UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

COSTO Y BENEFICIO DE UNA RED INALÁMBRICA

T E S I S

Para obtener el Título de

INGENIERO EN COMPUTACIÓN

P r e s e n t a

Margarita Monter García

Director de Tesis: Mtro. Marco Antonio Vigueras Villaseñor

México, D.F. 2006

A mi madre,
A mi padre. Los amo.

A mi mejor amigo…….

A Jorge por sacar siempre lo mejor de mí, aún lo que he considerado absurdo.

A Paco, Karina, Oscar, Agustin y mi familia por que aún creen en mí.

A Talis por ser mi amiga incondicional y contagiarme tu magia loca.

A Isa por ser amiga.

A Mer por tantos años de amistad.

A todos los amigos que una vez iniciamos un sueño.

A todos mis profesores que han dejado una huella en mi vida, pues sus enseñanzas me hicieron soñar.

A todos los que dejan huella con su ejemplo de vida.

"Gracias Totales"

Agradecimientos

Al Mtro. Marco Antonio Vigueras Villaseñor por confiar en este paso que para mí es importante.

A la Facultad de Ingeniería por la oportunidad de conocimiento.

A la Universidad Nacional Autónoma de México por abrirme las puertas.

ÍNDICE

Capítulo III: *WIFI CONCEPTOS*.

Lista de figuras:

Lista de tablas:

INTRODUCCIÓN

Una de las industrias *q*ue ha demostrado fuerza trascendente para modificar de manera profunda su entorno, son las telecomunicaciones y su mundo de convergencia digital de los medios.

El presente trabajo pretende señalar los beneficios y conveniencias de contar con una red inalámbrica dentro de una Institución, presentando características del servicio de red, pruebas de monitoreo al servicio que brinda, así como el beneficio económico generado.

Por razones de confidencialidad de la organización en cuestión, de ahora en adelante, se denominará "La Institución" y el área especifica de nuestro análisis como "El Departamento".

"La Institución" se encarga de la regulación y administración de sistemas de salud. "El Departamento" se anexó a la "La Institución" en 1998 con la finalidad principal de capacitación. Dentro de sus actividades de educación en tecnología está principalmente la capacitación (del personal de "La Institución") presencial, por videoconferencia y cursos en línea por Internet. De esta manera, utilizando los avances tecnológicos en el área computacional, "La Institución" optimiza sus funciones.

"El Departamento" es el encargado de implementar, administrar y organizar la capacitación en el ámbito informático por medio de salas equipadas con herramientas tecnológicas, cumpliendo así su compromiso de capacitación al personal de "La Institución".

PRÓLOGO

En el Capítulo I se describe la situación de “El departamento”, la definición del problema, objetivos y metas del trabajo.

El marco teórico, base para la comprensión de la investigación, en donde se describirá el modelo OSI y el modelo TCP/IP así como sus diferencias, características de las tecnologías de red; serán parte del Capítulo II. Mientras que el capítulo III describiremos brevemente la tecnología WiFi.

Respecto al capítulo IV se monitoreará con un software de análisis de red, tomando como muestra una de las salas nuevas que son agregadas a las ya existentes, obtendremos características que nos permitirán formular a partir de variables estadísticas, gráficas y tablas una serie de conclusiones respecto a la saturación y calidad de los servicios ofrecidos.

El capítulo V cubre el aspecto financiero de una red WLAN –inalámbrica- y una Lan cableada –comúnmente usada-, haciendo un comparativo entre ambos y exponiendo las ventajas económicas de dichas tecnologías.

Finalmente en las conclusiones se hace referencia a los resultados obtenidos en el capítulo IV y V concluyendo así la investigación que aquí se propone.

1.1 DEFINICIÓN DEL PROBLEMA

"El Departamento" cuenta con tres aulas para capacitación presencial, siendo una de ellas también para videoconferencia. Como consecuencia de la gran demanda de participantes de personal administrativo perteneciente a "La Institución", se hace insuficiente la infraestructura actual, provocando que dichas salas no cubran las necesidades de capacitación, ocasionando movilidad del personal a distintos lugares.

Igualmente la comunicación entre las áreas de la "La Institución" que requieren la propagación de eventos específicos es insuficiente, motivo por el cual se requiere anexar salas que cumplan ambas funciones de capacitación: presencial y videoconferencia con costos de inversión accesible.

Debido a lo anterior se anexarán 8 salas inalámbricas a las ya existentes, 6 de ellas estarán distribuidas en diferentes puntos del área metropolitana y 2 más en el república mexicana.

1.2 HIPÓTESIS

Existe una tecnología de red que permite la interconexión entre computadoras de manera inalámbrica, esto es, redes cuyos medios físicos no son cables de ningún tipo, lo que marca una diferencia notable de otras tecnologías de red, están basadas en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

Con el siguiente proyecto se pretende demostrar que la tecnología de red inalámbrica es la más adecuada y funcional para cubrir el tipo de necesidades de "La Institución", mejorando notablemente los servicios proporcionados actualmente en capacitación y videoconferencia.

1.3 OBJETIVOS Y METAS

Implementar en las nuevas salas tecnología de red inalámbrica para cubrir servicios y necesidades de "La Institución", reduciendo costos de operación y mantenimiento. Se pretende mostrar con el presente trabajo que una red de tipo inalámbrica es la mejor opción para la capacitación presencial y a distancia de su personal.

La investigación se limita exclusivamente al análisis de la implantación de la tecnología inalámbrica sobre una de las salas de nueva creación y la aplicación de pruebas de funcionalidad para determinar su rendimiento.

2.1 MODELO OSI (OPEN SYSTEM INTERCONNECTION)

El modelo se llama OSI (Interconexión de Sistemas Abiertos) porque tiene que ver con la conexión de sistemas abiertos, los cuales están abiertos a la comunicación con otros sistemas.

Surge frente a la necesidad de interconectar sistemas diversos en los que cada fabricante empleaba sus propios protocolos para el intercambio de señales, basado en una propuesta desarrollada por la Organización Internacional de Estandarización (ISO, Internacional Organization for Standarization) para el año de 1977 estableció un comité para el desarrollo de una arquitectura de comunicaciones, dando como resultado el modelo de referencia OSI. Aunque los elementos esenciales del modelo se definieron rápidamente, la norma ISO final, ISO 7498, no fue publicada hasta 1984

El modelo de referencia OSI es un conjunto jerárquico de capas, donde cada, mostradas en la figura 1, capa realiza un subconjunto de tareas relacionadas entre sí, necesarias para llegar a comunicarse con otros sistemas.

Cada capa se sustenta en la capa inmediatamente inferior, la cual realizará funciones más primitivas, ocultando los detalles a las capas superiores. Una capa proporciona servicios a la capa inmediatamente superior. Idealmente, las capas deberían estar definidas para que los cambios en una capa no aplicaran cambios en las otras capas. De esta forma, el problema se descompone en varios subproblemas más abordables.

Algunas directrices generales que se adoptaron en el diseño son:

- Crear una separación entre capas en todo punto en el que la descripción del servicio sea reducida y el número de interacciones a través de dicha separación sea pequeño.

- Agrupar funciones similares en misma capa

- Crear capas que puedan ser rediseñadas en su totalidad y los protocolos cambiados de forma drástica para aprovechar eficazmente cualquier innovación que surja tanto en la arquitectura, el hardware

o tecnología software sin tener que modificar los servicios obtenidos

- Cada nivel realiza tareas únicas y específicas, además debe ser creado cuando se necesite un grado diferente de abstracción (morfológico, sintáctico o semántico) a la hora de gestionar datos.

- Permitir que los cambios en las funciones o protocolos se puedan realizar sin afectar a otras capas

- Para cada capa establecer separaciones sólo con sus capas inmediatamente superiores o inferiores

- Todo nivel debe tener conocimiento de los niveles inmediatamente adyacentes y sólo de éstos.

A continuación mostraremos la figura correspondiente al modelo OSI:

Figura 1. Modelo OSI

La comunicación se realiza entre las dos aplicaciones de las dos computadoras, etiquetadas como aplicación X e Y como se muestra en la figura 2.

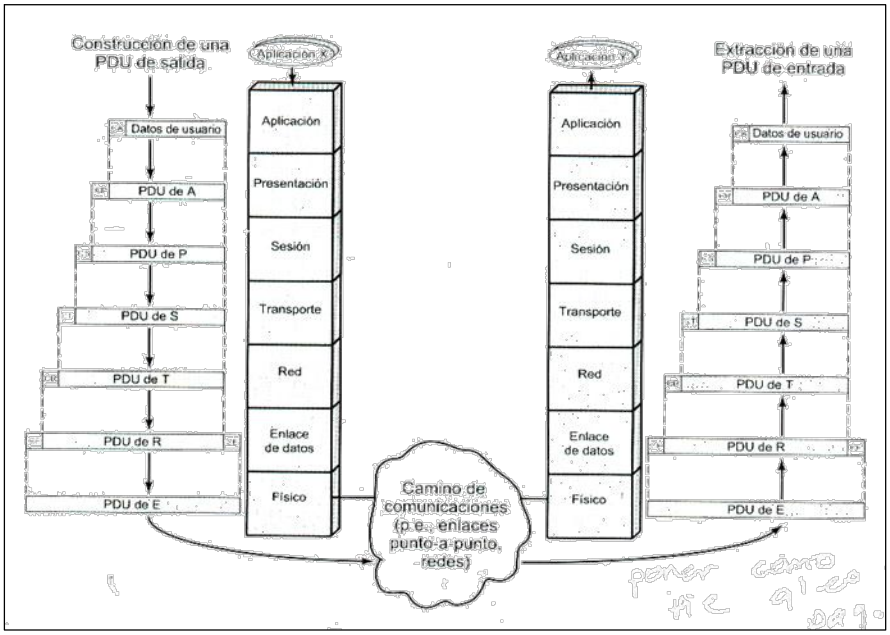


Figura 2. Pila del modelo OSI

Si la aplicación X quiere transmitir un mensaje a la aplicación Y, llama a la capa de aplicación (capa 7). La capa 7 establece una relación proporcional con la capa 7 de la computadora destino, usando protocolo de aplicación. Este protocolo necesita los servicios de la capa 6, de forma tal que las dos entidades de esta capa usan un protocolo común y conocido, y así sucesivamente hasta llegar a la capa física (capa 1), en la que realmente se transmite los bits a través del medio físico.

Es importante señalar que cuando la aplicación X tiene un mensaje para enviar a la aplicación Y, transfiere estos datos a una entidad de la capa de aplicación. A los datos se les añade una cabecera que contiene información necesaria para ser manejados por el protocolo de la capa 7 (encapsulado). Seguidamente los datos originales más la cabecera se pasa como una unidad a la capa 6.

La entidad de presentación trata a la unidad completa como datos y le añade un segundo encapsulado. Así sucesivamente continua hacia abajo hasta llegar a la capa 2, quien normalmente además de una cabecera añade una cola. La unidad de datos de la capa 2, llamada trama, se pasa al

medio de transmisión mediante la capa física. En el destino, al recibir la trama ocurre el proceso inverso. Conforme los datos ascienden cada capa elimina la cabecera más externa, actúa sobre la información de protocolo contenida en ella y pasa el resto de la información a la capa inmediata superior.

A continuación se describen brevemente cada una de las capas del modelo OSI:

2.1.1 Capa Física (Physical)

El propósito principal de esta capa es definir las reglas para garantizar que cuando la computadora emisora transmita el bit "1" la computadora receptora verifique que un "1" fue recibido y no un "0". Primordialmente este nivel es el encargado de la transmisión de los bits de datos (0s ó 1s) a través de los circuitos de comunicaciones.

Los aspectos de diseño tienen que ver mucho con interfaces mecánicas, eléctricas y de temporización, además del medio físico de transmisión que está bajo la capa física.

En esta capa se proveen los medios mecánicos, eléctricos, funcionales y de procedimiento:
Mecánicos: define el tipo de conector, sus dimensiones físicas, las distribuciones de pines, etc.
Eléctricos: concierne a las características eléctricas como su voltaje, nivel de impedancia, etc.

Funcionales: define el significado de los niveles de tensión en cada uno de los pines del conector.

De procedimiento: define las reglas aplicables a ciertas funciones y la secuencia en que estas deben incurrir.

2.1.2 Capa de Enlace (Data Link Layer)

Transforma un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión.

Logra esta tarea haciendo que el emisor fragmente los datos de entrada en tramas de datos de algunos cientos o miles de bytes y transmitiendo dichas tramas de manera secuencial, si el servicio es confiable, el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción.

Notifica al emisor si alguna trama se recibe en mal estado, si alguna de las tramas no se recibieron y se requiere que sean enviadas nuevamente (retransmisión), o si una trama esta duplicada.

Es responsable de la integridad de la recepción y envío de la información, así como de saber dónde comienza la transmisión de la trama y dónde termina, y garantizar que tanto el punto transmisor y receptor estén sincronizados en su reloj y que empleen el mismo sistema de codificación y decodificación.

Otra de las funciones de la capa de enlace de datos es hacer que un transmisor rápido no sature de datos a un receptor lento, generalmente es necesario un mecanismo de regulación de tráfico que indique al transmisor cuanto espacio de búfer tiene el receptor en ese momento, esta regulación de flujo y el manejo de errores están integradas.

Una interferencia de ruido puede destruir totalmente las tramas, en este caso el software de la capa de enlace de datos, como recurso de la máquina, puede retransmitir la trama.

La capa de enlace se subdivide en dos:

- LLC (Logical Link Control) que es la que maneja el control de errores y el control de flujo.
- MAC (Media Access Control), control de acceso al medio, que se encarga de agregar la dirección MAC del nodo fuente y del nodo destino en cada una de las tramas que se transmiten, descartar tramas duplicadas o erróneas, etc.

2.1.3 Capa de Red (Network)

Un aspecto clave del diseño es determinar como se enrutan los paquetes desde su origen a su destino.

Es responsable del direccionamiento de mensajes y de la conversión de las direcciones y nombres

lógicos a físicos, controla las operaciones de la subred. Determina la ruta del mensaje desde la fuente al destino (emisor y receptor), dependiendo de las condiciones de la red.

Las rutas pueden estar basadas en tablas estáticas (enrutamiento estático) codificadas en la red y que rara vez cambian.

Dentro de las funciones de ruteo de mensajes evalúa la mejor ruta que debe seguir el paquete, dependiendo del tráfico de la red, el nivel de servicios, etc. Los problemas de tráfico que controla tienen que ver con el ruteo (routing), intercambio (switching) y congestionamiento de paquetes en la red.

El flujo de datos que proviene de la capa de transporte se le agrega componentes apropiados para su ruteo en la red manteniendo un nivel de control de errores.

Cuando un paquete tiene que viajar de una red a otra para llegar a su destino, puede tener muchos problemas, la red receptora podría no aceptar todo el paquete por ser demasiado largo , protocolos diferentes, etc., por lo tanto, la capa de red tiene que resolver todos estos problemas para que las redes heterogéneas se interconecten.

2.1.4 Capa de Transporte (Transport)

La capa de transporte es una verdadera conexión de extremo a extremo, en toda la ruta desde el origen hasta el destino.

En este nivel se establecen, mantienen y terminan las conexiones lógicas para la transferencia de información entre usuarios. La capa de transporte se relaciona con las direcciones de la red, el establecimiento de circuitos virtuales y los procedimientos de entrada y salida a la red.

Crea una conexión de red múltiple dividiendo los datos entre la conexión de red para mejorar la transmisión.

En esta capa se verifica que la información esté en el orden adecuado, revisando si existe información duplicada o extraviada. Si la información recibida está en desorden, el nivel de transporte

corrige el problema y transfiere la información al nivel de sesión en donde se le dará un proceso adicional.

2.1.5 Capa de Sesión (Session)

Permite que dos aplicaciones en diferentes computadoras establezcan, usen y terminen la conexión llamada sesión.

Establece reglas para iniciar y terminar la comunicación entre dispositivos y brinda el servicio de recuperación de errores; si la comunicación falla y esta es detectada, el nivel de sesión puede retransmitir la información para completar el proceso en la comunicación.

El nivel de sesión es el responsable de iniciar, mantener, y terminar cada sesión lógica entre usuarios finales.

2.1.6 Capa de Presentación (Presentation)

Se define el formato en que la información será intercambiada entre aplicaciones, así como la sintaxis y semántica usada entre las mismas. La información que ha sido recibida de la capa de aplicación es traducida a otro medio reconocido.

La capa de presentación maneja servicios como la administración de la seguridad de la red, como la encriptación y otros servicios específicos, compresión y cifrado de datos. Proporciona reglas para la transferencia de la información y comprime datos para reducir el número de bits que necesitan ser transmitidos.

2.1.7 Aplication (Aplicación)

Es el medio por el cual los procesos de aplicación acceden al entorno OSI, por ello este nivel no interactúa con uno más alto. Proporciona los procedimientos precisos que permiten a los usuarios ejecutar comandos relativos a sus propias aplicaciones.

En esta capa encontramos todas aquellas herramientas para interactuar con la red, es la interfaz del usuario con la red, interpreta los formatos en información legible.

2.2 MODELO TCP/IP (TRANSMISION CONTROL PROTOCOL/ INTERNET PROTOCOL)

El modelo TCP/IP mostrado en la figura 3 comprende todo un conjunto de protocolos que prestan diversos servicios, sus siglas TCP/IP son originarias de dos protocolos que realizan las funciones de inicio del protocolo (protocolo de control de transmisión y el protocolo de Internet).

IP es uno de los protocolos de comunicaciones más viejos en los estándares de redes internas, fue desarrollado por el Departamento de Proyectos Avanzados de Investigación de la Defensa de Estados Unidos (DARPA), su propósito inicial fue resolver los problemas de heterogeneidad de las tecnologías de redes de cómputo. El protocolo que se dio en este modelo comenzó a utilizarse para la construcción del primer switcheo de paquetes en el mundo (ARPANET), lo que condujo al desarrollo del World Wide Internet, hoy una de las redes heterogéneas más grandes del mundo.

El hardware y software de estos dispositivos necesitan ser compatibles, por lo tanto las arquitecturas de redes han sido desarrolladas en la construcción de redes complejas, utilizando variedad de equipos.

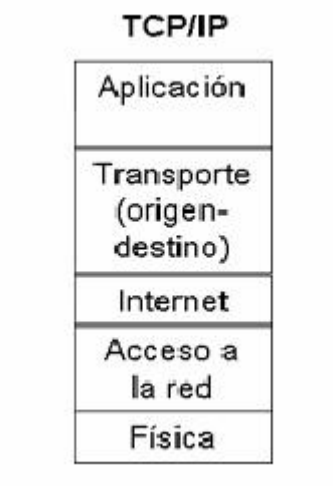


Figura 3. Modelo TCP/IP

2.2.1 Aplicación

Contiene toda la lógica indispensable para posibilitar las distintas aplicaciones de usuario.

Para cada aplicación es necesario tener módulos muy bien diferenciados.

El protocolo Telnet permite que un usuario en una máquina se registre en una máquina remota y pueda trabajar en ella.

El protocolo de transferencia de archivos proporciona una manera eficiente de mover datos de máquina a máquina.

El correo electrónico, en sus inicios, era un tipo de transferencia de datos, más adelante se desarrollo un protocolo especializado: SMTP (Transferencia Simple de Correo Electrónico). A través del tiempo se han ido agregando otros protocolos como el Sistema de Nombres de Dominio (DNS) para la resolución de nombres de host en direcciones de red, HTTP para páginas de World Web, y muchos otros.

2.2.2 Transporte

Independientemente de la naturaleza de las aplicaciones que se encuentren intercambiando datos, es necesario requerir que dichos datos sean intercambiados en forma segura, asegurar que estos lleguen a la aplicación destino y sobre todo en el mismo orden en el que fueron enviados.

Los mecanismos que nos proporcionan esta fiabilidad son en esencia independientes de la naturaleza intrínseca de las aplicaciones, por lo tanto dichos mecanismos están agrupados en una capa común compartida por todas las aplicaciones.

El protocolo más utilizado para controlar la transmisión es el TCP (protocolo control de transmisión). TCP segmenta la información e IP los encapsula, esta encapsulación es llamada datagramas IP, que permiten que los segmentos que fueron hechos por alguna aplicación, sean transmitidos o ruteados en la red.

TCP también maneja el control del flujo para asegurarse de que un emisor rápido no sature a un receptor lento con más mensajes de los que puede manejar.

El segundo protocolo que utiliza es Protocolo de Datagrama de Usuario (UDP), a diferencia de TCP/IP, y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP y que desean proporcionar el suyo, tiene un gran uso en consultas únicas de solicitud-respuesta de tipo cliente-servidor en un único envío así como en aplicaciones en las que la entrega a tiempo es mucho más importante, como en la transmisión de voz y vídeo.

2.2.3 Internet

En situaciones en que las que ambos dispositivos estén conectados a redes diferentes, es necesario seguir una serie de procedimientos que permitan que los datos atraviesen las distintas redes interconectadas, ésta es la función de la capa Internet.

Todos los requerimientos llevaron a elegir una red de conmutación de paquetes basada en una capa de Internet no orientada a la conexión, esta capa es la pieza clave que mantiene unida a la arquitectura.

Para ofrecer el servicio de enrouteamiento a través de varias redes se utiliza el protocolo IP, implementándose tanto en sistemas finales como en los encaminadotes intermedios.

Un encaminador es un procesador que conecta dos redes y cuya función principal es retransmitir datos desde una red a otra siguiendo la mejor ruta para alcanzar el destino.

Por todo lo anterior es razonable decir que la capa de Internet del modelo TCP/IP es similar en funcionalidad a la capa de red del modelo OSI.

2.2.4 Acceso a la red

Encargado del intercambio de los datos entre el sistema final y la red a la cual está conectado,

define una serie de protocolos de comunicación que determina cómo se realiza la comunicación.

El emisor debe proporcionar la dirección de destino, de tal forma que ésta pueda encaminar los datos adecuadamente, dicho emisor puede solicitar servicios como alguna prioridad, estos servicios los proporciona el nivel de red.

El software en particular que se utilice dependerá totalmente del tipo de red que se tenga. Así se han desarrollado estándares diversos para conmutación de circuitos, conmutación de paquetes que incluye retransmisión de tramas, y para redes de área local.

Permiten que la información sea enviada de un sistema a otro sin necesidad de que ambos sean del mismo fabricante, lo importante es que utilicen el mismo protocolo de comunicaciones.

Una vez separando en una capa diferente todas aquellas funciones que tengan que ver con el acceso a la red, el software de comunicaciones situado por encima de la capa de interface de red no tendrá que ocuparse de los detalles específicos de la red a utilizar, el software de las capas superiores, deberá por tanto, funcionar adecuadamente con independencia de la red a la que el sistema este conectado.

2.2.5 Física

Esta capa define la interfaz física entre el dispositivo de transmisión de datos y el medio de transmisión (red), encargándose de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de los datos, etc.

2.3 DIFERENCIA Y COMPARACIÓN ENTRE LOS MODELOS OSI Y TCP/IP.

Ambos modelos -mostrados en la figura 4- tiene mucho en común, se basan en el concepto de una pila de protocolos independientes. En los dos modelos las capas que están arriba incluyendo la capa de

transporte, están ahí para proporcionar un servicio de transporte individual de extremo a extremo a los procesos que desean comunicarse, formando el proveedor de transporte.

A pesar de las similitudes, los modelos tienen muchas diferencias clave, es importante hacer notar que haremos la comparación a los “modelos de referencia” no a las pilas de protocolos correspondientes.

Para el Modelo OSI hay tres conceptos básicos:

Servicios
Interfaces
Protocolos

Se considera como una contribución grande de dicho modelo, el hacer explícita la distinción entre estos conceptos.

La definición de servicio indica lo que hace la capa, de ninguna manera la forma en que la entidad superior tiene acceso a ella o cómo funciona dicha capa, solo define el aspecto semántico de la capa.

La interfaz indica a los procesos que están sobre ella como accederla especificando cuales son los parámetros y qué resultados se esperan. No dice nada sobre cómo funciona internamente la capa.

Una capa es la que debe decidir qué protocolos iguales utilizar, pueden ser cualesquiera en tanto consiga se haga el trabajo, es decir proporcione los servicios ofrecidos, también puede cambiarlos cuando se necesite sin afectar el software de capas superiores.

En el modelo TCP/IP los únicos servicios ofrecidos realmente por la capa de Internet son SEND IP PACKET y RECEIVE IP PACKET.

Como consecuencia los protocolos del modelo OSI están mejor ocultos que los del modelo TCP/IP y son fácilmente reemplazables conforme cambia la tecnología, el cual es el objetivo principal de tener protocolos en las capas.

El modelo OSI se vislumbro antes de que se diseñaran los protocolos, el modelo no estaba diseñado para un conjunto particular de protocolos, un hecho que lo hizo de ámbito general. Una

deficiencia de estar clasificado así es que los diseñadores no tenían mucha experiencia con el asunto y no tenían una idea concreta de que funcionalidad poner en cada capa.

Cuando se empezaron a construir redes reales y aparecieron redes de difusión que utilizaron OSI y los protocolos existentes se noto que estas redes no coincidían con las especificaciones de los servicios solicitados viéndose en la necesidad de integrar subcapas convergentes en el modelo para proporcionar un espacio para documentar, por lo tanto el modelo OSI no fue pensado para la interconectividad de redes ya que la capa de enlace de datos sólo trataba con redes punto a punto.

Con TCP/IP paso todo lo contrario, los protocolos llegaron primero y el modelo fue en realidad una descripción de los protocolos existentes. No había problemas para ajustar los protocolos al modelo estos encajaban a la perfección.

El problema es que el modelo no aceptaba otras pilas de protocolos, dando como consecuencia que este no fuera útil para describir otras redes que no fueran TCP/IP.

Una diferencia patente entre ambos es el número de capas OSI con siete y TCP/IP con cuatro, ambos con capas de red, transporte y aplicación, sin embargo las restantes capas difieren uno de otro.

Una diferencia más está en el área de la comunicación orientada a la conexión comparada con la no orientada a la conexión, OSI soporta ambas (capa red) sólo la comunicación orientada a la conexión en la capa de transporte donde es importante (porque el servidor de transporte es transparente para el usuario). TCP/IP solo tiene un modo en la capa de red y es el de no conexión, sin embargo soporta ambos modos en la capa de transporte, dando a los usuarios la oportunidad de elegir, importante especialmente para protocolos sencillos de solicitud-respuesta.

Diagrama comparativo de capas entre ambos modelos:

Figura 4. Comparación de amos modelos

2.4 DISPOSITIVOS DE RED

Los dispositivos de conectividad LAN permiten que distintas LAN's instaladas en un mismo edificio se interconecten y, en otros casos, la conexión a un medio de transmisión externo.

2.4.1 Repetidor (Repeater)

Este dispositivo trabaja en la capa física del modelo OSI. Es un dispositivo que simplemente amplifica o regenera señales débiles. Usado para extender las longitudes físicas de las redes, pero no contiene inteligencia para funciones de enrutamiento. Un repetidor se utiliza cuando dos segmentos están acercando sus longitudes físicas máximas, las cuales son limitadas por el cableado.

Al unir dos segmentos, tiene la desventaja de compartir el mismo ancho de banda con un máximo de cuatro repetidores como máximo.

2.4.2 Concentrador (Hub)

Es un dispositivo que puede crear workgroups (grupos de trabajo) y trabaja en la capa física. El hub da la facilidad de administración remota de la red, realiza una detección y resolución sencilla de problemas, así como el control en el crecimiento de la red, dando seguridad de las mismas.

Este dispositivo esta relacionado con una red Ethernet por que el tráfico es propagado a través de todos los segmentos, debido a que puede funcionar como el bus principal.

2.4.3 Puente (Bridge)

Un puente puede conectar dos grupos de trabajo LAN, particionando el tráfico en la red, también crea una forma de seguridad y facilidad en la administración de la red. Un bridge utiliza tablas dinámicas. Por el contrario puente tiene la posibilidad de extender los nodos de una red. Cuando un puente separa a un hub es llamado segmento.

2.4.4 Conmutador (Switch)

Un switch es un dispositivo que trabaja en capa de enlace del modelo OSI. Permite unir dos segmentos de red. Filtra, envía e inunda tramas basándose en la dirección destino de cada trama.

2.4.5 Enrutador (Router)

Ayuda a unir dos redes a nivel capa de Network (red), determinando mejor ruta. Este dispositivo interconecta segmentos de red o redes enteras.

La información se intercambia mediante direcciones lógicas, aunque tiene acceso a la información física. Un router se compone de interfaz de red y tabla de ruteo.

Los routers toman decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Los routers toman decisiones basándose en diversos parámetros. La más importante es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP). Otras serían la carga de tráfico de red en los distintos interfaces de red del router y la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

2.4.6 Puerta de enlace (Gateway)

Inicialmente fue conocido como un dispositivo de enrutamiento, pero ahora el término router se utiliza para describir los nodos que desempeñan esta función. Un Gateway es un dispositivo especial que realiza una conversión de la capa de aplicación de la información de una pila a otra. 0

2.5 MEDIOS DE TRANSMISIÓN

El camino físico entre el transmisor y receptor es llamado medio de transmisión. La calidad y características de una transmisión están determinadas por el tipo de señal y las características del medio.

En el diseño de un sistema de transmisión es tan importante la distancia como la velocidad de transmisión, estos deberán ser lo más grande posible. Los factores relacionados con el medio de transmisión y con la señal que determinan tanto la distancia como la velocidad de transmisión son: el ancho de banda, dificultades en la transmisión, interferencias y número de receptores.

2.5.1 Par trenzado

El par trenzado, figura 5, es el medio más económico, y a la vez, el más usado. Consiste en dos cables de cobre embutidos en un aislante entre cruzados en forma de bucle espiral. Cada par de cables

constituye un enlace de comunicación. Normalmente, varios pares se encapsulan conjuntamente mediante una envoltura protectora. Para largas distancia, la envoltura puede contener cientos de pares.

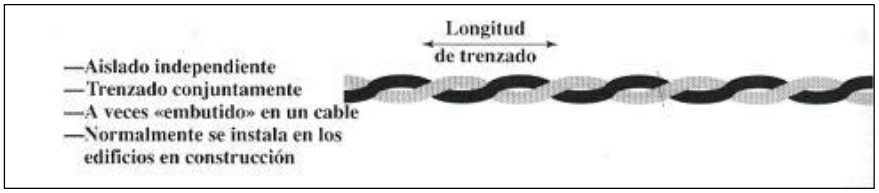


Figura 5. Par trenzado

Si se emplean circuitos controladores de línea y receptores apropiados, las líneas de par trenzado son convenientes para las tasas de bits de orden de 1 Mbps a distancias cortas -de menos de 100 metros- , y para tasas de bits más bajas a distancias más largas. Con circuitos controladores y receptores más avanzados es posible alcanzar tasas de bits similares, o incluso superiores a distancias mucho más largas. Estas líneas, denominadas pares trenzados no blindados (UTP: Unshield Twisted Pair), tienen un uso masivo en redes telefónicas y con circuitos integrados especiales) en muchas aplicaciones de comunicación de datos. Los pares trenzados blindados (STP: Shielded Twisted Pairs) se valen de una de una malla o blindaje protector para reducir aún más los efectos de las señales de interferencia.

El documento que publicó la EIA (Electronic Industries Association) denominado Estándar para los cables de telecomunicaciones en edificios comerciales en 1991, donde se define el uso de pares trenzados sin apantallar de calidad telefónica y de pares apantallados como medios de transmisión de datos en edificios fue nombrado el Estándar EIA-568. Como respuesta a esa necesidad, en 1995 se propuso el EIA-568A la cuál incorpora los avances más recientes, tanto en el diseño de cables y conectores como en e los métodos de test. En esta especificación se consideran cables de pares apantallados a 150 ohmios, y pares no apantallados de 100 ohmios. Para este estándar se consideran tres tipos o categorías de cables UTP:

Tipo 3.- cables y Hardware asociado, diseñados para frecuencias de hasta 16 MHz.

Tipo 4.- cables y Hardware asociado, diseñados para frecuencias de hasta 20 MHz.

Tipo 5.- cables y Hardware asociado, diseñados para frecuencias de hasta 100 MHz.

Los tipos 3 y 5 son los más utilizados a los entornos LAN. Teniendo un diseño apropiado y distancias limitadas, con cables tipo 3 se pueden conseguir velocidades de hasta 16 Mbps. Respecto al tipo 5, el cual es un cable de mejores características para transmisión de datos, es el más utilizado para la preinstalación en los edificios de reciente construcción. Teniendo un diseño apropiado y a distancias limitadas, con cables tipo 5 se pueden alcanzar 100 Mbps.

El par trenzado también se utiliza dentro de edificios como medio de transmisión para las redes de área local. Recientemente se han desarrollado redes de pares trenzados con velocidades de hasta 1 Gbps, aunque estas configuraciones están bastante limitadas en el número de posibles dispositivos a conectar y en la extensión geográfica de la red. Para aplicaciones de larga distancia el par trenzado se puede utilizar a velocidades a velocidades de 4 Mbps ó incluso mayores.

2.5.2 Cable coaxial

Conforme aumentan las tasa de bits y por tanto la frecuencia de la señal transmitida, la corriente que corre por los alambres atiende a escribir sólo por la superficie exterior del alambre de modo que no aprovecha la totalidad del área transversal disponible. Ello incrementa la resistencia eléctrica de los alambres cuando las señales son de frecuencia más alta, lo que ocasiona una atenuación mayor. También, a frecuencias más altas se tienen más potencia de la señal por causa de los efectos de radiación. Por todo lo anterior, si una aplicación exige una tasa de bits mayor que 1 Mbps se necesitaran circuitos controladores y receptores más avanzados o bien otro tipo de medio de transmisión.

El cable coaxial (figura 6) consiste en un conductor cilíndrico externo que rodea a un cable conductor interior. Éste último se protege con una cubierta o funda. El cable coaxial tiene un diámetro aproximado entre 1cm. y 2.5 cm.

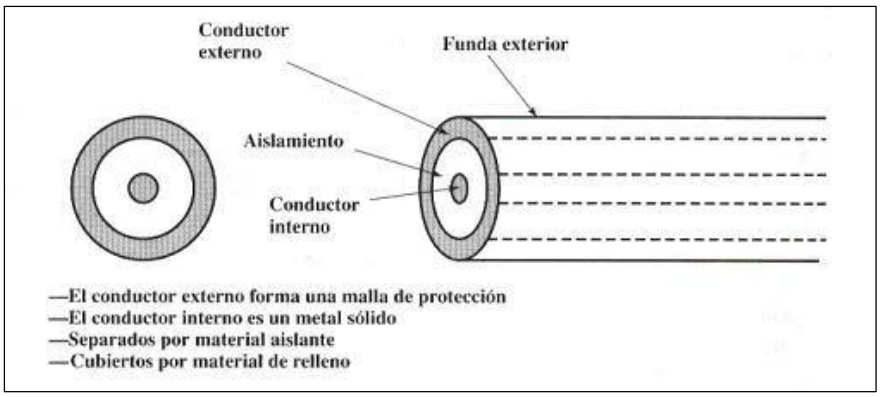


Figura 6. Cable coaxial

El coaxial se emplea para la distribución de señales para la TV por Cable y ha sido un elemento fundamental en la red de telefonía a larga distancia.

El cable coaxial pude transportar simultáneamente más de 10,000 canales de voz, también se usa frecuentemente para conexiones entre periféricos ó dispositivos a distancias cortas. Usando señalización digital, se pude utilizar como medio de transmisión en canales de entrada/salida (E/S) de alta velocidad en computadoras.

Se usa para transmitir tanto señales analógicas como digitales. Debido al apantallamiento, por construcción, el cable coaxial es mucho menos susceptible que el par trenzado tanto a interferencias como a diafonía. Sus principales limitaciones son la atenuación el ruido térmico y el ruido de intermodulación.

En la señalización digital es necesario un repetidor cada kilómetro de distancia aproximadamente, e incluso menos cuánto mayor sea la velocidad de transmisión. Respecto a la transmisión de señales analógicas a larga distancia se necesitan amplificadores separados entre sí a distancias del orden de poco kilómetros, siendo esta separación tanto menor cuando mayor sea la frecuencia de trabajo. Hasta 500MHz se extiende la señalización analógica aproximadamente.

2.5.3 Fibra óptica

Es un medio flexible y delgado de 2 a 125 μm, capaz de confinar un haz de naturaleza óptica, para construirla se utilizan diversos tipos de cristales y plásticos.

Las pérdidas de datos menores se han conseguido utilizando fibras de silicio ultrapuro fundido, sin embargo son difíciles de fabricar y tienen un mayor costo; las fibras de cristal multicomponente son económicas, aunque sufren mayores pérdidas, son recomendables, la fibra de plástico tiene todavía un costo menor, se utiliza en enlaces de distancias más cortas, en los que son aceptables pérdidas moderadamente altas.

Un cable de fibra óptica (figura 7) tiene forma cilíndrica y está formado por tres secciones concéntricas: el núcleo, el revestimiento y la cubierta. Los cables transportan los datos transmitidos en forma de un haz de luz fluctuante dentro de una fibra de vidrio, y no como una señal eléctrica en un alambre

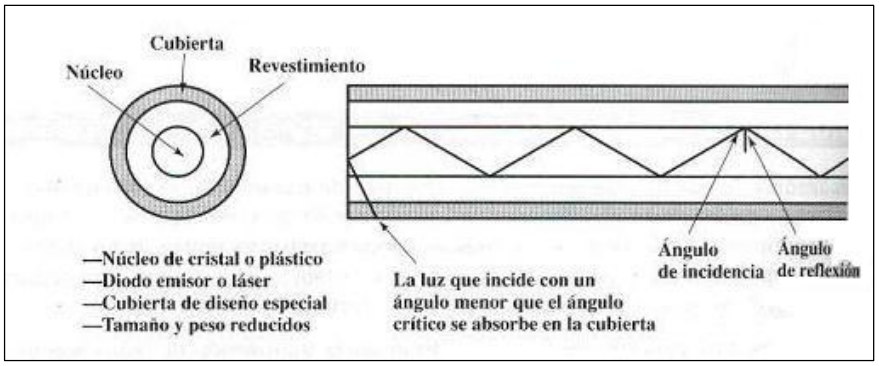


Figura 7. Cable de fibra óptica

La fibra disfruta de una gran aceptación para las telecomunicaciones a larga distancia, cada vez la utilizan más en aplicaciones militares. Las mejoras constantes en las prestaciones a precios cada vez inferiores, igual que sus ventajas inherentes, han ocasionado que la fibra sea un medio atractivo en los entornos de red de área local, algunas de sus ventajas son las siguientes:

- Mayor capacidad
- Menor tamaño y peso
- Atenuación menor
- Aislamiento electromagnético
- Mayor separación entre repetidores

Las cinco aplicaciones, en las que la fibra óptica tiene una importancia importante son:

- Transmisiones a larga distancia
- Transmisiones metropolitanas
- Acceso a áreas rurales
- Bucles de abonado
- Redes de área local

En redes de área local, recientemente se han desarrollado estándares y productos para redes de fibra óptica con capacidades que van desde 100 Mbps hasta 10 Gbps, las cuales a su vez permiten cientos, incluso miles de estaciones, en grandes edificios.

2.6 REDES DE AREA LOCAL (LOCAL AREA NETWORK-LAN)

Es un conjunto de computadoras o dispositivos conectados entre sí, de forma física y lógica con la finalidad de optimizar sus recursos y emular el proceso de un sistema único. Con una Red LAN podemos conectar entre sí estaciones de trabajo en las oficinas de un solo edificio o un grupo de edificios, como podría ser el caso de un campus universitario, o para interconectar equipos en una fábrica o un complejo hospitalario. En virtud de que todos los equipos se encuentran bajo un mismo establecimiento, es normal que la organización instale y mantenga la LAN, es por ello que se conocen también como redes de datos privada.

Una red LAN esta limitada en cobertura al entorno definido por el usuario, estas características dan a los usuarios muchas ventajas a diferencia de lo que pudiera desarrollar un usuario aislado, entre las principales se puede mencionar: La posibilidad de conectar equipos de diferentes tecnologías, acceso a bases de datos comunes, correo electrónico, así como utilizar aplicaciones en red y procesamiento distribuido, etc.

En una red LAN existen elementos de hardware y software, entre los cuales se pueden destacar: servidores, estaciones de trabajo, sistema operativo, protocolos de comunicación y tarjetas de red.

La diferencia principal entre un camino de comunicación establecido con una LAN y una conexión a través de una Red de datos pública. Es que una LAN suele contar con tasas de transmisión de datos mucho más altas debido a las distancia físicas relativamente cortas.

Hay 2 tipos muy distintos de LAN: LAN por cable y LAN inalámbricas (Wireless LAN), como sus nombres lo indican, las LAN por cable utilizan cableado fijo (par trenzado, cable coaxial ó fibra óptica) como medio de transmisión, en tanto que las WLAN utilizan ondas de radio o de luz.

2.6.1 Topologías

Una red presenta 2 tipos de topologías: Física y lógica. Sin embargo, dependiendo del método de acceso al medio utilizado, el funcionamiento lógico de la red corresponderá a determinada topología pudiendo ser distinta a la topología física.

La topología física se refiere a la forma de conectar físicamente a las estaciones de trabajo dentro de una red. Cada topología, independientemente de la forma o apariencia geométrica que pueda tener, cuenta con características propias que definen el material a utilizar como medio de transmisión, distancia máxima entre estaciones, grado de dificultad para realizar el cableado, así como para su mantenimiento, ya que la disposición de las estaciones en la red puede determinar si una falla afecta a uno o más elementos; favorece también determinados métodos de acceso. Entre las topologías más utilizadas se encuentran:

2.6.1.1 Topología en Bus

Por medio de una transmisión lineal donde todas las estaciones están directamente conectadas (figura 8) a través de interfases físicas llamadas tomas de conexión. Full dúplex es el funcionamiento entre la estación y la toma de conexión permitiendo la transmisión y recepción de datos a través del bus. Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de las estaciones. Al término de cada extremo del bus existe un terminador que absorbe las señales, eliminándolas del bus.

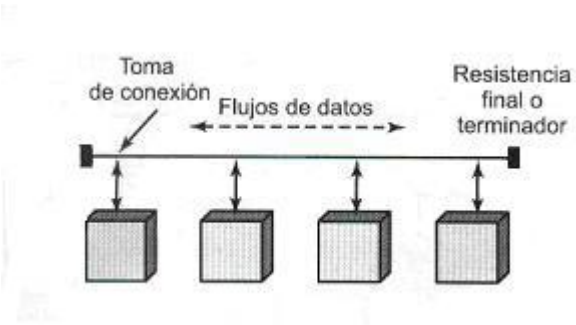


Figura 8. Bus

2.6.1.2 Topología en Anillo (Ring)

Es un conjunto de repetidores (figura 9) unidos por enlaces punto a punto formando un bucle cerrado. Un repetidor es capaz de recibir datos a través del enlace y transmitirlos bit a bit a través del otro enlace tan rápido como sean recibidos, estos enlaces son unidireccionales, es decir, los datos se transmiten en un solo sentido, de modo que estos circulan alrededor del anillo en el sentido de las agujas del reloj o en el contrario. Los datos se transmiten en tramas, circulando por el anillo y pasando por las demás estaciones de modo que la estación destino reconoce su dirección y copia la trama mientras esta la atraviesa en una memoria temporal total. La trama continúa circulando hasta que alcanza de nuevo la estación origen donde es eliminada del medio.

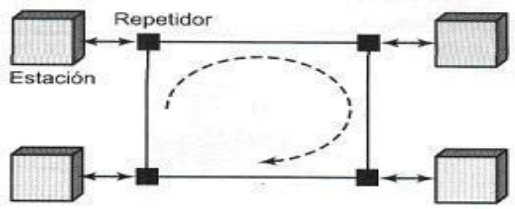


Figura 9. Anillo

2.6.1.3 Topología en estrella (Star)

Para esta topología cada estación está conectada a un nodo central común, usualmente a través de dos enlaces punto a punto, uno para transmitir y otro para recibir (figura 10). Hay dos alternativas para que el nodo central funcione:

La primera es el funcionamiento en modo de difusión, en el que la transmisión de la trama por parte de una estación se retransmite sobre todos los enlaces de salida del nodo central. En este caso, aunque la disposición física de una estrella, lógicamente funciona como un bus. En tal caso al dispositivo central se le conoce como concentrador (hub).

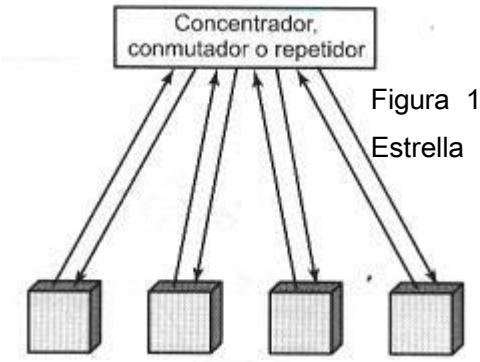


Figura 10. Estrella

La segunda es el funcionamiento del nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacena temporalmente en el nodo y se retransmite sobre un enlace de salida hacia la estación destino.

2.6.2 Ethernet IEEE 802.3

Sus principales características es que utiliza CSMA/CD como método acceso. También soporta velocidades de transmisión de datos de 10 Mbps. Aunque emplea una topología lógica de bus, puede utilizar topología física en bus o estrella. El medio de transmisión más empleado es el cable coaxial grueso de 50 Ohms con señalización de basebanda, sin embargo, existen especificaciones para otros medios de transmisión, las más comunes hoy en día son:

10Base T.- Utiliza topología en estrella, par trenzado no apantallado (UTP), la longitud de enlace se reduce a 100 mts, por lo que se puede utilizar un enlace de fibra óptica donde la longitud máxima es de 500 m.

10Base F.- Utiliza como medio la fibra óptica y una topología en estrella pasiva, para interconexión

de estaciones y repetidores con segmentos de hasta 1 km. de longitud.

2.6.3 Fast Ethernet

100Base T.- Es una red convencional ethernet conocida como 100Base T, sólo que con mayor rapidez, es decir la evolución de 10Base T con aumento en la velocidad de transmisión a 100 Mbps. Utiliza CSMA/CD y puede utilizar cable UTP de niveles 3, 4 y 5. Puede correr sobre la misma variedad de medios que 10Base T, incluyendo UTP, STP y fibra óptica.

100Base TX.- Para 2 pares de cable trenzado uno para transmisión y otro para recepción. Se permite UTP de categoría 5 y se usa el esquema de señalización MLT-3.

100Base T4.- Especifíca el uso de 4 líneas de par trenzado entre los nodos. Puede utilizar UTP de categoría 3, categoría 4 y además de UTP de categoría 5 de alta calidad.

100Base FX.- Utiliza 2 fibras ópticas una para enviar y otra para recibir, un uno binario se representa por un haz o pulso de luz, mientras que un cero binario es representado por la ausencia de pulso de luz ó uno de muy baja intensidad.

2.6.4 Token Ring IEEE 802.5

En coordinación con el estándar IEEE 802.5 utliza una topología logica de anillo pero físicamente utiliza topología en estrella. La velocidad de transmisión de datos es de 4 Mbps ó 16 Mbps y método de acceso Token Passing.

2.6.2 Métodos de Control de Acceso al Medio (MAC)

Las dos técnicas que se han adoptado en los diversos documentos de normas son el acceso múltiple por Detección de Portadora con Detección de Colisiones (CSMA/CD: Carrier-Sense Múltiple Access with Collision Detection) y Paso de Testigo (Token Passing) utilizada en una topología de anillo.

2.6.2.1 Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD)

Se usa ampliamente en las LANs en la subcapa MAC. En particular es la base de la popular LAN Ethernet.

Cuando una estación ha terminado de transmitir su trama cualquier otra estación que tenga una trama por enviar ahora puede intentar hacerlo. Si dos o más estaciones deciden transmitir en forma simultánea, habrá una colisión. Las colisiones pueden detectarse comparando la potencia o el ancho de pulso de la señal recibida con el de la señal transmitida.

Una vez que una estación detecta una colisión, aborta la transmisión, espera un tiempo aleatorio e intenta de nuevo, suponiendo que ninguna otra estación ha comenzado a transmitir durante este lapso. Por lo tanto, nuestro modelo de CSMA/CD consistirá en periodos alternantes de contención y transmisión, ocurriendo periodos de inactividad cuando todas las estaciones están en reposo (por ejemplo, por falta de trabajo).

El tiempo mínimo para detectar la colisión es sólo el tiempo que tarda la señal para propagarse de una estación a otra, por supuesto detecta la colisión casi de inmediato y se detiene, sin embargo la pequeña ráfaga de ruido causada por la colisión no regresa a la estación original, es decir en el peor de los casos una estación no puede estar segura de que ha tomado el canal hasta que ha transmitido durante algún tiempo sin detectar una colisión.

Es importante darse cuenta de que la detección de colisiones es un proceso analógico. El hardware de la estación debe escuchar el cable mientras transmite, si lo que lee es distinto de lo que puso en él, sabe que está ocurriendo una colisión. La implicación es que la codificación de la señal debe permitir que se detecten colisiones, por ejemplo una colisión de dos señales de 0 voltios bien podría ser imposible de detectar, por esta razón, se usa una codificación especial.

Vale la pena mencionar que una estación emisora debe monitorear de manera continua el canal en busca de ráfagas de ruido que puedan indicar una colisión. Por esta razón, CSMA/CD con un solo canal es inherentemente un sistema semidúplex. Es imposible que una estación transmita y reciba tramas al

mismo tiempo, debido a que la lógica de recepción está en uso, en busca de colisiones durante cada transmisión. Tenemos que hacer notar que ningún protocolo de subcapa MAC garantiza la entrega confiable, incluso en ausencia de colisiones, el receptor podría no haber copiado en forma correcta la trama por varias razones, por ejemplo falta de espacio de búfer o una interrupción no detectada.

Paso de Testigo (Token Passing)

El testigo (token) esta basado en el uso de una trama pequeña, que circula cuando todas las estaciones están libres. Es decir cuando una estación desea transmitir debe esperar a que le llegue el testigo, después toma el testigo cambiando uno de sus bits, lo que lo convierte en la secuencia de comienzo de las tramas de datos. Añade y trasmite el resto de campos requeridos en la construcción de la trama.

Una estación comienza a transmitir cuando toma el testigo, éste deja de estar presente en el anillo, de manera que el resto de las estaciones que deseen transmitir deben esperar. Se inicia una vuelta completa, la trama, al anillo y se absorbe en la estación transmisora, quien insertará un nuevo testigo en el anillo cuando se cumplan las siguientes condiciones:

- La trama ha sido transmitida por la estación.
- Cuando a la estación hayan vuelto los bits iniciales de la trama transmitida (después de una vuelta completa al anillo).

La ventaja principal del anillo con paso de testigo es el control de acceso flexible que ofrece. Es posible utilizar el anillo con paso de testigo para proporcionar prioridad y servicio con ancho de banda garantizado.

Por el contrario su mayor desventaja del anillo con paso de testigo es la necesidad de procedimientos para realizar el mantenimiento del anillo. Pues la pérdida del testigo impide posteriores utilizaciones del anillo, mientras que la duplicidad del mismo puede interrumpir también el funcionamiento del anillo. Se puede seleccionar una estación como monitora para asegurar que haya únicamente un

testigo con el anillo y para reinsertar un testigo libre en caso necesario. Cabe mencionar que Token ring utiliza como control de acceso al medio a Token Passing.

2.7 REDES DE ÁREA AMPLIA WAN

Cuando dos dispositivos se encuentran muy alejados no resulta productivo que se conecten directamente mediante un enlace punto a punto, o bien si existe la necesidad de conectarse entre ellos en instantes de tiempo diferente.

Una red WAN (Wide Area Network) es aquella que cubre una extensa área geográfica, requiriendo atravesar rutas de acceso público. Contiene un conjunto de máquinas diseñadas para programas (es decir, aplicaciones) de usuario, éstas máquinas son llamadas hosts.

Los clientes son quienes poseen a los hosts, es decir, las computadoras personales de los usuarios, mientras que, por lo general, las compañías telefónicas o los proveedores de servicios de Internet poseen y operan la subred de comunicación.

En la mayoría de las redes de área amplia la subred consta de dos componentes distintos: líneas de transmisión y elementos de conmutación.

Líneas de Transmisión

Mueven bits entre máquinas, pueden estar hechas de cable de cobre, fibra óptica o, incuso, radio enlaces.

Elementos de conmutación

Son computadoras especializadas que conectan tres o más líneas de transmisión. Cuando los datos llegan a una línea de entrada, el elemento de conmutación debe elegir una línea de salida en la cual reenviarlos. Estas computadoras de conmutación reciben varios nombres; switch y routers son los más comunes.

2.7.1 HDLC (High-Level Data Link Control)

Incluir en cada dispositivo de comunicación una capa de control que regule el flujo de información de punto a punto, además de detectar y controlar los errores, así como la posibilidad de regulación de la velocidad de datos por parte del receptor.

Este protocolo es el más importante para el control de enlace de datos, no sólo porque es ampliamente utilizado, si no también porque es la base de otros importantes protocolos de control de enlace, en los que se usan los mismos o similares formatos y los mismos procedimientos que los empleados por HDLC –Control del enlace de datos de alto nivel-.

Su funcionamiento consiste en intercambio de tramas-I, tramas-S y tramas-U entre dos estaciones.

Tramas-I: de Información transportan los datos generados por el usuario.

Tramas-S: de Supervisión: que proporcionan el mecanismo ARQ cuando no se usa la incorporación de las confirmaciones de las tramas de información.

Tramas-U: no numeradas proporcionan funciones complementarias para controlar el enlace.

2.7.2 Frame Relay

Frame Relay (Retransmisión de Tramas) se desarrollo teniendo presente que las velocidades de transmisión son mayores actualmente, así como las tasas de error menores. Las redes originales de conmutación de paquetes se diseñaron para ofrecer una velocidad de transmisión al usuario final de 64 kbps, las redes Frame Relay están diseñadas pra operar eficazmente a velocidades de transmisión de usuario de hasta 2 Mbps. El objetivo como se consiguen éstas velocidades está en eliminar la mayor parte de la información redundante usada para el control de errores, por consiguiente el procesamiento asociado.

La conmutación de paquetes surgió cuando los servicios de transmisión a larga distancia presentaban una tasa de error relativamente elevada, comparada con los servicios que actualmente se disponen. Posteriormente para compensar esos errores relativamente frecuentes, en los esquemas de conmutación de paquetes se realiza un esfuerzo considerable, que consiste en añadir información redundante en cada paquete, así como en la realización de un procesamiento extra, tanto en el destino final como en los nodos intermedios de conmutación, necesario para detectar los errores y ser corregidos.

2.7.3 ATM (Asynchronous Transfer Mode)

ATM (Modo de Transferencia Asincrono) en algunas ocasiones conocido como Retransmisión de Celdas, es la culminación de todos los desarrollos en conmutación de circuitos y conmutación de paquetes. Se considera como una evolución de la conmutación de circuitos: en donde se dispone de circuitos a velocidad fija de transmisión entre los sistemas finales.

ATM permite crear múltiples canales virtuales con velocidades de trasmisión que son definidas dinámicamente en el instante en que es definido el canal. El uso de celdas de tamaño fijo, es posible ofrecer velocidad constante en el canal.

La diferencia primordial entre Frame Relay y ATM es que la primera utiliza paquetes de longitud variable llamadas tramas, mientras que la segunda utiliza paquetes de longitud fija llamadas celdas. ATM de igual forma que Frame Relay introduce poca información adicional para el control de errores, confiando en la robustez del medio de transmisión, así como en la lógica adicional localizada en el sistema destino para detectar y corregir errores.

Al utilizar celdas, ATM reduce el esfuerzo adicional de procesamiento incluso todavía más que en Frame Relay. El resultado es que ATM se ha diseñado para trabajar a velocidades de transmisión del orden de 10 a 100 Mbps, e incluso del orden de Gbps.

Las Redes continuan evolucionado y en la actualidad no sólo se utilizan las tecnologías, los medios de transmisión, los estándares y los protocolos mencionadas en el capítulo. Anexados a éstos se encuentra la tecnología inálambrica que mencionaremos en el siguiente capítulo.

3.1 VISIÓN GENERA DE UNA RED LAN INALÁMBRICA (WIRELESS LAN)

Las tecnologías inalámbricas existen desde hace muchos años, TV por satélite, radio desde AM/FM, teléfonos celulares, dispositivos de control remoto, radares, sistemas de alarma, estaciones meteorológicas y teléfonos inalámbricos están integrados en nuestra vida diaria. Actualmente, las tecnologías inalámbricas son parte fundamental de los negocios y la vida personal.

Los distintos tipos de redes implican una conectividad física, sus ventajas son velocidad, fiabilidad y, hasta cierto punto la conveniencia. La conectividad física permite un incremento de la productividad al poder compartir impresoras, servidores y software. Sin embargo, los sistemas conectados en red requieren que la estación de trabajo permanezca en el sitio, permitiendo movimientos sólo dentro de los límites impuestos por el medio y la extensión de la oficina. Una red inalámbrica es un método alternativo para conectar una LAN. No necesita ligar ningún cable y puede trasladar fácilmente las computadoras.

Las señales inalámbricas son ondas electromagnéticas que pueden viajar por un medio como el aire. Por tanto, no se necesitan medios de cobre o fibra óptica para las señales inalámbricas. Esto hace de la comunicación inalámbrica una forma versátil de construir una red. Las transmisiones inalámbricas pueden cubrir grandes distancias utilizando señales de alta frecuencia. Cada señal utiliza una frecuencia diferente medida en hercios para que sean diferentes entre sí. Los fabricantes de WLANs migraron de la banda de 900MHz a la banda de 2.4. GHz para mejorar la velocidad de información. Este patrón continua al abrirse el estándar IEEE 802.11a en la banda de 5 GHz que promete muchas mejoras en velocidad.

3.1.1 Necesidades de WLAN

Al igual que una LAN, una WLAN debe cumplir un conjunto de necesidades específicas para entornos inalámbricos. Entre los requisitos más importantes se encuentran:

- Conexión a la LAN troncal.- El uso de módulos de control permite la conexión a una LAN troncal.

- Rendimiento.- Para maximizar el uso del medio inalámbrico, el control de acceso al medio deberá

hacer un uso eficiente del mismo.

- Número de Nodos.- Una red inalámbrica deberá dar soporte a cientos de nodos mediante el uso de varias celdas.

- Área de Servicio.- referida al área de cobertura de la red que tiene un diámetro típico entre 100 y 300 metros.

- Consumo de Energía.- Al usar adaptadores sin cable los usuarios móviles deberán garantizar una larga vida. Esto implica que sea inapropiado un control de acceso al medio (MAC) que requiera que los nodos móviles supervisen constantemente los puentos de acceso o realicen comunicaciones frecuentes con una estación base. Para reducir el consumo de potencia mientras no se esté usando la red, existe un modo de descanso en WLAN llamado (Sleep mode).

- Robustez en la transmisión y seguridad.- Si no existe un diseño apropiado una red inalámbrica está propensa a sufrir interferencias y escuchas. El diseño debe permitir transmisiones fiables incluso en entornos ruidosos ofreciendo un nivel de seguridad contra intrusos.

- Funcionamiento de redes adyacentes.-Si dos redes operan en la misma zona puede haber interferencia entre ellas, repercutiendo negativamente en el funcionamiento normal del algoritmo MAC permitiendo accesos no autorizados.

- Configuración Dinámica.- El direccionamiento MAC y gestión de la red LAN debería permitir la inserción, eliminación y trasalado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

- Traspasos (Handoff)/Itinerancia (Roaming).- El protocolo de control de acceso al medio debería permitir a las estaciones móviles desplazarse de una celda a otra.

- Licencia.- Un usuario preferirá adquirir y trabajar sobre una red inalámbrica que no precise de

una licencia para la banda de frecuencias usada por la red.

3.1.2 WECA (Wireless Ethernet Compatibility Alliance)

WECA es una organización en la que los principales proveedores de equipo y software inalámbrico están unidos con el propósito de garantizar la interoperabilidad de los productos Wi-Fi, además de promover a éste como estándar global para las redes locales inlámbricas en todos los mercados.

3.1.3 WiFi (Wireless Fidelity)

WiFi (Fidelidad Inalámbrica) es un término acuñado por la WECA donde los productos certificados por ésta organización operan entre sí como independencia del fabricante, es decir que un usuario que utiliza un producto WiFi puede utilizar un punto de acceso de cualquier marca con un cliente de hardware de cualquier otra marca, que haya sido diseñado para funcionar como WiFi. Éste acrónimo es comunmente llamado IEEE 802.11b así como Ethernet es utilizado en lugar de IEEE 802.3.

3.1.4 AP (Access Point)

Un AP (Punto de Acceso) se conecta a una LAN cableada a fin de proporcionar acceso a Internet y conectividad a la red cableada. Los AP están equipados con antenas y ofrecen conectividad inalámbrica sobre un área específica denominada celda.

Dependiendo de la composición estructural de la localización donde está instalado el AP y del tamaño y ganancia de la antena, el tamaño de la celda puede variar entre unas pocas decenas de metros y 40 kilómetros. Lo más frecuente es que el alcance esté entre 100 y 170 metros. Para dar servicio a grandes áreas, se pueden instalar varios AP con cierto grado de solapamiento, permitiendo el tránsito entre celdas,

Cuando un usuario esta dentro de una WLAN, inicia localizando un dispositivo compatible con el cual asociarse, este proceso de denomina escaneado y puede ser activo o pasivo.

El escaneado activo emite una solicitud de prueba para que sea enviada desde el nodo inalámbrico que pretende unir a la red. La solicitud de prueba contiene el SSID (Service Set Identifier) de la red a la que pretende unirse. Cuando se encuentra un AP con el mismo SSID, el AP emite una respuesta de prueba, completándose los pasos de autenticación y asociación.

Los nodos de escaneado pasivo escuchan en busca de tramas de administración de balizas (beacons), transmitidas por el AP (modo de infraestructura) o los nodos iguales (ad hoc). Cuando un nodo recibe una trama beacon que contiene el SSID de la red a la que intenta unirse, hay un intento de unirse a ella. El escaneado pasivo es un proceso contiguo y los nodos pueden asociarse o disociarse de los AP debido a cambios en la fuerza de la señal.

3.2 MEDIOS DE TRANSMISIÓN INALÁMBRICOS

Todas las LANS inalámbricas actuales se pueden clasificar de acuerdo a la técnica de transmisión usada.

a) LAN de Infrarrojo (IR, Infrared) es una categoría donde una celda individual esta limitada a una habitación, debido a que la luz infrarroja no es capaz de atravesar muros opacos.

b) LAN de Espectro Disperso hace uso del espectro disperso como tecnología de transmisión. La mayoría de las LAN funcionan en las bandas ISM (Industria Ciencia y Medicina), por lo que no se necesita una licencia FCC (Federal Communication Comission) para su utilización.

c) Microondas de banda estrecha, no utilizan el espectro disperso, operan en el rango de microondas. Existen productos que funcionan a frecuencias en las es necesaria una licencia FCC, mientras que otros lo hacen en la banda ISM.

3.2.1 Infrarrojos

Una serie de ventajas significativas que representa el uso de infrarrojos es que el espectro es virtualmente ilimitado, ofreciendo la posibilidad de alcanzar altas velocidades de datos. El espectro de infrarrojos no se encuentra regulado internacionalmente. Comparten también algunas propiedades con la luz visible haciendolos atractivos para el uso de ciertas configuraciones LAN.

Una luz infrarroja se refleja difusamente por los objetos de color, siendo así posible utilizar la reflexión producida en techo para proporcionar covertura a toda una habitación.

Una ventaja importante de la tecnología de infrarojos es que los equipos son relativamente baratos y simples, debido a que usan modulación en intensidad, los receptores IR Infrarrojos unicamente necesitan detectar la amplitud de las señales opticas.

Su principal desventaja es que muchos entornos de interior sufren una radiación infrarroja de fondo debida tanto a la luz natural como la artificial, obligando al uso de transmisores de alta potencia que limitan el alcance de la señal.

3.2.2 Bandas de Frecuencia

Las ondas de radiofrecuencia se utilizan ampliamente en muchas aplicaciones; entre ellas la difusión de radio, televisión y las redes de telefonía celular. Puesto que las ondas de radio se propagan fácilmente a través de objetos como paredes y puertas, se aplican controles muy estrictos al uso del espectro de radio. Además, la amplia gama de aplicaciones implica que el ancho de banda de radio es un recurso escaso. Para una aplicación en particular, es necesario que se asigne oficialmente una banda de frecuencia específica. En términos históricos, esto se ha hecho a nivel nacional, pero cada vez se están firmando más convenios internacionales que determinan bandas de frecuencia concretas para las aplicaciones que tienen alcance internacional.

La mayoría de las radiofrecuencias están autorizadas por las agencias gubernamentales, como la comisión federal para las comunicaciones (FCC, Federal Comunications Commission) en los Estados

Unidos, en México la COFETEL (Comisión Federal de Telecomunicaciones).

Las bandas de frecuencias sin licencia son más fáciles de implementar y suponen un ahorro de tiempo porque no requieren licencias. Hay tres bandas sin licencia

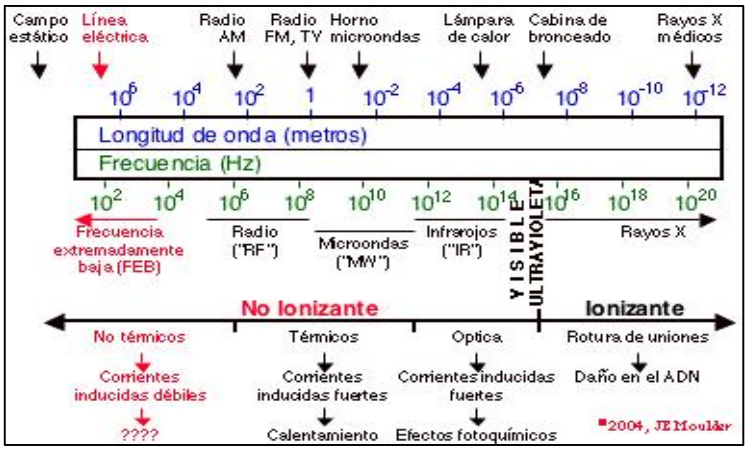


Figura 11 Espectro electromagnético

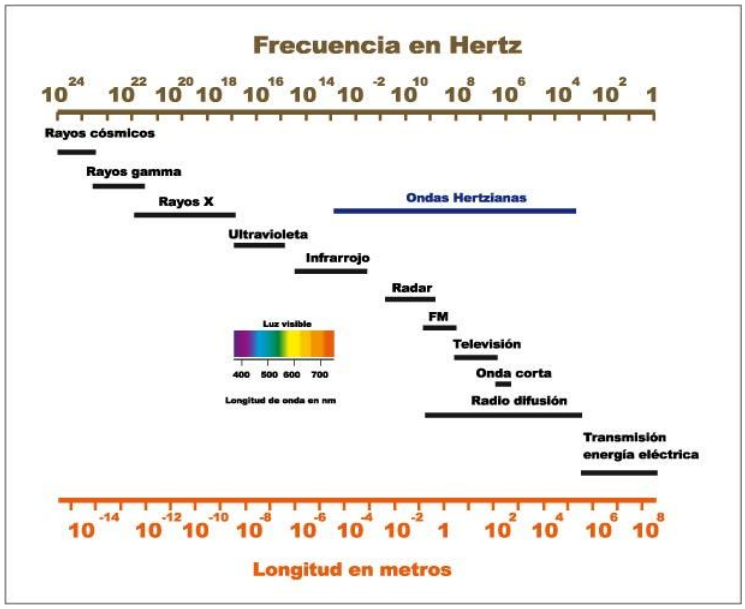


Figura 12. Espectro electromagnético 1

900 megahercios (MHz). La banda de 900 MHz es para los teléfonos inalámbricos y celulares.

2.4 gigarhercios (GHz). La norma 802.11b, la norma inalámbrica más extendida opera en la banda sin licencia de 2.4 GHz, entregando un ratio de datos máxima de 11Mbps

5 GHz. Recientemente la FCC abrió la banda de 5 GHz para uso sin licencia para dispositivos de comunicaciones de datos a altas velocidades. La norma 802.11a puede entregar un ratio de datos máximo de 54Mbps.

Existe una relación entre la frecuencia y la cantidad de datos que puede enviar. El concepto es parecido al de una tubería. Cuanto mas ancha es la banda, más frecuencias. Cuanto más ancho es el espectro mayor es el ratio de datos que puede transmitirse. La cantidad de espectro disponible determina la ratio de datos. Como la banda de 900 Mhz soporta teléfonos celulares y otros productos de consumidor, la banda esta superpoblada. Como resultado de ello, los usuarios a menudo experimentan interferencias o no pueden acceder a la red. La ventaja que ofrecen los 900 Mhz es un rango más amplio (para las mismas antenas de ganancia) que los de 2.4 Ghz. El inconveniente de los 900 Mhz es que la ratio de datos más fiable y rápida es solo la de 1mbps debido a lo limitado de su rango de frecuencias.

El rango de frecuencias de 2.4 GHz es más ancho que el de 900 MHz, lo que permite una ratios de datos más altas con un alcance fiable de hasta 40 km.

El rango de frecuencia de 5GHz permite una tasa de transferencia de datos más rápida debido a que su ancho de banda es mayor.

Con 5GHz será posible alcanzar tasas de datos mayores de 20 Mbps en este rango de frecuencias, sin embargo el inconveniente es su alcance limitado que en el interior es aproximadamente de 50 pies (17 metros) y en el exterior una limitación aproximada de 2500 pies (830 metros).

Para utilizar las bandas de radio sin licencia, tiene que utilizar las técnicas de espectro disperso. El espectro disperso del salto de frecuencia (FHSS, Frecuency Hopping Spread Spectrum) y el espectro disperso de secuencia directa (DSSS Direct Sequence Spread Spectrum) son dos formas de ejecutar un espectro disperso. Estas técnicas de espectro disperso diseminan la energía RF por la banda disponible.

La evolución recientemente publicada de la norma IEEE, 802.11b, proporciona para una tasa de datos de tipo Ethernet 11 Mbps sobre DSSS. La FHSS no soporta tasas de datos superiores a 2 Mb.

Como las señales de radio se debilitan a medida que las señales en el transmisor, el receptor también debe estar equipado con una antena. Cuando las ondas de radio inciden en una antena del receptor, las corrientes eléctricas débiles se generan en esa antena. Dichos corrientes, causados por las ondas de radio recibidas, son equivalentes a las corrientes que generaron originalmente las ondas de radio en la antena de transmisor. En un transmisor, la señales (datos) eléctricas de una computadora o una LAN no se envían directamente en la antena del transmisor. Más bien, esta señales de datos se utilizan para entregar una segunda señal fuerte denomina la señal portadora.

El receptor demodula la señal portadora que llega desde su antena e interpreta los cambios de fase de dicha señal y reconstruye la señal de datos eléctrica original a partir de ella.

3.2.3 Microondas Terrestres

El uso de enlaces terrestres de microondas para establecer enlaces de comunicación, cuando no resulta práctico o costeable instalar medios de transmisión físicos. Debido a que el haz de microondas colimado viaja a través de la atmósfera, puede sufrir perturbaciones por factores como construcciones o condiciones climáticas adversas. En cambio, con un enlace por satélite el principal medio de transmisión del haz es el espacio libre y por tanto es menos propenso a sufrir tales efectos. No obstante, la comunicación por microondas en línea recta a través de la atmósfera terrestre puede ser confiable hasta distancias de más de 50 kilómetros.

3.3 MÉTODOS DE CONTROL DE ACCESO AL MEDIO INALÁMBRICO

¿Cómo se comunican las LANS inalámbricas?

Después de establecer la conectividad con la WLAN, un nodo pasa por la trama de forma similar a cualquier otra red 802. Las WLAN no utilizan una trama 802.3 estándar. Por consiguiente, es engañoso utilizar el término Ethernet inalámbrico. Hay tres tipos de tramas: control, administración y datos. La siguiente lista enumera las tramas incluidas en cada tipo de trama:

- Tramas de administración
- Trama de solicitud de asociación
- Trama de solicitud de prueba
- Trama de respuesta de prueba
- Trama beacon
- Trama de autenticación
- Tramas de control
- Solicitud para enviar (RTS, Request To Send)
- Listo para enviar (CTS, Clear To Send)
- Acuse de recibo
- Tramas de datos

Solo la trama de datos es similar a las tramas 802.3. sin embargo, la sobrecarga de la tecnología inalámbrica y las tramas 802.3 es de 1500 bytes y una trama Ethernet no puede exceder 1518 bytes. Una trama inalámbrica puede llegar a 2346 bytes. Normalmente, el tamaño de la trama WLAN está limitada a 1518 bytes porque se conecta con más frecuencia en una red Ethernet cableada.

Como la RF es un medio compartido, se pueden producir colisiones. La diferencia significativa es que no hay un método por el que el nodo origen sea capaz de detectar que se ha producido una colisión. En vista de esto las WLAN utilizan un acceso múltiple de detección de portadora y anulación de colisión (CSMA/CA, Carrier Sense Múltiple Access Collision Avoidance). Esta característica es algo parecida al acceso múltiple con detección de portadora y detección de colisión (CSMA/CD, Carrier Sense Múltiple

Access Collision Detect) de Ethernet.

Cuando un nodo de origen envía una trama, el nodo receptor devuelve un acuse de recibido (ACK) positivo que puede provocar el consumo del 50% del ancho de banda disponible. Este consumo, en combinación con el coste que supone el protocolo de anulación de colisión, reduce la tasa de transferencia de datos un máximo de 5 a 5.5 Mbps en una LAN inalámbrica IEEE 802.11b cuya tasa es de hasta 11 Mbps.

El rendimiento de la red se ve afectado por la fuerza de la señal y la degradación de su calidad debida a la distancia o a las interferencias. A medida que la señal se hace más débil, puede invocarse una selección de tasa adaptativa (ARS) y la unidad de transmisión hará caer la tasa de datos desde 11 Mbps hasta 5.5 Mbps, desde 5.5 Mbps a 2 Mbps o desde 2 Mbps a 1 Mbps.

3.4 ESTÁNDAR INALÁMBRICO 802.11

En general los protocolos de la rama 802.x son un estándar de protocolo de comunicaciones de la IEEE, centrados en los dos niveles más bajos de la arquitectura OSI, especificando las normas de funcionamiento a esos niveles de las redes de área local, que definen la tecnología de redes locales, y en el caso que nos ocupa que es el de la 802.11, se define el uso de estos niveles en una WLAN.

El estándar original de este protocolo data de 1997, era el IEEE 802.11, tenía velocidades de 1 hasta 2 Mbps y trabajaba en la banda de frecuencia de 2,4 GHz. En la actualidad no se fabrican productos sobre este estándar. La siguiente modificación apareció en 1999 y es designada como IEEE 802.11b, esta especificación tenía velocidades de 5 hasta 11 Mbps, también trabajaba en la frecuencia de 2,4 GHz. También se realizo una especificación sobre una frecuencia de 5 Ghz que alcanzaba los 54 Mbps, era la 802.11a y resultaba incompatible con los productos de la B y por motivos técnicos casi no se desarrollaron productos. Posteriormente se incorporo un estándar a esa velocidad y compatible con el B que recibiría el

nombre 802.11g. En la actualidad la mayoría de productos son de la especificación B y de la G. (Actualmente se esta desarrollando la 802.11n que se espera que alcance los 500Mbps).

Éste estándar se sitúa en el espectro de frecuencias de radio comercial abierto al igual que otros muchos dispositivos, incluyendo bluetooth, los teléfonos inalámbricos. Debido a la interferencia que pueden ocasionar estos dispositivos, cuyo resultado es la disminución de flujo y la lentitud o ruptura de las conexiones.

3.4.1 802.11a

Esta especificación se encuentra en la banda de los 5 GHz y utiliza ocho canales de radio disponibles. En algunos países extranjeros, no obstante, es posible utilizar 12 canales. 802.11a permite una transmisión de hasta 54 Mbps por canal. El mayor ancho de transmisión disponible por usuario es la mitad de este valor aproximadamente, porque el ancho de banda se comparte entre varios usuarios, que normalmente están enviando datos por un canal de radio dado. Éste ancho de banda decrece proporcionalmente con la distancia, según aumenta ésta entre el usuario y el punto de acceso radio.

3.4.2 802.11b

Permite conexiones con tasas de transmisión de hasta 11Mbps en la banda de 2.4 GH. La especificación 802.11b utiliza sólo DSSS. Éste estándar fue inicialmente una mejora del 802.11 que se añadió en 1999 para permitir que la funcionalidad inalámbrica fuera análoga a las conexiones Ethernet cableadas.

3.4.3 802.11g

Es una extensión de IEEE 802.11b a mayor velocidad. Este esquema combina toda una gama de técnicas de codificación del medio físico utilizadas en 802.11ª y 802.11b para proporcionar servicio a diversas velocidades de datos.

Los estándares 802.11x inalámbricos no son compatibles entres si, además de mencionar que los dispositivos inalámbricos trabajan el la capa física, enlace de datos y de red.

3.5 ALGUNOS FACTORES DE SEGURIDAD

Garantizar la seguridad en una red inalámbrica consiste en aportar confianza suficiente para que los usuarios puedan acceder a la red, sin miedo de perder datos de misión crítica en las ondas o en l perímetro de la oficina.

Por lo que la seguridad se ocupa de garantizar que los curiosos no puedan leer o peor aún, modificar mensajes dirigidos a otros destinatarios, tiene que ver con gente que intenta acceder a servicios remotos no autorizados, se ocupa de mecanismos para verificar que los mensajes sean realmente enviados por quien firma.

Los accesos no autorizados a recursos de una red o una instalación física pueden ser de alto riesgo si se consigue acceder a un servidor con información no encriptada o si se consigue la destrucción de la información, por muy encriptada que esté, pues los ficheros críticos son susceptibles a ser destruidos, a pesar de estar encriptados.

Una LAN cableada puede ofrecer mayor seguridad que una WLAN porque físicamente está alojada en un edificio, mientras que una red inalámbrica dentro de un edificio no resulta protegida necesariamente de los accesos no autorizados si no se usa encriptación. WEP facilita la seguridad mediante la encriptación de los datos en las ondas de radio, con lo cual quedan protegidos en su transmisión de un punto a otro. Utilizando WEP en los segmentos de datos y en los niveles físicos no se consigue seguridad punto a punto.

3.5.1 Autenticación y Asociación

La autenticación WLAN tiene lugar en la capa 2 y es un proceso de autenticación del dispositivo no del usuario. Es importante recordar esto al considerar la seguridad WLAN, la resolución de problemas y la administración global.

La autenticación puede ser un proceso nulo, como en el caso de un AP (Access Point) y una tarjeta de red (NIC) nuevos con configuraciones predeterminadas. El cliente envía una trama de solicitud de autenticación al AP y este lo acepta o lo rechaza. El cliente recibe una notificación del curso de la acción a través de la trama de respuesta de autenticación, también podría configurarse el AP para pasar la tarea de autenticación a un servidor de autenticación, que ejecute un proceso credencial más completo.

La asociación, ejecutada después de la autenticación, es el estado que permite a un cliente utilizar los servicios de un AP para transferir datos.

Tipos de autenticación y asociación

Los tipos de autenticación y asociación son los siguientes:

Desautenticado y disociado. El nodo está desconectado de la red y no está asociado a un punto de acceso.

Autenticado y disociado. El nodo ha sido autenticado en la red aunque no asociado todavía en el punto de acceso.

Autenticado y asociado. El nodo está conectado a la red y listo para transmitir y recibir datos a través del punto de acceso.

Métodos de autenticación

La IEEE 802.11 enumera dos tipos de procesos de autenticación:

Sistema abierto. Este proceso es una norma de conectividad abierta en la que sólo debe coincidir el SSID. Puede utilizarse en un entorno seguro o no, aunque es bastante alta la posibilidad que un sniffer de red de bajo nivel determine el SSID de la WLAN.

Clave compartida. Este proceso requiere el uso del cifrado WEP (Wired Equivalent Privacy). La WEP es un algoritmo muy sencillo que utiliza claves de 64 y 128 bits. El AP está configurado con una clave de cifrado y los nodos que intentan acceder a la red a través del AP deben tener una clave coincidente. Las claves WEP estáticamente asignadas proporcionan un nivel de seguridad más alto que el sistema abierto, pero no son infalibles.

La susceptibilidad de desautorizar la entrada en las WLAN se controla mediante varias tecnologías de seguridad emergentes.

3.5.2 Seguridad mediante Encriptación

Un error en una WLAN es considerar a la seguridad como opcional. Al activar la seguridad en un dispositivo inalámbrico, se produce un cierto incremento de tráfico que reduce la velocidad media de la conexión porque se provoca un procesos de encriptación real en un extremo y un proceso de desencriptación real en el otro.

La mayoría de los routers inalámbricos permiten encriptación de 64 y 128 bits, con una clave de encriptación específica por usuario que altera los datos en función de la entrada. Este clave será necesaria en los puntos en que haya que descodificar los datos y devolverlos a un formato legible. Sin embargo, muchos usuarios mantienen desactivada esta opción y por lo tanto son vulnerables frente a cualquiera que intercepte el tráfico de la red o incluso la espíe.

3.5.2.1 WEP (Wired Encryption Privacy)

El estándar 802.11 establece un protocolo de seguridad en el nivel de capa de enlace de datos llamado WEP, diseñado para que la seguridad de una LAN inalámbrica sea tan buena como la de LAN cableada. Puesto que lo predeterminado para las LANs alámbricas no es la seguridad, este objetivo es fácil de alcanzar, y WEP lo consigue, como veremos más adelante.

Cuando se habilita la seguridad para el estándar 802.11, cada estación tiene una clave secreta que comparte con la estación base. La forma en que se distribuyen las claves no se especifica en el estándar. Éstas sólo pueden ser precargadas por el fabricante, pueden intercambiarse por adelantado a través de la red alámbrica. Por último, la estación base o la máquina del usuario puede tomar una clave aleatoria y enviársela al otro por aire encriptada con la clave pública del otro.

La encriptación WEB utiliza un cifrado de flujo en base en el algoritmo RC4, Éste fue diseñado por Ronald Rivest y se mantuvo en secreto hasta que fue filtrado y se publicó en Internet en 1994.

3.6 FUTURO DE LA REDES INALÁMBRICAS

Aunque existe la vulnerabilidad en la seguridad de una red inalámbrica, existen más ventajas en el uso de una WLAN en un entorno corporativo, en los que los dispositivos no desaparecerán en un futuro próximo del entorno IT de las organizaciones.

Debido a que no se puede garantizar una seguridad al 100%, se pueden adoptar las sencillas precauciones para identificar vulnerabilidades potenciales, tapar agujeros, y evitar que algún hacker corrompa los recursos. Pero si un intruso irrumple en una red, el mantenimiento de registros fiables es un método escelente de trazabilidad de esa actividad en una red, lo cual permite bloquear cualquier intento futuro.

Se deberá asegurar siempre un monitoreo de la red y de la actividad en tiempo real, estando pendientes de todos los registros y actividad de la red. El examinar los registros de actividad de la red, no sólo es posible detectar picos de actividad debido a usos anormales, también se puede buscar actividad hacking de bajo nivel, en la que éste pudiera intentar averiguar sobre la configuración, para posteriormente filtrase y no disparar posibles alarmas que hubieran podido ser configuradas en el sistema.

Respecto a la evolución de las LANs Inalámbricas, indudablemente mejorarán muchísimo en términos de velocidad, de utilización y de seguridad con el paso del tiempo. Los mecanismos de autenticación son sólo el comienzo del bloqueo de una WLAN para poder así controlar el acceso a cualquier recurso de la red.

Es importante tener presente que con un poco de prevención, es suficiente para preveer daños en la red inalámbrica antes de que ocurran. Se debe vigilar toda actividad sospechosa y asegurarse de informar a los usuarios de que permanezcan atentos sobre quiénes acceden a la red y qué usuarios específicos tengan accesos selectivo a los recursos. Por último enfatizar que si se monitorea una red y se vigilan todas las conexiones inalámbricas, se podrá estar seguro de que se está ofreciendo un nivel de seguridad suficiente para asegurar un uso dedicado de la red manteniéndola al margen de problemas.

En el siguiente capítulo con la ayuda de un software de monitoreo ejecutado en una de las salas inalámbricas, detectaremos las deficiencias y aciertos en los procesos de transmisión de la información sobre la red

Se tomará como muestra la sala ubicada en “el Departamento” donde ya se imparten cursos de computación a distacia y presencial, así como video conferencias.

3.7 Wi-MAX

Wi-Max (World Wide Interoperability for Microwave Access). - Interoperabilidad Mundial para el Acceso por Microondas es una tecnología inalámbrica basada en estándares que ofrece conectividad de banda ancha y alta velocidad.

Su alcance teórico es de 50 Km. y está probado en enlace de punto a punto en Nueva Zelanda. Wi-Max parte de Wi Fi, brindando más bondades en cobertura, calidad de servicio y seguridad.

Considerando que el 3% de los hogares cuenta con Internet de banda ancha, existiendo así un 97% del mercado por explotar con Wi-Max, que es más barata y fácil de implementar, por ello es considerado un parteaguas en las comunicaciones. En Wi-Max está la fuerza de la convergencia, porque el acceso móvil y fija se da a través de un sólo acceso.

Hace dos años, se anunció formalmente el Wi-Max, pero fue hasta abril de 2005 que se liberó el primer producto de Intel basado en el estándar, llamado PRO/Wireless 5116.

Wi-Max tiene mayor oportunidad en los mercados emergentes, justamente en países donde la infraestructura no está al 100% o no llega a todos lados. Para quienes no tienen infraestructura de cobre o de fibra, actualmente éste estándar fijo ofrece una solución alterna para llegar a las casas y empresas; inclusive, para los que ya tienen fibra, puede funcionar a manera de respaldo en aplicaciones de misión crítica.

Un ejemplo de Wi-Max actual que tiene una ventaja en México es el concepto e-Go, el cual abrió un mercado desde hace dos años y que lo ha ido educando al punto que ahora tiene un conocimiento previo y, por tanto, exige la tecnología. e-Go es un concepto de Internet inalámbrico de banda ancha que ofrece MVS, fue le primer servicio en el mundo considerado Pre-Wi-MAX. Trabaja en un espectro licenciado sobre frecuencias de 2.5 a 2.7 GHz, las cuales usan sin problemas de interferencia.

Actualmente México cuenta con suficiente infraestructura de postes y cables en los que los operadores como Alestra, Avantel, Telmex y Metronet, entre otros, pagaron; Asimismo, invirtieron en una

concesión muy cara, por lo que el problema para masificar es comercial. El objetivo será llegar a acuerdos que permitan por ejemplo a un ejecutivo que habla vía celular dejar de usar el tiempo aire de su teléfono, mientras se acerca a su edificio Web por el área Wi-Max continuando con su llamada sin que él sienta la diferencia.

Los beneficios más visibles para los usuarios es que podrán conseguir más opciones de acceso de banda ancha. Mientras que para los operadores habrá múltiples proveedores lo que los llevará a un menor riesgo al invertir, también podrán llenar los vacíos para acceso de banda ancha en residencial y negocio. Respecto a los fabricantes de equipo sólo se requerirá el desarrollo de piezas elementales de la solución, así como una innovación más rápida. Por último los fabricantes de componentes tendrán una oportunidad de volumen para los proveedores de silicio.

4.1 INTRODUCCIÓN

En el siguiente capítulo y con la ayuda de un software comercial de monitoreo ejecutado en una de las salas inlámbricas, detectaremos variables de rendimiento, asi como deficiencias y aciertos en los porcesos de transmisión de la información sobre una de las salas inalámbricas ubicadas en “El departartamento”.

Se tomarán muestras en los tiempos en que se esta utilizando la sala elegida, serán un intervalo por la mañana. Apartir de las muestras obtenidas y de ser filtradas para posteriormente generar los datos requeridos se trataran con una hoja de cálculo. Generaremos tablas, graficaremos e identicaremos las variables propuestas. Finalmente haremos algunas conclusiones preliminares correspondientes a éste capítulo.

4.1.2 Descripción

La Institución (antes del proyecto) contaba con dos salas de Capacitación internas ubicadas en “El departamento”. En ellas se imparten cursos de tecnología de la información de forma presencial, así como servicios de educación y capacitación a distancia.

Videoconferencia[1] es un recurso que también es utilizado para la educación a distancia operada por “El departamento”. Mediante el cuál se pretende impulsar el uso de las nuevas tecnologías de la información en sus diferentes modalidades.

[1] Videoconferencia es la combinación de dispositivos electrónicos y de comunicación para transmisión y recepción simultánea de audio, video y datos en tiempo real.

Aprovechando éste recurso en la actualización profesional del personal de “La Institución”, en la promoción, divulgación y actualización de tecnologías se pretende estar a la vanguardia en el área de informática.

Un factor en éste proyecto es el fomento al desarrollo de la conferencia como medio de comunicación y modalidad educativa, teniendo como reto la difusión remota en tiempo real que ofrece ésta tecnología y sus consecuentes ventajas con respecto a otros medios.

La red está basada en el conjunto de protocolos TCP/IP a través de la que se ofrecen servicios como HTTP, FTP, SMTP, POP3.

Respecto al sistema operativo utilizado en todos los nodos de las dos salas es Windows XP versión profesional.

La sala núm. **1** ya existente tiene un perímetro de 10m.X5m., es decir un área de 50m^2, además de los siguientes elementos:

1 Televisor.
1 Convertidor de VGA a RCA.
18 Computadoras Personales.
18 Tarjetas de Red.
1 Impresora Láser.

Mientras que la sala núm. **2** tiene un perímetro de 10m.X4m. equivalente a una área de 40m^2. Con los siguientes elementos:

1 Pantalla Transmisora.
Equipo de Videoconferencia[2]

[2] Compuesto por CODEC (codificador y decodificador), monitor (es), cámara(s), micrófono(s) y bocinas.

20 Computadoras Personales.

20 Tarjetas de Red.

1 Impresora Láser.

4.1.3 Topología Anterior

La red de las 2 salas del "Departamento" es representada en el siguiente diagrama:

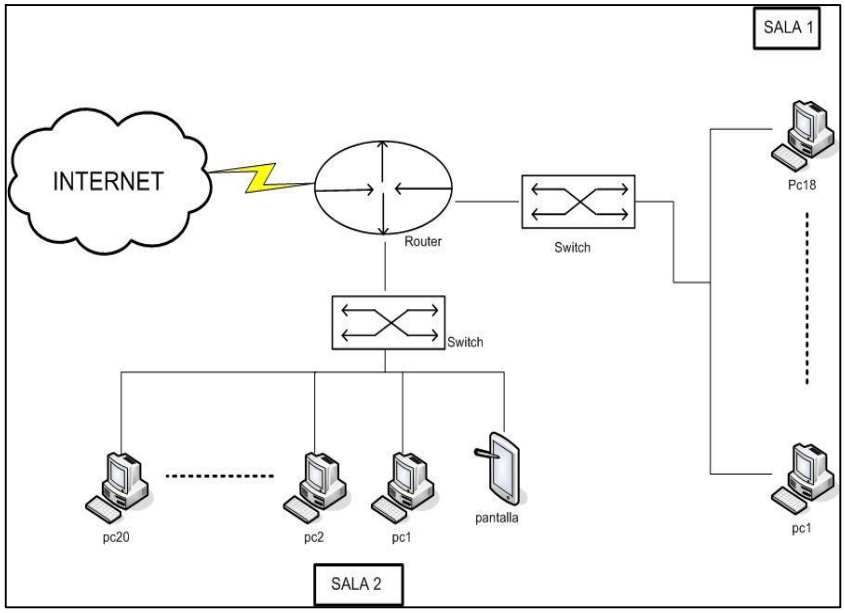


Figura 13. Diagrama de red de las dos salas

Direcciones de Red de **Subred** correspondiente a las dos salas:

Dirección de Red 10.55.2.0
Dirección de Broadcast *10.55.2.255*
Máscara de subred..... *255.255.255.0*
Rango de IP's..... ***10.55.2.1 - 10.55.2.39***

Tabla 1. Rango de IP's internas.

4.1.4. Problemas

La sala 2 utilizada para Videoconferencia lo es de igual forma para impartir cursos de capacitación presencial del "Departamento" además de ser la única sala para éste fin.

Debido a lo anterior y a la demanda del personal de la institución que asiste a capacitación, además del traslado en distancias y el costo en tiempo, se propuso como solución alternativa cursos a distancia de punto a punto o multipunto (un profesor puede verse mediante video grabado o en vivo), donde los asistentes podrán tomar su clase desde su lugar de trabajo ó bien desde una sala de capacitación (si el alumno no cuenta con equipo de cómputo personal). Generando así un proyecto de licitación directa a una empresa específica donde se solicitarán equipos de cómputo y telecomunicaciones necesarios para poner en marcha cursos a distancia y de igual forma presencial en las aulas de nueva apertura.

4.2 DISEÑO

El proyecto contempla 6 salas que se ubicarán en el Distrito Federal:

Ubicación
- 1 Sala en el norte
- 3 En el Sur
- 2 En el centro

Cada una de ellas proveerá los siguientes servicios:

→ Videoconferencias a nivel Institucional.
→ Cursos de capacitación en distintos niveles y a diferentes áreas educativas.

→ Capacitación del personal en forma presencial.
→ Capacitación a distancia a través de cursos en línea.
→ Uso de Internet.
→ Descarga de archivos vía FTP y/o Internet.
→ Kioscos♦ como valor agregado para los participantes a los cursos.

El diseño e implementación serán establecidos al igual que el funcionamiento de cada una de las salas. Es decir que la licitación convocada será de *Diseño / construcción o Llave en Mano.* Bajo este método, se selecciona una firma para diseñar y construir el proyecto y luego entregárselo al dueño del proyecto al completar el diseño e implementación (literalmente, "llave en mano") por un costo fijo o por un costo más una cantidad, con un monto máximo. Las ventajas de diseño/ construcción incluyen tiempo ahorrado en la secuencia, el proceso en etapas de diseño-licitación, construcción y las reducciones en las acciones legales buscando poner la responsabilidad por omisión de diseño o fallas de construcción en todas las personas (porque uno solo es responsable por todos los aspectos del desarrollo).

Es así como "El departamento" postula las necesidades y los parámetros tecnológicos requeridos. Ver apéndice A.

Las consideraciones de instalación y conexión se encuentran expresas en el manifiesto de la Junta de Aclaraciones de "La Institución" del año 2004

Después de la instalación de los equipos de cómputo, equipo de videoconferencia, audio e iluminación realizada por la empresa contratada, mostramos el diagrama general de las salas inalámbricas:

♦ Los Kioscos son un número determinado de equipo en cierta sala que es de uso común para los participantes, en las que podrán practicar y realizar tareas del curso que hayan tomado.

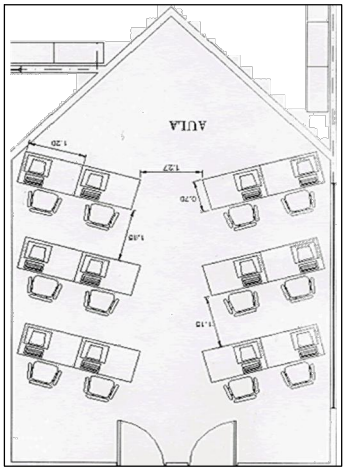


Figura 14. Diagrama general de las salas inalámbricas

4.2.1 Diagrama de Red

El diseño de red mostrado a continuación de las 6 nuevas salas, tiene salida a internet de manera independiente, es decir que se ha contratado a un proveedor quien proporcionará éste servicio.

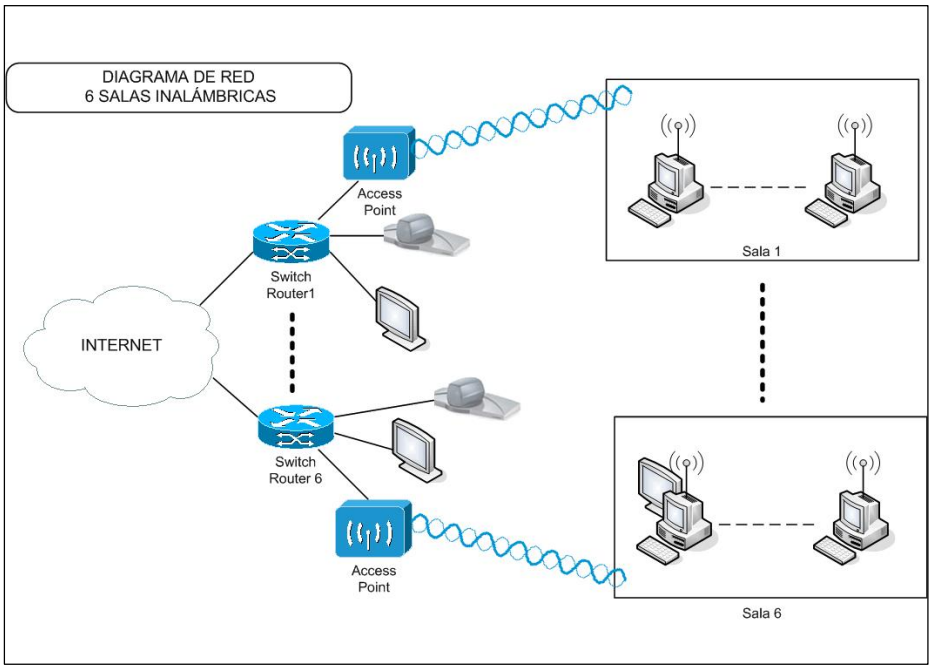


Figura 15. Diagrama de Red correspondiente a 6 salas en "La Institución".

4.2.2 Direccionamiento Lógico

Respecto a la dirección lógica que será utilizada para cada una de las salas ha sido segmentada por "El departamento" quien utilizará las siguientes direcciones:

Con dirección de Red Clase C segmentada
Broadcast *10.55.3.255*
Máscara.....*255.255.255.0*
IP's.....***10.55.3.1 - 10.55.1.254***

Tabla 2. Direcciones lógicas de cada sala.

Cabe señalar que sólo se liberaran 30 direcciones ip's debido a la seguridad.

4.2.3 Plano General de Salas

Mostramos el plano de una de las salas implementada, los restantes se muestran en el apéndice B.

En el plano podemos observar cómo serán ubicados el equipo de video conferencia, audio e ilumación dentro de cada recinto. Los planos se encuentran en el apéndice B.

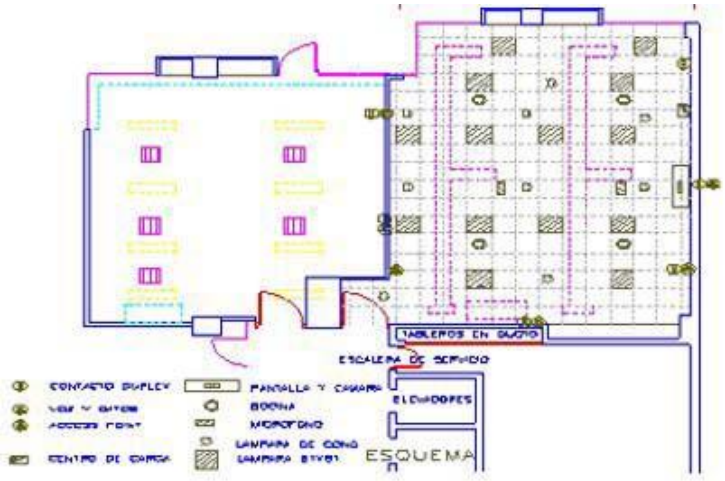


Figura 16. Esquema de una de las salas

4.2.4 Características Técnicas de Entrega

Para las salas nuevas de capacitación se contratan 6 enlaces ADSL con un proveedor de servicios de Telefónicos y de Internet. Cada sala tendrá su salida independiente a internet. Los componentes y servicios entregados por "El proveedor" en la licitación cumple los requerimientos establecidos en el diseño prouesto por "La Institución". A continuación describiremos las características entregadas por "El proveedor" teniendo de antemano que ha cumplido los requerimientos. Las marcas utilizadas por el proveedor son acuerdos que él tiene con las marcas.

Componentes PARA CADA SALA:

1 Pantalla de alta definición.
1 Codec.
1 Access Point.
16 Computadoras.
16 Tarjetas de red.

Equipo de Audio .
Sistema de bocinas y microfono en plafon.
Sistema Electrico.
Sistema de Iluminación.

Donde:

Pantalla de alta definición. Pantalla /televisor de proyección LCD 60" preparado para la alta definición marca SONY modelo kdf-60wf655.

equipo de Videoconferencia 128kbps IP marca Tandberg modelo 770MXP. Videocodec con cámara inter construida con multiplexor inverso integrado. El sistema cuenta con un control remoto inalámbrico, mando a distancia y menús en pantalla,

Access Point Airport Extreme- WiFi certificado para 802.11g con un alcance de 50pies de la estación a cada dispositivo a 54 Mbps y 150 pies a 11 Mbps. Frecuencia de 2.4 ghz. Potencia de radio de 15dBm

computadoras de marca con procesador Intel Pentium 4 a 3.2 Ghz con tecnología Hyper Threading, memoria RAM 512MB, Disco duro de 60GB. Pantalla TFT matriz activa.

16 tarjetas de red inalámbricas.

Equipo de Audio . Amplificador de audio
Sistema de bocinas y microfono en plafon.

Sistema Electrico.

Sistema de Iluminación.

4.2.5 Pruebas Aplicadas

Las pruebas realizadas en las salas de capacitación son de suma importancia debido a que las muestras registradas nos permitirán mejorar los servicios ofrecidos y comprobar si la decisión de adquirir una red inalámbrica se verá no sólo redituada en el aspecto económico, si no también en el desempeño de red.

Detectar el comportamiento de los protocolos, como el conjunto de TCP/IP, los servicios de transmisión de datos, acceso de archivos vía Internet y vía FTP facilitará la visión que hemos planteado en el capítulo 1. Observar en donde se pueden mejorar los servicios a partir de las variables observadas es uno de los objetivos a cumplir.

Para realizar las mediciones de monitoreo se tomo en cuenta que el horario en donde se tiene mayor accesos a la red es de 10 a 14h. aproximadamente, tomando como muestra una computadora, donde se instaló un software de monitoreo comercial.

Se obtuvo por cada horario de monitoreo –mostrado en la tabla siguiente- archivos con una duración aproximada de 20 a 30 min. Éste rango fue variable debido a la capacidad de la sala y la disposición de equipo.

Horario

Día 1	Día 2	Día 3	Día 4
10:40 archivo 1	09:20 archivo 5	10:07 archivo 10	11:11 archivo 12
11:19	09:56	10:59	11:55
13:03	10:42		12:46
13:37	11:35		13:18
	12:35		14:03 archivo 16

Tabla 3.Horario de inicio en la toma de muestras

Es entonces que se tiene 16 archivos dando un total 7.5h de muestreo total en cuatro días, a lo que:

7.5 h X 60 min./h = 450 min. de muestreo total.

Si el software de monitoreo tomó una muestra cada 10 seg. tenemos un total de:

[6muestras por minuto] x [450 min. de muestreo total]= **2700 muestras durante 7.5h de monitoreo.**

Los 17 archivos obtenidos por el software son mostrados en el apéndice C y mostramos uno de ellos:

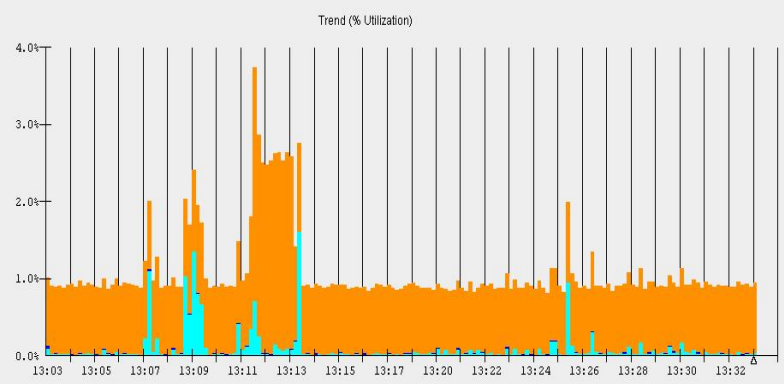


Figura 17. Gráfica de muestreo del software “Network Analyzer”, software utilizado en la toma de muestras.

Con este número de muestras obtenidas generamos y analizamos las siguientes variables importantes:

4.2.5.1 Porcentaje de Utilización

El porcentaje de utilización es una medida del promedio del tiempo en el que la red es usada para transmitir y recibir datos. Por consiguiente es una variable estadística importante que indica cuanto ancho de banda es usado de la red. Un alto porcentaje de utilización indica un nivel de tráfico excesivo.

Evidentemente que en una misma red Ethernet al haber muchas computadoras tratando de enviar datos al mismo tiempo y/o al haber una transferencia masiva de datos se crea un gran porcentaje de colisiones y utilización. Si rebasa del 1% de colisiones y/o 15% de utilización de cable ya se dice que la red está saturada. Además, las señales de este tipo de red tienden a degradarse con la distancia debido a la resistencia, la capacidad u otros factores. Inclusive la señal todavía se puede distorsionar por las interferencias eléctricas exteriores generadas por los motores, las luces fluorescentes y otros dispositivos eléctricos.

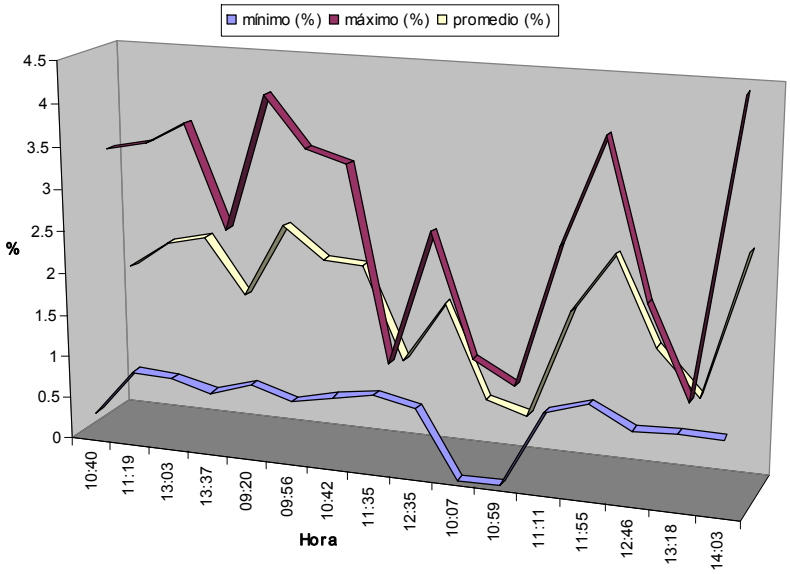
Es entonces que la definición podemos es generada de la siguiente forma:

Cálculo del % de Utilización= (Número de bits medidos en 1 segundo/ Tasa máxima por segundo) * 100

En la siguiente tabla se observan las siguientes variables:

- % Utilización mínima
- % Utilización promedio
- % Utilización máxima

	Día 1				Día 2					Día 3		Día 4				
Hora	10:40	11:19	13:03	13:37	09:20	09:56	10:42	11:35	12:35	10:07	10:59	11:11	11:55	12:46	13:18	14:03
mínimo (%)	0.28	0.84	0.81	0.69	0.85	0.7	0.8	0.89	0.78	0	0	0.91	1.06	0.82	0.84	0.84
máximo (%)	3.36	3.47	3.73	2.52	4.13	3.55	3.41	1.11	2.71	1.27	1.01	2.68	3.95	2.12	1.05	4.5
promedio (%)	1.82	2.155	2.27	1.605	2.49	2.125	2.105	1	1.745	0.635	0.505	1.795	2.505	1.47	0.945	2.67



Se han generado los valores para las variables que mencionamos , teniendo entonces en el eje de las x la hora en que fueron tomadas y en el eje de las y el valor en % partiendo de 0-100%. Para cada horario de monitoreo –archivo obtenido por el software, se obtiene le máximo, mínimo y por consiguiente el promedio.

Observemos que nunca rebasa el 5% del ancho de banda de la red (el valor máximo obtenido fue de 4.5% a las 14:03), esto quiere decir que no estuvo, en los tiempos de monitoreo, saturada. También observamos que el en porcentaje mínimo de utilización fue de "0" a las 11:11 y a las 10:59, momentos en lo que ningún dato era enviado, probablemente porque se perdiera la conexión o bien por que los equipos no realizaran ningún acceso a la red.

4.2.5.2 Distribución de protocolos

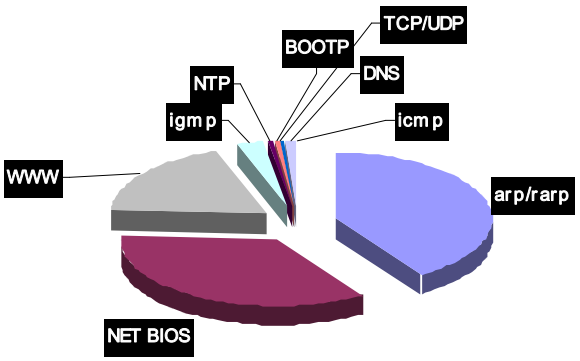
Las tablas *siguientes* representan el número de frames que han sido enviados desde que la medición inicio.

Para cada renglón se indica el nombre del protocolo, así como la suma de los frames enviados. Mostrando al final de la tabla una suma total del los frames enviados por protocolo, así como la suma total de éstos.

Así mismo la segunda *gráfica* muestra "otros" protocolos que el software considera importantes pero que no corresponden a la suite de IP.

IP	FRAMES																TOTAL FRAMES X PROTOCOLO
	10:40	11:19	13:03	13:37	09:20	09:56	10:42	11:35	12:35	10:07	10:59	11:11	11:55	12:46	13:18	14:03	
arp/rarp	2012	2103	1927	1634	3598	3953	3070	2627	2690	943	152	3846	2937	4038	3535	3347	*42412*
NET BIOS 137-139	695	937	526	492	20595	1514	3658	1118	882	250	56	1730	883	1753	707	924	*36720*
WWW (http) 80	661	560	2943	0	12	131	0	17	1388	0	0	2919	7315	406	0	2800	*19152*
igmp 2	220	226	209	190	193	233	224	201	191	47	17	221	139	236	201	182	*2930*
NTP 123	53	57	59	50	48	58	57	58	58	17	2	24	17	20	19	18	*615*
BOOTP 67,68	13	50	10	10	29	43	29	23	15	8	2	53	52	77	10	15	*439*
TCP/UDP 427	8	37	14	25	24	4	36	2	8	0	1	24	29	32	11	7	*262*
DNS 53	187	32	51	160	70	97	162	21	52	6	1	161	12	79	14	100	*1205*
icmp 1	11	5	2	3	0	0	1	0	1	0	0	2	0	6	8	35	*74*
																	103809

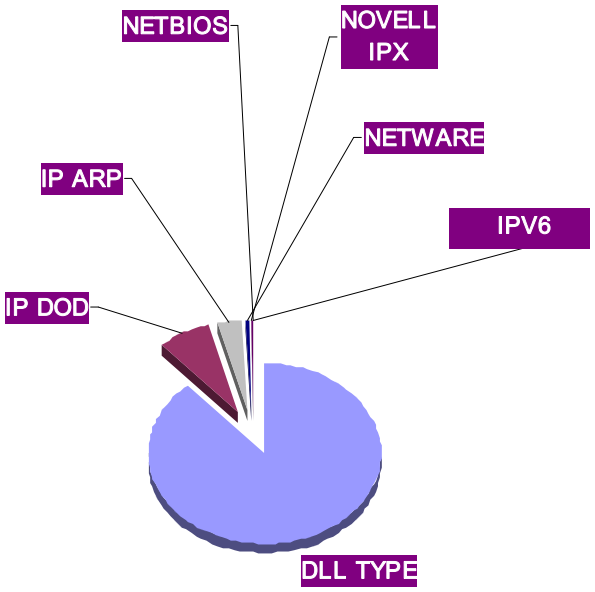
TOTAL FRAMES X PROTOCOLO	IP
42412	arp/rarp
36720	NET BIOS 137-139
19152	WWW (http) 80
2930	igmp 2
615	NTP 123
439	BOOTP 67,68
262	TCP/UDP 427
1205	DNS 53
74	icmp 1
103809	



El software de monitoreo arrojo también variables que hemos desglosado en la siguiente tabla, los comentarios correspondientes a el análisis los realizamos al final de éste capítulo donde realizamos algunas conclusiones.

	10:40	11:19	13:03	13:37	09:20	09:56	10:42	11:35	12:35	10:07	10:59	11:11	11:55	12:46	13:18	14:03	
OTHERS	**FRAMES**																***TOTAL FRAMES X PROTOCOLO***
DLL TYPE 8868	72276	76087	81337	76964	61987	87103	90472	76416	75119	18320	3094	75582	83846	74806	74730	74481	*1102620*
IP DOD 0800	2682	2501	4205	1176	42802	2451	6546	1732	2823	540	101	5582	8747	3200	1224	4149	*90461*
IP ARP 0806	2015	2103	1927	1634	3598	3953	3070	2627	2690	943	152	3846	2937	4038	3535	3347	*42415*
NETWARE IPX E0		417	413	356	325		344	427	420	146	11	378	291	437	350	316	*4631*
NOVELL IPX 8137		292	286	234	199	348	228	299	290	76	10	292	229	302	252	237	*3574*
NETBIOS F0		149	125	39	36	35	45	39	45	17	0	20	15	56	22	36	*679*
IPV6 86DD		34	23	16	102	1	32	5	0	2	6	44	17	69	0	0	*351*
																	1244731

TOTAL FRAMES X PROTOCOLO	OTHERS
1102620	DLL TYPE 8868
90461	IP DOD 0800
42415	IP ARP 0806
4631	NETWARE IPX E0
3574	NOVELL IPX 8137
679	NETBIOS F0
351	IPV6 86DD
1244731	



4.2.5.3 Toptalkers

Ésta tercera gráfica muestra las direcciones IP que han enviado el mayor número de información desde comenzó la medición. Es decir que por cada medición hecha se representa a las 5 IP's que envían un mayor número de bytes por cada horario –archivo – generado por el software. Partiendo de la tabla anterior se genera una final donde se muestras las 3 IP's que tienen mayor envío de bytes desde el nodo.

Tabla.-Toptalkers por Día

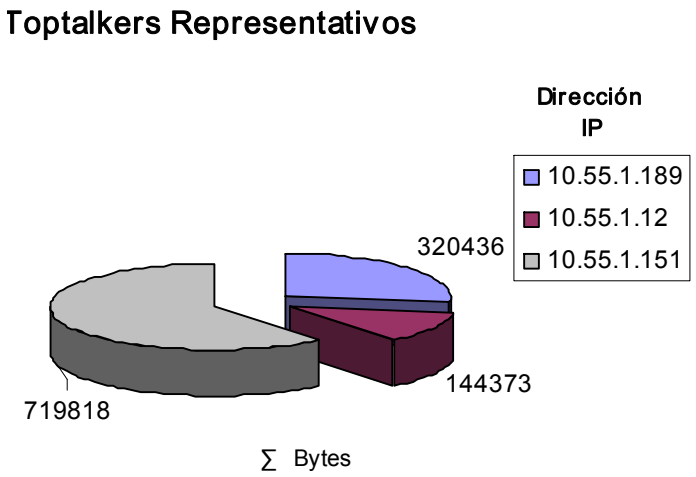
Día 1	
Dirección IP	10:40:00 a.m.
10.55.1.189	34228
10.55.151	17981
207.46.107.148	13251
10.55.112	10126
10.55.1.176	7721
	11:19:00 a.m.
10.55.1.189	31023
10.55.1.112	29424
207.46.108.139	19459
10.55.1.151	16758
207.46.107.148	10657
	01:03:00 p.m.
161.165.194.41	257555
10.55.1.151	37676
10.55.1.97	14960
207.46.107.148	7898
10.55.1.2	5848
	01:37:00 p.m.
10.55.1.112	17665
10.55.1.151	10163
10.55.1.120	9133
10.55.1.213	6296
10.55.1.2	5712

Día 2	
IP	09:20:00 a.m.
10.55.1.189	58926
10.55.1.212	31043
192..168.0.1	24509
10.55.1.75	23339
10.55.1.170	21324
	09:56:00 a.m.
10.55.1.75	98069
10.55.1.189	31495
10.55.1.170	18671
10.55.1.175	12085
10.55.1.151	11821
	10:42:00 a.m.
10.55.1.189	35398
10.55.1.123	23873
10.55.1.192	23172
10.55.1.170	16466
10.55.1.112	16067
	11:35:00 a.m.
10.55.1.170	21634
10.55.1.75	16847
10.55.1.105	16082
10.55.1.123	14978
10.55.1.189	14878
	12:35:00 p.m.
10.55.1.151	23947
10.55.1.170	21128
10.55.1.133	16922
216.92.154.20	8476
10.55.1.192	6825

Día 3	
IP	10:07:00 a.m.
10.55.1.98	104449
10.55.1.178	4894
10.55.1.151	3652
10.55.1.129	2022
10.55.1.2	1700
	10:59:00 a.m.
10.55.1.112	32920
10.55.1.9	1848
10.55.1.151	1605
10.55.1.198	1000
10.55.1.123	786

Día 4	
IP	11:11:00 a.m.
218.213.254.29	46969
10.55.1.189	34475
10.55.1.97	29450
10.55.1.242	28603
10.55.1.123	25657
	11:55:00 a.m.
218.213.254.29	7684342
10.55.1.151	536975
10.55.1.189	35398
10.55.1.196	18662
10.55.1.112	18581
	12:46:00 p.m.
10.55.1.189	44615
10.55.1.85	36120
10.55.1.9	28008
10.55.1.112	19590
10.55.1.151	16073
	01:18:00 p.m.
10.55.1.9	16530
207.46.106.13	10906
10.55.1.172	10688
10.55.1.232	8659
10.55.1.151	8343
	14:03
199.181.132.141	59412
65.54.194.118	36590
10.55.1.151	34824
10.55.1.9	20508
199.181.132.79	18860

Dirección IP	Bytes (go from node)															
	Día 1				Día 2					Día 3		Día 4				
	10:40	11:19	13:03	13:37	09:20	09:56	10:42	11:35	12:35	10:07	10:59	11:11	11:55	12:46	13:18	14:03
10.55.1.189	34228	31023			58926	31495	35398	14878				34475	35398	44615		
10.55.1.12	10126	29424		17665			16067				32920		18581	19590		
10.55.1.151	17981	16758	37676	10163		11821			23947	3652	1605		536975	16073	8343	34824



4.2.6 Algunas Conclusiones de las Pruebas Aplicadas

Observamos que respecto a la Distribución de protocolos los cataloga como IP porque es la manera abreviada de referirse a TCP/IP, y los protocolos que son de TCP/IP o IP son: NTP, igmp, BOOTP, TCP, UDP, DNS,icmp, arp/rarp y www (http).

NETBIOS es un protocolo de Windows fue creado por IBM y Microsoft como un protocolo de red sencillo y fácil de instalar, su información no puede ser ruteada, a diferencia de IP. Éste protocolo lo observamos como uno de los más utilizados en nuestro monitoreo y pertenece a la capa de sesión,

antecedido por arp/arp protocolos también utilizados en el nivel de red, el protocolo ARP (Address Resolution Protocol) es el encargado de relacionar una dirección MAC on una dirección IP.

Los otros (“others”, representados en una de las gráficas) son protocolos diferentes a TCP/IP aunque inclusive lo ponen también, protocolos de red: NETWARE/NOVELL/IPX (Netware también es una suite, IPX es parte de ella), NETBIOS (Windows), IPV6, e IP ARP son frames de ARP y no direcciones clase A, aunque la red es clase A. IP D (DOD) son simplemente frames de TCP/IP no multicast. DLL type se refieran a archivo DLL.

La gráfica 3 del documento, toptalkers, se refiere a los nodos que mas trafico generan los cuales son clase A 10.55.x.x pertenecientes a la red interna.

Las definiciones formales de los protocolos anteriormente mencionados se encuentran en el apéndice D

INTRODUCCIÓN

En este capítulo evaluaremos dos posbles situaciones para ıa ınstalación de las salas, es decir que haremos cálculos de inversión, propuestos a un tiempo de recuperación y denominaremos Proyecto A y Proyecto B, los cuales serán comparados y evaluados:

Proyecto aula cableada (proyecto A)
Proyecto de aula Inalámbrica (proyecto B)

Un instrumento de evaluación es el que analiza la diferencia porcentual entre ambos proyectos ya que esto determina cuál proyecto es más viable según la inversión que se desea realizar.

Por ende se elige el proyecto en el que se realiza una inversión menor, siempre y cuando cumpla con la calidad, servicio, parámetros tecnológicos y otros requerimientos. Para ello se utiliza la siguiente fórmula:

Diferencia Porcentual entre Proyectos = Proyecto de Mayor Inversión / Proyecto de Menor Inversión

Existen además otros instrumentos de evaluación de proyectos de inversión. Los más sencillos, tales como período de recuperación (Payout Time), período de recuperación descontado (Discount Payout Time DPT), tasa de rendimiento promedio (Average Return Rate ARR) y similares, los cuáles no toman en cuenta que un peso hoy es preferible a un peso mañana, particularmente en economías sujetas a inflación. Por esa razón utilizaremos solamente dos procedimientos que sí traen los flujos futuros a valor presente.

1. VPN: Valor Presente Neto

2. TIR: Tasa Interna de Rendimiento

3. K: Costo de Capital

1. VPN

$$VPN = \frac{\sum F\$n}{(1+K)^n} - Io$$

Donde:

F$n: Flujos de efectivo esperados

K: Costo de Capital, Tasa de interés

n: No. Periodos

Io: Inversión Inicial para el Proyecto

2. TIR es la tasa donde VPN=0

$$VPN = \left[\frac{\sum F\$n}{(1+K)^n} - Io = 0 \right]$$

3. TIR = K (Costo de Capital, Tasa de interés)

Para realizar este análisis necesitamos establecer los siguientes supuestos:

- Considerar que las 6 Salas con 16 nodos (CPUS) se rentarán tal como sucedería con un café Internet.
- Se rentan cada CPU por 8 hrs. al Día
- Se considera una renta por CPU de $10.00 pesos la h.
- Los sueldos y gastos fijos ascienden a $ 10,000.00 pesos mensuales
- El costo variable (CV) es el servicio de Internet por mes. El CV se estima en $ 500

INVERSIÓN SALA CABLEADA

Precios Unitario x Nodo		SIN IVA
Tarjeta de red	$	434.78
Cableado por cada nodo*	$	1,331.52
Switch de 24 nodos	$	17,391.30
Total x Nodo	**$**	**19,157.61**

Precios x 1 sala C/ 16 Nodos		
Tarjetas de red	$	6,956.52
Cableado de nodos	$	21,304.35
Switch de 24 nodos	$	17,391.30
Inversión Total x 1 sala C/ 16 Nodos	**$**	**45,652.17**

Proyecto 6 salas		
Inversión Total del Proyecto	**$**	**273,913.04**
IVA	$	41,086.96
Inversión Total del Proyecto	**$**	**315,000.00**

*En el apéndice D se muestra una tabla detallada del material empleado para cablear 16 nodos.

INVERSIÓN SALA INALÁMBRICA

Precios Unitario		
Tarjeta de red inalámbrica	$	1,200.00
Access Point	$	2,189.00
Nodo para el access point	$	1,331.52
Total unitario	**$**	**4,720.52**

Precios x 1 sala C/ 16 Computadoras		
Tarjetas de red inalámbricas	$	19,200.00
Access Point	$	2,189.00
Nodo para el access point	$	1,331.52
Total de inversión x 1 sala	**$**	**22,720.52**

Proyecto 6 salas		
Inversión Total del Proyecto	**$**	**136,323.13**
IVA	$	20,448.47
Inversión Total del Proyecto	**$**	**156,771.60**

RESUMEN DE INVERSIÓN		
Proyecto 6 Salas Cabledas C/16 Nodos C/U	**$**	**315,000.00**
Proyecto 6 Salas Inalámbricas C/16 Computadoras C/U	**$**	**156,771.60**
Diferencia Porcentual %		**2.01**

Análisis: La dif. porcentual 2.01% hace referencia a la relación entre el proyecto de inversión A vs B Este porcentaje representa que un nodo de red inalámbrica requiere la mitad de inversión a diferencia un nodo de red cableada normalmente.

EVALUACIÓN DE PROYECTOS DE INVERSIÓN

Supuestos:

Se rentan cada CPU por 6 Hrs al Día
Se considera una renta por CPU de $10.00 pesos la Hra.
Los sueldos y gastos fijos ascienden a $ 10,000.00 pesos
El costo variable es el servicio de internet por mes
El CV se estima en $ 500.00

Variables		
Inversión Proyecto A	$	315,000.00
Inversión Proyecto B	$	156,771.60
No. de Salas		6
No. de Nodos		16
Renta x hora	$	10.00
Horas		6
Días		240
CV (mensual)	$	500.00
CF (mensual)	$	10,000.00
Impuestos		40%

Estructura Financiera (anual)	
Ventas	1,382,400.00
Costos Variables	6,000.00
Costos Fijos	$ 120,000.00
Utilidad de Operaci	1,256,400.00
Impuestos	502,560.00
Utilidad Neta	**$ 753,840.00**

(FLUJO DE EFECTIVO)

Instrumento de Evaluación

Una vez que se obtiene los flujos de efectivo podrá calcularse mediante la siguiente fórmula el Valor Presente Neto de ambos proyectos de inversión.

VPN

$$VPN = \frac{SUM\ F\$D}{(1+K)\ n}$$

VPN	**Valor Presente Neto**
F$D	**Valor presente de los Flujos Futuros**
K	**Costo de Capital , Inflación o tasa de Interés**
n	**No. De Periodo**

Supuestos	
n	3 años
K	8%
F$D	Incremento 10% x año

Se considera el mismo Costo de Capital por 3 años y un Flujo de de efectivo que aumenta año con año en un 10 %,

PROYECTO A (CABLEADA)			
PERIODOS	FLUJOS EFECTIVO	K	Sum .F$D
0	-$ 315,000.00		-$ 315,000.00
1	$ 753,840.00	1.08	698000.00
2	829,224.00	1.17	710925.93
3	912,146.40	1.26	724091.22
VPN			**$ 1,818,017.15**

PROYECTO B (INALÁMBRICA)			
PERIODOS	FLUJOS EFECTIVO	K	Sum .F$D
0	-$ 156,771.60		-$ 156,771.60
1	$ 753,840.00	1.08	698000.00
2	$ 829,224.00	1.17	710925.93
3	$ 912,146.40	1.26	724091.22
VPN			**$ 1,976,245.55**

COMPARATIVOS

Análisis VAN:

Conviene el proyecto B ya que se recupera en menor tiempo la inversión inicial, promoviendo un flujo de efectivo mayor, desde el primer año y mucho mayor al termino de los 3 años.

PROYECTO A	
TASA TIR (Tasa Interna de Retorno)	**139%**

PROYECTO B
381%

ANÁLISIS:

Calculando la TIR hasta el periodo No. 1, se observa que conviene en gran medida el proyecto B ya que TASA TIR ES MAYOR QUE LA TASA TIR DEL PROYECTO A. En resumen al ser menor la inversión inicial del proyecto B, os flujos de efectivo subsecuentes son mayores en comparación con los del Proyecto A, dando como resultado un menor periodo de recuperación en el Proyecto B.

CONCLUSIONES

Partiendo de las pruebas realizadas, así como sus correspondientes gráficas, análisis financiero de ambos escenarios (cableada e inalámbrica) con el presente trabajo podemos concluir que tal modo de comunicación permitirá tener acceso a una red desde cualquier dispositivo o aparato en un periodo no muy lejano y que ambos escenarios que aunque diferentes en costo económico ofrecen las mismas variables a analizar.

Pero sabemos que las redes inalámbricas, por definición son abiertas y pueden ser atacadas; el número de ataques (conscientes de la vulnerabilidad existente) sin encriptación, es una clara invitación a los intrusos para escuchar o colarse en la red, con la ventaja de no encontrar ningún tipo de autenticación de sesión, permitiéndoles el acceso a la misma. Es por lo anterior que el nivel de encriptación más básico actualmente previene el saqueo de los recursos, motivando siempre a buscar y utilizar nuevos mecanismos de defensas y de control de intrusos no sólo en una red cableada comúnmente, si no que también en los medios ya explorados como una red inalámbrica.

Es por ellos que revisar periódicamente la vulnerabilidad y los recursos de la WLAN, como mecanismos de control para asegurarse de su integridad podrán potencialmente evitar daños en su disponibilidad. Los estándares se han incrementado en la variable velocidad pero conscientes de los niveles de seguridad en la transmisión de datos, deberán resolverse para que los intrusos no tengan el acceso a la información de los usuarios, podemos concluir que siempre serán un modo vulnerable del acceso a intrusos a redes cableadas e inalámbricas. Retos que seguirán dando pie a nuevas e innovadoras tecnologías en seguridad de la información.

También como parte de las conclusiones podemos afirmar que la apertura de las nuevas salas instaladas, con tecnología actual, en el área metropolitana, permite un mejor desempeño y rendimiento en las tareas ejecutadas por personal de “El departamento” y como consiguiente el de “La Institución”. Debido a que el traslado del personal para capacitación permitirá una mejora en el rendimiento de las labores de los mismos. Así como una capacitación constante a distancia como variable incremental.

La selección de una tecnología inalámbrica, como vanguardia a lo ya establecido comúnmente en el área de telecomunicaciones, demuestra que los ahorros obtenidos no son sólo económicos, como se mostró en el análisis financiero, si no que permitió ahorro en tiempos y en esfuerzos de instalación y habilitación de los servicios de Internet.

Observamos que la toma de muestras nos facilitó los mecanismos para concluir que la red no contiene saturación en el envío y recepción de paquetes, debido a que se observó un bajo porcentaje de utilización siempre menor a un 4.5% respecto al ancho de banda. Dándonos entonces un promedio general de 1.74% en la utilización. Respecto a la siguiente variable de medición observamos que el número de frames recibidos siempre es mayor a los enviados y que los tres protocolos más demandados –en el apéndice D se muestran con mayor detalle- correspondientes a la suite IP:

NetBios (protocolo de Windows) correspondiente a la capa de sesión que provee servicios de nombres, paquetes y sesión., ARP es un protocolo que funciona para encontrar la MAC de un Nodo si tienes su IP y RARP es para obtener la IP de un nodo, si tienes su MAC y HTTP (WWW) correspondiente al envío de peticiones para acceder a una página Web.

La dirección IP que más envía datos en la red es la 10.551.189, seguida por la 10.55.1.2 y finalmente la 10.55.1.151, usuarios que comúnmente tienen accesos a Internet, descarga de archivos o visitas a lugares donde se requiere un tiempo de acceso mayor al común.

Observamos que la parte financiera apoya la propuesta inicialmente en la que se postula un bajo costo en la inversión WLAN respecto a la comúnmente cableada. En resumen al ser menor la inversión inicial del proyecto B, los flujos de efectivo subsecuentes son mayores en comparación con los del Proyecto A (139 %), dando como resultado un menor periodo de recuperación en el primer año del Proyecto B (381%).

Finalmente el proyecto realizado por la institución ofrece servicios de educación a distancia, permitiéndole rentabilidad en tiempo y en convergencia con la tecnología de redes inalámbricas.

Dicho argumento nos permite formular que los avances en tecnología y en educación son variables que abren paso a nuevas consideraciones en la decisión de mejoras de lo ya implementado por La Institución.

Algunas de las variables que siempre deberán ser consideradas por los administradores y en general por el personal encargado de un centro de cómputo con servicio de red son la seguridad, la interferencia, el ancho de banda y otros factores externos que bloqueen la transmisión de señales.

Es por ello que en actualidad considerar la tecnología inalámbrica como solución a implementaciones con movilidad es sólo el inicio de una brecha ya disparada por un sueño sin cables.

APÉNDICE A.- Descripción de equipos adquiridos

CANT.	DESCRIPCIÓN
6	**PANTALLA** de proyección de 60 pulgadas con tecnología de cristal líquido (LCD) de alta definición. Interfases: entrada de componente DVD y HD, entrada de S-video, entrada de A/V, entrada para memory stick mejorada. Con índice de canal desplazable, potencia de audio de 15Wx2 altavoces, control remoto, cables de datos, audio, poder y video en RCA.
6	EQUIPO DE VIDEOCONFERENCIA Equipo de videoconferencia 128kbps ISDN/768kbps IP. Con fuente de alimentación de autosensado. Con cámara angular, panorámica con inclinación +15grados/-20grados, balance de blancos, control de cámara remoto. Videocodec con cámara con multiplexor inverso integrado, con puerto Ethernet 10/100 base-T, PCMCIA 802.11b hasta 11Mbit con soporte de encriptación WEP de 64 a 128bits. Que cumpla con los estándares: ITU H.320 hasta una velocidad de transmisión de 128kbps. Con al menos 15 cuadros por segundo desde 56-128kbps y 30 cuadros por segundo de 168kbps en adelante. ITU H.323 con hasta una velocidad de transmisión de 768kbps y 15 cuadros por segundo (fps) desde 56-128kbps y 30 fps de 168 en adelante. Características de red que debe soportar:

	Marcación automática H.320/H323, multiplexor inverso de software, encriptación de llamadas en ISDN e IP. Soporte de traducción de direcciones de red (NAT). Con manejo adaptativo de ancho de banda, manejo automático de Gatekeepers y sincronía de labios automático, recuperación de paquetes perdidos, H.245 e indicador de conflicto de direcciones IP. Características de video que debe soportar: los estándares ITU para las normas de video H.261, H.263+, H263++ (Natural video), H.264. Características de audio que debe soportar: estándar de la ITU G.711, G722, G.722.1, G728, MPEG4 AAC-LD. Con medidores de nivel de sonido, reducción de sonido automático, mezclador de audio, VCR ducking (reducción de audio de una reproducción de video ya sea en VCR o DVD automática cando alguien habla por el micrófono). Salidas de audio RCA, PHONO, MONO/ETEREO o análogo Soporte del estándar de software de la ITU T.120 con soporte streaming compatible con cisco IP/TV, Apple Quick Time, real placer. Con soporte estándar T.140 para Chat/closed captioning. Interfases: H.320, H.323. Que cuente con resoluciones de video XGA, SVGA, VGA, con soporte NTSC, natural video. Con entradas y salidas de video RCA, phono y compuesto con soporte NTSC, PAL, VGA, SVGA y XGA. Que cuente con accesorios: control remoto inalámbrico, mando a distancia y sistema de menús en la pantalla, selección de idioma. En la administración del sistema deberá soportar Managment Suite, administración mediante ser9rvidor de Web, SNMP, Telnet, FTP, XML y SOAP. Que cuente con niveles de

	seguridad como Https, IP password, código de acceso para marcación.
96	COMPUTADORA PERSONAL Computadora personal con procesador Intel® Pentium® IV o superior. Memoria RAM 512 MB mínimo Disco Duro de 60 GB o superior. Que cuente con unidad de CD, MODEM, tarjeta de red WIFI, tarjeta de video de 64MB o superior, entrada para micrófono, audífonos, puerto LAN RJ-45, puerto MODEM RJ-11, puerto paralelo. Pantalla LCD con soporte WXGA Con licencia de Sistema operativo.
6	ACCESS POINT Access Point con velocidad de transmisión de datos hasta 54 Mbps o superior compatible con WiFi 802.11b (11Mbps), que cuente con soporte para MAC y PC. Alcance ideal de 50pies de la estación a cada dispositivo de 54 Mbps ó 150pies a 11Mbps Con puerto WAN, LAN. Con un soporte de 30 ó 40 usuarios. Seguridad WEP con soporte de 40 ó 128bits de encriptación, NAT Firewall, soporte de autentificación RADIUS. Compatible con la especificación IEEE 802.11g y certificación Wi-Fi, IEEE 802.3,

	TCP/IP, NAT, DHCP, UDP, FTP, DNS, SNMP, Telnet.
6	SWITCH con 24 puertos LAN RJ-45 con auto negociación 10/100 Mbps, full/half duplex, con soporte para 802.1Q VLAN, priorizaciòn del trafico basado en 802.1p CoS, clasificación de paquetes Multi-Layer, con crecimiento para apilar otros switches mediante puerto especial resistente a fallos, con administración del trafico y con soporte para montaje sobre rack. Que soporte el estándar SNMP.
6	SISTEMA DE AUDIO Amplificador de Audio y dos pares de bocinas de plafón. Características: amplificador análogo de 6 canales, decodificación de 6.1 canales, Dobly Digital EX, DTS, Entrada Análoga de 5.1 canales, entrada frontal tipo RCA para audio/video, Entrada Óptica Digitalx 3 y Salida x1, entrada coaxial Digital x 2. Selector de altavoces, control remoto Bocinas: sistema de bocinas de plafón de 100 watts con respuesta de frecuencia de 75 Hz, con Woofer, frecuencia Crossover.
6	PIZARRON O PINTARRON BLANCO para plumón de agua 1.2 de alto x 2.40 de largo
6	TABLET PC Computadora tipo Tablet PC con Pentium III, 256 Mb en memoria RAM expandible, Disco Duro ATA de 30 GB, pantalla TFT de alta Luminiscencia de 12.1 pulgadas con resolución XGA soportando resoluciones de 640x480, 800x600 y 1024x768. Tarjeta de vides AGP 4x, puerto de Red, con tarjeta inalámbrica, puertos: FireWire, 2-USB, audífono, micrófono, puerto VGA, conector para estación “docking”.

12	MICROFONO DE TECHO Y PLAFON Micrófono de techo con sensitividad de circuito abierto, con nivel de ruido equivalente a 20 dBmin., SPL máximo a 3% THD, switch de selector de frecuencia para respuesta plana y creciente.

Respecto a la instalación se tiene:

CANT.	DESCRIPCION
6	INSTALACION DE EQUIPOS

TODOS LOS EQUIPOS, PLAFON E INSTALACIÒN ELECTRICA SERÁN INSTALADOS BAJO EL SIGUIENTE FORMATO:

Servicio de demolición de plafón falso a base de trablaroca, incluyendo retiro de canal de amarre, así como acopio de material producto de demolición dentro de la obra.

Servicio de desmontaje de lámparas empotrar existentes, incluyendo desmontaje de balastra y desmonte de instalación eléctrica existente.

Servicio de apertura de hueco para lámpara circular tipo downlight de 20cm. Aproximadamente.

Servicio, suministro y colocación de plafón falso color blanco, incluyendo alambre galvanizado para colgante, anclaje a losa.

Aplicación de pintura vinílica en muros y mano de sellador con 155 m^2 máximo.

Salidas de centro con tubo Conduit, pared delgada de 13mm de diámetro y cable thw cat. 12 y 14 antiflama.

Suministro y colocación de los centros de carga, salidas eléctricas, circuitos de alimentación de contactos y alumbrado

Nota: Las especificaciones de medidas se encuentran en los planos proporcionados por "El departamento"

CABLEADO DE NODOS DE RED

Cableado de nodos de red distribuidos.

UBICACIÒN Y CONEXIÓN DE LOS COMPONENTES

El espacio donde se instalará es de 7x10m y uno de los lados de 7m. se identificará como "frente", mientras que al otro lado 7m. será identificado como "parte posterior" y los dos de 10m. "lados".

El equipo de videoconferencia se colocará al frente del lugar, encima de la pantalla. Ubicación de micrófonos de techo: uno al frente a la altura del ponente (30 a 40 cms. hacia atrás de su posición) y el siguiente a la mitad de la sala (3.5 mts. Aprox.)

Las bocinas de plafón quedarán ubicadas en los extremos fuera de la cobertura central de los micrófonos de techo.

El Access Point se deberá fijar en la parte superior de la pared, al frente, fijándolo de tal forma que no se pueda remover fácilmente para evitar su pérdida.

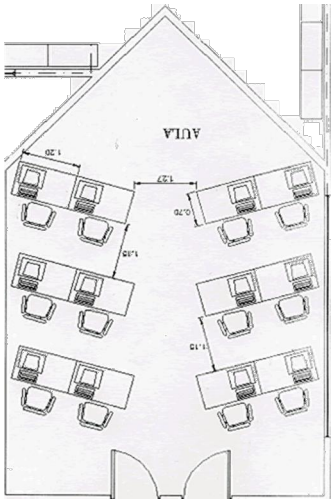
El switch se fijará dentro del gabinete.

El sistema de audio se colocará en el interior de la base de la pantalla.

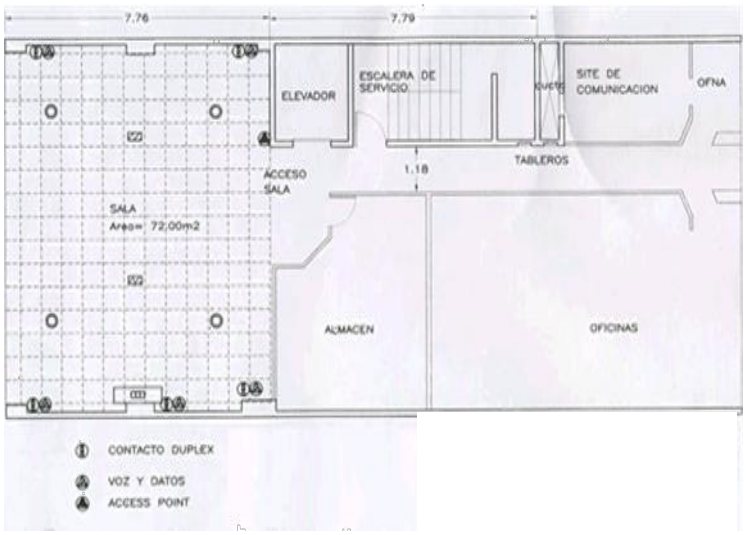
El pizarrón en la pared del lado derecho.

APÉNDICE B.- Esquemas y planos de salas inalámbricas

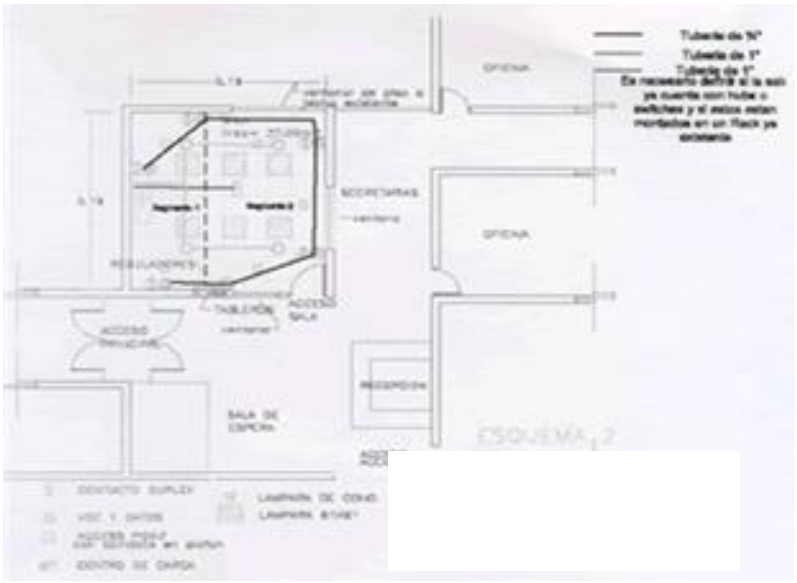
Esquema general de las aulas de Capacitación:



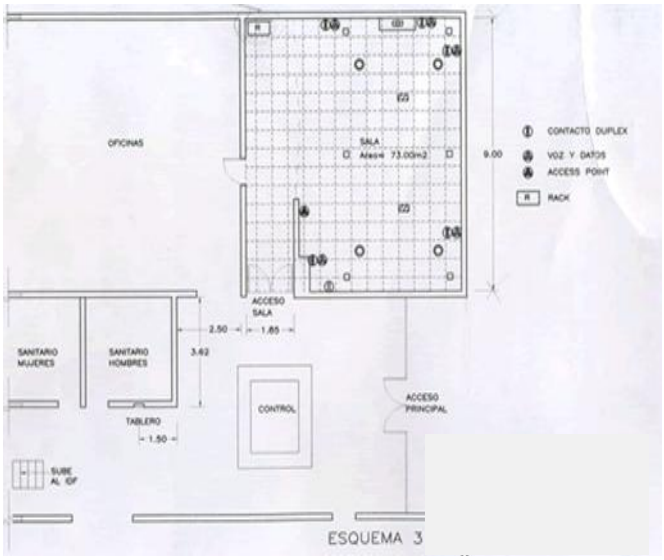
Plano Sala 1



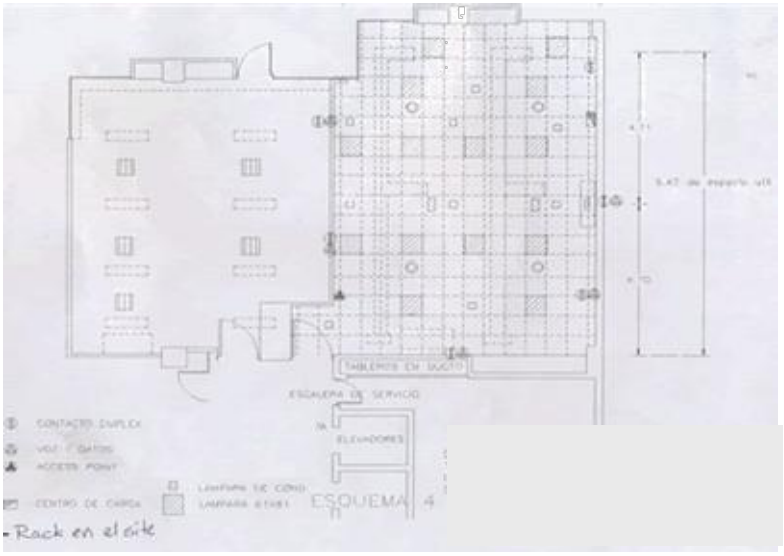
Plano Sala 2



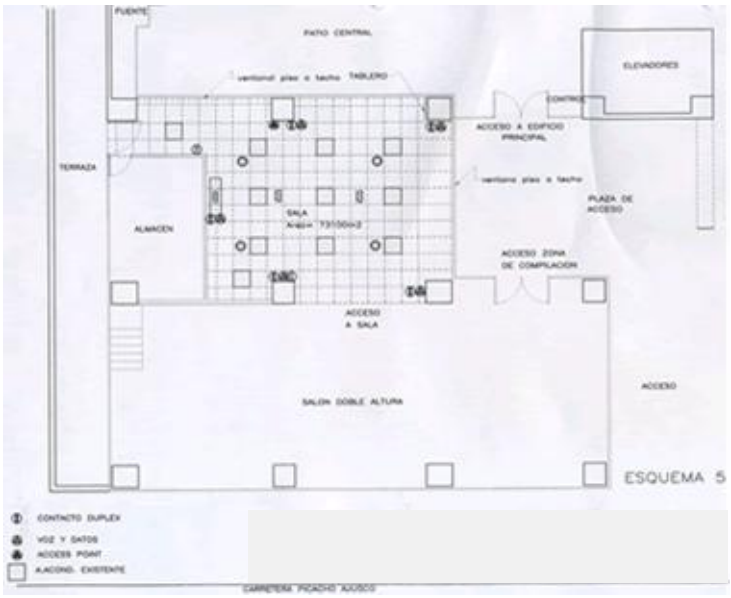
Plano Sala 3



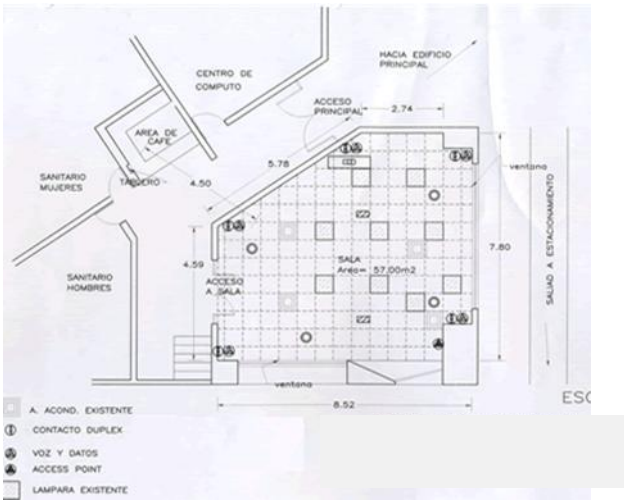
Plano Sala 4



Plano Sala 5



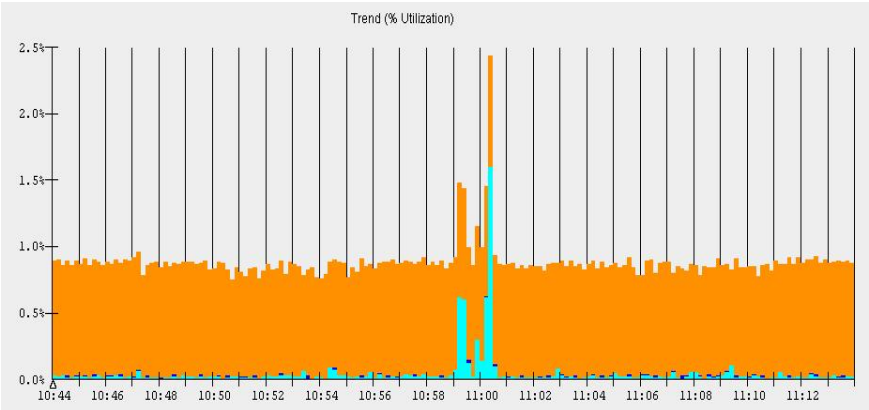
Plano Sala 6



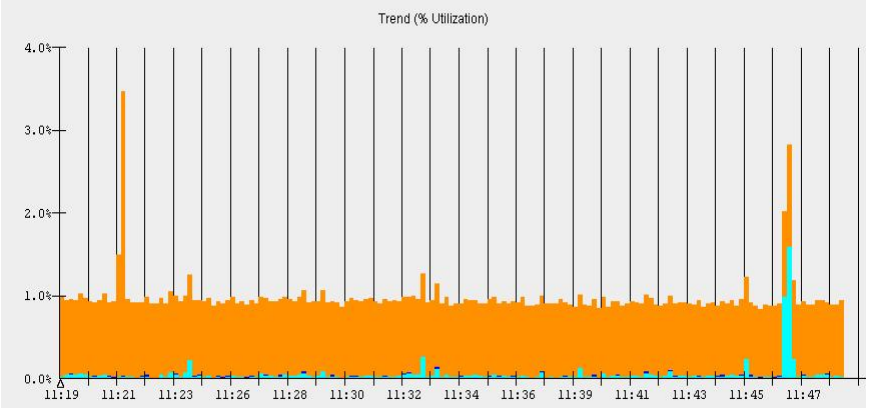
APÉNDICE C.- Gráficas obtenidas por el software de monitoreo

Gráficas obtenidas por el software de monitoreo correspondientes y utilizadas para obtener las gráficas: porcentaje de utilización, distribución de protocolos, toptalkers.

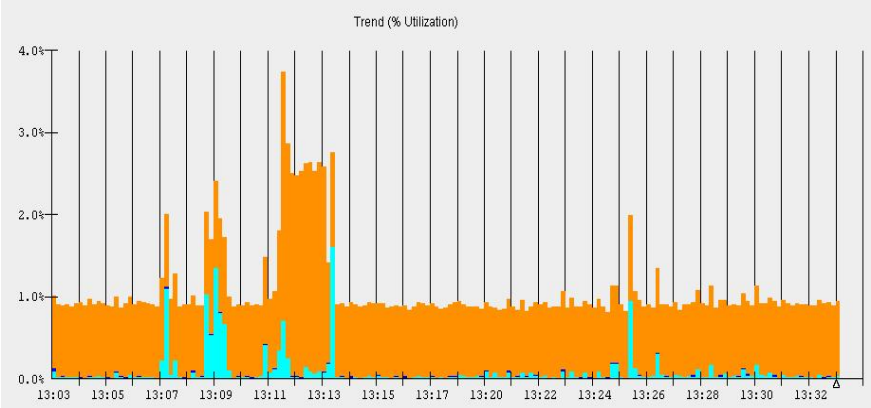
Día 1:



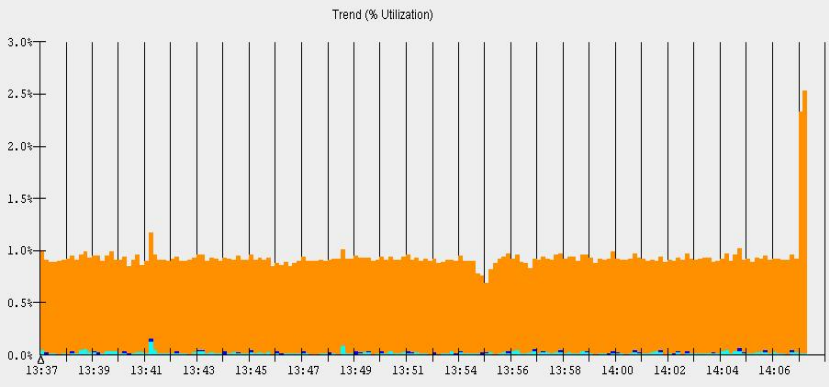
Horario: 10:40 h. Archivo 1



Horario: 11:19 h. Archivo 2

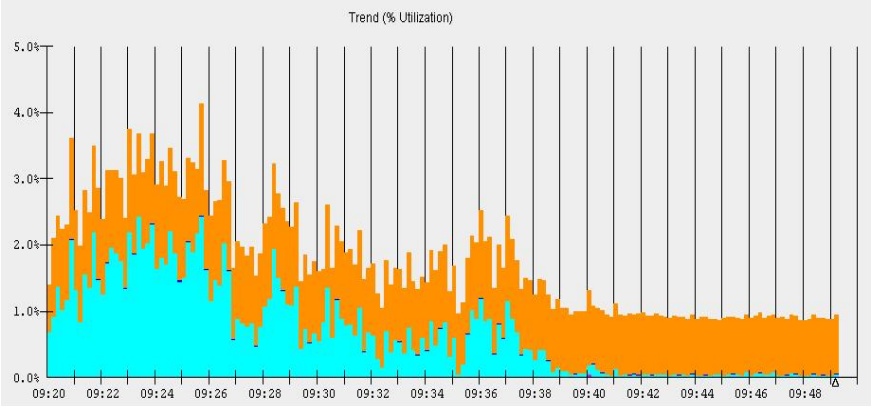


Horario: 13:30 h. Archivo 3

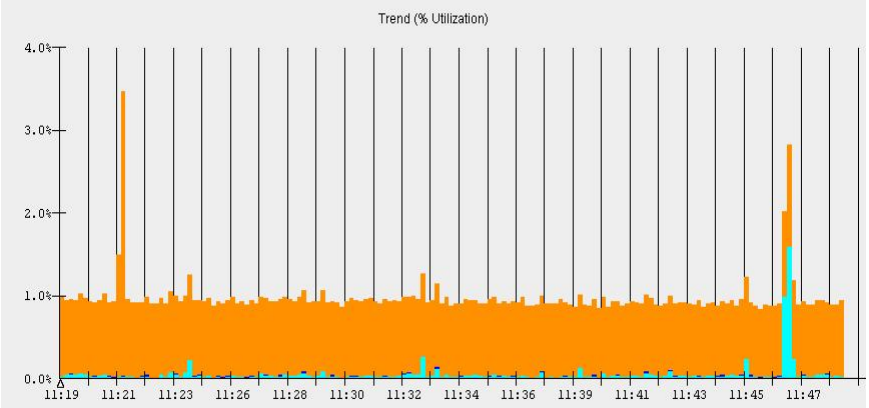


Horario: 13:37 h. Archivo 4

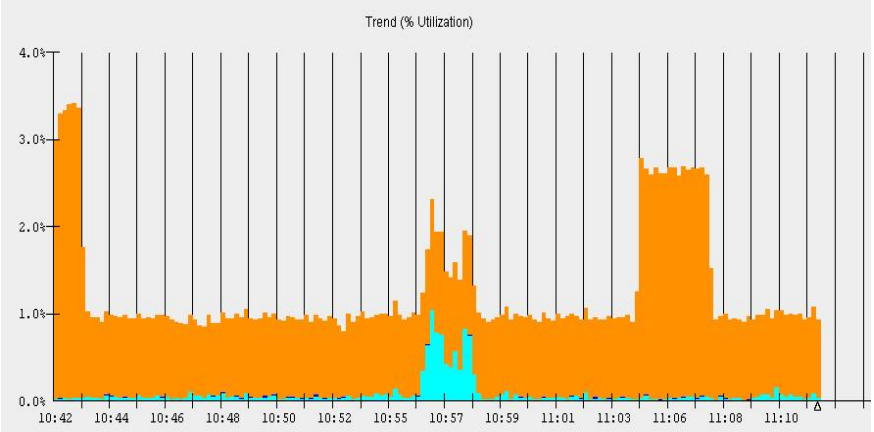
Día 2



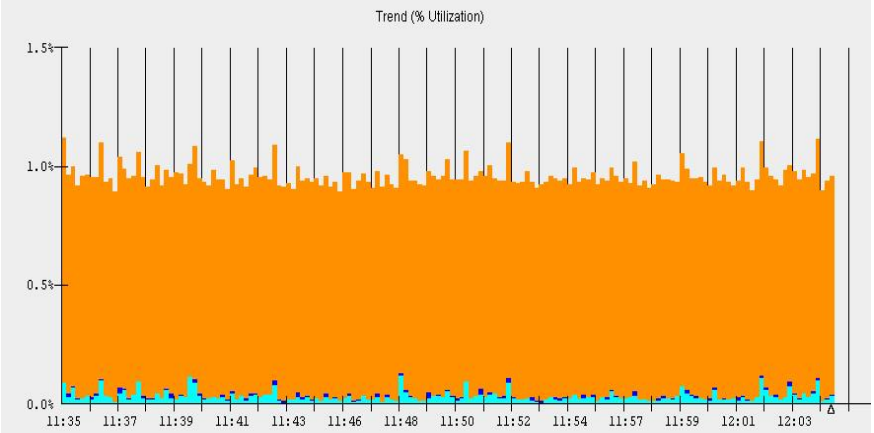
Horario: 9:20 h. Archivo 5



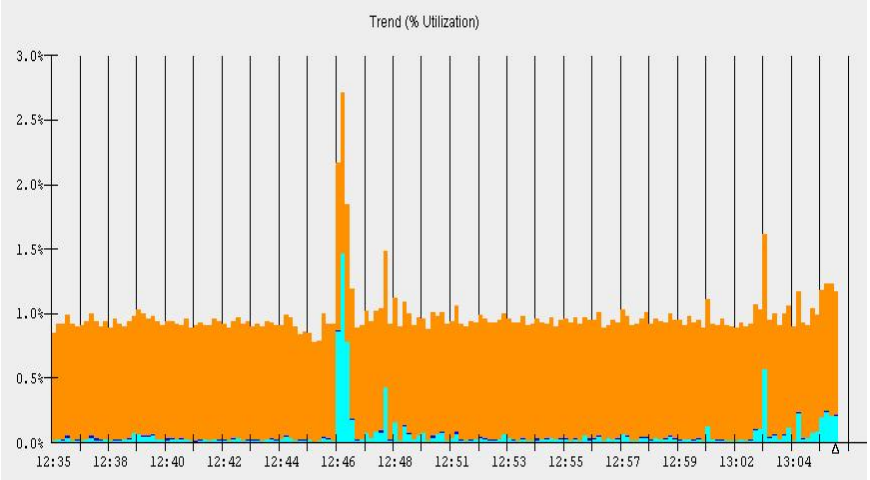
Horario: 9:56 h. Archivo 6



Horario: 10:42 h. Archivo 7

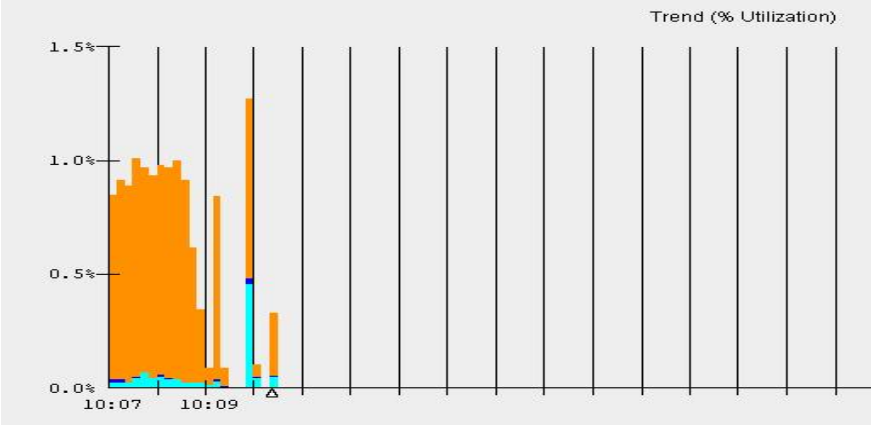


Horario: 11:35 h. Archivo 8

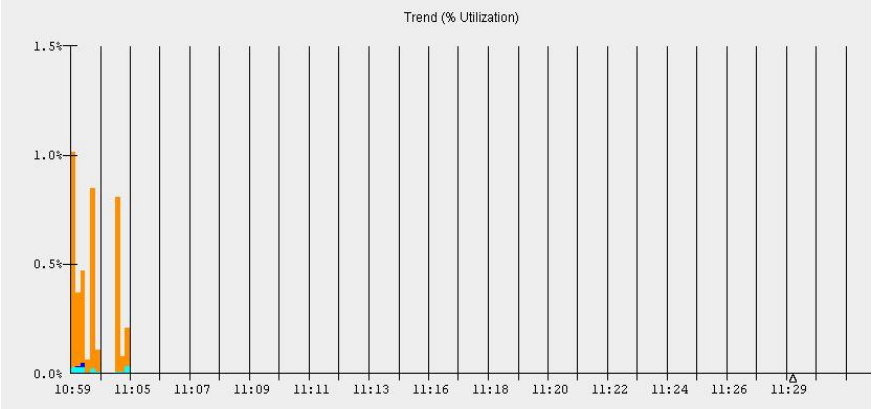


Horario: 12:35 h. Archivo 9

Día 3

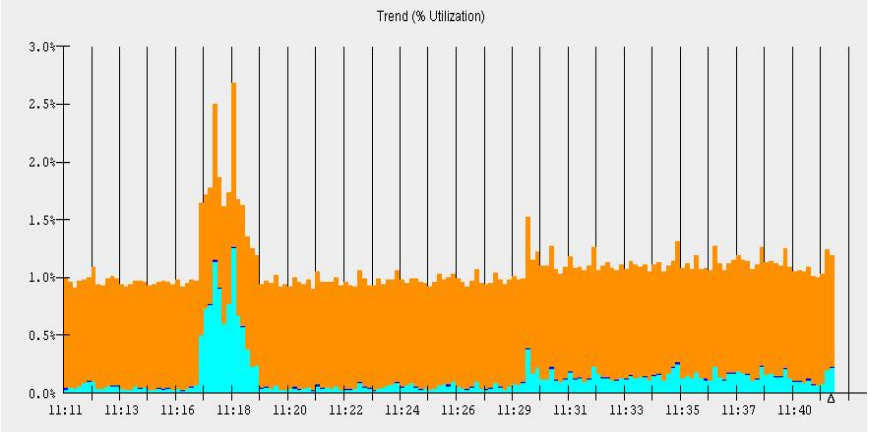


Horario: 10:07 h. Archivo 10

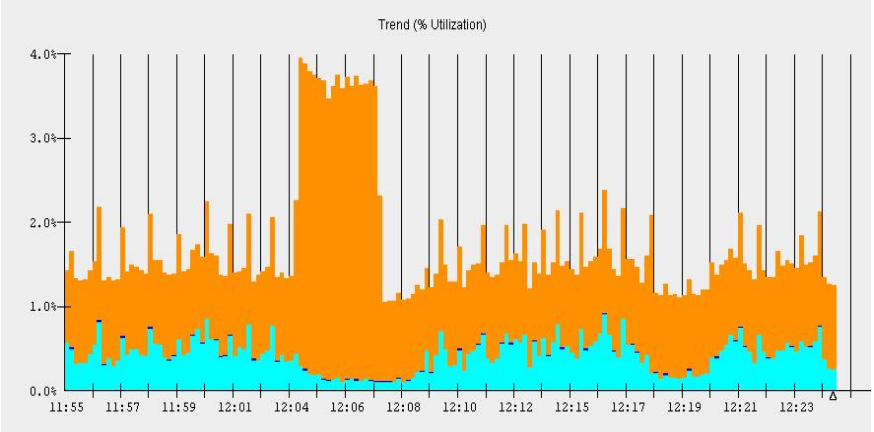


Horario: 10:59 h. Archivo 11

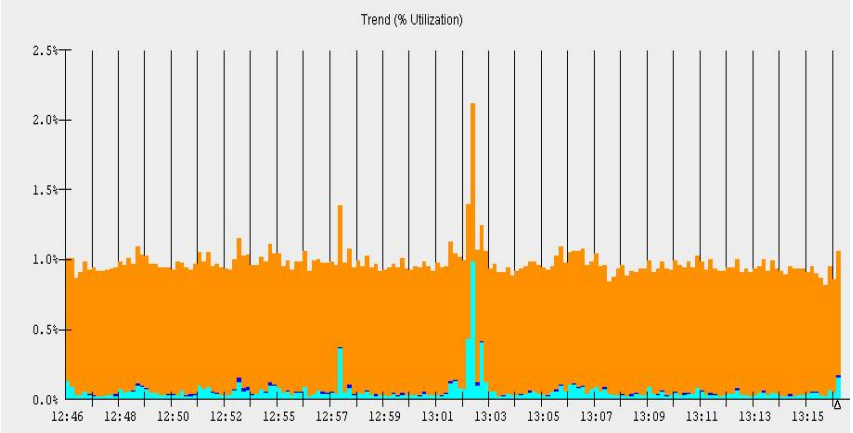
Día 4



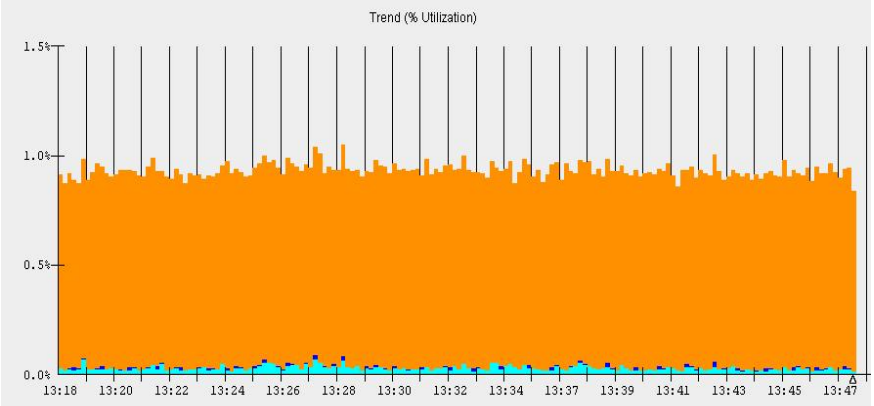
Horario: 11:11 h. Archivo 12



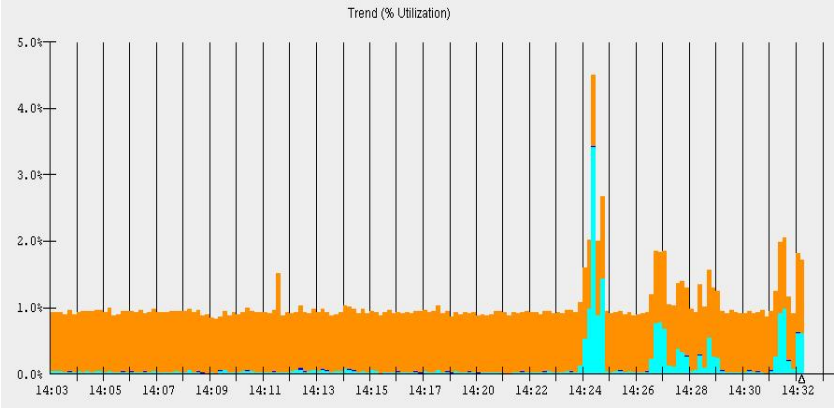
Horario: 11:55 h. Archivo 13



Horario: 12:46 h. Archivo 14



Horario 13:18 h. Archivo 15



Horario: 14:03 h. Archivo 16

APÉNDICE D.- Detalles del material empleado para cablear 16 nodos

Detalle del material empleado para cablear 16 nodos:		
Cantidad	**Tipo**	**Descripción**
1.8	Pieza	Bobina de cable UTP cat. 6 de 4 pares
16	Pieza	Face plate sencillo color blanco
16	Pieza	Jack cat. 6
16	Pieza	Caja plástica
1	Pieza	Panel de parcheo de 24 puntos cat. 6
1	Pieza	Organizador horizontal
18	Pieza	Patch cord de UTP cat. 6 4p de RJ45 a RJ45 de 1.5 metros.
18	Pieza	Patch cord de UTP cat. 6 4p de RJ45 a RJ45 de 3 metros.
1	Pieza	Block 110 de 100 pares con galletas de 4 pares.
29	pieza	Galletas de 4 pares.
4	pieza	Tubo de PVC pesado de 2".
2	pieza	Cople con Codo y Conector de PVC pesado de 2".
1	pieza	Caja de PVC con tapa de 2".
7	metros	Tubo de PVC pesado de ¾".
1	pieza	Cople de PVC pesado de ¾".
18	pieza	Codo de PVC pesado de ¾".
6	pieza	Conector para PVC pesado de ¾".
4	pieza	Caja de PVC con tapa de ¾".
1	pieza	Registro telefónico de 50 x 50.
9	pieza	Tramo de canaleta plástica de 1 vía.
9	pieza	Tramo de canaleta plástica de 3 vías.
68	pieza	Taquete plástico de ¼ (Thorsman Rojo) y Pija de No. 8 x 10.
45	pieza	Taquete plástico de ¼" (Thorsman Café).
68	pieza	Pija de No. 10 x 1 ½" con pija para tablaroca de 1".
1	kilogramo	Alambre galvanizado del No. 16.
1	pieza	Tramo de unicanal perforado.
1	pieza	Tramo de 3 metros de varilla roscada de ¼".
5	pieza	Taquete expansivo de ¼".
9	pieza	Abrazadera para unicanal de 2".
12	pieza	Abrazadera para unicanal de ¾".
0.5	kilogramo	Soldadura 6013 de 1/8" de espesor.
1	Servicio	Servicio de Mano de obra de instalación.

GLOSARIO

DEFINICIONES DE ALGUNOS PROTOCOLOS:

IP (Internet Protocol)

(Protocolo Internet).- Protocolo de capa de rede de la pila TCP/IP que ofrece un servicio de internetwork no orientado a conexión. IP proporciona funciones de direccionamiento, especificación del tipo de servicio, fragmentación y reensamblaje, y seguridad.

ARP (Address Resolution Protocol)

(Protocolo de Resolución de direcciones).- Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC.

RARP (Reverse Address Resolution Protocol)

(Protocolo de Resolución Inversa de Direcciones).- Protocolo de la pila de TCP/IP que facilita un método para encontrar direcciones IP en base a las direcciones MAC.

NET BIOS137-139 (Network Basic Input/Output System (Sistema Básico de Entrada/Salida de Red).- Interfaz de programación de aplicaciones que usan las aplicaciones de una LAN IBM para solicitar servicios a los procesos de red de nivel inferior. Estos servicios incluyen establecimiento y finalización de sesión, así como transferencia de información.

WWW 80 (World Wide Web).- Gran red de servidores de internet que ofrece servicios de hipertexto y otros servicios a las terminales que ejecutan aplicaciones cliente, como, por ejemplo, un explorador WWW. Permite importar hipertextos e imágenes desde varios lugares. Es el sistema de hipertexto que más se emplea y fue creado por el Centro Europeo de Física de Partículas (CERN) en Suiza.

IGMP 2 (Internet Group Management Protocol)

(Protocolo de Administración de Grupos de Internet).- Protocolo utilizado por los hosts IP para informar de los miembros de un grupo de multicast (multidifusión) a un router multicast (de multidifusión) adyacente.

NTP 123 (Net Time Protocol)

(Protocolo de Tiempo de Red).- Protocolo desarrollado sobre TCP que garantiza la precisión de la hora local, con referencia a los relojes de radio y atómicos ubicados en Internet. Este protocolo puede sincronizar los relojes distribuidos en milisegundos durante periodos de tiempo prolongados.

BOOTP 67,68 (Protocolo BOOTP).- Protocolo usado por un nodo de red para determinar la dirección IP de sus interfaces Ethernet para inicializar la red.

TCP/UDP 427 (Transmisión Control Protocol)

(Protocolo para el Control de la Transmisión).- Protocolo de la capa de Transporte orientado a conexión que proporciona una transmisión dúplex fiable de datos. TCP es parte de la pila de protocolos TCP/IP.

UDP (User Datagram Protocol)

(Protocolo de datagrama de usuario).- Protocolo sin conexión de capa de Trasporte de la pila de protocolos TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

DNS 53 (Domain Name Service)

(Servicio de Nombres de Dominio).- Servicio de asignación de nombres a las computadoras con una estructura jerárquica. Los nombres están formados por palabras separadas por puntos.

ICMP 1 (Internet Control Message Protocol)

(Protocolo de Mensajes de Control en Internet).- Protocolo de Internet de capa de Red que informa de los errores y proporciona información relativa al procesamiento de paquetes IP.

DLL Este protocolo de medición estadística muestra todos los tipos de paquetes de Ethernet y mensajes ocurridos en la Capa de Enlace (Data Link Layer, DLL). Cada tipo de paquete o mensaje es listado en una fila por separado.

IPX (Internet Packet Exchange)

(Intercambio de Paquetes entre Redes).- Protocolo de capa de red de NetWare utilizado para transferir datos desde los servidores a las estaciones de trabajo. IPX es similar a IP y XNS

BIBLIOGRAFÍA

1. TANENBAUM, Andrew S. Redes de Computadoras. 3ª Edición, México, Editorial Prentice Hall, 313pp.

2. STALLINGS, William. Comunicaciones y Redes de Computadores 7ª Edición, España, Editorial Pearson Prentice Hall, 830 pp.

3. NAVARRO, Anna S. Diccionario de Términos de Comunicaciones y Redes. 2003, Editorial Pearson Educación, Cisco Press. 612 pp.

4. MILLER, Stewart S. Seguridad en WiFi, España, Editorial McGraw-Hill. 268 pp.

5. CURTIS Nancy. Network+ Certification CompTia, 4ª Edición, E.U., Procert Labs.

6. HALL Fred S. Comunicación de Datos. Redes de Comutadoras y Sistemas Abiertos. Editorial.

7. DE LAET,Gert. Network Security Fundamentals. Cisco Press. 389 pp.

Glosario de TIC 2005, Revista RED, 112 pp.

Revista RED, La Comunidad de Expertos en Redes.
Núm. 181. Abril 2006.
"Bondades de las Redes inalámbricas" pág. 29

Núm. 177 Noviembre 2005
"Mimo la próxima generación de la tecnolgía
WiFi".