CAPÍTULO II

MARCO TEÓRICO

Al lograr definir el planteamiento del problema, precisamos los objetivos general y específicos que regirán los lineamientos de esta investigación, se hace necesario señalar trabajos realizados por investigadores independientes que sustentarán el objeto de estudio, a tal efecto se indican antecedentes hasta el momento relacionados al tema de investigación del modelo de optimización de interconexión de redes inalámbricas. Por su parte, Sabino C. (2000), expone que el punto de partida de una investigación para construir el marco teórico lo constituyen los conocimientos previos de los fenómenos que se abordan en la que se exponen las características dentro de lo que se denomina Antecedentes.

1.- ANTECEDENTES DE LA INVESTIGACIÓN

Antúnez M. (2002). En su trabajo especial de grado titulado: Redes inalámbricas para la interconexión de redes y acceso a Internet en entidades municipales en las zonas rurales. Universidad Dr. Rafael Belloso Chacín, Decanato de Investigación y Postgrado, Maestría en Telemática, Maracaibo. La presente investigación tiene como objeto de estudio el análisis del costo

beneficio que representan las redes inalámbricas, como alternativa de solución al problema de interconexión de forma tradicional (cableada) de las entidades de gobierno correspondientes al municipio Jesús Enrique Lossada del Estado Zulia. Este municipio es primordialmente agrícola, aunque también destaca en la explotación petrolera.

La disposición gubernamental y la dispersión de las entidades del poder local ofrecen condiciones especiales para la experimentación con la tecnología de redes inalámbricas, en tanto que las compañías de telefonía fija y móvil que prestan servicios en el país no han invertido en las áreas rurales por estimar que la inversión es muy alta y el número de usuarios muy pobre como para considerarse nichos interesantes de explotación comercial.

La alcaldía del municipio Jesús Enrique Lossada no tiene actualmente ningún tipo de comunicación entre ésta y sus dependencias, porque no se poseen los medios técnicos para disfrutar de un enlace de telecomunicaciones. La investigación abarca la selección de una solución con base en la alternativa tecnológica de las redes inalámbricas, el diseño de esta propuesta, la exposición de los recursos a emplear en la estructura de la red y la estimación de costos.

Este trabajo se clasifica como una investigación de campo, de la modalidad proyecto factible basado en un diseño no experimental descriptivo. Mediante una red inalámbrica se pretende dar solución a la necesidad de interconectar todos los entes del Gobierno local y brindar, paralelamente, la capacidad de compartir información en formato electrónico entre los

conectados, la posibilidad de establecer canales de voz para una conversación vía telefónica a través de la red, y el acceso a Internet para la búsqueda de información general y/o especializada.

Como resultado final de esta investigación se planteó un diseño de una red inalámbrica de voz y datos para interconectar ocho entidades municipales ubicadas en la zona urbana de La Concepción y las tres juntas parroquiales ubicadas en las parroquias del municipio.

La importancia del estudio mencionado radica en que el uso de las redes inalámbricas se presenta como alternativa para reducir los costos de cableado y la reducción de tiempo en el envió de información, lo que también se quiere lograr con la investigación presentada.

Morillo G. (2002). En su trabajo especial de grado titulado: Infraestructura tecnológica de vigilancia remota. Universidad Dr. Rafael Belloso Chacín, Decanato de Investigación y Postgrado, Maestría en Telemática, Maracaibo.

La investigación corresponde a una evaluación de las infraestructuras tecnológicas de vigilancia remota, a fin de determinar cual es estándar más adecuado a aplicar en la actualización de una infraestructura tecnológica de vigilancia remota existente, además se evalúan distintos fabricantes de este tipo de redes a fin de obtener el mejor de los productos, garantizando robustez, escalabilidad, soporte y seguridad, de igual manera se evaluaron los aspectos financieros de las mismas, para este tipo de aplicación.

La investigación se define como un proyecto factible, y cuyo diseño es no experimental, del tipo transeccional descriptivo ya que se indaga la incidencia

y los valores en que se manifiesta la variable. En cuanto al instrumento utilizado, fue el cuestionario el cual permitió recopilar información necesaria para el desarrollo de la propuesta, basados en las opiniones de la muestra de la investigación. En la investigación se puede notar que es altamente viable la optimización de la infraestructura tecnológica de vigilancia remota del puente General. Rafael Urdaneta, ya que las características de este tipo de redes y sus muchas aplicaciones así lo permiten, no obstante el estándar MPGE es el más adecuado para las aplicaciones de vídeo.

Por lo tanto esta optimización de la infraestructura tecnológica de vigilancia remota traerá muchos beneficios en todas las áreas de supervisión de la estructura del puente, y será una herramienta muy importante en el proceso de escalabilidad y mejoramiento de la plataforma de vigilancia remota, ya que seria de gran relevancia para la toma de decisiones y su costo de adquisición de la infraestructura y posterior mantenimiento sería bajo con respecto al que se encuentra en la actualidad.

Es importante señalar que el estudio, tiene relevancia para la investigación presentada, porque la utilización de la red prototipo como modelo de referencia para el diseño, así como también el análisis del diseño, presentación y evaluación del mismo para lograr obtener una mejor claridad de los objetivos y resultados que se deseen alcanzar en esta investigación.

Marko F. (2002). En su trabajo especial de grado titulado: Desarrollo de una solución de conexión inalámbrica en redes de área local. Universidad Dr.

Rafael Belloso Chacín, Decanato de Investigación y Postgrado, Maestría en Telemática, Maracaibo.

El propósito de la investigación fue desarrollar una solución de conexión inalámbrica en redes de área local que brinde flexibilidad, movilidad y facilidad en la transmisión, recepción y uso de la información sobre las redes de cableado existentes, fortaleciendo de esta manera la infraestructura de comunicaciones utilizada actualmente a través del estudio e implementación de las tecnologías inalámbricas.

Para la realización de la investigación se utilizó una metodología que surge de un eclecticismo de dos autores llamados Montilva, Jonás y Fitzgerald, J., la cual esta constituida por seis fases las cuales son: la investigación preliminar, la comprensión del sistema, el desarrollo de propuestas, las consideraciones de hardware y software, los costos de la red y los beneficios del diseño de la red. La investigación se cataloga de aplicada, descriptiva y de campo.

En el desarrollo de la investigación se evaluaron varias propuestas las cuales fueron analizadas para seleccionar la tecnología adecuada a las necesidades de conexión presentadas en la problemática planteada, en la cual resultó seleccionada la tecnología inalámbrica de radio frecuencias Spread Spectrum de secuencia directa por ser la más óptima en el cumplimiento de los objetivos planteados en la investigación logrando un alto nivel de satisfacción.

Este proyecto, proporcionó un aporte considerable, tal como, el tratamiento de la metodología en el análisis y aplicación de cada fase de la misma; para lograr una mejor claridad y aplicación en la medición de indicadores afines de optimizar la administración de un Modelo de Gestión de red.

Chavarría M. (2004). En su trabajo especial de grado titulado: Redes inalámbricas de área local (WLAN) de alta velocidad. Universidad de Costa Rica, Facultad de Ingeniería, Escuela de Ingeniería Eléctrica, San José, Costa Rica.

En este trabajo se realizó un estudio de los esquemas de modulación en redes inalámbricas para obtener altas velocidades de transmisión de datos, también se analizaron los dispositivos y sus posibles aplicaciones, y se establecieron las bases para realizar un diseño de una WLAN.

La necesidad de estudiar y entender el tipo de modulación que se utiliza en las normas de redes inalámbricas llevó no sólo a buscar en libros de referencia, sino también en artículos presentados por los fabricantes de los equipos y por los organismos encargados de estandarizarlos.

La seguridad es un elemento que se ha cuestionado mucho a todas las normas de redes inalámbricas, por lo tanto es necesario estudiar y analizar las diferentes variedades de configuraciones que se pueden obtener hoy en día para realizar un diseño que sea lo suficientemente seguro, utilizando los mecanismos necesarios como llaves de encriptación o redes privadas virtuales.

Los elementos básicos para la puesta en marcha de una red inalámbrica son los puntos de acceso y las tarjetas de acceso inalámbrico. Las antenas otorgan mayor versatilidad a las áreas de cobertura o enlaces entre edificios en las redes inalámbricas. Finalmente por limitaciones de equipo y de acceso a las instalaciones de la Facultad de Ingeniería los fines de semana, no fue posible realizar una propuesta para interconectar aulas donde se imparten lecciones de Ingeniería Eléctrica con la red de la escuela de forma inalámbrica.

Este trabajo ofrece un amplio marco de referencia práctica para el presente estudio, propone ciertos lineamientos para establecer una propuesta de interconexión de redes inalámbricas y su aplicabilidad real; aportando y confirmando una serie de indicadores de los cuales se hacen uso para la realización de esta investigación.

Abreu J. (2006). En su trabajo especial de grado titulado: Estudio de factibilidad de un enlace inalámbrico en las empresas de distribución de energía eléctrica. Universidad Dr. Rafael Belloso Chacín, Decanato de Investigación y Postgrado, Maestría en Telemática, Maracaibo.

El objetivo fundamental de esta investigación es realizar un estudio de factibilidad de un enlace inalámbrico en la empresa de distribución de energía eléctrica CADELA, basándose en aportes teóricos de diferentes autores con relación al área de la tecnología inalámbrica. El tipo de investigación que se utilizo se enmarca en proyecto factible, y la información se obtuvo a través de la ejecución del procedimiento planteado,

considerando las metas y objetivos que se presentaron para proponer el estudio de un enlace inalámbrico en la empresa CADELA, posteriormente se realizo un estudio de factibilidad y análisis de la situación actual de la misma, seleccionando así la frecuencia de operación 2.4 por ser la mas económica y la mas ajustable.

Además se evaluó la factibilidad técnica, operativa y de costo, demostrando que dicha tecnología ya esta disponible en el mercado siendo esta una de las más confiables para el desarrollo de aplicaciones inalámbricas. Dichos resultados ratifican un nivel de señal óptimo para los usuarios que se encuentran dentro del rango estipulado.

Es importante señalar que el antecedente sirvió como orientación metodológica en la investigación planteada para el desarrollo del estudio de factibilidad. Además se evaluó la factibilidad técnica y operacional demostrando que dicha tecnología ya esta disponible en el mercado siendo esta una de las más confiables para el desarrollo de aplicaciones inalámbricas.

2.- BASES TEÓRICAS

Sabino C. (2000) sugiere la realización de las bases de diversas teorías y conceptos relevantes de la investigación es dar un enfoque coordinado y coherente que permita integrar a la investigación en un ámbito donde se cobre sentido el objeto de estudio. Las consideraciones y el carácter teórico práctico del proceso de conocimiento son la base teórica en un conjunto de

conocimientos con el fin de ofrecer una conceptualizació0n adecuada de los términos utilizados. A tal efecto, la investigación se orientó a partir de comunicación de datos, redes inalámbricas y alámbricas, gestión de red, gestión de telecomunicaciones, plataformas para gestión de red, entre otros.

2.1.- COMUNICACIONES DE DATOS

En cuanto al desarrollo de la computación y su integración con las telecomunicaciones en la telemática Huidobro, J. (2002) sostiene que se ha propiciado el surgimiento de nuevas formas de comunicación, que son aceptadas cada vez por más personas. El desarrollo de las redes informáticas posibilito su conexión mutua y, finalmente, la existencia de Internet, una red de redes gracias a la cual una computadora puede intercambiar fácilmente información con otras situadas en regiones lejanas del planeta.

La información a la que se accede a través de Internet combina el texto con la imagen y el sonido, es decir, se trata de una información multimedia, una forma de comunicación que esta conociendo un enorme desarrollo gracias a la generalización de computadores personales dotadas del hardware y software necesarios. El último desarrollo en nuevas formas de comunicación es la realidad virtual, que permite al usuario acceder a una simulación de la realidad en tres dimensiones, en la cual es posible realizar acciones y obtener inmediatamente una respuesta.

El uso creciente de la tecnología de la información en la actividad económica ha dado lugar a un incremento sustancial en el número de puestos de trabajo informatizados, con una relación de terminales por empleado que aumenta constantemente en todos los sectores industriales. La movilidad lleva a unos porcentajes de cambio anual entre un 20 y un 50% del total de puestos de trabajo. Los costos de traslado pueden ser notables (nuevo tendido para equipos informáticos, teléfonos, entre otros.). Por tanto, se hace necesaria una racionalización de los medios de acceso de estos equipos con el objeto de minimizar dichos costos.

Las redes de área local (LAN) han sido creadas para responder a ésta problemática. El crecimiento de las redes locales a mediados de los años ochenta hizo que cambiase nuestra forma de comunicarnos con los ordenadores y la forma en que los ordenadores se comunicaban entre sí. La importancia de las LAN reside en que en un principio se puede conectar un número pequeño de ordenadores que puede ser ampliado a medida que crecen las necesidades. Son de vital importancia para empresas pequeñas puesto que suponen la solución a un entorno distribuido.

2.2.- TIPOS DE CONEXIONES DE REDES DE DATOS

De acuerdo a los tipos de conexiones Stallings, W. (2004), plantea que las características mas notables en la evolución de la tecnología de las computadoras es la tendencia a la modularidad. Los elementos básicos de una computadora se conciben, cada vez mas, como unidades dotadas de

autonomía, con posibilidad de comunicación con otras computadoras o con bancos de datos. La comunicación entre dos computadoras puede efectuarse mediante los tres tipos de conexión:

Conexión directa. A este tipo de conexión se le llama transferencia de datos on – line. Las informaciones digitales codificadas fluyen directamente desde una computadora hacia otra, sin ser transferidas a ningún soporte intermedio. Los datos pueden viajar a través de una interfaz serie o paralelo, formada simplemente por una conexión física adecuada, como por ejemplo un cable.

Conexión a media distancia. Es conocida como conexión off - line. La información digital codificada se graba en un soporte magnético o en una ficha perforada y se envía al centro de proceso de datos, donde será tratada por una unidad central u host.

Conexión a gran distancia. Con redes de transferencia de datos, de interfaces serie y módems se consiguen transferencia de información a grandes distancias.

La tecnología electrónica, con sus microprocesadores, memorias de capacidad cada vez más elevada y circuitos integrados, hace que los cambios en el sector de las comunicaciones puedan asociarse a los de las computadoras, porque forma parte de ambos. Hace ya algún tiempo que se están empleando redes telefónicas para las comunicaciones de textos, imágenes y sonidos. Por otro lado existen redes telefónicas, públicas y privadas, dedicadas solamente a la transmisión de datos.

Mediante el teléfono de nuestra casa se puede establecer comunicación con cualquier lugar del mundo, marcando las claves correctas. Si se dispone de la ayuda de una computadora, conectada a la línea telefónica mediante un modulador / demodulador (MODEM), se puede comunicar con otras computadoras que dispongan de los mismos elementos.

Cada día existe más demanda de servicios de telecomunicación entre computadoras, y entre éstas y terminales conectados en lugares alejados de ellas, lo cual abre más el abanico de posibilidades de la conjunción entre las comunicaciones y la computación o informática, conjunción a la que se da el nombre de telemática.

2.3.- MEDIOS DE COMUNICACIÓN

En un estudio reciente por Beltrao (1990), el medio de comunicación puede limitar la velocidad de intercambio de información y, además, es un aspecto que tiene relativa importancia a la hora de realizar la instalación de la red de un determinado edificio. Las redes de área local pueden funcionar con muchos de los medios de transmisión existentes. Los más utilizados se comentarán a continuación:

2.3.1.- CABLE PAR TRENZADO

Es de los más antiguos en el mercado y en algunos tipos de aplicaciones es el más común. Consiste en dos alambres de cobre o a veces de aluminio, aislados con un grosor de un milímetro aproximadamente. Los alambres se

trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se agrupan bajo una cubierta común de policloruro de vinilo (PVC) en cables multipares de pares trenzados (de 2, 4, 8, hasta 300 pares).

Un ejemplo de par trenzado es el sistema de telefonía, ya que la mayoría de aparatos se conectan a la central telefónica por medio de un par trenzado. Actualmente, se han convertido en un estándar en el ámbito de las redes de área local (LAN) como medio de transmisión en las redes de acceso a usuarios (típicamente cables de 2 ó 4 pares trenzados). A pesar que las propiedades de transmisión de cables de par trenzado son inferiores, y en especial la sensibilidad ante perturbaciones extremas, a las del cable coaxial, su gran adopción se debe al costo, su flexibilidad y facilidad de instalación, así como las mejoras tecnológicas constantes introducidas en enlaces de mayor velocidad, longitud, entre otros.

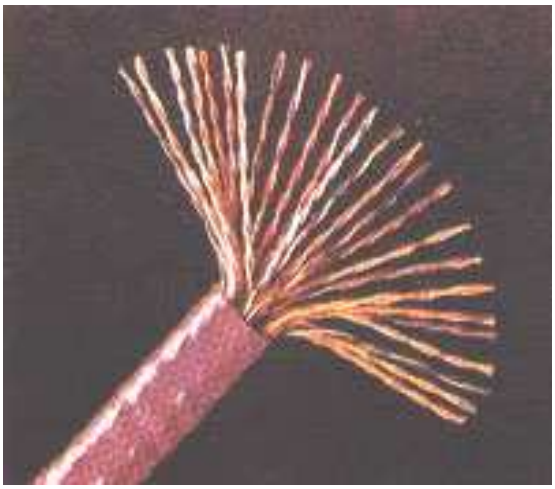

Figura 1. Par trenzado para sistema de telefonía
Fuente: Beltrao M. (1990)

2.3.2.- ESTRUCTURA DEL CABLE PAR TRENZADO

Por lo general, la estructura de todos los cables par trenzado no difieren significativamente, aunque es cierto que cada fabricante introduce algunas tecnologías adicionales mientras los estándares de fabricación se lo permitan. El cable está compuesto, por un conductor interno que es de alambre electrolítico recocido, de tipo circular, aislado por una capa de polietileno coloreado.

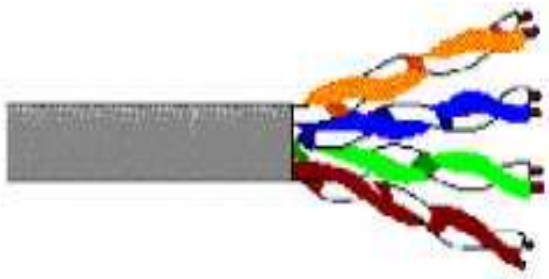

Figura 2. Estructura del cable par trenzado
Fuente: Beltrao M. (1990)

Debajo de la aislación coloreada existe otra capa de aislación también de polietileno, que contiene en su composición una sustancia antioxidante para evitar la corrosión del cable. El conducto sólo tiene un diámetro de aproximadamente medio milímetro, y más la aislación el diámetro puede superar el milímetro.

Sin embargo es importante aclarar que habitualmente este tipo de cable no se maneja por unidades, sino por pares y grupos de pares, paquete conocido como cable multipar. Todos los cables del multipar están trenzados

entre sí con el objeto de mejorar la resistencia de todo el grupo hacia diferentes tipos de interferencia electromagnética externa.

Por esta razón surge la necesidad de poder definir colores para los mismos que permitan al final de cada grupo de cables conocer qué cable va con cual otro. Los colores del aislante están normalizados a fin de su manipulación por grandes cantidades. Para Redes Locales los colores estandarizados son: Naranja / Blanco – Naranja. Verde / Blanco – Verde. Blanco / Azul – Azul Blanco / Marrón – Marrón.

En telefonía, es común encontrar dentro de las conexiones grandes cables telefónicos compuestos por cantidades de pares trenzados, aunque perfectamente identificables unos de otros a partir de la normalización de los mismos. Los cables una vez fabricados unitariamente y aislados, se trenzan de a pares de acuerdo al color de cada uno de ellos; aún así, estos se vuelven a unir a otros formando estructuras mayores: los pares se agrupan en subgrupos, los subgrupos de agrupan en grupos, los grupos se agrupan en superunidades, y las superunidades se agrupan en el denominado cable.

De esta forma se van uniendo los cables hasta llegar a capacidades de 2200 pares; un cable normalmente está compuesto por 22 superunidades; cada sub - unidad está compuesta por 12 pares aproximadamente; este valor es el mismo para las unidades menores. Los cables telefónicos pueden ser armados de 6, 10, 18, 20, 30, 50, 80, 100, 150, 200, 300, 400, 600, 900, 1200, 1500, 1800 ó 2200 pares.

2.3.3.- TIPOS DE CABLE PAR TRENZADO

Cable de par trenzado apantallado (STP). En este tipo de cable, cada par va recubierto por una malla conductora que actúa de apantalla frente a interferencias y ruido eléctrico. Su impedancia es de 150 Ohm.

Figura 3. Cable de par trenzado apantallado (STP)
Fuente: Beltrao M. (1990)

El nivel de protección del STP ante perturbaciones externas es mayor al ofrecido por UTP. Sin embargo es más costoso y requiere más instalación. La pantalla del STP, para que sea más eficaz, requiere una configuración de interconexión con tierra (dotada de continuidad hasta el terminal), con el STP se suele utilizar conectores RJ49.

Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.

Cable de par trenzado con pantalla global (FTP). En este tipo de cable como en el UTP, sus pares no están apantallados, pero sí dispone de una pantalla global para mejorar su nivel de protección ante interferencias

externas. Su impedancia característica típica es de 120 OHMIOS y sus propiedades de transmisión son más parecidas a las del UTP. Además, puede utilizar los mismos conectores RJ45. Tiene un precio intermedio entre el UTP y STP.

Cable par trenzado no apantallado (UTP). El cable par trenzado más simple y empleado, sin ningún tipo de pantalla adicional y con una impedancia característica de 100 Ohmios. El conector más frecuente con el UTP es el RJ45, aunque también puede usarse otro (RJ11, DB25, DB11, entre otros), dependiendo del adaptador de red.

Es sin duda el que hasta ahora ha sido mejor aceptado, por su costo accesibilidad y fácil instalación. Sus dos alambres de cobre torcidos aislados con plástico PVC han demostrado un buen desempeño en las aplicaciones de hoy. Sin embargo, a altas velocidades puede resultar vulnerable a las interferencias electromagnéticas del medio ambiente. El cable UTP es el más utilizado en telefonía.

Categorías del cable UTP. Cada categoría especifica unas características eléctricas para el cable: atenuación, capacidad de la línea e impedancia. Existen actualmente ocho categorías dentro del cable UTP:

Figura 4. Cable UTP
Fuente: Beltrao M. (1990)

Categoría 1: Este tipo de cable esta especialmente diseñado para redes telefónicas, es el típico cable empleado para teléfonos por las compañías telefónicas. Alcanzan como máximo velocidades de hasta 4 Mbps.

Categoría 2: De características idénticas al cable de categoría 1.

Categoría 3: Es utilizado en redes de ordenadores de hasta 16 Mbps. de velocidad y con un ancho de banda de hasta 16 Mhz.

Categoría 4: Esta definido para redes de ordenadores tipo anillo como Token Ring con un ancho de banda de hasta 20 Mhz y con una velocidad de 20 Mbps.

Categoría 5: Es un estándar dentro de las comunicaciones en redes LAN. Es capaz de soportar comunicaciones de hasta 100 Mbps. con un ancho de banda de hasta 100 Mhz. Este tipo de cable es de 8 hilos, es decir cuatro pares trenzados. La atenuación del cable de esta categoría viene dado por el Cuadro 1, referida a una distancia estándar de 100 metros:

Cuadro 1

Atenuación del Cable UTP

Velocidad de Transmisión de los Datos	**Nivel de Atenuación**
4 Mbps.	13 DB.
10 Mbps.	20 DB.
16 Mbps.	25 DB.
100 Mbps.	67 DB.

Categoría 5e: Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque si esta diferenciada por los diferentes organismos.

Categoría 6: No esta estandarizada aunque ya se está utilizando. Se definirán sus características para un ancho de banda de 250 Mhz.

Categoría 7: No esta definida y mucho menos estandarizada. Se definirá para un ancho de banda de 600 Mhz. El gran inconveniente de esta categoría es el tipo de conector seleccionado que es un RJ-45 de 1 pines.

En el Cuadro 2 se observan las diferentes categorías, teniendo en cuenta su ancho de banda, cual sería las distancias máximas recomendadas sin sufrir atenuaciones que hagan variar la señal:

Cuadro 2

Ancho de banda del Cable UTP

Ancho de Banda	**100 kHz**	**1 MHz**	**20 MHz**	**100 MHz**
Categoría 3	2 Km	500 m	100 m	No existe
Categoría 4	3 Km	600 m	150 m	No existe
Categoría 5	3 Km	700 m	160 m	100 m

2.4.- REDES

Forouzan (2006) sostiene que una red es un conjunto de dispositivos (a menudo denominados nodos) conectados por enlaces de un medio físico. Un

nodo puede ser una computadora, una impresora o cualquier otro dispositivo capaz de enviar y/o recibir datos generados por otros nodos de la red.

Las redes usan procesamiento distribuido en el aspecto en que una tarea está dividida entre múltiples computadoras. En lugar de usar una única máquina grande responsable de todos los aspectos de un proceso, cada computadora individual (habitualmente una computadora personal o una estación de trabajo) maneja un subconjunto de ellos. Para que sea considerada efectiva y eficiente, una red debe satisfacer un cierto número de criterios. Los más importantes son el rendimiento, la fiabilidad y la seguridad.

Rendimiento. El rendimiento se puede medir de muchas formas, incluyendo el tiempo de tránsito y de respuesta. El tiempo de tránsito es la cantidad de tiempo necesario para que un mensaje viaje desde un dispositivo al siguiente. El tiempo de respuesta es el tiempo que transcurre entre una petición y su respuesta. El rendimiento de una red depende de varios factores, incluyendo el número de usuarios, el tipo de medio de transmisión, la capacidad del hardware conectado y la eficiencia del software.

El rendimiento se mide a menudo usando dos métricas: ancho de banda y latencia. A menudo hace falta más ancho de banda y menos latencia. Sin embargo, ambos criterios son a menudo contradictorios. Si se intenta enviar más datos por la red, se incrementa el ancho de banda, pero también la latencia debido a la congestión de tráfico en la red.

Fiabilidad. Además de por la exactitud en la entrega, la fiabilidad de la red se mide por la frecuencia de fallo de la misma, el tiempo de recuperación de un enlace frente a un fallo y la robustez de la red ante una catástrofe.

Seguridad. Los aspectos de seguridad de la red incluyen protección de datos frente a accesos no autorizados, protección de datos frente a fallos y modificaciones e implementación de políticas y procedimientos para recuperarse de interrupciones y pérdidas de datos.

2.5.- COMPONENTES DE UNA RED

En cuanto a los componentes de una red Stallings (2004) explica que una red de computadoras están conectadas tanto por hardware como por software. El hardware incluye tanto las tarjetas de interfaz de red como los cables que las unen, y el software incluye los controladores (programas que se utilizan para gestionar los dispositivos y el sistema operativo de red que gestiona la red. A continuación se listan los componentes:

Servidor. Este ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo.

Estaciones de Trabajo. Cuando una computadora se conecta a una red, la primera se convierte en un nodo de la última y se puede tratar como una estación de trabajo o cliente. Las estaciones de trabajos pueden ser computadoras personales con el DOS, Macintosh, Unix, OS/2 o estaciones de trabajos sin discos.

Tarjetas o Placas de Interfaz de Red. Toda computadora que se conecta a una red necesita de una tarjeta de interfaz de red que soporte un esquema de red específico, como Ethernet, ArcNet o Token Ring. El cable de red se conectara a la parte trasera de la tarjeta.

Sistema de Cableado. El sistema de la red esta constituido por el cable utilizado para conectar entre si el servidor y las estaciones de trabajo.

Recursos y Periféricos Compartidos. Entre los recursos compartidos se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras, los trazadores y el resto de equipos que puedan ser utilizados por cualquiera en la red.

2.6.- ESTRUCTURA FÍSICA

Por otra parte Forouzan (2006) sugiere la realización de la estructura física involucrando los modos de conexión, los flujos de datos, entre otros; mediante una red compuesta por dos o más ordenadores que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento,) ó software (aplicaciones, archivos, datos); en este caso, es necesario definir algunos atributos de una red como lo son:

2.6.1.- TIPO DE CONEXIÓN

Una red está formada por dos o más dispositivos conectados a través de enlaces. Un enlace es el medio de comunicación físico que transfiere los datos de un dispositivo a otro. A efectos de visualización, es sencillo imaginar

cualquier enlace como una línea que se dibuja entre dos puntos. Para que haya comunicación, dos dispositivos deben estar conectados de alguna forma al mismo enlace simultáneamente. Hay dos configuraciones de línea posibles: punto a punto y multipunto.

Punto a punto. Una conexión punto a punto proporciona un enlace dedicado entre dos dispositivos. Toda la capacidad del canal se reserva para la transmisión entre ambos dispositivos. La mayoría de las configuraciones punto a punto usan cables para conectar los extremos, pero también son posibles otras opciones, como las microondas o los satélites de enlace (véase la Figura 5). Cuando se cambian los canales de una televisión con control remoto mediante mando a distancia por infrarrojos, se establecen conexiones punto a punto entre el mando a distancia y el sistema de control de la televisión.

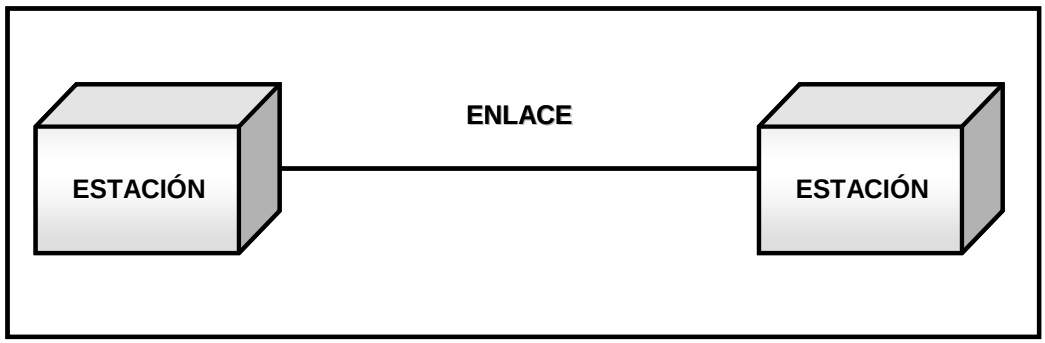

Figura 5. Punto a punto.
Fuente: Forouzan, B., (2006)

Multipunto. Una configuración de línea multipunto (también denominada multiconexión) es una configuración en la que varios dispositivos comparten

el mismo enlace (véase la Figura 6). En un entorno multipunto, la capacidad del canal es compartida en el espacio o en el tiempo. Si varios dispositivos pueden usar el enlace de forma simultánea, se dice que hay una configuración de línea compartida espacialmente. Si los usuarios deben compartir la línea por turnos, se dice que se trata de una configuración de línea de tiempo compartido.

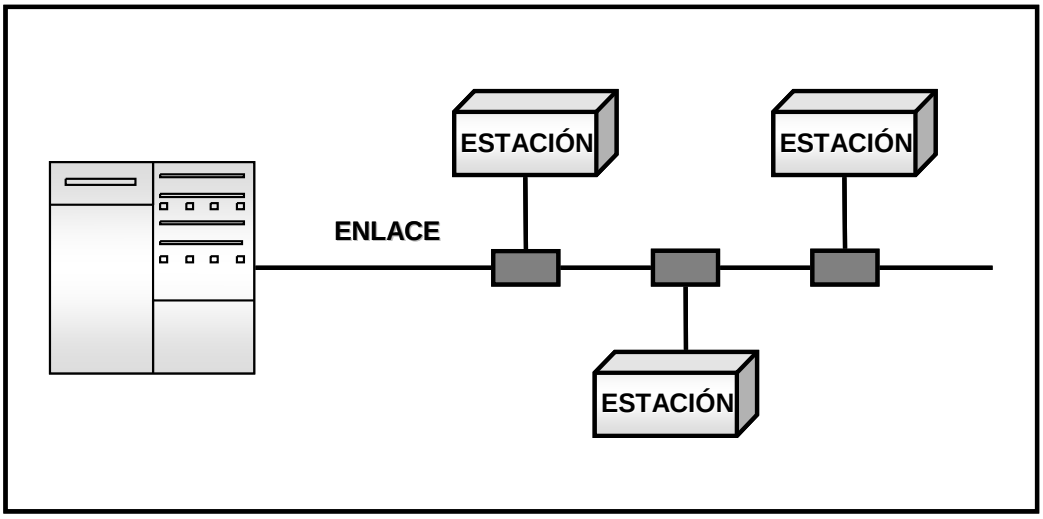

Figura 6. Multipunto.
Fuente: Forouzan, B., (2006)

2.6.2.- TOPOLOGÍA FÍSICA

El término topología física se refiere a la forma en que está diseñada la red físicamente. Dos o más dispositivos se conectan a un enlace; dos o más enlaces forman una topología. La topología de una red es la representación geométrica de la relación entre todos los enlaces y los dispositivos de los

enlazan entre sí (habitualmente denominados nodos). Hay cuatro posibles topologías básicas: malla, estrella, bus y anillo (véase la Figura 7).

Topología en malla. En una topología en malla, cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta. Para hallar el número de enlaces físicos necesarios en una malla con n nodos completamente conectados, es necesario considerar primero si cada nodo debe estar conectado a todos los demás.

El nodo 1 debe estar conectado a n−1 nodos, el nodo 2 a n−1 nodos y, finalmente, el nodo n deben estar conectados a n−1 nodos. Por tanto, se necesitan n(n−1) canales físicos. Sin embargo, si cada enlace físico permite comunicación bidireccional (modo duplex), se puede dividir el número de enlaces por 2.

En otras palabras, se puede decir que en una red en malla completamente conectada se necesitan n(n−1)/2 enlaces físicos duplex. Para acomodar tantos enlaces, cada dispositivo de la red debe tener n−1 puertos de entrada/salida (E/S), (véase la Figura Nº 7) para poder estar conectado a las restantes n−1 estaciones.

Una malla ofrece varias ventajas sobre otras topologías de red. En primer lugar, el uso de los enlaces dedicados garantiza que cada conexión sólo debe transportar la carga de datos propia de los dispositivos conectados, eliminando el problema que surge cuando los enlaces son compartidos por varios dispositivos. En segundo lugar, una topología en malla es robusta. Si

un enlace falla, no inhabilita todo el sistema. En tercer lugar, está la ventaja de la privacidad o la seguridad.

Cuando un mensaje viaja a través de una línea dedicada, solamente lo ve el receptor adecuado. Las fronteras físicas evitan que otros usuarios puedan tener acceso a los mensajes. Finalmente, los enlaces punto a punto hacen que se puedan identificar y aislar los fallos más fácilmente. El tráfico se puede encaminar para evitar los enlaces de los que se sospecha que tienen problemas. Esta facilidad permite que el gestor de red pueda descubrir la localización precisa del fallo y ayudar a buscar sus causas y posibles soluciones.

Las principales desventajas de la malla se relacionan con la cantidad de cable y el número de puertos de entrada/salida necesarios. En primer lugar, la instalación y reconfiguración de la red es difícil, debido a que cada dispositivo debe estar conectado a cualquier otro. En segundo lugar, la masa de cables puede ser mayor que el espacio disponible para acomodarla (en paredes, techos o suelos).

Finalmente, el hardware necesario para conectar cada enlace (puertos de E/S y cables) pueden ser caros. Por estas razones, las topologías en malla se suelen instalar habitualmente en entornos reducidos; por ejemplo, en una red troncal que conecte las computadoras principales de una red híbrida que puede incluir varias topologías más.

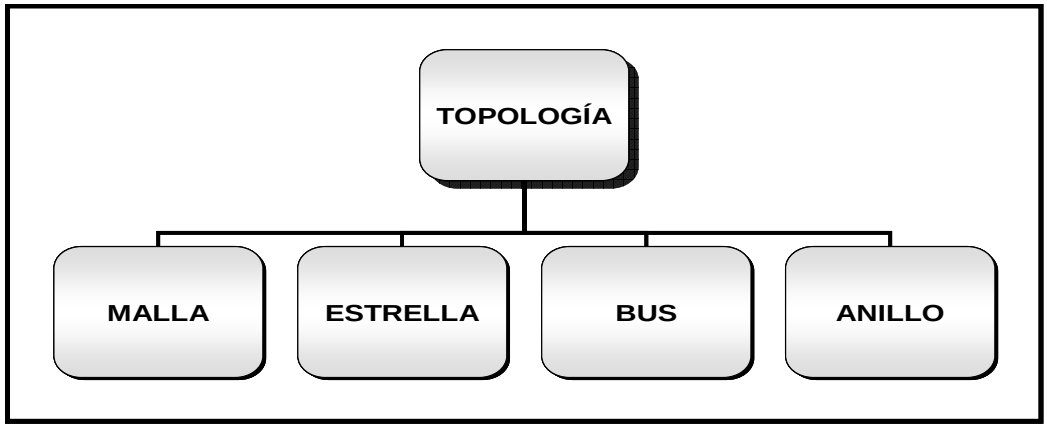

Figura 7. Clases de topologías.
Fuente: Forouzan, B., (2006)

Un ejemplo práctico de topología en malla es la conexión de las oficinas regionales de teléfonos, en las que cada oficina necesita estar conectada a todas las demás.

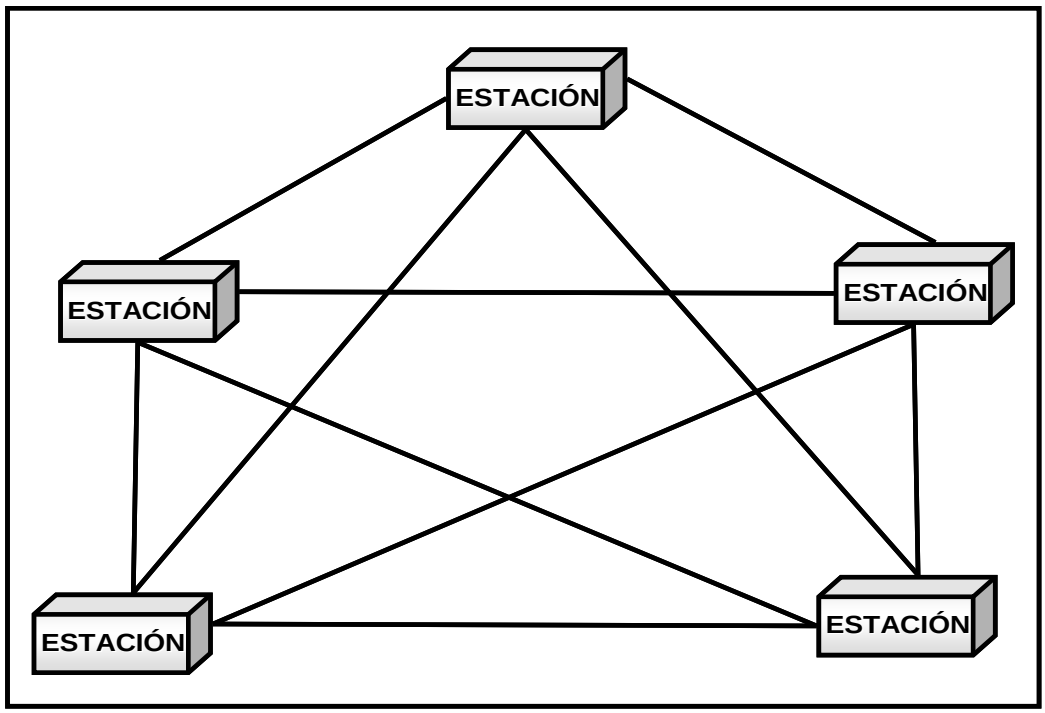

Figura 8. Topología en malla completamente conectada.
Fuente: Forouzan, B., (2006)

Topología en estrella. En las topologías en estrella cada dispositivo solamente tiene un enlace punto a punto dedicado con el controlador central, habitualmente llamado concentrador. Los dispositivos no están directamente enlazados entre sí. A diferencia de la topología en malla, la topología en estrella no permite el tráfico directo de dispositivos. El controlador actúa como un intercambiador: si un dispositivo quiere enviar datos a otro, envía los datos al controlador, que los retransmite al dispositivo final (véase la Figura 9).

Una topología en estrella es más barata que una topología en malla. En una estrella, cada dispositivo necesita solamente un enlace y un puerto de entrada/salida para conectarse a cualquier número de dispositivos. Este factor hace que también sea más fácil de instalar y reconfigurar. Además es necesario instalar menos cables y la conexión, desconexión y traslado de dispositivos afecta solamente a una conexión: la que existe entre el dispositivo y el concentrador. Otra ventaja de esta red es su robustez. Si falla un enlace, solamente este enlace se verá afectado. Todos los demás enlaces permanecen activos.

Este factor permite también identificar y aislar los fallos de una forma muy sencilla. Mientras funcione el concentrador, se puede usar como monitor para controlar los posibles problemas de los enlaces y para puentear los enlaces con defectos. Una gran desventaja de la topología en estrella es la dependencia que toda la topología tiene de un punto único, el concentrador. Si el concentrador falla, toda la red muere.

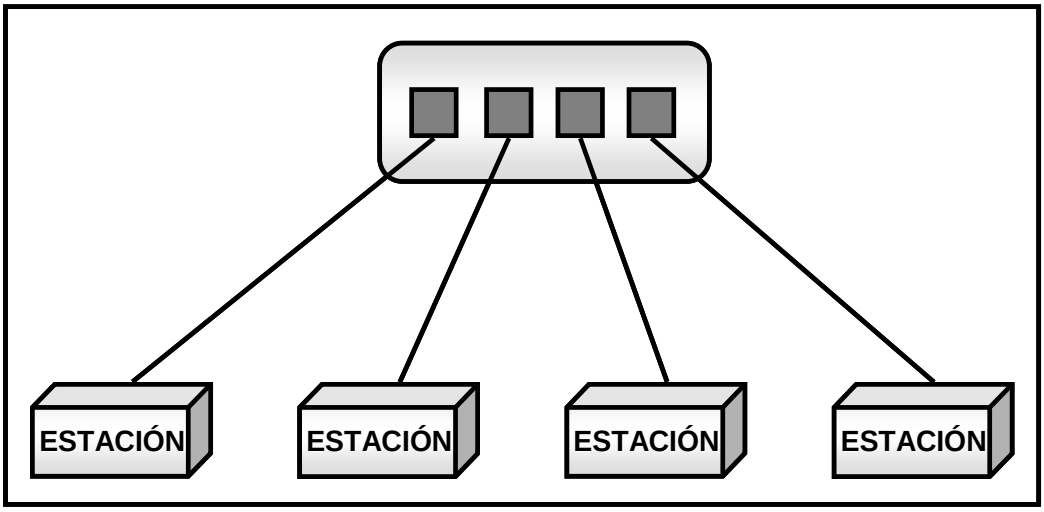

Figura 9. Una topología en estrella conectando cuatro estaciones.
Fuente: Forouzan, B., (2006)

Sin embargo, aunque una estrella necesita menos cable que una malla, cada nodo debe estar enlazado al nodo central. Por esta razón, en la estrella se requiere más cable que en otras topologías de red (como el árbol, el anillo o el bus). La topología en estrella se usa en redes de área local (LAN), las redes LAN de alta velocidad usan a menudo una topología en estrella con un concentrador central.

Topología de bus. Todos los ejemplos anteriores describen configuraciones punto a punto. Sin embargo, una topología de bus es multipunto. Un cable largo actúa como una red troncal que conecta todos los dispositivos en la red (véase la Figura 10). Los nodos se conectan al bus mediante cables de conexión (latiguillos) y sondas. Un cable de conexión es una conexión que va desde el dispositivo al cable principal. Una sonda es un conector que, o bien se conecta al cable principal, o se pincha en el cable

para crear un contacto con el núcleo metálico. Cuando las señales viajan a través de la red troncal, parte de su energía se transforma en calor, por lo que la señal se debilita a medida que viaja por el cable. Por esta razón, hay un límite en el número de conexiones que un bus puede soportar y en la distancia entre estas conexiones.

Entre las ventajas de la topología de bus se incluye la sencillez de instalación. El cable troncal puede tenderse por el camino más eficiente y, después, los nodos se pueden conectar al mismo mediante líneas de conexión de longitud variable. De esta forma se puede conseguir que un bus use menos cable que una malla, una estrella o una topología en árbol.

Por ejemplo, en una estrella cuatro dispositivos situados en la misma habitación necesitarían cuatro cables de longitud suficiente para recorrer todo el camino hasta el concentrador. Un bus elimina esta redundancia, solamente el cable troncal se extiende por toda la habitación. Cada línea de conexión únicamente tiene que ir hasta el punto del troncal más cercano.

Entre sus desventajas se incluye lo dificultoso de su reconfiguración y del aislamiento de los fallos. Habitualmente, los buses se diseñan para tener una eficiencia óptima cuando se instalan. Por tanto, puede ser difícil añadir nuevos dispositivos. Como se dijo anteriormente, la reflexión de la señal en los conectores puede causar degradación de su calidad. Esta degradación se puede controlar limitando el número y el espacio de los dispositivos conectados a una determinada longitud de cable. Añadir nuevos dispositivos puede obligar a modificar o reemplazar el cable troncal.

Además, un fallo o rotura en el cable del bus interrumpe todas las transmisiones, incluso entre dispositivos que están en la parte de red que no falla. Esto se debe a que el área dañada refleja las señales hacia la dirección del origen, creando ruido en ambas direcciones.

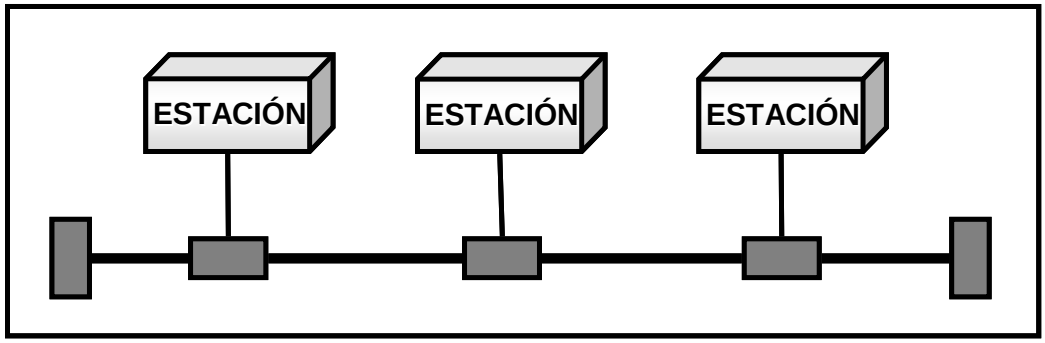

Figura 10. Topología de bus que conecta tres estaciones.
Fuente: Forouzan, B., (2006)

Topología en anillo. En una topología en anillo cada dispositivo tiene una línea de conexión dedicada y punto a punto solamente con los dos dispositivos que están a sus lados. La señal pasa a lo largo del anillo en una dirección, o de dispositivo a dispositivo, hasta que alcanza su destino. Cada dispositivo del anillo incorpora un repetidor. Cuando un dispositivo recibe una señal para otro dispositivo, su repetidor regenera los bits y los retransmite al anillo (véase la Figura 11).

Un anillo es relativamente fácil de instalar y reconfigurar. Cada dispositivo está enlazado solamente a sus vecinos inmediatos (bien físicos o lógicos). Para añadir o quitar dispositivos, solamente hay que mover dos conexiones.

Las únicas restricciones están relacionadas con aspectos del medio físico y el tráfico (máxima longitud del anillo y número de dispositivos).

Además, los fallos se pueden aislar de forma sencilla. Generalmente, en un anillo hay una señal en circulación continuamente. Si un dispositivo no recibe una señal en un período de tiempo especificado, puede emitir una alarma. La alarma alerta al operador de red de la existencia del problema y de su localización.

Sin embargo, el tráfico unidireccional puede ser una desventaja. En anillos sencillos, una rotura del anillo (como por ejemplo una estación inactiva) puede inhabilitar toda la red. Esta debilidad se puede resolver usando un anillo dual o un conmutador capaz de puentear la rotura. La topología en anillo fue usada por IBM en sus redes de área local Token Ring. Actualmente, la necesidad de LAN de alta velocidad ha hecho esta topología menos popular.

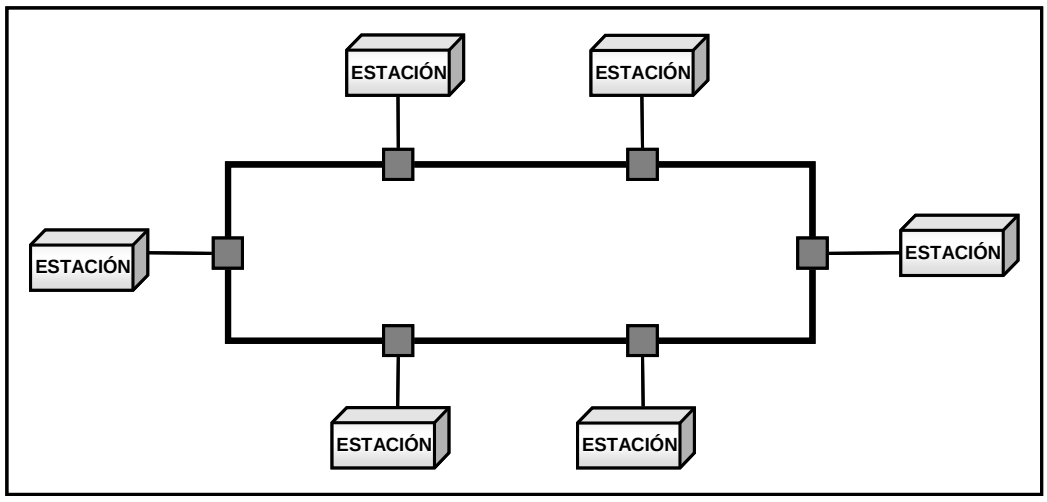

Figura 11. Topología en anillo que conecta seis estaciones.
Fuente: Forouzan, B., (2006)

Topologías híbridas Una red puede ser híbrida. Por ejemplo, se puede tener una topología en estrella en la que cada rama conecta varias estaciones usando topología de bus, como se muestra en la Figura 12.

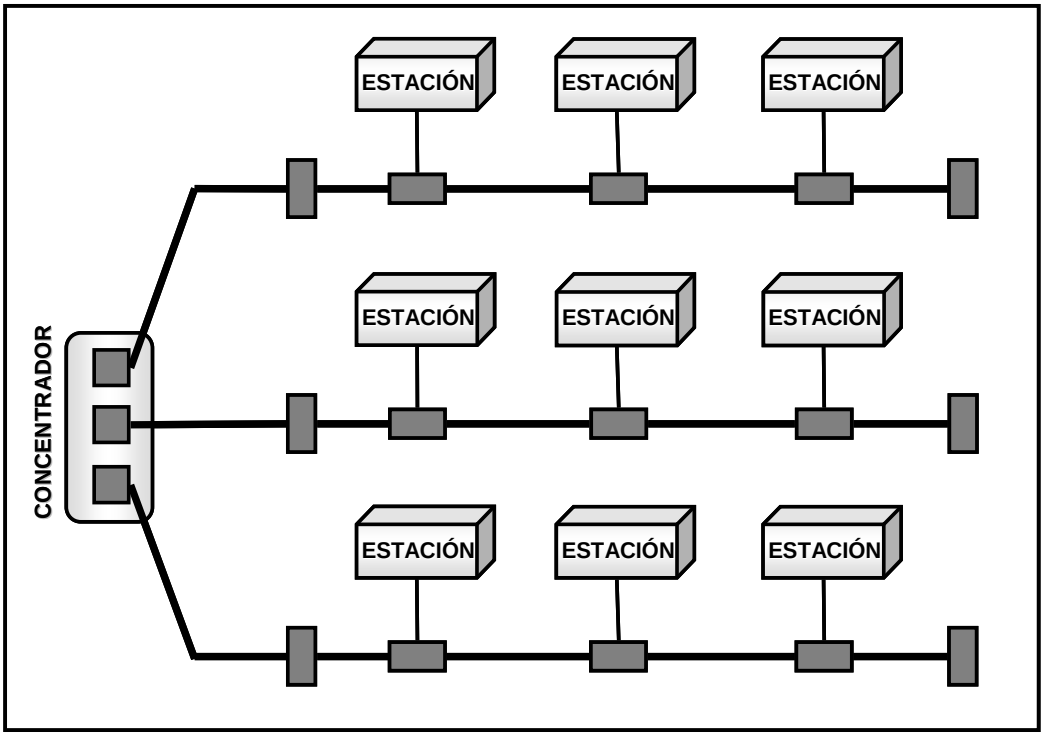

Figura 12. Topología híbrida.
Fuente: Forouzan, B., (2006)

2.6.3.- MODELOS DE REDES

Las redes de computadoras están formadas por distintas entidades. Se necesitan estándares de forma que estas redes heterogéneas se puedan comunicar entre sí. Los dos estándares más conocidos son el modelo OSI y el modelo de Internet. El modelo Open Systems Interconnection (OSI) define una red de siete niveles; el modelo de Internet define una red de cinco

niveles. Este libro se basa en el modelo de Internet con referencias ocasionales al modelo OSI.

Actualmente, cuando se habla de redes, se suele hablar de dos clases principales: redes de área local y redes de área extendida. La categoría a la que pertenece una red se determina por su tamaño. Una LAN cubre normalmente un área menor de 3 km.; una WAN puede extenderse a nivel normal. Las redes de tamaño intermedio se denominan habitualmente redes de área metropolitana y se extienden decenas de kilómetros.

Red de área local (LAN). Una red de área local suele ser una red de propiedad privada y conectar enlaces de una única oficina, edificio o campus (véase la Figura 13). Dependiendo de las necesidades de la organización donde se instale y del tipo de tecnología utilizada, una LAN puede ser tan sencilla como dos PC y una impresora situadas en la oficina de la casa de alguien; o se puede extender por toda una empresa e incluir periféricos de voz, sonido y vídeo. Actualmente, el tamaño de las LAN está limitado a unos pocos kilómetros.

Las LAN están diseñadas para permitir compartir recursos entre computadoras personales o estaciones de trabajo. Los recursos a compartir pueden incluir hardware (por ejemplo, una impresora), software (por ejemplo, un programa de aplicación) o datos. Un ejemplo frecuente de LAN, que se encuentra en muchos entornos de negocios, enlaza un grupo de trabajo de computadoras relacionadas con una cierta tarea, como, por ejemplo, estaciones de trabajo de ingeniería o PC de contabilidad. Una de las

computadoras puede tener un disco de gran capacidad y convertirse en servidora de los otros clientes. El software se puede almacenar en este servidor central para que sea usado por todo el grupo según las necesidades de cada miembro. En este ejemplo, el tamaño de la LAN puede estar determinado por restricciones en el número de licencias, por el número de usuarios, por copia de software o por restricciones en el número de usuarios con licencia para acceder al sistema operativo.

Además del tamaño, las LAN se distinguen de otros tipos de redes por su medio de transmisión y su topología. En general, una LAN determinada usará un único medio de transmisión. Las topologías más frecuentes de las LAN son el bus, el anillo y la estrella. Las primeras LAN tenían tasas de datos en un rango de entre 4 y 16 megabits por segundo (Mbps). Sin embargo, actualmente las velocidades se han incrementado y pueden alcanzar los 100 o 1000 Mbps.

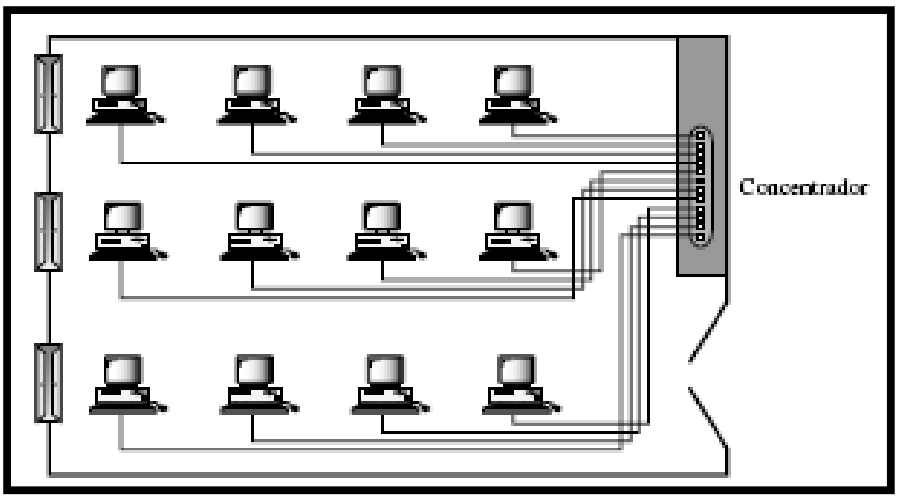

Figura 13. LAN que conecta 12 computadores a un concentrador.
Fuente: Forouzan, B., (2006)

Red de área amplia (WAN). Una red de área amplia proporciona un medio de transmisión a larga distancia de datos, voz, imágenes e información de vídeo sobre grandes áreas geográficas que pueden extenderse a un país, un continente o incluso al mundo entero. Una WAN puede ser tan compleja como las troncales que conectan Internet o tan simple como la línea telefónica que conecta una computadora casera a Internet. Normalmente se denomina a la primera WAN conmutada y a la segunda WAN punto a punto (ver Figura 14).

La WAN conmutada conecta los sistemas terminales, que habitualmente incluyen un enrutador (dispositivo de conexión entre redes) que conecta a otra LAN o WAN. La WAN punto a punto es normalmente una línea alquilada a un proveedor de telefonía o TV por cable que conecta una computadora casera a una LAN pequeña o a un proveedor de servicios de Internet (ISP, Internet Service Provider). Este tipo de WAN se usa a menudo para proporcionar acceso a Internet.

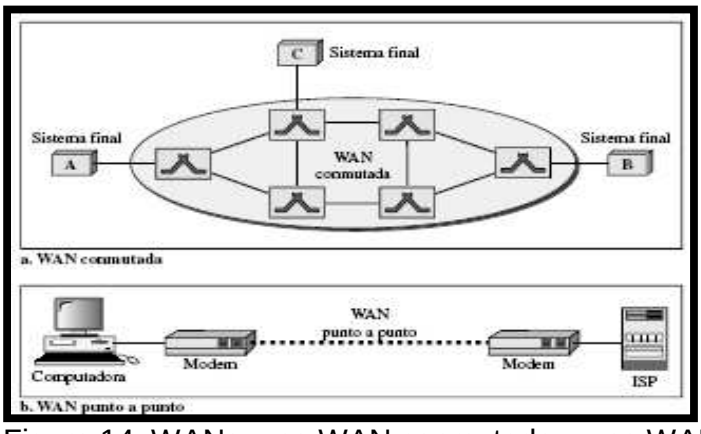

Figura 14. WANs: una WAN conmutada y una WAN punto a punto.
Fuente: Forouzan, B., (2006)

Un ejemplo temprano de una WAN conmutada es X.25, una red diseñada para proporcionar conectividad entre usuarios finales. Como veremos en el Capítulo 18, X.25 está siendo gradualmente reemplazada por una red de alta velocidad más eficiente denominada Retransmisión de Tramas (Frame Relay). Un buen ejemplo de WAN conmutada es la red ATM (Asynchronous Transfer Mode), una red con paquetes de tamaños fijos denominados celdas.

Redes de área metropolitana (MAN). La red de área metropolitana tiene un tamaño intermedio entre una LAN y una WAN. Normalmente cubre el área de una ciudad. Está diseñada para clientes que necesitan una conectividad de alta velocidad, normalmente a Internet, y tiene puntos de conexión extendidos por la ciudad o parte de ella. Un buen ejemplo de MAN es la parte de red de una compañía telefónica que puede producir una línea DSL a los clientes. Otro ejemplo es la red de TV por cable, diseñada originalmente para la TV por cable, y usada para conexiones de alta velocidad a Internet.

2.6.4.- INTERCONEXIÓN DE REDES (INTERREDES)

Actualmente es muy raro ver una LAN, WAN o MAN aislada; están conectadas entre sí. Cuando dos o más redes se conectan, se convierten en una inter-red, o Internet. Por ejemplo, suponga que una organización tiene dos oficinas, una en la costa este de EE.UU. y otra en la costa oeste. La de la costa oeste tiene una LAN con topología de bus; la nueva oficina de la costa este tiene una LAN con topología de estrella. El presidente de la compañía vive en algún lugar entre ambas oficinas y controla la compañía

desde casa. Para crear una WAN troncal que conecte estas tres entidades (dos LAN y la computadora del presidente), se ha alquilado una WAN conmutada (operada por un proveedor de servicios como una compañía telefónica). Sin embargo, para conectar las LAN a esta WAN conmutada se necesitan tres WAN punto a punto. Estas WAN punto a punto pueden ser líneas DSL de alta velocidad ofrecidas por una compañía telefónica o una línea de MODEM por cable ofrecida por un operador de TV por cable, como se muestra en la Figura 15.

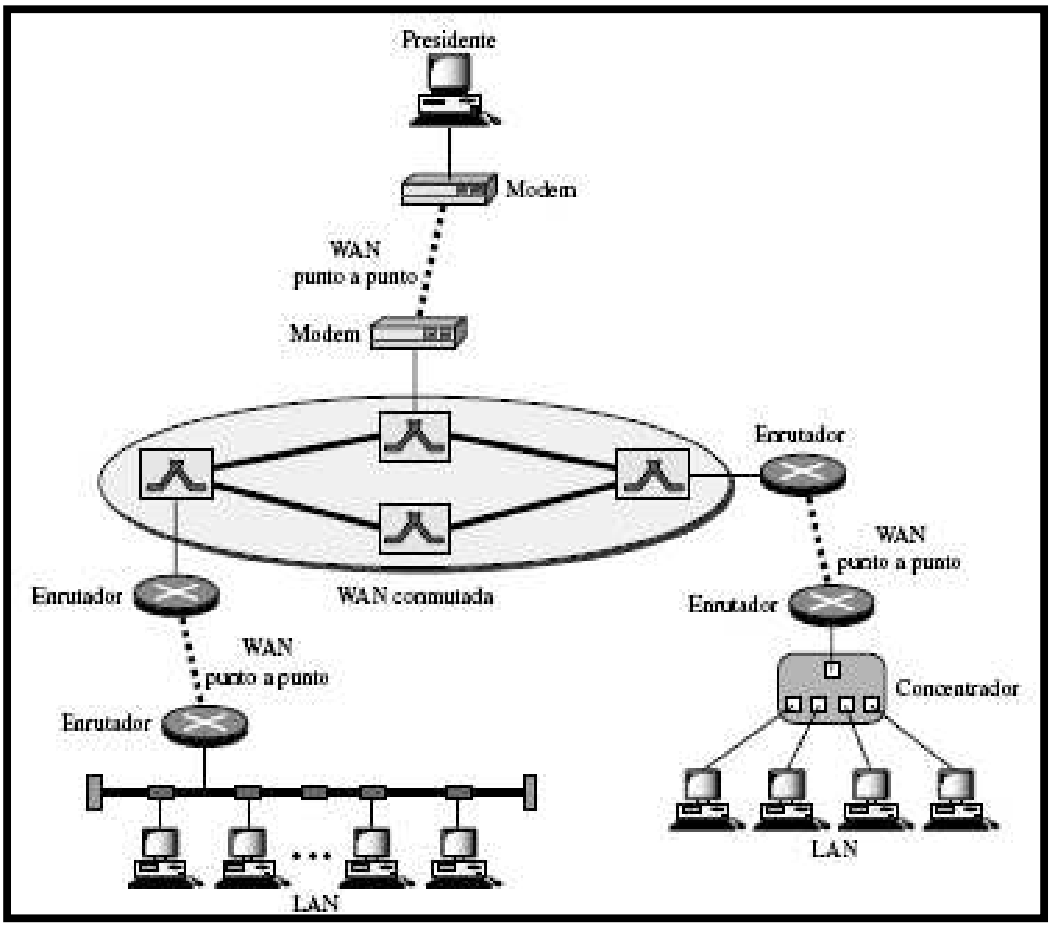

Figura 15. Una red heterogénea por cuatro WAN y dos LAN.
Fuente: Forouzan, B., (2006)

2.7.- VENTAJAS Y DESVENTAJAS DE LOS TIPOS DE REDES

Stallings, W. (2004) explica las siguientes ventajas y desventajas como se presenta a continuación:

VENTAJAS

Una LAN da la posibilidad de que los PC's compartan entre ellos programas, información, recursos entre otros. La máquina conectada (PC) cambia continuamente, así que permite que sea innovador este proceso y que se incremente sus recursos y capacidades.

Las WAN pueden utilizar un software especializado para incluir mini y macrocomputadoras como elementos de red. Las WAN no esta limitada a espacio geográfico para establecer comunicación entre PC's o mini o macrocomputadoras. Puede llegar a utilizar enlaces de satélites, fibra óptica, aparatos de rayos infrarrojos y de enlaces.

DESVENTAJAS

Para que ocurra el proceso de intercambiar la información los PC's deben estar cerca geográficamente. Solo pueden conectar PC's o microcomputadoras.

Los equipos deben poseer gran capacidad de memoria, si se quiere que el acceso sea rápido. Poca seguridad en las computadoras (infección de virus, eliminación de programas, entre otros).

2.8.- ENLACES INALÁMBRICOS

Sidnie (2000) mantiene que el servicio de enlaces inalámbricos consiste en ofrecer al cliente acceso ilimitado a Internet mediante una conexión sin hilos por medio de antenas, que le permiten utilizar un ancho de banda desde 64K hasta 2Mbps.

Trabajan por medio de radio frecuencia, desde 2Db de ganancia hasta 24 Db. Pueden transmitir en un radio inicial de 7° hasta 360°, dependiendo el estilo de la red (Tecnologías Omnidireccionales y Unidireccionales) y enlazan desde una pc hasta una red entera, creando una Intranet.

2.9.- REDES INALÁMBRICAS

Bates (2002) explica la importancia de conocer que una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada.

Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. También es útil para hacer posibles sistemas basados en plumas. Pero la realidad es que esta tecnología está todavía en pañales y se deben resolver varios obstáculos

técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen la velocidad máxima de transmisión de la tecnología 802.11b es de 11 Mbps.

Pero la velocidad típica es solo la mitad: entre 1,5 y 5 Mbps dependiendo de si se transmiten muchos archivos pequeños o unos pocos archivos grandes. La velocidad máxima de la tecnología 802.11g es de 54 Mbps. Pero la velocidad típica de esta última tecnología es solo unas 3 veces más rápida que la de 802.11b: entre 5 y 15 Mbps.

Sin embargo, es totalmente viable mezclar las redes cableadas y las inalámbricas, y de esta manera generar una “Red Híbrida” y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina. Existen dos amplias categorías de Redes Inalámbricas:

De Larga Distancia. Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.

De Corta Distancia. Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si, con velocidades del orden de 280 Kbps hasta los dos Mbps.

En síntesis una red inalámbrica es aquella que posibilita la conexión de dos o más equipos entre sí, sin que intervengan cables. Es una red que permite a los usuarios conectarse a una red local o a Internet sin estar conectado físicamente, no hace falta tener una toma de red o de teléfono. La comunicación se realiza a través de ondas que viajan por el aire, sin necesidad de cables.

Ahora bien, para iniciar la referencia de los objetivos específicos de la investigación, se indica que, con relación a las ventajas de utilizar una red inalámbrica para un modelo de optimización a través de interconexión de redes, en este caso la zona educativa del estado Trujillo, las principales son:

Facilidad de Instalación. La administración por Web es sencilla y la instalación de los equipos y de las tarjetas también es muy sencilla.

Movilidad. Las redes tienen un rango de aproximadamente 10 metros alrededor de donde esta ubicado el punto de acceso. Sin embargo, las paredes disminuyen la intensidad de la señal. Las redes inalámbricas proporcionan a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de la organización o el entorno público (zona limitada) en el que están desplegadas.

Facilidad de configuración para el usuario. La persona que se va a conectar a la red solo tiene que poner la llave de acceso en caso de que se tenga alguna seguridad configurada, si la red esta abierta no es necesario configurar nada, pues la tarjeta detecta la red automáticamente.

Costo de propiedad reducido. Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una LAN, la inversión de toda la instalación y el costo durante el ciclo de vida puede ser significativamente inferior.

Los beneficios a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes. Es la solución más segura a la hora de proteger la información que se transmite frente a posibles intrusos que deseen descifrar la información transmitida.

Fácilmente ampliable. Tan sólo es necesario insertar una tarjeta en el ordenador del usuario, configurarlo y listo. No es necesario instalar una toma de red adicional. Olvídese de las canaletas o de obras. Si dispone de almacenes sus encargados podrán gestionarlos cómodamente con un dispositivo portátil, sin necesidad de ir a buscar un ordenador.

Comunicación punto a punto. Es posible comunicarse entre varios equipos directamente sin necesidad de un engorroso cableado que los una, las ondas serán la vía de conexión entre los ordenadores. Si además queremos que la red tenga acceso a Internet, tendremos que dotarla de una puerta de enlace, comúnmente se trata de un router.

Instalación rápida y costes mínimos. Hoy en día montar una red inalámbrica es un procedimiento bastante económico y al alcance de cualquiera. Simplemente necesitaremos unos accesorios wifi, generalmente en forma de tarjetas PCI, y un punto de acceso inalámbrico para la conexión a Internet. Además, conservan compatibilidad con redes cableadas simplemente usando unos puntos de acceso compatibles con ambas tecnologías.

Configuración simple. La configuración general es muy sencilla, es decir, incluso que de una dificultad equiparable a la red tradicional cableada, sumando el hecho de configurar un extra, la seguridad de la red (WEP y demás).

Escalabilidad. Los sistemas de WLAN pueden ser configurados e una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red.

2.10.- VENTAJAS DE LAS REDES INALÁMBRICAS

Bates (2002) sostiene que las principales ventajas que ofrecen las redes inalámbricas frente a las redes cableadas son las siguientes:

Movilidad. La libertad de movimientos es uno de los beneficios más evidentes las redes inalámbricas. Un ordenador o cualquier otro dispositivo (por ejemplo, una PDA o una webcam) pueden situarse en cualquier punto dentro del área de cobertura de la red sin tener que depender de que si es

posible o no hacer llegar un cable hasta este sitio. Ya no es necesario estar atado a un cable para navegar en Internet, imprimir un documento o acceder a los recursos.

Compartidos desde cualquier lugar de ella, hacer presentaciones en la sala de reuniones, acceder a archivos, etc., sin tener que tender cables por mitad de la sala o depender de si el cable de red es o no suficientemente largo.

Desplazamiento. Con una computadora portátil o PDA no solo se puede acceder a Internet o a cualquier otro recurso de la red local desde cualquier parte de la oficina o de la casa, sino que nos podemos desplazar sin perder la comunicación. Esto no solo da cierta comodidad, sino que facilita el trabajo en determinadas tareas, como, por ejemplo, la de aquellos empleados cuyo trabajo les lleva a moverse por todo el edifico.

Flexibilidad. Las redes inalámbricas no solo nos permiten estar conectados mientras nos desplazamos por una computadora portátil, sino que también nos permite colocar una computadora de sobremesa en cualquier lugar sin tener que hacer el más mínimo cambio de configuración de la red. A veces extender una red cableada no es una tarea fácil ni barata.

En muchas ocasiones se colocan peligrosos cables por el suelo para evitar tener que hacer la obra de poner enchufes de red más cercanos. Las redes inalámbricas evitan todos estos problemas. Resulta también especialmente indicado para aquellos lugares en los que se necesitan accesos esporádicos.

Si en un momento dado existe la necesidad de que varias personas se conecten en la red en la sala de reuniones, la conexión inalámbrica evita llenar el suelo de cables. En sitios donde pueda haber invitados que necesiten conexión a Internet (centros de formación, hoteles, cafés, entornos de negocio o empresariales) las redes inalámbricas suponen una alternativa mucho mas viable que las redes cableadas.

Ahorro de costes. Diseñar o instalar una red cableada puede llegar a alcanzar un alto coste, no solamente económico, sino en tiempo y molestias. En entornos domésticos y en determinados entornos empresariales donde no se dispone de una red cableada por que su instalación presenta problemas, la instalación de una red inalámbrica permite ahorrar costes al permitir compartir recursos: acceso a Internet, impresoras, etc.

Escalabilidad. Se le llama escalabilidad a la facilidad de expandir la red después de su instalación inicial. Conectar una nueva computadora cuando se dispone de una red inalámbrica es algo tan sencillo como instalarle una tarjeta y listo. Con las redes cableadas esto mismo requiere instalar un nuevo cableado o lo que es peor, esperar hasta que el nuevo cableado quede instalado.

2.11.- CONSIDERACIONES DEL DISEÑO DE RED INALÁMBRICA

Vnunet (2002) sugiere la realización del diseño de la red inalámbrica que como paso previo a la aplicación de medidas de protección de una red sin

hilos, es importante diseñar la red de forma correcta. Algunas medidas básicas a implementar son:

Establecer redes privadas virtuales (VPN), a nivel de cortafuegos, para la encriptación del tráfico de la red inalámbrica.

No deben conectarse directamente a la red interna clásica de la empresa. Las redes inalámbricas deben recibir el mismo trato que cualquier otra red insegura, como puede ser la conexión a Internet. Por tanto, entre la red inalámbrica y la red clásica deberá existir un corta fuegos y mecanismos de autenticación.

Como ampliación del punto anterior, no deben colocarse detrás del corta fuegos.

Los clientes de las redes inalámbricas deben acceder a la red utilizando mecanismos tales como Secure Shell (SSH), redes privadas virtuales (VPN) o IPSec. Estos mecanismos facilitan los mínimos necesarios en lo referente a la autorización, autenticación y encriptación del tráfico.

En lo que tiene que ver con el aspecto de la seguridad en las redes inalámbricas, el mismo se inicia brindando una breve introducción al modelo, y conceptos claves de seguridad. Pero antes de introducir las ideas de seguridad inalámbrica en el contexto de IEEE 802.11 o WLAN. Se aborda la seguridad en el contexto de la seguridad de información y se describen y evalúan cinco atributos de seguridad (confidencialidad, autenticación, integridad, no-repudio y disponibilidad).

El estudio se enfoca en dar una imagen de la seguridad inalámbrica dentro de un contexto amplio de seguridad de la información. Además, se consideran elementos claves de seguridad que deben ser abordados en la fase de diseño de una red inalámbrica.

2.12.- SEGURIDAD EN REDES INALÁMBRICAS

Escudero (2007) sostiene que se aborda la seguridad en el contexto de la seguridad de información y se describen y evalúan cinco atributos de seguridad (confidencialidad, autenticación, integridad, no-repudio y disponibilidad). La unidad se enfoca en dar una imagen de la seguridad inalámbrica dentro de un contexto amplio de seguridad de la información.

Busca lograr un entendimiento acerca de dónde construir la seguridad en cada capa de la pila de protocolos OSI/TCP/IP. Además, considera elementos claves de seguridad que deben ser abordados en la fase de diseño de una red inalámbrica.

Seguridad Inalámbrica. La definición de seguridad es en gran medida específica al contexto; la palabra seguridad abarca un rango amplio de campos dentro y fuera del ámbito de la computación. Hablamos de seguridad cuando se describen medidas de seguridad en la carretera o cuando se describe una nueva plataforma de cómputo que es segura contra virus.

Se han desarrollado varias disciplinas para abordar cada aspecto de seguridad. Con esto en mente, se ha intentado enmarcar el término seguridad inalámbrica, en el contexto de seguridad de información. Cuando

hablamos de seguridad inalámbrica de hecho estamos hablando de seguridad de información en redes inalámbricas.

Seguridad de la Información. Para entender el significado de Seguridad Informática es necesario entender la manera en que el término ha evolucionado en el tiempo. Hasta fines de los años 70, esta área de seguridad fue referida como Seguridad de comunicaciones. Seguridad de Comunicaciones o COMSEC, por un acrónimo en inglés, fue definido por la U.S. Security Telecommunications and Information Systems Security Instruction (NSTISSI) como:

Medidas y controles que se toman para negar el acceso no autorizado de personas a información derivada de las telecomunicaciones y augurar la autenticidad de tales telecomunicaciones.

Es recomendable incluir algunas áreas como partes de las actividades de seguridad en el diseño de la red inalámbrica propuesta Seguridad de Transmisiones, Seguridad de Emisiones y Seguridad física. La seguridad incluye cuatro atributos: Confidencialidad, Autenticación, Integridad y Disponibilidad.

Confidencialidad. Asegurar que la información no es divulgada a personas no autorizadas, procesos o dispositivos. (Protección contra divulgación no autorizada).

Autenticación. Medida de seguridad diseñada para establecer la validez de una transmisión, mensaje o remitente, o un medio para verificar la autorización de un individuo para recibir categorías específicas de

información (Verificación de emisor). En los 80's con el crecimiento de las computadoras personales se inició una nueva era: Computación personal, y la seguridad aplicada a este campo (COMPUSEC). COMPUSEC fue definido por NSTISSI como:

Medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de sistemas de información incluyendo hardware, software, firmware e información que está siendo procesada, almacenada y comunicada.

Integridad. La calidad de un sistema de información refleja el correcto funcionamiento y confiabilidad de sistema operativo, la coherencia del hardware y software que implementan los sistemas de protección y la consistencia de las estructuras de datos de la información almacenada.

Disponibilidad. Se relaciona con el acceso oportuno y confiable a datos y servicios de información para usuarios autorizados.

Finalmente en los años 90, las dos eras de la información, COMSEC y COMPUSEC, fueron integradas para formar Seguridad en Sistemas de Información (INFOSEC). INFOSEC incluyó los cuatro atributos descritos: Confidencialidad, Autenticación, Integridad y Disponibilidad, pero también se agregó un nuevo atributo: No-repudio (non-repudiation).

No Repudiación (Rendición De Cuentas). Asegurar que el remitente de información es provisto de una prueba de envío y que el receptor es provisto de una prueba de la identidad del remitente, de manera que ninguna de las partes puede negar el proceso de dicha información.

Seguridad de Información y las Wlan. La NSTISSI define el concepto de Seguridad de Sistemas de información como: La protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea en el medio de almacenaje, procesamiento o tránsito, y contra la negación de servicio a los usuarios autorizados, o la provisión de servicio a usuarios no autorizados, incluyendo las medidas necesarias para detectar, documentar y contabilizar esas amenazas.

La seguridad inalámbrica se presenta desde el punto de vista de la seguridad de los sistemas de información o INFOSEC. Es muy común describir, en la literatura relacionada con la seguridad WLAN, aspectos prominentes de seguridad sin dar un marco de seguridad apropiado. Al describir aspectos prominentes el lector tiende a recordar acrónimos pero olvida el beneficio de cada prominencia.

Para evitar eso, se listan todos los atributos de seguridad que se presentan en WLAN, para presentar cada uno de los cinco atributos de seguridad de INFOSEC, y luego discutir la manera en que WLAN implementa cada uno de estos casos. Este acercamiento ayuda al autor de la presente investigación a tener un enfoque metodológico al diseñar redes inalámbricas seguras.

Atributos de Seguridad. El modelo de referencia OSI (Interconexión abierta de sistemas), creado por la ISO (organización internacional de estándares), es una descripción abstracta para diseño de protocolos de redes de cómputo.

El modelo divide las diferentes funciones de comunicación en siete capas que pueden funcionar de manera independiente una de otra.

Así como se describe en las redes avanzadas, el diseño de protocolos de la OSI sigue el principio de pila. Al tener un modelo de protocolos en capas o apilado implica que cada capa usa únicamente la funcionalidad de la capa inferior, y provee funcionalidad exclusivamente a la capa inmediata superior.

Este enfoque en capas tiene implicaciones directas en la manera en que se puede implementar atributos de seguridad. Los estándares de redes inalámbricas se refieren, normalmente, a la capa 1 y capa 2 de la pila de protocolos OSI, conservando el paquete IP sin cambios. Los paquetes IP se transportan sobre protocolos del nivel físico y de enlace de datos que son específicamente de carácter inalámbricos. Por ejemplo, si consideramos la confidencialidad del tráfico de datos entre dos puntos de acceso, podemos lograr resultados similares (protección de la información) actuando en tres capas diferentes:

La capa de aplicación. (mediante TLS/SSL)

La capa IP. (mediante IPSEC)

La capa de enlace. (mediante cifrado)

Es necesario recordar que cuando hablamos de seguridad inalámbrica, sólo se está examinando los mecanismos de seguridad en las capas 1 y 2, o sea, del cifrado (nivel de enlace). Otros mecanismos de seguridad presentes a nivel 3 y superiores son parte de la seguridad implementada en las capas de red o de aplicación.

Confidencialidad en Redes Inalámbricas. Se define la confidencialidad en redes inalámbricas como el acto de asegurar que la información transmitida entre los puntos de acceso y los clientes no sea revelada a personas no autorizadas. La confidencialidad debe asegurar que ya sea la comunicación entre un grupo de puntos de acceso en un sistema de distribución inalámbrico (WDS por sus siglas en inglés), o bien entre un punto de acceso (AP) y una estación o cliente, se conserva protegida contra intercepciones. A continuación se presentan las recomendaciones para confidencialidad en datos:

Si se necesita confidencialidad mediante el cifrado a nivel de enlace: la mejor opción es WPA2 en modo “corporativo” (WPA2-Enterprise”). En caso de usarse una solución más simple como la WPA2-Personal, deben tomarse precauciones especiales al escoger una contraseña (llave pre-compartida, PSK). El protocolo WEP y sus variantes WEP+, y WEP2, deben ser descartados.

Autenticación en redes inalámbricas. En el contexto de las redes LAN, la autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas En otros términos, la autenticación inalámbrica significa el derecho a enviar hacia y mediante el punto de acceso.

Para entender autenticación en redes inalámbricas, es necesario entender qué sucede en el inicio de la sesión de comunicación entre un punto de acceso y una estación inalámbrica. El inicio de una comunicación comienza

por un proceso llamado asociación. Cuando el estándar IEEE 802.11b fue diseñado, se introdujeron dos mecanismos de asociación: Autenticación abierta y Autenticación con llave compartida

La autenticación abierta implica NO seguridad y cualquiera puede hablarle al punto de acceso. En la autenticación de llave compartida, se comparte una contraseña entre el punto de acceso y la estación cliente. Un mecanismo de reto/respuesta le permite al punto de acceso verificar que el cliente conoce la llave compartida, y entonces concede el acceso.

A continuación se presentan las recomendaciones de autenticación inalámbrica:

La Autenticación inalámbrica mediante la capa 2 requiere el uso del modo WPA2-corporativo.

La Autenticación en las redes inalámbricas, como las implantadas por los proveedores de servicios inalámbricos, normalmente se utiliza en capas de red mas altas (capa IP) mediante portales cautivos (que requieren identificarse ante un sitio web).

Direcciones MAC como medida de seguridad. Se ha convertido en práctica común usar la dirección MAC de la interfaz inalámbrica como mecanismo para limitar el acceso a una red inalámbrica. La hipótesis detrás de esto es que las direcciones MAC están alambradas y no pueden ser modificadas por usuarios corrientes. La realidad es muy diferente y las direcciones MAC, en el común de las redes inalámbricas pueden ser fácilmente modificadas.

Portales cautivos para redes inalámbricas. La discusión acerca de los portales cautivos o inalámbrico" merece una unidad completa, pero al menos haremos una pequeña introducción en esta unidad, dada su relevancia en seguridad inalámbrica. Si bien hay varias implementaciones de portales cautivos, la mayoría de estos están basados en el mismo tipo de concepto.

En una red donde la Autenticación se hace mediante portales cautivos, a los clientes se les permite asociar con un punto de acceso (sin Autenticación inalámbrica) y obtener una dirección IP con el protocolo DHCP (no se requiere Autenticación para obtener la dirección IP).

Una vez que el cliente obtiene la dirección IP, todas las solicitudes HTTP se capturan y son enviadas al portal cautivo, y el cliente es forzado a identificarse en una página Web. Los portales cautivos son responsables de verificar la validez de la contraseña y luego modificar el estatus del cortafuego. Las reglas del cortafuego esta comúnmente basadas en la dirección MAC del cliente y las direcciones IP.

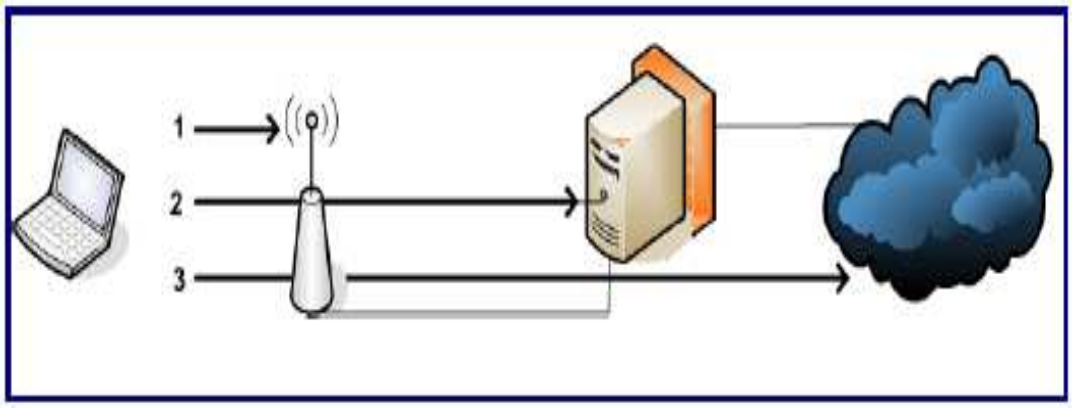

Figura 16. Portal cautivo con Autenticación en tres pasos.
Fuente: Escudero A. (2007)

En la figura 16, se observa la Autenticación del portal cautivo en tres pasos. El primer paso (1) requiere una asociación del cliente a la red inalámbrica. No se espera una Autenticación en términos de WEPWPA, y normalmente se anuncia la SSID. En el segundo paso (2) el cliente obtiene una dirección IP mediante DHCP. El tráfico se enlaza a través del punto de acceso sin Autenticación alguna.

En el último paso (3), el tráfico HTTP del cliente se redirecciona, al servidor del portal cautivo. El cliente se identifica (usando normalmente: HTTPS + nombre + contraseña). Finalmente el servidor del portal cautivo modifica o crea una regla en el cortafuego para permitir el tráfico hacia la Internet.

Integridad de datos en redes inalámbricas. Definimos integridad de datos como la capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas. En 1999, el protocolo WEP también buscó proveer integridad de tráfico de datos, pero desafortunadamente el mecanismo de integridad, o CRC (código de redundancia cíclica), resultó inseguro.

Disponibilidad en redes inalámbricas. Se define disponibilidad de la red inalámbrica como la capacidad de la tecnología que asegura un acceso confiable a servicios de datos e información para usuarios autorizados. Lo primero a considerar es que no es simple detener a alguien que busca interferir con su señal de radio.

Negación de servicio. Las redes inalámbricas son vulnerables a los ataques de Negación de Servicio mediante interferencia de radio. Considere un escenario donde otro operador de red decide configurar sus dispositivos de radio en el mismo canal en el que opera su red. Puede imaginar además qué sucede si se publica un SSID idéntico.

Para evitar esta clase de ataques, intencionales o no, debe considerar el rastreo periódico de frecuencias de radio. Para evitar la interferencia con otras redes, no sobrecargue la potencia de sus enlaces. Existen varias razones para que un enlace de desempeñe de manera deficiente o no esté disponible.

No repudiación en redes inalámbricas (rendición de cuentas). La familia de estándares en las redes inalámbricas no se hace cargo de la “rendición de cuentas” en el tráfico de datos. Los protocolos inalámbricos no tienen un mecanismo para asegurar que el emisor de datos tenga una prueba de envío de la información y que el receptor obtenga una prueba de la identidad del emisor. La rendición de cuentas debe ser implementada en protocolos de capas superiores.

2.13.- ADMINISTRACIÓN DE LA RED INALÁMBRICA

En un estudio reciente Joskowicz (2007) plantea que la administración de redes incluye las tareas de diseño, integración y coordinación de los equipos de hardware, los programas de software y los recursos humanos necesarios

para monitorear, testear, configurar, analizar, evaluar y controlar la red y sus recursos a los efectos de lograr la calidad de servicio requerida.

Desde el punto de vista corporativo, las tareas de administración de redes deben basarse en obtener en forma predecible y consistente una calidad de servicio adecuada a las necesidades, a un costo aceptable para la corporación.

Para poder realizar las tareas de administración, es necesario poder detectar fallas, aislarlas y corregirlas, al menor costo y en el menor tiempo posible. Es necesario también poder realizar cambios en las configuraciones afectando lo mínimo posible al servicio.

Una buena administración de red se basa en prever, en la medida de lo posible, posibles puntos de falla, y evitarlos antes de que sucedan. Esto se basa en tener medidas de utilización de la red, analizarlas y tomar acciones preventivas antes que correctivas.

2.14.- SISTEMA DE GESTIÓN DE REDES

De acuerdo a los sistemas de gestión de redes Thortonm (1998) señala que los proveedores de las redes están continuamente buscando hacia el futuro los sistemas de gestión de redes que poseerán la capacidad de configuraciones cambiantes proactivas de las redes y de enrutamiento de tráfico en tiempo real, con el fin de optimizar el ancho de banda del tráfico, y por lo tanto maximizar su margen de beneficio.

Según Chernand (1999) la interconexión de computadoras originó la creación de las LANs, permitiendo que varios usuarios ubicados en un área geográfica se conectaran a servidores de archivos, de aplicaciones, intercambiar mensajes, archivos, entre otros recursos. Las interconexiones trajo la necesidad de resolver ciertos retos tecnológicos en área de conectividad, confiabilidad, administración de redes y flexibilidad para ser eficientes y efectivas las redes.

Los problemas que se presentan en las interconexiones se debe a:

Dispositivos diferentes, por la gran variedad de marcas en el mercado en ocasiones las LANs tienen diferentes dispositivos

Administraciones diferentes; la interconexión entre redes de distinto propósito se administraban y gestionaban de manera distinta

Tecnologías de interconexión, diferentes topologías, diferentes tecnologías

Sin embargo, la principal barrera a la producción de verdaderos sistemas de gestión de redes en tiempo real es la tecnología, o la técnica, que permitirá la gran cantidad de datos de rendimiento de la red, son recogidos rutinariamente analizados, y que se puedan hacer los cambios en tiempo real.

Por la diversidad de tecnologías surgió la necesidad de implementar metodologías para la gestión de redes que fuera capaz de gestionar la configuración de sus componentes, la seguridad, las fallas, el desempeño. El rápido cambio emergente de modelos de gestión de redes parece ofrecer una solución a los problemas que suministrará la base para la provisión de

un sistema de gestión de redes en tiempo real en virtud de su posibilidad de estudiar rápidamente las grandes cantidades de datos.

El autor Thortonm sigue señalando que hay dos barreras que excluyen normalmente el uso día a día de los sistemas de gestión. La primera barrera es la falta de bases de conocimiento fiables y completamente suministrando información en cuanto a la acción correcta preventiva o paulatina, cuando una red presenta varias condiciones de pérdida de celdas en un determinado conmutador. Según Burn (1996), la segunda barrera es la velocidad de procesado de la información. Una gran cantidad de información de rendimiento se recoge rutinariamente de las redes, normalmente 15 MB en 15 minutos en una red ATM.

Con el fin de determinar los eventos que suceden en la red, un operador debe poder buscar rápidamente a través de grandes cantidades de información de rendimiento con el fin de hacer los cambios en la base de conocimiento de la red. La técnica usada para procesar los datos de rendimiento de la red necesitará ser tan rápida como sea posible.

La mayoría de los trabajos que se ha llevado a cabo hacia la meta final de suministrar sistemas de gestión de redes se ha focalizado en poder gestionar proactivamente una red usando el soporte de un sistema basado en el conocimiento, Laufmann (1997) sostiene que superando la primera barrera, se debe buscar superar la segunda, a saber estableciendo la técnica óptima que permite conseguir la gestión del sistema en verdadero tiempo real,

determinando rápidamente la información a partir de las grandes cantidades de datos de rendimiento.

De acuerdo al objetivo de gestión se garantiza un nivel de servicio de acuerdo a un coste, según figura 17.

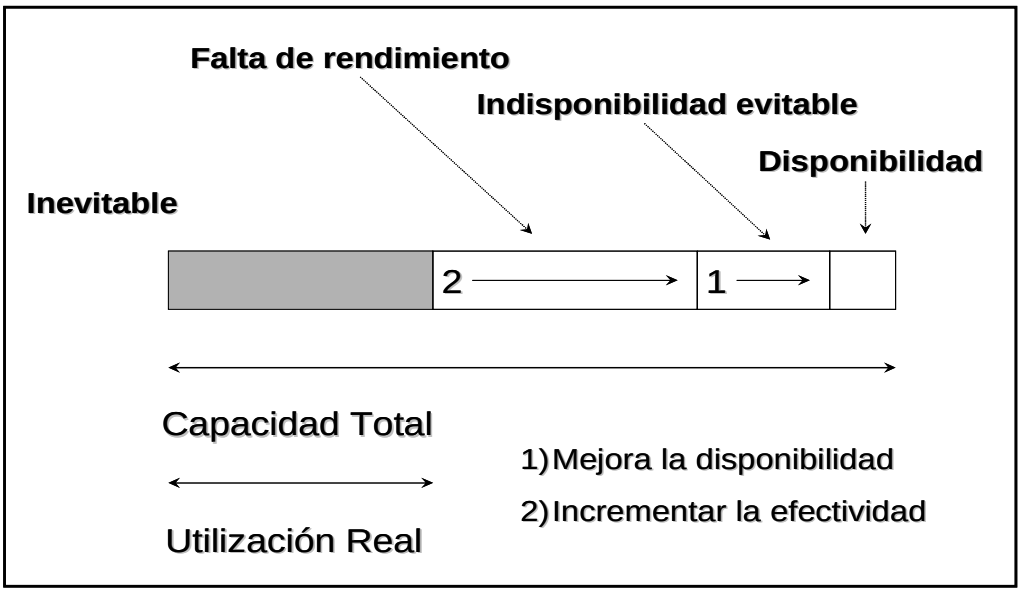

Figura 17. Niveles de Servicios.
Fuente: Thortonm, J. (1998)

Las redes del mundo de las telecomunicaciones de hoy en día están basadas en diferentes tecnologías para transmitir datos, telefonía, video-conferencia y otros servicios, utilizan sistemas de gestión que actualmente implican altos costos y una complejidad extremadamente elevada en cuanto a la utilización y a la gestión, es por ello que se buscan Modelos de gestión para sistemas heterogéneos de redes.

La gestión de redes basada en modelos, propuestas resuelve los problemas de gestión de los sistemas tradicionales dado que resulta evidente

la necesidad de utilizar lenguajes que soporten la especificación de gestión, de seguridad, entre otros.

2.15.- CONCEPTO DE GESTIÓN DE REDES

ISO (Organización internacional para la estandardización) define la gestión de red como el conjunto de elementos de control y supervisión de los recursos que permiten que la comunicación tenga lugar sobre la red (Cisco, 1999). Según Mindiola (1997), se entiende por gestión de redes al conjunto de actividades destinadas a garantizar los servicios que prestan las redes.

El uso de las redes en la actualidad han permitido relacionarse en el mundo de lo que llaman el uso de las nuevas tecnologías permitiendo a través de ellas comunicación a largas distancias con distintas empresas. Las redes de datos y comunicaciones son la base de los sistemas de información y uno de los elementos críticos del engranaje corporativo.

La gestión de redes se convierte en un factor muy importante ya que contribuye a su mantenimiento, la resolución, prevención de incidencias y en definitiva a asegurar la máxima disponibilidad de la red de comunicación. Mejora el rendimiento de la red detectando "Cuellos de botella", debido a saturación de tráfico en ciertos segmentos, o a un dimensional inadecuado de algún componente de la red.

La gestión de red permite la definición de alarmas que actúan en respuestas a eventos específicos (caídas de nodos, superación de umbrales error o tráfico), estas alarmas pueden asociarse a acciones que pueden

automatizar parte de la gestión, facilitando en gran medida el trabajo del administrador de la red al permitir la rápida detección y resolución de las incidencias. (Tobal, 1999).

Los aspectos funcionales de la gestión de red indican:

No existe funcionalidad común, depende de: tipo de red gestionada, tipo de equipos gestionados y objetivos específicos de la gestión de red.

A bajo nivel, todos los métodos se basan en: monitorización de la red (gestión de prestaciones, fallos, contabilidad, configuraciones) y Control de la red (gestión de configuraciones)

Thortonm (1998), señala un sistema de gestión de red es una colección de herramientas para monitorizar y controlar la red integrado en los siguientes sentidos:

Una interfaz de operador única con un conjunto de órdenes potente, pero agradables para el usuario, para llevar a cabo la mayoría o todas las tareas de la gestión de red.

Una cantidad mínima de equipamiento separado del sistema de gestión, esto es, la mayor parte del hardware y software requeridos para la gestión de red están incorporados en el equipamiento del usuario.

Las funciones de red se suelen agrupar en dos categorías:

Supervisión de la red, se considera una función de lectura y se encarga de observar y analizar el estado y comportamiento de la configuración de la red acompañado de sus componentes.

Para Cisco (1999), normalmente la supervisión se divide en tres áreas de diseño las cuales comprende:

Acceso a la información supervisada, trata de cómo definir la información supervisada y como trasladarla desde un recursos a un gestor.

Diseño de los mecanismos de supervisión, trata de determinar la mejor forma de obtener la información de un recurso.

Aplicaciones con la información supervisada, cómo se usa /a información en las distintas áreas funcionales

La supervisión de red se dirige hacia tres áreas funcionales:

Supervisión de rendimiento: es imposible una gestión de red sin medir el rendimiento de la misma, las medidas a cabo son: Disponibilidad, Tiempo de respuesta, Eficiencia, Rendimiento, Utilización.

Supervisión de fallos: pretende descubrir los fallos del sistema, identificarlos lo antes posible su causa y llevar a cabo las acciones para poder remediarlos

Supervisión de cuenta: lleva a cabo el control del uso de los distintos recursos de la red por parte de los usuarios. Algunos recursos sujetos a supervisión pueden ser: Facilidades de comunicación, hardware como estaciones de trabajo y servidores y servicios.

Control de red: se considera como una función de escritura y se encarga de alterar los parámetros de los distintos componentes de la configuración y hacer a cabo las acciones que se determinen. El control de la red, se encarga de la supervisión de red, modificación de parámetros y hacer que se

lleven a cabo las acciones por parte del sistema final, intermedio y las subredes que constituyen la configuración que debe ser gestionada.

El control de red se divide en áreas funcionales como:

Configuración: trata de la inicialización, mantenimiento y apagado de los componentes individuales, los subsistemas digitales del sistema.

Algunas funciones que se debe llevar a cabo en la gestión son las siguientes:

Floración de la información de la configuración.

Establecer y modificar los valores de configuración.

Definir y finalizar operaciones de red.

Distribución de software.

Informar el estado de la configuración.

Control de seguridad: se encarga de cumplir los siguientes requisitos:

Privacidad, la información sólo debe acceder aquel que este autorizado. Integridad, las características del sistema sólo deben poder modificarse por personas autorizadas. Disponibilidad, los recursos deben ser efectivos para uso de aquellos a los que se les permita.

En resumen la gestión de redes se divide en cinco áreas funcionales. En la figura 18 se señala como es el flujo de información de gestión en una red.

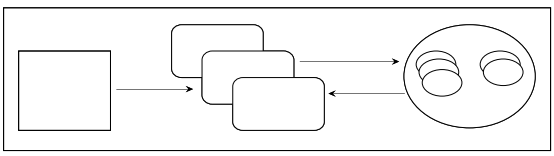

Figura 18. Flujo de información de gestión.
Fuente: Thortonm (1998)

Thortonm (1998) sugiere la realización del esquema de funcionamiento general de una plataforma de gestión como lo muestra la figura 19. En esta representación, el usuario a través de una interfaz unificada tiene acceso a la información procedente de diversas aplicaciones de gestión (gestores). Esto se requiere así puesto que la diversidad de elementos de red procedentes de diferentes fabricantes junto con la enormidad de funciones de gestión definidas por los estándares aconseja el procesado en paralelo.

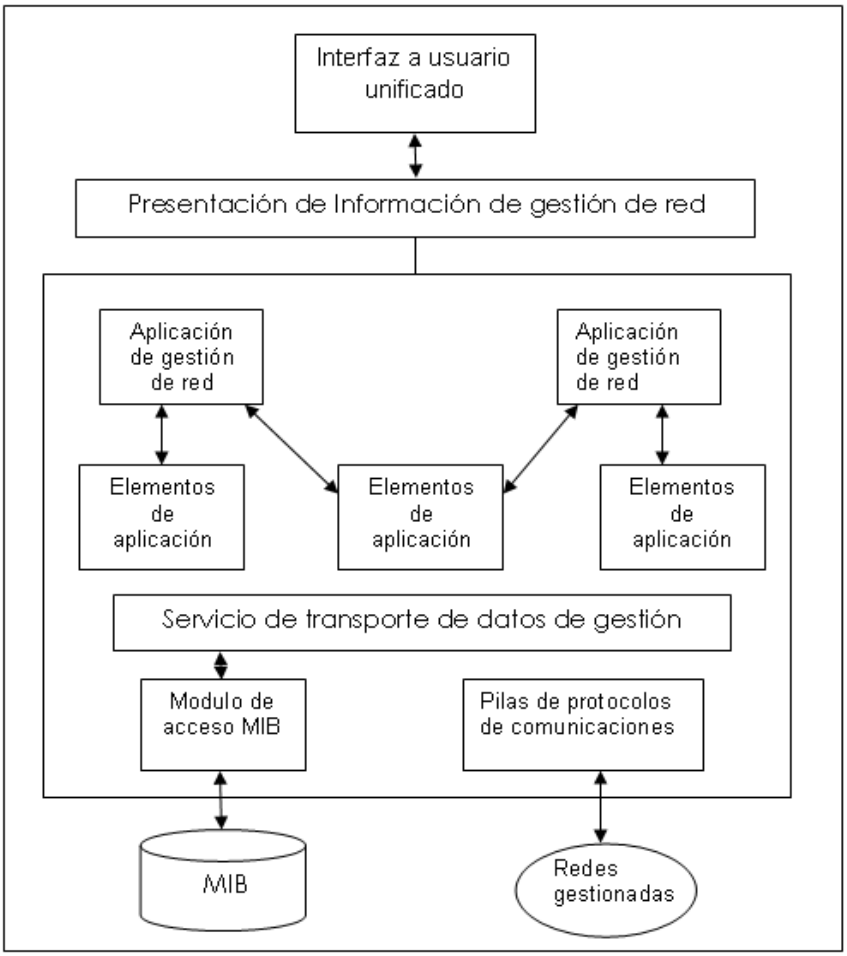

Figura 19. Modelo de referencias de un sistema de gestión de red.
Fuente: Thortonm (1998)

2.16.- ÁREAS FUNCIONALES DEL MODELO DE GESTIÓN DE REDES

Por otra parte Thortonm (1998) sostiene que partiendo de definir la gestión de red como la planificación, la organización, la supervisión y el control de elementos de comunicaciones se garantiza un adecuado nivel de servicio, de acuerdo con un determinado coste, y según las recomendaciones de la OSI, recogidas por la ITU, definen las siguientes áreas funcionales para la gestión de red.

Gestión de fallas o Supervisión de fallos. Según Sherman (1997) el objetivo de la gestión de fallas es manejar las condiciones de error que hacen que los usuarios pierdan toda o parte de las funcionabilidad de un recurso de la red.

Esta gestión establece la generación de notificaciones específicas de error (alarmas), el registro de las notificaciones de error y la verificación de los recursos de red para trazar e identificar fallas. También el conjunto de facilidades que permiten la detección, aislamiento y corrección de una operación anormal. Una falla puede ser originada por:

La degradación del desempeño de algún componente de la red, sobrepasando el umbral establecido.

Por la presencia de algún evento controlado o inesperado

Por la intervención planificada o inesperada de algún individuo.

De acuerdo a Mindiola, D. (1997) la gestión de fallas se lleva a cabo en los siguientes pasos:

Detectar o recibir notificaciones del problema. Lo ideal dentro del sistema de gestión de redes es que exista un mecanismo que permita detectar la presencia de algún problema antes que el usuario en todo caso, ante la complejidad de una infraestructura de redes y las limitaciones de los administradores de redes se debe implementar un proceso que permita al usuario notificar la presencia de una posible falla.

Registrar el problema y posteriormente su solución. El problema detectado por el administrador de red o notificado por el usuario debe ser registrado y almacenado en una base de datos de conocimientos que adicionalmente contendrá información relacionada con los pasos y detalles de la solución implementada para dicho problema. En la medida que esta base de conocimientos va enriqueciendo con las vivencias y experiencias surgidas ante cada problema en esa medida la capacidad para gestionar las fallas más eficientemente se va incrementando.

Diagnosticar y valorar el problema. Para diagnosticar y valorar el problema se debe resolver las siguientes interrogantes:

¿Cuáles son los componentes físicos y/o lógicos afectados directamente?.

¿Cómo se manifiesta el problema?.

¿Quiénes son los usuarios afectados?.

¿Cuáles son las posibles causas del problema y orden de prioridad?.

¿Qué componentes afecta indirectamente?.

¿Cuál es el nivelo magnitud de la falla?.

¿Qué recursos son necesarios para implementar la solución?.

¿Cuál es el tiempo estimado de solución de la falla?.

¿Es posible implementar una solución temporal alternativa?.

¿Hay algún problema similar registrado en la base de datos?.

Resolver o aislar el problema. Una vez culminado el diagnostico de la falla, consiste en la implementación de las acciones correctivas para cada una de las posibles causas, hasta dar con la solución definitiva. Los gestores de fallos tienen un Event Browser que filtra los eventos de acuerdo a una combinación configurable del tipo de evento, origen, cadena de mensaje, periodo de tiempo recibido e importancia.

El gestor agrupa los eventos en categorías basadas en la importancia y actúa sobre ellas por medio de acciones que el usuario puede definir, pueden realizarse operaciones de búsqueda, ordenación y filtrado. Por ejemplo, puede avisar a alguien cuando recibe un determinado tipo de interrupción SNMP, este componente proporciona monitorización en tiempo real de elementos de la red y resolución de problemas.

Los contadores de estadísticas en tiempo real pueden extraerse y convertirse en gráficos dinámicos utilizando la consulta SNMP, entidades como son los puertos pueden configurarse mediante ventanas de fácil manejo, las visualizaciones de los paneles frontales y posteriores de los elementos de la red muestran gráficamente el estado actual de las tarjetas y los subsistemas El objetivo de la gestión de fallos es mantener dinámicamente por medio de los siguientes niveles de servicio:

Gestión proactiva: evitar fallos detectando tendencias hacia fallos, caracterización de tendencias a determinación de umbrales de ciertos parámetros y con la monitorización detectar los umbrales o programar notificaciones automáticas

Gestión reactiva: asumir que existen fallos inevitables detectando lo antes posible el fallo y monitorizando periódicamente (no es posible las notificaciones).

En la gestión de fallas se evalúa el ciclo de vida de incidencias en la que se considera, detección de problema y gestión de pruebas preventivas. A través, de la determinación del problema, sobre el fallo puede no ser fiable en cuanto a la fuente de fallo Diagnosis del problema, procedimiento y Resolución del problema, la cual se obtienen los siguientes indicadores:

Por operadores de help-desk (80-85%).

Por operadores técnicos (5-10%).

Por especialistas en comunicaciones (2-5%).

Por especialista en aplicaciones (1-3%).

Por fabricante (1-2%).

Gestión de pruebas preventivas. Pruebas por conectividad, integridad de datos, integridad de protocolos, saturación de datos, saturación de conexiones, tiempo de repuestas, bucle y diagnósticos.

Gestión de configuración. Se distribuye en actividades de inicialización, instalación, abastecimiento, permite la colección de información de configuración y estado en demanda, proporcionando facilidades de

inventario. Soporta el anuncio de cambios de configuración a través de notificaciones relevantes, facilidades que permiten controlar, identificar, recoger y proporcionar datos a objetos gestionados, con el propósito de asistir a operar servicios de interconexión.

Para Cisco (1999), el objetivo de la gestión de configuración es controlar la información que describe las características físicas y lógicas de los recursos de la red, así como las relaciones entre dichos recursos. Cada componente de la red tiene una amplia gama de información respecto a su marca, modelo, capacidad, versión, velocidad, seriales, entre otros, que son almacenados en una base de datos controlada por el módulo de gestión de la configuración. Las funciones que ofrece la configuración son:

Obtener inventario de los recursos o componentes de la red, tanto física como lógica (servidores, enrutadores, concentradores).

Obtener los valores de las variables de cada uno de los componentes (memoria RAM, disco duro, CPU, tarjeta de red, versión del sistema operativo).

Obtener un datagrama de interconexión de los componentes.

Detectar cambios inesperados en características de los componentes físicos y lógicos.

Detectar cambios inesperados de interconexión de los componentes El gestor cubre automáticamente elementos de la red y muestra un mapa topológico gráfico que soporta bien visualizaciones autónomas de mapas topológicos o bien mapas Hp OpenView.

Las pantallas multicolores se actualizan en tiempo reales, en respuestas a los eventos que estén ocurriendo en la red.

El interfaz que muestra la topología soporta arrastre interactivo, selecciones múltiples, zoom de acercamiento/alejamiento, agrupaciones de nodos submapas entre otros. En la gestión está:

Gestión de acuerdos de nivel de servicios. Contrato entre cliente/proveedor o entre proveedores sobre servicios a proporcionar y calidades asociadas. Identificación de las partes contractuales, Identificación del trabajo a realizar, Objetivos de niveles de servicio, Niveles de servicios proporcionados, Multas por incumplimiento, Fecha de caducidad, Cláusulas de renegociación y Prestaciones actuales proporcionadas.

Gestión de Incidencias. Fecha y hora de informe de incidencia, Resolución de incidencia, Usuario/localización, equipo afectado, descripción del problema, estado, operador(es), grado de severidad, historial de incidencia, comentarios. Gestión de proveedores externos (ordenes de procesamiento / aprovisionamiento) y Gestión de cambios (reconfiguraciones)

Gestión de contabilidad. Consiste en actividades de recolección de información de contabilidad y su procesamiento para propósitos de cobranza y facturación. Estas actividades establecen un límite contable para que un conjunto de costos se combinen con recursos múltiples y se utilicen en un contexto de servicio, facilidades que permiten establecer cargos por el uso de determinados objetos e identificar costes por el uso de éstos.

Para mejorar el desempeño que se aplica cuando alguna de las variables de componentes mantiene sus valores cerca del umbral establecido en los parámetros de desempeño. La gestión de la contabilidad evita, minimiza y/o elimina los problemas de la red promoviendo y administrando en forma ordenada los cambios en sus componentes. La gestión de contabilidad abarca los siguientes pasos:

Medir la utilización de todos los recursos importantes de la red analizar los resultados para determinar los patrones de uso actuales.

Establecer cuotas de uso.

Efectuar subsecuencias mediciones y correcciones hasta establecer la utilización óptima y justa de los recursos.

Gestión de desempeño. Proporciona información en forma ordenada para determinar la carga del sistema y de la red bajo condiciones naturales y artificiales, proporcionando estadísticas, permitiendo actividades de planeación de configuración.

La información recabada por las funciones de gestión de desempeño es útil para determinar si se están alcanzando los objetivos de la red o si con base en el desempeño se deben iniciar procedimientos de determinación de problemas. La gestión de desempeño abarca los siguientes pasos:

Establecer cuales son los componentes físicos y lógicos de interés para los administradores de la red, ejemplo un servidor de red.

Establecer las variables de desempeño para cada uno de los componentes seleccionados, capacidad de memoria RAM y disco duro.

Reunir los datos de funcionamiento de los componentes seleccionados, registrando los valores para cada una de sus variables.

Analizar los datos para determinar los niveles normales de capacidad, funcionamiento, operación, entre otros., y establecer así los parámetros normales de comportamiento.

Determinar el umbral de desempeño máximo permitido para cada una de las variables y establecer los parámetros de desempeño.

Implementar mecanismos de alertas que deben activarse cuando los parámetros llegan a los valores umbrales como mensajes emergentes, registro de eventos, avisos sonoros. Monitorear las alertas.

La gestión de desempeño puede implementarse bajo un sistema proactivo a través de la simulación de eventos, se podría usar una simulación de la red para hacer una proyección de cómo se verán afectados los parámetros de desempeño por el crecimiento de la red. Se puede gestionar el rendimiento de la red utilizando un software que facilita la comprensión del funcionamiento interno de la red de manera que pueda resolver problemas con rapidez y optimizar el rendimiento.

Gestión de seguridad. Está relacionada con dos aspectos de la seguridad del sistema: aspectos que son esenciales en la gestión de red y que permiten proteger los objetos gestionados. La gestión de seguridad requiere la habilidad para supervisar, controlar la disponibilidad de facilidades de seguridad, reportar amenazas y rupturas en la seguridad. La seguridad de la gestión requiere la habilidad para autentificar usuarios y aplicaciones de

gestión, con el fin de garantizar la confidencialidad e integridad de intercambios de operaciones de gestión y prevenir accesos no autorizados a la información.

Existen varias formas de abordar la seguridad de un sistema, un punto de vista es entenderla como una forma de prevenir futuras pérdidas una manera de gestionar los riesgos relacionados con la tecnología. Otros consideran que es algo necesario para evitar que usuarios maliciosos entre al sistema.

La seguridad en sistemas de ordenadores es la protección de la integridad, disponibilidad y si es necesaria la confidencialidad de información y recursos que se usan para: Entrada, almacenamiento, proceso y comunicación de los mismos (Mindiola: 1997, p.51). Existe una serie de compromisos básicos sobre la seguridad de sistemas de red:

No dificultar las labores de los usuarios; el propósito es la protección de recursos considerados importantes dentro de la organización donde el sistema de seguridad está activo.

La seguridad es responsabilidad de la gestión de riesgos; una de las responsabilidades en la gestión de un sistema es el control de riesgo, control de toda la información. Se debe conseguir que la información este disponible, sea correcta y esté completa.

Se deben especificar claramente las responsabilidades en seguridad, es necesario que se haga de forma precisa los grupos a los que se le asigna esta tarea suelen ser los gestores de seguridad, operadores del sistema, gestores de aplicaciones, el encargado de la seguridad física, la oficina de

recuperación de desastres, los usuarios y los encargados de los informes e supervisión.

La seguridad requiere una estructura clara, la eficiencia de la seguridad precisa que distintos grupos, áreas dentro y fuera de la organización colaboren, la arquitectura o programa de seguridad se suele dividir en bloques que denominan controles agrupados en controles técnicos, de operaciones y de servicio. Para que sea la seguridad óptima hay que conocer esta estructuración y la interacción entre cada uno de ellos.

La protección del sistema debe tener un coste soportable, hay que tener en cuenta que una inversión en seguridad puede suponer disminuir el número de pérdidas debido a fallos del sistema, o por manipulación fraudulenta de los recursos. Los beneficios de la seguridad no son sólo monetarios, evita hackers así como otros elementos hostiles a nuestro sistema ayudando a ofrecer una buena imagen hacia el público.

La labor principal en seguridad es el aislamiento de los actos no deseables y la prevención de aquellos que no se hagan considerados, de forma que si se producen hagan el menor daño posible entre las distintas actividades que debe llevar a cabo se puede detectar las siguientes:

Identificación de los usuarios. Existen varias técnicas entre las que se encuentran contraseñas (password) o sistemas más sofisticados como reconocimiento de habla, huella dactilar o la retina del ojo.

Detección de intrusos en la red. Hay que detectar y actuar sobre cualquier acceso no autorizado a nuestro sistema, el objetivo es la detección de intrusos en tiempo real.

Análisis de riesgo. Función de la frecuencia con la que se producen dichas amenazas, vulnerabilidad de la protección contra las mismas y las pérdidas potenciales que se produjesen en el caso de que se diese una.

Clasificación apropiada de los datos. Gran cantidad de datos provenientes de los distintos programas de control generados a partir de la actuaciones que llevan a cabo los usuarios en el sistema; es importante para una buena supervisión en la seguridad se debe clasificar los datos convenientemente de tal forma que se ahorre tiempo en su análisis.

Control de las nuevas aplicaciones. Cuando se instala una nueva aplicación hay que comprobar que no introduzcan nuevas brechas de seguridad especialmente si se ejecuta con permisos de administrador.

Análisis de los accesos de los usuarios. Es necesario tener un control para poder detectar intentos de acceso no autorizados

La gestión de seguridad proporciona continuidad de la red y sus componentes en los distintos aspectos de seguridad: Acceso a las redes, a los sistemas, a la información en transito en las funciones de la gestión de seguridad esta: Definición de análisis de riesgos y política de seguridad. Implantación de servicios de seguridad e infraestructura asociada. Definición de alarmas registros e informes de seguridad.

2.17.- ARQUITECTURA DE LA GESTIÓN DE REDES

Para Computer Associates y Cisco (1999) la mayoría de las arquitecturas de gestión de redes utilizan el mismo conjunto de relaciones y estructura básica, como son: Gestores de redes, Consola de administración, Agentes, Dispositivos Administrados, Base de datos de administración, Protocolo de gestión. Esto se observa en la siguiente figura 20.

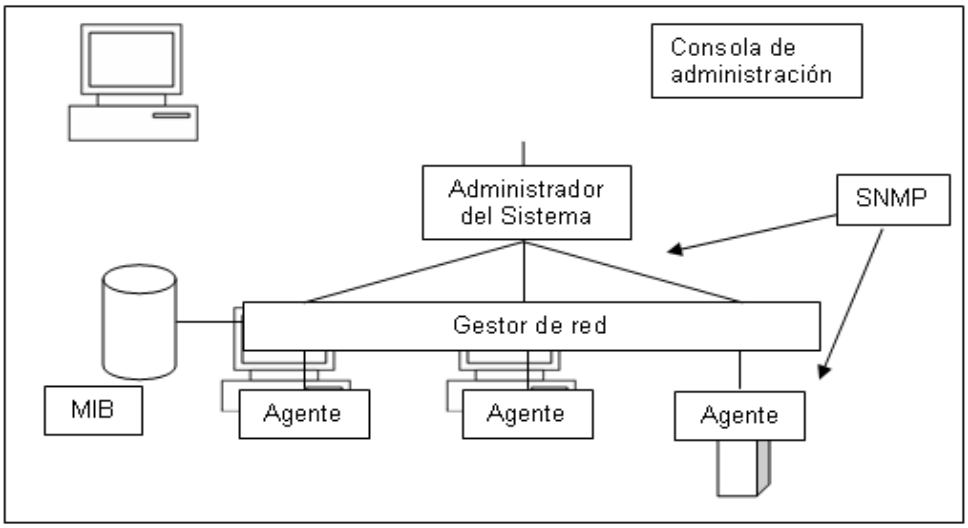

Figura 20. Arquitectura de la gestión de redes.
Fuente: Cisco (1999)

2.18.- ELEMENTOS DE UN SISTEMA DE GESTIÓN DE REDES

Thortonm (1998) sostiene que los elementos activos de la red proporcionan una realimentación regular de información del estado al centro de control de red. Un sistema de gestión de red tiene los siguientes elementos claves: Estación de gestión o gestor, Agente, Base de información de red, Protocolo de gestión de red.

Estación de gestión de red. Es un dispositivo autónomo pero puede ser implementado en un sistema compartido, la gestión de servicio sirve como interfaz entre el gestor de red humano y el sistema de gestión de red. La estación de gestión tendrá como mínimo:

Un conjunto de aplicaciones para el análisis de los datos, recuperación de fallos, entre otros.

Una interfaz a través de la cual el gestor de red puede monitorizar y controlar la red.

La capacidad de trasladar los requerimientos del gestor de red a la monitorización y control de red de los elementos.

Una base de datos de información de gestión de red extraída de las bases de datos de todas las entidades gestionadas en la red.

Agente. De acuerdo con Mindiola, D. (1997) un agente es un software que reside en un nodo de red y es responsable de comunicarse con los managers o administradores considerando el nodo, el nodo es representado como un objeto teniendo varios campos o variables que están definidos en el MIS apropiado. El agente tiene dos propósitos:

Responder a las solicitudes de los manegers, suministrando o cambiando los valores de las variables de los objetos según se solicitaron.

Generar advertencias para alertar a los administradores de los eventos notables que ocurren en el nodo, tales como una falla en un componente.

Los sistemas de gestión permiten reducir los costes de explotación mediante la centralización de la operación y mantenimiento de las distintas

redes y de los servicios que se apoyan en las mismas, la reducción de los tiempos de formación de los operadores y la simplificación en el manejo de la creciente complejidad de la tecnología. Así mismo, contribuyen a rentabilizar al máximo las inversiones realizadas en infraestructuras de red.

Se ha sugerido (Burn, T.,1996) que a partir de medidas estadísticas de tráfico, se puede analizar con detalle el uso real de las infraestructuras, y poner de manifiesto tanto aquellas con capacidad ociosa como las que presentan cuellos de botella que suponen pérdida de oportunidad de ingresos y deterioro de imagen ante los clientes.

Por otro lado, Góngora, A. (1998) sostiene que los sistemas de gestión permiten acortar, en buena medida, los plazos de provisión de nuevos servicios, gracias a la automatización de los procesos administrativos que intervienen en el alta y/o baja de los mismos y a la posibilidad de activar dichos servicios en los elementos de la red con seguridad e inmediatez.

2.19.- IMPORTANCIA DE LA GESTIÓN DE REDES

Para Soriano (2000) las redes de comunicaciones han evolucionado con el paso del tiempo ante la necesidad de satisfacer las demandas de los diferentes servicios de telecomunicaciones, que día a día necesitan un mayor ancho de banda y una mejor calidad de servicio para las nuevas aplicaciones que se han venido desarrollando hasta la actualidad.

La tecnología de redes ha incrementado su complejidad generándose la necesidad de contar con una mejor administración de los recursos de estos

sistemas, lo cual ha favorecido la evolución conjunta de la gestión de redes. Tiene como propósito la utilización y coordinación de los recursos para planificar, organizar, mantener, supervisar, evaluar, y controlar los elementos de las redes de comunicaciones para adaptarse a la calidad de servicio necesaria a un determinado costo.

Su campo de aplicación es amplio y de gran importancia dadas las características tecnológicas que poseen los sistemas de telecomunicaciones y los servicios que ofrecen, mantiene un cierto grado de complejidad al interactuar con sistemas heterogéneos que involucran diversos fabricantes con productos eminentemente propietarios.

Gervás, P. (2002) sostiene que la gestión de red juega un papel importante en el buen funcionamiento de las redes y se hace imprescindible su aplicación por las siguientes razones:

Los sistemas de información son vitales y están soportados sobre redes.

La información manejada tiende a ser cada día mayor más dispersa.

Las nuevas tecnologías de red requieren de una gestión cada vez más especializada, que le permita el empleo eficiente de sus recursos de telecomunicaciones.

El adecuado empleo de las tecnologías de gestión de red permite mejorar la eficiencia, disponibilidad y el rendimiento de las redes, aumentar la relación calidad/costo en el diseño de las redes, así como aumentar la satisfacción de los usuarios por el servicio de red proporcionado.

Desde 1998, Góngora recomienda que para lograr una gestión de red eficiente es necesario contar con un sistema integrado de gestión que conlleve a mejorar la eficiencia en la operación de la red. Un sistema integrado de gestión de red debe contar con los siguientes elementos: Recursos humanos, métodos de trabajo y desarrollo tecnológico. La gestión de redes es una necesidad primordial en las organizaciones, se espera que:

Asegure un servicio casi continuo a los usuarios finales descrito por la disponibilidad y velocidad de respuesta, sin que se vean afectados por las actualizaciones tecnológicas en la red.

Incremente el desempeño de una red con el empleo de la mejor tecnología de redes, recursos humanos adecuados, métodos de trabajo probados y herramientas integradas que automaticen las operaciones de gestión. Y controle los costos dedicados a las comunicaciones y a la seguridad de la información.

2.20.- MOTIVACIÓN DE LA GESTIÓN DE RED

Race (1994) sostiene que la importancia creciente de las redes y los sistemas de procesamiento distribuidos en las organizaciones, se refiere a los siguientes criterios:

Control de activos estratégicos.

Control de complejidad.

Mejorar servicio.

Equilibrar necesidades.

Reducir indisponibilidad.

Control de costes.

La pirámide de la gestión señalada en la figura Nº 21.

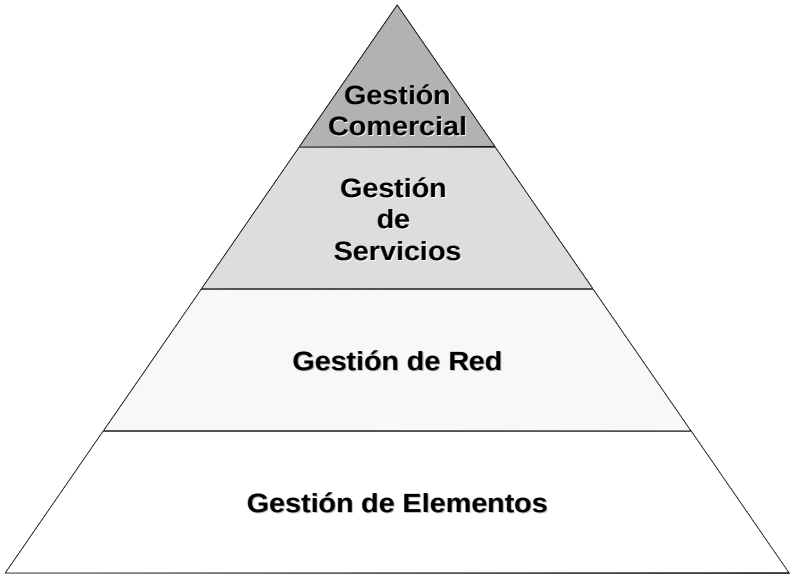

Figura 21. Sistemas de gestión actuales.
Fuente: Race (1994)

2.21.- APLICACIÓN DE GESTIÓN DE REDES Y SERVICIOS

En cuanto a la gestión de redes y servicios; Salavert (1998) mantiene que ante la heterogeneidad de modelos de gestión de red Integrada, y teniendo en cuenta que es muy probable el hecho de que en un mismo dominio de gestión necesite aplicar múltiples modelos simultáneamente. Ha sido necesario tradicionalmente establecer mecanismos que posibiliten la interoperabilidad entre los distintos dominios implicados, siendo ésta posible

si se consigue definir un conjunto de reglas que traduzcan el protocolo de comunicaciones y modelo de información de gestión.

Sin embargo, un aspecto que todavía no tiene fácil solución se presenta cuando en dos dominios distintos de gestión se representa un mismo concepto de distinta manera: una traducción meramente sintáctica del modelo de información de gestión origen no proporciona el concepto existente en el modelo destino. Se hace por tanto necesaria una traducción semántica que haga corresponder directamente los conceptos de ambos dominios.

La aplicación de gestión de red y servicios tiene como objetivo proponer soluciones que permitan perfeccionar la interoperabilidad en lo que se refiere a los modelos de información de gestión, ahondando en las posibilidades que existen para llevar a cabo la traducción semántica. Para ello, la técnica de representación del conocimiento conocida como ontología es una de las respuestas más adecuadas a este problema, dado que proporciona las construcciones necesarias para añadir semántica a información representada.

La aplicación de esta tecnología al campo de la gestión de red puede ser clave que permita realizar una gestión realmente integrada e inteligente de los diversos recursos que posee una empresa, que normalmente pertenecen a distintos dominios de gestión:

Conmutadores y encaminadores gestionados con ordenadores o servicios de comercio electrónico accesibles con una interfaz, se gestionarían de

manera unificada desde un gestor con un único modelo de información. El empleo de antologías puede permitir la definición de reglas que definan el comportamiento del gestor, de forma añadida al modelo de información de gestión que se haya especificado, definiendo así toda la información relativa a la gestión de manera unificada.

2.22.- GESTIÓN DE TELECOMUNICACIONES

Millán, L. (2000) encontraron datos que tradicionalmente las redes de telecomunicaciones tienen separados el nivel de gestión del nivel de comunicación; existe diferentes infraestructuras para la entrega de los datos del usuario y le entrega de la información, comandos intercambiados entre las entidades de gestión y los objetos gestionados.

La industria de telecomunicaciones es dinámica. Los operadores y proveedores de servicios están operando en un mercado ultra competitivo que posee un apetito insaciable por nuevos servicios y aplicaciones. El poder combinado entre la movilidad e Internet permitirá el acceso a toda hora y en cualquier lugar.

La migración desde redes de conmutador de circuito hacia conmutado por paquetes, significa que los operadores deben agregar nuevas tecnologías tales como ADSL, Media Gateways, ATM, entre otros; mientras las redes y servicios existentes que generan las actuales utilidades. En varias situaciones esto significa aumentar el equipamiento acudiendo a varios proveedores.

Sánchez, C. (2000) afirman que la feroz competencia no permite que los movimientos rápidos para introducir nuevos servicios en el mercado sean sacrificados. La creciente complejidad de las redes genera un aumento en la necesidad de contar con flexibles soluciones de gestión. Varios operadores actuarán como carriers, vendiendo capacidad a los proveedores de servicios y proveedores de acceso. La activación del servicio, la inter - operación y facturación será crucial utilizada frecuentemente.

Para cubrir la demanda del mercado se utiliza los mejores componentes, aplicaciones para proveer soluciones completas de gestión con flexibilidad para adaptar los cambios en la demanda de servicios y tecnología de redes. La migración hacia redes multi-servicio, es soportada con soluciones para el portafolio ENGINE, con alternación de circuitos AXE y convergencia IP.

De esta manera, se obtienen las soluciones ofrecidas para la Seguridad en las operaciones de las redes y servicios, brindando gestión en el performance, routing, configuración y tráfico. Las soluciones brindan calidad superior en los servicios a los usuarios finales, reducción de costos, planeación de redes y permite la creación de nuevos volúmenes de utilidad. La calidad de servicio se caracteriza de la siguiente manera:

La gestión del cliente, ofrece soluciones en las áreas de facturación, atención al cliente, pre-pago, fraude y mediación, mientras que la rentabilidad puede ser incrementada con mejoras en la atención al cliente y performance.

Abastecimiento en la gestión de servicios de telecomunicaciones, soluciones que soportan el servicio de abastecimiento de servicios de

próxima generación (actividades bancarias, pagos y mensajería unificada), pueden ser suministradas rápidamente, con alta calidad y bajo costo para los clientes. Mediación en la utilización ofrece una colección flexible, pre - procesamiento, y distribución de valiosos usos de datos para aplicaciones "downstream".

La seguridad en las redes está relacionada con los sistemas, programas y datos cuantos éstos existen en una red establecida. Los efectos de compartir en las redes tienen como resultado la existencia de más usuarios potenciales accediendo a los sistemas, las redes aumentan la vulnerabilidad de los sistemas informáticos.

A diferencia del modelo OSI el cual se definen cinco áreas funcionales, el estándar TMN no entra en consideraciones sobre las aplicaciones de la información gestionada. Por el contrario, se define le siguiente funcionalidad:

El intercambio de información entre la red gestionada y la red TMN.

El intercambio de información entre redes TMN.

La conversión de formatos de información para un intercambit consistente de información.

La transferencia de información entre puntos de una TMN.

El análisis de la información de gestión y la capacidad de actuar en función de ella.

La manipulación y presentación de la información de gestión en un formato útil para el usuario de la misma.

El control del acceso a la información de gestión por los usuarios autorizados.

2.23.- RED DE GERENCIA DE LAS TELECOMUNICACIONES (TMN)

El objetivo es proporcionar una estructura de la red organizada para conseguir la interconexión de los diversos tipos de sistemas de operación y equipos de telecomunicaciones usando una arquitectura estándar e interfaces normalizados.

La motivación de una arquitectura de TMN es por la heterogeneidad en la tecnología de redes de telecomunicaciones, redes analógicas, digitales banda estrecha, banda ancha, demandas sobre posibilidad de introducir nuevos servicios, alta calidad de servicios, posibilidad de reorganizar las redes, métodos eficientes de trabajo para operar las redes y competencia entre empresas operadoras privadas. ITU-T (1992), El modelo TMN define tres arquitecturas diferenciadas:

Arquitectura funcional, describe la distribución de la funcionalidad dentro de la TMN, con el objeto de definir los bloques funcionales a partir de los cuales se construye la TMN.

Arquitectura física, describe los interfaces y el modo en que los bloques funcionales se implementan en equipos físicos.

Arquitectura de la información, sigue los principios de los modelos OSI de gestión (CMIS y CMIP) y directorio (X500).

Estos bloques proporcionan la funcionalidad que permite a la TMN realizar sus funciones de gestión. A continuación se describen los distintos tipos de bloques funcionales:

Función de operación de sistemas (OSF). Los OSF procesan la información relativa a la gestión de la red con el objeto de monitorizar y controlar las funciones de gestión.

Función de estación de trabajo (WSF). Este bloque funciona proporciona los mecanismos para que un usuario pueda interactuar con la información gestionada por la TMN.

Función de elemento de red (NEF). Es el bloque que actúa como agente, susceptible de ser monitorizado y controlado.

Estos bloques proporcionan las funciones de intercambio de datos entre los usuarios de la red de telecomunicaciones gestionada.

Función de mediación (MF). La función de mediación se encarga de garantizar que la información intercambiada entre los bloques del tipo OSF o NEF cumple los requisitos demandados por cada uno de ellos.

Puede realizar funciones de almacenamiento, adaptación, filtrado y condensación de la información. Cada bloque funcional se compone a su vez de un conjunto de componentes funcionales, considerados como los bloques elementales para su construcción.

3.- DEFINICIÓN DE TÉRMINOS BÁSICOS

Es muy importante tener claro algunos conceptos básicos sobre las redes. Para ello, a continuación se presenta una definición de términos básicos que pueden ayudar a este propósito:

ANCHO DE BANDA: Determina la tasa a la cual la información puede ser enviada a través de un canal a mayor ancho de banda, mayor cantidad de información que puede ser enviada en un tiempo dado. (Boehm, 1981)

BRIDGES (puentes): Conectar dos o más redes entre sí, aún teniendo diferentes topologías, pero asumiendo que utilizan el mismo protocolo de red y segmentar una red en subredes. (Recio, 2001)

CARRIERS: Empresas que dan el servicio de comunicaciones locales (urbanas) no son las mismas que manejan las comunicaciones de larga distancia (interurbanas) (Sheldom, 1994)

CONMUTADOR O SWITCH: Es un dispositivo de conexión que permite la transmisión de datos desde distintos equipos de una red al mismo tiempo. (Sheldom, 1994)

DIRECCIÓN: Todos los nodos de la red deben tener una dirección que los identifique dentro de la red de forma única, La dirección de un nodo depende del protocolo de comunicación que se está utilizando. (Recio, 2001)

GATEWAYS (Pasarelas): Permiten interconectar redes de diferentes arquitecturas, topologías y protocolos. No sólo realiza funciones de

encaminamiento, sino que también realiza conversiones de protocolos. (Recio, 2001)

GESTIÓN: Todas las medidas que aseguran la efectiva y eficiente operación de un sistema adecuando sus recursos a un objetivo. (Recio, 2001)

HUBS (Concentradores): Se trata de un dispositivo que centraliza la conexión de los cables procedentes de las estaciones de trabajo. (Recio, 2001)

INSTITUTO NACIONAL AMERICANO DE ESTÁNDARES (ANSI): Diseña y propone recomendaciones para los estándares de comunicaciones internacionales. (Jones, 1986)

INTERCONEXIÓN DE REDES: La necesidad de interconectar dos o más redes es compartir recursos o la división en dos subredes de una red, para mejorar el rendimiento de ésta. En ambos casos es necesaria la presencia de un dispositivo (que puede ser un hubs, un bridges, un routers, entre otros). (Recio, 2001)

ISO (International Organization for Standardization): Organización de normalización reconocida mundialmente. Su objetivo es el de promover y desarrollar normas para el intercambio internacional. (Recio, 2001)

LINEA DE ACCESO: Una línea de comunicaciones (p.ej. circuito) que interconecta un dispositivo compatible. (Jones, 1986)

OSI (Open Systems Interconenection): Se trata de un modelo elaborado por la ISO que define los protocolos de comunicación en siete niveles diferentes. (Recio, 2001)

PAQUETE: Un paquete es básicamente el conjunto de información a transmitir entre dos nodos, añadiendo datos de control como la dirección de la máquina que envía la información y la dirección de la máquina a la que va destinada la información (dirección destino). (Recio, 2001)

ROUTERS (Encaminadores): Se trata de dispositivos que interconectan redes a nivel de red del modelo OSI de la ISO. Realizan funciones de control de tráfico, encaminamiento de paquetes por el camino más eficiente en cada momento. (Recio, 2001)

SNMP: Protocolo llamado Simple Netwoek Management Protocolo. Integra la gestión de diferentes tipos de redes mediante un diseño sencillo. (Jones, 1986)

TCP/IP: Son dos protocolos de comunicaciones: el protocolo TCP (Protocolo de control de transmisión) que se establece al nivel de transporte del modelo OSI y el protocolo IP (Internet protocolo) que pertenece al nivel de red. (Recio, 2001)

TRAMA: El concepto de trama es de más bajo nivel que el de paquete. Una trama es un paquete o parte de un paquete (a veces los paquetes se fragmentan si son muy grandes) al que se le añade información de control. Las tramas son los elementos que circulan por el medio físico. (Recio, 2001)

4.- CUADRO DE OPERACIONALIZACIÓN DE LA VARIABLE

Cuadro 03

Cuadro de Operacionalización de la Variable

Objetivo General: Diseñar una propuesta de interconexión de redes para el funcionamiento en la zona educativa del Estado Trujillo.

Objetivos Específicos	Variable	Dimensiones	Indicadores
Diagnosticar la situación presentada en la zona educativa del Estado Trujillo en cuanto a interconexión de redes.	Interconexión de Redes	Características de Redes	Tipo de Red. Equipos. Cableado Estructurado.
Determinar los mecanismos de gestión de red desarrollados por la zona educativa del Estado Trujillo.		Seguridad de la Información	Herramientas para monitorear. Recursos.
Determinar la factibilidad de la propuesta sobre interconexión de redes de la zona educativa del Estado Trujillo.		Teórica	Coherencia. Contenido Pertinente. Congruencia.
Elaborar la propuesta de interconexión de redes dirigida a la zona educativa del Estado Trujillo.		Práctica	Simulación

Fuente: Moreno (2008)