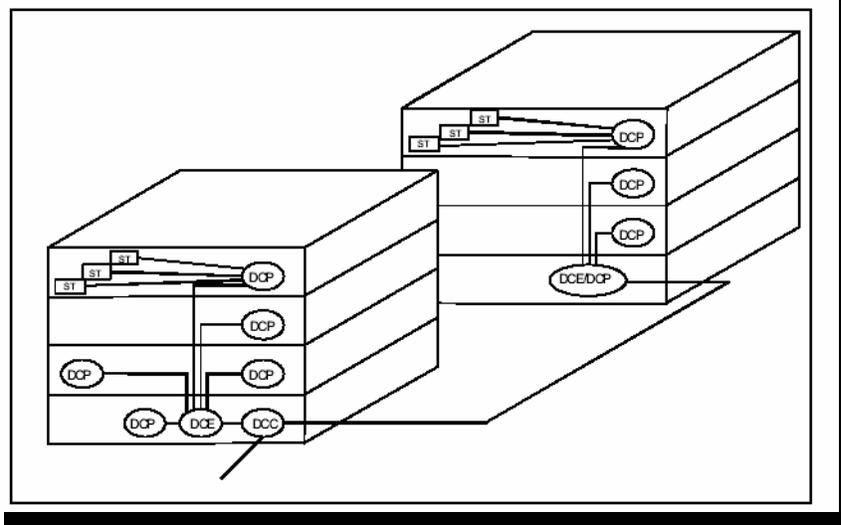


Figura 11.7 Cableado genérico en un campus.

Cableado horizontal

Aspectos generales del cableado horizontal.

El cableado horizontal debe de ser de punto a punto desde el distribuidor de cables de piso hasta la salida de telecomunicaciones. De igual manera, debe tomarse en consideración para el diseño del cableado de cobre, la proximidad del cableado horizontal a las instalaciones eléctricas que generan altos niveles de interferencia electromagnética. Los motores y los transformadores utilizados para soportar los requerimientos mecánicos del edificio próximos al área de trabajo, son ejemplos de este tipo de fuentes.

El cableado horizontal debe tener una topología de estrella, es decir, cada una de las salidas de telecomunicaciones distribuidas en las áreas de trabajo, debe ser conectada a un distribuidor de cables de piso, el cual debe estar instalado en el interior de un cuarto de telecomunicaciones. (Ver *figura 11.8*).

Cuando en un piso de oficinas se excedan las distancias máximas permitidas para el cableado horizontal, se permite la instalación de hasta dos distribuidores de cables.

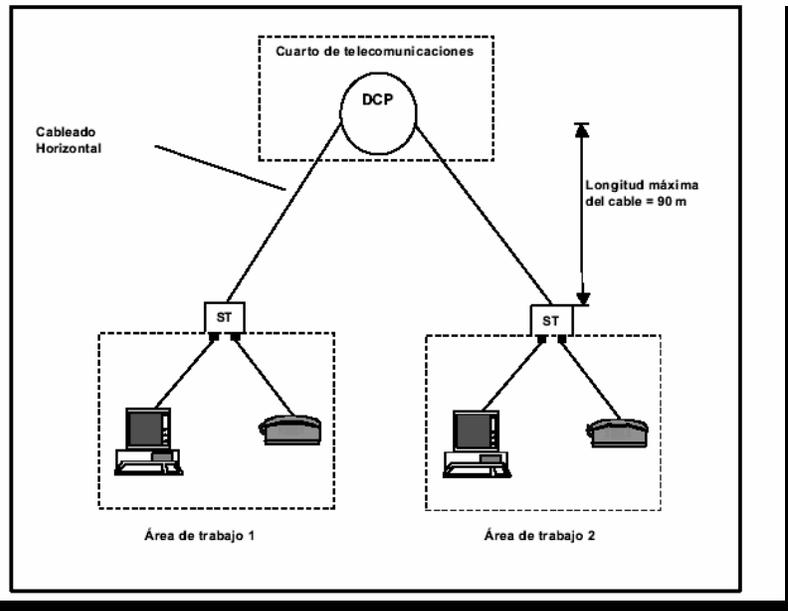


Figura 11.8. Cableado Horizontal.

Distribución de cableado

Ubicación de los distribuidores.

Los distribuidores de cableado deben ubicarse en el interior de los cuartos de telecomunicaciones o en el cuarto de equipos. (Ver figura 11.9) muestra la ubicación típica de los elementos funcionales en un edificio administrativo.

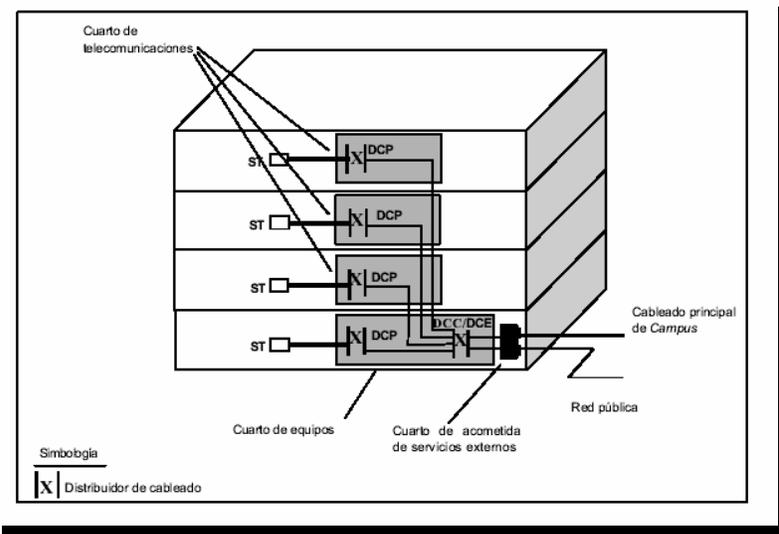


Figura 11.9 Cuarto de Telecomunicaciones.

Aquí muestra la ubicación típica de los elementos funcionales del cableado estructurado en un Campus.

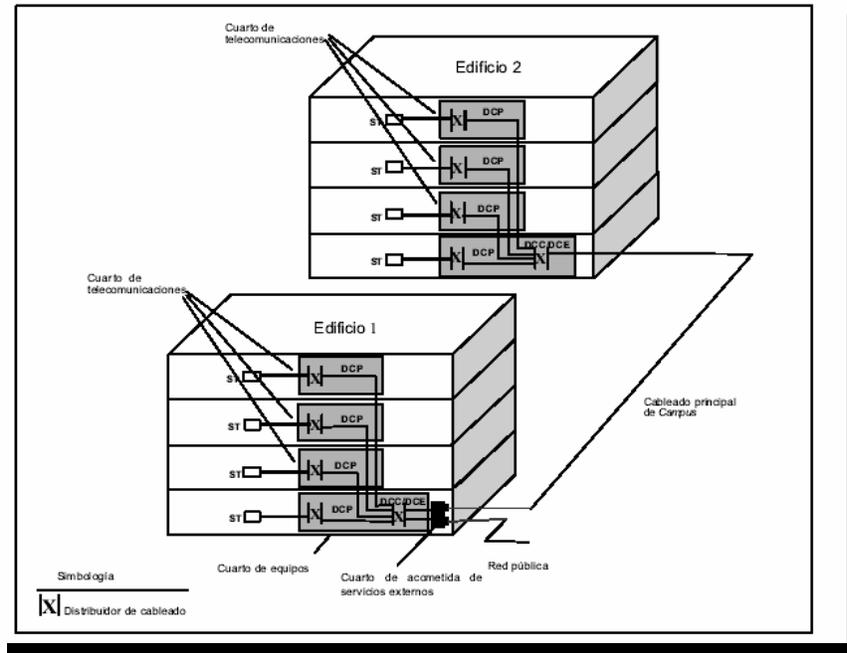


Figura 11.10 Cuarto de Telecomunicaciones.

2.5 Redes Inalámbricas

Por red de área local entendemos una red que cubre un entorno geográfico limitado, con una velocidad de transferencia de datos relativamente alta, baja tasa de errores y administrada de forma privada.

“De la misma forma por red inalámbrica entendemos una red que utiliza ondas electromagnéticas como medio de transmisión de la información, que viaja a través del canal inalámbrico enlazando los diferentes equipos o terminales móviles asociados a la red. Estos enlaces se implementan básicamente a través de tecnologías de microondas y de infrarrojos.”⁵

⁵ FOROUZAN Behrouz. Transmisión de datos y redes de comunicación. 4ª ed. España: McGraw-Hill, 2007.

En las redes tradicionales cableadas esta información viaja a través de cables coaxiales, pares trenzados o fibra óptica. Una red de área local inalámbrica, también llamada wireless LAN (WLAN), es un sistema flexible de comunicaciones que puede implementarse como una extensión o directamente como una alternativa a una red cableada, y que utiliza como medio de transmisión el aire.

Este tipo de redes utiliza tecnología de radiofrecuencia minimizando así la necesidad de conexiones cableadas. Este hecho proporciona al usuario una gran movilidad sin perder conectividad.

El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así, debido a que sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 54 Mbps frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general las WLAN se utilizarán como un complemento de las redes fijas.

Norma 802.11

La serie 802.11x desarrollada por el IEEE especifican una tecnología para redes wireless mediante microondas (más de 1 GHz). Las especificaciones 802.11, 802.11b y 802.11g (*Ver tabla ll.2*) operan en la banda de los 2.4 GHz; la norma 802.11a, en los 5 GHz.

<i>Norma</i>	<i>Velocidad máxima</i>	<i>Rango de frecuencia.</i>
802.11a	54 Mbps.	5.15 a 5.825 GHz.
802.11b	11 Mbps.	2.4 a 2.483 GHz.
802.11g	54 Mbps.	2.4 a 2.483 GHz.

Tabla ll.2 Especificaciones de la normas 802.11a, 802.11b y 802.11g

Especificaciones aprobadas. (Ver tabla ll.3)

<i>Standard</i>	<i>Descripción</i>	<i>Aprobado</i>
802.11	Operaciones de WLAN a velocidades de hasta 2 Mbps en la banda ISM (Industrial, Scientific and Medical) de los 2'4 GHz	Julio de 1997
802.11a	Operaciones de WLAN a velocidades de hasta 54 Mbps en la banda UNII (Unlicensed National Information Infraestructure) de los 5 GHz	Septiembre de 1999
802.11b	Operaciones de WLAN a velocidades de hasta 11 Mbps en la banda ISM (Industrial, Scientific and Medical) de los 2'4 GHz	Septiembre de 1999

Tabla ll.3 Especificaciones aprobadas de la normas 802.11, 802.11a y 802.11b

Especificaciones en borrador o aprobación condicional. (Ver tabla ll.4)

<i>Standard</i>	<i>Descripción</i>	<i>Estado actual</i>
802.11g	Extensión del 802.11b para velocidades de hasta 54 Mbps en la banda ISM (Industrial, Scientific and Medical) de los 2'4 GHz.	Borrador en Noviembre de 1999
802.15.1	Standard de PAN (Personal Área Network) basado en la especificación de Bluetooth, opera en la banda ISM (Industrial, Scientific and Medical) de los 2'4 GHz.	Aprobación condicional en Marzo de 2002

Tabla ll.4 Especificaciones en borrador o aprobación condicional.

Especificaciones en desarrollo. (Ver tabla ll.5)

<i>Standard</i>	<i>Descripción</i>
802.11e	Mejora del 802.11 Medium Access Control (MAC) para mejora y gestión de la calidad de servicio (QoS) y de los mecanismos de seguridad y autenticación.
802.11f	Prácticas recomendadas para el desarrollo de un Protocolo Inter-Access Point (IAPP) para obtener la interoperabilidad entre Access Points de distintos fabricantes a través de un sistema de distribución.
802.11h	Mejora del 802.11 Medium Access Control (MAC) y del 802.11a High Speed Physical Layer (PHY) en la banda de los 5 GHz, para cumplir con los requisitos de la regulación europea en dicha banda.

802.11i	Mejora del 802.11 Medium Access Control (MAC) para mejorar los mecanismos de seguridad y autenticación
802.15 TG2	Prácticas recomendadas para facilitar la coexistencia de entre WPAN (802.15) y WLAN (802.11)
802.15 TG3	Nuevo estándar para alta velocidad (20 Mbps o más) para WPAN

Tabla ll.5 Especificaciones en desarrollo.

2.5.1 Tecnología de operación de las redes inalámbricas

Estos canales en el estándar 802.11, en lo referente a la banda de los 2.4 GHz, define catorce canales para la comunicación inalámbrica, según su frecuencia central, con una separación de 5 MHz entre ellos. Sin embargo, hay que tener en cuenta que la disponibilidad de dichos canales se somete a las regulaciones de cada país. Así, en EEUU y Canadá sólo se dispone de los canales 1 a 11, mientras en Europa y Australia, podemos utilizar los trece primeros canales. *(Ver tablas ll.6)*

<i>Canal</i>	<i>Frecuencia central</i>	<i>Ancho de banda</i>
1	2412 MHz	2401 - 2423 MHz
2	2417 MHz	2406 - 2428 MHz
3	2422 MHz	2411 - 2433 MHz
4	2427 MHz	2416 - 2438 MHz
5	2432 MHz	2421 - 2443 MHz
6	2437 MHz	2426 - 2448 MHz
7	2442 MHz	2431 - 2453 MHz
8	2447 MHz	2436 - 2458 MHz
9	2452 MHz	2441 - 2463 MHz
10	2457 MHz	2446 - 2468 MHz
11	2462 MHz	2451 - 2473 MHz
12	2467 MHz	2456 - 2478 MHz
13	2472 MHz	2461 - 2483 MHz

Tabla ll.6 Canales.

Sin embargo, debido a la técnica de comunicación en espectro disperso empleada, el ancho de banda se expande más allá de la separación entre canales contiguos.

Como aproximación, se estima un ancho de banda de unos 22 MHz (más allá, la potencia emitida se sitúa en 30 dB por debajo de la frecuencia central) , por lo que cada canal emplea frecuencias de hasta 11 MHz por encima y por debajo de la frecuencia central, solapándose unos a otros.

Como resultado, dos dispositivos que empleen canales contiguos, o sin la debida separación, se crearán interferencias mutuamente, repercutiendo en las prestaciones de la red inalámbrica. Por lo tanto, es conveniente, en el caso de que existan varias redes inalámbricas en el mismo lugar, que se utilicen canales con la suficiente separación. Para evitar totalmente el solapamiento de los canales usados, se deben dejar cinco canales de separación. (*Ver figura 11.11*)

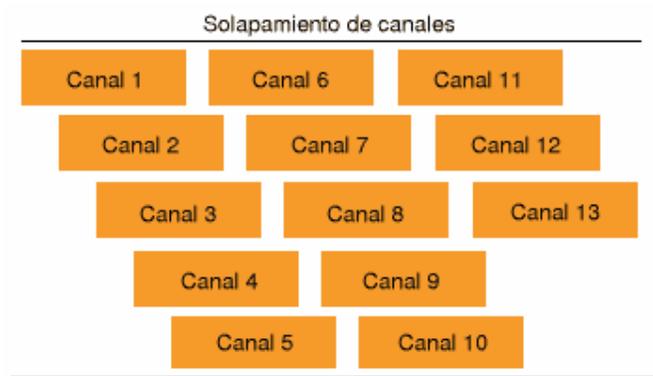


Figura 11.11 Solapamientos de canales.

Por lo tanto, esto nos lleva a que únicamente disponemos de tres canales (por ejemplo, el 1, el 6 y el 11) para una coexistencia sin interferencias de distintas redes wireless en el mismo área. Sin embargo, un análisis más profundo de la señal en redes wireless nos indica que la potencia se va reduciendo a medida que se separa de la frecuencia central, lo que nos permite en el caso de Europa, a utilizar hasta cuatro canales (1, 5, 9 y 13) con un solapamiento mínimo, y así las interferencias creadas apenas afectan a las prestaciones de la red.

Modos de funcionamiento.

El estándar 802.11 ofrece dos posibles Modos de operación de las redes wireless:

Modo Ad-Hoc o independiente

Es el modo de operación más simple de una red inalámbrica, actuando como una red punto a punto entre un conjunto de equipos con adaptadores wireless. No existen Puntos de Acceso ni ningún tipo de equipo que dé soporte a la red en sí.

La información viaja directamente entre el emisor y receptor sin pasar por ningún otro equipo. *(Ver figura ll. 12)*

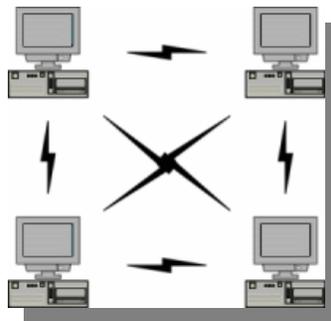


Figura ll.12 Modo Ad-Hoc o independiente.

Es más fácil, rápido y barato de establecer una red inalámbrica, pero presenta la enorme desventaja de que los equipos deben estar dentro del área de cobertura de los demás para comunicarse con ellos, por lo que sólo es aconsejable para redes con pocos equipos y próximos entre sí. Además, no existe un punto de interconexión con la red cableada, si ésta existiera, a no ser que alguno de los equipos actuara como un router.

Modo de infraestructura

Cada cliente wireless envía su información a un Punto de Acceso, que la hace llegar al destino adecuado.

La presencia de los Puntos de Acceso eleva el costo de inversión necesario para instalar una red wireless, pero ofrece numerosos beneficios gracias a sus capacidades. (Ver figura II. 13)

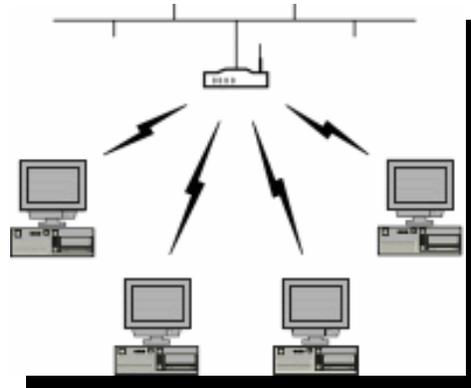


Figura II.13 Modo Infraestructura.

Los Puntos de Acceso permiten aumentar la cobertura de la red wireless, dado que los equipos clientes se comunican con él y no directamente entre sí, y por su condición de equipos fijos ubicados en zonas estratégicas y con antenas de más calidad, ofrecen una mayor cobertura y mejor fiabilidad del enlace. Además, existe la posibilidad de instalar varios puntos de acceso que actúen como repetidores para cubrir áreas mayores permitiendo el roaming de usuarios entre ellos.

Los Puntos de acceso actúan normalmente como puentes entre la red cableada y la red inalámbrica, lo que permite el acceso de los clientes wireless a los servicios de la red, aunque también pueden ofrecer servicios más avanzados, como servidores DHCP, así como la posibilidad del empleo de herramientas de seguridad y control de acceso a la red wireless.

En la propuesta realizaremos un análisis exhaustivo del escenario donde se va a desplegar la red wireless, estudiando las posibles localizaciones óptimas para la ubicación de los Puntos de Acceso, con el fin de reducir al máximo el costo de inversión necesario.

2.5.2 Seguridad

La utilización del aire como canal de comunicación hace a las redes wireless vulnerables a las escuchas y robos de información. Para proporcionar cierto nivel de seguridad, el estándar 802.11 define métodos de autenticación:

WEP

El protocolo Wired Equivalent Privacy es un protocolo de seguridad basado en el algoritmo RC4 utilizado por las normas 802.11 para seguridad de las comunicaciones inalámbricas. Emplea una clave de una determinada longitud que se debe introducir en cada uno de los dispositivos de la red. Sin embargo, dicha clave es fácilmente deducible mediante programas de libre acceso si se recoge la suficiente cantidad de información de la red wireless.

Los dispositivos wireless admiten claves de 64 y 128 bits; sin embargo, de este valor, se obtiene un vector de inicialización de 24 bits para el algoritmo RC4, por lo que las claves reales, de las que depende el nivel de seguridad, son de 40 y 104 bits.

Diversos estudios declararon que el protocolo WEP presenta graves problemas de seguridad, siendo el más importante de ellos el ataque que consiste en el análisis de paquetes de información cifrado con el mismo vector de inicialización y la misma clave.

Esta coincidencia ocurrirá tarde o temprano si no se renueva la clave de encriptación debido a lo reducido de la longitud del vector de inicialización (24 bits). Esto se puede evitar cambiando manualmente la clave WEP de la red wireless. Sin embargo, esta tarea consistiría en modificar la configuración de todos los equipos de una red, lo que puede convertirse en un trabajo bastante arduo a poco que se eleve el número de las computadoras en la red. La solución a este problema se encuentra en el estándar 802.11i, en fase borrador; para no esperar a la publicación oficial del mismo, la WECA lanzó el protocolo WPA como sustituto de las deficiencias del protocolo WEP.

WPA

Wi-Fi Protected Access (WPA) es un nuevo protocolo de seguridad desarrollado por la WECA para solucionar la debilidad del WEP. Este protocolo toma como base el borrador de la norma 802.11i, que aún se encuentra en fase de desarrollo.

WPA adopta la norma 802.1x para la autenticación de usuarios mediante el uso de un servidor RADIUS, donde se almacenan las credenciales y contraseñas de los usuarios de la red wireless. Para no obligar al uso de tal servidor para el despliegue de redes wireless, WPA permite la autenticación mediante clave compartida (PSK, Preshared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

La principal ventaja del WPA frente al WEP es que emplea un algoritmo de claves temporales (TKIP, Temporal Key Integrity Protocol), que automáticamente va cambiando las claves empleadas en la comunicación, por lo que se impide reproducir el ataque con el WEP dado que no se puede recoger la suficiente información cifrada bajo la misma clave.

Para obtener las mayores prestaciones del protocolo WPA, se requiere el uso de un servidor de autenticación externo como el RADIUS. Estas herramientas juntas, proporcionan una administración y un control de acceso centralizado de toda la red inalámbrica. Sin embargo, en redes pequeñas o domésticas no se dispone de un servicio como el RADIUS, por lo que el protocolo WPA permite operar en un modo más sencillo llamado PSK (PreShared Key), muy parecido al protocolo WEP, en el que se debe introducir una misma clave en todos los dispositivos de la red inalámbrica. Esta clave se emplea para autenticar al equipo en el momento del acceso a la red.

Autenticación Open System y Shared Key

Estos métodos de autenticación se realizan al comienzo de la comunicación entre un cliente wireless y un Punto de Acceso de la red.

A continuación de la autenticación, y si ésta se ha llevado a cabo de forma exitosa, se efectúa la asociación entre el cliente y el Punto de Acceso.

- **Open System.** Este método permite a cualquier dispositivo wireless acceder a la red siempre que el SSID que proporcione coincida con el del Access Point. Dado que el SSID se transmite sin cifrar en los paquetes de la red wireless, se obtiene fácilmente y por lo tanto, no ofrece ninguna garantía de seguridad. Además, opcionalmente, un cliente podría utilizar el SSID "ANY" para asociarse con cualquier Punto de Acceso que esté a su alcance, independientemente del valor real del SSID.
- **Shared Key.** Con este procedimiento, se exige al cliente poseer la misma clave WEP que posee el Punto de Acceso: el Punto de Acceso envía un texto en claro, denominado "desafío", al cliente, éste lo devuelve cifrado y el Punto de Acceso, lo descifra y lo compara con el texto inicial para verificar que ambos poseen la misma clave. Como vemos, la clave no viaja en ningún momento por la red, por lo que no puede ser obtenida a partir de escuchas pasivas de los mensajes; sin embargo, dada la debilidad del protocolo WEP, es posible obtener la clave recogiendo y analizando una cantidad determinada de tráfico en la red.

Medidas de seguridad recomendadas

Entre las posibles medidas que se pueden tomar en una red inalámbrica, se encuentran:

- Utilizar WEP. Aunque su grado de seguridad es cuestionado, ofrece un mínimo de privacidad. Siempre será mejor que nada.
- Emplear, si los dispositivos lo permiten, el protocolo WPA que permite la renovación automática de las claves de encriptación.
- Inhabilitar el servicio de DHCP para las redes dinámicas si no es estrictamente necesario.

- Mantener actualizados el firmware de los dispositivos para cubrir posibles agujeros en las diferentes soluciones wireless, con especial atención en los Puntos de Acceso.
- Utilizar Listas de Control de Acceso (ACL) de direcciones MAC, que permiten restringir los dispositivos clientes que pueden acceder a la red inalámbrica. Prácticamente la totalidad de los Puntos de Acceso comerciales poseen esta funcionalidad.
- Proporcionar un entorno físico seguro a los Puntos de Acceso y desactivarlos cuando se presentar periodos prolongados de inactividad.
- Cambiar el SSID por defecto que proporcionan los Puntos de Acceso, conocidos por todos: tsunami para Cisco, Intel para Intel, etc.
- Reducir la propagación de ondas de radio fuera del área de cobertura. Por ejemplo, evitando que salga al exterior de los edificios.
- Utilizar medidas de seguridad de red comunes como SSL, VPN, Firewalls, etc.

2.6 Servidores, plataformas y servicios

Windows 2003 Server es actualmente el principal sistema operativo en la gran mayoría de las empresas e Instituciones. Su versatilidad y estabilidad está más que probada y es uno de los pilares fundamentales de las redes corporativas. Su sistema centralizado de recursos basado en el Active Directory (Directorio Activo).

Es un ejemplo de estabilidad y escalabilidad rompiendo con todas las limitaciones de versiones anteriores. Incluyendo todos los servicios fundamentales: Servidor de archivos, DHCP, DNS, Wins, servicios de Terminal, que proporcionarán todo lo necesario para ofrecer una completa colección de servicios a una red de equipos Windows.

2.6.1 Servidor de Archivos

Este tipo de servidor en una red de computadoras nos ayudará a permitir el acceso remoto a archivos almacenados en él o directamente accesibles por este.

“En principio, cualquier computadora conectada a una red con un software apropiado como lo es Windows Server 2003, puede funcionar como un servidor de archivos. Desde el punto de vista del cliente de un servidor de archivos, la localización de los archivos compartidos es transparente. Normalmente no hay diferencias perceptibles si un archivo está almacenado en un servidor de archivos remoto o en el disco duro de la propia maquina.”⁶

Configurar el Servidor de Archivos

Para configurar un servidor de archivos, se iniciará el Asistente para configurar el servidor mediante una de las acciones siguientes:

Cuotas de disco del servidor de archivos

Dentro de estas puede configurarse cuotas de disco para realizar un seguimiento y controlar el uso del espacio en disco de los distintos usuarios en volúmenes NTFS. El Asistente para configurar el servidor aplica automáticamente cuotas de disco a los nuevos usuarios de cualquier sistema de archivos NTFS. Sólo se debe cambiar la información de la página “cuotas de disco de servidor de archivos” si se desea evitar que el servidor consuma una determinada cantidad de espacio en disco o si se tiene un espacio en disco limitado.

En la mayor parte de los casos, puede aceptarse la configuración predeterminada del sistema.

En esta forma puede especificarse si desea registrarse un suceso cuando un usuario supere el límite de espacio en disco especificado o cuando supere el nivel de advertencia de espacio en disco especificado (es decir, el punto en el que un usuario está próximo a su límite de cuota).

⁶ MICROSOFT CORPORATION. Windows Server 2003, implementación de servicios de red. USA: McGraw-Hill Interamericana, 2004, V. 7

Servicio de index server de servidor de archivos

Servicio de Index Server proporciona a los usuarios una manera rápida, fácil y segura de buscar información localmente o en la red. Los usuarios pueden buscar archivos en diferentes formatos e idiomas mediante el comando Buscar del menú Inicio o mediante páginas HTML que se muestran en un explorador.

En la página “Servicio de Index Server de servidor de archivos”, Se realiza una de las acciones siguientes:

- Si los usuarios buscan con frecuencia el contenido de los archivos del servidor, haga clic en Sí, para dejar activos los servicios de Index Server.
- Si desea conservar los recursos de memoria y CPU, haga clic en No, para desactivar los servicios de Index Server. El Servicio de Index Server puede disminuir el rendimiento del servidor.

Permisos

En la página Permisos, especifique los permisos de recurso compartido de la carpeta compartida. Para garantizar que sólo los usuarios autorizados tengan acceso a la información de la carpeta, es necesario establecer permisos en la carpeta creada. Los permisos de recurso compartido se aplican sólo a los usuarios que obtienen acceso al recurso a través de la red.

2.6.2 Servidor de correo electrónico

La idea de tener un propio servidor de correo electrónico es muy benéfica por la razón de considerar también el uso de Exchange.

A continuación exponemos seis razones por las que es aconsejable:

- Capacidad mejorada de uso del calendario.
- Exchange ofrece funciones ampliadas de correo electrónico que a su vez pueden mejorar la productividad de la Institución, en especial en el área de la colaboración.
- Por ejemplo, puede mostrar lado a lado vistas de los calendarios de compañeros de trabajo para ver la información de disponibilidad con el fin de planificar reuniones.
- Acceso al correo electrónico por Internet
- Exchange brinda a los usuarios acceso al correo electrónico, calendario y contactos a través de Internet mediante Outlook Web Access (OWA), que es un programa de correo electrónico incluido en Exchange que se ejecuta en su navegador. El concepto de OWA es similar al popular servicio de Hotmail, pero tiene el aspecto y muchas de las funciones de Outlook 2003.
- Con OWA, un usuario móvil puede iniciar una sesión en el servidor de Exchange con su nombre de usuario y contraseña, en todo lugar y momento, usando dispositivos como un equipo portátil y un teléfono móvil.

También está disponible la compatibilidad con Secure Sockets Layer (SSL) que ayuda a proteger estas conexiones de los piratas informáticos. El asistente instala también los servicios de servidor de seguridad que se requieren para frustrar los intentos de acceso de los piratas informáticos y otros intrusos.

Compartir información en carpetas públicas

Exchange permite el uso de calendarios compartidos tanto de Outlook 2003 como de Outlook Web Access (OWA). Al usar Exchange se cuenta con opciones adicionales para compartir en OWA.

OWA permite crear carpetas públicas, en las que puede almacenar mensajes de correo, documentos y otros tipos de archivos. En ellas se pueden copiar información cuando se necesite que todo el personal del Colegio que pueda consultarla y trabajar con ella.

Protección de datos integrada

Una de las preocupaciones de tener un servidor propio de correo electrónico es la protección de los mensajes y otros archivos almacenados en el servidor. Debe ser capaz de recuperar estos archivos en caso de que falle el servidor u ocurra cualquier otro problema.

Aquí es donde entra el asistente Server Backup Wizard. Este asistente ha sido creado para ayudar a hacer copias de seguridad de los servidores con mayor facilidad y menos problemas, y como guía durante todo el proceso. Con Outlook 2003 de Exchange, se contará con protecciones adicionales para la información. Outlook que permite al administrador y a los usuarios copiar mensajes de correo electrónico del servidor de Exchange a sus equipos.

Esto se logra usando una función de Outlook que sincroniza automáticamente los archivos de Exchange y de los equipos locales de manera que los usuarios tengan una copia actualizada de todo su correo en sus equipos personales.

No hay duda de que la idea de tener un propio servidor de correo electrónico Exchange Server 2003 podría resultar complicado, pero los asistentes de Windows Server simplifican todo el proceso. Además, se considera que realmente él Colegio aprovechará todas las ventajas de comunicación, productividad y optimización de trabajo que podría tener.

SMTP: Protocolo de Transferencia de Correo

Protocolo Simple de Transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc).

Funcionan con un conjunto de reglas limitado:

- Aceptan un mensaje entrante.
- Comprueban las direcciones del mensaje.

- Si son direcciones locales, almacenan el mensaje para después recuperarlo.
- Si son direcciones remotas, envían el mensaje.

Por tanto, los servidores SMTP son funcionalmente similares a los enrutadores de paquetes. Normalmente, un mensaje pasará a través de varias pasarelas SMTP antes de llegar a su destino final. En cada parada, el servidor SMTP evalúa el mensaje y lo almacena o lo envía.

También puede suceder que si el servidor SMTP encuentra un mensaje que no se puede enviar, este devuelva un mensaje de error al remitente explicando el problema.

POP: Protocolo de Oficina de Correos

El significado de las siglas POP es Post Office Protocol. Al contrario de otros protocolos creados con anterioridad como el SMTP, el POP no necesita una conexión permanente a Internet, puesto que en el momento de la conexión cuando solicita al servidor el envío de la correspondencia almacenada en el servidor será enviada para dicho usuario.

Si se está permanentemente conectado a Internet pueden configurarse los programas cliente de correo de tal forma que la petición al servidor de correo se efectúe automáticamente cada cierto tiempo y de esta forma avise al usuario de que tiene correo pendiente de recibir.

La situación actual es que se utiliza el protocolo SMTP para el envío y recepción de correo se utiliza el protocolo POP, pero ya en su tercera versión desde su aparición, el POP3.

2.6.3 Servidores de nombres DNS (Domain Name Service)

DNS es el servicio que básicamente ofrece la traducción de direcciones IP a nombres y viceversa. Este servicio es necesario porque los nombres son más fáciles de recordar que las direcciones IP.

El servicio de nombres funciona como una base de datos distribuida, de forma que cuando se busca traducir de un nombre a una dirección IP (por ejemplo cuando visitamos una dirección Web) se va consultando a servidores de nombres subiendo en una estructura jerárquica. Por la ruta indicada, llegará un momento que estos servidores se irán pasando llamadas descendiendo de nuevo hasta el servidor que contiene la traducción al nombre buscado. En este trayecto, se van usando las partes del nombre separadas por puntos, lo cual permite la estructura jerárquica.

En la configuración de un servidor de nombres se puede indicar zonas. Cada zona corresponde a lo que sería un sub-dominio. Cuando se configura una zona, se puede controlar esta zona (se actúa como amo en esa zona) o bien hay un servidor por debajo que se ocupa de ella (habría un servidor que actúa como esclavo).

La configuración de un servidor de nombres se hace en dos partes. En una se indica la configuración general del servidor, por ejemplo a qué redes atiende, si notifica los cambios a otros servidores, las zonas que se gestionan, etc. Por otro lado tenemos la configuración concreta de una zona, en la que se asocian nombres de computadoras y direcciones IP.

(Ver figura II.14).

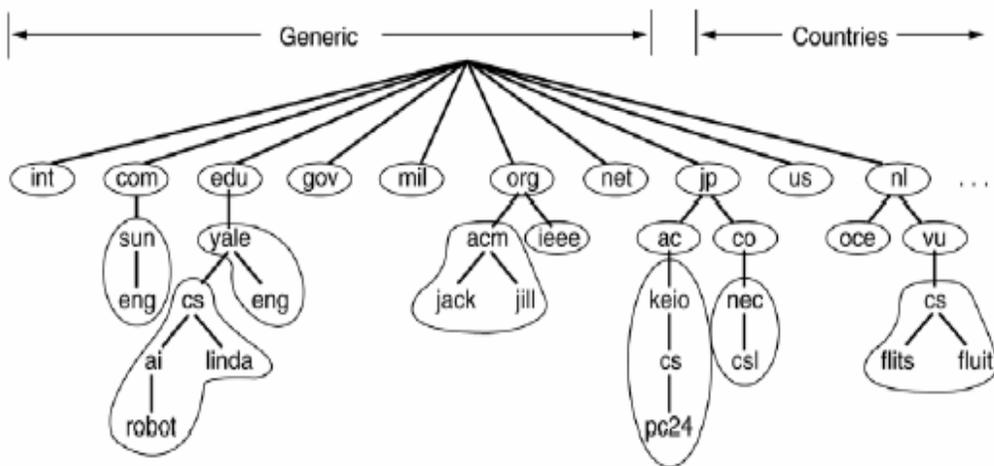


Figura II.14 Ejemplos de DNS.

Lo básico de todo esto es tener un acceso a Internet. Ese acceso debe de ser ininterrumpido y de ser posible mediante una dirección IP estática. Poder abrir y cerrar los puertos del enrutador es esencial para recibir y dar información.

Controlador de Dominios mediante Active Directory

“Es un sistema que sirve para compartir recursos en un conjunto de dominios. Para ello utiliza un sistema común de resolución de nombres (DNS) y un catálogo común que contiene una réplica completa de todos los objetos de directorio del dominio en que se aloja además de una replica parcial de todos los objetos de directorio de cada dominio del bosque.”⁷

El objetivo de un catálogo global es proporcionar autenticación a los inicios de sesión. Además contiene información sobre todos los objetos de todos los dominios del bosque, la búsqueda de información en el directorio no requiere consultas innecesarias a los dominios. Una única consulta al catálogo produce la información sobre donde se puede encontrar el objeto.

Con Active Directory se agilizan las búsquedas de recursos, se asegura la autenticación de usuarios y máquinas, se comparten mejor los recursos de la red, se abandona Netbios como protocolo para compartir recursos, ahora se resuelven mediante DNS y el catálogo global.

En redes grandes, es muy útil que se puedan dividir en dominios mas pequeños, centros de trabajo con varios dominios y redes intranet donde hay sucursales que comparten recursos. Puede incluir cada objeto individual (impresora, archivo o usuario), cada servidor y cada dominio en una sola red de área amplia. También puede incluir varias redes de área amplia combinadas.

⁷ ANTONI Barba Marti. Gestión de Red. México: Alfa-Omega, 2001. 54 p.

Servicio de directorio de Active Directory

Es uno de los componentes más importantes de una red. Los usuarios y administradores con frecuencia no saben el nombre exacto de los objetos en que están interesados. Quizá conozcan uno o más atributos de los objetos y puedan consultar el directorio para obtener una lista de objetos que concuerden con los atributos: por ejemplo, "Encontrar todas las impresoras Láser". Un servicio de directorio permite que un usuario encuentre cualquier objeto con sólo uno de sus atributos.

Objeto

Es cualquier cosa que tenga entidad en el directorio. Puede ser un programa, un usuario, una computadora, un enrutador, una impresora, un Proxy.

Dominio

Es un conjunto de normas que especifican, administran los recursos y los clientes en una red local. En un dominio hay lo que se llama un servidor principal llamado PDC (Primary Domain Controller) que es quien asigna derechos controla usuarios y recursos.

Árbol

Es un conjunto de dominios con relaciones de confianza entre sí que comparten recursos, clientes y un sistema de resolución de nombres.

Bosque

Es un conjunto de árboles de dominio con relaciones de confianza entre sí.

Active directory no controla computadoras, controla dominios y administra los recursos y clientes de esos dominios. Utiliza DNS como sistema de resolución de nombres (debe haber obligatoriamente uno). Active directory es accesible desde cualquier servidor de dominio.

Para empezar a planificar la administración de nuestro servidor es necesario empezar con hacernos algunas preguntas; ¿Qué estructura tiene el Colegio? Para responder a esto es necesario conocer completamente la red institucional (todas las subredes con sus características). También es necesario conocer completamente la jerarquía administrativa.

Una norma fundamental a la hora de planificar la estructura es siempre la siguiente: La solución más simple siempre es la correcta.

Aquí habrá que considerar algunas cuestiones con el servidor DNS por lo que llegado a este punto se deberá tener una idea clara de los recursos que va a necesitar cada área. El administrador de área deberá tener ya establecido claramente como va a funcionar cada cosa y que recursos necesita para ello.

Además se configura también el dominio raíz y el sistema de copia de seguridad sea cual sea. Normalmente se pone un servidor y otro que funge como seguridad ante desastres.

IIS (Internet Information Server)

Los Servicios de IIS 6.0 con el sistema operativo Microsoft Windows Server 2003 proporcionan una funcionalidad de servidor Web integrada, confiable, escalable, segura y administrable a través de una intranet, Internet o una Extranet. Es una herramienta para crear una sólida plataforma de comunicaciones de aplicaciones de red dinámicas. Organizaciones de todos los tamaños utilizan IIS para alojar y gestionar páginas Web en Internet o en su intranet, para alojar y gestionar sitios FTP.

Aprovecha los últimos estándares Web como Microsoft ASP.NET, XML y el Protocolo simple de acceso a objetos (SOAP) para el desarrollo, la implementación y la administración de aplicaciones Web. IIS 6.0 incluye nuevas funciones diseñadas para ayudar a las organizaciones, los profesionales de TI y los administradores de servidores a conseguir sus objetivos de rendimiento, confiabilidad, escalabilidad y seguridad para miles de sitios Web en un único servidor IIS o en varios servidores.

2.6.4 Servidor DHCP (Dynamic Host Configuration Protocol)

Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuanto tiempo la ha tenido y a quien se la ha asignado después.

El protocolo DHCP es muy utilizado en la administración de redes, ya que permite que los equipos configuren automáticamente los parámetros de red (dirección IP, máscara de red, dirección de difusión, enrutador por defecto, servidor de nombres).

El funcionamiento de DHCP es muy flexible; permite ofrecer dinámicamente direcciones prestadas temporalmente (leasing) u ofrecer una configuración fija a partir del dispositivo de red concreto (dirección Ethernet).

En la configuración dinámica cuando una computadora solicita una configuración, se le presta temporalmente una disponible de entre un intervalo previamente especificado en el servidor.

Las computadoras que se configuran a través del protocolo DHCP necesitan ejecutar (normalmente en el proceso de inicio) un cliente DHCP.

El funcionamiento del protocolo DHCP se resume en los siguientes pasos:

- Petición de parámetros de red.
- El cliente difunde una petición con dirección origen 0.0.0.0 y dirección destino 255.255.255.255. En este mensaje se incluye la dirección Ethernet de la tarjeta de red de esta forma se puede realizar una configuración fija para esa computadora, además de poderle contestar directamente.
- El servidor contesta con los parámetros de red:
 - Dirección IP, máscara, puerta de salida, nombre del dominio, nombre de los servidores de nombres, duración del préstamo (si es una configuración dinámica) y dirección IP del propio servidor (por si hay que renovar el préstamo).
- Comunicación de aceptación.
- El cliente difunde un mensaje de aceptación para que otros servidores DHCP no le hagan otra propuesta.
- El servidor DHCP envía un mensaje de reconocimiento al cliente.
- El cliente ya puede usar los parámetros que recibió.
- Antes de que expire el tiempo del préstamo, el cliente vuelve a enviar una petición al servidor DHCP.

Es importante indicar que el servidor que se utiliza de DHCP no es necesario que esté en la misma red de área local que los clientes.

El protocolo DHCP es especialmente útil cuando los equipos de la red se distribuyen en varias subredes físicas, y además los equipos cambian de ubicación (de subred) con cierta frecuencia. En este caso, cambiar el equipo de sitio no supone nunca reconfigurar manualmente sus parámetros de red, sino simplemente conectarlo a la nueva red y arrancarlo.

Concesión y Renovación de DHCP

Un cliente DHCP obtiene una concesión para una dirección IP del servidor DHCP. Antes que se acabe el tiempo de la concesión, el servidor DHCP debe renovar la concesión al cliente o bien este deberá obtener una nueva concesión. Estas se guardan en la base de datos del servidor DHCP aproximadamente un día después de que se agote su tiempo. Este periodo de gracia protege la concesión del cliente en caso de que este y el servidor se encuentren en diferentes zonas horarias, de que sus relojes internos no estén sincronizados o en caso de que el cliente esté fuera de la red cuando caduca el tiempo de la concesión.

La primera vez que inicia un cliente DHCP e intenta unirse a una red, se realiza automáticamente un proceso de inicialización para obtener una concesión del servidor

DHCP:

- El cliente DHCP solicita una dirección IP difundiendo un mensaje DHCP Discover.
- El servidor responde con un mensaje DHCP Offer proporcionando una dirección al cliente.
- El cliente acepta la oferta respondiendo con un mensaje DHCP Request.
- El servidor envía un mensaje DHCP Ack indicando que aprueba la concesión.
- Cuando el cliente recibe la confirmación entonces configura sus propiedades TCP/IP usando la información de la respuesta DHCP.

En raras ocasiones el servidor DHCP puede devolver una confirmación negativa al cliente. Esto suele ocurrir si el cliente solicita una dirección no válida o duplicada. Si un cliente recibe una confirmación negativa (DHCP Nack), entonces deberá comenzar el proceso de concesión. Cuando se inicia un cliente que ya tenía concedida una dirección IP previamente, este debe comprobar si dicha dirección sigue siendo válida. Para ello, difunde un mensaje DHCP Request en vez de un mensaje DHCP Discover.

El mensaje DHCP Request contiene una petición para la dirección IP que se le asignó previamente. Si el cliente puede usar la dirección IP solicitada, el servidor responde con un mensaje DHCP Ack.

Si el cliente no pudiera utilizarla porque ya no es válida, porque la esté usando otro cliente o porque el cliente se ha desplazado físicamente a otra subred, entonces el servidor responde con un mensaje DHCP Nack, obligando al cliente a reiniciar el proceso de concesión. Si el cliente no consigue localizar un servidor DHCP durante el proceso de renovación, entonces este intenta hacer un ping al gateway predeterminado que se lista en la concesión actual.

Si tiene éxito, el cliente DHCP supone que todavía se encuentra en la red en la que obtuvo la concesión actual y la seguirá usando. En segundo plano, el cliente intentará renovar la concesión actual cuando se agote el 50% del tiempo de la concesión asignada.

III. DEFINICIÓN DEL PROBLEMA

3.1 Diagnóstico actual de la red de cómputo del Colegio Asesoría Educativa Queen Mary School S.C.

El Colegio Asesoría Educativa Queen Mary School S.C. (QMS) es una construcción que consta de siete edificios distribuidos en una misma área (*Ver figura III.1*) que consta de:

1. Edificio Administrativo (Oficinas Administrativas, Direcciones de Secundaria y Preparatoria y acceso principal a las instalaciones). *^b
2. Edificio de Secundaria (Salones de Secundaria). *^b
3. Edificio de Preparatoria (Salones de Preparatoria, Biblioteca, Salón de Actos y laboratorios de Química y Física). *^c
4. Edificio Laboratorio de Cómputo (Lab. 35 y 36, Salón de Usos Múltiples). *^a
5. Edificio de Primaria 1 (Salones de Primaria, Servicios Escolares de Primaria, Salón de Juntas de Padres y Cubículo de coordinación de inglés preescolar y primaria). *^b
6. Edificio de Primaria 2 (Dirección de Primaria, Salón de Profesores de Primaria y Salones de Primaria). *^b
7. Edificio de Preescolar (Salones de Primaria y Preescolar, Dir. Preescolar y Lab. 50 de Cómputo). *^b

*^a Dos niveles en cada edificio (planta baja y primer piso).

*^b Tres niveles en cada edificio (planta baja, primer y segundo pisos).

*^c Cuatro niveles en cada edificio (planta baja, primer, segundo y tercer pisos).

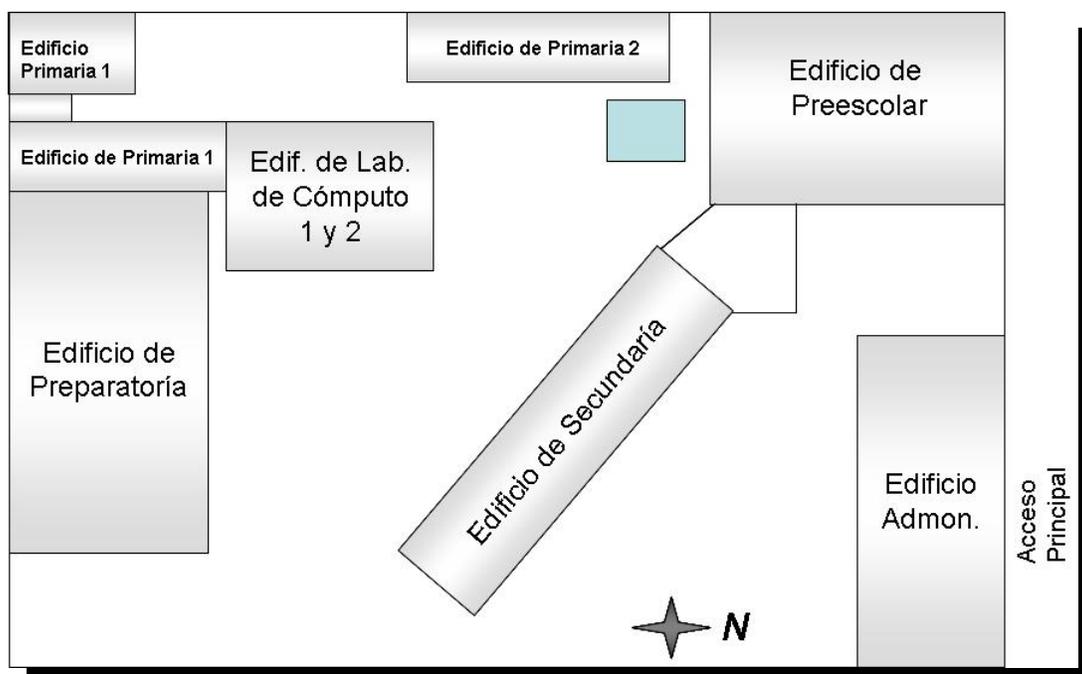


Figura III.1. Esquema de los siete edificios que conforman el QMS.

Para hacer referencia a cada uno de estos edificios con sus departamentos ó áreas se utilizarán en adelante los siguientes acrónimos. Así También para especificar el nivel del departamento del edificio al que nos estaremos refiriendo hemos propuesto un número para incluir el nivel.

EAD: Edificio Administrativo. (Ver tabla III.1)

Acrónimo	Departamentos ó áreas	Nivel
EADsc	Secretaria General	1
EADdp	Dirección Pedagógica.	1
EADse	Dirección de Secundaría.	1
EADpp	Dirección de Preparatoria.	1
EADsj	Sala de Juntas.	1
EADcu	Cubículos.	1
EADdg	Dirección General.	2

CAPÍTULO III DEFINICIÓN DEL PROBLEMA

EADc	Contabilidad.	2
EADcj	Caja.	2
EADcd	Coordinación Deportiva.	2
EADci	Coordinación de Inglés Post-Primaria.	3
EADps	Coordinación de Psicopedagogía.	3
EADlg	Logística.	3
EADsi	Salones de Inglés	3
EADsm	Salón de maestros secundaria y preparatoria	3

Tabla III.1 EAD

ESE: Edificio Secundaria. (Ver tabla III.2)

Acrónimo	Departamentos ó áreas	Nivel
ESEs1	Salón 1	1
ESEs2	Salón 2	1
ESEs3	Salón 3	1
ESEcf	Cafetería.	1
ESEs4	Salón 4	2
ESEs5	Salón 5	2
ESEs6	Salón 6	2
ESEs7	Salón 7	2
ESEs8	Salón 8	3
ESEs9	Salón 9	3
ESEs10	Salón 10	3
ESEs11	Salón 11	3

Tabla III.2 ESE

EPP: Edificio de Preparatoria. (Ver tabla III.3)

Acrónimo	Departamentos ó áreas	Nivel
EPPc	Cocina.	1
EPPb	Biblioteca.	1
EPPs	Salones de preparatoria.	2
EPPs	Salones de preparatoria.	3
EPPsa	Salón de actos.	3
EPPs	Salones de preparatoria.	4
EPPqf	Salones de Química y Física.	4

Tabla III.3 EPP

ELC: Edificio de Laboratorio de Cómputo. (Ver tabla III.4)

Acrónimo	Departamentos ó áreas	Nivel
ELCum	Salones de Usos Múltiples.	1
ELCic	Salones de Cómputo 35 y 36.	2

Tabla III.4 ELC

EP1: Edificio de Primaria. (Ver tabla III.5)

Acrónimo	Departamentos ó áreas	Nivel
EP1s	Salones de Primaria	1
EP1se	Servicios Escolares	1
EP1ci	Coordinación de Ingles	1
EP1sj	Salones de Junta de Padres	2
EP1s	Salones de Primaria	2

Tabla III.5 EP1

EP2: Edificio de Primaria 2. (Ver tabla III.6)

Acrónimo	Departamentos ó áreas	Nivel
EP2d	Dirección de Primaria	1
EP2sm	Salón de Maestros	2
EP2s	Salones de Primaria.	2

Tabla III.6 EP2

EPR: Edificio de Preescolar. (Ver tabla III.7)

Acrónimo	Departamentos ó áreas	Nivel
EPRspr	Salones de Preescolar.	1
EPRspm	Salones de Primaria.	1
EPRdp	Dirección de Preescolar.	1
EPRlc50	Laboratorio de Cómputo Salón 50.	2
EPRspm	Salones de Primaria.	2
EPRspr	Salones de Preescolar.	2
EPRspm	Salón de primaria.	3
EPRsap	Salón de artes plásticas.	3

Tabla III.7 EPR

3.2 Análisis de cada una de las áreas que conforman al Colegio

Edificio Administrativo (EAD)

La infraestructura actualmente instalada en el edificio administrativo, consiste en una red inalámbrica en cuanto a medio de comunicación se refiere. *(Ver tabla III.8)*

No. Pisos	No. Equipos			Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
3	11 nivel 1	6 nivel 2	6 nivel 3	Inalámbrica 11 Mbps.	En 1 repisa de Cristal.	1 Modem/Ruter Efficient Router 5200 AR5 Wireless con además 8 puertos LAN 10/100 Ethernet
Nivel 1, nivel 2 y nivel 3	Total 23 equipos conectados a una tarjeta inalámbrica USB Wireless-B 802.11g Linksys.			Wireless-B 802.11g Linksys.	Dispositivos de conectividad.	Puerta de salida o “default gateway” al que provee Prodigy Infinitum de Telmex. Proporciona el servicio de Internet de Banda ancha que permite conexión permanente a Internet a una velocidad de 1 Mbps.

Tabla III.8 Descripción de la red en EAD

EAD (nivel 1 ó Planta Baja)

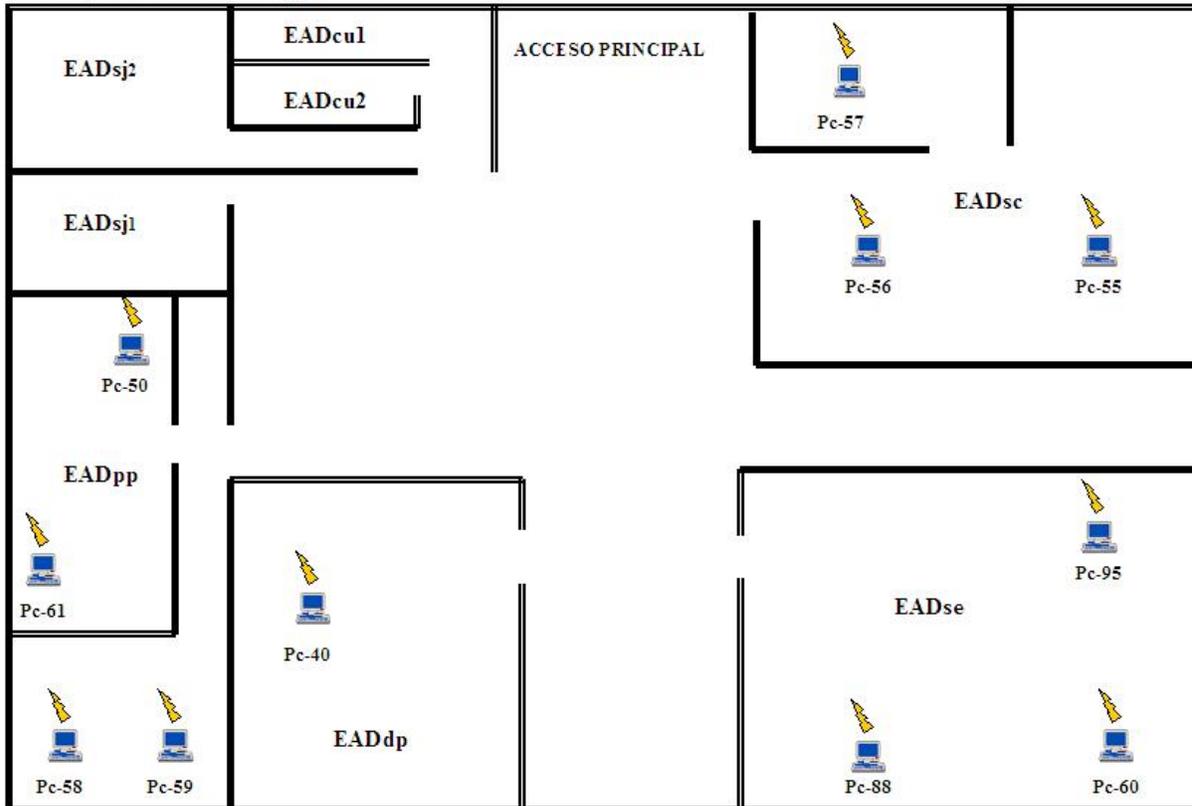


Figura III.2 Esquema del Edificio Admón. Nivel 1 ó Planta Baja.

En la planta baja del edificio administrativo se encuentran las áreas directivas y administrativas de secundaria, preparatoria, pedagogía y área de secretarías, así como salas de juntas y cubículos para entrevistas. (Ver Figura III.2)

Equipos Clientes Fijos Instalados actualmente: 11

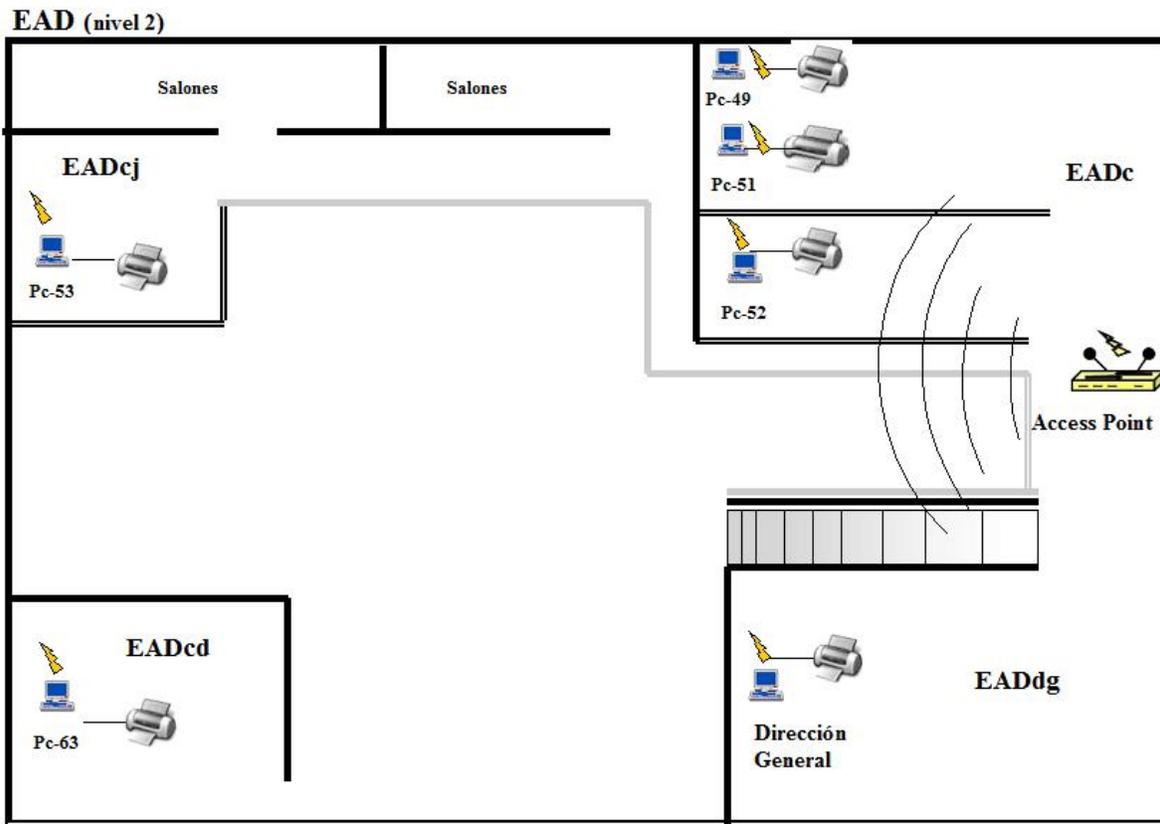


Figura III.3 Esquema del Edificio Admón. Nivel 2.

En el piso segundo del edificio administrativo se encuentran la oficina de Dirección General, Dirección Adjunta, Contabilidad, Caja, y la Coordinación Deportiva. (Ver Figura III.3)

Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo ya que la información que se maneja aquí es de suma importancia y confidencial.

Debemos señalar que es aquí en el segundo piso donde tenemos instalado el Modem/Ruteador que da servicio de Internet a todo el edificio.

Equipos Clientes Fijos Instalados actualmente: 6

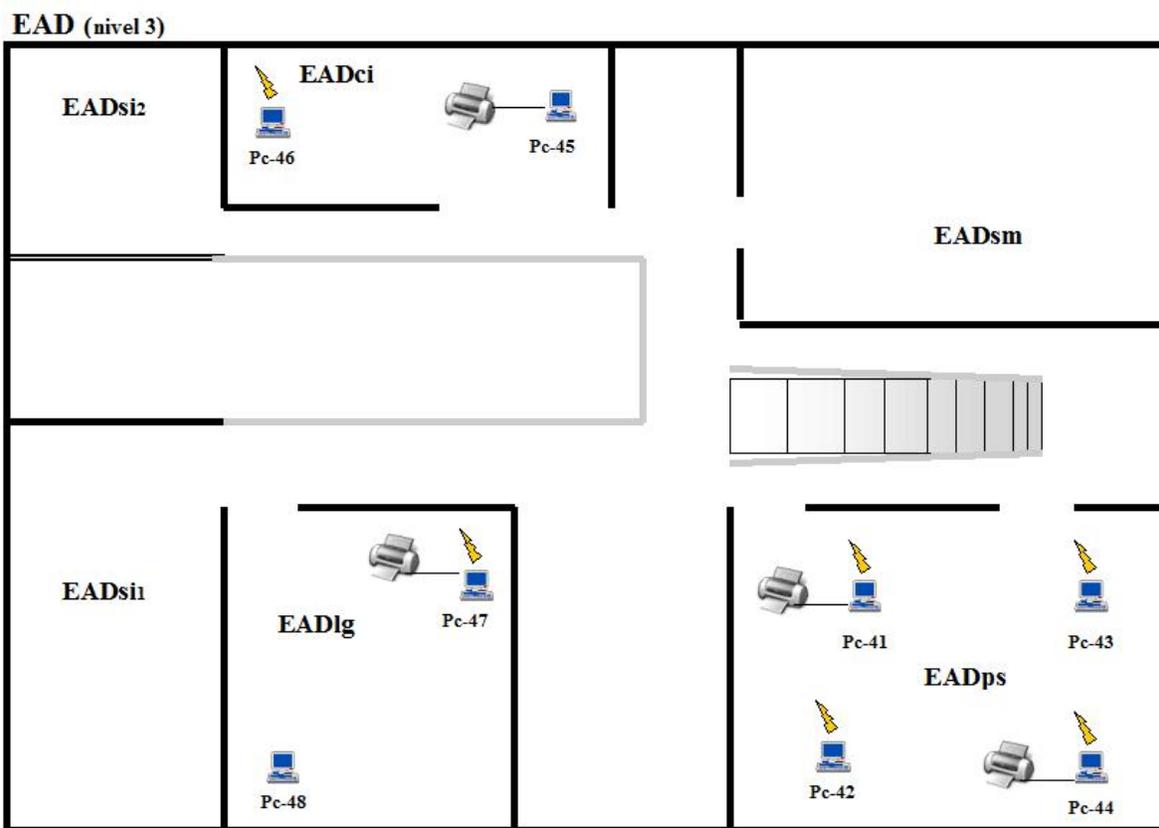


Figura III.4 Esquema del Edificio Admón. Nivel 3.

En el piso tercero del edificio administrativo se encuentran la coordinación de inglés, la coordinación de psicopedagogía y logística, además el salón de maestros de preparatoria y secundaria y dos salones de inglés. (Ver Figura III.4)

Equipos Clientes Fijos Instalados actualmente: 6

Edificio de Secundaria (ESE)

Actualmente en este edificio no existe una red de computadoras, por lo cual estamos proponiendo crear una red para que los profesores y alumnos cuenten con acceso a Internet en el salón de clases.

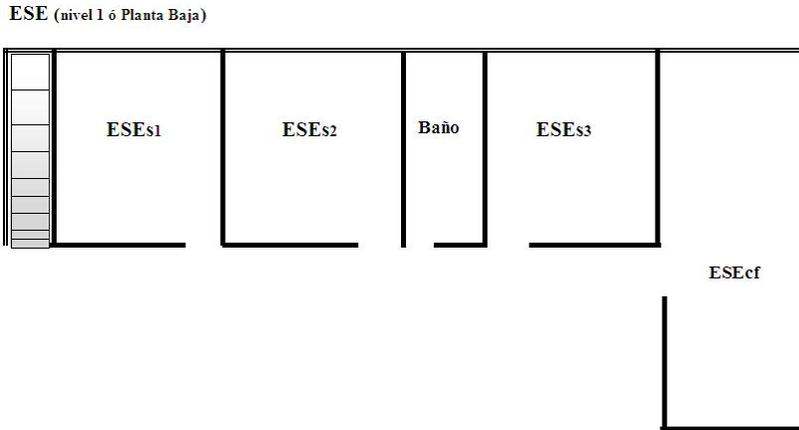


Figura III.5 Esquema del Edificio de Secundaria. Nivel 1 ó Planta Baja.

Se desea instalar un nodo en cada salón de clases, así como en la cafetería. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo. (Ver Figura III.5)

Nodos Instalados actualmente: 0

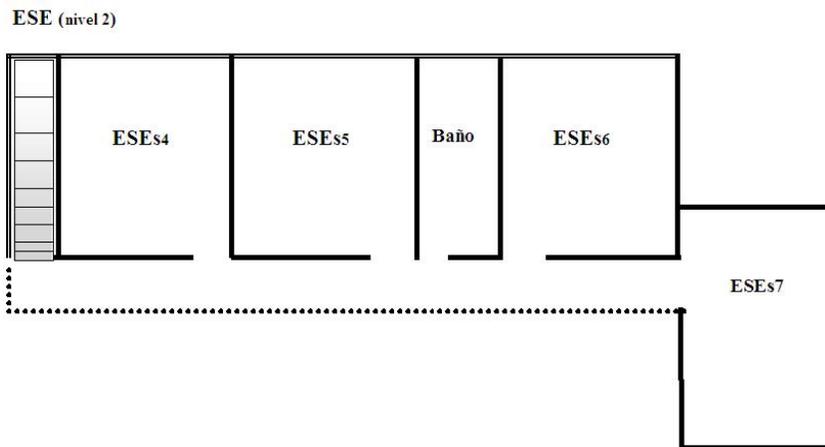


Figura III.6 Esquema del Edificio de Secundaria. Nivel 2.

Se propone instalar un nodo en cada salón de clases. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo. (Ver Figura III.6)

Nodos Instalados actualmente: 0

ESE (nivel 3)

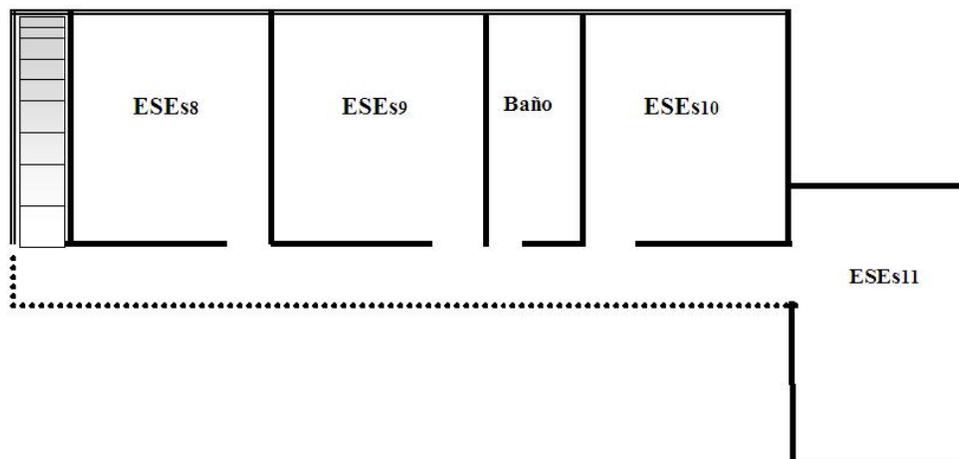


Figura III.7 Esquema del Edificio de Secundaria. Nivel 3.

Se desea instalar un nodo en cada salón de clases. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo. (Ver *Figura III.7*)

Nodos Instalados actualmente: 0

Edificio de Preparatoria (EPP)

No. Pisos	No. Equipos			Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
4	3 nivel 1	0 nivel 2	1 nivel 3	Cableado.	Conectado a ELC.	Conexión con ELCc.
	1 nivel 4					
nivel 1, nivel 2, nivel 3 y nivel 4	2 equipos conectados por UTP Nivel 5e. y 3 sin red. Total: 5			Tendido de cable UTP Nivel 5e (a 350 MHz.)		

Tabla III.9 Descripción de la red en EPP

Actualmente en el edificio de preparatoria existen cinco computadoras tres en la biblioteca, una en el salón de actos y otra más el laboratorio de Química y Física. (Ver Tabla III.9)

Por lo cual estamos proponiendo crear una red para que los profesores y alumnos cuenten con acceso a Internet en cada salón de clases y aumentar el número de equipos en la biblioteca y que toda computadora de este edificio tenga acceso al Internet, en donde deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo.

EPP (nivel 1 ó Planta Baja)

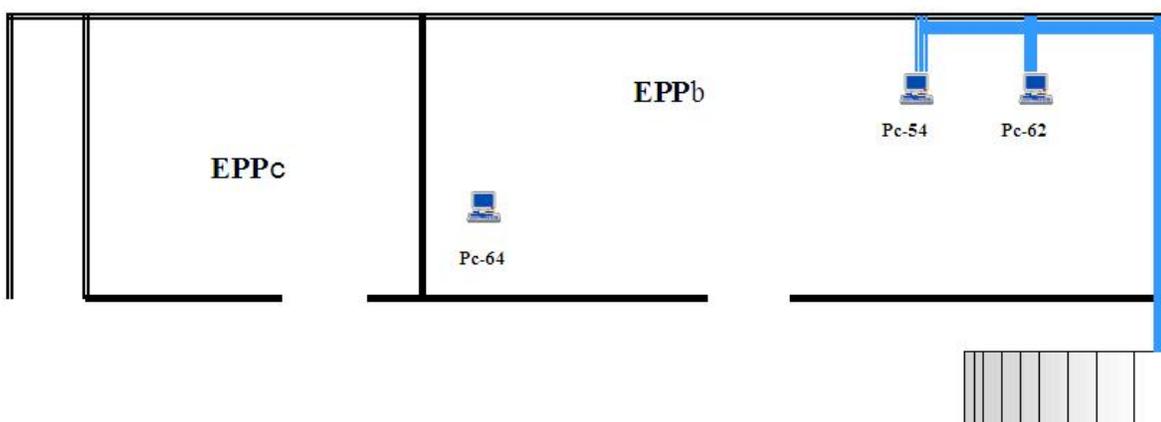


Figura III.8. Esquema del Edificio de Preparatoria. Nivel 1.

En esta área de tres computadoras que hay, solo dos computadoras tienen acceso al Internet que estas conectadas a la red del ELC (edificio de laboratorio de cómputo) con un tendido de cableado estructurado Nivel 5 (100 MHz) conectado al 3com Hub 16c Ethernet 10/100 de 16 puertos, y este proveniente del Ruteador y Modem que se encuentran en el edificio de laboratorio de cómputo 35 y 36 descrito mas adelante. (Ver Figura III.8)

Nodos Instalados actualmente: 2

EPP (nivel 2)

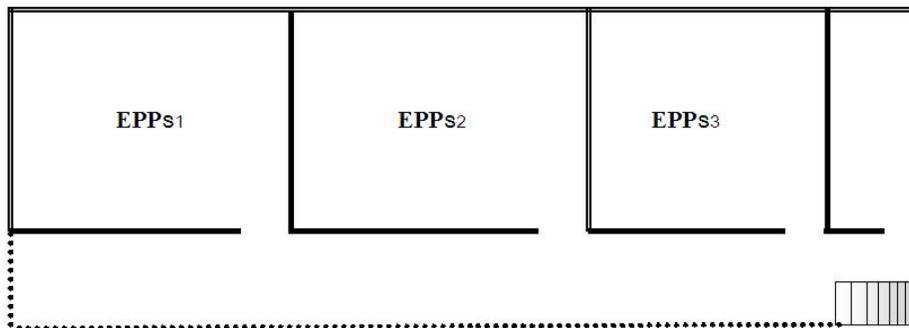


Figura III.9. Esquema del Edificio de Preparatoria. Nivel 2.

Se propone instalar un nodo en cada salón de clases. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo. (Ver *Figura III.9*)

Nodos Instalados actualmente: 0

EPP (nivel 3)

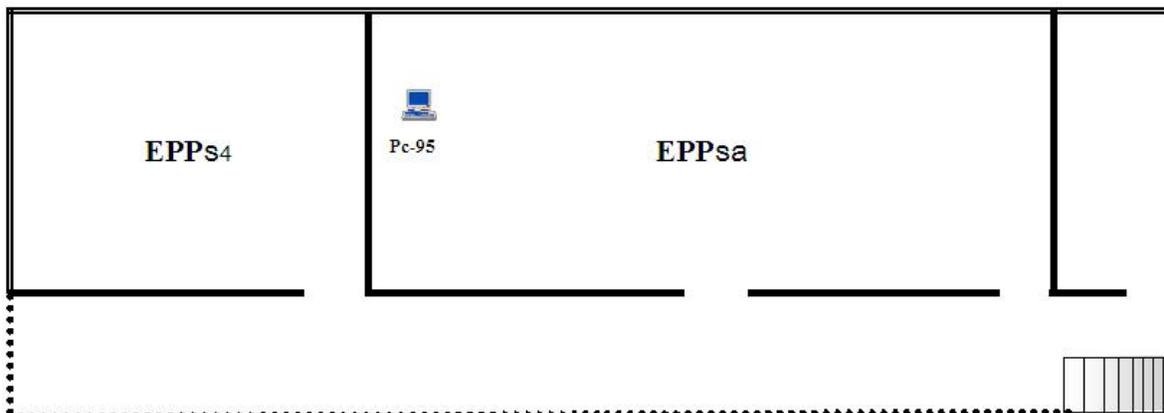


Figura III.10. Esquema del Edificio de Preparatoria. Nivel 3.

Solo se cuenta con una computadora sin conexión a red. (Ver *Figura III.10*)

Nodos Instalados actualmente: 0

EPP (nivel 4)

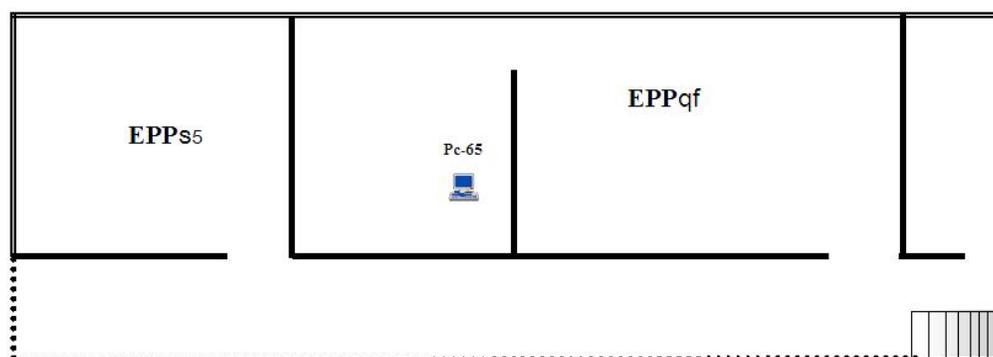


Figura III.11 Esquema del Edificio de Preparatoria. Nivel 4.

Se propone instalar un nodo en el salón s5 y conectar al Internet la PC-65 del laboratorio de Química y Física. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo. *(Ver Figura III.11)*

Nodos Instalados actualmente: 0

Edificio de Laboratorio de Cómputo (ELC)

No. Pisos	No. Equipos		Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
2	4 Profesores	30 Alumnos	Cableado.	1 rack de muro.	1 Modem 1000 ADSL –LP Alcatel Home 10 Base T/MDI-X.
	2 Biblioteca				
Salón 35 y 36.	Total 36 equipos cableados directamente a los dispositivos activos.		alámbrica con un tendido de cable UTP Nivel 5e (a 350 MHz) tubería de PVC de 14mm	2 Hub's 3 Com Ethernet 10/100 de 16 puertos. 1 Switch 3 Com Baseline Switch 2824 10/100/1000 Ethernet de 24 puertos.	Puerta de salida o "default gateway" al que provee Prodigy Infinitum de Telmex.
				1 Ruteador USB Robotics 8000 capa 1 de 4 puertos LAN 10/100 Ethernet.	Banda ancha permanente a Internet a una velocidad de 1 Mbps.

Tabla III.10 Descripción de la red en ELC

Actualmente en el edificio de laboratorio de cómputo cuenta con dos niveles en la planta baja esta el salón de usos múltiples donde no existe ningún nodo para tener red, en el nivel 2 tenemos dos laboratorios de cómputo el salón 35 y 36. (Ver tabla III.10).

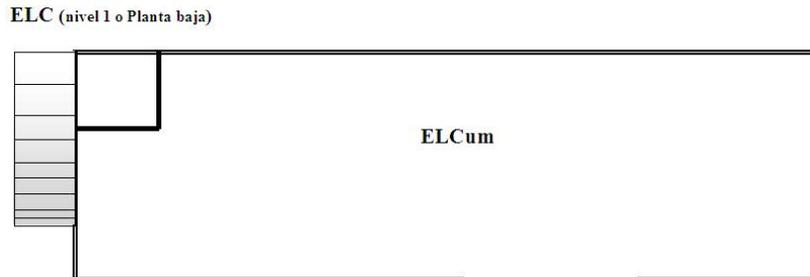


Figura III.12 Esquema del Edificio de ELC Salón de usos múltiples. Nivel 1.

Se propone instalar un nodo en el ELCum. Para tener acceso a la Internet. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo. (Ver Figura III.12)

Nodos Instalados actualmente: 0

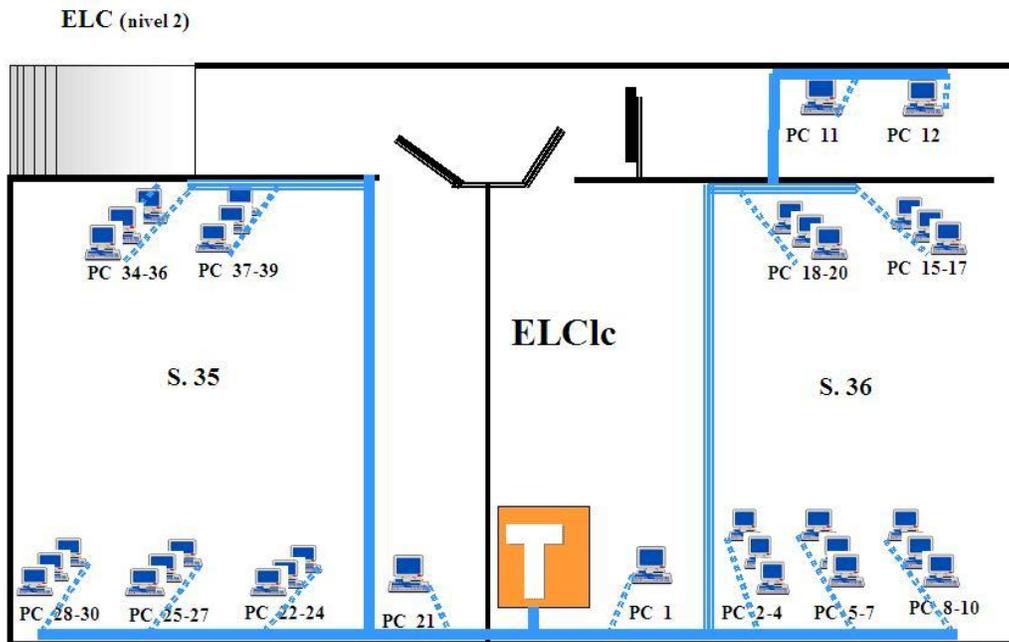


Figura III.13 Esquema del Edificio de Lab. de Cómputo salones 35 y 36. Nivel 2.

Laboratorio de cómputo con 34 maquinas para uso académico. *(Ver figura III.13)*

Nodos Instalados actualmente Profesores: 4

Nodos Instalados actualmente Alumnos: 30

Edificio Primaria 1. (EP1)

No. Pisos	No. Equipos		Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
2	4 nivel 1	0 Nivel 2	Cableado.	Conexión con Edificio	Conexión con EP2
nivel 1 y nivel 2	2 equipos conectados por UTP Nivel 5e.y 2 sin red. Total: 4		tendido de cable UTP Nivel 5e (a 350 MHz)	Hub 3com 8ptos.	

Tabla III.11 Descripción de la red en EP1

Actualmente en el edificio de primaria1 existen cuatro computadoras, de las cuales solo dos de ellas cuentan con servicio de Internet, por lo cual estamos proponiendo crear una red para que los profesores y alumnos cuenten con acceso a Internet en los salones de clases. En donde deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo. *(Ver tabla III.11).*

EP1 (nivel 1 ó Planta Baja)

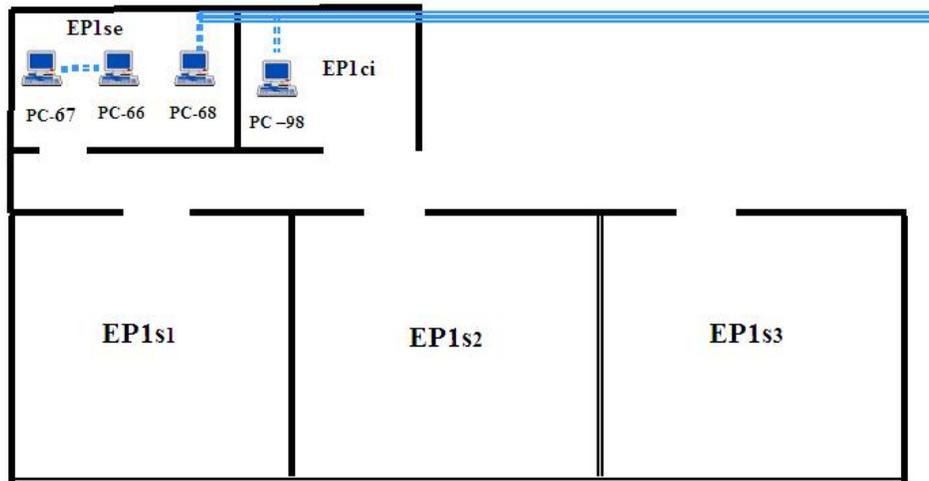


Figura III.14 Esquema del Edificio de Primaria 1. Nivel 1.

En el área de servicios escolares, la coordinación de inglés de preescolar y primaria es donde tenemos cuatro computadoras pero solo dos de ellas la pc-68 y la pc-98 cuentan con salida a Internet. (Ver Figura III.14)

Nodos Instalados actualmente: 2

EP1 (nivel 2)

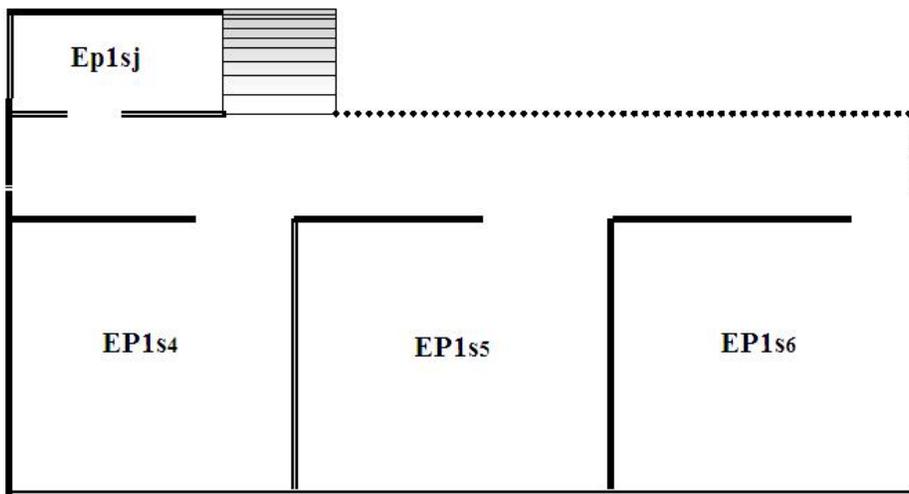


Figura III.15 Esquema del Edificio de Primaria 1. Nivel 2.

No se cuenta con ninguna computadora. (Ver Figura III.15)

Nodos Instalados actualmente: 0

Edificio Primaria 2. (EP2)

No. Pisos	No. Equipos		Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
2	1 nivel 1	1 Nivel 2	Cableado.	En 1 Armario	Modem DSL 2WIRE Gateway 2070 LAN Ethernet 10/100
nivel 1 y nivel 2	1 equipos conectados por UTP Nivel 5e. y 1 sin red. Total: 2		tendido de cable UTP Nivel 5e (a 350 MHz)	1 Hub Trendnet TE-800 Ethernet 10/100 de 8 puertos.	Prodigy Infinitum de Telmex (Teléfonos de México). conexión permanente a Internet a una velocidad de 1 Mbps.

Tabla III.12 Descripción de la red en EP2

Actualmente en el edificio de primaria 2 existen dos computadoras, de las cuales solo dos de ellas cuentan con servicio de Internet, por lo cual estamos proponiendo crear una red para que los profesores cuenten con acceso a Internet.

En donde deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo. (Ver tabla III.12)

EP2 (nivel 1 ó Planta Baja)

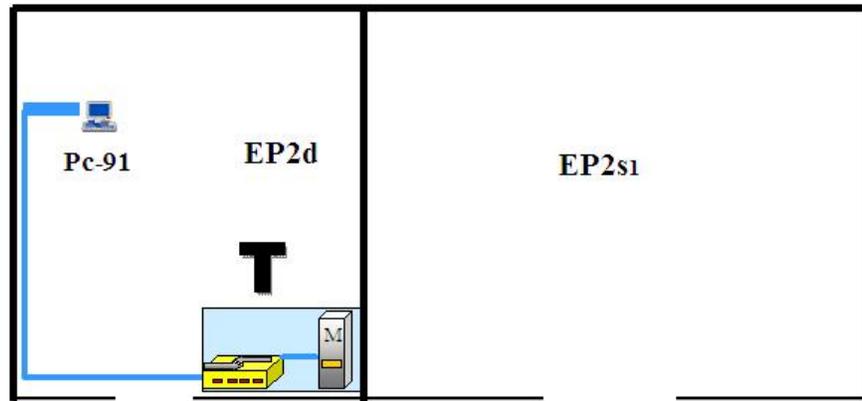


Figura III.16 Esquema del Edificio de Primaria 2. Nivel 1.

Se propone instalar un nodo para el salón EP2s1 y otro más para el EP2d para tener una salida a la red y el Internet, firmados a un dominio para que un servidor tenga control de acceso. (Ver figura III.16)

Nodos Instalados actualmente: 1

EP2 (nivel 2)

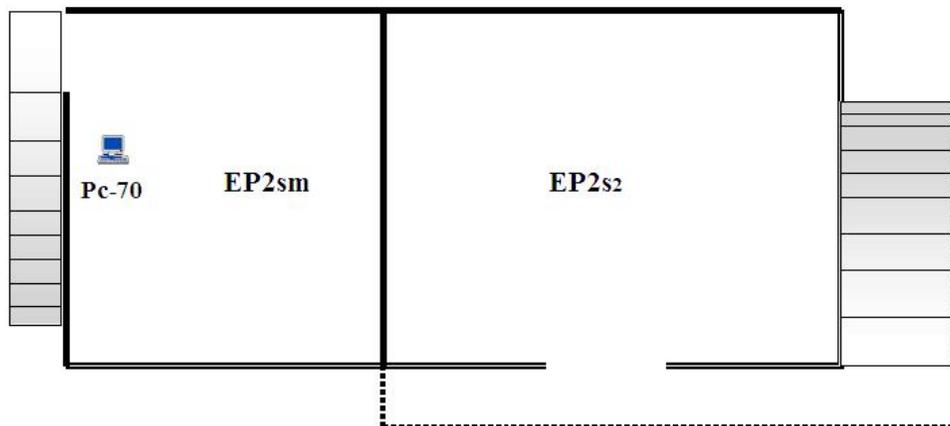


Figura III.17 Esquema del Edificio de Primaria 2. Nivel 2.

Aquí existe solo una pc sin conexión a red. (Ver figura III.17)

Nodos Instalados actualmente: 0

Edificio de Preescolar (EPR)

No. Pisos	No. Equipos		Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
3	1 nivel 1	18 nivel 2	Inalámbrica 11 Mbps.	En 1 Back Bone	1 Modem ADSL Wireless 2WIRE Home Portal 1800 HW de 4 puertos LAN 10/100 Ethernet
nivel 1 nivel 2 nivel 3	0 nivel 3		Cableado		
nivel 1 nivel 2 nivel 3	18 equipos conectados a una tarjeta inalámbrica. y 1 por UTP Nivel 5e. Total: 19		USB Robotics 802.11g Wireless 54 Mbs. Canaleta tendido de cable UTP Nivel 5e (a 350 MHz)		Una de las salidas funge como puerta de salida o “default gateway” que provee Prodigy Infinitum de Telmex (Teléfonos de México).

Tabla III.13 Descripción de la red en EPR

Actualmente en el edificio de preescolar se cuenta con salones de Preescolar, Primaria y con un laboratorio de cómputo (salón 50) Este último cuenta con una infraestructura, de una red inalámbrica en cuanto a medio de comunicación se refiere. (Ver tabla III.13).

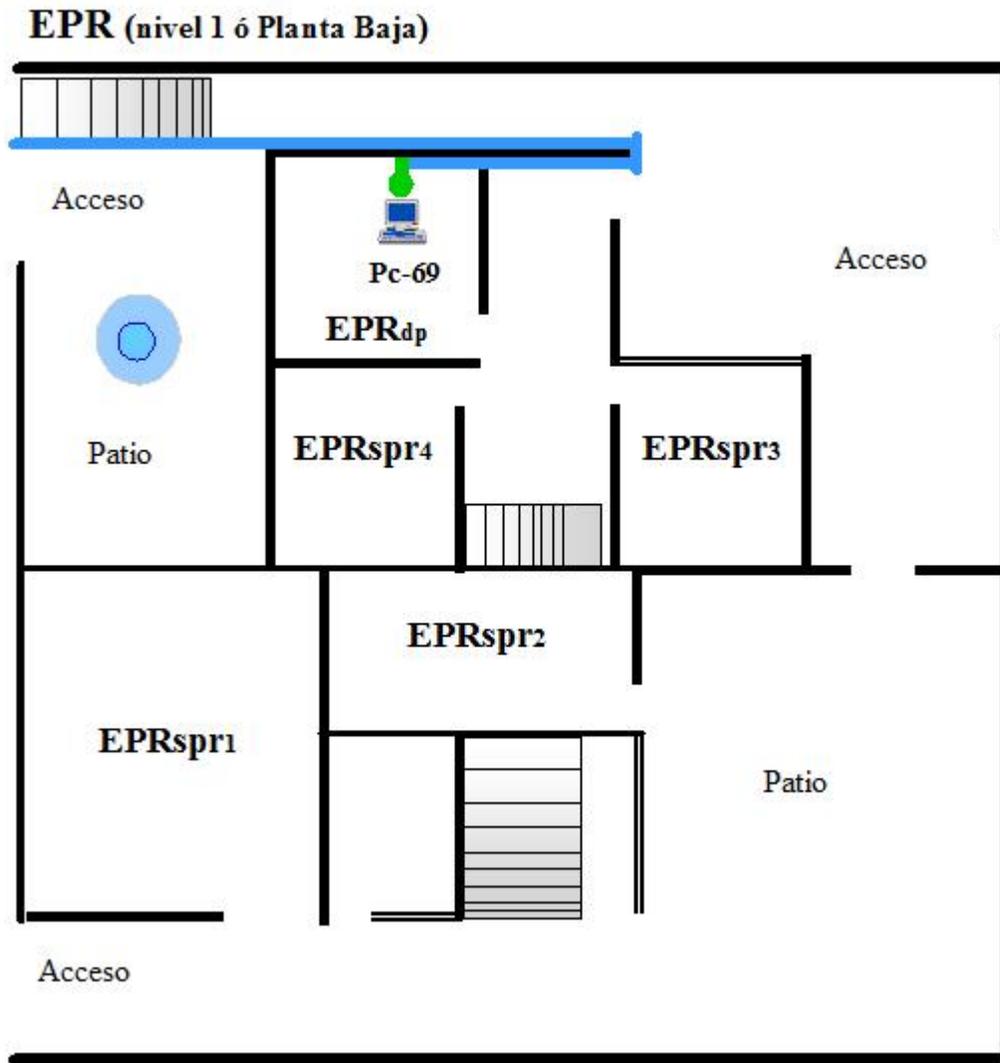


Figura III.18 Esquema del Edificio de Preescolar. Nivel 1.

Pero los salones de preescolar y primaria no cuentan con nodos para tener una conexión a la red por lo cual estamos proponiendo crear una red para que los profesores de primaria y preescolar cuenten con acceso a Internet en sus salones. En donde deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas en cuanto a su manejo.

(Ver figura III.18)

Nodos Instalados actualmente: 1

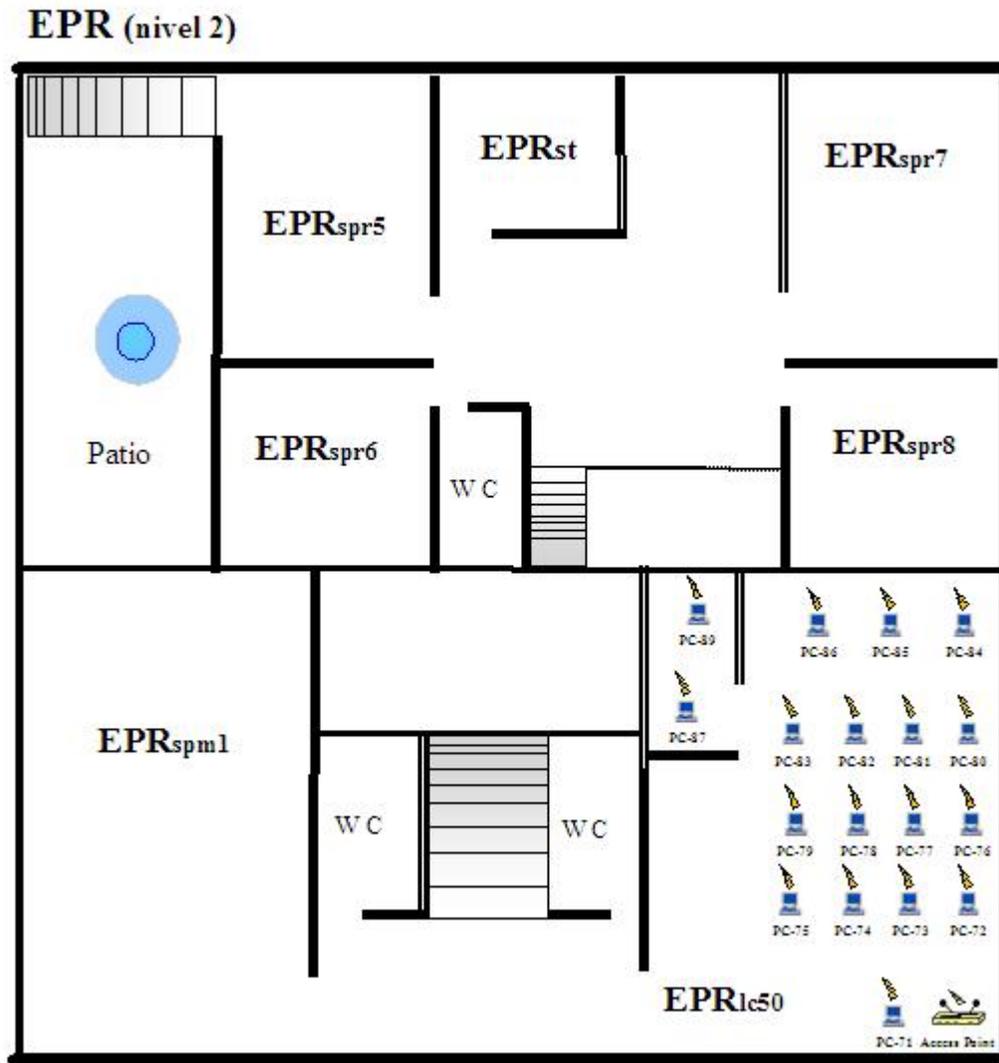


Figura III.19 Esquema del Edificio de Preescolar. Nivel 2.

En este nivel es donde contamos con la red del laboratorio 50, se propone instalar un servidor para el control de acceso a la red y el Internet, añadiendo más nodos para los salones de Preescolar (EPRspr). (Ver figura III.19)

Nodos Instalados actualmente: 18

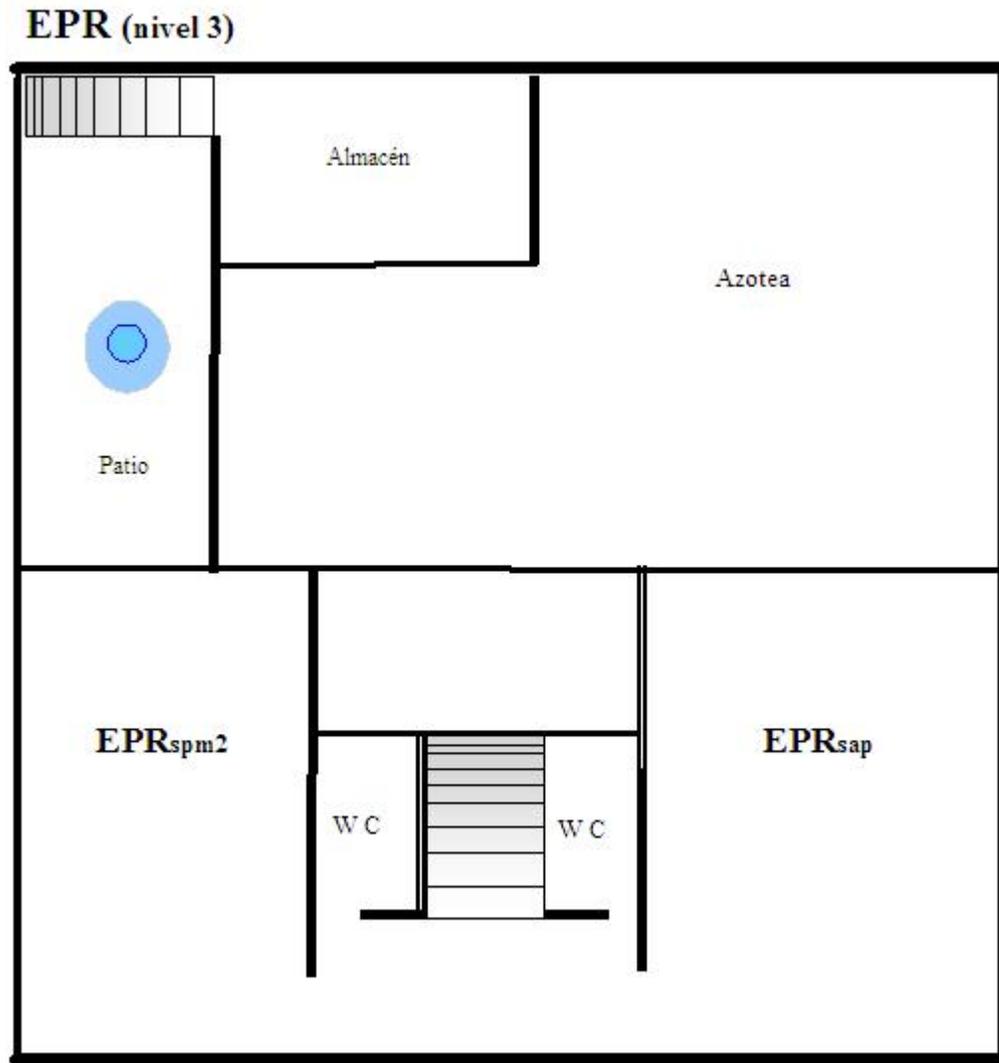


Figura III.20 Esquema del Edificio de Preescolar. Nivel 3.

Aquí no se cuenta con ningún acceso a la red. Solo se propone instalar nodos para los salones y que alumnos y profesores se apoyen en buen uso de la Internet por medio de un servidor por seguridad informática. (Ver figura III.20)

Nodos Instalados actualmente: 0

3.3 OBJETIVO

El establecimiento de las especificaciones para el diseño, construcción, instalación, administración y mantenimiento de una red de alto desempeño en las instalaciones definitivas del Colegio Asesoría Educativa Queen Mary School S.C. (QMS), que garantice la correcta operación de los servicios de telecomunicaciones con tecnología de vanguardia, estableciendo los siguientes aspectos:

- Diseño y especificación de una red inalámbrica estructurada genérica para servicios de datos, en el edificio administrativo del Colegio.
- Diseño y especificación de las canalizaciones para el soporte e instalación del cableado estructurado de telecomunicaciones, en las áreas ya mencionadas.
- Diseño y especificación de los espacios o áreas para la instalación de los equipos de telecomunicaciones, sistemas auxiliares y distribuidores de las redes de cableado estructurado.
- Propuesta de instalación de equipo de telecomunicaciones para la interconexión eficiente del cableado en las distintas áreas.
- Esquema de administración uniforme para las redes de cableado estructurado de telecomunicaciones.
- Especificación del direccionamiento lógico que deberán llevar cada una de las subredes que conforman la red general del Colegio buscando evitar grandes dominios de choque para la optimización de procesos.
- Especificación de la instalación de servidores necesarios y sus aplicaciones para solventar las necesidades primordiales del Colegio.

IV. DESARROLLO: PROPUESTA DE REESTRUCTURACIÓN Y OPTIMIZACIÓN DE LA RED

4.1 Cableado e implementación de la red inalámbrica para las diferentes áreas del Colegio

Siguiendo con el modelo de referencia ISO-OSI, la primera parte en la que nos enfocaremos será el nivel 1 en donde definiremos las características mecánicas y eléctricas del medio de comunicación. Cabe mencionar que haremos mención a dos tipos de medios de comunicación con el que contaremos para esta propuesta de optimización.

CABLEADO

Comenzaremos describiendo algunos elementos adicionales necesarios para el cableado estructurado de la red a realizar.

Se propone hacer un tendido nuevo de cable UTP Cat-6, cables para interconexión de computadores y concentradores (llamados patch cord) Ethernet con puertos RJ-45, que usan componentes, físicamente similares, sobre sistemas de cableado UTP, FTP, o S-FTP y, en la definición del estándar, soporta redes 100 Base-T (100 Mbps) o Gigabit Ethernet (1000 Mbps).

El estándar Gigabit Ethernet del IEEE 802.3ab está enfocado a suministrar 1000 Base T sobre sistemas de cableado de Categoría 5 mejorada.

Para que un sistema cumpla categoría 6 debe cumplir todas las especificaciones de canal. De acuerdo con la norma, el canal más exigente está formado por 90m de cableado horizontal de cable con conductores de cobre sólido en la tirada horizontal, más 10 m.

Esta Norma reconoce la importancia que tienen los servicios de voz y de datos en un edificio administrativo, campus o área Industrial.

- *Características:* Barra de carga interna que asegura el posicionamiento preciso de los pares y un alto rendimiento constante. Es perfecta en combinación con redes 100 Base-T y Gigabit Ethernet. La arquitectura del conector RJ-45 protege contra daños durante la instalación.
- *Canalización:* Para la distribución hacia el área de trabajo se propone el uso de ductos ahogados, que son sistemas de canalización para llevar cables de telecomunicaciones y eléctricos. El sistema consta de ductos de distribución y alimentación.
- *Cumplimiento de Estándares de Seguridad contra Incendios:* NOM-SEDE-001 y ASTM-E814.
- *Cumplimiento de estándares de Administración:* ANSI/TIA/EIA-606 Estándar ANSI/TIA /EIA 606 de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.

Empecemos a diseñar nuestro cableado siguiendo la normatividad vista con anterioridad en donde se detallan los subsistemas, teniendo en cuenta que:

La función de los subsistemas de cableado principal de campus y de edificio es proporcionar interconexiones entre los DCP's, DCE's y DCC's. (Distribuidores de cable por Piso, Edificio ó Campus).

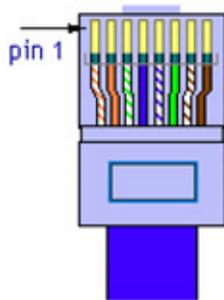
Por lo tanto necesitaremos

- Cables UTP en Cat-6
- RJ45-RJ-45 Conectores Cat6 RJ-45 Keystone.
- Páneles de parcheo (Patch panels) Cat-6 RJ-45 Keystone Standard.
- Placas de pared.
- Jacks.

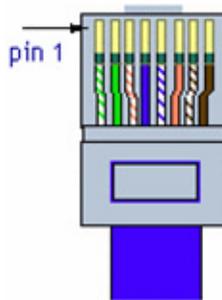
Asignaciones del conector modular RJ-45 de 8 hilos, que forma parte del cableado horizontal.

El conector RJ-45 de 8 hilos/posiciones es el más empleado para aplicaciones de redes (El término RJ viene de Registered Jack).

Los conectores de 8 posiciones están numerados del 1 a 8, de izquierda a derecha, cuando el conector es visto desde la parte posterior al gancho de ensamble (la parte plana de los contactos), tal como se muestra en las figuras (IV.1 y IV.2).



568B *Figura IV.1 Norma 568B*



568A *Figura IV.2 Norma 568A*

Como ya se ha visto, dos esquemas de asignación de terminales (pins) están definidos por la EIA/TIA, el 568A y el 568B. Ambos esquemas son casi idénticos, excepto que los pares 2 y 3, están invertidos.

Cualquier configuración puede ser usada para ISDN (Integrate Services Digital Network) y aplicaciones de alta velocidad. Las Categorías de cables transmisión 3, 4, 5, 5e y 6 son sólo aplicables a este tipo de grupos de pares.

Para aplicaciones de RED, (Ethernet 10/100baset, o Token Ring) solo son usados dos pares, los dos pares restantes se utilizarían para otro tipo de aplicaciones, voz, por ejemplo. (*Ver Figura IV.3*)

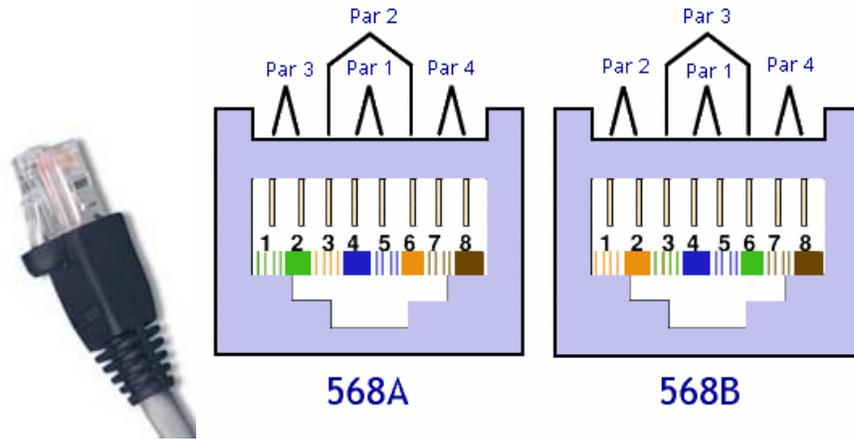


Figura IV.3 Asignación de Pares en las Normas 568A y 568B.

El área de trabajo

El primer objetivo del cableado horizontal es constituir el área de trabajo hacia el cuarto de telecomunicaciones, tal como lo muestra la figura siguiente tendremos un servicio de dato por nodo. (Ver figura IV.4)

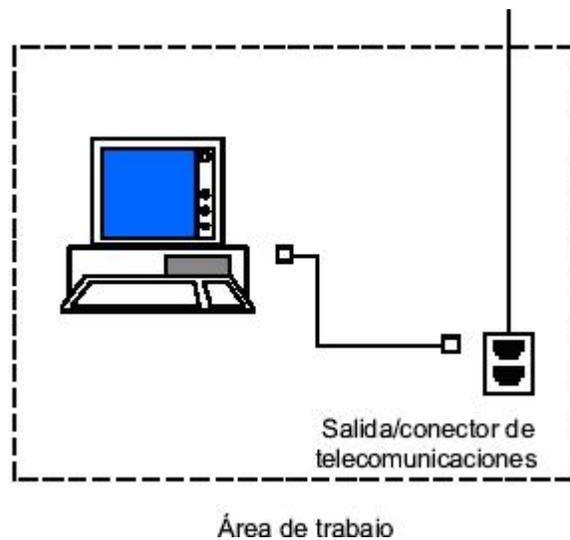


Figura IV.4

Se debe proporcionar un mínimo de dos salidas/conectores de telecomunicaciones, por cada área de trabajo individual, (pueden estar integradas en una misma toma de telecomunicaciones).

Una salida/conector de telecomunicaciones puede estar asociada a datos. Debe considerarse la instalación de salidas/conectores adicionales basándose en las necesidades actuales y proyectadas.

Las salidas/conectores de telecomunicaciones deben ser configuradas de la siguiente manera:

Conector para servicio de datos. El conector para servicio de datos debe ser RJ-45 hembra, compatible con el cable de cobre de 4 pares trenzados de 100 Ω ., categoría 6, según con la categoría que corresponda.

Inalámbrico

A continuación, describimos varios puntos que debemos tener en cuenta para nuestra reestructuración de las redes wireless con que se cuenta en el Colegio Queen Mary School.

- Instalación de los Puntos de Acceso y pruebas de cobertura. Interconexión, si procede, con la red de cable ya existente o con la conexión a inalámbrica del cliente.
- Configuración de las medidas de seguridad necesarias (protocolo WPA, entre otras) para garantizar la privacidad de las transmisiones por la red inalámbrica.
- Instalación (opcional) de los adaptadores inalámbricos en los equipos clientes.
- La distancia que las ondas electromagnéticas pueden alcanzar dependen de dos factores: el diseño de los dispositivos y el medio en el que se transmiten.

Éste último puede ser muy variado, y modificarse a lo largo del tiempo, por lo que presenta mayores problemas a la hora de la instalación de una red Wireless.

“Las ondas empleadas en las redes Wireless 802.11, ondas electromagnéticas mayores de 1 GHz, pueden atravesar los materiales, pero la atenuación que presenta depende del material de que esté fabricado el obstáculo, de la forma del mismo, etc.

En el caso particular de la banda ISM de los 2.4 GHz, el agua presenta un poder de absorción muy alto a esa frecuencia, por lo que los materiales con un mayor porcentaje de agua (por ejemplo, las personas) afectan muy negativamente a la propagación de las ondas electromagnéticas.

El radio de cobertura de un dispositivo Wireless puede ir desde unos pocos metros, hasta alcanzar un promedio de 100 metros de radio a la redonda, dependiendo del entorno y el equipamiento empleado (potencia, tipos de antenas, etc).⁸

Diseño básico

A continuación trataremos de explicar de la forma más sencilla posible la arquitectura Wireless. Está conformada por nodos de acceso, por este motivo empezaremos con un pequeño gráfico ilustrativo de lo que sería un nodo de acceso y que elementos lo forman:
(Ver figura IV.5)



Figura IV.5 Esquema básico de un nodo.

⁸ HALLBERG Bruce. Fundamentos de Redes. 4a ed. México: McGraw-Hill, 2006. 512 p.

Como podemos observar un nodo lo forman básicamente una antena, un cable y un punto de acceso. La antena puede ser casera (construida manualmente) o comprada.

Cada nodo es mantenido y administrado por su creador y es éste en última instancia quien determina el tipo de servicio que quiere proveer.

Antes de empezar a proponer la implementación de la red de cómputo es necesario hacer mención de los siguientes conceptos, para así localizarlos físicamente y empezar a diseñar el sistema de conectividad que será el siguiente paso a seguir para la interconectividad de las áreas.

Cuarto Principal de Telecomunicaciones

En este cuarto, se ubicarán, los paneles de parcheo, que estarán acoplados a los equipos de conectividad. En este también se ubicarán los servidores.

Instalación de entrada o acometida

Son las áreas dentro del cuarto de telecomunicaciones principal, y a esta área llega la red de distribución que provee Prodigy de Telmex que funge como puerta de salida o “default gateway”. Hacia el Internet.

Después de la especificación de la estructura fundamental de los sistemas de cableado estructurado, la ubicación en detalle de los nodos en cada uno de los pisos y departamentos de los edificios es como se indica a continuación y de acuerdo con la siguiente nomenclatura:

(Ver tabla IV.1)

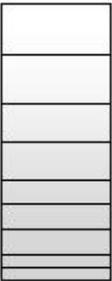
 Canaleta Profesional T70 con Cable UTP Categoría 6.	 Switch Layer 2
 Nodo con servicios de Datos	 Impresora conectada a la red
 Estación de trabajo Fija conectada a la red	 Maps
 Estación de trabajo Aleatoria conectada a la red inalámbrica.	 Router ADSL
 Estación de trabajo Fija conectada a la red alámbrica.	 Router
 Impresora conectada a pc.	 Cuarto de Telecomunicaciones
 Servidor Admón.	 Back Bone
 Servidor de impresión	 Escaleras
 Punto de Acceso inalámbrico.	
 Switch Administrable Layer 3	 Internet Internet

Tabla IV.1 Nomenclatura.

Como lo hemos detallado en el CAPÍTULO tres “Definición del Problema”. El Colegio Asesoría Educativa Queen Mary School S.C. (QMS) es una construcción que consta de siete edificios distribuidos en una misma área (*Ver figura III.1*).

Para hacer referencia a cada uno de estos edificios con sus departamentos ó áreas se utilizarán en adelante los mismos acrónimos que hemos venido utilizando en el capítulo tres. (*Ver Tabla III.1- Tabla III.7*)

EDIFICIO ADMINISTRATIVO (EAD)

Infraestructura que se propone instalar en el edificio administrativo. (*Ver tabla IV.2*)

No. Pisos	No. Equipos			Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
3	17 nivel 1	19 nivel 2	12 nivel 3	Inalámbrica 11 Mbps.	En 1 Cuarto de telecomunicaciones	1 3com office connect router/modem adsl (A) wireless 108 mbps 11g firewall.
Nivel 1, nivel 2 y nivel 3	44 equipos conectados a una tarjeta inalámbrica. y 4 por UTP Nivel 6. Total: 48 equipos.			Wireless-B 802.11g Linksys.	1 3com wireless Lan managed access point 2750. 1 3com switch 3 (a) 4500 26-port (capa 3). 1 3com office connect wireless 11a/b/g access point. 1 Server Administración.	Puerta de salida o “default gateway” al que provee Prodigy Infinitum de Telmex. Proporciona el servicio de Internet de Banda ancha que permite conexión permanente a Internet a una velocidad de 1 Mbps.

Tabla IV.2 Descripción de la red en EAD.

Dar servicio Wireless Lan Privado seguro con cobertura total a cada una de las estaciones de trabajo: Planta principal de recepción. (Ver figura IV.6)

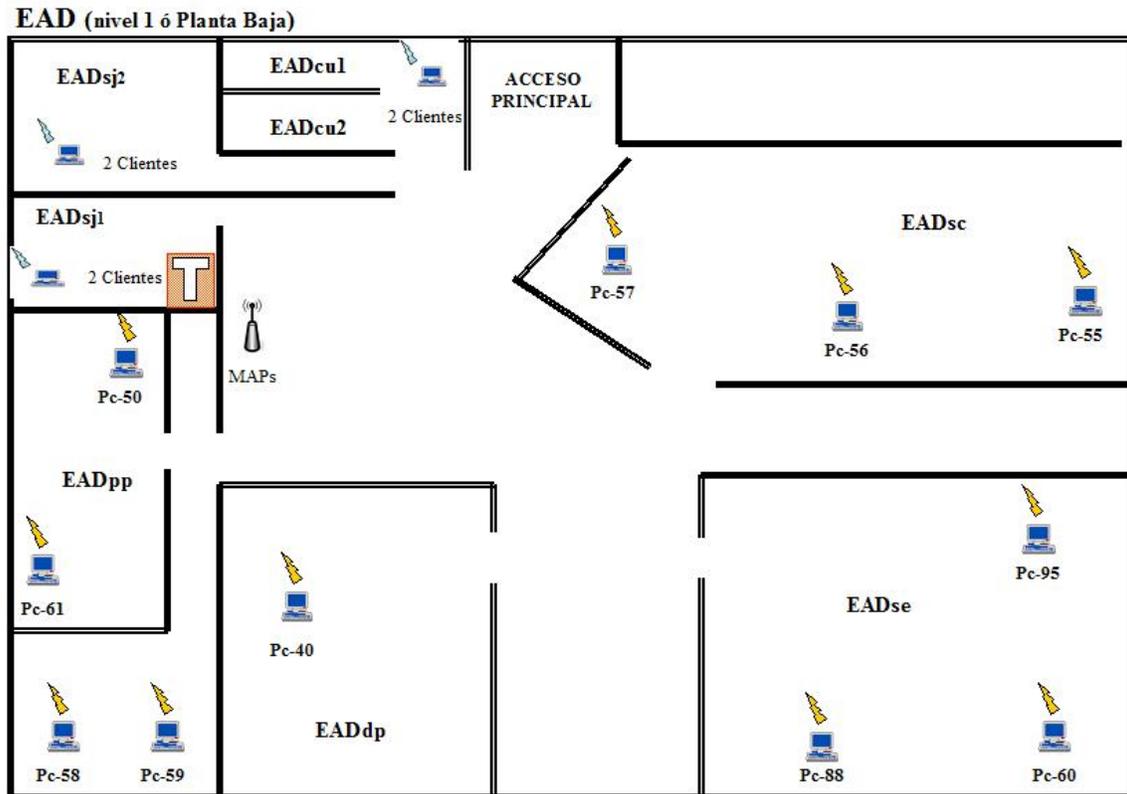


Figura IV.6 Esquema del Edificio Admón. Nivel 1 ó Planta Baja.

Concurrencia máxima prevista de usuarios conectados: 11

Dar servicio Wireless Lan Público seguro con cobertura total a la planta principal donde se ubica la recepción.

Concurrencia máxima prevista de usuarios conectados: 6

Total de Equipos Clientes: 17

En este caso los canales utilizados son el 1 y el 11. Ello nos permite doblar el ancho de banda disponible hasta 22 Mbps así como balancear usuarios entre ambos canales de forma dinámica en función de la calidad del enlace radio que el usuario perciba mejor. Con el fin de evitar interferencias entre ambas tarjetas radio, haremos conectar una antena exterior. Así mismo gracias a la ganancia adicional de dicha antena hemos aumentado la potencia de señal transmitida para dar el servicio externo al público.

La ubicación de dicha antena exterior habrá de ser en la planta de recepción a una altura de un par de metros a fin de que el tránsito de personas no afecte su rendimiento. En este caso a pesar de que el área de cobertura de ambos perfiles se solapa no hay interferencias entre canales.

En dicho edificio noble por su constitución y estructura (estancias bastante abiertas) el área de cobertura de un punto del acceso Modem/Ruteador que da servicio de Internet a todo el edificio tipo Linksys ubicado en este nivel 2 cubre perfectamente la planta superior e inferior con un nivel de señal superior al umbral establecido. (Ver figura IV.7)

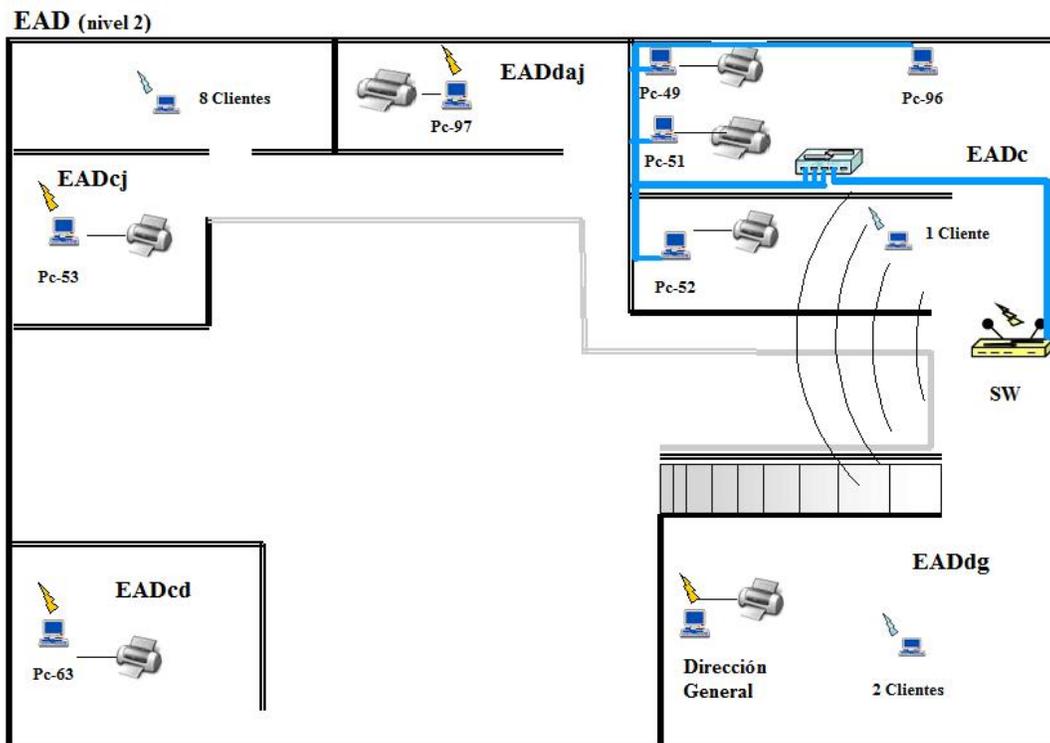


Figura IV.7 Esquema del Edificio Admón. Nivel 2.

Respecto al EADc (Contabilidad), estos puntos de acceso dan acceso a una red alámbrica diferente y aislada de la inalámbrica, con direccionamiento diferente y servicios diferentes.

Equipos Clientes Fijos: 4

Equipos Clientes Aleatorios: 11

Nodos por cableado par trenzado: 4

Total de Equipos en Servicio: 19

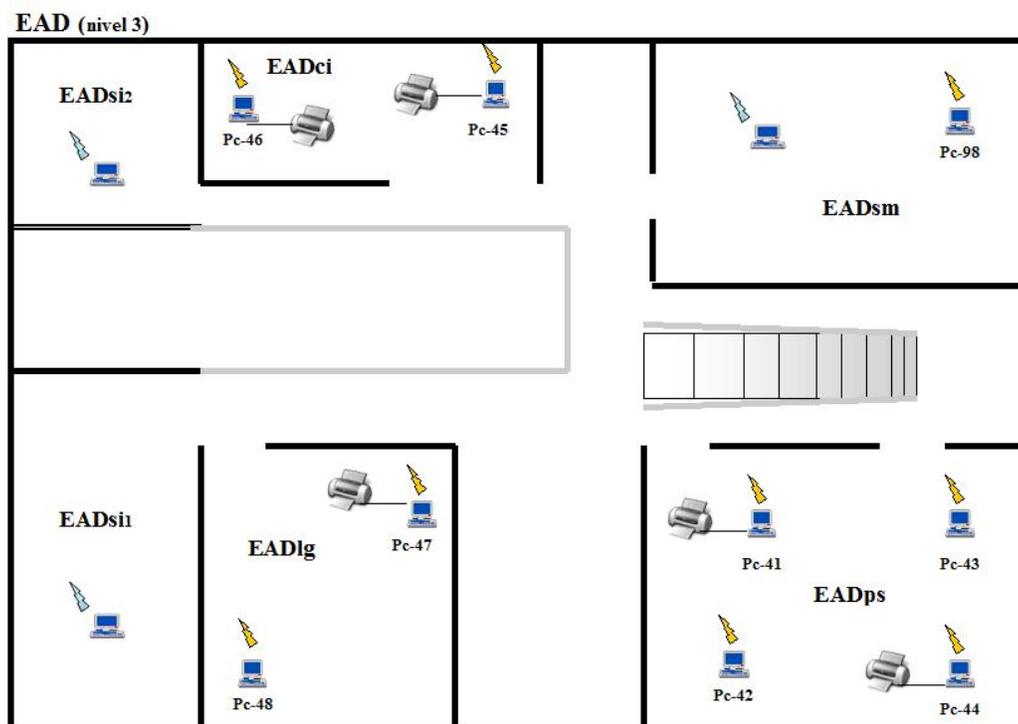


Figura IV.8 Esquema del Edificio Admón. Nivel 3

En las áreas EADsi y EADsm habrá acceso inalámbrico de Internet para poder tener el servicio de Internet. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.8)

Equipos Clientes Fijos Instalados: 9

Equipos Clientes Aleatorios: 3

Total de Equipos Clientes: 12

Edificio de Secundaria (ESE)

Infraestructura que se propone instalar en el edificio de Secundaria. (Ver tabla IV.3)

No. Pisos	No. Equipos			Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
3	11 nivel 1	4 nivel 2	4 nivel 3	Inalámbrica 11 Mbps. Cableado	En 1 Back Bone.	1 3com wireless Lan managed access point 2750. 1 3com switch (b) 3 4500 26-port (capa 3).
Nivel 1, nivel 2 y nivel 3	8 equipos conectados a una tarjeta inalámbrica. y 11 por UTP Nivel 6. Total: 19 equipos.			Wireless-B 802.11g Linksys. Canaleta Profesional Modelo T70 Y LD-10	.	Conexión con Router (A) and (B).

Tabla IV.3 Descripción de la red en ESE.

ESE (nivel 1 ó Planta Baja)

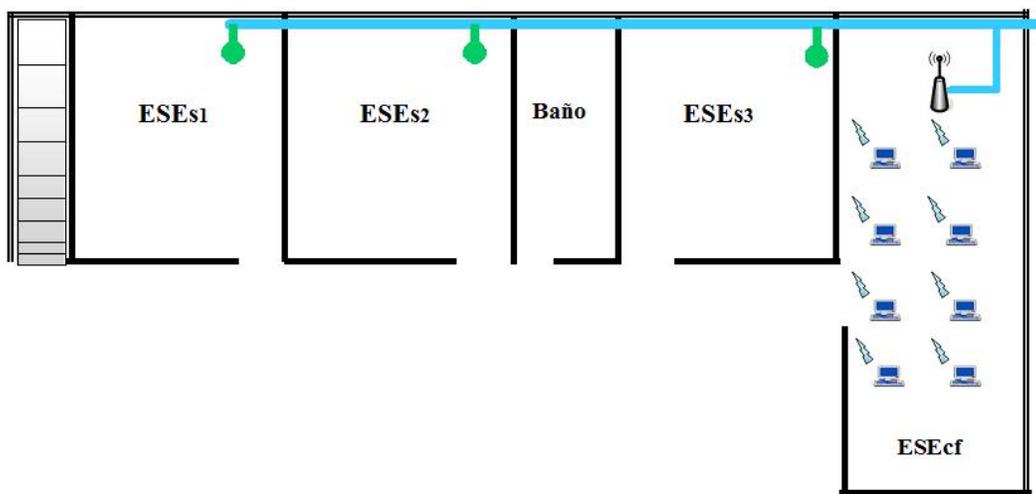


Figura IV.9 Esquema del Edificio de Secundaria. Nivel 1 ó Planta Baja.

En el área ESEcf habrá acceso inalámbrico de Internet para poder contar con este servicio, en las demás áreas será el acceso por cableado. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.9)

Nodos por cableado par trenzado: 3

Equipos Clientes Aleatorios: 8

Total de Equipos en Servicio: 11

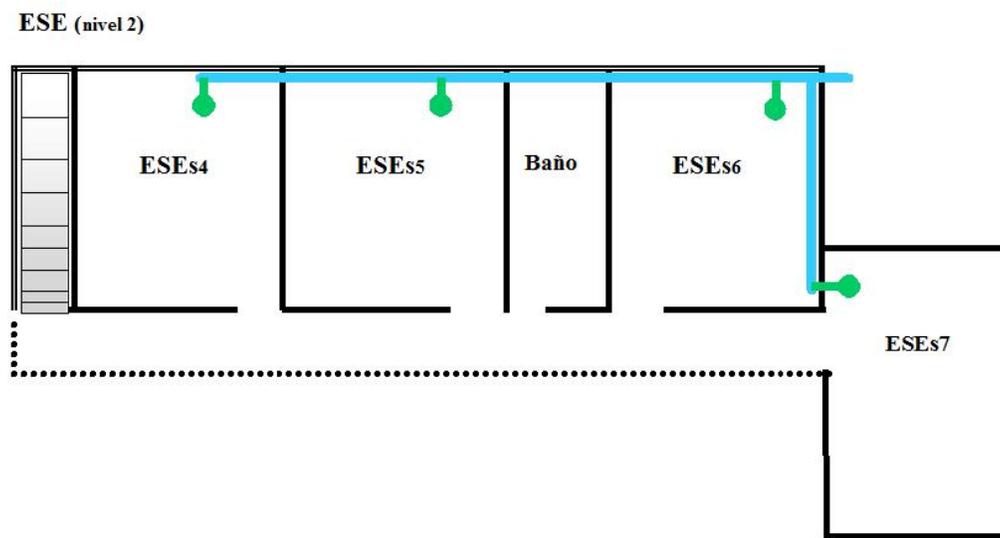


Figura IV.10 Esquema del Edificio de Secundaria, Nivel 2.

Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.10)

Nodos por cableado par trenzado: 4

Equipos Clientes Aleatorios: 0

Total de Equipos en Servicio: 4

ESE (nivel 3)

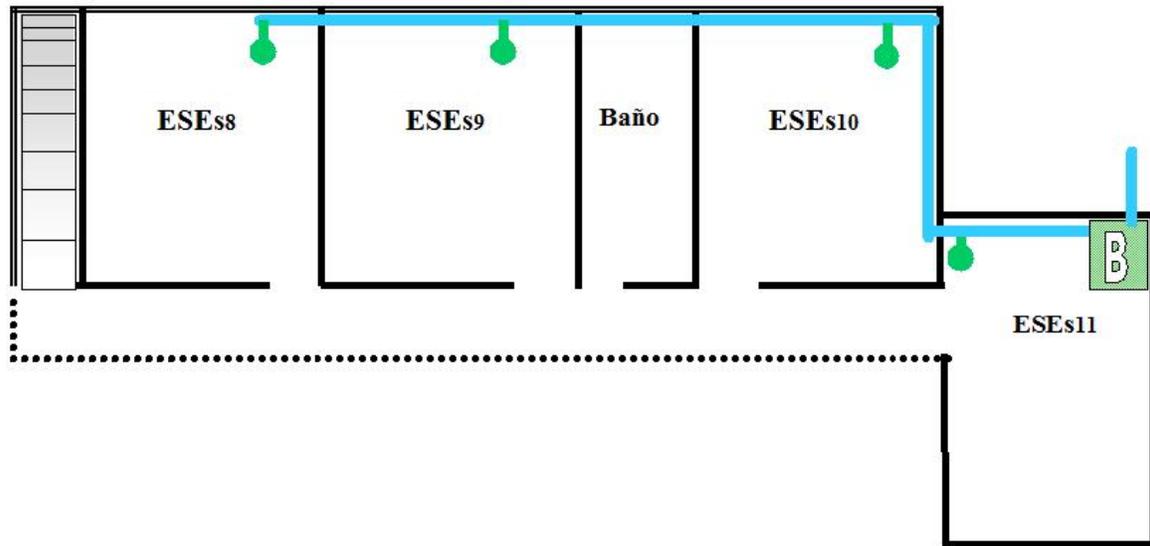


Figura IV.11 Esquema del Edificio de Secundaria. Nivel 3

Al igual que en el nivel 2 estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.11)

Nodos por cableado par trenzado: 4

Equipos Clientes Aleatorios: 0

Total de Equipos en Servicio: 4

Edificio de Preparatoria (EPP)

Infraestructura que se propone instalar en el edificio de Preparatoria. (Ver tabla IV.4)

No. Pisos	No. Equipos			Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
4	11 nivel 1	3 nivel 2	3 nivel 3	Inalámbrica 11 Mbps.	En 1 Back Bone.	1 3com wireless Lan managed access point 2750. 1 3com switch (e) 3 4500 26-port (capa 3).
	2 nivel 4			Cableado		
nivel 1 nivel 2 nivel 3 nivel 4	9 equipos conectados a una tarjeta inalámbrica. y 10 por UTP Nivel 6. Total: 19			Wireless-B 802.11g Linksys. Canaleta Profesional Modelo T70 Y LD-10		Conexión con Router (A) and (C).

Tabla IV.4 Descripción de la red en EPP.

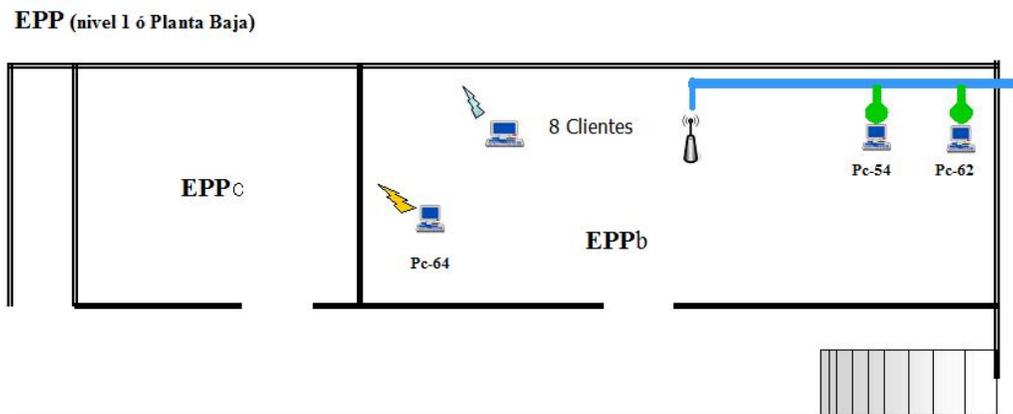


Figura IV.12. Esquema del Edificio de Preparatoria. Nivel 1

En el área EPPb habrá acceso inalámbrico de Internet para poder contar con este servicio, solo en dos computadoras será el acceso por cableado. (Ver figura IV.12)

Nodos por cableado par trenzado: 2

Equipos Clientes Aleatorios: 1

Equipos Clientes Aleatorios: 8

Total de Equipos en Servicio: 11

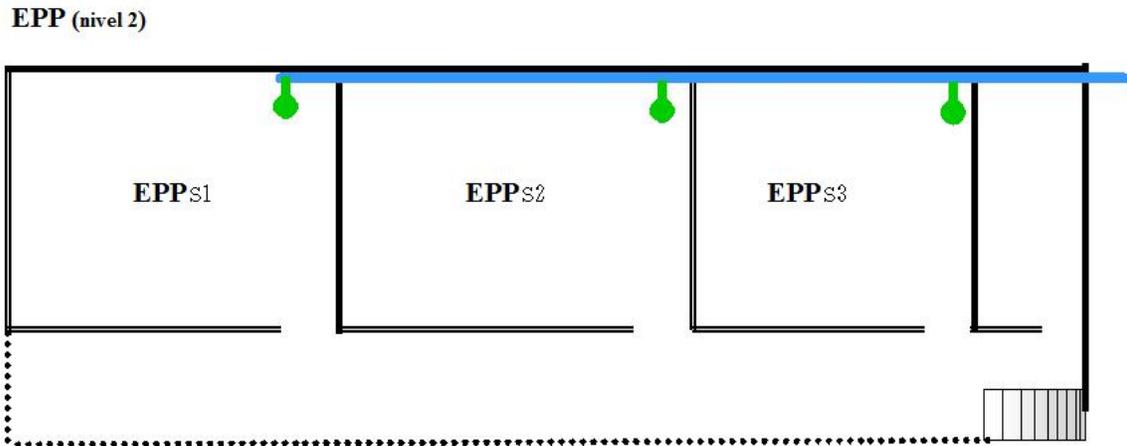


Figura IV.13 Esquema del Edificio de Preparatoria. Nivel 2

Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.13)

Nodos por cableado par trenzado: 3

Equipos Clientes Aleatorios: 0

Total de Equipos en Servicio: 3

EPP (nivel 3)

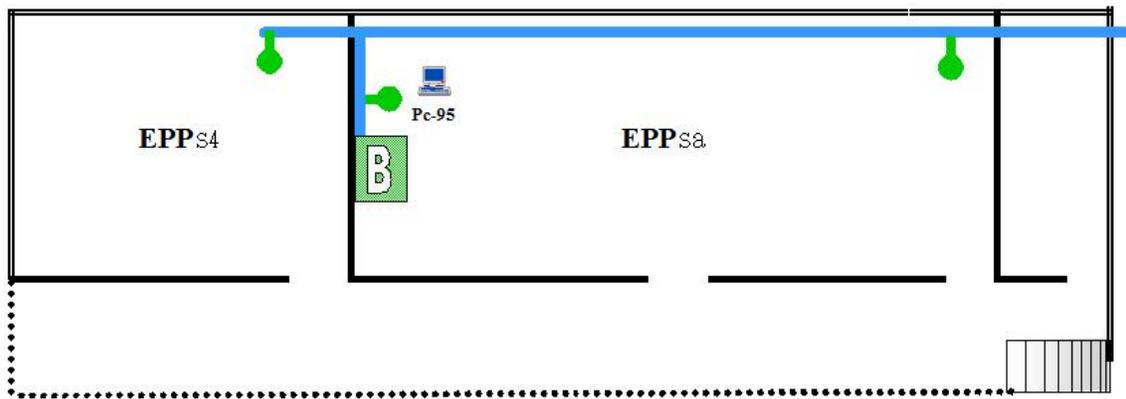


Figura IV.14 Esquema del Edificio de Preparatoria. Nivel 3

En el área EPPsa estará el backbone para dar acceso de Internet al EPP. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.14)

Nodos por cableado par trenzado: 3

Equipos Clientes Aleatorios: 0

Total de Equipos en Servicio: 3

EPP (nivel 4)

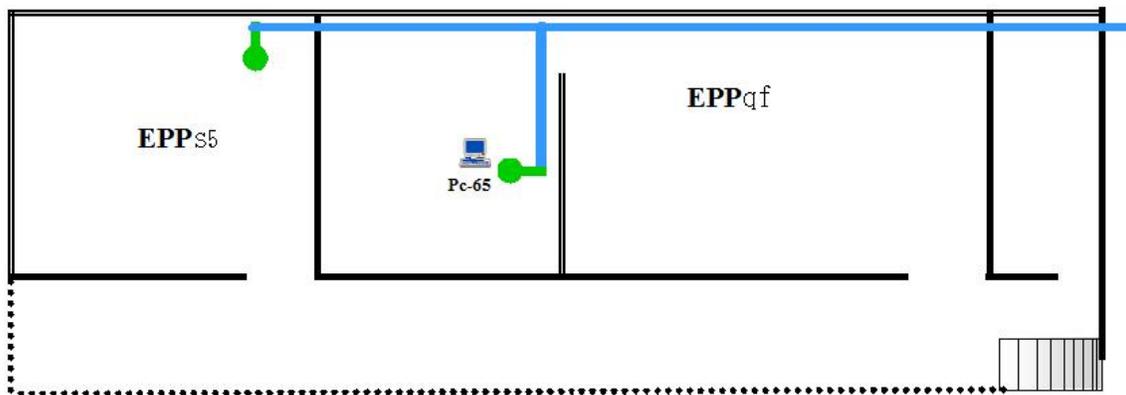


Figura IV.15 Esquema del Edificio de Preparatoria. Nivel 4

Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.15)

Nodos por cableado par trenzado: 2

Equipos Clientes Aleatorios: 0

Total de Equipos en Servicio: 2

Edificio de Laboratorio de Cómputo (ELC)

Infraestructura que se propone instalar en ELC. *(Ver tabla IV.5)*

No. Pisos	No. Equipos		Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
2	4 Profesores	34 Alumnos	Cableado.	1 Cuarto de Telecomunicaciones.	1 Switch 3Com 3 (d) S Administrable capa 3 10/100 26 puertos. 1 Switch 3 Com 2 (c) Baseline Switch 2824 10/100/1000 Ethernet de 24 puertos. 1 Server Web.
	1 ELCum				
Salón 35 y 36.	Total 39 equipos conectados a un nodo o Jack.		alámbrica con un tendido de cable UTP Nivel 6 (a 1000 MHz) Canaleta Profesional Modelo T70 Y LD-10	1 Panel de parcheo 1 rack de 7" Dispositivos de conectividad.Ethernet de 24 puertos.	3com OfficeConnect secure router (C).
				1 Ruteador USB Robotics 8000 capa 1 de 4 puertos LAN 10/100 Ethernet.	Conexión con router (A) and router (B).

Tabla IV.5 Descripción de la red en ELC

ELC (nivel 1 o Planta baja)

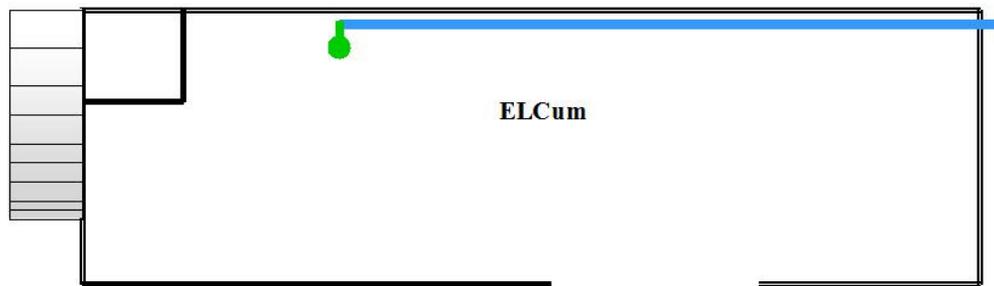


Figura IV.16 Esquema del Edificio de ELC Salón de usos múltiples. Nivel 1

Instalar un nodo en el área de ELCum este equipo deberá firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.16)

Nodos por cableado par trenzado: 1

Equipos Clientes Aleatorios: 0

Total de Equipos en Servicio: 1

ELC (nivel 2)

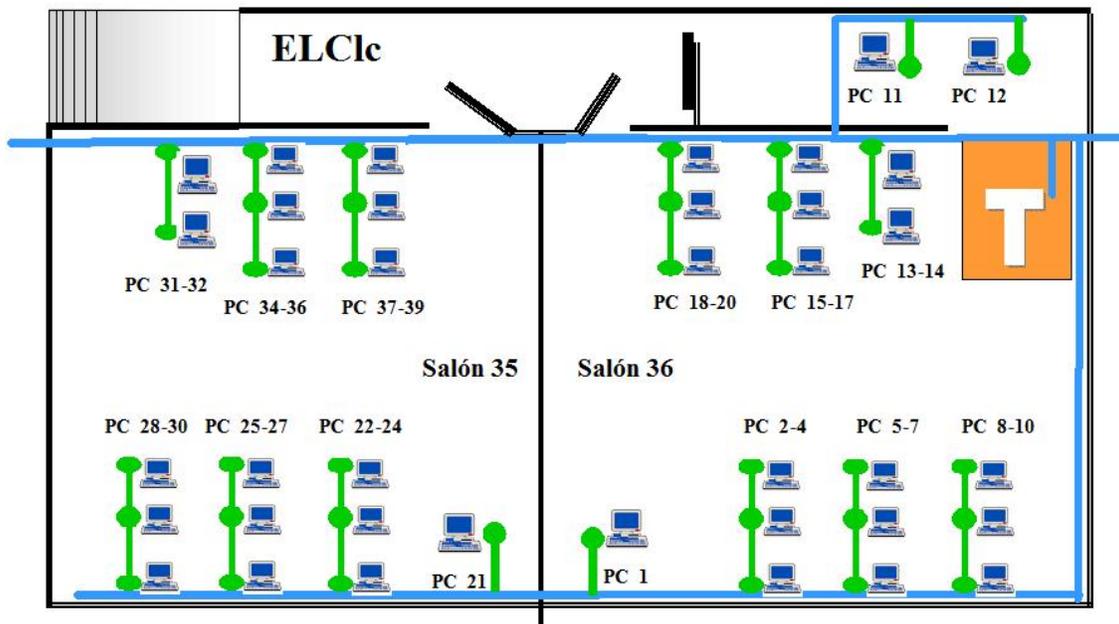


Figura IV.17 Esquema del Edificio de Lab. de Cómputo salones 35 y 36. Nivel 2

Con estos conceptos detallados obtendríamos nuestro cableado horizontal en el salón 35 y 36. En cada nodo se instalan las rosetas (terminaciones de los cables) que sean necesarias en cada área. De estas rosetas parten los cables que se tienden por canaletas profesionales Modelo T70 Y LD-10 que serán colocadas sustituyendo a la canalización actualmente existente (tubería de PVC) para concentrar cables hacia el panel de parcheo. Todos los cables se concentran en el armario (rack) dentro del cuarto de telecomunicaciones.

En algunos casos, según el diseño que requiera la red, puede tratarse de un elemento activo o pasivo de comunicaciones, es decir, un panel de parcheo. En cualquier caso, este panel de parcheo concentra todos los cables procedentes de una misma planta. *(Ver figura IV.17)*

Edificio Primaria 1. (EP1)

Infraestructura que se propone instalar en EP1. *(Ver tabla IV.6)*

No. Pisos	No. Equipos		Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
2	7 nivel 1	4 Nivel 2	Cableado.	En 1 Back Bone.	Conexión Switch 3com superstacks 3 switch (a) 3870. (capa 2).
nivel 1 y nivel 2	11 equipos conectados por UTP Nivel 6. Total: 11		tendido de cable UTP Nivel 6 (a 1 GHz) Canaleta Profesional Modelo T70 Y LD-10	1 3com superstack 3 switch (b) 3870, 12 puertos (capa 2).	

Tabla IV.6 Descripción de la red en EPI

Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. *(Ver figuras IV.18 y IV.19)*

EP1 (nivel 1 ó Planta Baja)

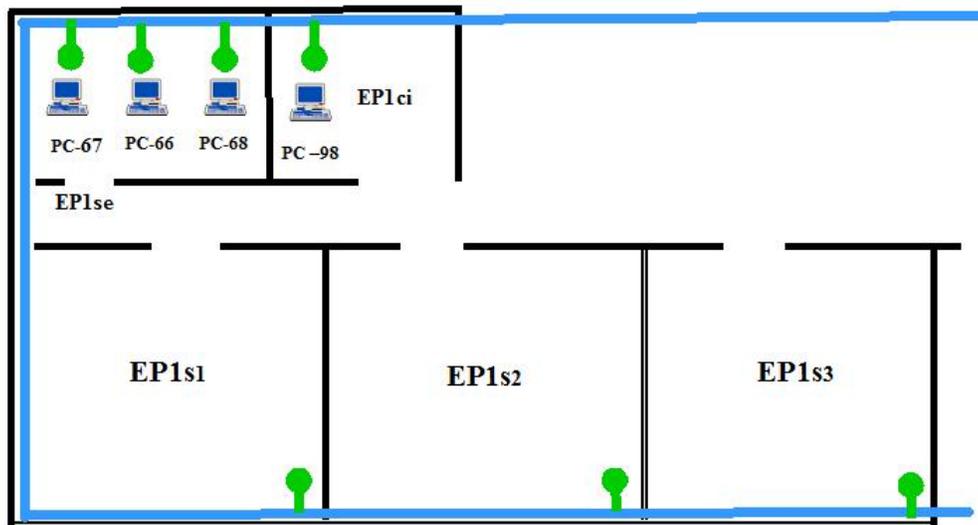


Figura IV.18 Esquema del Edificio de Primaria 1. Nivel 1

Nodos por cableado par trenzado: 7

Total de Equipos en Servicio: 7

EP1 (nivel 2)

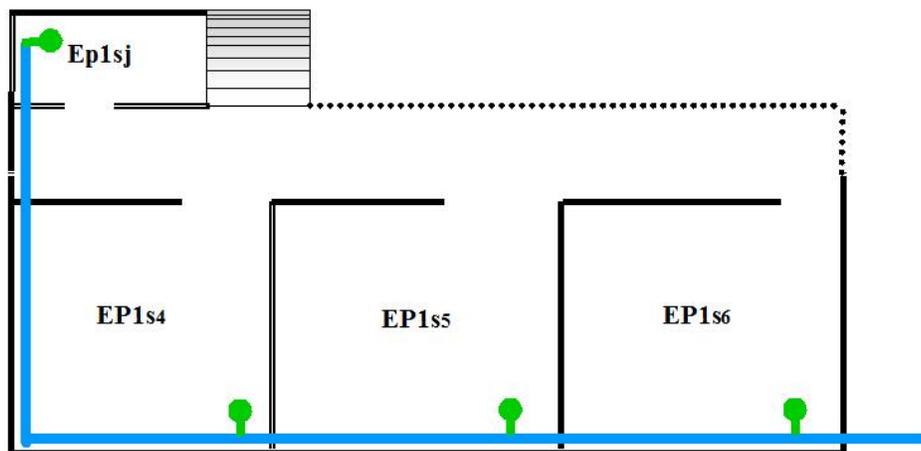


Figura IV.19 Esquema del Edificio de Primaria 1. Nivel 2

Nodos por cableado par trenzado: 4

Total de Equipos en Servicio: 4

Edificio de primaria 2. (EP2)

Infraestructura que se propone instalar en EP2. (Ver tabla IV.7)

No. Pisos	No. Equipos		Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
2	4 nivel 1	2 Nivel 2	Cableado.	En 1 Back Bone.	1 3com superstack 3 switch (a) 3870, 12 puertos (capa 2).
nivel 1 y nivel 2	6 equipos conectados por UTP Nivel 6. Total: 6		Canaleta Profesional Modelo T70 Y LD-10		Conexión con Router (B) and (C).

Tabla IV.7 Descripción de la red en EP2

EP2 (nivel 1 ó Planta Baja)



Figura IV.20 Esquema del Edificio de Primaria 2. Nivel 1

En el área EP2d estará el backbone para dar acceso de Internet al EP2. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.20)

Nodos por cableado par trenzado: 4

Total de Equipos en Servicio: 4

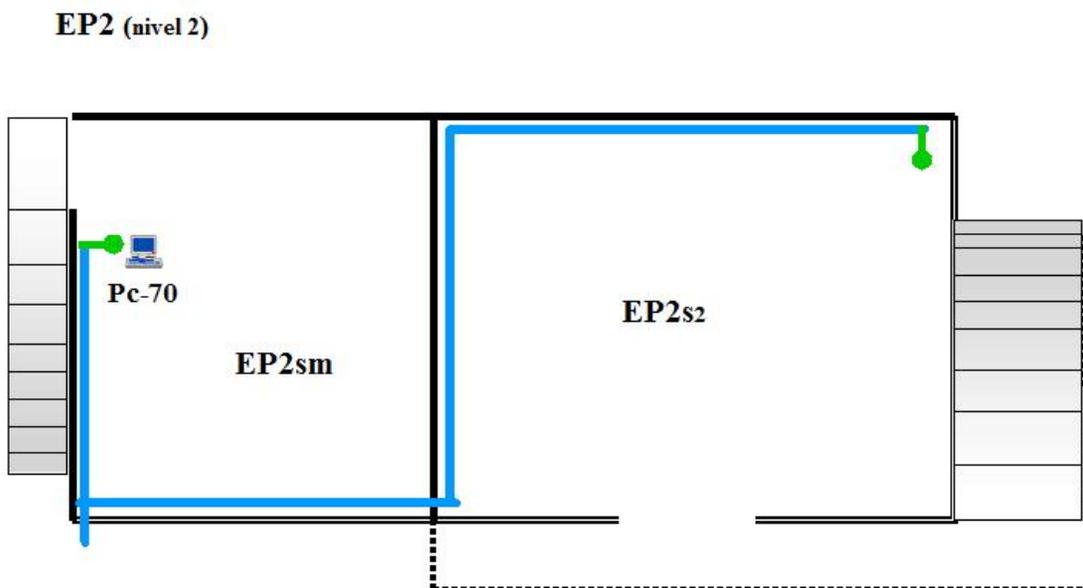


Figura IV.21 Esquema del Edificio de Primaria 2. Nivel 2

Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.21)

Total de Equipos en Servicio: 2

Edificio de Preescolar. (EPR)

Infraestructura que se propone instalar en EPR. *(Ver tabla IV.8)*

No. Pisos	No. Equipos		Medio de comunicación.	Concentración de equipos Activos.	Dispositivos activos de conectividad.
3	1 nivel 1	19 nivel 2	Inalámbrica 11 Mbps.	En 1 Cuarto de telecomunicaciones.	3com OfficeConnect secure router (B).
	1 nivel 3		Cableado		
nivel 1 nivel 2 nivel 3	19 equipos conectados a una tarjeta inalámbrica. y 2 por UTP Nivel 6. Total: 21		USB Robotics 802.11g Wireless 54 Mbs. Canaleta Profesional Modelo T70 Y LD-10	1 3com switch 3 (c) 4500 26-port (capa 3). 1 3com office connect wireless 11a/b/g access point. 1 Server Mail.	Conexión con router (A) and (C).

Tabla IV.8 Descripción de la red en EPR

Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. *(Ver figura IV.22)*

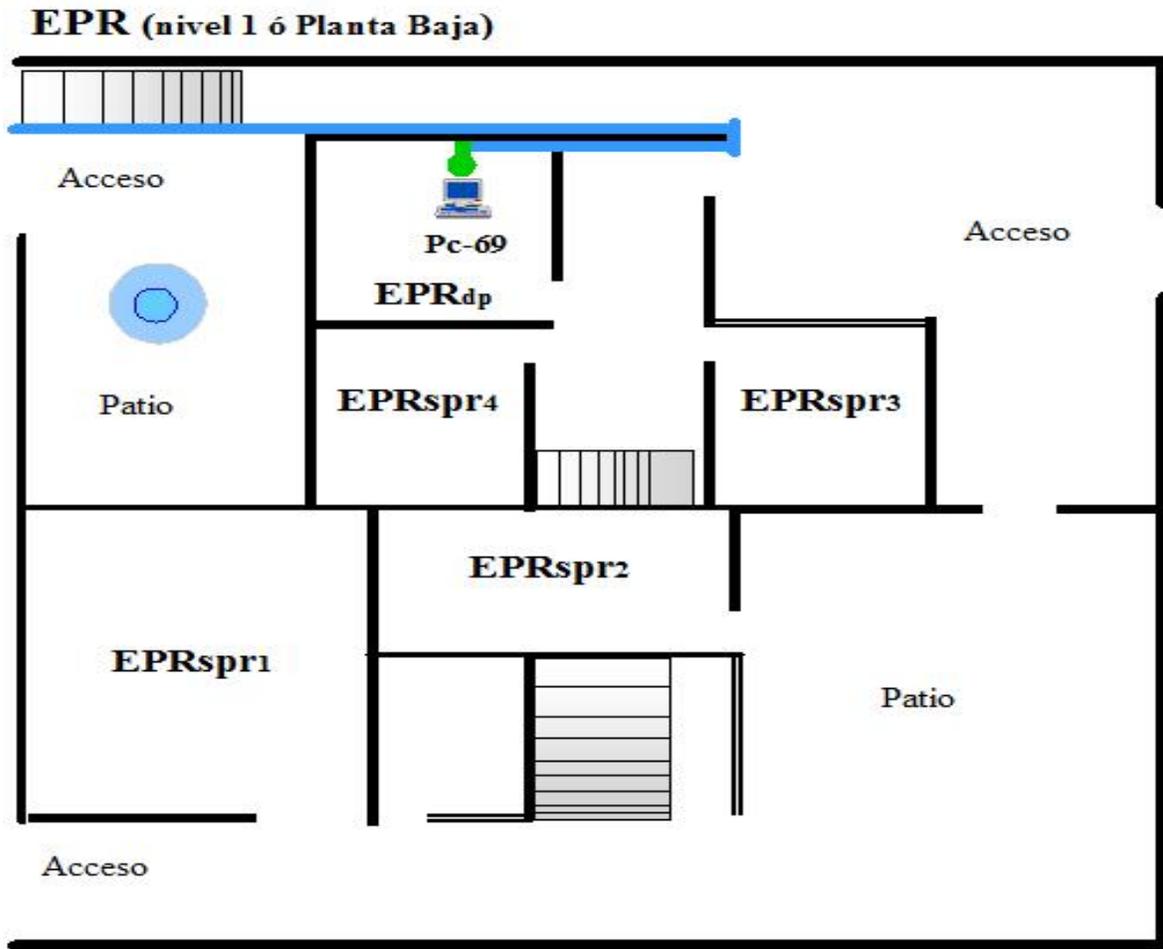


Figura IV.22 Esquema del Edificio de Preescolar. Nivel 1

Nodos por cableado par trenzado: 1

Total de Equipos en Servicio: 1

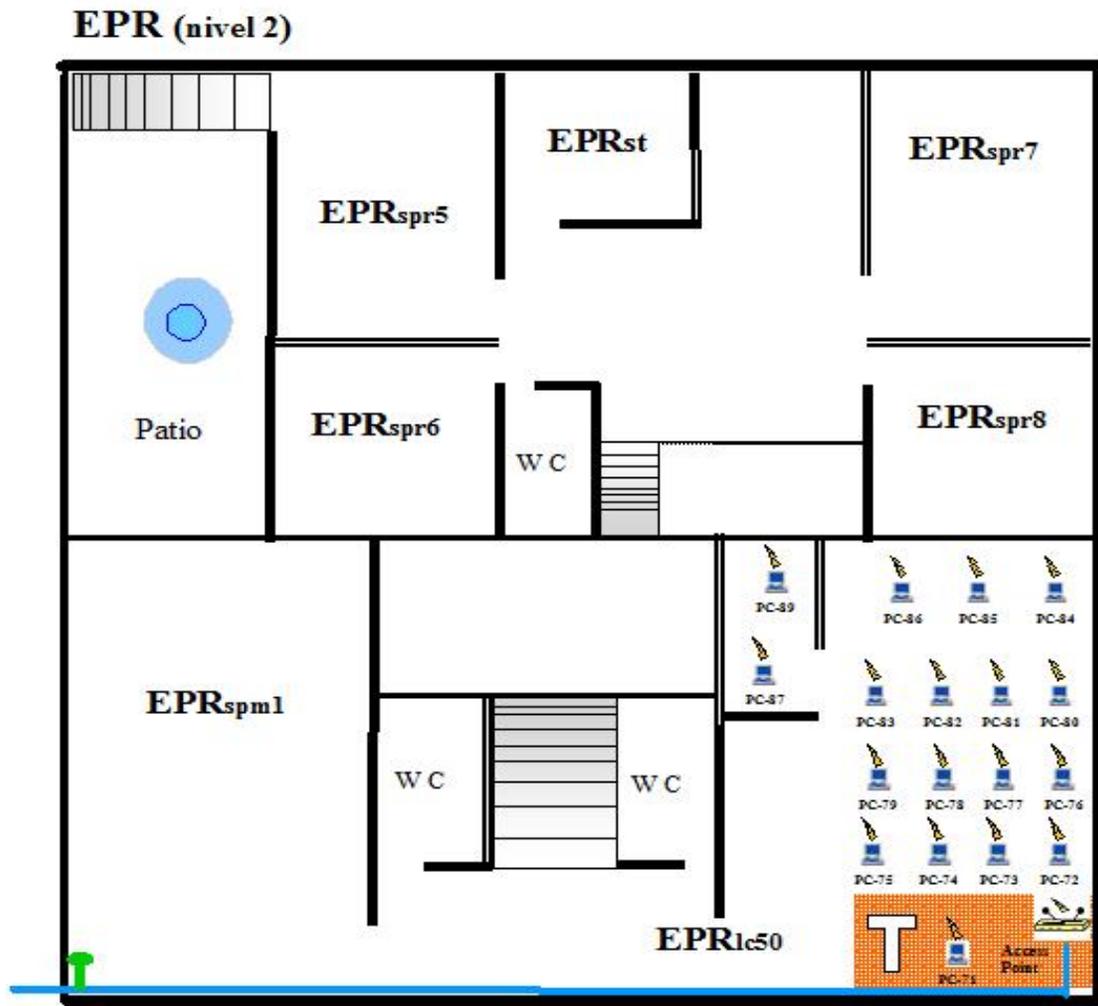


Figura IV.23 Esquema del Edificio de Preescolar. Nivel 2

En el área EPRlc50 habrá acceso inalámbrico de Internet para poder contar con este servicio, aquí se encontrará otro cuarto de telecomunicaciones. Estos equipos deberán firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.23)

Equipos Clientes Fijos: 18

Nodos por cableado par trenzado: 1

Total de Equipos en Servicio: 19

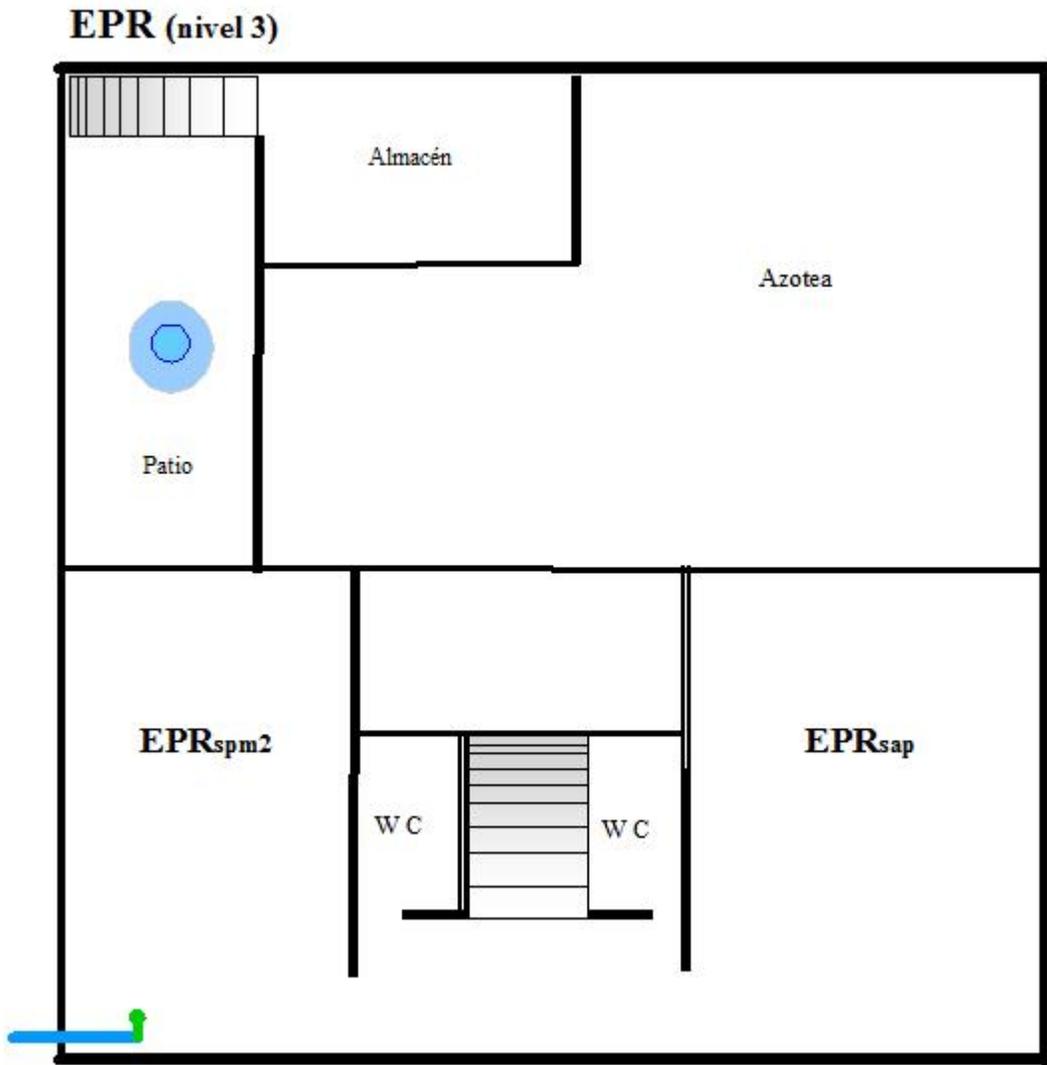


Figura IV.24 Esquema del Edificio de Preescolar. Nivel 3

Esté equipo deberá firmarse a un dominio en un servidor para establecer las políticas restrictivas. (Ver figura IV.24)

Nodos por cableado par trenzado: 1

Total de Equipos en Servicio: 1

4.2 Equipo de conectividad

De acuerdo con el modelo de referencia ISO-OSI, la siguiente capa es la “capa dos” que es de enlace de datos, en donde englobamos los equipos que permiten la interconexión en la red y que son una de las partes medulares para el diseño de una red de alto desempeño.

En los diagramas anteriores hemos descrito tres Cuartos de Telecomunicaciones principales, con esta simbología **T** (ubicado en tres edificios principales del colegio) aquí se localizarán los equipos activos específicamente módems, routers, switches y servidores de aplicación que se detallarán más adelante. Que permitirán la interconectividad de la red entre los edificios.

De igual manera, en los diagramas hemos descrito tres cuartos de Back Bone, con esta simbología **B** en esta se ubicarán (switches y servidores de aplicación). Debido a la demanda de nodos y servicios que requiere la instalación, éste espacio nos proporcionará el espacio necesario para la conectividad de la red interna LAN. (Ver figura IV.25)

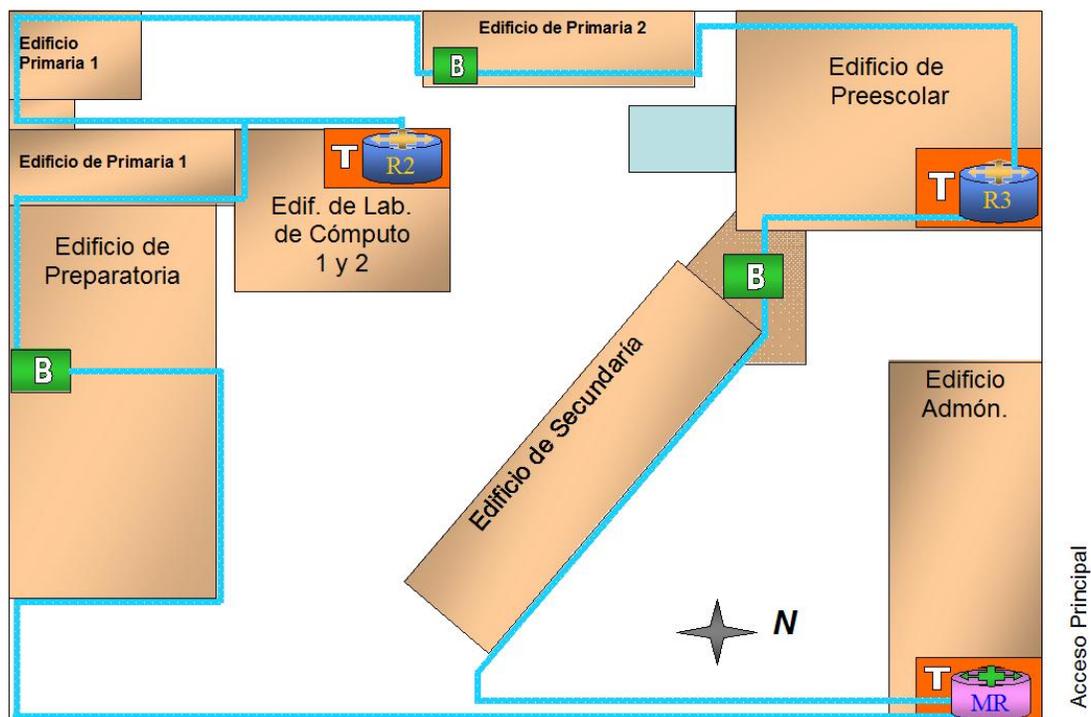


Figura IV.25 Plano de la infraestructura de la red del Queen Mary School.

Se propone la utilización de 1 Modem/Router, 2 Router, 5 switches layer 3, 3 switches layer 2, 2 Acces Point y 3 MAPs Lan Managed Access Point. Para la interconexión de los edificios del Colegio. *(Ver figura IV.26)*

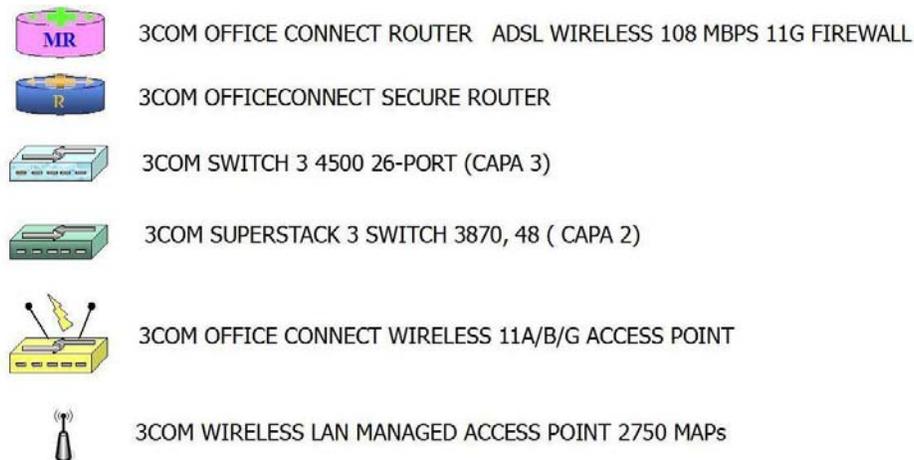


Figura IV.26 Dispositivos Activos.

Diseño del sistema de conectividad que será el siguiente pasó a seguir para la interconectividad de las áreas, estas son:

- Cuarto Principal de Telecomunicaciones.
- Backbone
- Instalación de entrada o acometida.

Después de la especificación de la estructura fundamental de los sistemas de cableado estructurado, la ubicación en detalle de los nodos en cada unos de los pisos y alas de los edificios es como se indica a continuación y de acuerdo con el siguiente Diagrama:

(Ver figura IV.27)

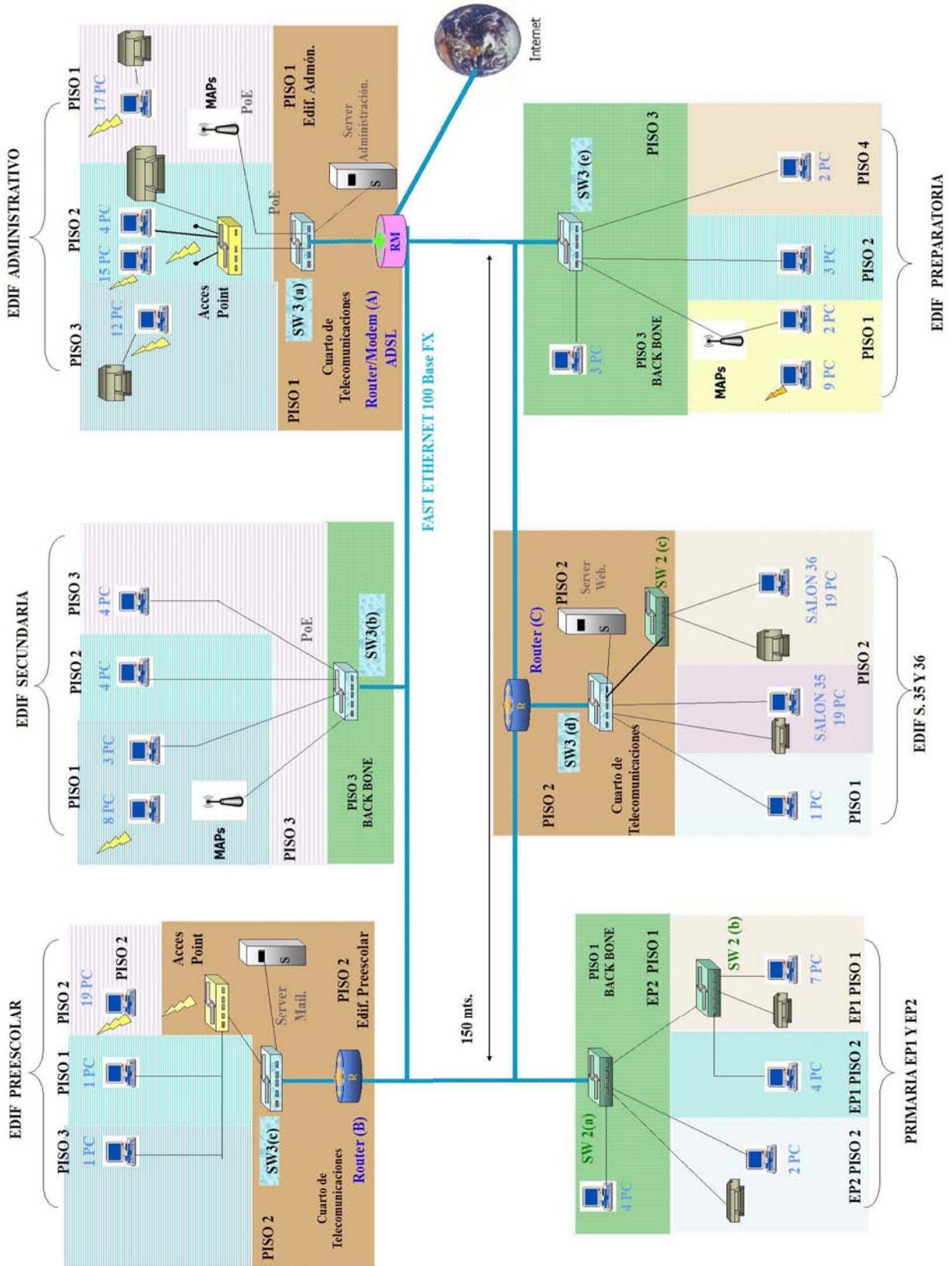


Figura IV.27 Diagrama con los equipos activos interconectados.

DESCRIPCIÓN DEL EQUIPO DE CONECTIVIDAD

3COM OFFICE CONNECT ROUTER ADSL WIRELESS 108 MBPS 11G FIREWALL. (Ver figura IV.28)



Figura IV.28 Router 3Com Office Connect.

Características y ventajas

Acceso compartido a Internet de alto rendimiento, 108 Mbps, y alcance extendido para usuarios cableados e inalámbricos.

El 3Com OfficeConnect ADSL Wireless 108 Mbps 11g Firewall Router con tecnología de alcance extendido (XR) combina un módem ADSL, un router, un punto de acceso inalámbrico 802.11g, un conmutador de cuatro puertos, y un firewall para permitir a hasta un total de 253 usuarios (64 de ellos inalámbricos) compartir de forma segura y económica una única conexión ADSL. El motor de routing de alta velocidad y caudal inalámbrico de 108 Mbps maneja fácilmente grandes transferencias de datos y descargas de Internet, incluyendo las de aplicaciones multimedia.

Proporciona una conexión inalámbrica de alta velocidad de 108 Mbps para usuarios con PCs y portátiles equipados con 802.11g de 108 Mbps, y también es compatible hacia atrás con equipos de LAN inalámbrica 802.11b, protegiendo las inversiones de red existentes. Este router con Certificación Wi-Fi ofrece también soporte del Sistema de Distribución Inalámbrica (WDS). WDS simplifica la configuración de una ampliación inalámbrica de red o de una red totalmente inalámbrica.

Especificaciones de producto

Usuarios soportados: Hasta 253 usuarios (64 inalámbricos) simultáneos.

Puertos totales: puertos de LAN: 4 puertos RJ45 10 BASE-T/100BASE-TX con detección automática; WAN: 1 puerto RJ-11 3C10450A: 802.11g: 108, 54, 48, 36, 24, 18, 12, 9 y 6 Mbps.

Alcance inalámbrico operativo: Máximo en interiores (con obstáculos): 100 m; máximo en exteriores (sin obstáculos): 350 m.

Banda inalámbrica de frecuencias: 2,4 - 2,4835 GHz (depende de las regulaciones locales).

Conjunto de protocolos: Direccionamiento IP dinámico y estático, servidor DHCP, NAT/PAT (con TCP y UDP), PPTP/PPPoE, CHAP, IPCP, SNTP.

Seguridad: Cifrado inalámbrica WPA/WPA2 de 128 bits con TKIP/AES, cifrado WEP de 40/64 y 128 bits, permitir/denegar listas de control de acceso, filtrado de URLs o de palabras clave, desactivar la difusión de SSID, y filtrado de direcciones MAC, NAT/PAT (con TCP y UDP), medición de tráfico, servicio de filtrado de contenidos web de SurfControl (basado en suscripción, se incluye un periodo de prueba gratuita de 14 días sujeto al registro del producto en esupport.3com.com).

Configuración y administración: Interfaz de usuario basada en navegador, detección de dispositivos, ajustes por defecto, administración remota, guardar y restaurar archivos de configuración.

3COM OFFICECONNECT SECURE ROUTER. (*Ver figura IV.29*)



Figura IV.29 Router Office Connect Secure.

Características y ventajas

Acceso compartido a Internet seguro y de alta velocidad para pequeñas oficinas y oficinas domésticas.

El 3Com Office Connect Secure Router proporciona un acceso a Internet protegido y de alta velocidad para múltiples usuarios en contextos domésticos y de pequeñas oficinas o sucursales. Con este router, hasta 253 usuarios pueden compartir de forma económica una única conexión a Internet por cable o DSL, eliminando así la necesidad de adquirir o mantener múltiples líneas y direcciones IP. El router también soporta dos túneles VPN para una comunicación segura y remota de sitio a sitio o de usuario a sitio. El switch integrado de cuatro puertos se conecta a múltiples usuarios o a otra LAN.

Las múltiples características de seguridad protegen la integridad de la red y la privacidad de los datos.

Un avanzado firewall de inspección de estado de paquetes con detección de patrón de hacker y características de protección de denegación de servicio proporciona una defensa contra ataques e intrusiones.

El filtrado de red y el registro de eventos permiten controlar aun más el acceso a sitios web y aumenta la seguridad de las conexiones a Internet de cable o DSL "siempre conectadas".

Sus sencillos asistentes de configuración y su intuitiva interfaz de administración basada en navegador están diseñados para facilitar la instalación y el uso del router Office Connect.

Características tales como routing IP (RIP 1 y 2), routing estático y servidor DHCP proporcionan a los usuarios un sólido rendimiento y una privacidad propios de un router en un paquete económico. Las capacidades de servidor virtual y el soporte de aplicaciones especiales y DNS dinámico proporcionan flexibilidad para un amplio abanico de necesidades de pequeñas oficinas.

El routing de traducción de direcciones de red (NAT) permite a hasta 253 usuarios simultáneos acceder a Internet usando una única conexión de cable o DSL. Cuatro puertos de LAN Ethernet 10/100 con auto MID/MIX proporcionan conectividad de LAN cableada a múltiples usuarios o a otra LAN.

La robusta plataforma hardware ofrece un caudal sin cifrado de LAN a WAN de hasta 20 Mbps, para sacar un total provecho de las velocidades de banda ancha. Un avanzado firewall de inspección de estado de paquetes con detección de patrón de hacker y soporte DoS (denegación de servicio) protege la red contra ataques e intrusiones de hackers.

El soporte de tránsito VPN (red privada virtual) y de iniciación/terminación de dos túneles VPN proporciona conexiones seguras a usuarios o sitios remotos. El registro de eventos ofrece información detallada para la administración del control y de la seguridad del acceso a Internet.

El DNS (servicio de nombres de dominio) dinámico permite a los usuarios conectarse a Internet con direcciones IP dinámicas para usar aplicaciones de red como por ejemplo la Web o servidores FTP que requieren normalmente direcciones IP estáticas (se requiere una suscripción con proveedores de DNS Dinámico).

El servidor DHCP (protocolo dinámico de configuración de host) proporciona automáticamente direcciones de red a PCs, simplificando la configuración y administración. El filtrado de URL controla el acceso a sitios web inapropiados.

Las características de servidor virtual, soporte de aplicaciones especiales y DMZ (zona desmilitarizada) virtual permiten a las empresas configurar servicios de web externos sin comprometer la seguridad de la LAN.

El routing IP (RIP 1 y 2) y el routing estático permiten usar el router en múltiples contextos de red. La medición de tráfico ayuda a monitorizar el uso de Internet.

Especificaciones de producto

Puertos Lan: 4 puertos 10BASE-T/100BASE-TX con detección automática.

Puertos WAN: 1 puerto 10BASE-T/100BASE-TX con detección automática.

Seguridad: Firewall de inspección de estado de paquetes, filtros pre-configurados para los protocolos usados con más frecuencia, filtros configurables por el usuario para paquetes UDP y TCP con números de puerto específicos, capacidad de servidor virtual, DMZ virtual

Soporte de VPN: Iniciación, terminación y tránsito VPN para IPSec. Terminación y tránsito VPN para PPTP; compatible con (MPPE) con claves de sesión de 40 y 128 bits; compatible con esquemas y estándares de cifrado IPSec, incluyendo IKE (intercambio de claves de Internet), HAM (modo de autenticación híbrido), ISAKMP/Oakley DES y 3DES, así como autenticación por clave secreta compartida.

Protocolos soportados: Direccionamiento IP dinámico, direccionamiento IP estático, servidor DHCP, PPPoE, PAP, CHAP, UDP, IP, TCP, IPCP, PPTP, SNTP, NAT/PAT (con TCP y UDP)

Administración: Administración basada en navegador, asistentes de detección de dispositivos, ajustes por defecto, administración remota, guardar y restaurar archivos de configuración.

3COM SWITCH 3 4500 26-PORT (CAPA 3). (Ver figura IV.30)



Figura IV.30. 3 Com Switch 4500.

Características y ventajas

Switch apilable de clase empresarial para aplicaciones de extremo; responde a las necesidades más exigentes de redes convergentes seguras.

El switch 10/100 Ethernet apilable 3Com Switch 4500 26-Port ofrece switching de Capa 2 y routing dinámico de Capa 3 con amplia variedad de características, en una plataforma competitiva de alto rendimiento.

Con una seguridad robusta, y amplias funcionalidades de administración, priorización de tráfico, y calidad de servicio, el Switch 4500 26-Port es capaz de manejar aplicaciones empresariales emergentes.

Se pueden apilar hasta ocho switches mediante puertos Gigabit Ethernet, por lo que toda una pila puede administrarse como una única entidad de administración IP.

24 puertos 10/100 y dos puertos Gigabit de uso dual permiten al Switch 4500 proporcionar una conectividad de LAN segura y fiable para redes de pequeñas y medianas empresas y de sucursales.

Seguridad: El control de acceso de red basado en el estándar 802.1X combinado con la autenticación RADIUS garantiza un acceso seguro a los recursos. Además, el RADA (acceso a dispositivo autenticado mediante RADIUS) permite la autenticación de los dispositivos conectados mediante la dirección MAC.

Las listas de control de acceso (ACLs) basado en puerto habilitan de forma efectiva políticas de uso en cada punto de acceso a la red mediante el switch. El soporte de Secure Shell (SSHv2) y SNMPv3 garantiza un acceso de administración seguro a los switches mediante la autenticación y encriptación del tráfico de administración.

Voz sobre IP dinámica: La exclusiva funcionalidad de VLAN de voz detecta la presencia de teléfonos IP, y asigna dinámicamente puertos de switching a la VLAN de voz, permitiendo así una configuración y priorización automatizadas del tráfico VoIP. Esta potente funcionalidad permite minimizar los costes y la complejidad asociados con la instalación adicional o el traslado de teléfonos IP.

Rendimiento: Capacidad agregada de switching de hasta 8,8 Gbps. Los uplinks Gigabit duales en cada unidad de switching permiten establecer conexiones de alta velocidad con la red troncal, o con los servidores conectados localmente.

Administración y control: La familia Switch 4500 funciona con el sistema operativo de 3Com, el mismo software comprobado y compartido por los switches empresariales de primera clase de 3Com, incluyendo las familias Switch 5500, Switch 7700, y Switch 8800. Las funcionalidades de configuración y control de red son accesibles mediante interfaz de línea de comando (CLI), o bien usando software de administración SNMP, como por ejemplo 3Com Enterprise Management Suite (EMS) y 3Com Network Director.

Facilidad de uso: El routing dinámico con RIP (protocolo de información de routing) permite la actualización automática de topologías de red de Capa 3. La velocidad y el modo duplex en todos los puertos se negocian automáticamente, evitando así la posibilidad de configuración inadecuada.

Especificaciones de producto

Puertos: 24 puertos 10BASE-T/100BASE-TX con auto-negociación configurados como auto MDI/MDIX; 2 pares de puertos Gigabit de uso dual: configurables por el usuario para RJ45 (cobre), o interfaces basadas en SFP (fibra).

Rendimiento: Ancho de banda de transmisión de hasta 8,8 Gbps, hasta 6,5 millones de paquetes por segundo, y un máximo de 8.000 direcciones MAC.

Capacidad de apilamiento: Hasta ocho unidades de switch, o 192 puertos 10/100; Dirección IP única e interfaces de administración para control en toda la pila.

Capa 2: VLANs basadas en puerto (802.1Q): 256, 802.3ad (LACP), agregación manual, grupos de troncal: 13 grupos (26 puertos), 8 puertos 10/100 ó 2 puertos Gigabit por grupo, auto-negociación de velocidad de puerto y duplex, control de flujo full-duplex 802.3x, control de flujo de la presión trasera para el modo half-duplex, 802.1D (STP), 802.1w (RSTP), protección BPDU incluida en Arranque Rápido, snooping IGMP (Protocolo de gestión de grupos de Internet) v1 y v2, Analizador IGMP, filtrado para 128 grupos multicast.

Capa 3: Routing basado en hardware, rutas estáticas 12 además de la dirección por defecto, entradas ARP dinámicas / estáticas: 1990 / 10, interfaces IP: 4, RIP, v1 y v2: 2.000 rutas por defecto y 10 rutas mediante aprendizaje local, snooping IGMP v1 y v2, Relay DHCP: 2 KB máx.

Sistema operativo: Sistema operativo de 3Com; compartido con los 3Com Switch 8800, 7700 y Router 6000.

Administration 3Com: 3Com Network Supervisor, 3Com Network Director, 3Com Enterprise Management Suite.

3COM SUPERSTACK 3 SWITCH 3870, 48 PUERTOS (CAPA 2). (Ver figura IV.31)



Figura IV.31 3 Com Superstack Switch 3870.

Características y ventajas

Switching gigabit apilable con administración, para las redes corporativas Ethernet que necesitan una solución de switching Gigabit escalable, apilable y preparada para el futuro, se recomienda el 3Com SuperStack 3 Switch 3870 de 48 Puertos. Resulta idóneo para aplicaciones en grupos de trabajo de alto rendimiento, puede constituir la plataforma para soportar un paso gradual a velocidades Gigabit.

Este switch 10/100/1000 Gigabit Ethernet de 48 puertos combina switching a velocidad de cable y Capa 2 con apilabilidad de hasta ocho unidades mediante una arquitectura de apilamiento de 40 Gbps. para una escalabilidad impresionante- hasta 384 puertos en total. El hardware soporta una ranura de expansión de 10 Gigabit con capacidad para Capa 3, para proteger la inversión.

Cuarenta y ocho puertos 10/100/1000 de cobre con autosensing proporcionan conexiones flexibles para grupo de trabajo y desktop, que pueden facilitar la migración y servidores habilitados para 10/100 y Gigabit. Cuatro ranuras de uso dual soportan SFPs que pueden conectarse a cableado de fibra para conexiones flexibles Gigabit Ethernet a backbone y servidores.

Las características de resistencia ante fallos tales como IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree y la agregación de enlaces a través de las unidades apiladas IEEE 802.3ad ayudan a garantizar el tiempo de actividad y la disponibilidad.

Especificaciones de producto

48 puertos con auto-negociación para una migración sin discontinuidades de Ethernet o Fast Ethernet a Gigabit Ethernet.

Puertos duales integrados de apilamiento de 10 Gbps. full-duplex con un ancho de banda total de apilamiento de 40 Gbps-para una pila de hasta ocho unidades.

Incluye cuatro puertos de uso dual, soportando ranuras para SFP para alojar conectividad 1000BASE-SX, 1000BASE-LX y 1000BASE-LH.

Soporta un módulo 10Gigabit IEEE 802.3ae para conexiones de alta velocidad entre switches. Se pueden configurar hasta 32 troncales, cada una con ocho puertos, usando IEEE 802.3ad LACP, proporcionando uplinks con un ancho de banda de 8 Gbps por troncal; los puertos de troncales pueden pasar por unidades apiladas.

Total de puertos: 48 puertos 10BASE-T/100BASE-TX/1000BASE-T con autosensing (de los cuales cuatro son de uso dual con las ranuras para SFP), 4 ranuras para SFP capaces de alojar SFPs 1000BASE-SX, 1000BASE-LX y 1000BASE-LH (los SFPs han de pedirse por separado); puerto de consola; 2 puertos de apilamiento; ranura de expansión de 10-Gigabit.

Interfaces con los medios: RJ-45 (dispositivo del switch), LC (SFP opcional), 10GBASE-X (mediante Xenpaks).

Administración: Administración mediante interfaz web, administración mediante interfaz de línea de comandos, SNMP, 3Com Network Supervisor

Cable de consola (RJ-45 a DB9).

3COM OFFICE CONNECT WIRELESS 11A/B/G ACCESS POINT.

(Ver figura IV.32)



Figura IV.32 Com Office Connect Wireless Acces Point.

Especificaciones de producto

- Usuarios soportados: 120 usuarios simultáneos.
- Standard: Wi-Fi certified, IEEE 802.11b, IEEE 802.11g, IEEE 802.11a
- Banda de Frecuencia: 802.11b: 11, 5.5, 2 & 1 Mbps 802.11a/g: 108, 54, 48, 36, 24, 18, 12, 9 & 6 Mbps.
- Rango de Operación: 802.11a: I máx.: 50 metros (164 pies) 802.11b/g: máx.: 100 metros (328 pies).
- Seguridad: 256-bit WPA cifrado; 40/64 & 128, -bit WEP shared-key cifrado; SSID Broadcast Disable, MAC lista de control.
- Protocolo de Acceso: CSMA/CA.
- Computadora con una tarjeta Ethernet 10BASE-T, 10/100, o 10/100/1000.
- Para wireless, PCs ó laptops requiere 802.11g, 802.11b, 802.11a, o 802.11a/b/g PC ó PCI Tarjetas o USB Adaptadores.

3COM WIRELESS LAN MANAGED ACCESS POINT 2750.

(Ver figura IV.33)



Figura IV.33 Acces Point 2750.

Características y ventajas

Permite a los usuarios conectarse a la LAN inalámbrica de forma segura mientras se desplazan, como componente integrante del Sistema de Movilidad para LAN Inalámbrica de 3Com, el 3Com AP2750 aumenta la seguridad móvil y proporciona conectividad inalámbrica para usuarios de LAN inalámbrica.

El AP2750 utiliza integración basada en estándares con el switch y/o controlador de LAN inalámbrica para una instalación plug-and-play. Los datos de configuración para todos los MAPs están distribuidos de forma centralizada para mayor consistencia y exactitud, obteniendo así unos despliegues iniciales simplificados y mayor facilidad de administración. Los controles automatizados de red en el switch inalámbrico mejoran la cobertura y el servicio de MAP al optimizar la ganancia de RF, asignar canales de radio, balancear la carga e incluso rastrear el contexto RF según se necesite, tanto de forma continua como bajo demanda.

El cifrado de MAP proporciona cifrado local de tráfico y distribuye el procesamiento de encriptación en toda la red, en vez de depender de un único dispositivo central. Los escaneos de RF no sólo pueden usarse para localizar usuarios, sino también para identificar y aislar los APs no autorizados u otros infiltradores potencialmente perjudiciales.

Soporta 802.11 a o b/g para velocidades de hasta 54 Mbps a distancias de hasta 100 metros (328 pies) para usuarios 802.11b/g, y de hasta 50 metros (164 pies) para usuarios 802.11a.

Soporta Power over Ethernet (PoE) compatible con 802.3af, de forma que los datos y la alimentación se suministran sobre el mismo cable Ethernet, eliminando así la necesidad de fuentes de alimentación, cables de alimentación o tomas AC.

Las antenas de modo dual 802.11a y 802.11b/g ofrecen un rendimiento y una cobertura excelentes en contextos con elevado multipath; el AP2750 soporta gran variedad de antenas externas de modo dual para unas opciones de instalación flexibles.

Realiza el cifrado de paquetes sobre el aire para WEP, TKIP y AES dinámicos.

Permite el cifrado y aislamiento de subredes o VLANs de forma independiente usando al tiempo un mismo SSID.

El rastreo multi-banda de RF permite a cualquier AP2750 escanear el contexto RF en busca de puntos de acceso no autorizados tanto 802.11a como 802.11b/g, usuarios ad-hoc u otras señales interferentes de RF.

No requiere preparativos ni configuración previa de los puntos de acceso, de forma que los nuevos MAPs, o los de sustitución, heredan la información de configuración del switch o controlador de LAN inalámbrica.

Permite a los MAPs estar conectados directa y/o indirectamente a su switch y/o controlador de LAN inalámbrica, ofreciendo una amplia variedad de escenarios flexibles de despliegue.

Especificaciones del producto

Puertos totales: Un puerto integrado PoE 10BASE-T/100BASE-TX compatible con 802.3af con auto-negociación. Interfaces con los medios: RJ-45, 802.11a, 802.11b, 802.11g, DB-9.

Banda de frecuencia: 802.11a: 5 GHz., 802.11b/g: 2,4 GHz.

Distancia operativa: 802.11a: hasta 50 metros para transmisión y recepción; 802.11b/g: hasta 100 metros para transmisión y recepción. Consumo de alimentación: 6W máximo (puerto PoE o fuente de alimentación externa).

Seguridad: Cifrado WEP de 40/64 y 104/128 bits, TKIP WPA y WPA2 (802.11i/RSN), cifrado AES de 64/128 bits; soporte de SSID de broadcast múltiple en el MAP; login de red IEEE 802.1X; autenticación IEEE 802.11i o RADIUS 802.1X; soporte de ACL y VLAN en el conmutador de WLAN.

4.3 Direccionamiento

Siguiendo con el modelo de referencia ISO-OSI, en la capa 3 (RED), corresponde definir el direccionamiento lógico que se seguirá. Se propone el establecimiento de subredes por área geográfica con la finalidad de reducir los posibles dominios de colisión y aumentar el desempeño interno de la misma red.

La asignación de subredes que se proponen se hará estableciendo una subred por cada edificio.

Esto implica la utilización de 6 subredes válidas. Haciendo uso de direcciones IP no homologadas, clase B, se cuenta con el intervalo:

172.16.0.0

Por ser de clase B, estas direcciones son de la forma:

R.R.N.N.

Donde R: implica un octeto que define una Red válida y N define un nodo o host válido.

La máscara de subred válida para este tipo de direcciones es 255.255.0.0

Como se requiere hacer la división en 6 subredes válidas, se hace uso de la ecuación:

$$2^n - 2 = \# \text{ subredes válidas}$$

Como no existe una potencia de dos que entregue como resultado el número exacto deseado, se toma el inmediato superior, con lo que:

$$2^3 - 2 =$$

$$8 - 2 = 6$$

Esto indica que existen 8 redes de las cuales 6 son utilizables, debido a que la terminada en 0.0 y la terminada en 255.255 son las direcciones llamadas de identificación de la subred y de broadcast respectivamente.

Cada subred tiene un número de nodos o hosts válidos igual a $(N-3).N$, es decir, 3 es el número de bits que se tomarán del “siguiente octeto útil”, esto es, del siguiente octeto al último que implica una red.

En este caso tenemos que los octetos 172.16. Se refieren a las redes válidas de esta clase de direcciones y los octetos 0.0 se refieren al número de nodos válidos. El “siguiente octeto útil” es el primer octeto de nodos válidos, por lo que se toman 3 bits de ese octeto para la definición de las subredes. La combinación binaria de los dos octetos de host quedaría:

$$r r r n n n n n . n n n n n n n n$$

En donde r r r. Implican los bits que se “toman” del siguiente octeto útil y n n n n n, los bits que se refieren a hosts válidos.

El número de hosts que resultan para cada una de las subredes es de 8192, de las cuales 8190 son utilizables, por las mismas razones de la existencia de las direcciones de identificación de red y de broadcast en cada una de ellas.

Las subredes válidas resultan de la combinación binaria de estos 3 dígitos y llevan asociada una máscara de subred también basada en la combinación binaria.

Como la máscara de subred “discrimina” los bits de host, aplica un operador AND lógico a la dirección IP, con lo que se mantienen los bits de red en 1 lógico y los bits de host en 0 lógico.

Para hacer el cálculo de la máscara de subred, se “elevan” a unos los bits de red y se ponen en ceros los bits de host:

Si se tiene la dirección IP: R.R.rrrrnnnn.N, en donde:

R: Octeto que se refiere a una red.

r: Bit que se refiere a redes

n: Bit que se refiere a nodos

N Octeto que se refiere a un conjunto de nodos

Elevando a 1 los bits de red y poniendo a 0 los bits de nodo:

11111111.11111111.11100000.00000000

Lo cual nos da la máscara de subred:

Máscara de Subred

255.255.224.0

Intervalo a utilizar Área geográfica Nodos. (Ver tabla IV.9)

Máscara de Subred	Intervalo a Utilizar		Área geográfica	Nodos
255.255.224.0	172.16.32.1	172.16.32.55	Edificio de Balsas	55
255.255.224.0	172.16.64.1	172.16.64.22	Edificio de Secundaria	22
255.255.224.0	172.16.96.1	172.16.96.21	Edificio de Preparatoria	21
255.255.224.0	172.16.128.1	172.16.128.45	Edificio del Salón 35 y 36	45
255.255.224.0	172.16.160.1	172.16.160.21	Edificio de Primaria	21
255.255.224.0	172.16.192.1	172.16.192.25	Edificio de Preescolar	25

Tabla IV.9 Direccionamiento para las áreas del Colegio.

Para tener acceso hacia la Internet (WWW), se propone el uso del protocolo NAT (Network Address Translation, de sus siglas en inglés) que permite la traducción de direcciones privadas en direcciones públicas haciendo uso de un servidor con ese propósito. Gracias al uso de este protocolo, se aumenta el número de direcciones que puede asignarse a las estaciones de trabajo que requieran “salir” a Internet, con lo que se ve disminuida en cierta medida la escasez de direcciones después del crecimiento tan alto que ha sufrido la WWW en los últimos años.

Prodigy de Telmex provee al Colegio con un intervalo de direcciones homologadas clase B con la dirección 189.179.9.1 hasta la 189.179.9.253. La dirección 189.179.9.254 corresponde a la puerta de salida hacia el enrutador. Estas direcciones proporcionadas por Prodigy de Telmex son las que se configurarán dentro del NAT para tener la salida hacia el Internet.

4.4 Configuración de servidores, plataformas y servicios

De acuerdo con la secuencia del desarrollo del presente trabajo, las capas superiores del modelo ISO-OSI, se tratarán en conjunto en esta sección en donde se verán las plataformas sobre las que se instalarán las aplicaciones y los servicios que estas proporcionarán a los usuarios.

La propuesta es instalar en los servidores de arquitectura robusta (procesador Intel Xeon, 2Gb en RAM, Disco Duro de 200 GB. Tarjeta de red Ethernet de 64 bits) el Sistema Operativo Windows 2003 Server para las aplicaciones de mayor demanda y por otra parte, en un servidor de arquitectura menos robusta (Procesador Pentium IV, 1Gb. en RAM, Disco Duro de 120Gb y tarjeta de red de 64 bits) el sistema operativo Fedora de Linux para el servicio de DHCP que se describirá más adelante.

En lo que respecta a los servidores de impresión, se utilizarán los AXIS 5600+. Este tipo de servidores conecta impresoras directamente a una red y permite que los usuarios puedan imprimir independientemente de los demás servidores.

Los servidores y aplicaciones que manejaremos basados sobre Windows 2003 Server son:

- Servidor de Archivos informáticos
- Servidor de Correo electrónico SMTP/POP
- Controlador de Dominios mediante Active Directory (DNS incluido)
- Servidor de IIS

Los servidores que manejaremos basados sobre Fedora de Linux son:

- Servidor DHCP

El servidor en el que se propone la instalación de Windows 2003 Server, ubicado en los cuartos de telecomunicaciones principales proporcionará las aplicaciones que se enumeraron anteriormente. Este servidor se denominará Servidor Principal.

Servidor de archivos informáticos

Como Servidor de archivos, se designará un volumen para los archivos que se compartirán entre este servidor principal y los usuarios que así lo requieran, estableciendo permisos en función de las necesidades de cada una de las áreas que necesita compartir ó hacer uso de este servicio.

Servidor de correo electrónico

Se definirán dentro del servidor Windows 2003 Server, el protocolo estándar de correo SMTP y el protocolo POP3 para establecer el servidor de correo electrónico que permite la configuración de los diferentes agentes que entran en juego en el intercambio de e-mail.

Con esta aplicación se proporcionarán los servicios de envío y recepción de mensajes de los distintos usuarios explotando los recursos que brinda la infraestructura instalada. Se propone la configuración y administración de cuentas para el personal académico y administrativo del Colegio.

Configuración de Active Directory

Dentro de Servidor principal, se hará la instalación de Active Directory, definiendo como árbol principal del bosque a este y se especificará el dominio queenmaryschool.net

Al instalar el servidor Windows 2003 se ejecutará el asistente de active directory.

Este asistente lo que hace en realidad es crear un servidor de dominio PDC (si no hubiera otro servidor) o bien BDC (si lo hubiera).

Después busca un servidor DNS y si lo encuentra lo anexa al árbol de active directory. Si no lo encuentra instala uno, este servidor DNS es imprescindible porque en adelante los clientes localizarán un controlador de dominio para la validez mediante el envío de una petición al servidor DNS identificado en sus configuraciones TCP/IP cliente. Active Directory utilizará DNS para almacenar información sobre los controladores de dominio de la red. Active Directory actuará no solo como servidor de dominio sino también como servidor DNS.

Cada vez que se necesite hacer modificaciones respecto a active directory, se deberá acceder a la consola desde el panel de control-herramientas administrativas configuración del servidor (también se puede ejecutar el comando “dcpromo.exe”).

En el caso que se propone, del nombre del dominio queenmaryschool.net se pueden derivar sub-dominios como podría ser “publicaciones.queenmaryschool.net” para el acceso al dominio publicaciones.

Las ventajas que representa, son consultas a recursos de la red mucho más rápidas porque se resuelven mediante el catálogo global en vez de búsquedas Netbios.

La administración del directorio activo puede realizarse desde cualquier servidor de dominio de toda la red. La autenticación también se resuelve mediante el catálogo, lo que resuelve problemas de seguridad variados. Un directorio activo es lo mas seguro que tiene Windows hoy por hoy.

Instalación del servidor Web (IIS)

La plataforma Windows 2003 Server trae consigo el servidor IIS (Internet Information Server). El primer paso es ir al panel de control y seleccionar la opción de instalar componentes Windows y en las opciones se selecciona IIS. Y sin más pasos, ya se tiene instalado un servidor Web.

Dentro del menú de administración se genera el “Personal Web Manager” que permite administrar el sistema: (Ver figura IV.34)

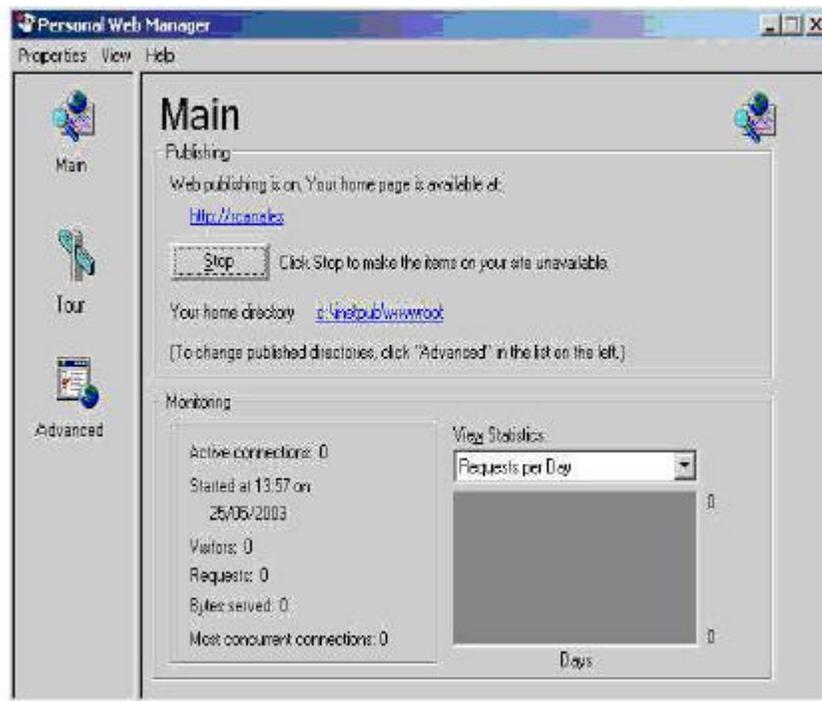


Figura IV.34 Personal Web Manager.

Esta herramienta, permite a los administradores gestionar su sistema, comprobar los accesos, etc.

Ya teniendo el DNS funcionando, enlazado con el servicio TCP/IP y los dominios dados de alta en el DNS, se procede a configurar el IIS para que acepte estos nombres de dominio en lugar de la IP y poder crear las páginas Web que se requieran sin necesidad de que todas estén dentro de la carpeta c:\inetpub\wwwroot

Una vez creada la página Web, pulsamos sobre el botón derecho y seleccionamos propiedades, en menú contextual donde aparece la dirección IP, pulsamos el botón avanzadas y sobre la nueva pantalla seleccionamos la IP, en este momento tenemos una ventana donde asignaremos la dirección IP, el puerto y las cabeceras.

En donde está el valor del encabezado host tenemos que escribir el nombre de domino, por ejemplo pondremos queenmaryschool.net Podemos poner tantos Webs como queramos y repetir este proceso por cada Web nuevo que deseemos instalar.

Con este último paso ya se tiene configurado. Todo lo que queremos publicar en nuestro Web, debe estar ubicado dentro de la carpeta c:\inetpub\wwwroot

Al abrir un navegador y escribir: http://localhost, se verá la página que aparece. Por defecto: localstart.asp, esto es debido a que el sistema busca automáticamente una página llamada Default.htm o Default.asp o iisstart.asp: (Ver figura IV.35)

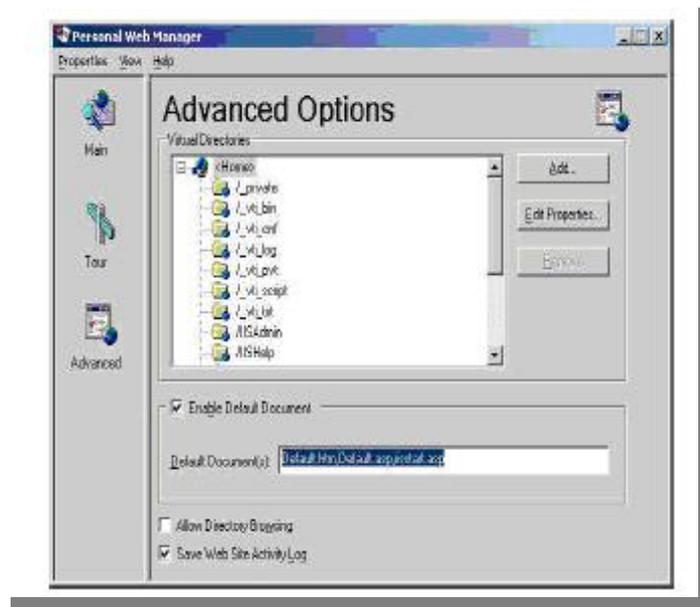


Figura IV.35 Opciones avanzadas.

En esta ventana se puede seleccionar el nombre de la página web que se buscará de inicio.

IIS cuenta con acciones avanzadas que permiten la configuración personalizada del servidor Web. (Ver figura IV.36)

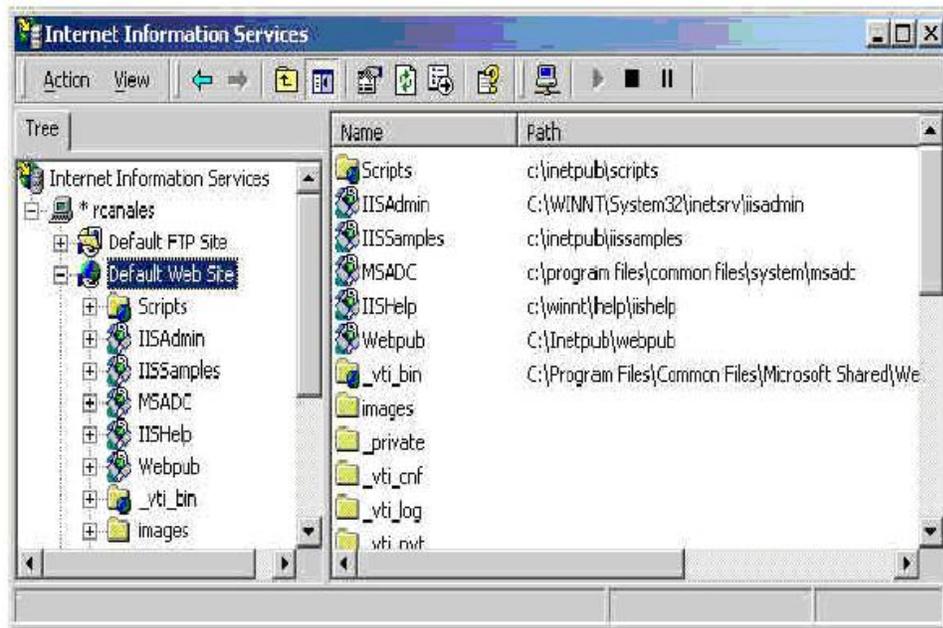


Figura IV.36 Opciones de configuración de IIS.

Dentro de las propiedades, se encuentran las opciones avanzadas de administración.

(Ver figura IV.37)

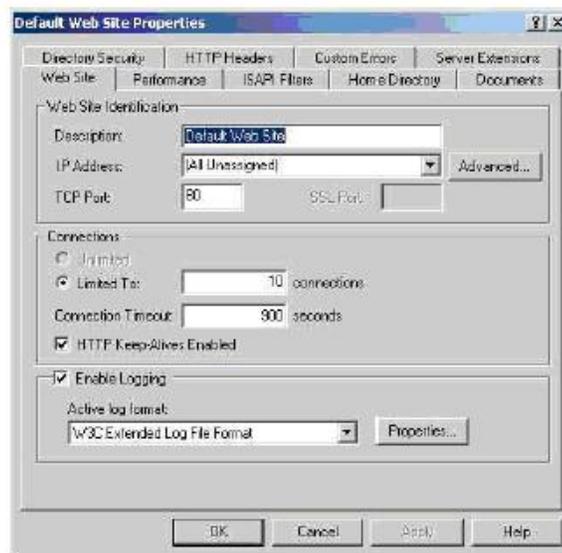


Figura IV.37 Opciones avanzadas de configuración.

Es posible cambiar configuraciones como por ejemplo el número de usuarios que van a acceder para mejorar el rendimiento del sistema en general.

Actualmente la página Web del Colegio se encuentra alojada en un servidor externo a las instalaciones que proporciona Prodigy Infinitum de Telmex, en esta propuesta se pretende dejar el servicio habilitado para que se migre de su ubicación actual hacia el servidor que estamos instalando y que se tenga centralizada la administración de la misma.

Configuración del servidor DHCP en Fedora de Linux

Debido a que el uso de este protocolo no demanda recursos en extremo abundantes, como lo demandaría Windows 2003 Server, se opta por la configuración del servidor DHCP sobre la plataforma Linux. Este servidor se ubicará físicamente en el área de Soporte Técnico y dará servicio a las salas de cómputo que tienen una gran concentración de equipos y asistencia masiva de usuarios.

La función básica de usar este protocolo es evitar que el administrador de la red del Colegio, tenga que configurar manualmente las características propias del protocolo TCP/IP en cada equipo. Para ello, se instala el servidor DHCP, que será capaz de asignar la configuración TCP/IP al resto de las máquinas que así lo requieran en la red, o clientes DHCP, cuando estos inician.

Entre los datos que proporciona el servidor a los clientes se incluyen:

- Una dirección IP por cada tarjeta de red que posea el cliente.
- La máscara de subred.
- La puerta de enlace o gateway.
- Otros parámetros adicionales, como el sufijo del dominio DNS, o el propio servidor DNS.

En esta red pueden convivir equipos que sean clientes DHCP con otros cuya configuración se haya establecido manualmente. Aquellos que estén configurados como clientes DHCP necesitarán encontrar en la red local un servidor DHCP para que les proporcione los parámetros TCP/IP.

Cuando un cliente inicia por primera vez, lanza por la red un mensaje de difusión, solicitando una dirección IP. Como en la red del Colegio solo existirá un solo servidor DHCP, cuando este reciba el mensaje contestará al cliente asociándole una dirección IP junto con el resto de parámetros de configuración.

El DHCP no es un protocolo específico de Linux, sino que se trata de un estándar para cualquier tipo de sistema conectado a una red TCP/IP.

“Para configurar nuestro servidor DHCP hay que crear el archivo `/etc/dhcpd.conf`.

Normalmente lo que se pretenderá es asignar direcciones IP de un intervalo definido de forma dinámica, sin que importe qué cliente escoja qué dirección IP.”⁹

⁹ Morrill L. Daniel. Configuración de sistemas Linux. Madrid: Anaya Multimedia, 2002. 403 p.

Esto se podría conseguir con una configuración parecida a la siguiente:

```
{
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.224.0;
option broadcast-address 172.16.32.255;
option routers 189.179.9.254;
option domain-name-servers 189.179.204.1, 189.179.10.2;
option domain-name "queenmaryschool.net";
subnet 172.16.32.0 netmask 255.255.32.0 {
range 172.16.32.88 172.16.32.99;

}
}
```

En este caso, el servidor DHCP otorgaría una dirección IP al cliente en el intervalo 172.16.32.88 - 172.16.32.99, y concedería la dirección por un tiempo de 600 segundos, mientras el cliente no marque ese tiempo, y en todo caso la concesión máxima será de 7200 segundos. Además configurará el cliente para que use la máscara de red 255.255.224.0, la dirección de difusión 172.16.32.255, el gateway 189.179.9.254, los servidores de nombres 189.179.204.1, 189.179.10.2; y el nombre de dominio queenmaryschool.net

CONCLUSIONES

Al terminar el desarrollo del presente trabajo y recordando los objetivos que fueron planteados en un inicio, debe considerarse diversos aspectos a resaltarse.

- El modelo de referencia ISO-OSI fungió como guía para llevar a cabo el desarrollo de este trabajo al tener cada una de sus capas perfectamente bien especificadas y definidas, con lo cual el análisis y el diseño de la propuesta se pudo hacer de manera esquematizada, buscando la mejor solución en cada uno de los aspectos que se trataron.
- Como todo proceso de planeación debe iniciarse, se hizo un diagnóstico situacional del Colegio, en lo que respecta a infraestructura de red y con ello se logró observar la problemática a la que se enfrenta actualmente, que sirve de base para ubicar las necesidades que se deben satisfacer y por ende, plantear los objetivos que se deben cubrir.
- Desde el punto de vista teórico, los conceptos que aquí se plasmaron, sirvieron como marco para encontrar la solución que satisfizo las necesidades que se plantearon después de llevar a cabo el diagnóstico inicial. La detallada y clara descripción teórica de cada uno de los aspectos que se tocan en el desarrollo, permite que al aplicarlos se tenga la base fundamental que las justifica.
- El desarrollo de la propuesta arroja como resultado las especificaciones que se deben seguir para el diseño, instauración, administración y mantenimiento de una red de alto desempeño en el Colegio.
- En el proceso de diseño se inició por la capa más baja del modelo de referencia.

La descripción detallada del cableado que se propuso, tomando en consideración las características físicas de los edificios, cumple con las características de un cableado estructurado y es este medio de transmisión de la información quien determina gran parte del desempeño de la red, por lo que su adecuada instalación es un aspecto que se debe tomar con mucha seriedad.

- La adecuada selección de los equipos de conectividad que permiten realizar el enlace de datos lleva implícito otro factor que afecta el rendimiento de una red, razón por la cual se propuso el equipamiento que consideramos fuera el adecuado, que sustituye al que está instalado actualmente, para evitar colisiones entre paquetes de información y saturación de alguno de los canales de comunicación. Un concepto que se hace fundamental es el de colapsar el backbone.

Con este proceso se optimiza el desempeño de la red al mantenerse escalada la tasa de transferencia de información.

- Un adecuado direccionamiento, haciendo uso del protocolo IP, permite la segmentación de la red en subredes, lo cual ayuda a minimizar las posibles colisiones entre paquetes de información que viajen dentro de la misma, permite dirigir cada uno de ellos a su destino sin necesidad de recorrer trayectorias inútiles y acelerar procesos que se desarrollen dentro de un mismo segmento de la red. Por esta razón se pensó en establecer una segmentación por área geográfica de acuerdo con la arquitectura de los edificios.
- La inserción de servidores que soporten las aplicaciones y servicios a que los usuarios tendrán acceso, es fundamental en la administración de los mismos y la selección que se realizó fue con base en las necesidades propias del Colegio.

En forma general, y a mi consideración, el desarrollo de esta Tesis cubre los objetivos planteados y entrega una propuesta de diseño e instalación de una red que tendrá un alto desempeño para el COLEGIO ASESORÍA EDUCATIVA QUEEN MARY SCHOOL S.C. en una situación real y viable a corto y mediano plazo.

Al mismo tiempo que me permitió aplicar los conocimientos adquiridos de mis estudios universitarios en la carrera de Ingeniería en Computación en esta máxima casa de estudios y sobre todo de en la F.E.S. ARAGON UNAM, de un Diplomado en Redes de Telecomunicaciones Convergentes de Voz y Datos por (DECFI) División de Educación Continua de la Facultad de Ingeniería de la UNAM y de mis conocimientos adquiridos en el ámbito laboral al permitirme mi participación activa en el análisis y propuesta de reestructuración para la optimización de la red de cómputo académico y administrativo para la institución en la cual trabajo como Pasante de Ingeniero en Computación en el Colegio Asesoría Educativa Queen Mary School S.C. a la cuál he propuesto la optimización de la red en este proyecto de tesis.

GLOSARIO

Ancho De Banda (Bandwidth): Las frecuencias que se pueden pasar a través de un canal de comunicación. Se expresa en términos de la diferencia entre el límite de la frecuencia alta y el límite de la frecuencia baja.

ANSI: American National Standard Institute; Organización no gubernamental donde sus miembros apoyan, diseñan, adoptan y generan estándares en los Estados Unidos, aunque a veces muchos otros países también los adoptan.

Acceso (Access): Conexión a Internet. Tipo de conexión a Internet (Acceso a la red).

Autenticación: Verificación de la identidad de una persona o proceso.

Backbone: Línea de transmisión de información de alta velocidad o una serie de conexiones que juntas forman una vía con gran ancho de banda. Un backbone conecta dos puntos o redes distanciados geográficamente, a altas velocidades.

Bit: Unidad básica de medida de un archivo electrónico. Dígito en notación binaria. Cada uno de los dígitos 0 (off) o 1 (on) usados para representar una de las dos únicas posibilidades en el sistema binario.

Cliente:

- a) Una aplicación que permite a un usuario obtener un servicio de un servidor localizado en la red.
- b) Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio.

- Desmodulación:** Engloba el conjunto de técnicas utilizadas para recuperar la información transportada por una onda portadora, que en el extremo transmisor había sido modulada con dicha información. Este término es el opuesto a modulación.
- Dirección IP:** La dirección del protocolo de Internet (IP) es la dirección numérica de una computadora en Internet. Cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP esta compuesta de cuatro octetos como 132.248.53.10
- DNS:** Sistema de nomenclatura de dominios (Domain Name System). Es un sistema que se establece en un servidor (que se encarga de un dominio) que traduce nombres de computadoras (como servidor.dgsca.unam.mx) a domicilios numéricos de Internet (direcciones IP) (como 132.248.10.1).
- Fibra óptica:** Combinación de vidrio y materiales plásticos. A diferencia del cable coaxial y del par trenzado no se apoya en los impulsos eléctricos, sino que transmite por medio de impulsos luminosos. Es el medio físico por medio del cual se pueden conectar varias computadoras.
- Host. (Anfitrión):** Computadora a la que tenemos acceso de diversas formas (telnet, FTP, World Wide Web, etc). Es el servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente.

- IAB:** Consejo de Arquitectura de Internet (Internet Architecture Board <http://www.iab.org/iab/>). Es el consejo que reglamenta y que toma decisiones sobre estándares que regirán a Internet. Determina las necesidades técnicas a medio y largo plazo, y toma las decisiones sobre la orientación tecnológica de Internet.
- IIS:** Microsoft Internet Information Services. Servicios de Información de Internet de Microsoft. IIS es un conjunto de servicios basados en Internet, para maquinas con Windows. Originalmente se proporcionaba como opcional en Windows NT, pero posteriormente fue integrado a Windows 2000 y Windows Server 2003.
- InterNIC :** Es el nombre que se le da al conjunto de proveedores de servicios de registro. El InterNIC define los nombres de dominio a nivel mundial. El sitio de la Internic (<http://www.internic.net>) es mantenido además por la Nacional Science Fundation (NSF <http://www.nsf.gov>) y la compañía de telecomunicaciones ATT (<http://www.att.com>).
- Kbps:** Kilobits por segundo. Unidad de medida de la velocidad de transmisión por una línea de telecomunicación. Cada kilobit esta formado por mil bits.
- Linux:** Sistema operativo (apoyado en las normas de GNU), similar al UNIX. Linux tiene todas las características que se pueden esperar de un moderno y flexible UNIX. Incluye multitarea real, memoria virtual, librerías compartidas, dirección y manejo propio de memoria.

Microsoft: Compañía creadora del sistema operativo y plataformas Windows, de los controles Active X, desarrolladora del visualizador del World Wide Web Internet Explorer, entre otros recursos.

Nodo: Computadora conectada a una red de área local por un medio físico.

NAT ("Network Address Translation"): NAT es el método por el cual se traduce la dirección de un nodo en Red a otra dirección, su uso principal es cuando existen varios nodos IP en una LAN que requieren comunicarse al exterior pero solo existe un solo nodo al exterior, en otras palabras, NAT coordina varias direcciones a través de una sola dirección IP , su funcionamiento es similar a un "Proxy Server".

OCTETO: Un octeto es un conjunto de 8 bits.

OSI (Open Systems Interconnection):

Un modelo de siete (7) capas propuesto por ISO o International Organization for Standardization en 1983 con la finalidad de asegurar la interoperabilidad entre redes de área local, amplia e incluso mundial, coordinando las funciones comunes a todas las redes de comunicaciones en una arquitectura jerárquica muy bien definida.

Protocolo: Es la definición de como deben comunicarse dos computadoras, sus reglas de comportamiento, etc.

- Rack:** El Rack es un armario que ayuda a tener organizado todo el sistema informático de una empresa. Posee unos soportes para conectar los equipos con una separación estándar de 19". Debe estar provisto de ventiladores y extractores de aire, además de conexiones adecuadas de corriente.
- Raíz (Root):** Directorio inicial de un sistema de archivos mientras que en entornos UNIX también se refiere al usuario principal.
- Router (enrutador):** Un router interconecta dos o más segmentos de una red, separados física o lógicamente. Semejante a un puente, cuando múltiples segmentos de redes son unidos por un enrutador, estos mantienen separadas sus identidades lógicas y pasan a constituir una red Internet --un grupo de redes conectadas por enrutadores. Estos operan en el nivel 3 del modelo OSI.
- Servidor:** Computadora dedicada a gestionar el uso de la red por otras computadoras llamadas clientes. Contiene archivos y recursos que pueden ser accedidos desde otras computadoras (terminales).
- Subnet Mask:** Cuando debemos indicar la dirección IP de una computadora debemos conocer, por supuesto, esa dirección única que diferenciará a esa máquina del resto y la máscara de la subred o subnet mask. El subnet mask no es más que una dirección de 32 bits, que indica cuantos de esos bits están siendo utilizados para el Network ID. Recordaremos que las direcciones IP están conformadas de un segmento izquierdo o Network ID y el derecho o Host ID. El Network ID identifica a una red o segmento en particular --donde un host

o grupo de estos residen físicamente-- y es utilizado para enviar información desde un origen a la interfaz de red indicada en un router. Una vez que la información llega a la red adecuada, los datos son despachados a la computadora (host) que los espera gracias al Host ID. Máscaras por defecto de las Clases A, B y C.

Clase A	255.0.0.0	11111111.00000000.00000000.00000000
Clase B	255.255.0.0	11111111.11111111.00000000.00000000
Clase C	255.255.255.0	11111111.11111111.11111111.00000000

VPN (Virtual Private Network): Una red privada virtual (VPN por sus siglas en inglés - Virtual Private Network) es una red privada de datos que hace uso de una infraestructura pública de telecomunicaciones como podría ser Internet, manteniendo la privacidad a través del uso de un protocolo de entubamiento y de procedimientos de seguridad.

Wireless: Redes sin hilos. Las redes sin cables permiten compartir periféricos y acceso a Internet.

WLAN: Acrónimo en inglés para Wireless Local Area Network. Red inalámbrica de área local permite que un usuario móvil pueda conectarse a una red de área local (LAN) por medio de una conexión inalámbrica de radio. Hoy en día puede cubrir áreas desde 20 a 70 metros dentro de edificios y hasta 350 metros afuera.

WAP: (Wireless Application Protocol). Protocolo de Aplicaciones Inalámbricas. Es un estándar que define una nueva forma de acceso a datos a través del teléfono móvil.

WEP: Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.

INDICE GRÁFICO

CAPÍTULO II FUNDAMENTOS TEÓRICOS

FIGURAS

Figura II.1 Topología de redes en Bus.	8
Figura II.2 Topología de redes en anillo.	8
Figura II.3 Topología de redes en estrella.	9
Figura II.4 Topología de redes en malla.	9
Figura II.5 Cableado Genérico.	33
Figura II.6 Topología del cableado genérico.	34
Figura II.7 Cableado genérico en un campus.	35
Figura II.8 Cableado Horizontal.	36
Figura II.9 Cuarto de telecomunicaciones.	36
Figura II.10 Cuarto de telecomunicaciones.	37
Figura II.11 Solapamientos de canales.	41
Figura II.12 Modo Ad-Hoc o independiente.	42
Figura II.13 Modo Infraestructura.	43
Figura II.14 Ejemplos de DNS.	53

TABLAS

Tabla II.1 Comparación entre el Modelo OSI y TCP/IP.	26
Tabla II.2 Especificaciones de la normas 802.11a, 802.11b y 802.11g.	38
Tabla II.3 Especificaciones aprobadas de la normas 802.11, 802.11a y 802.11b.	39
Tabla II.4 Especificaciones en borrador o aprobación condicional.	39
Tabla II.5 Especificaciones en desarrollo.	40
Tabla II.6 Canales.	40

CAPÍTULO III DEFINICIÓN DEL PROBLEMA

FIGURAS

Figura III.1 Esquema de los siete edificios que conforman el QMS.	62
Figura III.2 Esquema del Edificio Admón. Nivel 1 ó Planta Baja.	67
Figura III.3 Esquema del Edificio Admón. Nivel 2.	68
Figura III.4 Esquema del Edificio Admón. Nivel 3.	69
Figura III.5 Esquema del Edificio de Secundaría. Nivel 1 ó Planta Baja.	70
Figura III.6 Esquema del Edificio de Secundaría. Nivel 2.	70
Figura III.7 Esquema del Edificio de Secundaría. Nivel 3.	71
Figura III.8 Esquema del Edificio de Preparatoria. Nivel 1.	72
Figura III.9 Esquema del Edificio de Preparatoria. Nivel 2.	73
Figura III.10 Esquema del Edificio de Preparatoria. Nivel 3.	73
Figura III.11 Esquema del Edificio de Preparatoria. Nivel 4.	74
Figura III.12 Esquema del Edificio de ELC Salón de usos múltiples. Nivel 1.	75
Figura III.13 Esquema del Edificio de Lab. de Cómputo salones 35 y 36. Nivel 2.	75
Figura III.14 Esquema del Edificio de Primaria 1. Nivel 1.	77
Figura III.15 Esquema del Edificio de Primaria 1. Nivel 2.	77
Figura III.16 Esquema del Edificio de Primaria 2. Nivel 1.	79
Figura III.17 Esquema del Edificio de Primaria 2. Nivel 2.	79
Figura III.18 Esquema del Edificio de Preescolar. Nivel 1.	81
Figura III.19 Esquema del Edificio de Preescolar. Nivel 2.	82
Figura III.20 Esquema del Edificio de Preescolar. Nivel 3.	83

TABLAS

Tabla III.1 EAD.	62
Tabla III.2 ESE.	63
Tabla III.3 EPP.	64
Tabla III.4 ELC.	64

Tabla III.5 EP1.	64
Tabla III.6 EP2.	65
Tabla III.7 EPR.	65
Tabla III.8 Descripción de la red en EAD.	66
Tabla III.9 Descripción de la red en EPP.	71
Tabla III.10 Descripción de la red en ELC.	74
Tabla III.11 Descripción de la red en EP1.	76
Tabla III.12 Descripción de la red en EP2.	78
Tabla III.13 Descripción de la red en EPR.	80

CAPÍTULO IV DESARROLLO

FIGURAS

Figura IV.1 Norma 568B.	87
Figura IV.2 Norma 568A.	87
Figura IV.3 Asignación de Pares en las Normas 568A y 568B.	88
Figura IV.4 Área de trabajo.	88
Figura IV.5 Esquema básico de un nodo.	90
Figura IV.6 Esquema del Edificio Admón. Nivel 1 ó Planta Baja.	94
Figura IV.7 Esquema del Edificio Admón. Nivel 2.	95
Figura IV.8 Esquema del Edificio Admón. Nivel 3.	96
Figura IV.9 Esquema del Edificio de Secundaria. Nivel 1 ó Planta Baja.	97
Figura IV.10 Esquema del Edificio de Secundaria. Nivel 2.	98
Figura IV.11 Esquema del Edificio de Secundaria. Nivel 3.	99
Figura IV.12 Esquema del Edificio de Preparatoria. Nivel 1.	100
Figura IV.13 Esquema del Edificio de Preparatoria. Nivel 2.	101
Figura IV.14 Esquema del Edificio de Preparatoria. Nivel 3.	102
Figura IV.15 Esquema del Edificio de Preparatoria. Nivel 4.	102
Figura IV.16 Esquema del Edificio de ELC Salón de usos múltiples. Nivel 1.	104
Figura IV.17 Esquema del Edificio de Lab. de Cómputo salones 35 y 36. Nivel 2.	104
Figura IV.18 Esquema del Edificio de Primaria 1. Nivel 1.	106

Figura IV.19	Esquema del Edificio de Primaria 1. Nivel 2.	106
Figura IV.20	Esquema del Edificio de Primaria 2. Nivel 1.	107
Figura IV.21	Esquema del Edificio de Primaria 2. Nivel 2.	108
Figura IV.22	Esquema del Edificio de Preescolar. Nivel 1	110
Figura IV.23	Esquema del Edificio de Preescolar. Nivel 2.	111
Figura IV.24	Esquema del Edificio de Preescolar. Nivel 3.	112
Figura IV.25	Plano de la infraestructura de la red del Queen Mary School.	113
Figura IV.26	Dispositivos Activos.	114
Figura IV.27	Diagrama con los equipos activos interconectados.	115
Figura IV.28	Router 3Com Office Connect.	116
Figura IV.29	Router Office Connect Secure.	118
Figura IV.30	3 Com Switch 4500.	121
Figura IV.31	3 Com Superstack Switch 3870.	124
Figura IV.32	Com Office Connect Wireless Acces Point.	126
Figura IV.33	Acces Point 2750.	127
Figura IV.34	Personal Web Manager.	136
Figura IV.35	Opciones avanzadas.	137
Figura IV.36	Opciones de configuración de IIS.	138
Figura IV.37	Opciones avanzadas de configuración.	138

TABLAS

Tabla IV.1	Nomenclatura.	92
Tabla IV.2	Descripción de la red en EAD.	93
Tabla IV.3	Descripción de la red en ESE.	97
Tabla IV.4	Descripción de la red en EPP.	100
Tabla IV.5	Descripción de la red en ELC.	103
Tabla IV.6	Descripción de la red en EP1.	105
Tabla IV.7	Descripción de la red en EP2.	107
Tabla IV.8	Descripción de la red en EPR.	109
Tabla IV.9	Direccionamiento para las áreas del Colegio.	132

BIBLIOGRAFÍA

MOLINA Francisco Javier. Instalación y mantenimiento de servicios de redes locales. España: alfa-omega, 2004. 512 p.

HERRERA Pérez Enrique. Introducción a las telecomunicaciones modernas. México: Limusa. 2001. 410 p.

FITZGERALD AND DENNIS. Redes y comunicación de datos en los negocios. 3ª ed. México: Limusa, 2003. 274 p.

FOROUZAN Behrouz. Transmisión de datos y redes de comunicación. 4ª ed. España: McGraw-Hill, 2007. 870 p.

JAMES Martin. Telecommunications and the Computer. 2ª ed. New York: Prentice-Hall, 1990. 720 p.

MAIWALD Eric. Fundamentos de Seguridad de redes. Madrid: McGraw-Hill, 2004. 496 p.

MICROSOFT CORPORATION. Windows Server 2003, implementación de servicios de red. USA: McGraw-Hill Interamericana, 2004, V. 7

HALLBERG Bruce. Fundamentos de Redes. 4ª ed. México: McGraw-Hill, 2006. 512 p.

ANTONI Barba Martí. Gestión de Red. México: Alfa-Omega, 2001. 231 p.

Morrill L. Daniel. Configuración de sistemas Linux. Madrid: Anaya Multimedia, 2002. 403 p.

TANENBAUM, Andrew S. Computer Networks. 4th. New Jersey: Prentice-Hall, 2003. 912 p.

REFERENCIA ELECTRÓNICA

Education world: Recursos sobre educación <http://www.education-world.com>

Estándares de Internet: <http://info.isoc.org:80/standards/index.html>

Google: <http://www.google.com> Buscar recursos de Internet

<http://cwsapps.fibr.net/cwsa.html>

<http://www.w3.org/pub/DataSources/WWW/Servers.html>

InfoSeek: <http://www.infoseek.com> Buscar recursos de Internet

Linux Documentation Project <http://sunsite.unc.edu/mdw>

Linux en México: <http://www.linux.org.mx>

Microsoft: <http://www.microsoft.com/latam/busqueda/default>.

Microsoft México: <http://www.microsoft.com/mexico/>

Microsoft network <http://www.msn.com>

Servicios de Información: <http://info.isoc.org:80/infosvc/index.html>

<http://lat.3com.com/lat/>

OTRAS FUENTES

Diseño y Administración de Redes WAN Corporativas de Alto Desempeño para voz y datos en “Telecomunicaciones y Redes Convergentes de Voz y Datos”. MAGAÑA Cisneros Adrián. México: UNAM, 2006. Moduló II-B CD ROM.

Diseño y Administración de Servidores Windows y Linux para Empresas Corporativas de Alto Desempeño para voz y datos en “Telecomunicaciones y Redes Convergentes de Voz y Datos”. MAGAÑA Cisneros Adrián. México: UNAM, 2006. Moduló V-I CD ROM.

ROOB, Jones. Ip addressing and subnetting workbook v.1.1.

CISCO NETWORKING ACADEMY.