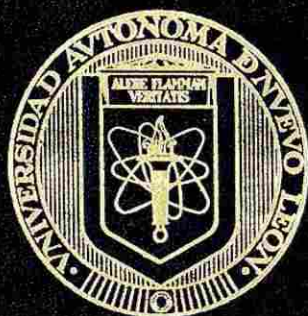


UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE INGENIERIA MECANICA Y ELECTRICA
DIVISION DE ESTUDIOS DE POST-GRADO



**TECNOLOGIAS E INTERCONEXIONES DE REDES DE
TELECOMUNICACIONES**

POR

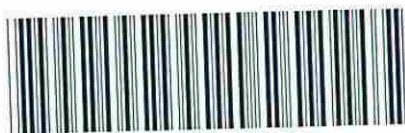
ING. JESUS EVARISTO RAMIREZ RODRIGUEZ

T E S I S

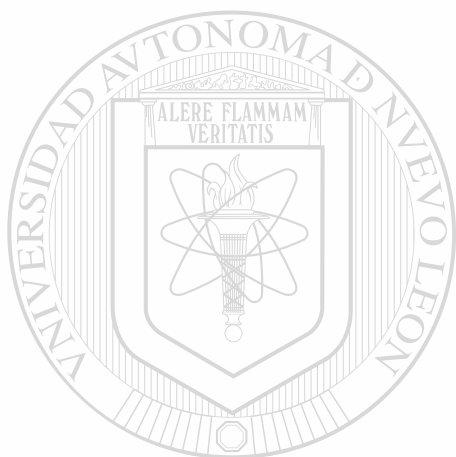
**EN OPCION AL GRADO DE MAESTRO EN CIENCIAS
DE LA INGENIERIA ELECTRICA CON ESPECIALIDAD
EN TELECOMUNICACIONES**

SAN NICOLAS DE LOS GARZA, N. L.

JUNIO DE 2000



1020146049



UANL

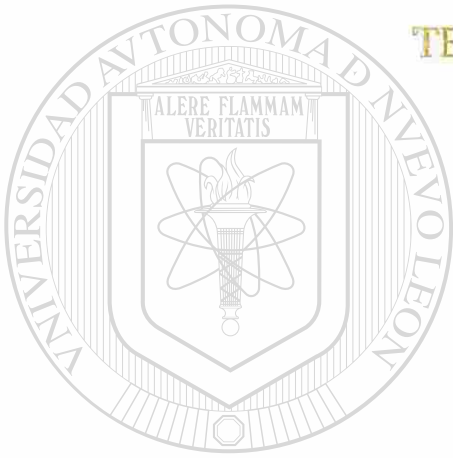
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



DIRECCIÓN GENERAL DE BIBLIOTECAS

UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE INGENIERIA MECANICA Y ELECTRICA
DIVISION DE ESTUDIOS DE POST-GRADO

TECNOLOGIAS E INTERCONEXIONES DE REDES DE
TELECOMUNICACIONES



UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

POR

DIRECCIÓN GENERAL DE BIBLIOTECAS
ING. JESUS EVARISTO RAMIREZ RODRIGUEZ

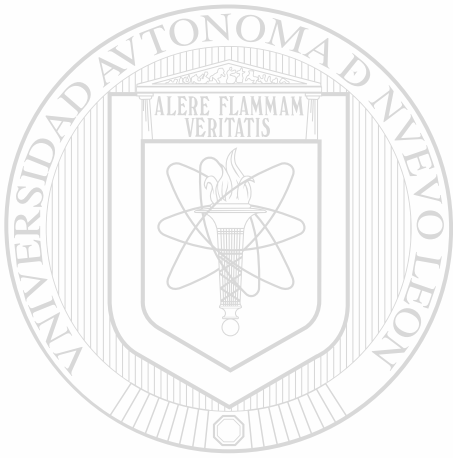
T E S I S

EN OPCION AL GRADO DE MAESTRO EN CIENCIAS
DE LA INGENIERIA ELECTRICA CON ESPECIALIDAD
EN TELECOMUNICACIONES

SAN NICOLAS DE LOS GARZA, N. L. JUNIO DE 2000

0151-40960.

TH
25853
•Ma
FINE
2000
R354



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

®

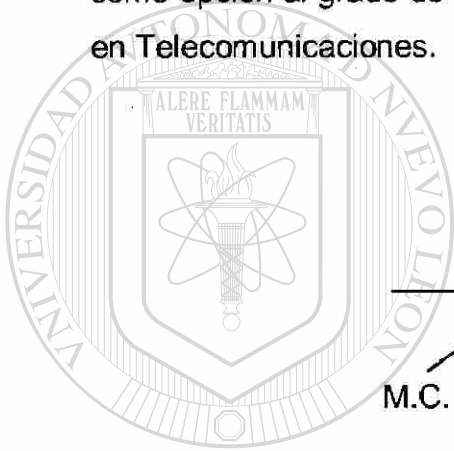
DIRECCIÓN GENERAL DE BIBLIOTECAS



FONDO
TESIS

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA.
DIVISIÓN DE ESTUDIOS DE POST-GRADO


Los miembros del comité de tesis recomendamos que la tesis "Tecnologías e Interconexión de Redes de Telecomunicaciones" realizada por el alumno Jesús Evaristo Ramírez Rodríguez, matrícula 788013 sea aceptada para su defensa como opción al grado de Maestro en Ciencias de la Ingeniería con especialidad en Telecomunicaciones.




El Comité de Tesis.


Asesor
M.C. Leopoldo Rene Villarreal Jiménez.

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN


Coasesor
M.C. Ciro Calderon Cardenas.


Coasesor
M.C. Fernando Estrada Salazar.


Vo.Bo.
M.C. Roberto Villarreal Garza.
División de Estudios de Post-grado.

San Nicolás de los Garza, N.L. a 26 de Mayo de 2000.

Prologo

La necesidad es la madre de toda invención, y como tal la comunicación es el ejemplo mas claro que pueda existir. Es muy probable que la comunicación de datos comenzara mucho antes de registrar el paso del tiempo. El ser humano siempre a tenido la necesidad de comunicarse con otras personas, ya que una de sus cualidades es ser sociable. Por esta razón, el ser humano ha buscado desde épocas muy remotas la manera de satisfacer esta necesidad.

De esta manera, el ser humano desarrollo el lenguaje y la escritura como un medio para poder comunicarse con otras personas. Sin embargo, como muchas de las personas con las que se necesitaba comunicar se encontraban en lugares distantes, busco la manera de poder comunicarse con ellos. Por ello desarrollo las señales. Telecomunicación, del griego tele:lejos y del latín communicatio: comunicación. Comunicación a grandes distancias.

La telecomunicación es el poder de comunicarse con otras personas que se encuentran en lugares distantes. Entonces, podemos decir que el ser humano desarrollo la telecomunicación desde épocas muy remotas, la cual hoy en día, la distancia es relativa.

Para establecer cualquier comunicación, bien sea entre personas o entre maquinas, siempre hacen falta una serie de normas que regulen dicho proceso. En el caso de las comunicaciones entre personas, las normas las establece la sociedad y son aplicadas por cada persona de acuerdo con su educación; en el caso de las maquinas, las normas las establecen los organismos internacionales de normalización y son aplicadas por las computadoras de acuerdo con el protocolo software que estén utilizando. Pero la diferencia fundamental entre personas y maquinas es la inteligencia y es por eso que las computadoras deben tener protocolos mas estrictos, que tengan previstos los

posibles casos que se puedan presentar en una comunicación, sin dejar nada al azar.

La necesidad de estar bien comunicado hoy en día es indispensable. Para satisfacer las grandes demandas en los servicios de comunicación, se requieren redes de telecomunicaciones sumamente rápidas, seguras y eficientes, es decir, se requieren redes de telecomunicaciones bien administradas analizando los puntos a favor y en contra perfectamente, teniendo en cuenta la rápida evolución que presentan las tecnologías actuales.

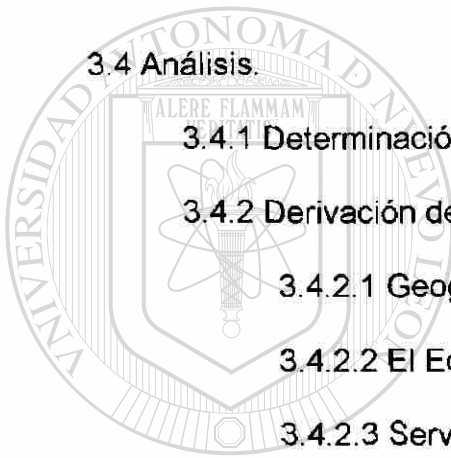
El objetivo de esta investigación, es abordar las tecnologías actuales en redes de telecomunicaciones de una manera clara y sencilla, a fin de entender sus diferencias y por ende sus aplicaciones, con un amplio conocimiento de cómo administrarlas e implementarlas. Para asimilar mejor el contenido de esta investigación, se deben tener sólidos los fundamentos sobre la comunicación de información, sin embargo, si no se tienen estos, no es limitante alguna para comprender el contenido de este material.

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN[®]
DIRECCIÓN GENERAL DE BIBLIOTECAS

Indice

	Página.
Síntesis	10
Capítulo 1	12
INTRODUCCIÓN.	12
1.1 Descripción del Problema a Resolver.	12
1.2 Objetivo de la Tesis.	12
1.3 Definición de la Hipótesis.	13
1.4 Justificación de la Tesis.	13
1.5 Limite del Estudio.	14
1.6 Metodología.	14
1.7 Revisión Bibliográfica.	15
Capítulo 2	16
INTRODUCCIÓN A LAS TELECOMUNICACIONES.	16
2.1 Calidad de Servicio.	16
2.1.1 Definición de Qos.	16
2.1.2 Garantías de Qos.	20
2.1.3. Obtención de Qos.	22
2.2 Integración de Voz y Datos.	24
2.3 Interconexión de Redes.	27
2.4 Evolución de las Redes Ethernet: Hacia el GigaEthernet.	33
2.4.1 Conceptos Básicos.	33
2.4.2 Ethernet Compartida.	37
2.4.3 Fast Ethernet.	40
2.4.4 Red Compartida y Red Conmutada.	41
2.4.5 GigaEthernet.	44

Capitulo 3	50
METODOLOGÍA PARA LA PLANEACIÓN DE UNA RED.	50
3.1 Introduccion.	50
3.2 Fases de Ciclo de Vida de una Red de Comunicación.	52
3.3 Planeación.	52
3.3.1 Definición del Proyecto.	53
3.3.2 Formación del Equipo de Trabajo.	55
3.3.3 Elaboración de un Plan de Trabajo.	56
3.4 Análisis.	58
3.4.1 Determinación de los Requerimientos.	58
3.4.2 Derivación de las Especificaciones.	60
3.4.2.1 Geografía a la que se va a Servir.	61
3.4.2.2 El Equipo que se Utilizará.	62
3.4.2.3 Servicios de Red.	62
3.4.2.4 Especificaciones de Tráfico.	63
3.4.2.5 Capacidad de la Red y Rendimiento.	63
3.4.2.6 Interfases al Usuario.	63
3.4.2.7 Software.	64
3.4.2.8 Tipo de Procesamiento.	64
3.4.2.9 Seguridad.	64
3.4.2.10 Parámetros de Construcción.	65
3.4.2.11 Comunicación.	65
3.4.3 Justificación Económica.	66



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN
DIRECCIÓN GENERAL DE BIBLIOTECAS



3.4 Diseño.	66
3.4.1 Definición de la Arquitectura y Subsistemas.	67
3.4.2 Verificación de la Solución.	68
Capitulo 4	71
METODOLOGÍA PARA ADMINISTRACIÓN DE UNA RED.	71
4.1 Herramientas de Software para la Planeación y Diseño de la Red.	71
4.2 Desarrollo e Instrumentación.	72
4.2.1 Plan de Implementación e Instalación.	72
4.2.2 Selección y Adecuación del Sitio de Instalación.	73
4.2.3 Planeación, Administración e Instalación del Cableado.	74
4.2.4 Contratación de Circuitos y Enlaces Públicos.	75
4.2.5 Selección y Adquisición de Equipo.	76
4.2.6 Instalación del Hardware/Software.	77
4.2.7 Pruebas y Verificación del Funcionamiento.	79
4.2.8 Capacitación de Usuarios y Personal de Explotación.	80
4.2.9 Inicio de la Explotación y Administración.	81
4.3 Explotación y Administración.	82
4.3.1 Funciones de Administración de la Red.	83
4.3.2 Control de la Red.	84
4.3.3 Seguridad de la Red.	86
4.3.3.1 Seguridad Física.	86
4.3.3.2 Control de Acceso.	87
4.3.3.3 Seguridad de la Transmisión.	89
4.4 Análisis del Requerimiento de la Red.	91

4.5 Planeación y Reconfiguración de la Red.	91
Capitulo 5	93
AREAS FUNCIONALES DE LA ADMINISTRACIÓN DE REDES.	93
5.1 Administración de la Configuración.	93
5.2 Administración del Desempeño y la Contabilidad.	94
5.3 Administración de Problemas.	94
5.4 Administración de Operaciones.	95
5.5 Administración de Cambios.	95
5.6 Arquitectura de la Administración de Red.	96
5.6.1 Arquitectura ONA.	96
5.6.2 System View.	97
5.7 Plataformas de Administración de la Red.	97
5.8 Administrador LAN	98
5.9 Protocolo SNMP.	98
5.9.1 Una Amplia Base de Información (MIB de SNMP).	101
5.9.2 Administración de Sistemas Extendidos.	103
5.9.3 Tipos de Mensajes Entre Agentes y Administradores.	104
5.9.4 Factores de Seguridad en SNMP.	105
5.9.5 Formato del Mensaje de SNMPv2.	106
5.9.6 Formato PDU GetBulk.	108
5.9.7 Gestión a Distancia.	109
Capitulo 6	
CONCLUSIONES Y RECOMENDACIONES.	
6.1 Conclusiones.	114
6.2 Recomendaciones.	116
BIBLIOGRAFÍA.	118
LISTADO DE TABLAS Y FIGURAS.	119
GLOSARIO	120
RESUMEN AUTOBIOGRAFICO.	131

Síntesis.

Cada una de las diversas redes de telecomunicaciones de área amplia así como las redes de área local tienen distintas características particulares, por lo que la elección de la red de comunicaciones ideal para las necesidades de un usuario puede resultar un tanto complicado, al proponerla se debe tomar en cuenta diversos aspectos como el diseño, planeación, seguridad y administración entre otros de acuerdo a la necesidad específica del usuario cuidando siempre el costo – beneficio.

Cabe mencionar que esta investigación es abordar las tecnologías y algunos métodos de administración de proyectos de redes, más actuales en redes de telecomunicaciones de una manera clara y sencilla, a fin de entender sus diferencias y por ende, sus aplicaciones.

La presente investigación introduce a las telecomunicaciones analizando algunos aspectos generales de la calidad de servicio que son básicamente las base fundamentales de cualquier misión. La calidad de servicio es un concepto basado en el hecho de que no todas las aplicaciones necesitan el mismo desempeño de la red sobre la que corren. Por lo cual, las aplicaciones deben indicar sus requerimientos específicos a la red, antes de que empiecen a transmitir sus datos. Las redes locales proporcionan muchas ventajas, pero quizás nos hemos olvidado de las ventajas más técnicas y que quizás el usuario final no aprecia. Las redes locales son muy flexibles en su instalación, tiene una gran capacidad de expansión ya que hacen posible el crecimiento, se controlan de manera local y su mantenimiento es relativamente sencillo. Dada su gran capacidad de transmisión y que pueden organizarse de manera departamental podemos decir que su costo de adquisición / mantenimiento / funcionalidad está en un punto medio bajo. Se muestra el esquema metodológico presentado para la implantación de redes corporativas lo podemos dividir en tres fases secuenciales dentro de un ciclo de aprendizaje de las telecomunicaciones de la empresa de la siguiente forma: Planeación, análisis y diseño. Desarrollo e

instrumentación. Explotación y administración. Estas fases están englobadas dentro de un marco general de administración y seguimiento de un proyecto. El proceso de desarrollo de un sistema teleinformático es repetitivo y termina cuando se encuentra la solución más adecuada para satisfacer las necesidades de la empresa o negocio que solicita la red. Cada una de las etapas por las que pasa el proyecto de telecomunicaciones puede ocasionar modificaciones en las anteriores, es decir, los planes pueden ir cambiando dependiendo de las condiciones o circunstancias que se presenten durante el avance del proyecto. La administración de una red abarca las actividades necesarias para operar y mantener la red en las condiciones necesarias para que a través de su vida útil satisfaga las necesidades de los usuarios; tales como disponibilidad, eficiencia y estabilidad y las necesidades del negocio; las nuevas aplicaciones, los nuevos clientes, adoptar nueva tecnología, operación remota, cambios y crecimiento. En términos generales la administración de una red consiste de un conjunto de acciones, métodos y procedimientos que se llevan a cabo para mantener la operación continua de una red. El capítulo 5 veremos algunas áreas funcionales de administración de redes las cuales se dividen en cinco funciones basadas en el usuario: administración de la configuración, administración del desempeño y la contabilidad, administración de problemas, administración de operaciones y administración de cambios. Así mismo como diversos tipos de arquitecturas de red, plataformas y un protocolo muy importante, el protocolo de administración simple de red y sus componentes más importantes.

CAPITULO 1

INTRODUCCIÓN

1.1 Descripción del Problema a Resolver.

El personal encargado de las telecomunicaciones en las empresas o universidades, se enfrentan a grandes problemas, como compatibilidades de equipos, eficiencia en su red de telecomunicación, altos costos en comunicaciones a través de voz, datos e imagen. Estos problemas se ven reflejados al implementar o emigrar a nuevas tecnologías en redes de telecomunicaciones.

1.2 Objetivo de la Tesis.

El objetivo de esta tesis es el de analizar circuitos eléctricos y electrónicos en los sistemas y redes de telecomunicaciones proporcionando de una manera sencilla conceptos, alternativas, beneficios, desventajas de algunas tecnologías existentes en el mercado, dando énfasis a los siguientes puntos:

- 1.- Proporcionar de manera objetiva y clara, algunos conceptos, descripciones y formas de operación de algunas tecnologías, que se encuentran en el estudio y en la practica de la ingeniería eléctrica así como fundamentos y principios básicos.
2. - El enfoque está dirigido a maestros y estudiantes de ingeniería eléctrica.

3. - Suministrar una herramienta para la correcta elección de las tecnologías para la implementación de una red de telecomunicaciones.

1.3 Definición de la Hipótesis.

La variedad de opciones disponibles en cuanto a la tecnología de red adecuada para transporte de esa información naturalmente hace que crezcan las dudas al tener que ser tomada una decisión. Los requerimientos típicos en una organización al deber seleccionar entre una y otra, son que la tendencia escogida responda principalmente a las exigencias funcionales de sus aplicaciones, unido a una mayor productividad en términos de costo-beneficio.

Con esta tesis se pretende demostrar que la tecnología escogida debe permitir evolucionar de una manera práctica a tendencias futuras, de forma tal que permita sea más perdurable la selección, mediante un estudio profundo de los antecedentes y la nueva tecnología a usar que debe de brindar una compatibilidad de equipos así como aumentar la eficiencia de las redes de telecomunicaciones y aprovechar los recursos para la transmisión de voz, datos y vídeo para reducir los costos. Además para la toma de una decisión una organización necesita conocer cuáles son las características, ventajas y facilidades de cada una de las arquitecturas de red disponibles. ®

DIRECCIÓN GENERAL DE BIBLIOTECAS

1.4 Justificación de la Tesis.

Las redes para el transporte de información, en cualquiera de sus presentaciones, constituyen hoy día un medio fundamental, de definitivo peso en los resultados de cualquier actividad productiva.

Esta tesis será escrita para dar soluciones alternativas para la elección apropiada de acuerdo a las necesidades específicas del usuario o administrador de una red de telecomunicaciones ya sea para implementarla, ayudándole a

seleccionar el equipo y tecnologías existentes en el mercado, que se adecue a sus necesidades y represente una inversión económica a largo plazo siendo escalable con las recientes tecnologías o simplemente emigrar a una nueva tecnología, analizando el reutilizamiento de los recursos existente.

Así como apoyo a los programas académicos y proporcionar una herramienta a los cursos universitarios a nivel licenciatura, tomando en cuenta que el uso de las computadoras y telecomunicaciones hoy en día en la vida profesional de cualquier persona es ya indispensable. Con base a lo anteriormente expuesto, se cubren los fundamentos esenciales tratando todos los tópicos a un nivel que no se requiere un conocimiento avanzado por parte del lector en el área de las telecomunicaciones y redes.

1.5 Limite del Estudio.

La tecnología en telecomunicaciones crece a pasos agigantados, razón por la cual las tecnologías quedan obsoletas en poco tiempo, sin embargo estas tecnologías son bases firmes para tecnologías futuras en el área de las redes de telecomunicaciones.

La investigación por separado de diversas instituciones para integrar en sus productos diversas características y hacerlos más competitivos ante su competencia, sin perder las normas establecidas de compatibilidad entre equipos, nos conduce a un mundo de información bastante grande y enriquecido, razón por la cual solo se trataran algunos fabricantes.

1.6 Metodología.

Se describe algunas tecnologías de transporte de información utilizadas en redes de telecomunicaciones incluyendo antecedentes, forma de operación, la tecnología según el modelo OSI, mostrando con un proyecto las aplicaciones al finalizar.

Se realizara una semblanza de cómo definir las necesidades existentes en el área que se desee implementar o emigrar a una nueva tecnología, haciendo una revisión de los antecedentes de la red existente, relación de estudios de campo que llevan al estudio a una plataforma mas objetiva para determinar las compatibilidades, ventajas y desventajas de las nuevas tecnologías, así como recomendaciones aplicando todo lo anterior a un caso práctico en la interconexión de las redes de telecomunicaciones.

1.7 Revisión Bibliográfica.

Las similitudes de estas tesis con otros estudios es que los equipos, las configuraciones, son utilizados internacionalmente, de esta manera podemos apoyarnos con otras empresas dentro y fuera del país, para la revisión de equipo, configuraciones o maneras adecuadas para la perfecta conectividad.

Una de las principales diferencias es que los textos se enfocan al mercado, protocolos y estándares norteamericanos y en ocasiones no son compatibles en nuestro país. Aquí se adoptan estas tecnologías, protocolos y estándares compatibles con los europeos.

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

DIRECCIÓN GENERAL DE BIBLIOTECAS



CAPITULO 2

INTRODUCCION A LAS TELECOMUNICACIONES.

2.1 Calidad de Servicio.

Todos los que tienen relación con las redes y telecomunicaciones, están vinculados con el término QoS (Quality of service; Calidad de servicio). Comúnmente, en el área de investigación se han publicado artículos en revistas técnicas, o se ha hablado de la expresión en conferencias o seminarios; incluso hay libros enteros dedicados solamente a este concepto, al igual que en la industria también la palabra es muy común.

Siendo QoS un término frecuentemente utilizado, es uno de los tópicos más confusos, ambiguos y poco entendidos de la industria de las redes y telecomunicaciones. Parece mentira que un concepto en apariencia tan simple pueda crear tanto desconcierto.

2.1.1 Definición de QoS.

Como ya se mencionó, QoS es un acrónimo del término en inglés Quality of Service, que literalmente se traduce como calidad de servicio. Los problemas empiezan por ahí, ya que tanto calidad como servicio significan diferentes cosas para muchas personas. Usualmente se utiliza el adjetivo "calidad", al describir el proceso de enviar datos en confiable y eficaz. Por su parte, "servicio es

también un término ambiguo que puede significar algo que se ofrece a los usuarios de una red (por ejemplo, los servicios de e-mail).

La calidad de servicio es un concepto que se maneja incluso en medios de transporte de información no computarizados. Los servicios postales y de mensajería ofrecen distribución de entrega normal, entrega inmediata, envíos certificados, etcétera. Obviamente los clientes pagarán diferentes cuotas por distintos tipos de servicios. El mismo concepto de otorgar diversos niveles de servicio a los usuarios es aplicable a las redes, porque es cierto que no todas las aplicaciones poseen los mismos requerimientos y, por lo tanto, para hacer uso adecuado de los recursos disponibles, se les debe brindar el nivel de calidad de servicio que resulte apropiado.

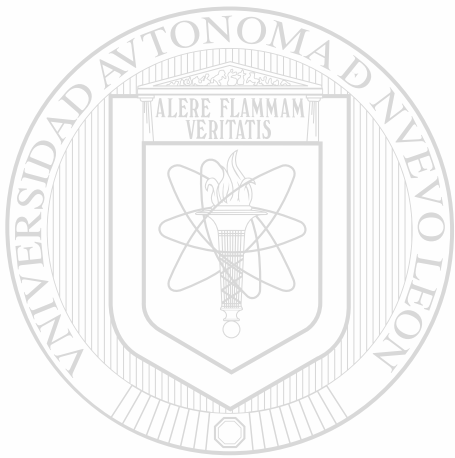
De entre las diferentes definiciones del concepto "calidad de servicio", podemos encontrar:

"La calidad de servicio es un concepto basado en el hecho de que no todas las aplicaciones necesitan el mismo desempeño de la red sobre la que corren. Por lo cual, las aplicaciones deben indicar sus requerimientos específicos a la red, antes de que empiecen a transmitir sus datos".

"QoS es la especificación cuantitativa y cualitativa de los requerimientos de una aplicación, los cuales deben satisfacer un sistema multimedia con el fin de obtener la calidad deseada de la aplicación."

Algunas de las conclusiones principales que se pueden obtener de las anteriores definiciones son: 1) Las aplicaciones especifican sus requerimientos de QoS; 2) Los sistemas proveen (o intentan proveer) garantías de QoS. De hecho, varias cosas pueden pasar entre estas dos acciones, ya que el sistema, antes que nada, deberá determinar si tiene suficientes recursos para satisfacer los requerimientos; y de ser así, reservará los recursos necesarios. Pero si no

JERR



**TECNOLOGÍAS E INTERCONEXIONES DE REDES DE
TELECOMUNICACIONES**

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

DIRECCIÓN GENERAL DE BIBLIOTECAS

TM
Z5853
.M2
FIME
2000
R354

2000

resulta de esta forma, podrá optar por rechazar la petición de la aplicación, o bien sugerir un nuevo conjunto de requerimientos que sí puede satisfacer.

Bajo esta última opción, la aplicación podrá aceptar la propuesta y continuar con su ejecución, o no aceptarla y someterse al rechazo por parte del sistema. Claro que la aplicación podrá, posteriormente, volver a iniciar el proceso de negociación, en espera de que se hayan liberado recursos que puedan asignársela. De lo anterior, se tienen los siguientes elementos necesarios para proveer garantías de QoS:

- Un mecanismo de especificación de QoS, mediante el cual las aplicaciones puedan determinar sus requerimientos.
- Control de admisión para determinar si las nuevas aplicaciones pueden ser admitidas en el sistema sin afectar el nivel de QoS, de las otras que ya fueron admitidas.
- Un sistema de negociación (Y renegociación) de QoS para servir a tantas aplicaciones como sea posible.
- Reserva y calendarización de recursos para satisfacer los requerimientos de las aplicaciones aceptadas.
- Monitoreo, como políticas de tráfico, para asegurar que las aplicaciones no se salgan de los límites de los requerimientos aceptados.

CoS: otro acrónimo a la lista

Son muchos los acrónimos que se manejan en el ambiente de las redes, pero eso no detiene el avance de la creación de otros, es por eso que ha surgido uno nuevo que tiene relación con el de calidad de servicio: CoS (Classes of Service; Clases de servicio).

Es muy usual que se confundan los conceptos de CoS y QoS, llegando incluso a pensar que son lo mismos, aunque en realidad existen diferencias quizá sutiles. QoS, por lo general, tiene connotaciones más amplias (y

ambiguas). Por su parte, CoS implica que los servicios se categorizarán en clases diferentes, las cuales, a su vez, serán tratadas individualmente. De modo que, antes de proveer una mayor calidad de servicio a un cliente, aplicación o protocolo, se debe clasificar el tráfico, y luego determinar la forma de manejo de las diferentes clases de tráfico que se muevan por la red.

Los métodos más usuales de realizar la diferenciación y clasificación de tráfico tienen como base alguno de los siguientes aspectos:

- **Protocolo.** Protocolos de red y transporte tales como IP (Internet Protocol; Protocolo Internet), TCP (Transmission Control Protocol; Protocolo de control de transmisiones), UDP (User Datagram Protocol; Protocolo de datagrama de usuarios), IPX (Internetworking Packet exchange; Intercambio de paquetes de interconexión de redes).
- **Puerto del protocolo.** Para protocolos de aplicación tales como Telnet, SAPs (Service Access Point; Punto de acceso al servicio) de IPX.
- **Dirección del host.** Dirección del host específica al protocolo, indicando origen o destino del tráfico.
- **Interfase del dispositivo fuente.** Interfase sobre la cual el tráfico entra a un dispositivo particular, conocida también como interfase de ingreso.

La diferenciación se realiza usualmente para clasificar el tráfico, de forma tal, que se pueda apegar a los mecanismos que implementan las políticas definidas por el administrador de red.

2.1.2 Garantías del QoS

Se ha visto que cuando una aplicación hace una especificación de parámetros de calidad de servicio, es porque se espera que la red haga algo al respecto. En otras palabras, si la red acepta la especificación, entonces debe cumplir con ciertas obligaciones para satisfacer la calidad respectiva deseada. Esto puede sonar trivial pero en realidad es más complejo de lo que parece a primera vista.

Cuando se establece una conexión con un nivel de QoS especificado, los parámetros de éste se traducen y negocian entre los diferentes subsistemas involucrados. Solamente cuando todos los subsistemas han llegado a acuerdos y pueden otorgar garantías respecto a los parámetros especificados, será que se satisfagan los requerimientos de QoS de extremo a extremo.

Durante el proceso de negociación de QoS pueden suceder una serie de pasos. Primero, los parámetros de QoS son mapeados o traducidos de una capa (o subsistema) a otra. Segundo, cada capa o subsistema deberá determinar si puede dar soporte al servicio requerido (entrando en juego los algoritmos de control de admisión); de ser así, deberán reservarse ciertos recursos para la sesión, sólo hasta que todos los subsistemas hayan aceptado los parámetros de QoS, porque de otra forma la sesión es rechazada.

Asimismo, habrá sistemas sofisticados que puedan indicar al usuario el nivel de QoS para el cual tienen soporte, de tal forma que si el usuario está satisfecho con el nivel sugerido, entonces se podrá asentar la sesión. También habrá sistemas que permitan renegociar el nivel de QoS una vez establecida la sesión, esto con el fin de adaptarse a las condiciones cambiantes de uso de la aplicación. Falta precisar que las garantías de QoS en realidad pueden ser de cualquiera de los siguientes tres tipos:

Garantías determinísticas (o rígidas).

El nivel de QoS especificado por el usuario debe ser satisfecho al cien por ciento. Esta garantía es la más cara en cuanto a recursos del sistema. Usualmente se reservan los recursos para la aplicación con base al escenario del peor caso. Aún cuando no se estén usando algunos recursos, éstos no pueden ser utilizados por otra aplicación, lo cual resulta un desperdicio.

Por ejemplo, un video codificado con tasa variable de bits tiene una salida de 200 Kbps a 4 Mbps; para satisfacer el flujo en un cien por ciento se deben almacenar recursos tomando en cuenta la tasa de 4 Mbps. Cuando el flujo de video no está a su tasa máxima, habrá algunos recursos reservados que están siendo desperdiciados. No obstante, una garantía rígida es fácil de implementar, ya que los recursos se aprovisionan en forma estática.

Garantías estadísticas (o suaves).

El nivel de QoS especificado por el usuario debe ser satisfecho en un porcentaje determinado. Este tipo de garantía es la que resulta más apropiada para medios continuos, los cuales usualmente no requieren una precisión del cien por ciento al ser tocados o reproducidos; al igual que este tipo de garantías usa en forma más eficiente los bienes.

El empleo de recursos se basa en multicanalización estadística: los recursos que no están siendo usados por una aplicación podrán ser utilizados por otras. Este es el modo de operación deseado para la comunicación multimedia, aunque resulta difícil de implementarlo debido a la naturaleza dinámica del tráfico y utilización de medios.

Mejor esfuerzo.

No se proveen garantías y la aplicación se ejecuta con los recursos que se encuentren disponibles. Las redes convencionales Ethernet y las IPv4 (Internet Protocol version 4; Protocolo Internet versión 4) son ejemplos de redes que operan bajo este esquema. Debe tomarse en cuenta que en una sesión de comunicación multimedia pueden requerirse los tres tipos de garantías anteriores, ya que se darán diversas garantías a distintos tipos de tráfico. Habrá incluso casos en que se utilicen diferentes modelos de garantías para varios parámetros de QoS,

Por ejemplo, el usuario puede pedir una tasa de error garantizada al cien por ciento (garantía rígida), pero que el retardo se satisfaga en un 90 por ciento (garantía suave).

2.1.3 Obtención de QoS

Recordemos que el modelo general (y básico) de la comunicación comprende al emisor, el canal y el receptor; aplicando este modelo a redes de comunicaciones tendremos elementos como computadoras, dispositivos de conmutación e interconexión (switches, routers, entre otros), enlaces (alámbricos, inalámbricos, y demás). Por lo tanto, para lograr una comunicación con QoS garantizado, se tienen que involucrar todos los elementos desde un extremo a otro.

Esto es en teoría, porque en la práctica ya existen diferentes elementos que proveen QoS, pero poder encontrar ambientes donde todos los elementos garanticen un nivel de QoS es bastante difícil.

Actualmente se tienen protocolos como ATM (Asynchronous Transfer Mode; Modo de transferencia asíncrona), los cuales fueron diseñados con capacidades inherentes para el manejo de QoS. Otros como TCP/IP (Transmission Control Protocol / Internet Protocol; Protocolo de control de transmisiones / Protocolo Internet) no contemplan en su diseño las capacidades de ATM, pero se han encontrado soluciones tales como RSVP (Resource Reservation Protocol), que es un protocolo para reservar recursos a lo largo de un flujo de comunicación.

Es un hecho que el tráfico en las redes de comunicaciones sigue creciendo conforme el ancho de banda lo permite; lo cual se ve acentuado conforme surgen nuevas aplicaciones con capacidades multimedia que demandan cada vez más recursos. Ante este problema, algunos adoptan la posición de aumentar la capacidad de la red: "Si el tráfico crece, entonces aumento el ancho de banda y asunto solucionado".

La implantación de capacidades de manejo de QoS provee una alternativa de solución con más largo alcance. El uso de mecanismos de diferenciación de tráfico en clases de servicio permite a los proveedores de servicios de comunicaciones tener mayor control sobre el tráfico y tarifarlo adecuadamente.

DIRECCIÓN GENERAL DE BIBLIOTECAS

2.2 Integración de Voz y Datos

Tiempo atrás la función de una red era ahorrar dinero optimizando el uso de los enlaces de transmisión de baja velocidad y costo elevado, pero con el paso del tiempo estos enlaces han pasado a ser de gran capacidad y bajo costo. Aunque esta es una de las principales razones del aumento del número de redes existentes, en la práctica hay muchas otras razones para instalarse una red.

La razón por la que el costo del ancho de banda necesario es tan pequeño es porque los enlaces individuales son muy rápidos de forma que son compartidos por varios usuarios.

En el caso de varias estaciones y dispositivos, un usuario sólo precisa un sencillo dispositivo para comunicarse con el resto simultáneamente. Sin una red habría que tener un enlace punto a punto desde cada dispositivo hasta el otro con el que se quiere comunicar, con lo que cada uno precisa de un número elevado de conexiones, cada una de las cuales se incluyen en el costo total.

Con una red cada dispositivo tan sólo necesita una conexión.

Por razones de rentabilidad a menudo son necesarias múltiples rutas de acceso entre usuarios / dispositivos finales para obtener disponibilidad total. El bajo precio de las comunicaciones y su disponibilidad han hecho que aplicaciones potenciales que por razones de costo antes no eran posibles, sean ahora muy atractivas.

Hay tres requerimientos demandados por los usuarios con relación a las nuevas tecnologías.

1. La implementación de nuevas aplicaciones que utilicen el proceso de imágenes y gráficos.

2. Adaptar las aplicaciones existentes que estaban muy limitadas por el alto costo de las comunicaciones para que ofrezcan un abanico más amplio de posibilidades aprovechando la mayor rapidez de respuesta de los sistemas.

3. La integración de voz, vídeo y datos. Unificar las diferentes redes que tiene cada usuario ya que la mayoría de ellos posee una red de datos (TCP/IP, SNA, DECNET o X.25) separada de la línea de fax y voz.

Por razones de gestión y de optimización del costo, los usuarios quieren una sola red donde conviva todo el tráfico.

Resulta atractivo pensar que la voz digital llegue a ser de alguna forma igual que los datos. Hasta cierto punto puede ser cierto, pero existen algunas diferencias entre ambas que son un problema para la integración.

La diferencia más importante entre voz y datos está en que las llamadas de voz tienen una duración media de 3 minutos, mientras que las de datos pueden durar varias horas. La red telefónica ha sido diseñada para soportar un elevado número de líneas externas pero relativamente pocos caminos entre terminales de llamada, por lo cual es posible que la llamada sea bloqueada en el caso que la línea este saturada, con lo que este problema se acentúa al realizar transmisión de datos a través de estas líneas. Las nuevas PBX's digitales solucionan este problema permitiendo más capacidad de llamada que número de terminales existentes.

El ancho de banda necesario para la transmisión de voz depende de la técnica de digitalización utilizada, pero el circuito utilizado estará en uso a su máxima capacidad o estará libre, no existe la posibilidad de aumentar o disminuir la velocidad de la voz (el circuito de voz debe estar utilizado a la máxima velocidad o parado). En cambio los datos pueden ser controlados

desde un ordenador que tiene gran capacidad para la generación de tráfico de datos.

Los datos son transmitidos en bloques de diferente tamaño a través de la red, mientras que el tráfico telefónico es continuo. Este tráfico telefónico puede ser considerado como bloques de datos muy largos de longitud indeterminada, pero la red no permite la recepción de una ráfaga de datos como un bloque único y su transporte con características de tiempo real.

Un retardo de 200 ms es aceptable para una red de datos en tiempo real. Lo más usual es un retardo de unos 500 ms. El tráfico de datos Batch no tiene problemas con el retardo, pero para transmisión de voz de alta calidad el retardo del tráfico no puede ser mayor a 50 ms. Por lo tanto el retardo del tráfico variable hace que la transmisión de voz sea imposible. Los paquetes de voz han de ser distribuidos al receptor a una frecuencia uniforme.

Lo más importante para el tráfico de datos es que los errores puedan ser controlados, detectados, o preferiblemente detectados y corregidos. El mecanismo de corrección a menudo sólo es posible realizarlo por contexto y requiere retransmisión para recuperarlo. En el caso de la voz no es factible el retardo de tiempo de las recuperaciones y no tiene en cuenta errores ocasionales o ráfagas de errores.

En la actualidad en el cableado estructurado de edificios no diferenciamos por el tipo de cableado utilizado entre dos tipos de tomas. Tanto para las tomas informáticas como para las tomas telefónicas utilizamos el mismo cableado de forma que nos permite esconder cualquier combinación en cuanto a los tipos de tomas que necesitamos en cada punto de conexión variando tan sólo el equipo de conexión al otro extremo del cable.

2.3 Interconexión de Redes

Las redes locales proporcionan muchas ventajas, pero quizás nos hemos olvidado de las ventajas más técnicas y que quizás el usuario final no aprecia. Las redes locales son muy flexibles en su instalación, tiene una gran capacidad de expansión ya que hacen posible el crecimiento, se controlan de manera local y su mantenimiento es relativamente sencillo. Dada su gran capacidad de transmisión y que pueden organizarse de manera departamental podemos decir que su costo de adquisición / mantenimiento / funcionalidad está en un punto medio bajo.

El problema viene cuando distintos departamentos, distintas redes locales con objetivos independientes, desean intercalarse, como puede ser el caso de cualquier empresa o universidad. Si a esto le añadimos un problema generalmente bastante común, la distancia geográfica, hace que nuestra red local se quede en un pequeño punto aislado de nuestra oficina, edificio, ciudad o país.

Pero ¿ por qué la mayoría de las empresas no hacen una red global y no pequeñas redes locales? . Una de las ventajas de segmentar una red en varias LAN's es acomodar la carga, la información se transmitirá de una forma más clara (sin colisiones) y por lo tanto más rápidamente, también debemos actuar de esta manera debido a la distancia entre los ordenadores ya que habría un retardo considerable entre máquinas muy distantes.

Además, si por lo que fuese (un fallo de tensión, conflictos de configuración,...) una máquina dejase de trabajar segmentando la red en pequeñas redes evitaríamos que el sistema cayese por completo. Otro punto a considerar es la seguridad ya que podemos limitar el acceso entre dos segmentos, estableciendo una LAN de acceso restringido a una LAN de acceso general.

Si a todo esto le añadimos que actualmente hay un gran impacto tecnología, de estándares, que la competencia entre fabricantes es cada vez mayor, que en el mercado hay muchas redes heterogéneas y que la necesidad de comunicación está alcanzando cotas insospechadas, nos encontramos con el siguiente problema: Interconectar redes.

La interconexión de redes puede entenderse como la posibilidad de compartir recursos globales a la vez que se mantiene y reserva la independencia y la autonomía de los elementos que se conectan.

Las situaciones más típicas pueden ser, la ampliación física de una LAN más allá de su capacidad de base, la interconexión de distintas LAN's en una red pública, la integración de una LAN con una red de hosts o la interconexión de dos redes de hosts.

Por lo tanto, a continuación se menciona aspectos generales como, qué son y cómo funcionan los dispositivos de interconexión de redes.

Concentradores

Comúnmente conocidos como hubs, estos elementos se basan en el principio de interconexión más básico. Podemos entenderlos como un armario de conexiones donde se centralizan todas las conexiones de una red, o sea un dispositivo con entradas y salidas, que no hace nada más que centralizar conexiones.

Suelen utilizarse para implementar topologías físicas en estrella, pero funcionando como un anillo o un bus lógico.

Podemos distinguir entre dos tipos de hubs, los activos y los pasivos. Ver tabla 2.0 que se muestra a continuación

Activos	Pasivos
Pueden conectar nodos a 600 metros como distancia máxima.	Únicamente son cajas de conexión.
Tienen unos 10 puertos o mas.	Tienen unos 10 puertos o mas.
Pueden amplificar y repetir señales, hay algunos que realizan estadísticas.	Pueden conectar nodos a 30 metros de distancia como máximo.

Repetidores

Estos operan en el nivel físico de la OSI, ya que interconectan redes iguales (del mismo tipo). Su utilización sirve para extender la distancia máxima de la LAN o para unir o interconectar distintos soportes de comunicación, aunque también puede servir para unir varios segmentos o varios anillos constituyendo una LAN física y lógica única.

Hay que tener claro que un repetidor no analiza la información que le llega, hace una transmisión transparente de todas las tramas de un segmento de LAN a otro (en ambos sentidos). Regenera las señales y no realiza ningún filtrado de trama. Lo que sí hace es restaurar el preámbulo (parte que activa los sincronismos) dado que no varía nunca; el resto lo amplifica. También corrige la frecuencia y la amplitud. Ofrece la conversión de señales y de interfaz para acoplar distintos soportes de comunicación manteniendo a nivel lógico una sola LAN.

Puentes

Los puentes o "bridges" son dispositivos que operan en el nivel de enlace de datos. No analizan los campos de datos. Los puentes, delimitan el tráfico entre redes a las redes que tiene acceso directo y deben preservar las características de las LAN's que interconectan (retardo de transmisión, capacidad de transmisión, probabilidad de pérdida, etc.). Estos elementos filtran el tráfico en función de una tabla de direcciones. La decisión si son transmitidos hacia delante o no se toma en función de la dirección destino que se halla en cada paquete.

Hay tres tipos de puentes, simple, transparente y puente de encaminamiento de fuente.

En el puente simple, la tabla de direcciones está basada en un conocimiento previo. Las ventajas que tiene son la velocidad y la simplicidad pero peca de falta de flexibilidad y de que el número de estaciones depende del tamaño de la tabla.

Los puentes transparentes, operan en el nivel MAC, su inicialización es automática y realiza funciones de reenvío de tramas, de autoaprendizaje de las estaciones de la red, y de resolución de los posibles bucles que existan en la topología de la red.

Puentes de encaminamiento fuente se desarrolló por el comité IEEE 802.5. La estación origen, determina la ruta que seguirá la trama e incluye esta información en la misma en forma de identificadores de puentes y de LAN's. De manera que un puente retransmite la trama si su identificador está en la ruta designada, sino, la desecha. En este tipo de puentes no se requiere tablas de encaminamiento en los puentes ya que este únicamente debe conocer sus

identificadores. La ruta que escoge la estación origen hasta cualquier destino viene dada por unos modos de direccionamiento y unas directrices de enrutado.

Routers

Actúan en el nivel de red. Ofrecen un servicio más sofisticado que un puente: puede seleccionar uno de entre varios caminos según parámetros como retardo de transmisión, congestión, etc.

Estos dispositivos, dependen del protocolo usado. En el nivel de red se controla el tiempo de vida de un paquete, el tiempo requerido para que un paquete vaya de un punto a otro de la Internet (interconexión de redes) hará que el tamaño máximo de esta sea mayor o menor.

El Cisco TRouter es un router multiprotocolo, puede actuar de servidor de terminales: hasta 16 dispositivos asíncronos de velocidad hasta 34.4 Kbps, proporcionando acceso remoto para conexión de múltiples dispositivos asíncronos. Cisco Trouter proporciona interfaces a: Ethernet / IEEE 802.3 y enlaces serie (HDLC, LAPB, X.25). Soporta los protocolos de enrutado (TCP/IP, DECNet, XNS, IPX, AppleTalk).

Brouter

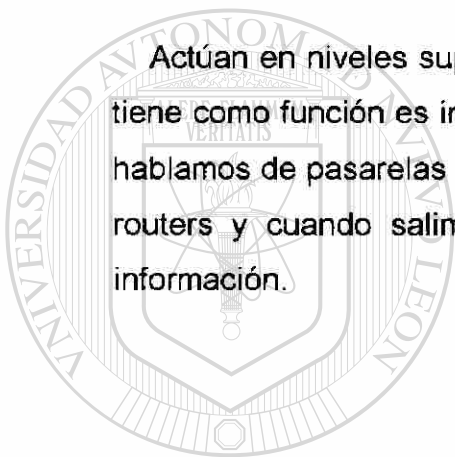
Dispositivo que combina las funciones de puente y router. Tiene la capacidad de encaminamiento de un router y la velocidad de procesado de un puente. Un brouter, es independiente del protocolo, pero puede dirigir el tráfico de una LAN a otras redes dependiendo del protocolo.

Un ejemplo de brouter sería el Halley ConnectLAN 202, que es un dispositivo de interconexión de Token Ring, usando una tabla de encaminamiento y participando en el descubrimiento real de las rutas.

Otro brouter podría ser por ejemplo, la familia 3Com NETBuilder con sus dispositivos BR/2000 y BR/3000, que además filtran el tráfico en función de la dirección de trama, del protocolo (XNS, IP), de la longitud de trama. También autorizan retransmisiones de tramas específicas y soportan XNS (IDP, RIP), TCP/IP (IP, EGP, RIP, ICMP, RAP), OSI (CLNP), actuando de puente para los otros protocolos.

Pasarelas

Actúan en niveles superiores, a partir de la capa 4 de OSI. Este dispositivo, tiene como función es interconectar redes totalmente distintas. Aunque cuando hablamos de pasarelas en el ámbito de LAN estamos haciendo referencia a los routers y cuando salimos de las LAN's estas actúan como traductoras de información.



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



DIRECCIÓN GENERAL DE BIBLIOTECAS

2.4 Evolución de las Redes Ethernet: Hacia el GigaEthernet .

Con el rápido crecimiento en poder de procesamiento en servidores y estaciones de trabajo, la proliferación de aplicaciones que demandan gran ancho de banda, y el crecimiento explosivo en redes de área local, provoca que muchos gestores de red se planteen urgentemente la necesidad de más ancho de banda. La necesidad de ancho de banda es un tema común, workgroup en grandes LANs con cientos de usuarios enviando mails y ejecutando aplicaciones de productividad en la oficina, LANs que necesitan ancho de banda para videoconferencia, aplicaciones multimedia, acceso a WWW, pequeños grupos de usuarios ejecutando aplicaciones CAD y gráficas, o incluso varias oficinas remotas compartiendo datos con una o mas servidores.

Según la consultora IDC más del 80% de las redes locales utilizan la tecnología Ethernet, por su facilidad de configuración, gestión, precio y por el magnífico soporte ofrecido por todas las grandes compañías del Networking como Cisco, 3Com, Bay Network, Nortell, LanTronix, por citar algunas.

El objetivo de este artículo es ofrecer una idea clara, pero sin perder una buena base teórica, de las tecnologías Ethernet desde un punto de vista evolutivo, es decir, comenzando por la Ethernet Compartida, Segmentada, Fast Ethernet, Conmutación y acabando en su último estadio llamada Gigabit Ethernet. En este paseo veremos también la evolución de los elementos de una red Hub, Bridges, Routers, Switchers, no siendo la intención del mismo profundizar en estos dispositivos.

2.4.1 Conceptos Básicos.

Durante la última década las redes locales se han basado en una tecnología de acceso compartido. Esto significa que todos los equipos conectados a la

LAN comparten un único medio de comunicación, normalmente coaxial, par trenzado o fibra óptica.

El estándar Ethernet fue definido por el IEEE en una norma conocida como 802.3, que cubre las reglas para configurar las redes Ethernet, los tipos de medios que se pueden utilizar y cómo los elementos de la red deberían interactuar, como el método de acceso, la velocidad, esta norma fija la velocidad a 10 Mbps.

Existen dos topologías básicas de una red Ethernet, en Bus y en Estrella. Observemos la topología en Bus que nos servirá como referencia para la siguiente explicación:

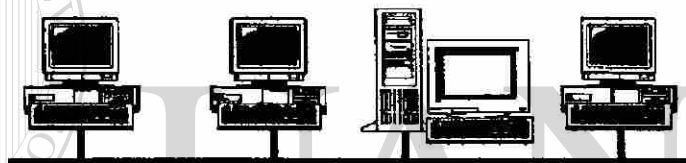


Figura 2.1. Topología Bus

La norma IEEE 802.3 se utiliza en las redes tipo LAN con el protocolo de acceso al medio denominado 1-persistente CSMA/CD (Carrier Sense Multiple Access/Collision Detection: Acceso Múltiple Sensible a la Portadora con Detección de Colisiones). Revisemos esta idea: cuando una estación desea transmitir, escucha la información que fluye a través del cable. Si el cable se encuentra ocupado, la estación espera hasta que esté en estado inactivo, en caso contrario transmite de inmediato. Si dos o más estaciones, de forma simultánea, comienzan a transmitir a través de un cable inactivo, generarán una colisión. Estas estaciones al detectar que lo que circula por el cable no es lo mismo que envían (detectan la colisión), terminarán su transmisión, esperarán un tiempo aleatorio y repetirán de nuevo todo el proceso completo. Podemos decir que es una técnica de acceso de competición.

La norma IEEE establece que el transmisor debe detectar una colisión si la señal a través del cable en la toma de conexión excede el valor máximo que puede ser producido por el transmisor de forma aislada. Debido a que la señal se atenúa la norma restringe la longitud máxima del cable a 500 m para 10Base5, a 200 metros para 10Base2, En una topología en estrella la detección se realiza mediante niveles lógicos, detectando que existe actividad en más de una entrada al concentrador, generando una señal de aviso, para que paren de emitir las estaciones.

En el siguiente diagrama de flujo podemos observar el proceso:

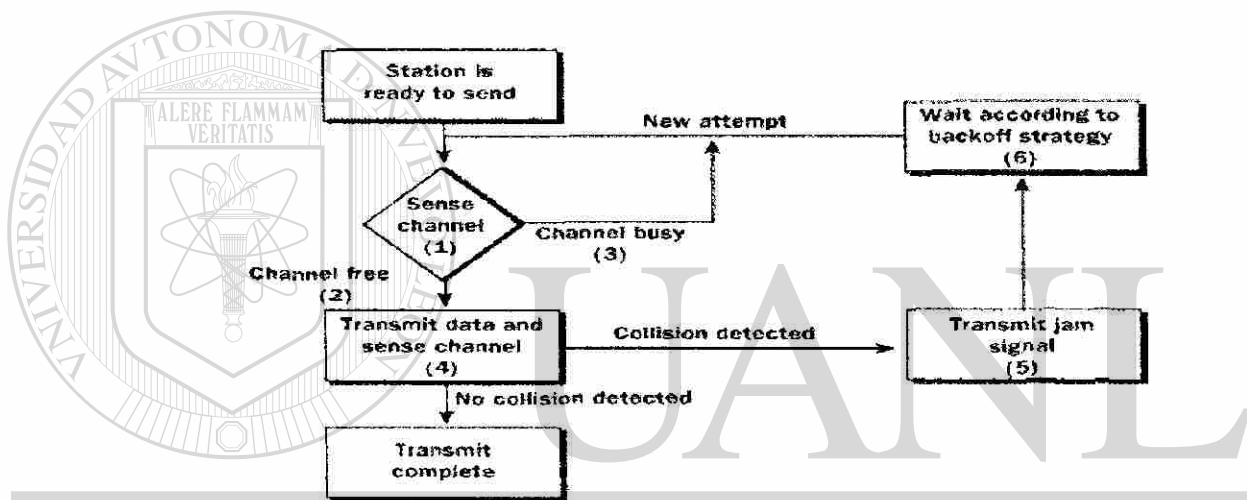


Figura 2.2. Diagrama de Flujo del Control de Acceso al Medio CSMA/CD.®
DIRECCIÓN GENERAL DE BIBLIOTECAS

Ethernet divide la información que se desea transmitir en tramas. Estas tramas contienen un preámbulo de sincronismo, la dirección MAC de destino, la dirección MAC de origen, longitud del campo de datos, el campo de datos y 4 bytes de control de errores. El tamaño de las tramas es variable y puede ir desde los 64 Bytes a los 1514 Bytes.

Formato de la trama IEEE 802.3

Preámbulo

SFD: Delimitador de comienzo de trama

DA: Dirección destino

SA: Dirección origen

Longitud, Datos LLC, Relleno

FCS: Secuencia de comprobación de trama

Una regla importante aplicada a los sistemas CSMA/CD consiste en que la trama debe ser lo suficientemente larga como para permitir la detección de la colisión antes de que finalice la transmisión. Si se usan tramas más cortas, no se produce la detección de la colisión, y el sistema falla. Este fenómeno junto con la atenuación limita la longitud de las redes Ethernet.

La norma IEEE 802.3 define diferentes alternativas para el medio de transmisión: Ver tabla 2.1 a continuación.

	10BASE5	10BASE2	10BASE-T	10BROAD36	10BASE-FP
Medios de Transmisión	Cable coaxial 50W	Cable coaxial 50W	Par Trenzado no apantallado	Cable coaxial 75W	Fibra óptica 850 nm
Técnica de Señalización	Banda Base (Manchester)	Banda Base (Manchester)	Banda Base (Manchester)	Banda Ancha (DSPK)	Manchester/ si-no
Topología	Bus	Bus	Estrella	Bus/árbol	Estrella
Longitud Máxima (m)	500	185	100	1800	500
Nodos por Segmento	100	30	-	-	33
Diámetro del cable (mm)	10	5	0.4-0.6	0.4-1.0	62.5/125m

2.4.2. Ethernet Compartida.

Las topologías de una red Ethernet pueden ser dos: en bus o en estrella. Cuando la red contiene pocos ordenadores la solución más barata, pero menos flexible, es montar una red en bus con cable coaxial. Esta configuración es muy poco flexible ya que obliga a cortar el cable coaxial, cualquier cambio de disposición de los ordenadores provoca grandes problemas y es difícil poder ampliar la red a nuevos usuarios. La alternativa es la utilización de un Hub o concentrador en una configuración tipo estrella, siendo el medio de transmisión

más utilizado el par trenzado. Esta configuración es muy flexible y escalable, siendo su topología típica la mostrada en la figura 2.3.

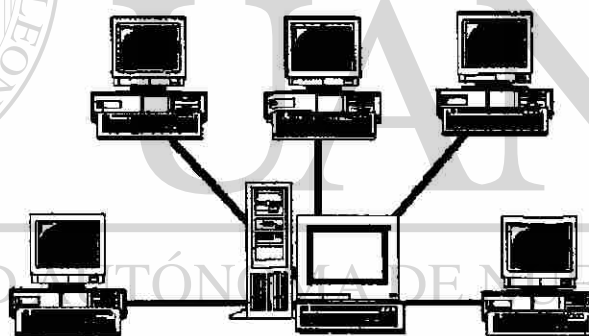


Figura 2.3. Topología en Estrella. Utilización de un concentrador o Hub.

El Hub es un equipo que dispone de un cierto número de puertos en los que se conectan estaciones de trabajo y servidores. Todos los equipos conectados comparten el medio de transmisión y por lo tanto todos comparten los 10 Mbps disponibles en el medio. En esta configuración se dice que todos los dispositivos de la red se encuentran en un mismo dominio de colisión por lo que el ancho de banda efectivo es muy inferior a los 10 Mbps, ocurriendo colisiones de forma continua. Al aumentar el nº de estaciones aumenta la probabilidad de colisiones y por lo tanto disminuye el ancho de banda efectivo. Recordando el

método de acceso al medio y ya que el medio es compartido, al enviar o recibir paquetes un usuario el resto debe esperar.

La posibilidad de conectar en cascada varios Hubs separando las estaciones no supone ninguna mejora ya que siguen compartiendo el medio todos los ordenadores: ver la figura 2.4.

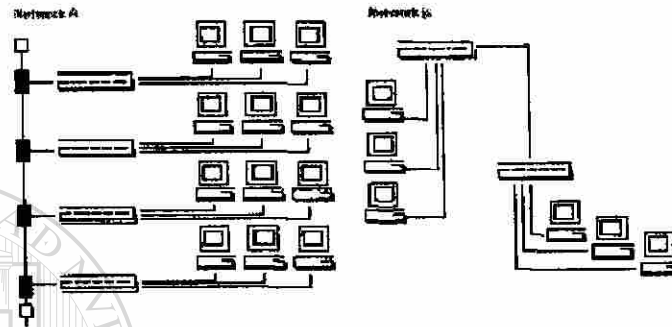


Figura 2.4. Topología en cascada con Hubs.

Segmentación: Bridge y Router

Pensando en separar dominios de colisión surge el concepto de segmentación y la necesidad de otros dispositivos. El primer dispositivo que aparece es el Bridge o puente, barato y de lógica simple. El Bridge filtra los paquetes entre segmentos o subredes de LANs tomando una decisión simple de retransmisión o no retransmisión de cada paquete recibido desde cualquier segmento al que esté conectado, no modificando el contenido del paquete. Si el paquete está dirigido a una estación que se encuentra en el mismo segmento donde ha sido originada no se retransmite, si no, se retransmite a todas las redes conectadas a él. El Bridge actúa a nivel de dirección física o MAC, por lo tanto, debe conocer las direcciones de las estaciones de cada red a la que está conectada, en función de cómo conoce estas direcciones aparecen diferentes tipos de puentes.

Con este primer dispositivo inteligente, el puente, conseguimos separar dominios de colisión ya que si una estación de un segmento desea comunicarse con otra estación de ese mismo segmento, el dominio de colisión se reduce, no interfiriendo con el resto de subredes o segmentos.

El segundo dispositivo que permite la segmentación es el Router. Mucho más complejo que el Bridge y por lo tanto más caro, opera en la capa de red lo que le permite encaminar los paquetes a su destino a través de las rutas adecuadas. Para conocer la topología de la red el router se comunica con el resto de routers de la red compartiendo información que les permitirán elegir la mejor ruta a través de los complejos enlaces que tenga la red. El router examina la dirección IP destino, determina la dirección de la red destino y comprueba en su tabla de rutas a quién (si la red destino también está conectada al router) o a qué (si la red no está conectada directamente) router o dispositivo enviarlo. Por lo tanto proporciona una segmentación de dominios de colisión más inteligente que el Bridge, obteniendo como resultado un ancho de banda efectivo superior. Si conectamos estaciones directamente al router, obtendrán 10 Mbps dedicados.

Además proporciona herramientas de gestión de red que permite controlar los recursos de la misma de una forma exhaustiva y eficiente. También ofrece la posibilidad de conexión a redes de área extensa (WAN) de una manera sencilla.

El primer objetivo: reducir el dominio de colisión en segmentos independientes interconectados con dispositivos inteligentes como el Bridge o el Router, se ha conseguido. Ahora podemos disponer de aproximadamente 10 Mbps en segmentos, pero conforme va pasando el tiempo surgen nuevos problemas: Los servidores utilizan 10 Mbps para servir a toda la red, las aplicaciones que requieren más ancho de banda, accesos recurrentes a los recursos del servidor, correo electrónico, consiguen saturar el enlace con el servidor, además los enlaces entre routers/bridges deben soportar sobre 10

Mbps demasiadas conexiones, todos estos problemas provocan que el rendimiento global de la red sea insatisfactorio. Es en este momento cuando parece claro que se necesitan enlaces de más de 10 Mbps.

2.4.3 Fast Ethernet

Cuando la red sufre picos de demanda de capacidad por encima de los 10 Mbps es necesario emigrar hacia el concepto de Fast Ethernet. Fast Ethernet o Ethernet de alta velocidad es un conjunto de especificaciones desarrolladas por el comité IEEE 802.3 con el fin de proporcionar una red LAN de bajo costo compatible con Ethernet y funcionando a 100 Mbps. La designación global para estas normalizaciones es 100Base-T. El incremento de velocidad se basa en la técnica de codificación multinivel.

La siguiente tabla resume las características más importantes de las opciones 100BASE-T: ver tabla 2.2 mostrada a continuación.

	100 BASE-TX	100BASE-FX	100BASE-T4
Medio de Transmisión 2 pares STP	2 pares UTP de clase 5	2 fibras ópticas	4 pares UTP de clase 3, 4 o 5
Técnica de señalización 4B 5B,NRZI	4B 5B,NRZI	4B 5B,NRZI	8B6T,NRZ
Tasa de datos 100 Mbps	100 Mbps	100 Mbps	100 Mbps
Longitud Máxima de segmento 100 m	100 m	100 m-2 Km	100 m
Expansión de red 200 m	200 m	200 m	200 m

Con esta nueva norma aparecen Hubs y tarjetas a 100 Mbps, que permiten que las terminales con gran volumen de tráfico no congestionen la red pero a un precio elevado. Permitiendo, además, enlazar routers con líneas de alta

velocidad. El problema básico de Ethernet es que la red es compartida por todos los usuarios. Una primera solución es segmentarla en subredes e interconectarlas con dispositivos (bridge o router) que las separan en dominios de colisión independientes. El router proporciona mayores prestaciones que el bridge pero a un mayor costo. Al necesitar más ancho de banda para conectar servidores y para interconectar routers surge la red Ethernet de Alta velocidad, que proporciona 100 Mbps, esto origina que la red vaya más rápida y por lo tanto que las colisiones disminuyan, pero también a un costo alto, no asumible por las pequeñas o medianas empresas. Es entonces cuando aparece un nuevo actor: el conmutador.

2.4.4 Red Compartida y Red Conmutada.

Con la conmutación decimos adiós a la red compartida. A diferencia del Hub que difunde los paquetes a toda la red y por lo tanto sólo permite que haya una terminal enviando/recibiendo datos, el Conmutador o Switch es más inteligente y envía el paquete sólo a su destinatario, y por lo tanto, pueden existir varios usuarios enviándose paquetes siempre y cuando el destinatario (no la red) esté libre. Ver figura 2.5 mostrada a continuación.

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

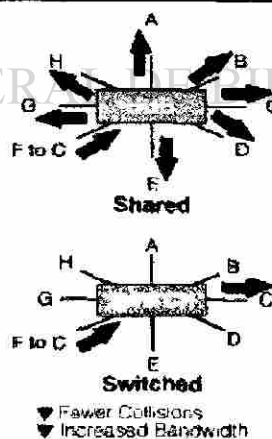


Figura 2.5. Red compartida(Hub) vs. Red conmutada (Conmutador).

Así con el conmutador se consiguen 10 Mbps dedicados entre origen y destino.

Entonces surge la pregunta, ¿Cuál es la diferencia con el router?. En primer lugar existen diferentes tipos de conmutadores, en función de su inteligencia (la capa en donde trabajen) y de su costo. Los conmutadores de capa 2 toman decisiones de envío basándose en la dirección física o MAC de destino contenida en cada paquete. Al contrario que el bridge, el switch puede reenviar los datos con periodos de latencia muy bajos. Existen dos tipos de conmutadores de capa 2 según el modo de reenvío: (1) Cut-Thorough: los conmutadores inician el proceso de reenvío antes de haber recibido la trama completada (no comprueba la integridad de la trama) y (2) Store-and-forward: que leen y validan el paquete entero, incrementando la latencia proporcionalmente al tamaño del paquete, pero ganando control de flujo. En definitiva, los entornos más beneficiados son aquellas redes LAN complejas que en la actualidad utilizan routers para su segmentación. En este caso el conmutador sustituye con ventaja al router por su bajo tiempo de latencia y su inferior costo por puerto. El uso de Circuitos Integrados Específicos permite a los conmutadores enviar paquetes de forma simultánea a través de todos los puertos, proporcionando así un nivel de prestaciones muy superior al de los bridges tradicionales. Los conmutadores de capa 3 leen la dirección de destino de la capa de red (en redes TCP/IP la dirección IP). Para conseguir estas prestaciones se utilizan Circuitos en los que se integra la tecnología de ruteo. Junto con el control y la velocidad, las principales ventajas de la conmutación de capa 3 son su mayor rendimiento, simplicidad, seguridad y flexibilidad. Como vimos en el artículo "Conmutación de capa 3: el siguiente paso en la evolución de las redes LAN", los conmutadores de capa 3 son el futuro a corto plazo del networking, consiguiendo día a día nuevas funciones que lo convierten en el dispositivo clave de las redes de alta velocidad.

Otro avance importante en la conmutación son las tarjetas de red Full Duplex que permite a las máquinas enviar y recibir datos de forma simultánea. Con la actual sobrecarga de las redes, el servidor puede beneficiarse de notables ventajas al introducir mayor velocidad en las conexiones utilizando conexiones full duplex con el conmutador debido a la necesidad de recibir y enviar datos de forma simultánea.

Pero, ¿Cómo integramos todos estos dispositivos en una red? Un ecosistema conmutado

Caso 1. Migración radical de red compartida a red conmutada y a Fast Ethernet. Imaginemos una red con 10 usuarios de alto rendimiento que utilizan aplicaciones de Groupware que atacan al servidor, además de utilizar recursos ubicados en el servidor. Con un Hub comparten 10 Mbps, lo cual provoca que la red se congestione y que el rendimiento de los usuarios no sea el óptimo. La solución es cambiar el Hub por un conmutador de forma que ahora tienen 10 Mbps dedicados hacia el servidor. Pero evidentemente el servidor al disponer sólo de 10 Mbps no puede dar servicio a todos los usuarios con la velocidad que requieren, entonces la solución es un conmutador que disponga, además de las puertas a 10 Mbps, de una puerta de 100 Mbps a la que se conectará el servidor (instalándole una tarjeta a 100).

Por ejemplo, el LinkSwitch de 3Com es un conmutador Ethernet/Fast Ethernet que proporciona 12/24 puertos 10Base-T y 2 puertos 100Base-T.

Caso 2. Coexistencia de Ethernet compartida, conmutada y Fast Ethernet

Supongamos 30 usuarios, 10 de ellos utilizan aplicaciones Groupware situado en el servidor A, otras 10 utilizan ficheros administrativos e impresoras del servidor B, 8 utilizan ficheros de informática del servidor C y 2 utilizan aplicaciones CAD/CAM y mueven ficheros de gran volumen entre los 3 servidores.

Para el primer grupo de usuarios que necesitan de gran ancho de banda, usaremos un conmutador que tenga como mínimo 10 puertos a 10 Mbps y uno

a 100 Mbps al que conectaremos el Servidor A. Los 8 usuarios que utilizan aplicaciones con bajas necesidades compartirán 10 Mbps con un Hub de 8 puertos mínimo. Para los usuarios de CAD/CAM tenemos dos posibilidades: un Hub a 100 Mbps al que se conectarán los dos usuarios, el servidor C y los conmutadores, y como segunda posibilidad un conmutador que tenga un mínimo de 3 puertos a 100 Mbps para los dos usuarios y el Servidor, además se interconectarán los conmutadores/Hub de los otros grupos a este conmutador utilizando puertos de 10 o 100.

Actualmente existen Conmutadores y Hubs 10/100 denominados Auto-Sensing que detectan cual es la velocidad a la que puede ir un dispositivo conectado a cualquiera de sus puertos, autoconfigurándose a 10 o a 100 Mbps.

Del 80/20 al 20/80 : Mayor capacidad en la troncal. Durante mucho tiempo, el 80 por ciento del tráfico de las redes locales permanecía dentro del grupo de trabajo (segmento), mientras que sólo el 20 por ciento restante llegaba a cruzar la red troncal. La tendencia actual hacia la centralización de recursos, principalmente de los servidores, resultando más fácil gestionar la red, así como mantener la seguridad y realizar las tareas de backup está dando la vuelta a esta regla. A su vez, este nuevo modelo impone que las redes troncales aumenten su capacidad de forma radical buscando enlaces que superen los 100 Mbps.

2.4.5. GigaEthernet.

Al desarrollar la nueva tecnología del Gigabit una de las premisas básicas es la compatibilidad con los estándares Ethernet para propiciar una migración sencilla. No obstante esta velocidad de proceso impone ciertas restricciones o variaciones respecto a la norma 802.3.

En Julio de 1996 se creó el grupo 802.3z para crear la norma que regiría el estándar Gigabit Ethernet (GEN), los objetivos iniciales fueron: Permitir operaciones half-duplex y full-duplex a una velocidad de 1000 Mbps. Usar el formato de trama 802.3 Usar el método de acceso CSMA/CD Compatibilidad con las tecnologías Ethernet 10BASE-T y 100BASE-T

Los objetivos iniciales de este grupo fue desarrollar enlaces de diferentes distancias: un enlace con fibra óptica multimodo de 550m de longitud máxima, un enlace con fibra óptica mono modo de 3Km de long. max, un enlace con par trenzado apantallado STP ("twinax" STP de 150 W) a 25 m y por último, un objetivo a largo plazo de desarrollar enlaces con UTP cat. 5.

Los elementos funcionales del desarrollo de la tecnología GEN la podemos observar en la siguiente figura 2.6.

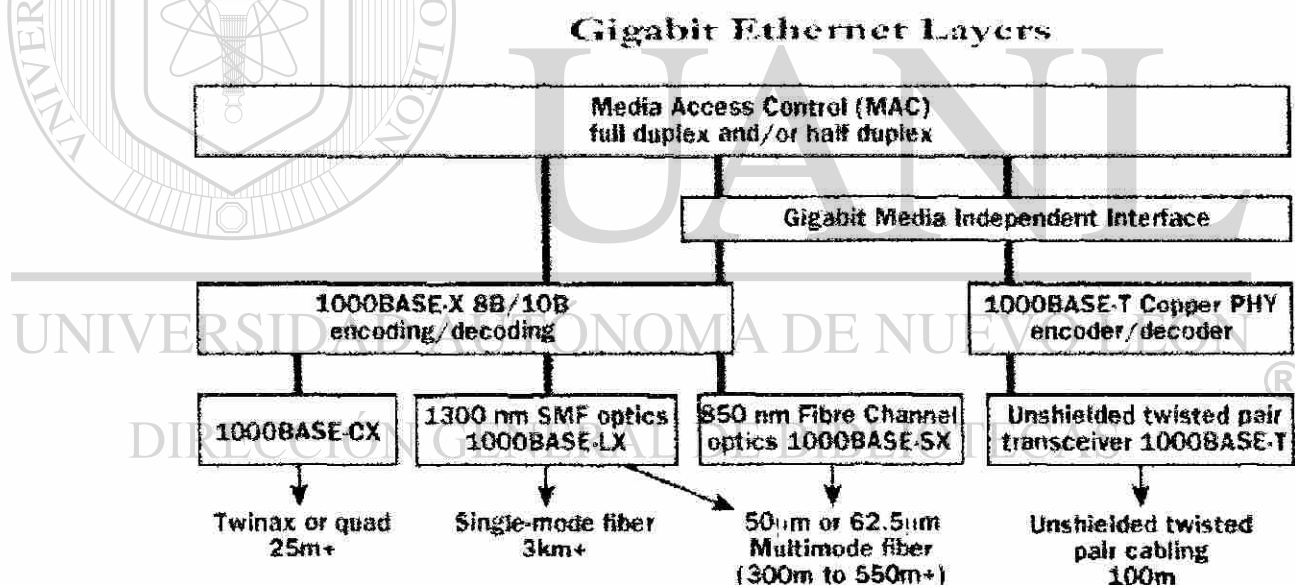


Figura 2.6. Elementos funcionales de la Tecnología Gigabit Ethernet.

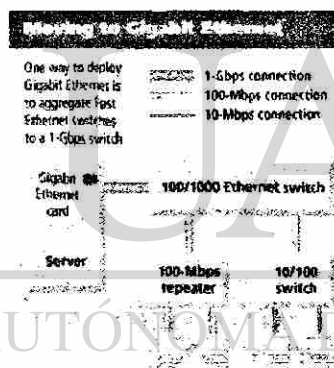
Con el objetivo de mantener la compatibilidad con CSMA/CD y conseguir un diámetro de colisión de 200 m a velocidades de gigabit, se tuvo que modificar la longitud mínima de los paquetes Ethernet, pasando de los 64 Bytes a los 512 Bytes. Los paquetes con tamaño inferior a los 512 Bytes tendrán una extensión de portadora. Estos cambios no afectarán a las redes que funcionen en modo

full-duplex (conmutadores o distribuidores con buffers), manteniendo los 64 Bytes.

Escenarios de Gigabit Ethernet

Evidentemente Gigabit Ethernet (GEN) tiene unos escenarios para los cuales proporciona un máximo rendimiento. En estos momentos se pueden describir 4 grandes escenarios donde Gigabit Ethernet tendrá grandes posibilidades:

1. Conexión entre conmutadores
2. Conexión entre conmutadores y servidores
3. Conexión de estaciones de trabajo a conmutadores.
4. Actualización de troncales Fast Ethernet o FDDI hacia el Gigabit



Source: Gigabit Ethernet Alliance

Figura 2.7. Topología típica 10/100/1000.

1. De conmutador a conmutador.
2. En estos momentos las grandes instalaciones de red se basan en conmutadores, que proporcionan gran ancho de banda a bajo costo, pero esto a su vez conlleva ciertos problemas:

1. Tener docenas de enlaces de 10 Mbps conectados a un conmutador dotado de un solo enlace Fast Ethernet hacia otro conmutador supone un riesgo de que aparezca congestión en el enlace entre conmutadores.

2. Si disponemos de servidores conectados a un conmutador a 100 Mbps y es objeto de conexiones provenientes de otros conmutadores, la congestión está prácticamente asegurada.

La solución a esta necesidad de mayor ancho de banda es utilizar un enlace punto a punto GEN. Esta actualización es relativamente simple ya que sólo se deberá añadir un módulo GEN a cada conmutador y conectarlos mediante cualquiera de los medios de transmisión recomendados.

3. De servidor a conmutador.

4. Cuando se quiere eliminar situaciones de congestión, los servidores suelen estar en el punto de mira. Como es muy probable que algunos servidores que operan a escala corporativa, que suelen tener múltiples procesadores y ofrecer prestaciones a tolerancias a fallos, como discos RAID, den servicio a cientos de usuarios simultáneamente, los administradores de redes querrán evitar que se produzcan "cuellos de botella".

Los enlaces de servidor GEN pueden ser considerados como una evolución natural de la tendencia a dedicar a los servidores un ancho de banda determinado.

Cuando aparecieron los conmutadores Ethernet, un objetivo clave de su implementación fue conseguir conexiones directas con los servidores. De ese modo, eliminando las posibilidades de que surgieran colisiones, se obtenían mejoras inmediatas de la capacidad de proceso.

Después vinieron las conexiones Ethernet Full-duplex en dos sentidos, que proporcionaron velocidades de 20 Mbps en total. Permitiendo el tráfico viajar a y

desde el servidor, simultáneamente, se eliminaba el cuello de botella que suelen crear las transmisiones half-duplex en un solo sentido, propias del Ethernet convencional.

Las conexiones dedicadas con el servidor exigen gran ancho de banda que ahora proporciona Gigabit Ethernet. Mostrada en la figura 2.8.

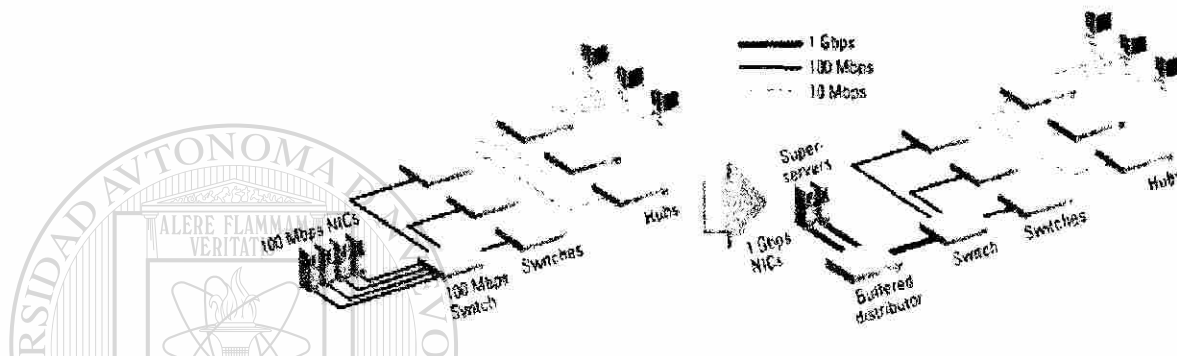


Figura 2.8. Actualización de enlaces conmutador-servidor con GEN. (3Com)

5. De estación a Conmutador

6. Para aquellas terminales de alto rendimiento o que utilicen aplicaciones de gran ancho de banda, la actualización de sus enlaces FDDI o Fast Ethernet a Gigabit Ethernet les supondrá el fin de las largas esperas. ®

7. Actualización de Troncales Conmutadas/FDDI.

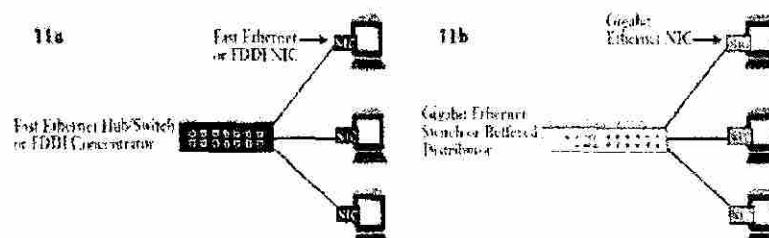


Figura 2.9. Actualizar enlaces a terminales de alto rendimiento.

Una migración lógica es actualizar sus troncales de conmutadores o FDDI a troncales Gigabit Ethernet.

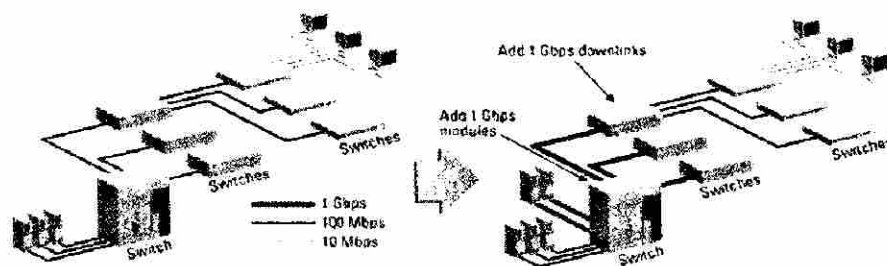
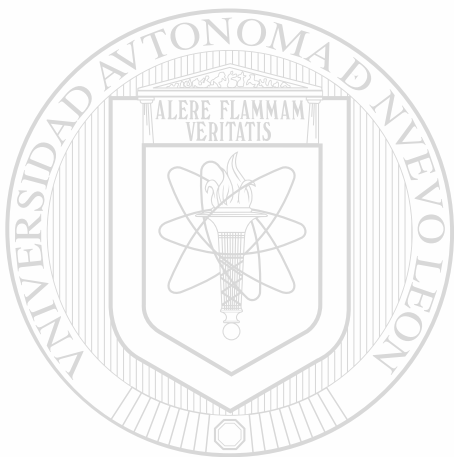


Figura 2.10. Actualización de troncales conmutadas a GEN. (3Com)



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

DIRECCIÓN GENERAL DE BIBLIOTECAS



CAPÍTULO 3

METODOLOGÍA PARA LA PLANEACIÓN DE UNA RED

3.1. Introducción.

La información dentro de la empresa ha tenido siempre un lugar estratégico. Hace algunos años, la empresa mas competitiva era aquella que procesaba la mayor cantidad de información por unidad de tiempo. Actualmente, una empresa altamente competitiva es aquella que posee la información en el menor tiempo. Este concepto de posesión implica la compartición, el procesamiento y la transmisión de la información.

En los últimos cinco años hemos visto que la mayoría de las empresas en México han desarrollado rápidamente sus redes de empresa para atender una creciente demanda de comparación y procesamiento de información. La cantidad de elementos a conectar así como la diversidad de arquitecturas, protocolos, servicios, etc. Origina problemas metodológicos complejos para la realización de una red empresarial corporativa. Es necesario tomar en cuenta las necesidades de comunicación en constante evolución (voz, datos, textos, imagen, etc.) interesarse a las redes internas de cada sitio (PABX, LAN's) así como a los medios de comunicación entre esos sitios (WAN, VLANs) escoger entre las diferentes tecnologías y servicios de comunicación, hasta optimizar la estructura y dimensionamiento de las redes así definidas.

El responsable de llevar a cabo ese procedimiento en la empresa ve abrirse frente a él un horizonte aparentemente insondeable. Él tiene la carga de aplicaciones tales como la voz, los datos, los textos, la imagen, etc. Él se ocupa de la comunicación al interior de un edificio o campus así como de la comunicación externa con otros edificios o campus. Él se enfrenta a la selección de tecnologías y servicios que aumenta día a día. Para poder atacar este problema complejo, se requiere de una formalización de los diferentes procedimientos que pueden ser empleados desde la planeación hasta la explotación de una red de comunicaciones corporativa.

La amplia experiencia acumulada en el dominio de la planeación y desarrollo de redes públicas de comunicación desgraciadamente no es directamente aplicable en una red de una empresa. Esto se debe a que las consideraciones son muy diferentes. Una red pública se planea considerando muchos utilizadores para un número limitado de aplicaciones. Al contrario, en una red privada existen relativamente pocos utilizadores para un número elevado de aplicaciones. En consecuencia, aplicar los métodos y las técnicas clásicas sería completamente inadecuado. Entonces en el contexto actual en el que las redes de comunicación en la empresa toman un carácter estratégico, se hace necesario aplicar metodologías y herramientas informáticas prácticas y eficaces para su implantación en la empresa.

En esta comunicación se presenta una proposición de metodología para llevar a cabo el proceso de planeación, análisis y diseño de una red privada. Todas las fases constituyentes del procedimiento están inscritas en un ciclo evolutivo de aprendizaje de utilización de la red privada.

3.2. Fases del Ciclo de Vida de una Red de Comunicación.

El esquema metodológico presentado para la implantación de redes corporativas lo podemos dividir en tres fases secuenciales dentro de un ciclo de aprendizaje de las telecomunicaciones de la empresa de la siguiente forma:

- Planeación, análisis y diseño.
- Desarrollo e instrumentación.
- Explotación y administración.

Estas fases están englobadas dentro de un marco general de administración y seguimiento de un proyecto. El proceso de desarrollo de un sistema teleinformático es repetitivo y termina cuando se encuentra la solución más adecuada para satisfacer las necesidades de la empresa o negocio que solicita la red. Cada una de las etapas por las que pasa el proyecto de telecomunicaciones puede ocasionar modificaciones en las anteriores, es decir, los planes pueden ir cambiando dependiendo de las condiciones o circunstancias que se presenten durante el avance del proyecto.

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

3.3. Planeación.

DIRECCIÓN GENERAL DE BIBLIOTECAS

El propósito principal de la etapa de planeación es clarificar los objetivos, necesidades, restricciones y actividades y recursos para alcanzar la meta. Esta etapa se ve afectada por la falta de información precisa respecto a las metas del proyecto, las necesidades del cliente y las restricciones existentes entre otros factores, todos ellos tienden a pensar que la planeación no puede hacerse correctamente, pero es necesaria para evitar demoras, gastos no contemplados que desequilibren el presupuesto, altos costos de mantenimiento y operación y mala calidad en el producto final.

La planeación inicial es un documento que va afectándose durante la evolución del proyecto, pero proporciona una estimación inicial del tiempo, costo y beneficio del mismo que sirve como base para el seguimiento y control del proyecto.

La planeación de una red, como se mencionaba anteriormente, es un proceso continuo en el que se involucran las siguientes actividades:

- Analizar la situación actual de la empresa, observando las características de la red y los sistemas existentes
- Reconocer las necesidades y restricciones del ambiente.
- Desarrollar estrategias para soportar las operaciones de la empresa y darle a esta una ventaja competitiva haciendo uso de las telecomunicaciones.
- Evaluar las diversas soluciones técnicas que ofrece el mercado.
- Pronosticar las necesidades y tecnología futura.
- Desarrollar planes apropiados a corto, mediano y largo plazo.
- Modificar los planes basados en los resultados del desarrollo actual del proyecto.

3.3.1 Definición del Proyecto.

El primer paso en la planeación de un sistema teleinformático es preparar, en términos de la empresa o negocio, un estatuto conciso del problema que se va a resolver y las restricciones que existen para su solución. La definición del problema debe incluir una descripción de la situación actual de comunicaciones en la empresa y los objetivos que se pretenden alcanzar con el nuevo sistema teleinformático.

La definición del problema requiere de entender el dominio y el ambiente del problema. Para obtener esta información es necesario entrevistar a las

personas que van a hacer uso de la red, observar como desarrollan su trabajo, reconocer los problemas y evaluar el rendimiento del sistema de comunicación actual.

El segundo paso en la planeación es determinar si el sistema teleinformático es la solución más adecuada para resolver el problema y aquí deben observarse factores de tiempo, económicos, técnicos, ambientales, organizacionales y políticos entre otros. Un sistema teleinformático que desplaza muchos trabajadores puede ser económicamente y técnicamente posible, pero puede ser que la empresa no lo acepte por razones sociales o políticas.

Una vez que se ha determinado que el sistema teleinformático es la solución más apropiada se debe de proceder a definir que personas formaran el equipo de trabajo en su desarrollo. Además, debe de estructurarse un plan de trabajo en el cual se definan las actividades a realizarse, se asignen las actividades entre los miembros del equipo de trabajo, se estime el tiempo para cada actividad y los recursos que se necesitaran.

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

El proceso de definición del problema puede descomponerse en los siguientes pasos:

- Análisis de la situación actual. En este paso se analiza la situación de la empresa con respecto al sistema de comunicación que tiene, el cual se pretende modificar o rediseñar. Si la empresa no tiene una red establecida será necesario conocer las operaciones que se desean realizar a través de un sistema de comunicaciones, reconociendo las localidades a comunicar y la relación que tienen unas con otras.

- **Análisis de necesidades.** Elaborar una lista de necesidades de comunicación de la empresa sin entrar en detalles internos del funcionamiento del sistema (software y hardware) y en base a la situación actual que se describió anteriormente.

- **Análisis de Restricciones.** Las restricciones son factores internos o externos a la empresa que tienen impacto sobre el diseño de la red, entre las que se encuentran las restricciones técnicas, jurídicas, financieras, de tiempo, relativas al personal, ambientales, psicológicas o sociológicas.

- **Análisis de posibles Soluciones.** Después del reconocimiento de las necesidades de comunicación existentes en la empresa es conveniente proceder a realizar una investigación preliminar con el propósito de buscar alternativas de comunicación existentes en el mercado del país para satisfacer las necesidades planteadas. En este momento se utiliza la información de proveedores de equipo, de usuarios de redes de comunicación y de revistas especializadas. Una vez que se tienen varias alternativas, se procede a hacer un análisis y descartara aquellas que por su costo, operación o disponibilidad no son factibles.

- **Estudio de Factibilidad.** En este paso se verifica que los diversos elementos cualitativos y cuantitativos que se solicitan para el sistema no conduzcan a un diseño irrealizable. Se consideran factores funcionales, técnicos, operaciones y financieros.

3.3.2 Formación del Equipo de Trabajo.

Debe formarse un equipo base de trabajo que participe en todas las etapas del desarrollo del proyecto. El numero de integrantes depende de la magnitud del proyecto y la complejidad de la organización. En general, mientras mas

grande sea la organización, mas grupos de trabajo distintos estarán involucrados en el proyecto de telecomunicaciones y como consecuencia debe haber varios representantes de dichos grupos en el equipo del proyecto.

Se recomienda que en el equipo de trabajo se involucren directivos o dueños del negocio, desarrolladores, usuarios del sistema y, en la medida posible, personas que reciban el servicio que proporcionara la empresa a través de la red de comunicaciones(clientes).

Además, es recomendable contar con la asesoría externa de un experto en comunicaciones para que apoye en los estudios de factibilidad, análisis de costo / beneficio y en el proceso de evaluación de las alternativas propuestas por los proveedores. Las responsabilidades principales de estos miembros del equipo son:

- Determinar una lista detallada de las actividades y subactividades que se realizarán.
- Determinar la secuencia en la cual se llevarán a cabo dichas actividades.
- Estimar fechas de inicio y fin de cada actividad.
- Fijar puntos de control.
- Determinar los recursos necesarios para el proyecto.
- Aceptar la responsabilidad de una tarea especifica y si es necesario, coordinar su propio grupo de trabajo.
- Hacer las revisiones necesarias de los avances del proyecto.

3.3.3 Elaboración del Plan de Trabajo.

Para controlar un proyecto es muy importante tener un calendario detallado de eventos. Una vez que dicho calendario ha sido desarrollado y aprobado, se convierte en el núcleo alrededor del cual los grupos de trabajo definen a detalle

las actividades que van a realizar y los recursos que utilizarán. Las gráficas de GANTT o diagramas PERT son comúnmente usadas en el proceso de calendarización de un proyecto.

Para asignar una secuencia a las actividades o tareas se deben identificar dependencias entre ellas y resulta muy conveniente aprovechar todas las oportunidades posibles para desarrollar actividades en paralelo y de esta forma optimizar el tiempo.

Las actividades principales que deben ser consideradas en el plan de trabajo son:

- Elaboración del documento de requerimientos.
- Elaboración del documento de especificaciones.
- Seleccionar una herramienta de software que apoye en la planeación y diseño de la red.
- Definición de la arquitectura de la red.
- Contactar a proveedores tomando en cuenta los documentos de requerimientos, especificaciones y arquitectura de la red.
- Programación de visitas a instalaciones de usuarios para aprovechar la experiencia adquirida por varias empresas en el uso de las redes de comunicación. Es conveniente elaborar una encuesta con aspectos técnicos, operacionales y legales.
- Visitar instalaciones de proveedores para conocer de cerca de cada uno de ellos y observar cuanto personal emplean, que tipo de instalaciones tienen, si es solo un proveedor de equipo u ofrece un valor agregado.
- Evaluar las propuestas de los proveedores.
- Seleccionar las propuestas que cumplan con las necesidades establecidas.
- Instalar la red.

- Planear y desarrollar las pruebas que se le harán a la red para medir su rendimiento.
- Capacitar al personal.
- Administrar los recursos de la red.

Una buena opción para la planeación de las actividades del diseño de la red es el método de análisis estructurado y técnica de datos.

3.4 Análisis.

Durante la fase de análisis se reúnen y modelan los requerimientos y especificaciones formales del sistema teleinformático y se realiza un análisis costo-beneficio, generando de esta forma un plan inicial para el diseño y adquisición de la red.

Las etapas que comprende esta fase:

- Determinación de requerimientos.
- Derivación de especificaciones.
- Justificación económica.

DIRECCIÓN GENERAL DE BIBLIOTECAS

3.4.1 Determinación de los Requerimientos.

La base de un buen diseño de sistemas de comunicaciones es un exhaustivo estudio del medio al cual se incorporara la red. Por eso la importancia de que los requerimientos, tanto funcionales, ambientales y de configuración, sean determinados completamente y mostrados en un formato adecuado.

En la determinación de requerimientos las necesidades originales deben ser definidas, evaluadas y verificadas. Los requerimientos necesariamente reflejan una orientación de la empresa mas que una orientación tecnológica.

Un conjunto de requerimientos debe incluir gran información de la empresa además de las funciones del sistema teleinformatico. Alguna de la información que debe estar contenida en el documento de los requerimientos incluye:

- El papel que desempeña el sistema dentro de la empresa.
 - La relación de este sistema particular con otros sistemas, ya sea existentes o propuestos.
 - Las características operacionales y restricciones del sistema.
 - La información que el sistema necesita y la que provee.
 - La velocidad de respuesta que se necesita cuando se hace uso del sistema.
 - El número promedio y máximo en un mismo momento de usuarios en el sistema.
 - Número de localidades que se van a comunicar y distancia entre si.
 - Tipo de servicio que el usuario requiere.
 - La necesidad de un tipo de transacción específica.
-
- La información completa que debe manejar el sistema durante una transacción determinada.
 - El volumen de datos que el sistema maneja.
 - Requerimientos de confiabilidad, las consecuencias aceptables de una avería. (disponibilidad, tiempo de reparación, etc.)

El modelo del negocio es de fundamental importancia para la verificación de los requerimientos ya que provee un punto de vista del negocio independiente de la tecnología, de tal forma que las decisiones de los sistemas y procedimientos puedan ser hechas para cubrir necesidades del negocio y una vista completa del negocio y su interacción con varias unidades organizacionales y sus responsabilidades.

Iniciando con un modelo de negocio, desarrollar una arquitectura técnica complementaria y utilizar una metodología de desarrollo adecuada permitirá a la empresa utilizar la tecnología para servir a sus necesidades y desarrollar un ambiente competitivo. Este modelo debe existir en todas las empresas pero quizá necesite actualizarse o, si no se tiene, desarrollarse.

Las discusiones y contactos frecuentes con los usuarios es la actividad típica que se desarrolla en este punto del proyecto para modificar dinámicamente sus requerimientos y posteriormente verificar el borrador de especificaciones.

Los requerimientos son utilizados por muchos de los subsecuentes pasos de la metodología. Por lo tanto, el formato de los requerimientos es muy importante. Los requerimientos pueden presentarse como un texto, diagramas de flujo, diagramas entidad-relación, análisis estructurado, diagramas de estado, tablas, árboles, etc.

La verificación de los requerimientos contra las necesidades del negocio es uno de los aspectos mas importantes de la determinación de requerimientos. ®

Sin este proceso de verificación puede resultar que el sistema no refleje adecuadamente las necesidades reales del negocio. El propósito de un sistema teleinformático es cubrir las necesidades de la empresa no forzar un cambio en el comportamiento de la misma.

La Simulación puede utilizarse para mostrar al usuario un panorama inicial de la operación y características de la red donde quizá no todos los requerimientos puedan ser simulados.

3.4.2 Derivación de las Especificaciones.

Las especificaciones del sistema forman un documento técnico que será utilizado para iniciar el proceso de diseño. Durante la fase de definición de la arquitectura del sistema y selección de los componentes se agregaran mas especificaciones. No existe garantía de que se pueda desarrollar un conjunto de especificaciones para cada sistema que llega hasta este paso, ya que probablemente la tecnología actual o la que se obtenga en un futuro no muy lejano no proporcionen una solución económica o técnica en el tiempo que se requiere.

Aunque las especificaciones están basadas en los requerimientos y en la tecnología, no se debe confundir esta fase con el desarrollo de la arquitectura del sistema ni con la de selección de componentes. Las mismas especificaciones pueden usarse para obtener distintos diseños del sistema, donde cada diseño es consiente con dichas especificaciones.

Las especificaciones deben establecerse en términos funcionales, de tal forma que pueda considerarse la amplia variedad de alternativas para satisfacerlas. Dichas especificaciones surgen del análisis de los requerimientos definidos anteriormente.

La información que debe presentarse en el documento de especificaciones debe incluir los puntos que se describen a continuación:

3.4.2.1 Geografía a la que se va a Servir.

- Numero de localidades (usuarios individuales)
- Distancia máxima entre dos usuarios.
- Grupos de usuarios.
- Características del área donde se instalara la red (Terreno, edificios, caminos públicos, etc.)

- Preparación para cables existentes.

3.4.2.2 Equipo que se Utilizara.

Indicar donde estarán los dispositivos en que cantidad y que función estarán desarrollando.

- Terminales.
- Computadoras personales (tamaño y velocidad del CPU, memoria principal)
- Monitores.
- Dispositivos de almacenamiento.
- Tipo de computadoras.
- Fuentes de Datos Análogos.(teléfonos, cámaras de video y equipos sensores).
- Dispositivos de Impresión.(tipos de impresoras).
- Otros dispositivos como scanner, mouses, tabletas graficas, plumas ópticas, cajas registradoras, lectores de códigos de barras).

3.4.2.3 Servicios de Red.

Estos servicios son proporcionados por servidores de la red que pueden ofrecer uno o varios servicios. En esta etapa solo se deben identificar los tipos de servicios que se requieren, no como serán provistos.

- Almacenamiento de los archivos de los usuarios.
- Bases de datos y aplicaciones comunes para acceso compartido.
- Correo electrónico.
- Gateways, módems, bridges para redes externas.
- Servicio de impresión.

3.4.2.4 Especificaciones de Trafico.

Estas especificaciones son medidas en términos de tipo (datos, voz o video) y volumen de datos (bits por segundo, erlangs o numero de canales).

Una solución en forma matricial para incorporar todos estos requerimientos distintos para obtener el total de trafico en la red. El trafico de la red se establece cuando un usuario envía mensajes a otro, por lo cual es necesario identificar a cada emisor y receptor y estimar cuanto trafico enviara a los demás. La estimación del trafico puede complementarse por un análisis de las aplicaciones que serán usadas en la red. Estimar el volumen de trafico que será generado por cada aplicación incorporarla a la de los usuarios. Cuando se tienen distintos tipos de trafico, las estimaciones deber ser expresadas en bits por segundo.

3.4.2.5 Capacidad de la Red y Rendimiento.

La capacidad de la red es el trafico total que puede soportar en cualquier intervalo de tiempo. El rendimiento de una red es descrito generalmente en términos de tiempo de respuesta o del retraso punto a punto a través de la red.

DIRECCIÓN GENERAL DE BIBLIOTECAS

3.4.2.6 Interfases al Usuario.

- Diálogos.
- Puntos de contacto con otras unidades del sistema.
- Estándares a utilizar (X- Windows, Macintosh, Motif etc.)
- Características de las interfases al usuario; uso de ventanas, descripcion de menus, colores, ayuda en linea. Etc.

3.4.2.7 Software.

- Características de los sistemas operativos.
- Manejadores de base de datos (jerárquicos de red, relacionales u orientados a objetos).
- Tipos de aplicaciones
- Utilerías.
- Software de control, seguridad y administración de la red.
- Lenguajes que serán utilizados para el desarrollo de aplicaciones.

3.4.2.8 Tipo de Procesamiento.

- Batch.
- Transacción en línea.
- Tiempo real o científico.

3.4.2.9 Seguridad.

- Passwords.
- Encriptación.
- Respaldos
- Control de paquetes transmitidos.
- Alarmas.
- Monitores.

3.4.2.10 Parámetros de Construcción.

- Construcción Modular.
- Dimensiones.
- Tipo de conectores.
- Tipo de cableado (fibras ópticas, cable coaxial, etc.).
- Interfases (RS-232, RS-449).

3.4.2.11 Comunicación.

- Líneas de comunicación: Punto a punto, multipunto, half duplex, full duplex, análogas, digitales, 2 o 4 cables.
- Modos de transmisión (Banda base o banda ancha).
- Métodos de Acceso (Token bus, token ring, bus CSMA/CD).
- Protocolos (HDLC, SDLC, X.25, etc.).
- Anchos de banda.
- Tipo de redes locales (Ethernet, Decnet, etc.).
- Utilización de redes públicas, nacionales y/o internacionales, o líneas privadas.

3.4.3 Justificación Económica.

El análisis de costo-beneficio proporciona una justificación económica para iniciar el diseño de la red de comunicaciones o para detenerlo si la compañía no puede solventar en ese momento tal inversión. Una vez que se ha pasado por todo el análisis de los requerimientos de la empresa y se han derivado las especificaciones se puede proceder sobre bases precisas a estimar el costo del proyecto y los beneficios que este aportara. La información que al respecto proporcionen los vendedores de equipo será muy importante en este paso para obtener varias alternativas de inversión.

Las alternativas de inversión son comparadas entre si en términos del costo de adquisición, instalación, soporte, capacitación, mantenimiento y operación de la red contra los beneficios por reducción de costos y tiempo, oportunidad de la información control de los procesos que se realizan en la empresa, ventaja competitiva que se adquiere, mejoramiento de las actividades de los usuarios, capacidad para atender a mas clientes etc.

Debe considerarse que existe el riesgo de que el costo puede ser mayor del estimado o que los beneficios pueden ser menos que los estimados.

3.4 Diseño.

Una vez que el problema ha sido definido apropiadamente, las funciones del diseño giran alrededor de producir un modelo adecuado del sistema de comunicaciones. Durante esta etapa el mayor esfuerzo consiste en concentrarse en la intersección de las necesidades del que solicita la red de comunicaciones con las posibilidades técnicas y económicas.

Tomando como base los requerimientos y las especificaciones fijadas previamente es posible desarrollar una serie de alternativas de diseño. Estos diseños son considerados desde el punto de vista del rendimiento del hardware y software y sus costos.

Antes de iniciar la definición de la arquitectura de la red, es recomendable aprender de la experiencia de otras empresas que enfrentaron los mismos problemas. Para lograr esto se puede buscar información en artículos con casos parecidos o visitar a un conjunto seleccionado de empresas.

3.4.1 Definición de la Arquitectura y Subsistemas.

La definición de la arquitectura de la red debe ser lo mas independiente posible del proveedor de equipo, es decir, debe ser expresada en términos funcionales.

Durante el desarrollo de alternativas de diseño es necesario, antes que nada, escoger las posibles topologías con respecto a las especificaciones funcionales y ambientales (esto esta estrictamente relacionado con la elección del medio de transmisión). Después, es necesario acoplar cada topología con el medio de acceso mas apropiado.

Para definir la configuración física de la red se produce una representación visual de la red en la cual se presentan y localizan los componentes, volumen de trafico, tiempos de respuesta, aplicaciones se ejecutan en cada localidad y se muestran los problemas eléctricos. Además, existen otros atributos que definen la información ambiental de cada componente de la red, tales como: tamaño del componente, tamaño en bytes de los datos (para calcular la memoria), distribución de canal y distribución de numero de dispositivos por canal en los sistemas de banda ancha, asignacion de prioridades de acceso a los servicios, tipo de procesamiento, interconectividad o dependencia de otras tareas, etc.

El método para configurar una red es básicamente el mismo en todos los casos. Esencialmente, son tres los factores a considerar:

- El equipo a instalar en la periferia.
- El equipo a instalar en el o los centros.
- Las enlaces de comunicación que conectan los equipos.

Una vez que se tiene una vista preliminar de la red, se puede comenzar el diseño de la red física. En este punto, es muy importante tener el apoyo de alguien con experiencia en sistemas teleinformáticos y contar con el consejo especializado de los proveedores de equipo.

La red física se define en términos de un número de factores, incluyendo:

- Uso de enlaces de comunicación públicos o privados.
- Velocidad de los enlaces de comunicación.
- Colocación física de los enlaces de comunicación.
- Uso PBX, concentradores y/o multiplexores.
- Número, capacidad y localización de los centros de procesamiento.
- Uso de procesadores frontales.
- Terminales y distribución de inteligencia.
- Colocación física de terminales.

Una vez que el diseño preliminar de la red se ha completado, el siguiente paso es optimizarlo. El propósito de la optimización es minimizar el costo y los tiempos de respuesta de la red, obteniendo la ruta mínima posible entre cada dos localidades, proporcionando varias alternativas de ruteo de la información (previando que ciertas líneas se saturen o sufran algún accidente), equilibrar el tráfico en la red y tratar de soportar la mayor cantidad de datos transmitidos.

3.4.2 Verificación de la Solución.

Después de que la arquitectura de la red se ha terminado, los resultados deben ser verificados con respecto a los requerimientos y especificaciones para asegurar que el sistema refleje adecuadamente estas necesidades y es necesario tratar de pronosticar el comportamiento de la red en el ambiente donde esta operando. Para apoyar a la verificación existe un conjunto de

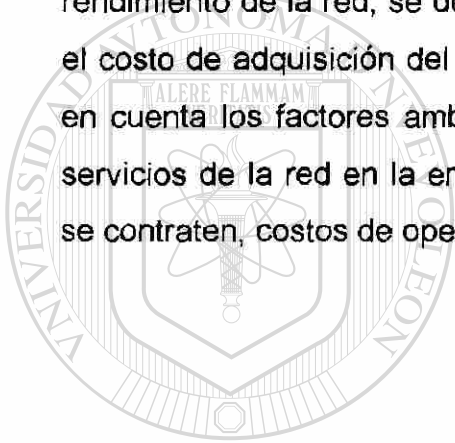
herramientas y técnicas disponibles en paquetes de software. Si no se lleva a cabo el proceso de verificación no existe una garantía de que el sistema cumpla con los requerimientos y especificaciones. Obviamente que esto será descubierto cuando el sistema final sea entregado a los usuarios.

Para estimar el rendimiento de la red se deben examinar algunos parámetros de importancia como, por ejemplo:

- El efecto de la distribución geográfica de los componentes de la red, analizando distancia que recorrerá la información y considerando las rutas alternas.
 - Métodos de acceso al medio.
 - Tiempos de respuesta.
 - Integridad de la red. El diseño de la red debe ser tal que las características y funciones de la red sean consistentes y trabajen para dar un servicio completo.
 - La capacidad de crecimiento. El sistema debe estar diseñado de tal forma que pueda crecer sin necesidad de rediseñarlo o degradar su rendimiento.
-
- La capacidad de crecimiento se mide por la máxima extensión de la red y el número de dispositivos de enlace.
- Modularidad del hardware y software. Representa la flexibilidad del sistema de comunicaciones para futuros desarrollos o cambios y posibles interfases con otros sistemas.
 - La seguridad de la red. La existencia de facilidades de red tales como administración de la clave de acceso, protección y encriptación de archivos y el nivel de seguridad ofrecido por el medio físico.
 - Facilidades para controlar la red. Capacidad para controlar las configuraciones de la red, recursos, capacidades, claves de acceso, protección y encriptación de archivos.
 - Confiabilidad. El nivel de confiabilidad de los dispositivos y de toda la red.

- **Conectividad.** Capacidad de conexión con otras redes o enlazar terminales heterogéneas u homogéneas que tengan diferentes características de operación.
- **Facilidad de uso de las aplicaciones y servicios en red.** Las aplicaciones y servicios deben proveer interfases al usuario eficientes y adecuadas a las personas que van a interactuar con ellas.

En la evaluación de las alternativas de diseño que se tienen el costo es por lo general un factor determinante, es por eso que una vez que se ha medido el rendimiento de la red, se determina el costo total de cada diseño considerando el costo de adquisición del software y hardware, costo de instalación (tomando en cuenta los factores ambientales), costos de capacitación y difusión de los servicios de la red en la empresa, costos ocasionados por los empleados que se contraten, costos de operación y costos de mantenimiento.



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



DIRECCIÓN GENERAL DE BIBLIOTECAS

CAPITULO 4

METODOLOGÍA PARA ADMINISTRACIÓN DE UNA RED.

4.1 Herramientas de Software para la Planeación y Diseño de la Red.

Se han desarrollado paquetes de software que pueden asistir en la planeación, diseño y evaluación de una red. Estos paquetes pueden ser usados para evaluar alternativas de topologías de red, predecir el rendimiento de la red, calcular costos considerando las tarifas actuales en comunicación y los costos del equipo de red.

Las herramientas de diseño de red han sido desarrolladas usando algoritmos heurísticos que abrevian enormemente el proceso de optimización del diseño de una red con unas cuantas aproximaciones bien escogidas. Para evaluar eficientemente un diseño de red y pronosticar su rendimiento, se usan básicamente técnicas de modelos analíticos, de simulación y emulación.

Estas herramientas permiten trabajar en forma interactiva sobre un diseño de red y hacerle modificaciones, tales como agregar o quitar recursos (procesadores frontales, multiplexores, controladores, etc). Colocar nuevas rutas de comunicación, establecer la velocidad de las líneas, especificar la longitud y distribución de los datos, indicar las características de los protocolos utilizados, asignar cargas al sistema incluyendo cuellos de botella y observar como se comporta la arquitectura de la red bajo las condiciones definidas. En esta forma se puede obtener la configuración optima de la red

y realizar un análisis de costo/rendimiento, el cual genera una familia de curvas que muestran el comportamiento de los parámetros evaluados.

4.2 Desarrollo e Instrumentación.

La instrumentación de una red es la etapa mas critica del proyecto. Necesita de una planeación especifica para minimizar la incertidumbre. La instrumentación debe seguir las siguientes etapas.

- Plan de implementación e instalación.
- Adecuación del sitio de instalación.
- Planeación y administración del cableado.
- Contratación de circuitos y enlaces públicos.
- Selección y adquisición de productos, equipos, software, etc.
- Instalación del hardware / software.
- Pruebas y verificación del funcionamiento.
- Capacitación de usuarios y personal de explotación.
- Puesta en operación.
- Inicio de la explotación y administración.

4.2.1 Plan de Implementación e Instalación.

Es el inicio de la fase de instrumentación, debe incluir los pasos a ser completados, la estimación del nivel de esfuerzo requerido y el calendario de eventos. Es recomendable utilizar un diagrama de barras para resumir el plan de implementación. El objetivo del plan es:

- Asistir en el desarrollo de la instalación.
- Estimar el esfuerzo involucrado en cada segmento.
- Identifica segmentos en la ruta critica.
- Mide el progreso durante el proyecto.
- Sirve como una base para futuras estimaciones.

La identificación los pasos de instalación incluyen:

- La organización.
- Diseño detallado.
- La adecuación de los sitios.
- La entrega de los materiales hardware y software.
- La instalación de los equipos y sistemas.
- La verificación y pruebas.
- La contingencias.
- Los riesgos.

El plan debe contemplar un marco de tiempo.

- Fechas de terminación de tareas o segmentos.
- Traslapé entre segmentos.
- Consideraciones sobre el personal involucrado.
- Requerimientos de balanceo del personal.
- Considerar la simultaneidad de proyectos.
- La coordinación multiproyecto.
- La documentación.

4.2.2 Selección y Adecuación del Sitio de Instalación.

Se deben considerar los siguientes factores en la selección del sitio:

- Requerimientos de nuevos equipos y tiempo para obtenerlos.
- Localización del sitio en relación a las funciones de oficina.
- El sitio existente y su eventual remodelación.
- Requerimientos de ductos y canalizaciones.
- Requerimientos de seguridad.
- Requerimientos de energía eléctrica, aire acondicionado, agua.
- Requerimientos de alarmas en caso de fuego, inundación, terremoto, etc.

La adecuación del sitio de instalación, una vez que este ha sido seleccionado, debe asegurar que se tiene la disponibilidad de los siguientes documentos:

- Especificaciones de construcción o remodelación del sitio.
- Documentación de espacios físicos necesarios para equipo.
- Desarrollo de la agenda de preparación.
- Monitoreo de fechas.
- Seguridad del equipo y del sitio (fuego, humo, terremotos, inundación).
- Mantenimiento del inventario de equipos y refacciones.
- Planes de contingencia para elementos críticos.

4.2.3 Planeación, Administración e Instalación del Cableado.

El cableado y su instalación representa en la mayoría de las redes el 50% del costo total del sistema. Por lo que requiere de una administración efectiva. Para poder planear una instalación de cableado se debe responder preguntas tales como:

¿ Cual es la localización de los nodos?

¿Cuál es el impacto de la dispersión geográfica?

¿ Los ductos actuales soportan cableado adicional?

¿ Que tan volátil es el ambiente(reubicaciones)?

¿ Existen fuentes de interferencia electromagnética?

Las reglas seguidas para una instalación de cableado exitosa son:

- Probar el cable(todos sus pares) y documentar los resultados.
- Elaborar planos para identificar rutas de cableado y equipos.
- Etiquetar cada conector y cada segmento de cable.
- Mantener el cable al menos 30 cms. lejos del cable eléctrico.
- Los cables de LAN's deberán correr perpendicular al cable eléctrico y separado a 30 cms.

- Para evitar averías al cable, debe ponerse en canaletas y jalarlo de abajo del conjunto.
- Jalar los cables en grupo a un punto de distribución central. Asegurar los cables con "sostenedores".
- No colocar los cables sobre los materiales del techo.
- No colocar los cables en donde la gente pueda pisarlos, tropezarse, romperlos o aplastarlos con muebles o sillas.

La administración del cableado es administrada por medio de un sistema de software (incluye CAD y bases de datos). Constituido de una plataforma hardware y un software.

4.2.4 Contratación de Circuitos y Enlaces Públicos.

Las empresas constituidas de infraestructuras distribuidas geográficamente, en la mayoría de los casos requieren de la renta de circuitos públicos para conformar su red privada. En países como México en donde las infraestructuras públicas son relativamente limitadas o costosas, esta contratación toma una gran cantidad de tiempo y afecta de manera importante el proceso de instrumentación de la red. Entonces debe considerarse la disponibilidad de circuitos por parte de los prestadores de servicios. Y considerar el tiempo para obtener el circuito operacional. Para lograr este objetivo debe elaborarse una memoria técnica por cada enlace, la cual es aprobada por un gestor (perito) que otorgue su visto bueno. Para que una empresa pueda beneficiar del servicio, es necesario que cumpla con los requerimientos de una preparación del sitio, o de interfaces en donde el enlace es colocado. Depende del tipo de circuito o enlace a contratar:

- Línea privada (local o interurbana).
- Enlace vía satélite (infraestructura pública).
- Segmento espacial (para uso de red privada).
- Red Digital integrada (local o interurbana).
- Microonda digital (urbana).

4.2.5 Selección y Adquisición de Equipo.

Cuando la adquisición de la infraestructura es muy grande o costosa, se hace necesario plantear y elaborar un documento a ser entregado a los posibles proveedores. Este documento es conocido como RFP(request for proposal). El RFP resume todos los requerimientos del equipo y solicita a los proveedores potenciales responder con una propuesta técnica y una cotización del costo. Los RFP son una forma adecuada de solicitar un amplio rango de soluciones y encontrar al proveedor que verdaderamente tenga la solución.

La evaluación de las respuestas es un evento crítico. Es importante asegurar que el procedimiento de evaluación es objetivo. Los pasos recomendados para establecer la selección final incluyen:

- Asegurar que los requerimientos establecidos en el diseño de la red son cumplidos los mas cercanamente posible, y con el nivel de detalle especificado.
- Es recomendable asegurarse que un sistema similar esta en instalado y operando en al menos 2 empresas diferentes. Esto ayuda a conocer a través de sus usuarios las experiencias de utilización del sistema.
- El acceso a los registros de rendimiento del sistema.
- La respuesta seleccionada no es siempre la mas barata. Deberá estar en el menor rango de costo y cumplir ampliamente con los requerimientos.

En el proceso de selección de equipos los pasos que se recomiendan son los siguientes:

- Eliminar los RFP's que no cumplen con los requerimientos obligatorios.
- Crear una tabla de respuestas. La cual deberá mostrar las características deseadas y su costo.
- Revisar las características detalladamente. Los requerimientos son cotejados contra las hojas de respuesta (RFP) y la información originada (tablas).

- Realizar un análisis del ciclo de vida. Las propuestas se someten a un análisis detallado de costos en que se incurrirá a lo largo de la vida del sistema. En este paso la selección se limita a 2 o 3 productos que ofrecen las mejores características.
- Revisar el rendimiento técnico de las mejores propuestas. Se prueban las características de operación, las estaciones y terminales se evalúan, los métodos de mantenimiento y administración se examinan y se revisan los procedimientos de soporte de los vendedores.
- Asignar un peso a las características deseadas. No todas las características son de igual importancia, por lo tanto es necesario usar una ponderación de acuerdo a su grado de importancia.
- Desarrollar una evaluación final del producto. Para llevar a cabo esto debemos decidir que factores se incluirán en la selección del proceso y la importancia de cada uno de ellos. Los factores típicos son:
 - Costo del ciclo de vida.
 - Capacidad y experiencia del vendedor.
 - Evaluación de las características obligatorias.
 - Evaluación de las características deseadas.
 - Plan de soporte del proveedor.

4.2.6 Instalación del Hardware / Software.

Para proceder a la instalación del equipo hardware / software se recomienda seguir los siguientes lineamientos:

Revisar y aprobar la preparación completa del sitio de instalación. Esta actividad consta de:

- Disponer del inventario del sitio físico y de requerimientos de facilidades.
- Los sistemas de soporte deben estar aprobados (Energía eléctrica aire acondicionado, etc.).
- Disponer de la programación detallada de la entrega de materiales e instalación del equipo.
- Disponer de los planos de cada área de trabajo.

- Disponer del resumen de las características del hardware / software.
- Disponer del programa detallado de pruebas de hardware y software.

Recepción e instalación del equipo(hardware).

- Asistencia del proveedor para instalar e inspeccionar el equipo.
- El equipo del proyecto deberá asegurarse de las características del equipo requerido.
- Asegurarse que el proveedor ha probado las opciones no estándar solicitadas.

Recepción e instalación del software

- Asegurar que los programas fuente, objeto, y librerías han sido asignados y cargados adecuadamente.
 - El software nuevo es probado por el proveedor y debe suministrar los datos y resultados de las pruebas.
 - Asegurar que no existe discrepancias entre esos resultados y el rendimiento del software esperado para el sistema.
-
- Restringir las modificaciones a los cambios que son necesarios para hacer el software operacional.
 - Hacer una copia de respaldo del software probado, incluyendo el programa, el lenguaje de control, las instrucciones de operación y los manuales.
 - Manejar las contingencias y diferencias encontradas.

4.2.7 Pruebas y Verificación del Funcionamiento.

El equipo del proyecto deberá formar un equipo de trabajo para efectuar las pruebas necesarias. Es muy importante tener la aprobación del usuario, quien deberá revisar y aprobar que las pruebas propuestas son esenciales para el funcionamiento del sistema. El equipo de pruebas deberá conducir el proceso de pruebas. Se deben involucrar analistas, diseñadores, representantes de usuarios y expertos de pruebas del sistema. En caso de que el resultado de las pruebas conduzca a cambios en el diseño. Se deben usar procedimientos formales y documentos para evaluar y obtener la aprobación final a cada cambio propuesto. Además se debe asegurar que el sistema funciona de acuerdo a los tiempos de respuesta esperados en el diseño. Y finalmente se debe escribir la aprobación, con el objeto de identificar modificaciones y establecer el nivel de confianza del sistema.

Algunas de las pruebas que debe ser aplicadas en este proceso incluyen:

- Probar las capacidades de transferencia de archivos con todos los tipos de archivos soportados.
- Probar que todos los equipos funcionen adecuadamente con los diferentes tipos de Sistemas Operativos.
- Si la red lo soporta, enviar múltiples archivos a nodos únicos simultáneamente, para probar sincronización y acceso a la red.
- Si es soportado el software de terminal virtual, se debe probar la conexión con diferentes sistemas y aspectos de enlace (edición de pantallas, formas, graficas, etc).
- Escribir programas "muestras" para probar librerías y futuras aplicaciones.
- Probar las facilidades ofrecidas por el software de control o administración de la red. (desconectar equipos y observar)
- Probar las aplicaciones que actualmente se encuentran operacionales. Para observar compatibilidad con el nuevo sistema.
- Desconectar nodos y verificar estabilidad de la red. Esto se hace a mitad de una sesión para verificar el control de error y recuperación.

- Probar el rendimiento del sistema:
 - a) Tiempo de establecimiento de sesión o conexión.
 - b) Tiempo de respuesta en la transmisión de datos / archivos.
 - c) Medición del “throughput” del sistema.
 - d) Medición de los “time out’s”.

4.2.8 Capacitación de Usuarios y Personal de Explotación.

Posteriormente al establecimiento de los procedimientos, es necesario entrenar al personal en las nuevas funciones o procedimientos. El equipo encargado de las operaciones de la red deberá ser entrenado antes del comienzo de la instalación, con el objeto de recuperar todo ese conocimiento. El entrenamiento es requerido por los siguientes grupos:

- Control de la red para el diagnóstico en los nuevos equipos.
- Los usuarios para el aprendizaje de los nuevos procedimientos de operación de la red.
- Servicio al usuario, para las nuevas reglas de asistencia a usuarios.

Es necesario desarrollar un programa específico de entrenamiento, que incluya los siguientes puntos:

- Objetivos.
- Tipo de Audiencia.
- Tópicos a ser cubiertos.
- Método de entrenamiento sugerido.
- Longitud estimada de cada tópico.
- Actividades y ejercicios en cada tópico.
- Numero y tipo de sesiones de entrenamiento y fechas requeridas para su finalización.

El entrenamiento debe identificar necesidades continuas de entrenamiento, mantener el material desarrollado en forma modular, y asegurar el nivel de detalle para homogeneizar el conocimiento de los instructores. Un aspecto muy importante en este proceso es el de organizar el desarrollo de equipos de entrenamiento. En el cual una persona debe coordinar el desarrollo del material. El líder de proyecto y un analista funcional desarrollan el programa de entrenamiento. Y los analistas funcionales involucrados en el diseño detallado y documentación desarrollan el material para los usuarios. Es conveniente que las otras áreas también desarrollen su material.

4.2.9 Inicio de la Explotación y Administración.

El momento culminante del proyecto es cuando el sistema entra en operación. Sin embargo antes de la puesta en operación del sistema se deben contar con los siguientes requerimientos:

- Mecanismo de soporte de problemas: Cuando algo no funciona o se tiene duda ¿Quién resuelve los problemas?
- Actualizar las políticas de administración de la seguridad en un ambiente de redes.
- Finalizar los contratos de mantenimiento y soporte con el proveedor. Comunicar estos al grupo de soporte interno.
- Producir, copiar y distribuir guías y manuales de usuario. Estos son documentos de consulta rápida.
- Establecer los procedimientos de control y administración. Esto sirve para saber como es controlada la red, como se hacen las actualizaciones, los respaldos y las otras tareas relacionadas a la administración.
- Crear o modificar los planes de recuperación en caso de desastre. Para reflejar la necesidad y utilización de la red en una operación de recuperación siguiendo a un desastre.
- Otros elementos relacionados.

4.3 Explotación y Administración

La explotación y la administración de una red abarca las actividades necesarias para operar y mantener la red en las condiciones necesarias para que a través de su vida útil satisfaga las necesidades de los usuarios; tales como disponibilidad, eficiencia y estabilidad y las necesidades del negocio; las nuevas aplicaciones, los nuevos clientes, adoptar nueva tecnología, operación remota, cambios y crecimiento.

En términos generales la administración de una red consiste de un conjunto de acciones, métodos y procedimientos que se llevan a cabo para mantener la operación continua de una red. Sus objetivos principales son:

- Lograr la operación continua y eficiente de los sistemas de comunicación
- Mejorar la productividad de la red.
- Obtener un mejor rendimiento de los recursos.
- Mejorar la calidad de servicio ofrecido a los usuarios.
- Anticiparse a los problemas; evitarlos, minimizar inconvenientes y controlar los daños.
- Planear crecimiento futuro.
- Reducir costos.

Las responsabilidades principales del administrador de la red son:

- Instalación de la red.
- Mantenimiento preventivo y correctivo.
- Actualización tanto en hardware como en software.
- Resolver problemas de la red.
- Predecir crecimiento de la red.
- Seguridad en el sistema.
- Contabilización de recursos.
- Historial.

El administrador de la red se encuentra ante la problemática de que los componentes de las redes en una empresa generalmente son de distintos proveedores y se encuentran en una situación geográfica dispersa en constante crecimiento y con aplicaciones y datos distribuidos. Por lo que el proceso de administración tiene como elementos fundamentales a los administradores de la red, las herramientas de monitoreo y los procedimientos.

Las funciones de la administración de redes pueden organizarse en varias áreas:

- Administración de la red.
- Control de la red.
- Seguridad de la red.

Las funciones, políticas, responsabilidades y mecanismos de la administración deben ser planeadas de tal forma que el arranque de la red con los usuarios sea un éxito.

4.3.1 Funciones de Administración de la Red.

La administración de una red trata con una gran cantidad de funciones no técnicas involucradas en la operación de la red en su ciclo de vida. La administración incluye:

- Planeación y presupuesto.
- Evaluar del nivel de servicio, lo cual puede observarse en los reportes de rendimiento de la red o a través de los usuarios.
- Determinar mecanismos para registro y análisis de los problemas de la red que se presenten.
- Evaluación del tráfico de la red.
- Administración de la configuración.
- Procurar la seguridad de la red.
- Ordenar, instalar y aceptar equipo nuevo para la red.

- Control de inventario. Del equipo, de los proveedores, de mantenimiento .
- Asignación de nombres y mantenimiento del directorio.
- Respaldo de archivos.
- Control y distribución de las nuevas versiones de software.
- Mantenimiento preventivo.
- Administrar los cambios mediante una adecuada planeación, desarrollo y documentación.

En redes pequeñas, la responsabilidad de la administración de la red puede ser parte de las actividades de una persona. Pero, conforme la red crece, llega a ser necesario un equipo de tiempo completo. Es necesario el personal que asista a los usuarios en el arranque de la red y les ayude a resolver los problemas que se les presenten. La buena documentación es necesaria, pero no es suficiente.

Para la administración de la red los siguientes parámetros de vital importancia: tiempo de respuesta, disponibilidad, utilización, seguridad y tráfico.

El nivel requerido de soporte debe haberse incluido en el análisis costo-beneficio y en el plan de administración.

4.3.2 Control de la Red.

El control de la red consiste en mantener a la red en un estado de operación completo, por lo que sus funciones principales son:

- Monitorear la red.
- Diagnosticar fallas.
- Mantenimiento remedial.

El monitoreo de la red puede efectuarse en tres formas principalmente:

- Escuchando pasivamente todo el tráfico en la red, así se pueden observar problemas y notificar al operador.
- Comunicándose con otros componentes inteligentes en la red para obtener reportes de sobre la integridad de todas las partes de la red.
- A través de comandos para activar componentes que remedien ciertos tipos de fallas.
 - Cargando copias de software que ha sido alterado o dañado.
 - Desconectando de la red los elementos que no funcionan bien.
 - Reinicializando los parámetros de operación a aquellos que coincidan con las condiciones de tiempo-real.

El monitoreo de la red puede realizarse automáticamente o con un operador para identificar y diagnosticar fallas en la red, aun si no pueden repararse remotamente. Dada la complejidad de las redes y la creciente variedad de hardware, software y componentes de transmisión, el problema de identificar la fuente de una falla no es algo trivial; por lo que el uso de un sistema de control de red es muy valioso.

Las siguientes son las responsabilidades mas importantes del controlador de la operación de una red.

- DIRECCIÓN GENERAL DE BIBLIOTECAS
- Recabar datos acerca del servicio y utilización de la red.
 - Dar servicio al cliente.
 - Evaluar alertas y notificaciones de fallas.
 - Tomar resoluciones cuando se presenta un problema.
 - Reparar los componentes de la red y determinar procedimientos de respaldo de la información.
 - Hacer pruebas periódicas a los componentes para comprobar su buen funcionamiento.
 - Controlar la configuración de la red (balance de la carga, alternar prioridades, rutas alternas, correo etc.)
 - Generación de software de red.

- Activar, desactivar o reinicializar sistemas y componentes de la red.
- Dar mantenimiento preventivo y remedial.
- Utilizar herramientas de diagnostico de fallas.
- Evaluar estadísticas de error.

4.3.3 Seguridad de la Red.

La seguridad de la red se refiere a la protección de los recursos que contiene la red. Puede ser dividida en:

- Seguridad física.
- Control de acceso.
- Seguridad de transmisión.

Uno de los objetivos del sistema de seguridad es prevenir que los usuarios no autorizados penetren en el sistema, y dado el caso de estos se hayan introducido detectar esto lo antes posible para tomar medidas al respecto e impedir que el individuo tome o altere información.

4.3.3.1 Seguridad Física.

La seguridad física trata de proteger a la red de daños ocasionados por personas o causas naturales.

La principal amenaza para el cable de una red parecen ser los trabajadores que ignoran cual es el cable estropeado y cortan uno que no era. Marcar la localización de los cables puede ofrecer una medida de protección contra esto.

Los mismos usuarios pueden dañar los cables desconectándolos o enroscándolos, particularmente si estos están expuestos en las oficinas donde se conecto una terminal. La mejor solución para esto es tener una salida en la pared a la cual se conecta la terminal.

Existen cierto riesgo de que el cable sea dañado por los animales, como roedores. Una zanja profunda o salidas con cubiertas muy fuertes pueden ayudar en estas situaciones.

La integridad de la red puede ser afectada también por causas naturales como inundaciones e incendios los cuales pueden dañar cables y o servidores. Los servidores pueden dañar por exceso de calor o humedad es necesario una cuidadosa planeación de la instalación de cable y servidores.

4.3.3.2 Control de Acceso.

Las funciones principales de control de acceso son autorizadas a ciertos usuarios para que utilicen los recursos de la red e impide que los usuarios no autorizados no hagan uso de la red.

En mecanismo mas comúnmente empleado es el uso de passwords. Los passwords pueden ser usados para limitar el acceso algunos o todos los recursos de la red. Cada dispositivo o recurso puede tener su propia lista de passwords, de tal manera que el usuario tenga que dar varios passwords durante una sesión o tener un password para acceder todos los recursos autorizados.

Frecuentemente los passwords no resultan efectivos porque los usuarios no tienen cuidado de elegir un password apropiado o protegerlo de que los descubran. Una política de seguridad efectiva puede ser:

- Asignar passwords a través del sistema o por una persona de seguridad.
- Incluir una mezcla de caracteres alfabéticos y no despleables (return, escape, etc.).
- Cambiar regularmente los passwords.
- Enfatizar a los usuarios la necesidad de proteger los passwords y quizá penalizar la falta de cuidado.

Los procedimientos para administrar los passwords, incluyendo como deben ser definidos y distribuidos y que tan frecuentemente deben ser cambiados, debe ser parte del plan de seguridad de la red.

Es conveniente realizar una revisión periódica de los puntos vulnerables de la red para evitar que por medio de ellos se introduzcan usuarios sin autorización. Estos puntos más vulnerables son:

Cuartos de equipo y gabinetes de cables. Como puntos de concentración de una gran cantidad de circuitos, los cuartos de equipo y gabinetes de cables son particularmente vulnerables. Estos deben permanecer bien cerrados y asignar las llaves a personas autorizadas.

Seguridad en el password. Los programas que se dan de alta automáticamente a través de passwords deben evitarse excepto cuando la información no es muy sensible. Existen programas que permiten leer cualquier porción de disco y que pueden ser usados por intrusos expertos que podrán descubrir el password que necesitan para ingresar al sistema.

Circuitos de Dial Up. Los aparatos que están conectados a la red pública de teléfonos son vulnerables para el acceso no autorizado. Por ejemplo, si un individuo quiere el número telefónico de una terminal dial up, todo lo que necesita es una copia de un recibo telefónico. Una medida de seguridad es usar módems dial back.

Niveles de Seguridad en Base de Datos. Una base de datos puede ser programada para aceptar acceso a los archivos solo desde las terminales autorizadas además, como es difícil asegurar que personas no autorizadas utilicen estas terminales, es conveniente que además de códigos de terminales se tengan passwords en una base de datos se pueden manejar las siguientes clasificaciones:

- Los archivos personales solo pueden ser accesados por sus dueños.
- Los archivos privados solo pueden ser accesados para lectura y escritura por la lista de passwords autorizados.
- Los archivos compartidos pueden ser leídos por todos, pero escritos solo por un grupo limitados.
- Los archivos públicos pueden ser leídos por todos lo que tengan acceso a la base de datos.

Comportamiento del medio de transmisión. Las redes locales y multidrop están diseñadas para compartir el mismo medio de transmisión. Los dispositivos de estas redes son capaces de copiar todos los mensajes y descartar los mensajes dirigidos a otros dispositivos. Los analizadores de protocolos pueden monitorear todo el tráfico de la red y fácilmente desplegar el contenido de los mensajes. La encriptación es la mejor solución a este problema.

Transmisión por radio. Es imposible evitar que personas no autorizadas reciban las transmisiones por radio. Esto aplica tanto para microondas como satélite. La única forma es a través de la encriptación. El medio de comunicación mas seguro es la fibra óptica, pero obviamente no es factible para todos los casos.

4.3.3.3 Seguridad en la Transmisión.

La seguridad en la transmisión se refiere a la protección de la información en transito en la red de las amenazas de fugas o inyección de información.

Fugas de información se refiere al acceso no autorizado con el fin de obtener información de la red. Esto comúnmente sucede a través de conexiones secretas pasivas.

Inyectar información se refiere introducir información señales en la red, las cuales se disfrazan como señales autenticas o alteran las señales

auténticas. La inyección es una característica de una conexión secreta activa.

La encriptación es una de las soluciones tanto para la fuga como inyección de información. Con la encriptación los mensajes son traducidos a otro código. (Según el procedimiento de encriptación usado) en la estación origen y transmitidos al otro extremo, donde al recibir el mensaje se descifra. Sin el conocimiento del proceso de encriptación usado, el mensaje es ilegible.

Cuando se usa una encriptación, la fuga de información deja de ser un problema porque el mensaje es ilegible para la persona no autorizada que lo pretende leer. La inyección de información también se previene porque el perpetrador no conoce las reglas que debe seguir para encriptar correctamente.

Al desarrollar un plan de seguridad para la red es conveniente atacar los siguientes puntos:

- Protección Operacional.
- Encriptación.
- Manejo de llaves.
- Autenticación.
- Numeración secuencial de los paquetes transmitidos.
- Procedimientos de Log – on y password.

4.4 Análisis del Rendimiento de la Red.

El análisis de rendimiento de la red es una investigación cuantitativa y cualitativa que se realiza para:

- Verificar que el nivel de servicio se mantengan.
- Identificar actuales o potenciales cuellos de botella.
- Establecer y reportar las tendencias en cuanto a la toma de decisiones administrativas y planeación.

Las principales responsabilidades del analista de la red son las siguientes:

- Establecer y mantener una base de datos donde se guarde la información recogida sobre los valores de los parámetros utilizados para medir el rendimiento de la red.
- Hacer un análisis del tiempo de respuesta en función del sistema y de la carga de la red y con respecto a la productividad del cliente.
- Definir indicadores de rendimiento.
- Preparación de procedimiento para el control operacional.

El análisis cuantitativo se lleva a cabo por medio de la utilización de herramientas de administración.

DIRECCIÓN GENERAL DE BIBLIOTECAS

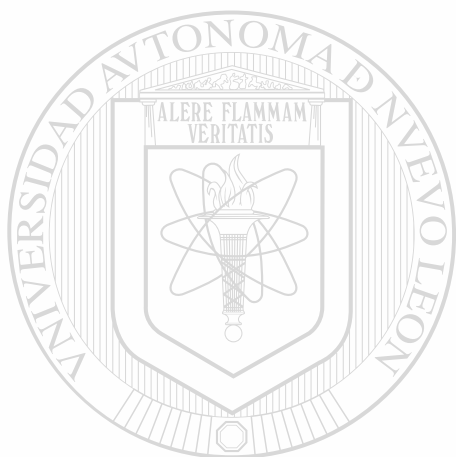
4.5 Planeación y Reconfiguración de la red.

El proceso de planear la capacidad de la red se base en los datos obtenidos sobre el rendimiento de la red, el flujo de trafico, la utilización de recursos, requerimientos de la red, tendencias de la tecnologías y la estimación de crecimiento de las aplicaciones presentes y futuras.

Las actividades principales de esta planeación son:

- Colección de datos.
- Establecer requerimientos.
- Diseño y optimización.
- Desarrollo.

Con el proceso de planeación de la capacidad de la red estamos cerrando un ciclo de vida de la red.



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



DIRECCIÓN GENERAL DE BIBLIOTECAS

CAPITULO 5

AREAS FUNCIONALES DE LA ADMINISTRACION DE REDES.

Algunas compañías dividen la administración de red en las cinco siguientes funciones basadas en el usuario: administración de la configuración, administración del desempeño y la contabilidad, administración de problemas, administración de operaciones y administración de cambios.

5.1 Administración de la Configuración.

La primera de las cinco funciones controla la información que describe las características físicas y lógicas de los recursos de la red, así como las relaciones entre dichos recursos. Un sistema de administración central almacena los datos en la base de datos de la administración de la configuración e incluye información como los números de versión del software del sistema o micro código; números de serie del hardware y software; ubicación física de los dispositivos de red; nombre, direcciones y números telefónicos de contactos. Los elementos de la administración de la configuración ayudan a llevar un inventario de los recursos de la red y asegurar que los cambios en la configuración de la red se reflejen en la base de datos de la administración de la configuración. La administración de la configuración también proporciona información que se utiliza en los sistemas de administración de problemas y en la administración de cambios. Los sistemas de administración de problemas utilizan esta información para comparar las diferencias en versión y para ubicar,

identificar y verificar las características de los recursos de la red. Los sistemas de administración de cambios utilizan la información para analizar el efecto de los cambios y para programar los cambios en momentos de impacto mínimo de la red.

5.2 Administración del Desempeño y la Contabilidad.

La segunda función proporciona información respecto al funcionamiento de los recursos de red. Las funciones de los equipos de administración de desempeño y contabilidad incluyen el monitoreo de los tiempos de respuesta de los sistemas; la medición de los recursos disponibles; la sintonía, rastreo y control del desempeño de la red. La información recabada por las funciones de administración de la contabilidad y el desempeño es útil para determinar si se están alcanzando los objetivos de desempeño de la red o si, con base en el desempeño se deben iniciar procedimientos de determinación de problemas.

5.3 Administración de Problemas.

Aquí se maneja las condiciones de error que hacen que los usuarios pierdan toda la funcionalidad de un recurso de la red. La administración de problemas se lleva a cabo en cinco pasos: determinación del problema, diagnóstico del problema, recuperación y desvío del problema, resolución del problema, rastreo y control del problema. La determinación del problema consiste en detectar un problema y dar todos los pasos necesarios para comenzar el diagnóstico del problema, como confinar el problema a un subsistema en particular. El diagnóstico del problema consiste en determinar la causa precisa del mismo y la medida que es necesario tomar para resolverlo. El desvío y recuperación del problema son intentos para desviar el problema, parcial o totalmente. Solo da una solución temporal y depende del módulo de resolución de problemas para resolverlo permanentemente. La resolución del problema es la suma de los esfuerzos para eliminarlo. En general comienza una vez terminado el

diagnostico del problema y suele implicar acciones correctivas, como el reemplazo de hardware o software en estado de falla. El rastreo y control de problemas consiste en el rastreo de cada uno de ellos hasta llegar a su solución final. La información vital que describe el problema se almacena en una base de datos de problemas.

5.4 Administración de Operaciones.

Consiste en administración distribuida de los recursos de la red desde un punto central por medio de dos conjuntos de funciones: servicios de administración de operaciones y servicios de operaciones comunes. Los servicios de administración de operaciones permiten controlar los recursos remotos centralmente por medio de las funciones siguientes: activación y desactivación de recursos, cancelación de comandos y configuración del reloj. Los servicios de administración de operaciones se pueden iniciar automáticamente en respuesta a ciertas notificaciones de problemas en el sistema.

Los servicios de operaciones comunes permiten la administración de recursos que no son manejados explícitamente por otras áreas de administración, por medio de una comunicación especializada a través de aplicaciones nuevas y más capaces. Los servicios de operaciones comunes proporcionan dos servicios importantes, el comando ejecutar y la administración de recursos. El comando ejecutar representa una forma estándar para ejecutar comandos remotos. El servicio de administración de recursos proporciona una forma de transportar información en una manera independiente del contexto.

5.5 Administración de Cambios.

Rastrea los cambios en la red y mantiene archivos de modificaciones en los nodos remotos. Los cambios en la red ocurren principalmente por dos razones: cambios en los requerimientos del usuario y evitar problemas. Los cambios en

los requerimientos del usuario incluyen las actualizaciones en hardware y software, nuevas aplicaciones, servicios y otros factores que modifican constantemente las necesidades de los usuarios de la red. Evitar problemas es necesario para enfrentar cambios inesperados producidos como resultado de la falla de hardware, software u otros componentes de la red. La administración de cambios tiene como objetivo minimizar los problemas promoviendo de manera ordenada los cambios de la red y administrando los archivos de cambios, los cuales guardan una bitácora de las modificaciones realizadas en la red.

5.6 Arquitecturas de la Administración de Red.

5.6.1 Arquitectura ONA.

Arquitectura de Redes Abierta es una arquitectura generalizada de administración de red que define cuatro entidades de administración clave: el punto focal, el punto de colección, el punto de parámetro y el punto de servicio. El punto focal es una entidad de administración que proporciona el soporte para las operaciones de administración de red centralizada. Responde a las alertas de la estación terminal, conserva las bases de datos de administración y representa una interfase de usuario para el operador de administración de la red. Existen tres tipos de puntos focales: principal, secundario y anidado. Los puntos focales principales llevan a cabo todas las funciones focales. El punto focal secundario actúa como respaldo de los puntos focales principales y se utiliza en el caso de una falla en el punto focal principal. El punto focal anidado proporciona el soporte de la administración distribuida en redes grandes. Los puntos focales anidados son responsables del reenvío de información crítica a los puntos focales globales.

Los puntos de reunión transfieren información desde las subredes SNA auto contenidas hasta los puntos focales y se suelen utilizar para reenviar datos desde redes entre equivalentes de IBM hasta una jerarquía ONA.

Un punto de parámetro es un dispositivo SNA que puede implementar un ONA en sí mismo y otros dispositivos. La mayor parte de los dispositivos SNA estándar tienen la capacidad de ser puntos de parámetros.

Un Punto de servicio es un sistema que ofrece acceso a ONA, para dispositivos no SNA y es, en esencia, una puerta de enlace hacia ONA. Los puntos de servicio tienen la capacidad de enviar información de administración sobre sistemas no SNA hacia los puntos focales, recibir comando de los puntos focales, traducir comandos en un formato aceptable hacia dispositivos no SNA y reenviar comandos a dispositivos no SNA para su ejecución.

5.6.2 System View

Es un plano de prueba que sirve para crear aplicaciones de administración capaces de manejar sistemas de información de diferentes proveedores. Describe como las administraciones que manejan las redes heterogéneas operan con otros sistemas de administración. Es la estrategia oficial de administración de sistemas de la arquitectura de sistemas de aplicación.

5.7 Plataformas de Administración de la Red.

Es una plataforma de administración de red corporativa de IBM de gran alcance, que ofrece servicios de administración de red SNA centralizados. Se utiliza en mainframes IBM y parte del ONA. NetView consta de equipo de control de comandos, monitor de hardware, monitor de sesión, función de ayuda, monitor de status, monitor de desempeño y monitor de distribución. El equipo de control de comandos proporciona el control de la red mediante la generación de comandos básicos de operación y de acceso a archivos a las aplicaciones VTAM, controladores, sistemas operativos y NetView/ PC. La función de monitor de sesión actúa como un monitor del desempeño de VTAM y permite determinar problemas de software y administrar la configuración. La función de ayuda proporciona ayuda a los usuarios de NetView e incluye un

equipo de navegación, un equipo de escritorio de ayuda y una biblioteca de las situaciones de operación de red que se presentan mas comúnmente. El monitor de status describe y presenta información sobre el status de la red. La función del monitor del desempeño vigila el desempeño de los FEPs (Procesadores de sistema frontal), el NCP (Programa de Control de Red) y otros recursos conectados. El administrador de distribución planea, programa y rastrea la distribución de datos, software y micro código en entornos SNA.

5.8 Administrador de LAN.

LNM (Administrador de la Red LAN) es una aplicación de administración de red de IBM que controla las LANs Token Ring desde una ubicación de soporte central. LNM es un producto basado en la edición extendida del OS/2 que ínter opera con NetView de IBM (que esta al tanto de actividades LNM como las alarmas) y otros software de administración de IBM.

5.9 Protocolo SNMP

La administración de la red se puede implementar mediante SNMP(Protocolo Simple De Administración de Red) este es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de la red. SNMP hace posible que los administradores de red administren el desempeño de la misma, encuentren y resuelvan problemas en ella y planeen su crecimiento.

En sus distintas versiones, es un conjunto de aplicaciones de gestión de red que emplea los servicios ofrecidos por TCP/IP, protocolo del mundo UNIX, y que ha llegado a convertirse en un estándar. Surge a raíz del interés en encontrar un protocolo de gestión que fuese válido para la red Internet, dada la necesidad del mismo debido a las grandes dimensiones que estaba tomando. Los tres grupos de trabajo que inicialmente se formaron llegaron a conclusiones distintas, siendo finalmente el SNMP (RFC 1098) el adoptado, incluyendo éste

algunos de los aspectos más relevantes presentados por los otros dos: HEMS (Sistemas de Administración de Alto Nivel) y SGMP (Protocolo Simple de Monitoreo de Puerta de Enlace).

Para el protocolo SNMP la red constituye un conjunto de elementos básicos Administradores ubicados en el /los equipo /s de gestión de red y Gestores (elementos pasivos ubicados en los nodos host, routers, modems, multiplexores, etc.- a ser gestionados), siendo los segundos los que envían información a los primeros, relativa a los elementos gestionados, por iniciativa propia o al ser interrogados (polling) de manera secuencial, apoyándose en los parámetros contenidos en sus MIB (Base de Información de Administración). Su principal inconveniente es el exceso de tráfico que se genera, lo que lo puede hacer incompatible para entornos amplios de red.

Es un protocolo de administración distribuida. Un sistema puede operar exclusivamente como un NMS (Sistemas de Administración de Red) o como un agente, o bien puede realizar las funciones de ambos. Cuando un sistema opera tanto como NMS, y como un agente, otro NMS puede requerir que el sistema solicite dispositivos administrados y ofrezca un resumen de la información aprendida, o que reporte información de administración almacenada localmente.

Una red administrada por SNMP consta de tres componentes clave: dispositivos administrados, agentes y NMSs (Sistema de Administración de Red). Ver Figura 5.0

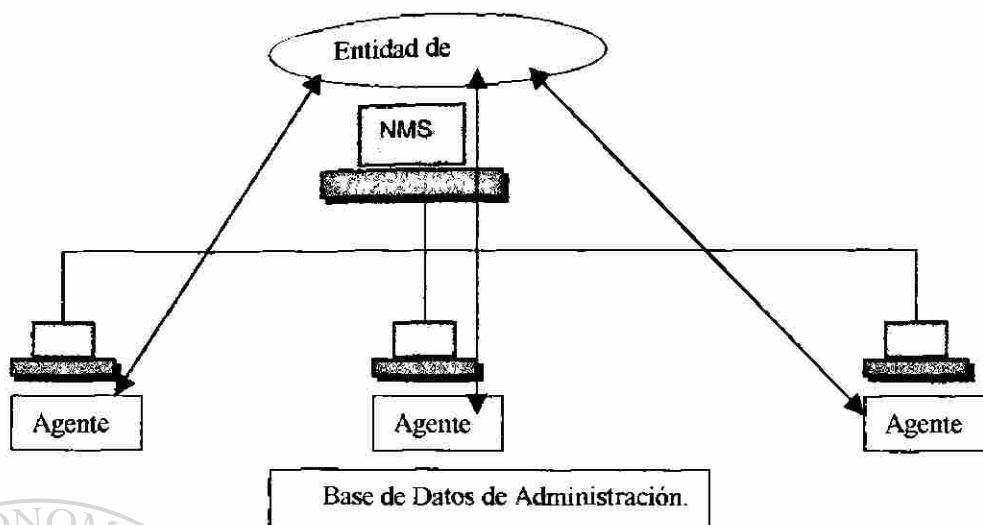


Fig. 5.0

Una red administrada por el protocolo SNMP consta de dispositivos administrados, agentes y NMSs.

Un dispositivo administrado es un nodo de la red que contiene un agente SNMP y reside en una red administrada. Los dispositivos administrados recaban y almacenan información de administración y proporcionan esta información a los NMSs por medio del SNMP. Los dispositivos administrados, a menudo llamados elementos de red, pueden ser ruteadores y servidores de acceso, conmutados y puentes, concentradores, hosts de computadora o impresoras.

Un agente es un módulo de software de administración de la red que reside en un dispositivo administrado. Un agente tiene un conocimiento local de la información de administración y traduce esa información para que sea compatible con el SNMP. Un NMS ejecuta aplicaciones que monitorean y controlan los dispositivos administrados. Los NMSs proporcionan el grueso de los recursos de procesamiento y memoria que se requieren para la administración de la red. Debe haber uno o más NMSs en cualquier red administrada.

Los dispositivos administrados se monitorean y controlan a través de cuatro comandos básicos de SNMP: lectura, escritura, captura y operaciones

transversales. NMS utiliza el comando de lectura para monitorear los dispositivos administrados. Examina diferentes variables que conservan los dispositivos administrados.

NMS utiliza el comando de escritura para controlar los dispositivos administrados. Asimismo, cambia los valores de las variables almacenadas en los dispositivos administrados. El comando de captura es utilizado por los dispositivos administrados para reportar eventos al NMS de manera asíncrona. Cuando se presenta determinado tipo de eventos, un dispositivo administrado envía una captura a NMS.

NMS utiliza las operaciones transversales para determinar que variables soporta un dispositivo administrado y reunir secuencialmente información en tablas de variables, como sería una tabla de ruteo.

5.9.1 Una Amplia Base de Información (MIB de SNMP).

A través del MIB se tiene acceso a la información para la gestión, contenida en la memoria interna del dispositivo en cuestión. Es la información organizada de manera jerárquica. Los MIBs se accesan por medio de un protocolo de administración de la red como SNMP. MIB es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos (información sobre variables/valores que se pueden adoptar), con identificadores exclusivos para cada objeto.

La arquitectura SNMP opera con un reducido grupo de objetos que se encuentran definido con detalle en la RFC 1066 "Base de información de gestión para la gestión de redes sobre TCP/IP". Un objeto administrado es una característica específica de un dispositivo administrado. Los Objetos administrados se componen de una o mas instancias de objetos, esencialmente variables.

Hay dos tipos de objetos administrados: escalares y tabulares. Los objetos escalares definen una sola instancia del objeto. Los objetos tabulares definen

múltiples instancias de objetos relacionados que están agrupados en tablas MIB.

Un ejemplo de objeto administrado es atInput, que es un objeto escalar que contiene una sola instancia de objetos, el valor entero que indica el total de paquetes AppleTalk de entrada en una interfase del ruteador.

Un identificador de objetos identifica de manera única un objeto administrado en la jerarquía del MIB. La jerarquía del MIB puede ser descrita como un árbol con una raíz sin nombre, cuyos niveles son asignados por diferentes organizaciones. Los Ids de Objetos de alto nivel en MIB pertenecen a las diferentes organizaciones de estándares, en tanto que los Ids de objetos de nivel inferior son asignados por organizaciones asociadas.

Los 8 grupos de objetos habitualmente manejados por MIB (MIB-I), que definen un total de 114 objetos (recientemente, con la introducción de MIB-II se definen hasta un total de 185 objetos), son:

- Sistema: Incluye la identidad del vendedor y el tiempo desde la última reinicialización del sistema de gestión.

- Interfaces: Un único o múltiples interfaces, local o remoto, etc.

- ATT (Tabla de Traducción de Direcciones): Contiene la dirección de la red y las equivalencias con las direcciones físicas.

- IP (Internet Protocolo): Proporciona las tablas de rutas, y mantiene estadísticas sobre los datagramas IP recibidos.

- ICMP (Internet Protocolo de Administración de Comunicación): Cuenta el número de mensajes ICMP recibidos y los errores.

- TCP (Protocolo De Control de Transmisión): Facilita información acerca de las conexiones TCP, retransmisiones, etc.

-UDP (Usuario Datagrama Protocolo): Cuenta el número de datagramas UDP, enviados, recibidos y entregados.

- EGP (Protocolo de Puerta de Enlace Externo): Recoge información sobre el número de mensajes EGP recibidos, generados, etc.

5.9.2 Administración de Sistemas Extendidos.

La versión 2 de SNMP aporta una serie de mejoras frente a la original, que, fundamentalmente, se manifiestan en tres áreas particulares: seguridad (autenticación, privacidad y control de accesos), transferencia de datos y comunicaciones Administrador a Administrador. SNMPv2 (SNMP Versión 2) es una evolución de la versión inicial SNMPv1. Se publicó en 1993 como un conjunto de estándares propuestos para Internet; actualmente, es un Borrador de Estándar. Igual que con SNMPv1, SNMPv2 funciona dentro de las especificaciones de SMI (Estructura de Administración de la Información). En teoría, SNMPv2 presenta muchas mejoras a SNMPv1, incluyendo operaciones adicionales del protocolo.

SMI define las reglas para describir la información de administración, utilizando ASN.1 SMI de SNMPv2 esta descrita en el RFC 1902. Incluye ciertas adiciones y mejoras a los tipos de datos específicos del SMI de SNMPv1, como la inclusión de cadenas de bits, direcciones de red y contadores. Las cadenas de bits se definen solamente en el SNMPv2 y comprenden cero o más bits nombrados que especifican un valor. Las direcciones de red representan una dirección de una familia de protocolos en particular. Los Contadores son enteros no negativos que se incrementan hasta que alcanzan un valor máximo y después regresan a cero.

SMI de SNMPv2 también especifica módulos de información que a su vez especifica un grupo de definiciones relacionadas. Hay tres tipos de módulos de información SMI: módulos MIB, declaraciones de cumplimiento y declaraciones de aptitud. Los módulos MIB contienen definiciones de objetos administrados interrelacionados. Las declaraciones de cumplimiento proveen una forma

-- sistemática de describir un grupo de objetos administrados que deben implementar para cumplir con un estándar. Las declaraciones de aptitud se utilizan para indicar el nivel preciso de soporte que un agente reclama con respecto a un grupo MIB. Un NMS puede ajustar su comportamiento hacia agentes de acuerdo con las declaraciones de aptitud asociadas con cada uno de ellos.

5.9.3 Tipos de Mensajes Entre Agentes y Administradores.

Los cinco tipos de mensajes SNMP intercambiados entre los Agentes y los Administradores, son:

- Get Request

Una petición del Administrador al Agente para que envíe los valores contenidos en el MIB (base de datos).

- Get Next Request

Una petición del Administrador al Agente para que envíe los valores contenidos en el MIB referente al objeto siguiente al especificado anteriormente.

- Get Response

La respuesta del Agente a la petición de información lanzada por el Administrador.

- Set Request

Una petición del Administrador al Agente para que cambie el valor contenido en el MIB referente a un determinado objeto.

- Trap

- Un mensaje espontáneo enviado por el Agente al Administrador, al detectar una condición predeterminada, como es la conexión / desconexión de una estación o una alarma.

El protocolo de gestión SNMP facilita, pues, de una manera simple y flexible el intercambio de información en forma estructurada y efectiva, proporcionando significantes beneficios para la gestión de redes multivendedor, aunque necesita de otras aplicaciones en el NMS que complementen sus funciones y que los dispositivos tengan un software Agente funcionando en todo momento y dediquen recursos a su ejecución y recogida de datos.

Las Operaciones Get, GetNext y Set que se utilizan en SNMPv1 son exactamente las mismas que se utilizan en SNMPv2. Sin embargo, SNMPv2 agrega y mejora algunas operaciones del protocolo. La operación Captura en SNMPv2, por ejemplo, cumple con la misma función que la utilizada en SNMP1. Sin embargo, utiliza un formato de mensaje diferente y esta diseñada para reemplazar la captura en SNMPv1. SNMPv2 también define dos nuevas operaciones del protocolo: GetBulk e Inform. Las operaciones GetBulk es utilizada por el NMS para acceder eficientemente grandes bloques de datos, como rengiones múltiples en una tabla. GetBulk llena un mensaje de respuesta con tantos datos solicitados como le quepan. La operaciones Inform permite que un NMS envíe información de captura a otro NMS y reciba una respuesta. En SNMPv2, si el agente que responde a las operaciones GetBulk no puede proporcionar valores para todas las variables en una lista, proporciona resultados parciales.

5.9.4 Factores de Seguridad en SNMP.

SNMP carece de alguna característica de autenticación, lo que la hace vulnerable a una gran variedad de amenazas relacionadas con la seguridad. Entre estas se cuentan la mascarada, la modificación de la información, las modificaciones de la secuencia de mensajes y de temporización y el destape. La mascarada consiste en una entidad no autorizada que trata de realizar

operaciones administrativas asumiendo la identidad de una entidad autorizada. La modificación de la información consiste en que una entidad no autorizada intenta alterar un mensaje generado por una entidad autorizada por lo que el mensaje provoca operaciones de administración de la contabilidad o de administración de la configuración no autorizadas. Las modificaciones de la secuencia de mensajes y de la temporización se presentan cuando una entidad no autorizada extrae los valores almacenados en objetos administrados o sabe de eventos notificables al monitorear los intercambios entre los gerentes y los agentes. Debido a que SNMP no implementa la función de autenticación, muchos fabricantes no implementan operaciones Set y así reducen SNMP a un equipo de monitoreo.

5.9.5 Formato del Mensaje De SNMPv2.

Los mensajes SNMPv2 constan de un encabezado y un PDU. La figura 5.1 muestra el formato básico de un mensaje SNMPv2.

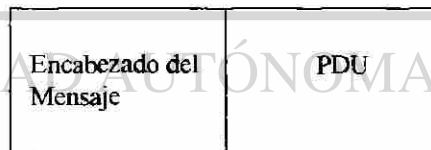


Fig. 5.1 Formato básico de un mensaje SNMPv2.

Encabezado del Mensaje en SNMPv2.

Los encabezados del mensaje en SNMPv2 constan de dos campos: Números de versión y Nombre de la comunidad. Las descripciones siguientes se refieren a estos campos.

Números de versión

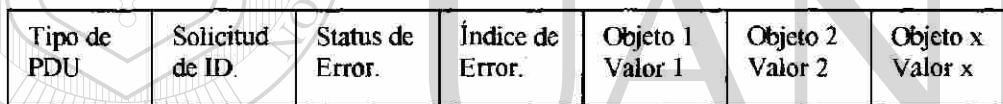
Especifica la versión de SNMP que se está utilizando.

Nombre de la comunidad

Define un ambiente de acceso para un grupo de NMSs. Se dice que los NMSs dentro de una comunidad existen dentro del mismo dominio administrativo. Los nombres de comunidad sirven como una forma vaga de autenticación ya que los dispositivos que no saben el nombre adecuado de la comunidad son eliminados de las operaciones en SNMP.

SNMPv2 especifica dos formatos de PDU, dependiendo de la operación del protocolo SNMP. Los campos PDU de SNMPv2 son de longitud variable, tal como los prescribe ASN.1 (Notación Sintáctica Abstracta Uno).

La figura 5.2 Muestra los campos de las PDUs Get, GetNext, Inform, Response, Set y Captura en SNMPv2.



Tipo de PDU	Solicitud de ID.	Status de Error.	Índice de Error.	Objeto 1 Valor 1	Objeto 2 Valor 2	Objeto x Valor x
-------------	------------------	------------------	------------------	------------------	------------------	------------------

Enlace de Variables

Fig. 5.2 Muestra las PDUs Get, GetNext, Inform, Response, Set y Trap en SNMPv2 consta de los mismos campos.

DIRECCIÓN GENERAL DE BIBLIOTECAS

- Tipo de PDU.- Identifica el tipo de PDU transmitido (Get, GetNext, Inform, Response, Set o Trap).
- Solicitud de ID.- Asocia las solicitudes de SNMP con respuestas.
- Status de Error. Indica uno de muchos errores y tipos de error. Solamente la operación respuesta activa este campo. Las demás operaciones fijan el valor de este campo en cero.
- Índice de Error.- Asocia un error con una instancia de objeto particular. Solamente la operación respuesta activa este campo. Las demás operaciones fijan el valor de este campo en cero.

- e) Enlaces de variables.- Sirven como el campo de datos del PDU en Snmpv2. Cada enlace de variable asocia una instancia de objeto particular con su valor actual.

5.9.6 Formato PDU GetBulk.

La Fig. 5.3 muestra los Campos de PDU GetBulk en SNMPv2.

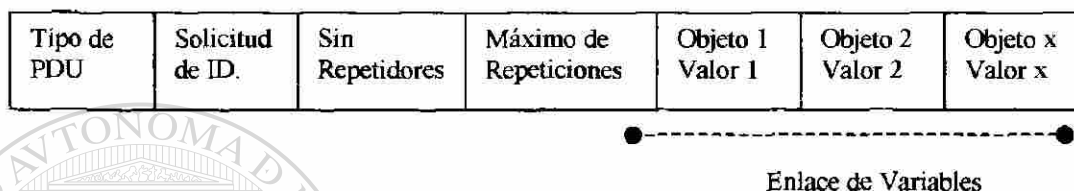


Fig. 5.3
PDU GetBulk en SNMPv2 consta de siete campos.

- a) Tipo de PDU.- Identifica la PDU como una operación GetBulk.
- b) Solicitud de ID.- Asocia las solicitudes de SNMP con respuestas.
- c) Sin Repetidores.- Especifica el numero de instancias del objeto en el campo de enlaces variables que se deben acceder no mas de una vez desde el comienzo de la solicitud. Este Campo se utiliza cuando algunas de las instancias son objetos escalares con una sola variable.
- d) Máximo de Repeticiones.- Define la cantidad máxima de veces que se deben acceder otras variables, que no sean las especificadas en el campo sin repetidores.
- e) Enlaces de Variables.- Sirve como el campo de datos de PDU en SNMPv2. Cada enlace de variables asocia una instancia de objeto particular con su valor actual (a excepción de las solicitudes Get y GetNext, para las cuales se ignora el valor).

5.9.7 Gestión a Distancia

Además de éstos, ciertos fabricantes están cooperando para el desarrollo de extensiones particulares para ciertas clases de productos y la gestión remota de dispositivos, conocidas como RMON (Monitor Remoto), normas RFC 1757 (antes 1271) para Ethernet y RFC 1513 para Token Ring del IETF (Fuerza de Trabajo de Ingeniería de Internet), que incluyen sobre unos 200 objetos clasificados en 9 grupos: Alarmas, Estadísticas, Historias, Filtros, Ordenadores, N Principales, Matriz de Tráfico, Captura de Paquetes y Sucesos. Con RMONv2 se decodifican paquetes a nivel 3 de OSI, lo que implica que el tráfico puede monitorizarse a nivel de direcciones de red (puertos de los dispositivos) y aplicaciones específicas.

RMON es una especificación de monitoreo estándar que permite que varios monitores de red y sistemas de consola intercambien datos sobre el monitoreo de la red. RMON ofrece a los administradores de red mayor libertad al seleccionar sensores y consolas para el monitoreo de red con características que satisfagan sus necesidades particulares de conectividad.

RMON define un conjunto de estadísticas y funciones que se pueden intercambiar entre los administradores de consola que cumplen con RMON y los sensores de red. Como tales, el RMON proporciona a los administradores de red información muy completa acerca del diagnóstico de fallas de red, planeación y puesta a tono del sistema. En la Figura 5.4 se muestra como sensor RMON puede enviar información estadística a una consola RMON.

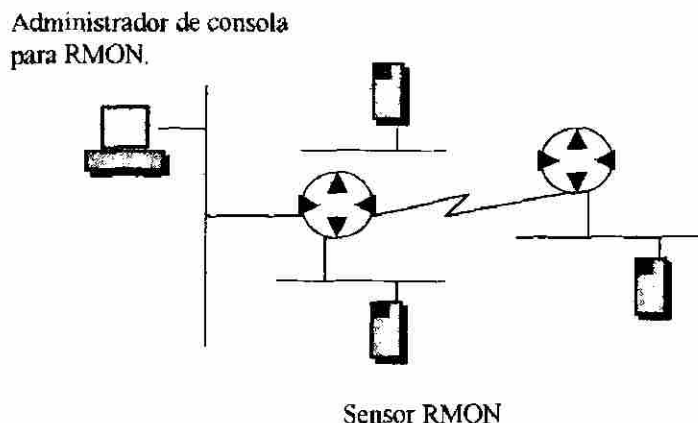


Fig. 5.4

Muestra un sensor RMON capaz de monitorear un segmento Ethernet y transmitir información estadística de regreso a la consola para RMON.

RMON define las funciones de supervisión de la red y los interfaces de comunicaciones entre la plataforma de gestión SNMP, los monitores remotos y los Agentes de supervisión que incorporan los dispositivos inteligentes. Entrega información en nueve grupos de elementos de monitoreo; cada uno de ellos proporciona conjuntos específicos de datos para cumplir con los requerimientos comunes de monitoreo de la red. Cada grupo es opcional, por lo que los proveedores no necesitan soportar todos los grupos dentro de una MIB. Algunos grupos rmon necesitan soporte de otros grupos rmon para funcionar adecuadamente, los nueve grupos de monitoreo especificados en el RFC 1757 Ethernet RMON MIB a continuación.

Alarmas:

Informa de cambios en las características de la red, basado en valores umbrales para cualquier variable MIB de interés. Permite que los usuarios configuren una alarma para cualquier Objeto gestionado. Cada cierto tiempo toma muestras estadísticas de las variables en el sensor y las compara con los niveles previamente configurados. Si la variable monitoreada cruza un umbral, se genera un evento.

Estadísticas:

Mantiene utilización de bajo nivel y estadísticas de error. Contiene estadísticas tomadas por el sensor de cada interfase monitoreada en este dispositivo.

Historias:

Analiza la tendencia, según instrucciones de los usuarios, basándose en la información que mantiene el grupo de estadísticas. Periódicamente toma muestras estadísticas de una red y las guarda para utilizarlas mas adelante.

Filtros:

Incluye una memoria para paquetes entrantes y un número cualquiera de filtros definidos por el usuario, para la captura selectiva de información; incluye las operaciones lógicas AND, OR y NOT. Permiten la comparación de los paquetes a una ecuación de filtro. Estos paquetes comparados forman una ráfaga de datos que se debe capturar o generar nuevos eventos.

Ordenadores:

Una tabla estadística basada en las direcciones MAC, que incluye información sobre los datos transmitidos y recibidos en cada ordenador.

Los N principales:

Contiene solamente estadísticas ordenadas de los "N" ordenadores definidos por el usuario, con lo que se evita recibir información que no es de utilidad.

Matriz de tráfico:

Proporciona información de errores y utilización de la red, en forma de una matriz basada en pares de direcciones, para correlacionar las conversaciones en los nodos más activos. Almacena estadísticas de conversaciones entre conjuntos de dos direcciones. A medida que el dispositivo detecta una nueva conversación, crea un nuevo parámetro en su tabla.

Captura de paquetes:

Permite definir buffers para la captura de paquetes que cumplen las condiciones de filtrado. Permite la captura de paquetes después de que han fluido a través de un canal.

Sucesos:

Registra tres tipos de sucesos basados en los umbrales definidos por el usuario: ascendente, descendente y acoplamiento de paquetes, pudiendo generar interrupciones para cada uno de ellos. Controla la generación y notificación de eventos de este dispositivo.

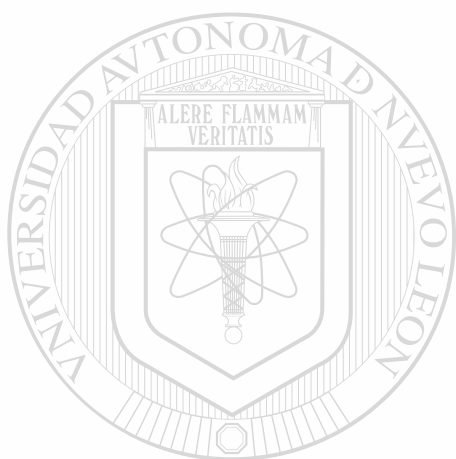
Hoy en día se utilizan cada vez más las LANs de alta velocidad y las interredes conmutadas, sobre todo porque operan a velocidades muy altas y soportan aplicaciones de gran ancho de banda como voz, video conferencias entre otras.

La tecnología de inter conectividad de redes surgió como una solución a tres problemas: LANs aisladas, duplicación de recursos y falta de administración de recursos. Las LANs aisladas imposibilitaban la comunicación electrónica entre diferentes oficinas o departamentos. La duplicación de recursos significaba que se debía suministrar el mismo hardware y software a cada departamento y oficina, así como tener grupos de soporte separados. Esta falta de administración de red provocó que no hubiera un método centralizado para administrar y reparar las redes. Esto es con el fin de definir algunos aspectos que sean corregido durante los últimos años.

Para la implementación de una red funcional se deben enfrentar muchos retos, sobre todo en las áreas de conectividad, confiabilidad, administración de redes y flexibilidad. Cada área es clave en el establecimiento de una red de comunicaciones eficientes y efectiva.

Al conectar varios sistemas es soportar la comunicación entre tecnologías diferentes ya que, por ejemplo, varios sitios pueden utilizar diferentes medios de transmisión con las características de acuerdo a sus necesidades particulares así como costos o bien operar a velocidades variables.

Toda red se debe tener siempre una atención esencial hacia la confiabilidad del servicio. Tanto usuarios individuales como organizaciones empresariales dependen del acceso constante y confiable a los recursos de la red.



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



DIRECCIÓN GENERAL DE BIBLIOTECAS

Capítulo 6

6.1 Conclusiones.

En el proceso del desarrollo e instrumentación de una red empresarial se encuentran diversos problemas técnicos y no técnicos que provocan fallas y retrasos. Estos pueden ser en diversas formas atribuidos a factores tales como: la ausencia de un plan ordenado de implantación, a una pobre definición de requerimientos, a un diseño erróneo, a la incapacidad de presentar adecuadamente el proyecto a la alta administración.

Si bien existen métodos claramente establecidos para el desarrollo de sistemas de software que son aplicados hoy por hoy en las empresas, es más raro encontrar un proceso similar para el desarrollo de sus sistemas de telecomunicación.

La capacidad de respuesta, el grado de conocimiento del personal de comunicaciones, las herramientas computacionales y sobre todo los procedimientos, son los factores de éxito en el desarrollo de proyectos en telecomunicaciones.

A nivel global se puede decir que las tecnologías usadas para interconectar diversas redes, es cada uno de estos enfoques tecnológicos tiene su campo de acción particular. Más que la superioridad de una u otra, una organización debe pesar todas las bondades que ofrecen cada una de ellas a los requerimientos y necesidades particulares que se tengan, y tomando en consideración igualmente aquellos esfuerzos de fabricantes y organismos de lograr cada vez una mayor compatibilidad entre estas tecnologías.

Algunos elementos claves para la selección de la tecnología de red serían: Costos de equipos, tanto de la parte de usuario como la de red. Este punto es considerado como la debilidad actual de algunas tecnologías, y que a pesar del desarrollo de interfaces y equipos compatibles con esta tecnologías, siguen siendo mas costosas que otras. El empleo de equipos existentes mediante cambios a nivel programación. Soporte, disponibilidad y compatibilidad de equipos ofrecidos por los diversos fabricantes.

Los avances en los sistemas multimedia distribuidos han tenido un significativo efecto en el desarrollo de servicios multimedia sobre demanda. El espectro del mundo computacional muestra a la multimedia, las comunicaciones y el "broadcasting" (envío de transmisiones a todas las direcciones de una red o subred) como áreas emergentes y de gran futuro.

La mayoría de los nuevos computadores son capaces de presentar y aceptar múltiples medios tales como imágenes, sonido, video, audio, texto y elementos gráficos. Esas nuevas potencialidades de las estaciones finales están cada vez mas en un excelente nivel costo-beneficio, lo cual anticipa el incremento de su interconexión como estaciones de multimedia. Muchos negocios y aplicaciones comerciales están siendo previstas para adoptar tales capacidades.

DIRECCIÓN GENERAL DE BIBLIOTECAS

6.2 Recomendaciones.

La información dentro de la empresa ha tenido siempre un lugar estratégico. Hace algunos años, la empresa mas competitiva era aquella que procesaba la mayor cantidad de información por unidad de tiempo. Actualmente, una empresa altamente competitiva es aquella que posee la información en el menor tiempo. Este concepto de posesión implica la compartición, el procesamiento y la transmisión de la información.

En los últimos cinco años hemos visto que la mayoría de las empresas en México han desarrollado rápidamente sus redes de empresa para atender una creciente demanda de comparación y procesamiento de información. La cantidad de elementos a conectar así como la diversidad de arquitecturas, protocolos, servicios, etc. Origina problemas metodológicos complejos para la realización de una red empresarial corporativa. Es necesario tomar en cuenta las necesidades de comunicación en constante evolución (voz, datos, textos, imagen, etc.) interesarse a las redes internas de cada sitio (PABX, LAN's) así como a los medios de comunicación entre esos sitios (WAN, VLANs) escoger entre las diferentes tecnologías y servicios de comunicación, hasta optimizar la estructura y dimensionamiento de las redes así definidas.

El responsable de llevar a cabo ese procedimiento en la empresa ve abrirse frente a el un horizonte aparentemente insondeable. El tiene la carga de aplicaciones tales como la voz, los datos, los textos, la imagen, etc. El se ocupa de la comunicación al interior de un edificio o campus así como de la comunicación externa con otros edificios o campus. El se enfrenta a la selección de tecnologías y servicios que aumenta día a día. Para poder atacar este problema complejo, se requiere de una formalización de los diferentes procedimientos que pueden ser empleados desde la planeación hasta la explotación de una red de comunicaciones.

La amplia experiencia acumulada en el dominio de la planeación y desarrollo de redes publicas de comunicación desgraciadamente no es directamente aplicable en una red de una empresa. Esto se debe a que las consideraciones son muy diferentes. Una red publica se planea considerando muchos utilizadores para un numero limitado de aplicaciones.

Al contrario, en una red privada existen relativamente pocos utilizadores para un numero elevado de aplicaciones. En consecuencia, aplicar los métodos y las técnicas clásicas seria completamente inadaptado. Entonces en el contexto actual en el que las redes de comunicación en la empresa toman un carácter estratégico, se hace necesario aplicar metodologías y herramientas informáticas practicas y eficaces para su implantación en la empresa. Algunos paquetes informaticos de análisis de redes se mencionan a continuación.

- a) **Comnet** : Análisis de desempeño, utilización de hardware.
- b) **Network**: Ejecución de software, tiempos de respuesta, tamaño de filas de espera.
- c) **Bones**: Análisis de desempeño, utilización de hardware, ejecución de software, tiempos de respuesta, tamaño de filas de espera.
- d) **Netool**: Desempeño, utilización, costos.
- e) **Opnet**: Análisis de desempeño, utilización de hardware, ejecución de software, tiempos de respuesta, tamaño de filas de espera.
- f) **Autonet**: Optimizacion de desempeño y de costos, costo de circuitos, análisis de desempeño, utilización de hw, ejecución de de software, tiempos de respuesta, tamaño de filas de espera.

En esta comunicación se presenta una proposición de metodología para llevar a cabo el proceso de planeación, análisis y diseño de una red privada. Todas las fases constituyentes del procedimiento están inscritas en un ciclo evolutivo de aprendizaje de utilización de la red privada.

BIBLIOGRAFÍA.

Autor: Merilee Ford, H. Kim Lew.

Título: Tecnologías de Interconectividad de Redes.

Editorial: Prentice Hall Hispanoamericana S.A.

Fecha de Edición: 1998.

Autor: Wayne Tomasi.

Título: Sistemas de Comunicaciones Electrónicas.

Editorial: Prentice Hall Hispanoamericana S.A.

Fecha de Edición: 1996.

Autor: A. Chianese , M De Santos.

Título: Methodology for LAN design.

Editorial: Computer Communications

Fecha de Edición: 1986.

Autor: Robert B. Walford.

Título: Information Networks, a design and implementation Methodology.

Editorial: Computer Communications

Fecha de Edición: 1986.

<http://www.iies.es/teleco/bit/bit102/quees.htm>

<http://www.iies.es/teleco/bit/bit102/sumario.htm>

<http://www.disc.ua.es/asignaturas/rc/trabajos/snmp/cuerpo.html>

LISTADO DE TABLAS Y FIGURAS.

	Paginas.
Tabla 2.0 Tipos de Hubs, los activos y los pasivos.	29
Tabla 2.1 Diferentes Alternativas para el Medio de Transmisión	36
Tabla 2.2 Características más Importantes de las Opciones 100BaseT.	40
Figura 2.1 Topología Bus.	34
Figura 2.2 Diagrama de Flujo del Control de Acceso al Medio CSMA/CD.	35
Figura 2.3 Topología en Estrella.	37
Figura 2.4 Topología en Cascada con Hubs.	38
Figura 2.5 Red Compartida vs. Red Conmutada.	41
Figura 2.6 Elementos Funcionales de la Tecnología Gigabit Ethernet.	45
Figura 2.7 Topología típica 10/100/100.	46
Figura 2.8 Actualización de Enlaces Conmutador-Servidor con GEN.	48
Figura 2.9 Actualizar Enlaces a Terminales de Alto Rendimiento.	48
Figura 2.10 Actualización de Troncales conmutadas a GEN.	49
Figura 5.0 Componente de una Red Administrada por SNMP.	100
Figura 5.1 Formato Básico de un Mensaje SNMPv2.	106
Figura 5.2 Los Campos PDU de SNMPv2	107
Figura 5.3 Muestra los Campos de PDU GetBulk en SNMPv2	108
Figura 5.4 Sensor RMON.	110

GLOSARIO

A

ACK Acknowledgment. Reconocimiento. Señal de respuesta.

ADSL Asymmetric Digital Subscriber Line. Línea Digital Asimétrica de Abonado. Sistema asimétrico de transmisión de datos sobre líneas telefónicas convencionales. Existen sistemas en funcionamiento que alcanzan velocidades de 1,5 y 6 Megabits por segundo en un sentido y entre 16 y 576 Kilobits en el otro.

ANSI American National Standard Institute. Instituto Nacional Americano de Estándar.

API Application Program Interface. Interfaz de Aplicación del Programa. Es el conjunto de rutinas del sistema que se pueden usar en un programa para la gestión de entrada / salida, gestión de ficheros etc.

ARPA Advanced Research Projects Agency. Agencia de Proyectos de Investigación Avanzada.

ARPANET Advanced Research Projects Agency Network. Red de la Agencia de Proyectos de Investigación Avanzada. Red militar Norteamericana a través de líneas telefónicas de la que posteriormente derivó Internet.

ASAP As Soon As Possible. Tan Pronto Como Sea Posible. Mandato u opción en una red o programa que determina la prioridad de una tarea.

ASCII. American Standard Code for Information Interchange. Estándar Americano para Intercambio de Información. La tabla básica de caracteres ASCII esta compuesta por 128 caracteres incluyendo símbolos y caracteres de control. Existe una versión extendida de 256

ASN Autonomous System Number. Número de sistema autónomo. Grupo de Routers y redes controlados por una única autoridad administrativa.

B

Backbone Estructura de transmisión de datos de una red o conjunto de ellas en Internet. Literalmente: "columna vertebral"

Bandwith Ancho de Banda. Capacidad de un medio de transmisión.

BBS Bulletin Board System. Tablero de Anuncios Electrónico. Servidor de comunicaciones que proporciona a los usuarios servicios variados como e-mail o transferencia de ficheros. Originalmente funcionaban a través de líneas telefónicas normales, en la actualidad se pueden encontrar también en Internet.

Baud Baudio. Unidad de medida. Número de cambios de estado de una señal por segundo.

BIOS Basic Input Output System. Sistema Básico de Entrada / salida. Programa residente normalmente en Eprom que controla la interacciones básicas entre el hardware y el Software.

BIT Binary Digit. Dígito Binario. Unidad mínima de información, puede tener dos estados "0" o "1".

BOOTP Bootstrap Protocol. Protocolo de Arranque-Asignación. Proporciona a una máquina una dirección IP, Gateway y Netmask. Usado en comunicaciones a través de línea telefónica.

BOT Automatismo, programa o script que realiza funciones que de otra manera habría que hacer de forma manual.

BPS Bits per second. Bits por segundo. Medida de la velocidad de transmisión de datos en la transmisión en serie.

Bridge. Puente. Dispositivo que interconecta redes de área local (LAN) en la capa de enlace de datos OSI. Filtra y retransmite tramas según las direcciones a Nivel MAC.

BUS. Vía o canal de Transmisión. Típicamente un BUS es una conexión eléctrica de uno o más conductores, en el cual todos los dispositivos ligados reciben simultáneamente todo lo que se transmite

C

Carrier Operator de Telefonía que proporciona conexión a Internet a alto nivel.

Caudal Cantidad de ocupación en un ancho de banda. Ejp. En una línea de 1Mbps. puede haber un caudal de 256Kbps. con lo que los 768Kbps. restantes del ancho de banda permanecen desocupados.

CCITT. International Consultative Committee on Telegraphy and Telephony. Comité Consultivo de Telegrafía y Telefonía. Organización que establece estándares internacionales sobre telecomunicaciones. Hoy ITU.

CDA. Communications Decency Act. Acta de decencia en las Telecomunicaciones. Proyecto de ley americano que pretendía ejercer una especie de censura sobre Internet. Por el momento ha sido declarado anticonstitucional.

CERN. Consejo Europeo para la Investigación Nuclear. Institución europea que desarrolló, para sus necesidades internas, el primer navegador y el primer servidor WWW. Y por tanto el HTTP. Ha contribuido decisivamente a la difusión de esta tecnología y es uno de los rectores del W3 Consortium

CERT. Computer Emergency Response Team. Equipo de Respuesta a Emergencias Informáticas.

CGI Common Gateway Interface. Interfaz de Acceso Común. Programas usados para hacer llamadas a rutinas o controlar otros programas o bases de datos desde una página Web. También pueden generar directamente HTML.

CIR Committed Information Rate. Es el Caudal mínimo de información que garantiza el operador telefónico al cliente (normalmente el proveedor de acceso) el resto del ancho de banda esta pues sujeto al estado de la red y las necesidades del operador telefónico.

CIX Comercial Internet Exchange. Intercambio Comercial Internet.

Connection Provider Proveedor de Conexión Entidad que proporciona y gestiona enlace físico a Internet

CSMA Carrier Sense Multiple Access. Acceso Múltiple por Detección de Portadora. Protocolo de Red para compartir un canal. Antes de transmitir la estación emisora comprueba si el canal esta libre.

CSMA/CD Carrier Sense Multiple Access / Collision Detection. Detección de portadora de acceso múltiple / colisión. En este protocolo las estaciones escucha al bus y sólo transmiten cuando el bus está desocupado. Si se produce una colisión el paquete es transmitido tras un intervalo (time-out) aleatorio.

D

DATAGRAM Datagrama. Usualmente se refiere a la estructura interna de un paquete de datos.

DCD Data Carrier Detected. Detectada Portadora de Datos.

DCE Data Communication Equipment. Equipo de Comunicación de Datos

DDE Dynamic Data Exchange. Intercambio Dinámico de Datos. Conjunto de especificaciones de Microsoft para el intercambio de datos y control de flujo entre aplicaciones.

DNS Domain Name System. Sistema de nombres de Dominio. Base de datos distribuida que gestiona la conversión de direcciones de Internet expresadas en lenguaje natural a una dirección numérica IP. Ejemplo: 121.120.10.1

Domain Dominio. Sistema de denominación de Hosts en Internet. Los dominios van separados por un punto y jerárquicamente están organizados de derecha a izquierda. ejp: mercadeo.com

DS-3. Digital Signal 3. Señal Digital Jerarquía 3 (45 Mbps para un T3).

DTE Data Terminal Equipment. Equipo Terminal de Datos. Se refiere por ejemplo al computador conectado a un modem que recibe datos de este.

DTMF Dual Tone Multifrequency. Multi frecuencia de doble tono. Son los tonos que se utilizan en telefonía para marcar un número telefónico.

DUPLEX Capacidad de un dispositivo para operar de dos maneras. En comunicaciones se refiere normalmente a la capacidad de un dispositivo para recibir/transmitir. Existen dos modalidades **HALF-DUPLEX**: Cuando puede recibir y transmitir alternativamente y **FULL-DUPLEX** cuando puede hacer ambas cosas simultáneamente.

EBCDIC Extended Binary Coded Decimal Interchange Code. Código Extendido de Binario Codificado Decimal. Sistema mejorado de empaquetamiento de números decimales en sistema binario.

EFF Electronic Frontier Foundation. Fundación Frontera Electrónica. Organización para la defensa de los derechos en el Ciberespacio. **E-mail** Electronic Mail. Correo Electrónico. Sistema de mensajería informática similar en muchos aspectos al correo ordinario pero muchísimo más rápido.

Ethernet. Diseño de red de área local normalizado como IEEE 802.3. Utiliza transmisión a 10 Mbps por un bus Coaxial. Método de acceso es CSMA/CD.

ETSI European Telecommunication Standard Institute. Instituto Europeo de Estándares en Telecomunicaciones.

DIRECCIÓN GENERAL DE BIBLIOTECAS

FAT File Allocation Table. Tabla de Localización de Ficheros. Sistema de organización de ficheros en discos duros. Muy usado en PC.

FDDI Fiber Digital Device Interface. Dispositivo Interface de Fibra (óptica) Digital.

Firewall. Cortina de Fuego. Router diseñado para proveer seguridad en la periferia de la red. Se trata de cualquier programa que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del firewall.

Frame. Estructura. También trama de datos. Grupo de bits transmitido de manera serial sobre un canal de comunicación. En Browsers de WWW como Netscape se refiere a una estructura de sub-ventanas dentro de un documento HTML.

Frame Relay. Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.

Full Duplex. Circuito o dispositivo que permite la transmisión en ambos sentidos simultáneamente.

G

Gateway. Pasarela. Puerta de Acceso. Dispositivo que permite conectar entre si dos redes normalmente de distinto protocolo o un Host a una red.

GT Global Time. Tiempo Global. Sistema horario de referencia en Internet.

H

Half Duplex. Un circuito que permite de manera alternante la transmisión y la recepción de señales, pero no de manera simultánea.

HDLC High-Level Data Link Control. Control de Enlace de Datos de Alto Nivel. Es un protocolo orientado al bit.

HDSL High bit rate Digital Subscriber Line. Línea Digital de Abonado de alta velocidad. Sistema de transmisión de datos de alta velocidad que utiliza dos pares trenzados. Se consiguen velocidades superiores al Megabit en ambos sentidos.

Header Cabecera. Primera parte de un paquete de datos que contiene información sobre las características de este.

Hit. Se usa para referirse a cada vez que un link es pulsado en una página WEB. Literalmente "golpe".

Host. Anfitrión. Computador conectado a Internet. Computador en general.

HPFS High Performance File System. Sistema de Archivos de Alto Rendimiento. Sistema que utiliza el OS/2 opcionalmente para organizar el disco duro en lugar del habitual de FAT.

HTML HyperText Markup Language. Lenguaje de Marcas de Hipertexto. Lenguaje para elaborar páginas Web actualmente se encuentra en su versión 3. Fue desarrollado en el CERN.

HTTP HyperText Transfer Protocol. Protocolo de Transferencia de Hipertexto. Protocolo usado en WWW.

I

IANA Internet Assigned Number Authority. Autoridad de Asignación de Números en Internet. Se trata de la entidad que gestiona la asignación de direcciones IP en Internet.

IEEE Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos. Asociación Norteamericana. IEEE 802.3 Protocolo para la red LAN de la IEEE que especifica una implementación del nivel físico y de la subcapa MAC, en la capa de enlace de datos. El IEEE 802.3 utiliza CSMA/CD a una variedad de velocidades de acceso sobre una variedad de medios físicos. Extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet.

IETF Internet Engineering Task Force. Grupo de Tareas de Ingeniería de Internet. Asociación de técnicos que organizan las tareas de ingeniería principalmente de telecomunicaciones en Internet. Por ejemplo: mejorar protocolos o declarar obsoletos otros.

INTERNET. Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funciona como una sola gran red.

INTERNIC Entidad administrativa de Internet que se encarga de gestionar los nombres de dominio en EEUU.

INTRANET Se llaman así a las redes tipo Internet pero que son de uso interno, por ejemplo, la red corporativa de una empresa que utilizara protocolo TCP/IP y servicios similares como WWW. IP Internet Protocol. Protocolo de Internet. Bajo este se agrupan los protocolos de Internet. También se refiere a las direcciones de red Internet.

IPI Intelligent Peripheral Interface. Interface Inteligente de Periféricos. En ATM: Initial Protocol Identifier. Identificador Inicial de Protocolo.

IPX Internet Packet Exchange. Intercambio de Paquetes entre Redes. Inicialmente protocolo de Novell para el intercambio de información entre aplicaciones en una red Netware.

IRC Internet Relay Chat. Canal de Chat de Internet. Sistema para transmisión de texto multiusuario a través de un servidor IRC. Usado normalmente para conversar on-line también sirve para transmitir ficheros.

ISDN Integrated Services Digital Network. Red Digital de Servicios Integrados. Servicio provisto por una empresa de comunicaciones que permite transmitir simultáneamente diversos tipos de datos digitales conmutados y voz.

ISO International Standard Organization. Organización Internacional de Estándares.

ITU International Telecommunications Union. Unión Internacional de Telecomunicaciones. Forma parte de la CCITT. Organización que desarrolla estándares a nivel mundial para la tecnología de las telecomunicaciones.

L

LAN Local Area Network. Red de Área Local. Una red de área local es un sistema de comunicación de alta velocidad de transmisión. Estos sistemas están diseñados para permitir la comunicación y transmisión de datos entre estaciones de trabajo inteligentes, comúnmente conocidas como Computadoras Personales. Todas las PCs, conectadas a una red local, pueden enviar y recibir información. Como su mismo nombre lo indica, una red local es un sistema que cubre distancias cortas. Una red local se limita a una planta o un edificio.

M

MAC Media Access Control. Control de Acceso a Medio. Protocolo que define las condiciones en las cuales las estaciones de trabajo acceden al medio. su uso está difundido en las LAN. En las LAN tipo IEEE la capa MAC es la subcapa más baja del protocolo de la capa de enlace de datos.

MAN Metropolitan Area Network. Red de Área Metropolitana.

MRU Maximum Receive Unit. Unidad Máxima de Recepción. En algunos protocolos de Internet se refiere al máximo tamaño del paquete de datos.

MTU Maximum Transmission Unit. Unidad Máxima de Transmisión. Tamaño máximo de paquete en protocolos IP como el SLIP.

MULTICASTING Técnica de transmisión de datos a través de Internet en la que se envían paquetes desde un punto a varios simultáneamente.

N

NACR Network Announcement Request. Petición de participación en la Red. Es la petición de alta en Internet para una sub red o dominio.

NAP Network Access Point. Punto de Acceso a la Red. Normalmente se refiere a los tres puntos principales por los que se accede a la red Internet en U.S.

NC Network Computer. Computador de Red. Computador concebido para funcionar conectado a Internet. Según muchos el futuro. Se trata de equipos de hardware muy reducido (algunos no tienen ni disco duro).

NCP Network Control Protocol. Protocolo de Control de Red. Es un protocolo del Network Layer

NETBIOS Network BIOS. Network Basic Input/Output System. Bios de una red, es decir, Sistema Básico de Entrada / salida de red.

• **Nodo** Por definición punto donde convergen más de dos líneas. A veces se refiere a una única máquina en Internet. Normalmente se refiere a un punto de confluencia en una red. Punto de interconexión a una RED.

NSA National Security Agency. Agencia Nacional de Seguridad. Organismo americano para la seguridad entre otras asuntos relacionados con la informática.

○

OS2 Operating System 2. Sistema operativo de 32 bits multitarea creado por IBM. Creado para PC con entorno gráfico de usuario. La versión actual es la 4 la cual soporta ordenes habladas y dictado.

OSI Open Systems Interconnection. Interconexión de Sistemas Abiertos. Modelo de referencia de interconexión de sistemas abiertos propuesto por la ISO. Divide las tareas de la red en siete niveles

Packet Driver Pequeño programa situado entre la tarjeta de red y el programa de TCP de manera que proporciona un interfaz estándar que los programas pueden usar como si de un driver se tratase.

Packet Paquete Cantidad mínima de datos que se transmite en una red o entre dispositivos. Tiene una estructura y longitud distinta según el protocolo al que pertenezca. También llamado TRAMA.

PAN Personal Area Network. Red de Área Personal. Sistema de red conectado directamente a la piel. La transmisión de datos se realiza por contacto físico.

PAP Password Authentication Protocol. Protocolo de Autenticación por Password. Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante password.

PBX Private Branch Exchange. Central Privada

PEER En una conexión punto a punto se refiere a cada uno de los extremos.

PING Packet Internet Groper. Rastreador de Paquetes Internet. Programa utilizado para comprobar si un Host está disponible. Envía paquetes de control para comprobar si el anfitrión está activo y los devuelve.

PPP Point to Point Protocol. Protocolo Punto a Punto. Un sucesor del SLIP. El PPP provee las conexiones sobre los circuitos síncronos o asíncronos, entre router y router, o entre host y la red. Protocolo Internet para establecer enlace entre dos puntos.

PROXY. Servidor Caché. El Proxy es un servidor de que conectado normalmente al servidor de acceso a la WWW de un proveedor de acceso va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.

PVC Permanent Virtual Circuit. Circuito Virtual Permanente. Línea punto a punto virtual establecida normalmente mediante conmutaciones de carácter permanente. Es decir a través de un circuito establecido.

Q

QAM Quadrature Amplitude Modulation. Modulación de Amplitud en Cuadratura. Sistema de modulación para transmisión de datos y telecomunicaciones.

S

SDH Synchronous Digital Hierarchy. Estándar Europeo que define un grupo de formato que son transmitidos usando señalización óptica sobre fibra. El SDH es similar al SONET, con un rango básico de 155.52 Mbps, diseñado para viajar a STM-1.

SDLC Synchronous Data Link Controller. Controlador de Enlace de Datos Síncrono. También se trata de un protocolo para enlace síncrono a través de línea telefónica. Protocolo propietario de IBM orientado al bit.

SDSL Symmetric Digital Subscriber Line. Línea Digital Simétrica de Abonado. Sistema de transferencia de datos de alta velocidad en líneas telefónicas normales.

SLIP Serial Line Internet Protocol. Protocolo Internet en Línea Serial. Protocolo, antecesor del PPP, que permite establecer conexiones TCP/IP a través de enlaces seriales.

SNA System Network Architecture. Arquitectura de Sistemas de Redes. Arquitectura de red exclusiva de IBM. Principalmente orientada a Mainframes.

SQL Structured Query Language. Lenguaje de Petición Estructurada. Lenguaje para base de datos.

T

T1 Velocidad de transmisión a nivel WAN. Puede transportar datos a una velocidad de 1.54 Mbps a través de una red telefónica.

T3 Velocidad de transmisión a nivel WAN. Puede transportar datos a una velocidad de 44.7 Mbps a través de una red telefónica.

TCP/IP Transmission Control Protocol / Internet Protocol. Protocolo de Control de Transmisión / Protocolo Internet. Nombre común para una serie de protocolos desarrollados por DARPA en los Estados Unidos en los años 70, para dar soporte a la construcción de redes interconectadas a nivel mundial. TCP corresponde a la capa (layer) de transporte del model OSI y ofrece transmisión de datos. El IP corresponde a la capa de red y ofrece servicios de datagramas sin conexión. Su principal característica es comunicar sistemas diferentes. Fueron diseñados inicialmente para ambiente Unix por Victor G. Cerf y Robert E. Kahn. El TCP / IP son básicamente dos de los mejores protocolos conocidos.

TELNET Protocolo y aplicaciones que permiten conexión como terminal remota a una computadora anfitriona, en una localización remota.

Time-out Parámetro que indica a un programa el tiempo máximo de espera antes de abortar una tarea o función. También mensaje de error.

Tunneling Transporte de paquetes Multicast a través de dispositivos y Routers unicast. Los paquetes multicast se encuentran encapsulados como paquetes normales de esta manera pueden viajar por Internet a través de dispositivos que solo soportan protocolos unicast.

U

UDP User Datagram Protocol. Protocolo de Datagrama de Usuario. Protocolo abierto en el que el usuario (programador) define su propio tipo de paquete.

UNIX Sistema operativo multitarea, multiusuario. Gran parte de las características de otros sistemas más conocidos como MS-DOS están basadas en este sistema muy extendido para grandes servidores. Internet no se puede comprender en su totalidad sin conocer el Unix, ya que las comunicaciones son una parte fundamental en Unix.

URL Uniform Resource Locator. Localizador Uniforme de Recursos. Denominación que no solo representa una dirección de Internet sino que apunta aun recurso concreto dentro de esa dirección.

UUCP Unix to Unix Communication Protocol. Protocolo de Comunicaciones de Unix a Unix. Uno de los protocolos que utilizan los sistemas Unix para comunicarse entre si.

W

WAIS Wide Área Information Server Servidores de Información de Área Amplia. Sistema de obtención de información patrocinado por Apple, Thinking Machines y Dow Jones.

WAN Wide Area Network. Red de Área Ancha.

WWW, WEB o W3 World Wide Web. Telaraña mundial. Sistema de arquitectura cliente-servidor para distribución y obtención de información en Internet, basado en hipertexto e hipermedia. Fue creado en el Laboratorio de Física de Energía Nuclear del CERN, en Suiza, en 1991 y ha sido el elemento clave en el desarrollo y masificación del uso de Internet.

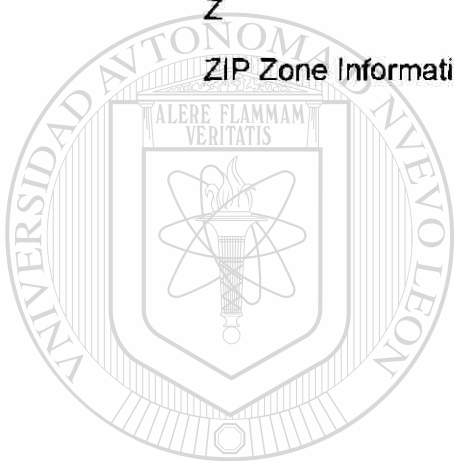
X

X Window System. Sistema de Ventanas X. El sistema de Ventanas X permite que cada ventana se conecte con una computadora remota.

X.25 Protocolo de transmisión de datos. Establece circuitos virtuales, enlaces y canales. Es una tecnología antigua de red usada en Europa.

Z

ZIP Zone Information Protocol. Protocolo de Información de Zona.



UANL

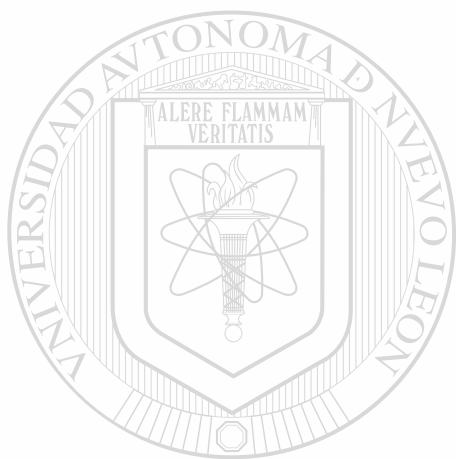
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

®

DIRECCIÓN GENERAL DE BIBLIOTECAS

RESUMEN AUTOBIOGRÁFICO.

El grado que se desea obtener es Maestro en Ciencias de la Ingeniería Con Especialidad en Telecomunicaciones. La tesis lleva por título "Tecnologías e Interconexión de Redes de Telecomunicaciones", el campo profesional las telecomunicaciones, Nací en el Poblado El Limón Tamaulipas el 13 de Abril de 1975. Mi Madre la Sra. Sanjuana Ramírez Rodríguez, me gradué de la Facultad de Ingeniería Mecánica y Eléctrica perteneciente a la Universidad Autónoma de Nuevo León en la que obtuve el título de Ingeniero en Electrónica y Comunicaciones.



UANL

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



DIRECCIÓN GENERAL DE BIBLIOTECAS

