

**DISEÑO Y ARQUITECTURA DE REDES ENFOCADO EN LA
ÍTERCONECTIVIDAD DE REDES**

**CÉSAR AUGUSTO GAVIRIA HERRERA
LUZ MARIA GUERRERO MERCADO**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
INGENIERÍA DE SISTEMAS
CARTAGENA – COLOMBIA
2008**

**DISEÑO Y ARQUITECTURA DE REDES ENFOCADO EN LA
ÍTERCONECTIVIDAD DE REDES**

**CÉSAR AUGUSTO GAVIRIA HERRERA
LUZ MARIA GUERRERO MERCADO**

**Monografía presentada como requisito para optar el título de
Ingenieros de sistemas**

**Director
ISAAC ZUÑIGA SILGADO**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
INGENIERÍA DE SISTEMAS
CARTAGENA – COLOMBIA
2008**

Nota de aceptación

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Cartagena D.T.y C. Julio de 2008

DEDICATORIA

A Dios por darme el regalo más preciado del mundo ¡la vida! Y la oportunidad de vencer los obstáculos que en el camino se me han presentado, pero que gracias a él he logrado afrontarlos con valentía para hoy llegar a cumplir una de mis metas.

A mi madre por su apoyo económico y por traerme al mundo y permitirme llegar hasta donde estoy.

A mis hermanos por su apoyo moral e incondicional.

A mis abuelos por sus sabios consejos y por su valioso amor y ternura.

A mis profesores por su educación brindada, porque me regalaron cada uno de sus conocimientos y por educarme en valores humanos y enseñarme cada una de las teorías de esta profesión.

A mis familiares, amigos y a todo el que hizo posible mi educación en valores y moral, con los que un hombre puede contar en la vida para ser útil a sí misma, y lo más importante a la sociedad.

¡Gracias!

CÉSAR GAVIRIA HERRERA

DEDICATORIA

Desde el inicio de mi carrera al orar con Dios, le dije que le dedicaba mis títulos por que gracias a Él he alcanzado una de mis grandes metas, mi título como profesional. Realizando esta dedicatoria vino a mí una cita bíblica que dice:

“Acuérdate de tu Creador en los días de tu juventud, antes que vengan los días malos, y lleguen los años de los cuales digas: No tengo en ellos contentamiento”. Eclesiastés 12: 1

En efecto Dios tiene que ser lo primordial en la vida de cada quien y así alcanzaremos nuestras metas, y podamos alcanzar los objetivos propuestos, como dice su palabra apartados de él no podemos hacer nada.

E igualmente con el mismo amor y pasión le doy gracias a mis padres por el esfuerzo tan enorme que hicieron por mí, al darme estudios y preocuparse por mi bienestar y futuro; su apoyo fue incondicional como lo manifiesta el verdadero amor de padres. A Mi hermano gracias por su apoyo se que a pesar de su extraña personalidad me quiere y desea lo mejor para mí.

Luz María Guerrero Mercado

AGRADECIMIENTOS

Agradecemos sinceramente:

A nuestro director Isaac Zúñiga Silgado, por la orientación brindada durante la investigación y poder llevar a cabo esta monografía.

A todos los docentes del Minor y a la institución, por brindarnos las herramientas de apoyo necesario para el desarrollo académico e investigativo.

A todos los profesores que tuvimos durante los estudios universitarios mil gracias.

Cartagena D.T.y C. Julio de 2008

Señores:

COMITÉ DE EVALUACIÓN DE PROYECTOS

Programa de Ingeniería de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

La ciudad

Respetados señores:

Con la atención nos dirigimos a ustedes con el fin de presentarles a su consideración, estudio y aprobación la monografía titulada **DISEÑO Y ARQUITECTURA DE REDES ENFOCADO EN LA ÍNTERCONNECTIVIDAD DE REDES** como requisito parcial para optar el título de Ingenieros de sistemas.

Atentamente,

CÉSAR GAVIRIA HERRERA

C.C: 8.648.586

LUZ MARIA GUERRERO

C.C: 1047.368.220

Cartagena D.T.y C. Julio de 2008

Señores:

Comité Facultad de Ingeniería de Sistemas
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
La ciudad

Respetados señores:

A través de la presente me permito entregar la monografía titulada **DISEÑO Y ARQUITECTURA DE REDES ENFOCADO EN LA ÍNTERCONNECTIVIDAD DE REDES** para su estudio y evaluación, la cual fue realizada por los estudiantes CÉSAR AUGUSTO GAVIRIA HERRERA y LUZ MARIA GUERRERO MERCADO.

Como director de la monografía considero que el trabajo es satisfactorio y amerita ser presentado para su evaluación.

Atentamente,

ISAAC ZUÑIGA SILGADO
Ingeniero de Sistemas

Cartagena D.T.y C. Julio de 2008

Señores:

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

Comité de Evaluación de Proyectos

Ciudad

Estimados señores

Con el mayor agrado me dirijo a ustedes para poner a consideración la monografía titula **DISEÑO Y ARQUITECTURA DE REDES ENFOCADO EN LA INTERCONECTIVIDAD DE REDES**. La cual fué llevada a cabo por los estudiantes CÉSAR AUGUSTO GAVIRIA HERRERA y LUZ MARIA GUERRERO MERCADO, bajo mi orientación como asesor.

Agradeciendo su amable atención.

Atentamente,

ISAAC ZUÑIGA SILGADO
Ingeniero de Sistemas

AUTORIZACIÓN

Cartagena D.T.y C. Julio de 2008

Yo **CÉSAR AUGUSTO GAVIRIA HERRERA**, identificado con cédula de ciudadanía 8.648.586 de Sabanalarga Atlántico, autorizo a la universidad Tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catalogo online de la biblioteca.

CÉSAR AUGUSTO GAVIRIA HERRERA
C.C: 8.648.586

AUTORIZACIÓN

Cartagena D.T.y C. Julio de 2008

Yo **LUZ MARIA GUERRERO MERCADO**, identificada con cédula de ciudadanía 1047.368.220 de Cartagena, autorizo a la universidad Tecnológica de Bolívar, para hacer uso de mi trabajo de monografía y publicarlo en el catalogo online de la biblioteca.

LUZ MARIA GUERRERO MERCADO

C.C: 1047.368.220

BREVE DESCRIPCION DEL PROBLEMA

Las redes han experimentado un importante auge en los últimos años debido a la aparición de nuevos dispositivos, tecnologías, medios de transmisión (cableado) que han hecho que las redes tengan un buen funcionamiento. Sin embargo algunas empresas todavía presentan un mal funcionamiento en las redes esto se debe de pronto a que no están utilizando los dispositivos apropiados o no cuentan con un presupuesto para tener un diseño óptimo.

Teniendo en cuenta cada uno de los dispositivos que hacen parte del diseño y arquitectura de red, y la mala organización y utilización de estos en algunas organizaciones; nace la necesidad de saber como está constituida la arquitectura y los elementos que hacen parte del diseño de la misma. Es por eso que esta investigación se enfocará en la interconexión de las redes. Además los dispositivos y tipos de Interconexión que existen.

La ínterconectividad de redes es importante para compartir recursos y tener acceso a las base de datos compartidas en forma casi instantánea, además de permitir al administrador de la red una administración de la misma en forma centralizada. Si una empresa trabaja con una red, ésta reducirá sus costos de presupuesto en tiempo y en dinero.

JUSTIFICACIÓN

La razón principal por la cual se realizará esta monografía es para dar a conocer los diferentes factores que intervienen en el funcionamiento y arquitectura de una red, por lo que se realizará una explicación de aspectos determinantes y útiles al momento de pensar en la realización del diseño de la red de diferentes organizaciones, con la finalidad de optimizar, garantizar escalabilizar y reducir costos, para aquellas empresas o instituciones que desean tener un buen funcionamiento en la red pero que no cuentan con un presupuesto o con los recursos para el buen funcionamiento de esta. Así mismo dar a conocer algunas generalidades de la interconectividad de las redes.

OBJETIVOS

GENERAL

Dar a conocer los diferentes elementos que intervienen en la interconexión de redes para el buen desarrollo de un diseño de red, con el fin de obtener una estructura óptima.

ESPECIFICOS

- ✓ Dar a conocer algunas generalidades de la interconectividad de redes (Modelo OSI, topologías, medios de transmisión, estándar Ethernet entre otros)
- ✓ Dar a conocer el proceso evolutivo de la interconectividad, el reto al conectar varios sistemas de comunicación entre tecnologías diferentes, y los tipos de interconexión de redes. Así mismo los dispositivos de interconexión.
- ✓ Describir como se transfiere la información a través de una red desde un origen hasta un destino, es decir; todo lo concerniente al ruteo, protocolos de red y de ruteo, algoritmos entre otros
- ✓ Describir de manera concisa los pasos a seguir para la realización del diseño de una red, teniendo en cuenta que cada una de ellas presenta su propia estructura. Además mostrar algunos casos prácticos, donde se observe la interconectividad de las redes.

RESUMEN

Los desarrollos tecnológicos y las siempre cambiantes realidades de las organizaciones se han convertido en agentes que han obligado a los diseñadores a optimizar la estructura de la red. El incremento en el número de usuarios y en el número de aplicaciones que utilizan la red incrementó el tráfico a volúmenes nunca antes previstos, se hizo entonces necesario concebir su estructura como una estructura jerárquica, con diferentes requerimientos de capacidad y desempeño en cada nivel, y obligó a entender su diseño como un proceso. Por lo que en este documento se presentará la evolución que ha tenido la arquitectura de una red para responder a los frecuentes cambios a los que se ven expuestas las organizaciones en las que existen.

Teniendo en cuenta cada uno de los dispositivos que hacen parte del diseño y arquitectura de red, y la mala organización y utilización de estos en algunas organizaciones; nace la necesidad de saber como está constituida la arquitectura y los elementos que hacen parte del diseño de la misma. Es por eso que esta investigación se enfocará en la interconexión de las redes.

Esta monografía es de cobertura local y geográfica; puesto que está compuesta por las redes de interconexión LAN, y WAN. Además este documento puede ir dirigido a cualquier empresa que posea una red, porque se darán a conocer los diferentes tipos de dispositivos de interconexión de redes, tomando como ejemplo el diseño de red de algunas organizaciones, las cuales serian muy útiles para las empresas que lo deseen poner en práctica.

En el primer capítulo se hace referencia a la arquitectura de red como tal; que es el medio más efectivo en cuanto a costos para desarrollar e implementar un conjunto de dispositivos que se puedan interconectar, dentro de las características de la arquitectura se encuentran la amplia conectividad, la administración de la

red, puesto que dentro de la arquitectura se debe permitir que el usuario defina, opere, cambie, proteja y de mantenimiento a la red, además debe ser de facilidad de uso, ya que mediante la arquitectura de red los diseñadores pueden centrar su atención en las interfaces primarias de la red y por tanto hacerlas amigables para el usuario. Por otra parte, uno de los pasos más importantes para el diseño y arquitectura de una red es la topología a utilizar, la topología es un mapa en donde se identifican segmentos, puntos de interconexión y los usuarios que van a estar en la red; actualmente se están utilizando mucho la topología en estrella y las topologías jerárquicas. Además se hizo referencia al modelo OSI; este es una propuesta que desarrolló la organización internacional de normas, la cual logró la estandarización internacional que se usan en las diferentes capas de este modelo y que permite llevar a cabo un diseño y arquitectura de una red orientada a interconexión de la misma; y está compuesta por siete capas.

Por otro lado, la tecnología de interconectividad de redes surgió como una solución a tres problemas: LANs aisladas, duplicación de recursos y falta de administración de recursos. Las LANs aisladas imposibilitan 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 separar las redes.

El termino “Internetworking” hace referencia a todo proceso de interconexión entre redes, de igual o diferente estructura, como las redes de área local (LANs) o redes de área extensa (WANs). Los diferentes equipos de interconexión facilitan el proceso de conectar equipos, sistemas, y/o redes no solo de un único proveedor, sino de múltiples proveedores entre si. El objetivo principal de la interconexión de redes es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Asimismo

algunas de las ventajas que plantea la interconexión de redes de datos son: compartición de recursos dispersos, coordinación de tareas de diversos grupos de trabajo, reducción de costos, al utilizar recursos de otras redes, aumento de la cobertura geográfica. Además en la interconectividad de redes se presentan los siguientes retos técnicos: equipos de diferentes fabricantes, arquitecturas, plataformas, sistemas operativos, protocolos, medios de comunicación diferentes, limitaciones en distancia y en tamaño de los paquetes, y además limitaciones en ancho de banda y potencia.

En esta investigación no solo se tendrá en cuenta la parte física de la red (Arquitectura) sino también la parte lógica; es decir, como es el proceso de transferencia de la información a través de una red desde un origen hasta un destino; es decir, algunos conceptos como: ruteo, protocolos de red y de ruteo, algoritmos de ruteo, métricas de ruteo, entre otros.

Por otra parte; para lograr crear un buen diseño es necesario tener en cuenta en primera instancia la lógica del negocio, es decir, la forma como se aproveche cada dispositivo de interconexión, medios de transmisión y otros elementos que hacen parte de la arquitectura de la red. Para luego establecer el tipo de topología a emplear. Puesto que un buen diseño de red es fundamental para evitar problemas de pérdidas de información, caídas continuas de la red, problemas de lentitud en el procesamiento de la información y problemas de seguridad informática. Asimismo al momento que sea necesario optimizar una red la cual se quiere que sea de alto rendimiento y de baja latencia, se debe tener conocimiento de ciertos temas para que la arquitectura de red se construya con éxito y que el cliente final como tal quede con total satisfacción del diseño de red entregado. Para lo cual es necesario conocer como actúan los dispositivos de interconexión, medios de transmisión, el modelo sobre el cual se piensa diseñar, los costos, la distancia geográfica, lo que se puede reutilizar etc.

En conclusión en este documento se logró el objetivo general que era dar a conocer los diferentes elementos que intervienen en la interconexión de redes para el buen desarrollo de un diseño de red, con el fin de obtener una estructura óptima.

Aunque este documento tiene un contenido bastante fructífero se puede complementar un poco más acerca de los dispositivos de interconexión de redes puesto que estos se encuentran en constantes cambios, por lo que tanto proveedores de servicios de Internet o cualquier servicio de montaje de una red, profesionales dedicados a la administración de una red o cualquier persona que necesita estar continuamente actualizado para lograr con éxito su trabajo necesita estar informado acerca de las últimas tendencias de las tecnologías que existan.

TABLA DE CONTENIDO

	Pág.
LISTA DE FIGURAS	22
INTRODUCCIÓN	23
CAPITULO I	
1. ASPECTOS GENERALES DE LA ÍNTERCONNECTIVIDAD DE REDES	24
1.1 Antecedentes del diseño y arquitectura de redes	24
1.2 Topologías de red	26
1.3 Modelo de referencia OSI	28
1.3.1 Medios de transmisión	30
1.3.1.1 Medios de transmisión guiados	30
1.3.1.2 Medios de transmisión no guiados	32
1.3.2 Estándar Ethernet	33
1.3.3 Retos tecnológicos en la interconectividad de las redes	35
CAPITULO II	
2. INTERCONNECTIVIDAD DE REDES	36
2.1 Historia de la interconectividad de redes	36
2.2 Dispositivos de interconexión de redes	37
2.2.1 Evolución de los Repetidores	37
2.2.2 Evolución de los Hubs	39
2.2.3 Evolución de los Puentes	42
2.2.4 Evolución de los Switches	43
2.2.5 Evolución de los Routers	46
2.2.6 Evolución de los Módems	48

2.3	Tipos de Interconexión de redes	50
2.3.1	Interred	51
2.3.2	Interconexión de área local	52
2.3.3	Interconexión de área Extensa	56
2.3.4	Interconexión de área Metropolitana	58
2.4	Definición de la interconectividad de redes	58
2.5	Control de Flujo	58

CAPITULO III

3.	FUNDAMENTOS DEL RUTEO	60
3.1	Definición de ruteo	60
3.2	Protocolos de red	61
3.3	Protocolos de ruteo	63
3.4	Protocolos LAN	65
3.5	Protocolos WAN	66
3.6	Algoritmos de ruteo	69
3.6.1	Objetivos de diseño	70
3.7	Métricas de ruteo	71

CAPITULO IV

4.	DISEÑO DE REDES	73
4.1	Pasos a tener en cuenta al diseñar una red	73
4.2	Diseño de una red	73
4.2.1	Escalabilidad de la red	74
4.2.2	Desempeño de la red	75
4.2.3	Seguridad de la red	75
4.2.4	Fiabilidad de la red	76
4.2.5	Redundancia en la red	76

4.2.5.1 Redundancia en medios de transmisión o de camino	76
4.2.5.2 Redundancia en equipos	77
4.2.6 Compatibilidad en los dispositivos	78
4.2.7 Compatibilidad entre la organización y la gente	78
4.2.8 Costos	79
4.3 Normalización	79
CONCLUSIÓN	80
RECOMENDACIONES	82
GLOSARIO	83
BIBLIOGRAFÍAS	86
ANEXOS	88

LISTA DE TABLAS Y FIGURAS

	Pág.
Figura 1. Telégrafo	24
Figura 2. Conmutación de paquetes	25
Figura 3. Topología Jerárquica	27
Figura 4. Medios de transmisión guiados	31
Figura 5. Medio de transmisión no guiado	33
Figura 6. Estándar Ethernet	34
Figura 7. Repetidor	38
Figura 8. Concentrador Múltipuestos	40
Figura 9. Switch	44
Figura 10. Línea de productos Cisco (Switches).	45
Figura 11. Módems	48
Figura 12. Tipos de Interconexión de redes	51
Figura 13. Interred	52
Figura 14. Red LAN	53
Figura 15. Red WAN	56
Figura 16. Control de Flujo	59
Figura 17. Redes Interconectadas	61
Figura 18. Funcionamiento del protocolo X25	68
Figura 19. Redundancia en cables	77
Figura 20. Redundancia en dispositivos	77
Tabla 1. Ficha Técnica del Switch Cisco Catalyst 2960G-48TC	54
Tabla 2. Ficha Técnica del Router Cisco 2851 Security Bundle	55
Tabla 3. Ficha Técnica del Router Cisco Catalyst 3560E-24TD	57

INTRODUCCIÓN

A lo largo del tiempo hemos sido partícipes del auge y amplio desarrollo de las redes en el mundo, estas han evolucionado y seguirán evolucionando a medida que la tecnología de interconectividad que las soporta, se siga desarrollando; su evolución concierne en mucho, al desarrollo de nuevas corrientes en la gestión de los servicios Informáticos, al surgimiento de nuevos dispositivos y tecnologías y a las nuevas utilidades que la computación y las redes presentan a la sociedad.

Gracias a la presencia de los dispositivos de interconexión, es que hoy en día se puede tener acceso a Internet sin duda alguna uno de los logros más grandes y más recientes ha sido la posibilidad de comunicarse vía Internet. Y más aun a la presencia de los medios de transmisión. Cabe resaltar que una red es un conjunto de computadores conectados entre si que tienen como objetivo compartir recursos e intercambiar información, pero este objetivo no fuese posible sin la existencia de los dispositivos de interconexión y más aun a la interconectividad de redes. Aspecto en el cual se enfocará esta monografía.

La interconectividad de redes es importante para compartir recursos y tener acceso a las base de datos compartidas en forma casi instantánea, además de permitir al administrador de la red una administración de la misma en forma centralizada. Si una empresa trabaja con una red, ésta reducirá sus costos de presupuesto en tiempo y en dinero.

Además se darán a conocer algunos aspectos determinantes y útiles al momento de pensar en la realización del diseño de la red de diferentes organizaciones, con la finalidad de optimizar, garantizar escalabilizar entre otros; para aquellas empresas o instituciones que desean tener un diseño de red.

CAPITULO I

1. ASPECTOS GENERALES DE LA ÍNTERCONECTIVIDAD DE REDES

1.1 Antecedentes del diseño, arquitectura e interconectividad de redes

Las redes desde sus inicios no tenían un diseño y arquitectura como tal, sino que se empezó por un telégrafo que comunicaba cierto números de países lo cual se originó en el siglo XX aproximadamente. A continuación se ilustra como era el proceso de comunicación en el telégrafo desde el emisor hasta el receptor.

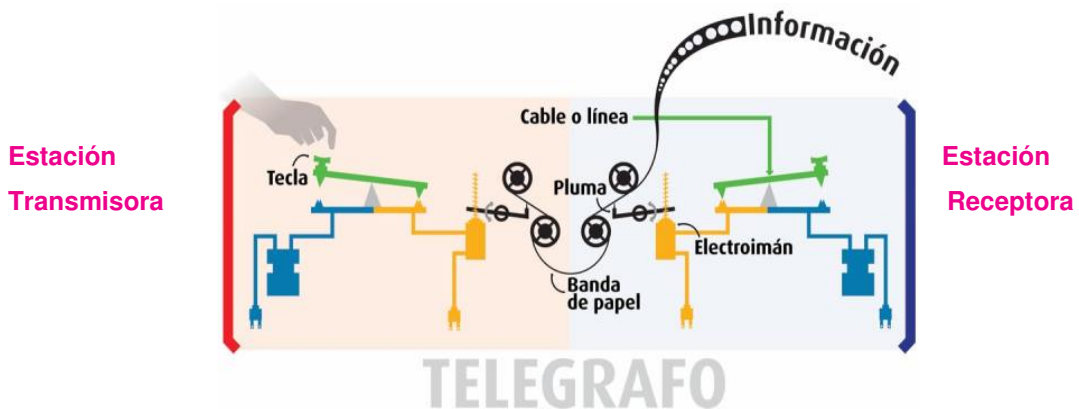


Figura 1. Telégrafo. Tomada de: <http://creativestudioinc.net/weblog/wp-content/telegrafo.jpg>

Hubo muchos avances, pero la verdadera historia del diseño y arquitectura de la red comienza en los años 60 con el establecimiento de las redes de conmutación de paquetes; la cual permite fragmentar los mensajes en varias partes y cuando llegan a su destino se unen nuevamente, deduciendo así que para lograr este avance, se estarían utilizando dispositivos de interconexión para la comunicación, por lo tanto; se tendría que buscar la forma de como ubicar dichos dispositivos, por lo que ya se estaría hablando de una arquitectura. En la figura siguiente se muestra el proceso de conmutación de paquetes.

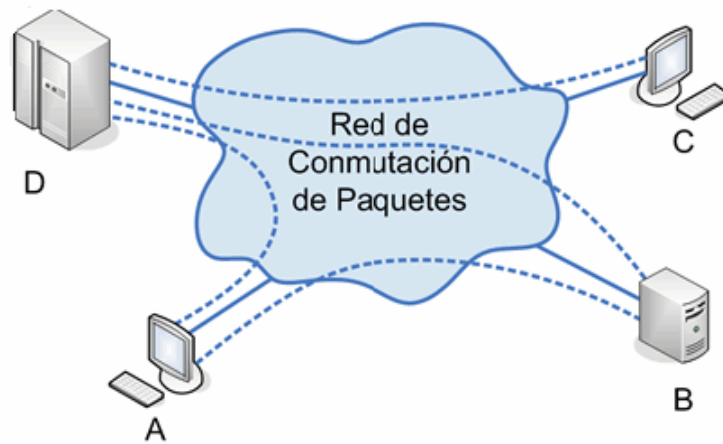


Figura 2. Conmutación de paquetes. Tomada de:
<http://www.textoscientificos.com/imagenes/redes/conmutacion-paquetes.gif>

Con el transcurrir del tiempo la tecnología ha avanzado sorprendentemente de la mano con las redes; tanto así que hoy en día ya se habla del diseño y arquitectura de red como tal; utilizando dentro de está, dispositivos de alto rendimiento, topologías, medios de transmisión, tecnologías, y otros factores que hacen parte del buen funcionamiento de la misma.

Se puede decir que una red es un conjunto de computadores conectados entre si que tienen como objetivo compartir recursos e intercambiar información, pero este objetivo no fuese posible sin la interconectividad de las redes; tema en el cual se enfatizará en el transcurso de esta monografía.

1.2 Topologías de red

Uno de los pasos importantes para el diseño y arquitectura de una red es la topología a utilizar, la topología es un mapa en donde se identifican segmentos, puntos de interconexión y los usuarios que van a estar en la red, por lo que a continuación se definirán las topologías más utilizadas:

La topología en anillo posee una escalabilidad limitada y además aumenta la latencia si dos extremos desean comunicarse. Conectan a un host con el siguiente al último con el primero para crear un anillo físico con el cable.

Posteriormente en la topología en bus los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; el bus. Además es el tipo de instalación más sencillo y un fallo en un nodo no provoca la caída del sistema de la red. Por lo que se puede decir que una ruptura del bus es difícil de localizar pero dependiendo de la longitud del cable y el número de terminales conectados a él provocando así la inutilidad de todo el sistema.

Por otra parte en la topología en estrella la escalabilidad queda limitada por el número de puertos en el nodo central y hay un punto único de fallas y un cuello de botella de procesamiento. Además, es buena configuración para administración y seguridad.

Por consiguiente en la topología en malla hay al menos dos nodos con dos o más caminos entre ellos es sumamente cara, y el desempeño depende del número de vecinos que tiene el nodo ruteador, consume demasiados recursos de la CPU, entre más vecinos ruteadores haya, peor será el desempeño.

Por último la topología jerárquica es una estructura en capas que se diseñan en orden cada capa realiza una función específica como se muestra en la siguiente figura:

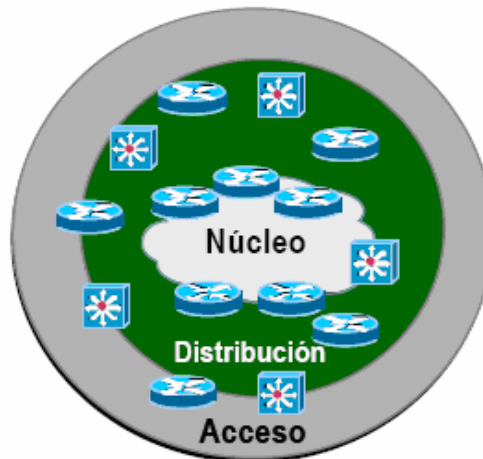


Figura 3. Topología Jerárquica. Tomada de:
http://webs.um.es/barzana/11/li09_images/dgwzmf82_69txzjz5fs.jpg

La capa de acceso de la red es el punto en el que cada usuario se conecta a la red, el tráfico hacia y desde recursos locales está confinado entre los recursos, switches y usuarios finales; en la capa de acceso se puede encontrar múltiples grupos de usuarios con sus correspondientes recursos. Posteriormente la capa de distribución marca el punto medio entre la capa de acceso y los servicios principales de la red, la función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN, y finalmente la capa de núcleo se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios; estos servicios se conocen como servicios globales o corporativos. Algunos de tales servicios pueden ser e-mail, el acceso a Internet o la videoconferencia. Cuando un usuario necesita acceder a un servicio corporativo, la petición se procesa al nivel de la capa de distribución. El dispositivo de la capa de distribución envía la petición del usuario al núcleo, este se limita al proporcionar un transporte rápido hasta el servicio corporativo solicitado. El dispositivo de la capa de distribución se encarga de proporcionar un acceso controlado a la capa de núcleo.

Es importante resaltar que las topologías es un tema de gran ayuda para la realización de esta monografía por que para el diseño y arquitectura de redes enfocados en la interconexión de la misma, es necesario en primera instancia tener en cuenta la lógica del negocio como se mencionó anteriormente y por ende saber que topología o estructura se va utilizar, y los dispositivos involucrados en el diseño, pero teniendo en cuenta que las características particulares de los equipos se saben hasta que se arma la red. Además la topología mas utilizada actualmente es la jerárquica por su división en capas.

1.3 Modelo de referencia OSI

Es una propuesta que desarrolló la organización internacional de normas, la cual logró la estandarización internacional que se usan en las diferentes capas de este modelo y que permite llevar a cabo un diseño y arquitectura de una red orientada a interconexión de la misma. Este modelo se ocupa de los sistemas de la conexión de sistemas abiertos.

Actualmente, las funciones propias de una red de computadoras pueden ser divididas en 7 capas propuestas por el modelo OSI.

La capa física define las especificaciones eléctricas, mecánicas de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas de redes de comunicaciones. Las especificaciones de la capa física definen características como niveles de voltaje, velocidades de transferencia de información, distancias máximas de información y conectores físicos.

Por otra parte la capa de enlace de datos proporciona el tráfico confiable de datos a través del enlace de red. Diferentes especificaciones de la capa de enlace de datos definen diferentes características de red y de protocolo, incluyendo el

direccionamiento físico, la topología de red, la notificación de error, la secuencia de tramas y el control de flujo.

Posteriormente la capa de red proporciona el ruteo y funciones relacionadas que permiten a múltiples enlaces de datos combinarse en una red. Esto se logra a través del direccionamiento lógico de los dispositivos. Además soporta servicios orientados y no orientados a la conexión de los protocolos de las capas superiores. Los protocolos de la capa de red con de hecho protocolos de ruteo, sin embargo también otro tipo de protocolos están implementados en la capa de red.

Por otro lado la capa de transporte es la que implementa servicios confiables de datos entre redes, transparentes a las capas superiores; entre las funciones habituales de la capa de transporte se cuentan el control de flujo, el multiplexaje, la administración de circuitos virtuales y la verificación y recuperación de errores.

Por consiguiente la capa de sesión establece, administra y finaliza las sesiones de comunicación entre las entidades de la capa de presentación; las sesiones de comunicación constan de solicitudes y respuestas de servicios que se presentan entre aplicaciones ubicadas en diferentes dispositivos de red, estas solicitudes y respuestas están coordinadas por protocolos implementados en la capa de sesión.

Posteriormente la capa de presentación brinda una gama de funciones de codificación y conversión que se aplican a los datos de la capa de aplicación, estas funciones aseguran que la información enviada desde la capa de aplicación de un sistema sea legible por la capa de aplicación de otro sistema.

Por último la capa de aplicación; esta es la capa más cercana al usuario final, lo que significa que tanto la capa de aplicación como el usuario interactúan de manera directa con la aplicación de software. Esta capa interactúa con las aplicaciones de software que implementan un componente de comunicación;

dichos programas están fuera del alcance del modelo OSI. Las funciones de la capa de aplicación incluyen la identificación de socios de comunicación, la determinación de la disponibilidad de recursos y la sincronización de la comunicación.

[Ver más información en: TANENBAUM, Andrew. Redes de computadoras. 3 ed. México: Ediciones Prentice Hall, 1997. Pág 77]

1.3.1 Medios de transmisión

Consiste en ese elemento físico que conecta físicamente las estaciones de trabajo con los servidores y los dispositivos de red. Se pueden usar varios medios físicos para la transmisión real; pero la selección del medio depende de las características de la aplicación en particular ya que cada medio tiene sus propias características costo, facilidad de instalación, ancho de banda, y velocidades de transmisión soportada. Estos suelen clasificarse en medios guiados y no guiados.

1.3.1.1 Medios de transmisión guiados

Son aquellos que proporcionan un conductor de un dispositivo a otro e incluyen los cables de par trenzado, el cable coaxial y los cables de fibra óptica.

El par trenzado es utilizado en las comunicaciones telefónicas y la mayoría de las redes Ethernet; y está constituido por un par de cables retorcidos juntos que conforman un circuito que puede transmitir datos. Su propósito es proporcionar protección contra el ruido generado por pares adyacentes. Es un medio bastante utilizado debido a su bajo costo, siendo esta una ventaja, pero su inconveniente principal es su corto alcance y su baja velocidad de transmisión.

Por otro lado el cable coaxial transporta señales con rangos de frecuencia más altos que los cables de pares trenzados. Consiste de un núcleo conductor central

formado por un hilo sólido o enfilado de cobre rodeado por un aislante, el cual a su vez está rodeado por una hoja exterior de metal conductor, malla o una combinación de ambos. Se utiliza mucho para las conexiones de TV cable.

Otro medio de transmisión guiado es fibra óptica este medio esta hecho de plástico o de cristal y transmite las señales en forma de luz la fibra óptica utiliza la reflexión para transportar la luz a través de un canal. Se utiliza mucho en redes troncales porque su gran ancho de banda es rentable frente al coste; la fibra óptica tiene varias ventajas con respecto a los anteriores medios y son: mayor ancho de banda, Inmune a interferencia electromagnética, ligereza, menor atenuación de la señal, mayor inmunidad a los pinchazos. Además dentro de desventajas se encuentran el alto costo, instalación/mantenimiento. Propagación unidireccional, si se requiere comunicación bidireccional se necesitan dos cables de fibra óptica. A continuación se ilustran los tipos de medios transmisión guiados utilizados en la interconexión de redes.



Fibra Óptica



Coaxial



Par Trenzado

Figura 4. Medios de transmisión guiados Tomada de:
http://webs.um.es/barzana/II/li09_images/dgwzmf82_69txzjz5fs.jpg

Estos son los medios LANs empleados para conectar computadoras aunque varían mucho de acuerdo a sus requerimientos. Por lo que en la actualidad se

están utilizando mucho los Cable UTP categoría 5e su estándar es TIA/EIA-568-B y ofrece muchas ventajas como por ejemplo su flexibilidad puesto que es un cable delgado, Además UTP es pequeño, por lo tanto no llenan rápidamente ductos de cableado, y lo más importante su bajo costo. (El precio del cable UTP cuesta menos por kilómetro que cualquier otro tipo de cable LAN). Otro tipo de cable UTP muy utilizado actualmente es el cable UTP categoría 6A utiliza el mismo estándar que el anterior y mayor ancho de banda puesto que es un cable mucho más grueso.

Otro cable muy utilizado actualmente es el cable coaxial que se utiliza para las conexiones de TV cable, por otra parte la fibra óptica es otro cable con mucha demanda en la actualidad puesto que su ancho de banda es muy grande (teóricamente de hasta 1 THz), Además es inmune totalmente a las interferencias electromagnéticas. Algunos tipos de cables de fibra óptica utilizados actualmente son el cable de fibra óptica híbrido por lo contiene tanto fibras ópticas como pares de cobre, y el Cable en abanico puesto que es un cable de estructura ajustada con un número pequeño de fibras y diseñado para una conexión directa y fácil (no se requiere un panel de conexiones), entre otros.

1.3.1.2 Medios de transmisión no guiados

Son aquellos que transportan ondas electromagnéticas sin usar un conductor físico; a este tipo de comunicación se le denomina también comunicación inalámbrica. Las señales se irradian al aire y está para cualquiera que tenga un dispositivo capaz de recibirla. Dentro de este tipo de medios están los infrarrojos que poseen las mismas técnicas que las empleadas por la fibra óptica pero son por el aire, son una excelente opción para las distancias cortas, hasta los 2km generalmente. Otro medio de transmisión no guiado es microondas; aquí las emisiones pueden ser de forma analógica o digitales pero han de estar en la línea

visible. Posteriormente el medio satelital es muy utilizado como medio no guiado puesto que ofrece muchas ventajas como lo son la libertad geográfica, y su alta velocidad. Por otra parte las ondas cortas; también llamadas radio de alta frecuencia; se utilizan mucho porque pueden transmitir señales a grandes distancias con poca potencia y su desventaja es que son menos fiables que otras ondas; y las ondas de luz son las ondas que utilizan la fibra óptica para transmitir por el vidrio. A continuación se ilustra la forma en que se transportan las ondas electromagnéticas sin usar un conductor físico.

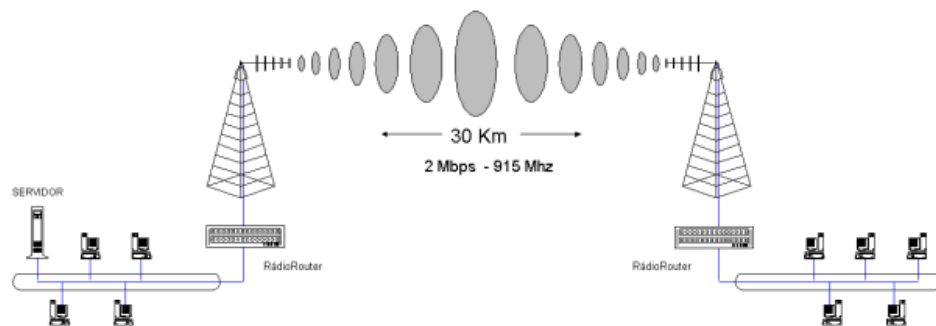


Figura 5. Medio de transmisión no guiado. Tomada de:
<http://www.forest.ula.ve/~mana/cursos/redes/Image12.gif>

1.3.2 Estándar Ethernet

En pocas palabras se puede decir que Ethernet es una tecnología de medio compartido, basada inicialmente en una topología tipo bus. Su referencia según la IEEE es la 802.3 (físico) y la 802.2 (lógico). Desarrollada inicialmente para ambientes LAN. Es una tecnología de capa 2. Inicialmente podían manejar información a 10 Mb/s, aunque actualmente se han desarrollado estándares mucho más veloces, como son: Ethernet a 100 Mb/s: Es una especificación LAN, conocida como Fast Ethernet, que opera a 100 Mb/s a través del cable par trenzado. Ethernet a 1000 Mb/s: Es una especificación LAN, conocida como

Gigabit Ethernet, que opera a 1000 Mb/s a través de los cables par trenzado y fibra óptica.

La red Ethernet ha prevalecido como una tecnología de transmisión fundamental, gracias a su tremenda flexibilidad y a que es relativamente fácil de comprender e implementar. Aunque se han propuesto otras tecnologías como sus posibles reemplazos, los administradores de red prefieren la red Ethernet y sus tecnologías derivadas como soluciones eficaces para un amplio rango de requerimientos de implementación en el campo de las redes. A continuación se muestra gráficamente el estándar Ethernet y la forma en que se basada inicialmente.

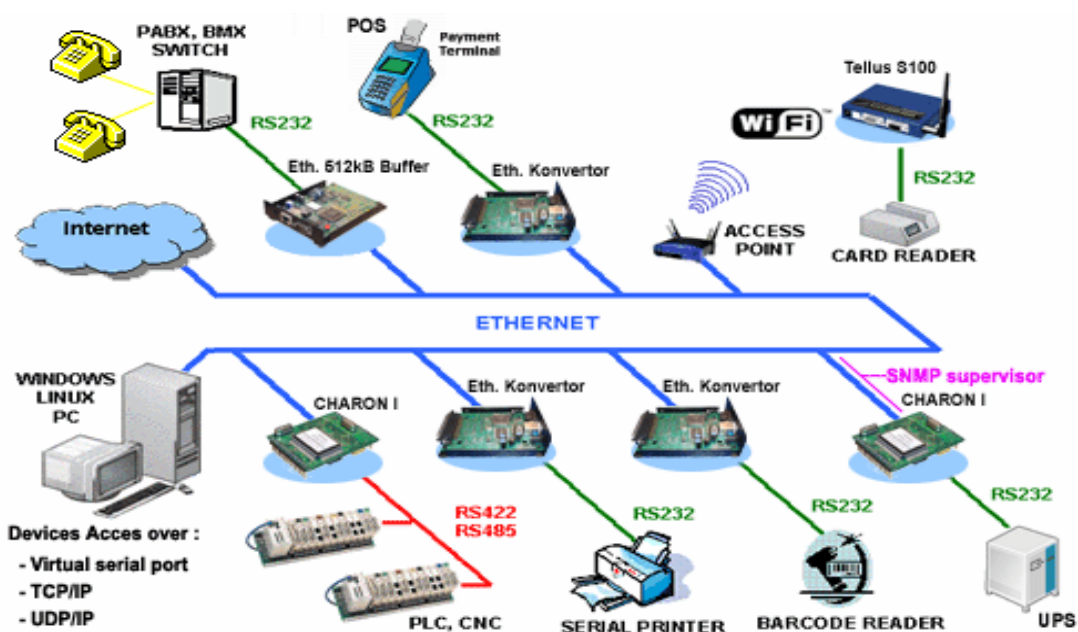


Figura 6. Estándar Ethernet. Tomada de: <http://static.howstuffworks.com/gif/ethernet3.gif>

1.3.3 Retos tecnológicos en la interconectividad de las redes

La implementación de una red funcional no es tarea fácil. 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 interred eficiente y efectiva. El reto al conectar varios sistemas es soportar la comunicación entre tecnologías diferentes ya que, por ejemplo, varios sitios pueden utilizar diferentes medios de transmisión, o bien operar a velocidades variables.

En 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. Además, la administración de la red debe proporcionar soporte centralizado y capacidades de corrección de fallas en una red. Para que ésta funcione adecuadamente se deben tener en cuenta aspectos como configuración, seguridad, desempeño, confiabilidad, localización, aislamiento, corrección y prevención de fallas, y planeación hacia el futuro.¹

La flexibilidad, el último aspecto, es necesaria para la expansión de la red y la implementación de nuevas aplicaciones y servicios, entre otros factores. Estos son algunos de los retos que existen en la interconectividad de redes: Reducción de presupuestos (tiempo, dinero), Escasez de ingenieros especializados en redes, Capacidad de planeación, administración y soporte, Retos técnicos y retos de admisnitración de redes.

Pero cabe resaltar que el verdadero reto de la interconectividad es la conectividad del transporte de información entre LAN dispersas geográficamente.

¹ FORD, Merilee; SPANIER, Steve; STEVENSON, Tim; LEW, Kim. Tecnologías de interconectividad de redes. México: Ediciones Pearson, 1998. Pág. 5

CAPITULO II

2. INTERCONECTIVIDAD DE REDES

2.1 Historia de la interconectividad de redes.²

Las primeras redes fueron redes de tiempo compartido que utilizaban mainframes y terminales conectadas. Dichos entornos se implementaban con la SNA (Arquitectura de Sistemas de Redes) de IBM y la arquitectura de red de digital.

Las LANs (Redes de Área Local) surgieron a partir de la revolución de PC. Las LANs permitieron que varios usuarios ubicados en un área geográfica relativamente pequeña pudieran intercambiar mensajes y archivos, y tener acceso a recursos compartidos como los servidores de archivos. Posteriormente las WANs (Redes de Área Amplia) interconectan LANs por medio de líneas telefónicas normales (y otros medios de transmisión) y de esta manera interconectan a usuarios geográficamente dispersos.

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 y video conferencia.

La tecnología de interconectividad de redes surgió como una solución a tres problemas: LANs aisladas, duplicación de recursos y falta de administración de recursos. Las LANs aisladas imposibilitan 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,

² <http://www.edufuturo.com/imageBDE/EF/78923.historiainteronectividad.pdf>

así como tener grupos de soporte separados. Esta falta de administración de red provocó que no hubiera un método centralizado para administrar y separar las redes.

2.2 Dispositivos de interconexión de redes

Las redes se conectan mediante equipos de telecomunicaciones conocidos como equipos de interconexión. Estos dispositivos de interconexión que conectan dos o más redes que están separadas con el fin de intercambiar datos o recursos y a su vez forman una interred. A estos dispositivos que realizan esta tarea se les llama equipos de Interconexión. Por lo que a continuación se hará una breve descripción de algunos de los dispositivos de interconexión a nivel de LANs y WANs.

2.2.1 Evolución de los Repetidores.³

Los repetidores estaban dotados de dos puertos AUI y se conectaban mediante dos cables AUI de dos transceptores puestos en dos segmentos de red entre los cuales la señal se debía relanzar. Posteriormente la evolución de los medios de transmisión de Ethernet ha impuesto cambios inclusive a los repetidores que hoy poseen interfaces diferentes de la sencilla AUI. La tendencia actual es dotar de más inteligencia y flexibilidad a los repetidores, de tal forma que ofrezcan capacidad de gestión y soporte de múltiples medios físicos, como Ethernet sobre par trenzado (10BaseT), ThickEthernet (10Base5), ThinEthernet (10Base2), TokenRing, fibra óptica, etc.

³ PIÑEROS OROZCO, Karen Cecilia; GONZÁLEZ ZUÑIGA, Darwin. Dispositivos de Interconexión de redes y medios de transmisión. Universidad Tecnológica de Bolívar, Minor en redes y Telecomunicaciones, Facultad de Ingeniería de Sistemas y Electrónica. 2004

¿Que es un Repetidor?

Un repetidor limpia, amplifica y reenvía una señal debilitada por la longitud del cable, su propósito es regenerar y reenviar las señales de red a nivel de bits para hacer posible que éstas viajen largas distancias por los medios. Son dispositivos de la capa 1 del modelo OSI, porque actúan sólo a nivel de bits. Además es un dispositivo utilizado a nivel de LANs escasamente se utiliza pues su uso es cuando existen distancias a 100 mts entre dos segmentos de red; esto no quiere decir que no se este empleando en algunos diseños de red.

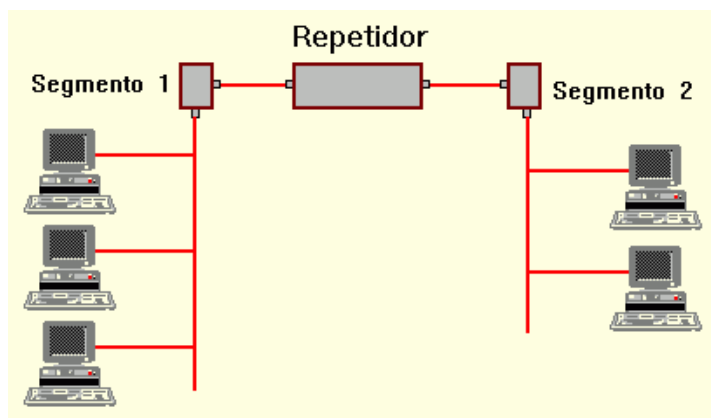


Figura 7. Repetidor. Tomada de: <http://www.csi.map.es/csi/silice/Redcon9.html>

En la gráfica anterior se muestra un ejemplo de utilización de un repetidor puesto que su uso está limitado por la distancia máxima de la red y el tamaño máximo de cada uno de los segmentos de red conectados.

Ventajas de un Repetidor

- ✓ Retransmite los datos sin retardos
- ✓ Conecta redes con diferentes medios de transmisión.
- ✓ Es transparente a los niveles superiores físicos

- ✓ Incrementa la distancia cubierta por la LAN.

Desventajas de un Repetidor

- ✓ Incrementa la carga en los segmentos que interconecta.
- ✓ Sólo se pueden utilizar para unir dos redes que tengan los mismos protocolos de nivel físico.

2.2.2 Evolución de los Hubs.⁴

Los primeros concentradores para redes de área local nacieron como concentradores de cableado a mediados de los años ochenta, fundamentalmente, para redes tipo CSMA/CD con cable de pares telefónico, 10BaseT. Los primeros hubs o de primera generación son cajas de cableado avanzadas que ofrecen un punto central de conexión conectado a varios puntos. Sus principales beneficios son la conversión de medio, y algunas funciones de gestión bastante primitivas como particionamiento automático cuando se detecta un problema en un segmento determinado.

Posteriormente aparecen los concentradores multimedio, que permiten la conexión a diferentes medios físicos: 10Base2, 10Base5, 10BaseT, etc.

Los Hubs inteligentes de segunda generación basan su potencial en las posibilidades de gestión ofrecidas por las topologías radiales (TokenRing y Ethernet). Tiene la capacidad de gestión, supervisión y control remoto, dando a los gestores de la red la oportunidad de ofrecer un periodo mayor de funcionamiento de la red gracias a la aceleración del diagnóstico y solución de problemas.

⁴ Academia de networking de Cisco Systems: Guía del primer año. 2 ed. Pág. 889

La tercera generación de concentradores soporta múltiples segmentos de redes de área local de distintas arquitecturas, como pueden ser Ethernet, pase de testigo en anillo. FDDI, etc., utilizándose puentes o encaminadores integrados en el concentrador para interconectar los distintos segmentos. Los nuevos hubs de tercera generación ofrecen proceso basado en arquitectura RISC (Reduced Instructions Set Computer) junto con múltiples placas de alta velocidad. Estas placas están formadas por varios buses independientes Ethernet, TokenRing, FDDI y de gestión, lo que elimina la saturación de tráfico de los actuales productos de segunda generación.

A un hub Ethernet se le denomina repetidor múltipuerto. El dispositivo repite simultáneamente la señal a múltiples cables conectados en cada uno de los puertos del hub. Un hub Ethernet se convierte en un hub inteligente (smart hub) cuando puede soportar inteligencia añadida para realizar monitorización y funciones de control. En el siguiente gráfico se muestra el esquema del concentrador múltipuerto.

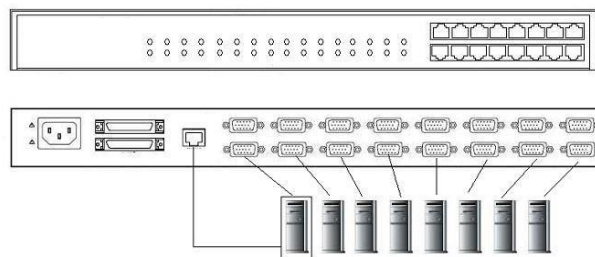


Figura 8. Concentrador Múltipuertos Tomada de: http://www.scisl.com/esquema_concentrador.JPG

Los concentradores inteligentes permiten a los usuarios dividir la red en segmentos de fácil detección de errores a la vez que proporcionan una estructura de crecimiento ordenado de la red. El tipo de hub Ethernet más popular es el hub 10BaseT. En este sistema la señal llega a través de cables de par trenzado a una

de las puertas, siendo regenerada eléctricamente y enviada a las demás salidas. Este elemento también se encarga de desconectar las salidas cuando se produce una situación de error.

¿Que es un Hub?

Es un dispositivo que se utiliza en el centro de la red con el objetivo de propagación de información. Además son equipos de capa uno. No hay inteligencia o nivel de procesamiento en ellos. Hoy en día no se utilizan. Tiene como función regenerar y reenviar señales, propagar las señales en la red, además no pueden filtrar el tráfico de la red, no pueden determinar la mejor ruta, y se utilizan como puntos de concentración de la red. Y funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tengan acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Los Hubs son otro tipo de dispositivo a nivel de LANs aunque actualmente poco se utilizan.

Tendencia en el uso de Hubs

Cisco ofrece una amplia gama de Hubs. La línea de productos Cisco evoluciona continuamente en respuesta a las necesidades de los clientes y otros aspectos relacionados con la migración de la tecnología.

El criterio que se usa para seleccionar los Hubs incluye la velocidad media y el número de puertos que se necesitan, la facilidad de instalación y la posibilidad de administrarlo de forma remota. Antes de implementar los Hubs, evalúe qué estaciones de trabajo necesitan actualizarse a 100 Mbps, mientras que los de rango medio son autosensibles a la velocidad de datos de las tramas de Ethernet

y proporcionan de 10 Mbps a 100 Mbps. Este rango medio se puede manejar según las necesidades actuales y futuras.

Dentro de los Hubs que ofrece Cisco se encuentran:

- ✓ Cisco 1500 Micro Hub
- ✓ Cisco 1528 Micro Hub 10/100
- ✓ Cisco FastHub100
- ✓ Cisco FastHub200
- ✓ Cisco FastHub300
- ✓ Cisco FastHub400

El objetivo de consolidar las conexiones se refiere a la cantidad de puertos Hubs que necesitan los usuarios. Los hubs permiten varias densidades de puertos, y el usuario puede apilarlos para obtener múltiples densidades de hubs. La mayoría de los hubs son sólo para conectar y para operar. No existe puerto de consola para la mayoría de ellos. Si desea un hub administrable que contenga una consola integrada, selecciónelo en las series del extremo superior.

2.2.3 Evolución de los Puentes o Bridges.⁵

Los primeros puentes transparentes fueron desarrollados por DEC a principios de los ochenta, apareciendo los primeros productos comerciales en 1984. Aunque caros y de bajo rendimiento comparados con los actuales, suponían una alternativa interesante a los routers por su sencillez y relación precio/prestaciones.

En 1987 el IEEE se puso en marcha para estandarizar el funcionamiento de los puentes. El resultado fue el estándar 802.1D aprobado en 1990.

⁵ Academia de networking de Cisco Systems: Guía del primer año. 2 ed. Pág. 84

En 1991 una empresa de reciente creación denominada Kalpana comercializó un nuevo tipo de puentes Ethernet con un número elevado de interfaces y alto rendimiento. Estos equipos se anunciaban como conmutadores LAN para diferenciarlos de los tradicionales puentes, aun cuando su principio de funcionamiento era el mismo.

¿Qué son los Puentes o Bridges?

Dividen una red en segmentos y filtran el tráfico. Además es un dispositivo de capa 2 diseñado para crear dos o más segmentos LAN, cada uno de ellos con un dominio de colisión separado. Es decir; han sido elaborados para crear un ancho de banda más utilizable. El propósito de un puente es filtrar el tráfico de la LAN, para mantener el tráfico local, permitiendo la conectividad con otras partes de la LAN para el tráfico se dirige allí. Los puentes filtran el tráfico de la red fijándose sólo en las direcciones MAC. Por tanto, pueden enviar rápidamente tráfico representando cualquier protocolo de capa de red.

2.2.4 Evolución de los Switches.⁶

El precio de la tecnología del switchg continua descendiendo, como resultado del desarrollo ASIC unido con la eficiencia de la manufactura y técnicas de distribución. Como el costo por puerto del switch se aproxima al de los hubs, muchos usuarios eligen el switch.

La extensa disponibilidad de la tecnología de switch de bajo costo tiene implicaciones para las redes de los edificios y el backbone de campus. Habrá una

⁶ PIÑEROS OROZCO, Karen Cecilia; GONZÁLEZ ZUÑIGA, Darwin. Dispositivos de Interconexión de redes y medios de transmisión. Universidad Tecnológica de Bolívar, Minor en redes y Telecomunicaciones, Facultad de Ingeniería de Sistemas y Electrónica. 2004

demanda creciente para switches de backbone de alta densidad, con un número grande de puertos de alta velocidad, para enlazar grupos de trabajo individuales.

Eventualmente el equipo de escritorio será dedicado a enlaces de 10 Mbps, la mayoría de los servidores estarán conectados a los switch de alta velocidad y ATM se usará en enlaces internos del edificio y al backbone de campus.

¿Que es un Switch?

Los switches son equipos de capa 2. Por que parte de su virtud está en que hace el envío y recepción de tramas en base a la dirección MAC de los host que tienen conectados. Los switches son más rápidos porque todo el procesamiento es a nivel de hardware. No sube a capas de aplicación y eliminan las colisiones. Dentro de sus funciones están el reenvío o filtrado de tramas, y se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola, al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs. Cabe resaltar que este tipo de dispositivo es uno de los más utilizados a nivel de LANs por sus grandes ventajas.



Figura 9. Switch. Tomada de: <http://www.microalcarria.com/global/php/imagen.php?camino=/uknaaxyhr/&nombre=drftbtzx/CBY-0747J.oif>

Ventajas de los Switches:

- ✓ Son usados para reenviar paquetes a un segmento particular utilizando el direccionamiento de hardware MAC (como los puentes).
- ✓ Debido a que los switches son basados en hardware, estos pueden conmutar paquetes más rápido que un puente.
- ✓ Pueden soportar numerosas comunicaciones simultáneas.
- ✓ Se utilizan para aumentar el rendimiento en las redes de las organizaciones, segmentando las grandes en varias más pequeñas.
- ✓ Realiza transferencia de tráfico de broadcast y de multicast, pero disminuye el dominio de colisión al mínimo.

Tendencia en el uso de Switches

Cisco ofrece una amplia gama de Switches Catalyst como se ilustra en la siguiente figura:

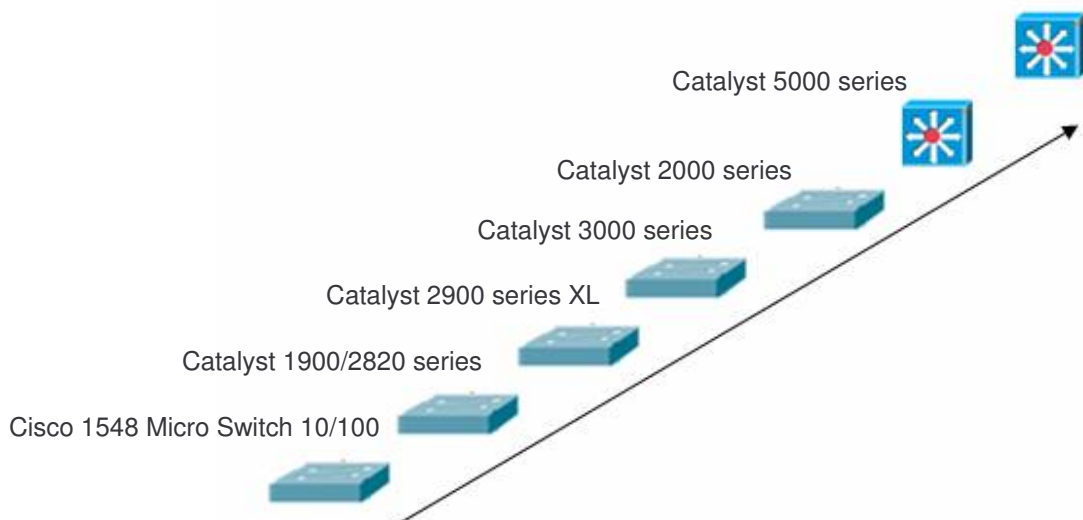


Figura 10. Línea de productos Cisco (Switches). Tomada de: Academia de networking de Cisco Systems: Guía del primer año. 2 ed. Pág. 91

Conforme nos acercamos a los switches Catalyst de gama alta, la densidad de los puertos (número de puertos disponibles en el switch) aumenta (alrededor de 100 puertos FastEthernet por Switch). Los switches del extremo superior también pueden integrar módulos para conmutar paquetes con ATM.

2.2.5 Evolución del Router.⁷

Los routers son uno de los equipos más importantes dentro de una red, así como son el núcleo del enrutamiento de Internet. Es uno de los equipos que más adelantos tecnológicos ha sufrido, adaptándose a los avances en los protocolos y a los nuevos requerimientos en servicios. Estos equipos, ya no sólo transportan datos sino que también han incluido la posibilidad de transportar aplicaciones antes no presupuestadas, como la voz. La voz sobre IP emerge como una tecnología muy prometedora, y los Routers son los protagonistas en este avance.

El ruteo es la llave para desarrollar redes internas. El desafío es integrar el switch con ruteo para que el sistema aproveche el diseño de la red. Cada uno de los grandes vendedores de ruteadores tiene investigando más de 300 millones de dólares en hora/hombre, desarrollando líneas de código para sus productos. Cada liberación de software representa un tremendo esfuerzo de ingeniería, para asegurar que el ruteador soporte la última tecnología y dirección de diseño en redes internas.

⁷ PIÑEROS OROZCO, Karen Cecilia; GONZÁLEZ ZUÑIGA, Darwin. Dispositivos de Interconexión de redes y medios de transmisión. Universidad Tecnológica de Bolívar, Minor en redes y Telecomunicaciones, Facultad de Ingeniería de Sistemas y Electrónica. 2004

¿Qué es el Router?

El router tiene como función examinar los paquetes entrantes de los datos que se encuentran de la capa 3 del modelo OSI, elegir la mejor ruta a través de la red y luego los conmuta al mejor puerto de salida es su función. Además son el dispositivo regulador de tráfico más importante en redes robustas, y permiten que cualquier tipo de computador se comuniquen con otro en cualquier parte del mundo. Es el principal dispositivo con el que se trabaja en la capa 3 del modelo OSI el cual permite al router tomar decisiones basándose en las direcciones de red. A continuación se muestra la manera como opera un router en una estructura de red. Este es uno de los dispositivos más utilizados a nivel de LANs y WANs por sus grandes ventajas.

Tendencia en el uso de Router

Un criterio que resulta clave para seleccionar un router es saber qué funciones del router se necesitan. Los diversos routers de la línea de productos Cisco incorporan funciones diferentes. Las densidades de los puertos y la velocidad de la interfaz normalmente aumentan según se desplace hacia el extremo superior de las diferentes familias de routers Cisco. Por ejemplo, la serie 12000 es el primer producto de la clase gigabit switch routers (GSR). El GSR Cisco 12000 soporta inicialmente enlaces con el backbone IP de OC-12 (622 Mbps), y puede escalarse hasta manipular enlaces de OC-48 (2,4 Gbps).

Si su red necesita enlaces WAN, la selección del router supondrá saber qué router proporciona los enlaces necesarios de un modo rentable. Normalmente, una red de producción tiene varios Switches LAN interconectados a las WAN mediante routers.

Dentro de los Routers que ofrece Cisco se encuentran:

- ✓ Cisco 700/800 Series
- ✓ Cisco 1600/1700 Series
- ✓ Cisco 2500 Series
- ✓ Cisco 2600 Series
- ✓ Cisco 3600 Series
- ✓ AS 5000 Series
- ✓ Cisco 4000 Series
- ✓ Cisco 7000 Series
- ✓ Cisco 12000 GSR Series

2.2.6 Evolución de los Módems.⁸

Cuando se planteó la necesidad de buscar un medio de transmisión que permitiera conectar dos equipos de datos muy alejados entre si, se pensó en la red telefónica debido a su enorme difusión. Sin embargo, había un inconveniente que impedía la conexión directa entre los dos equipos: la red era analógica, y los datos, digitales. Se hizo necesario, por tanto, el desarrollo de un equipo que adaptara los datos digitales de forma que éstos pudieran transmitirse a través de un canal analógico telefónico. Este equipo se denominó Módem.

La palabra módem es una contracción modulador-demodulador. Es fácil adivinar, por tanto, que la adaptación que realiza el módem consiste en la modulación de una portadora con los datos recibidos del terminal. El demodulador, por su parte, demodula los datos recibidos a través de la línea y procedentes de un terminal u ordenador remoto.

⁸ PIÑEROS OROZCO, Karen Cecilia; GONZÁLEZ ZUÑIGA, Darwin. Dispositivos de Interconexión de redes y medios de transmisión. Universidad Tecnológica de Bolívar, Minor en redes y Telecomunicaciones, Facultad de Ingeniería de Sistemas y Electrónica. 2004

Hoy en día estos equipos han evolucionado tanto que el modulador-demodulador descrito anteriormente es sólo una pequeña parte de lo que hoy se denomina módem. Los equipos actuales incluyen generadores de secuencias aleatorias, codificadores, ecualizadores, llamada y respuesta automática, facilidades de prueba, control de errores y un sin fin de nuevos elementos más permiten continuamente aumentar las prestaciones y la velocidad del módem.

¿Qué es un Módems?

Dispositivo que tiene como objetivo convertir señales digitales a señales analógicas de un ordenador utilizando la línea telefónica de forma que puedan intercambiar información entre sí. Los módems han adquirido gran popularidad gracias a su uso en los ordenadores, sin embargo los módems son usados en un sin fin de aplicaciones, como las comunicaciones telefónicas, radiofónicas y de televisión. Además es uno de los métodos más extendidos para la interconexión de ordenadores como se mencionó anteriormente debido a su sencillez y bajo costo; y se pueden clasificar de diferentes maneras, siendo una de ellas la clasificación por el tipo de moduladora empleada, teniendo así los módems digitales, en los cuales la moduladora es una señal digital y los módems analógicos, en donde la moduladora es una señal analógica.



Figura 11. Módems. Tomada de: http://img.alibaba.com/photo/11414118/Modems_Dtu_Hdsl.jpg

Tipos de Módems

- ✓ Módems acústicos
- ✓ Módems de conexión directa
- ✓ Módems digitales
- ✓ Módems analógicos
- ✓ Módems de línea conmutada
- ✓ Módems de línea privada
- ✓ Módems internos
- ✓ Módems externos

Ventajas de los Módems

- ✓ Es uno de los métodos más extendidos para la interconexión de ordenadores por su sencillez y bajo costo.
- ✓ Permite conectar dos ordenadores remotos utilizando la línea telefónica de forma que puedan intercambiar información entre si.

Desventajas de los Módems

- ✓ Cuando dos Módems vayan a intercambiar información deben operar con el mismo estándar de comunicación.

2.3 Tipos de Interconexión de redes

En la siguiente gráfica se muestran los diferentes tipos de interconexión de redes en las cuales nos enfocaremos en el transcurso de este documento.

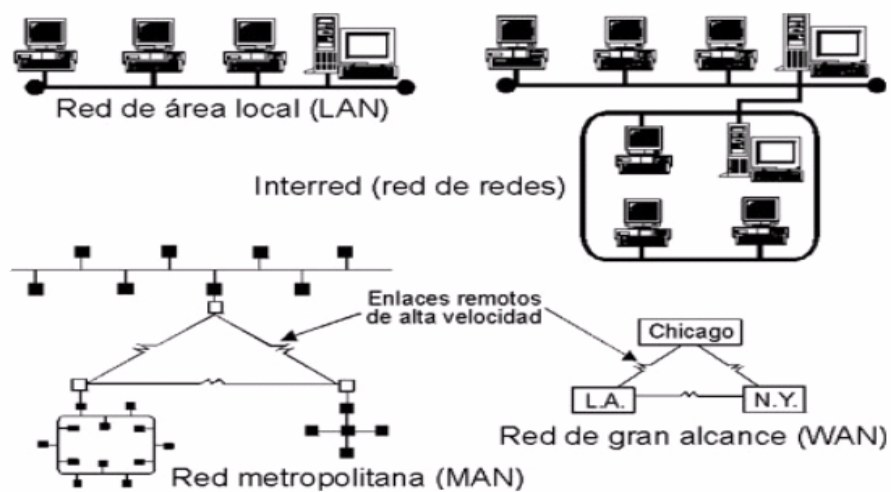


Figura 12. Tipos de Interconexión de redes. Tomada de http://redesinformaticas.wikispaces.com/space/showImage/Lan_man_wan.jpg

2.3.1 Interred

Una interred es el conjunto de redes individuales conectadas a través de dispositivos intermedios de conectividad de redes que funcionan como una sola red. Las interredes se construyen a partir de varias redes; estas están interconectadas por computadoras dedicadas llamadas routers y computadores de propósito general llamadas gateways, y por un subsistema integrado de comunicaciones producidos por una capa de software que soporta el direccionamiento y la transmisión de datos a los computadores a través de la interred. Los resultados pueden contemplarse como una red virtual construida a partir de solapar una capa de interred sobre un medio de comunicación que consiste en varias redes, routers y gateways subyacentes. A través de la siguiente figura se muestra la forma en que dos redes se conectan a través de un router formando de esta manera una interred.

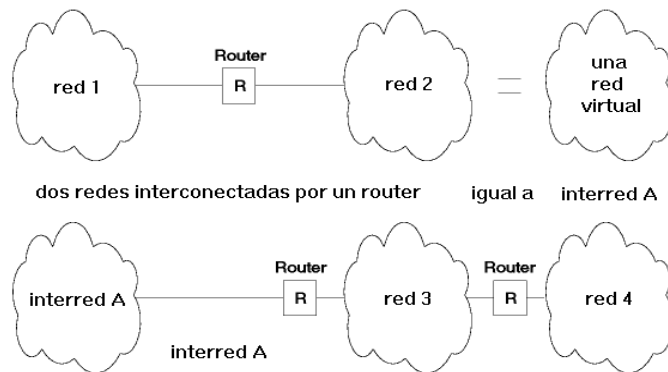


Figura 13. Interred. Tomada de: <http://personales.upv.es/rmartin/Tcplp/imagenes/interred.gif>

Para construir una red integrada (una interred) de debe integrar muchas subredes, cada una de las cuales se basa en una tecnología de red. Para hacerlo se necesita.

- ✓ Un esquema de direccionamiento unificado que posibilite que los paquetes sean dirigidos a cualquier hosts conectado en cualquier subred.
- ✓ Un protocolo que defina el formato de paquetes interred y las reglas según las cuales serán gestionados.
- ✓ Componentes de interconexión que encaminen paquetes hacia su destino en términos de dirección interred, transmitiendo los paquetes utilizando subredes con tecnología de red variada.

2.3.2 Interconexión de área local

Una LAN es una red de datos de alta velocidad, tolerante a fallas, que cubre un área geográfica relativamente pequeña. Las LAN tienen muchas ventajas para los usuarios de computadoras, entre otras el acceso compartido a dispositivos y aplicaciones, el intercambio de archivos entre los usuarios conectados entre otros.

Además están constituidas por computadoras, tarjetas de interfaz de red, medios de red, dispositivos del control del tráfico de la red y dispositivos periféricos. Las LAN permiten a las empresas que emplean tecnología informática compartir de forma eficiente elementos, tales como archivos e impresoras, y posibilitar las comunicaciones, como el correo electrónico. A través de la siguiente gráfica se muestra como es la distribución de una red LAN y la distancia que puede cubrir.

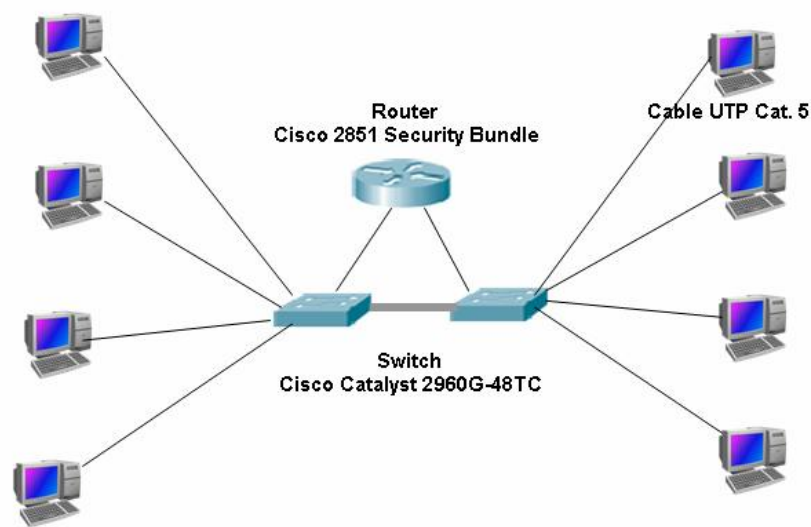


Figura 14. Red LAN.

Dentro de esta red LAN encontramos dos switches Cisco Catalyst 2960G-48TC y Router Cisco 2851 Security Bundle conectados mediante el cable UTP categoría 5. A continuación se muestra la ficha técnica de los dispositivos utilizados dentro de esta red LAN.

[Ver más Información en: ABAD DOMINGO, Alfredo. Redes de área local. 3 ed. México: Ediciones McGraw-Hill, 2005. Pág. 52]

CISCO Catalyst 2960G-48TC	
Características	Descripción
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 2U
Anchura	43.82 cm
Profundidad	41.66 cm
Altura	8.89 cm
Peso	11.4 kg
Memoria RAM	256 MB (instalados) / 1 GB (máx.)
Memoria Flash	64 MB (instalados) / 256 MB (máx.)
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Indicadores de estado	Actividad de enlace, alimentación
Cumplimiento de normas	IEEE 802.3af
Códex de voz	G.711, G.723.1, G.728, G.729, G.729a, G.729ab, G.726
Funciones de telefonía IP	Cancelación de eco (G.168)
Tipo de Comunicación	Módulo de fax / voz
Dispositivo de alimentación	Fuente de alimentación - interna
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	5 - 95%

Tabla 1. Ficha Técnica del Switch Cisco Catalyst 2960G-48TC

CISCO 2851 Security Bundle	
Características	Descripción
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 2U
Anchura	43.82 cm
Profundidad	41.66 cm
Altura	8.89 cm
Peso	11.4 kg
Memoria RAM	256 MB (instalados) / 1 GB (máx.)
Memoria Flash	64 MB (instalados) / 256 MB (máx.)
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Indicadores de estado	Actividad de enlace, alimentación
Cumplimiento de normas	IEEE 802.3af
Total ranuras de expansión (libres)	4 (4) x HWIC 2 (2) x AIM 1 (1) x NME-XD 1 (1) x EVM 3 (3) x PVDM 2 memoria 1 Tarjeta CompactFlash
Interfaces	2 x red - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 2 x USB 1 x gestión - consola 1 x red - auxiliar
Algoritmo de cifrado	DES, Triple DES, AES
Cumplimiento de normas	CISPR 22 Class A, CISPR 24, EN 61000-3-2, VCCI Class A ITE, IEC 60950, EN 61000-3-3, EN55024, EN55022 Class A, UL 60950, EN50082-1, CSA 22.2 No. 60950, AS/NZ 3548 Class A, JATE, FCC Part 15, ICES-003 Class A, CS-03, EN 61000-6-2
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C

Tabla 2. Ficha Técnica del Router Cisco 2851 Security Bundle

Dentro de esta red WAN encontramos dos switches Cisco Catalyst 2960G-48TC y dos Routers Cisco 2851 Security Bundle conectados mediante el cable UTP categoría 6A. A continuación se muestra la ficha técnica del Switch Cisco Catalyst 3560E-24TD puesto que la ficha técnica de los demás dispositivos se puede observar en la gráfica de redes LAN.

CISCO Catalyst 3560E-24TD	
Características	Descripción
Tipo de dispositivo	Conmutador
Tipo incluido	Montable en bastidor - 1U
Anchura	44.5 cm
Profundidad	46 cm
Altura	4.5 cm
Peso	8.1 kg
Memoria RAM	128 MB
Memoria Flash	64 MB Flash
Cantidad de puertos	24 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T
Velocidad de transferencia de datos	1 Gbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, Gigabit Ethernet
Protocolo de direccionamiento	OSPF, BGP-4, RIP-1, RIP-2, EIGRP, HSRP, DVMRP, PIM-SM, direccionamiento IP estático, PIM-DM, OSPFv3
Protocolo de gestión remota	RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3
Tecnología de conectividad	Cableado
Modo comunicación	Semidúplex, dúplex pleno
Protocolo de conmutación	Ethernet
Servicio y mantenimiento	Garantía de 90 días
Detalles de Servicio y Mantenimiento	Garantía limitada - 90 días
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	45 °C
Ámbito de humedad de funcionamiento	0 - 95%

Tabla 3. Ficha Técnica del Router Cisco Catalyst 3560E-24TD

2.3.4 Interconexión de área Metropolitana

Otro tipo de interconexión de redes es la MAN (Redes de área metropolitana) por lo que se definirá muy someramente; ya que nos basaremos en los tipos de interconexión anteriormente mencionados. Se define como una red de alta velocidad dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado, la tecnología de pares de cobre se posiciona como una excelente alternativa para la creación de redes metropolitanas.

2.4 Definición de la interconectividad de redes

La interconectividad se define como el proceso de comunicación que sucede entre dos o más redes que están conectadas entre sí; asimismo es importante porque permite compartir recursos, el acceso instantáneo a bases de datos compartidas, la insensibilidad a la distancia física y a la limitación en el número de nodos, permite la administración centralizada de la red y además da una ventaja estratégica en el mercado competitivo global.

2.5 Control de Flujo

El control de flujo es una función que evita la saturación en la red asegurando que los dispositivos de transmisión no saturen de datos a los de recepción. Hay un sin número de causas posibles de saturación en una red. Una computadora de alta velocidad, puede generar tráfico más rápidamente que el que la red pueda transferir, o más rápido de lo que el dispositivo pueda recibir y procesar. Los tres métodos que se utilizan con más frecuencia para el manejo de la saturación en la

red son el almacenamiento en el buffers, el envío de mensajes de destrucción origen y el manejo de ventanas.⁹

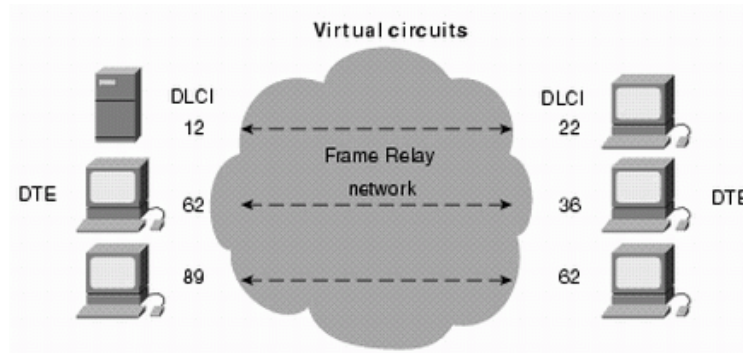


Figura 16. Control de Flujo Tomada de: <http://www.monografias.com/trabajos38/conexion-cables-red/con8.gif>

Por lo tanto, el control de flujo es un mecanismo que permite al receptor controlar la razón a la que envía datos de un transmisor. El control flujo hace posible que un receptor que opera en una computadora de baja velocidad pueda aceptar datos de una alta velocidad sin verse saturada

⁹ FORD, Merilee; SPANIER, Steve; STEVENSON, Tim; LEW, Kim. Tecnologías de interconectividad de redes. México: Ediciones Pearson, 1998. Pág. 8

CAPITULO III

3. FUNDAMENTOS DEL RUTEO

En esta investigación no solo se tendrá en cuenta la parte física de la red (Arquitectura) sino también la parte lógica; es decir, como es el proceso de transferencia de la información a través de una red desde un origen hasta un destino. Por lo que se definirán algunos conceptos necesarios a tener en cuenta.

3.1 Definición de ruteo

Entonces se puede decir que el ruteo es el proceso mediante el cual un paquete conoce el camino para llegar desde el nodo A hasta el nodo B. Es importante saber que cada nodo de una red TCP/IP está identificado por la IP, y que una red es un grupo de números IP. Estas redes están conectadas unas con otras mediante Gateways.

En la siguiente figura se muestra un problema de ruteo, además hay que tener en cuenta que no sólo es importante el lugar de destino, sino el lugar de partida de los paquetes, por ejemplo, un paquete que sale desde 192.168.1.2 con destino 192.168.3.2 no sigue el mismo camino que uno que sale desde 182.168.3.1 aunque vaya al mismo destino.

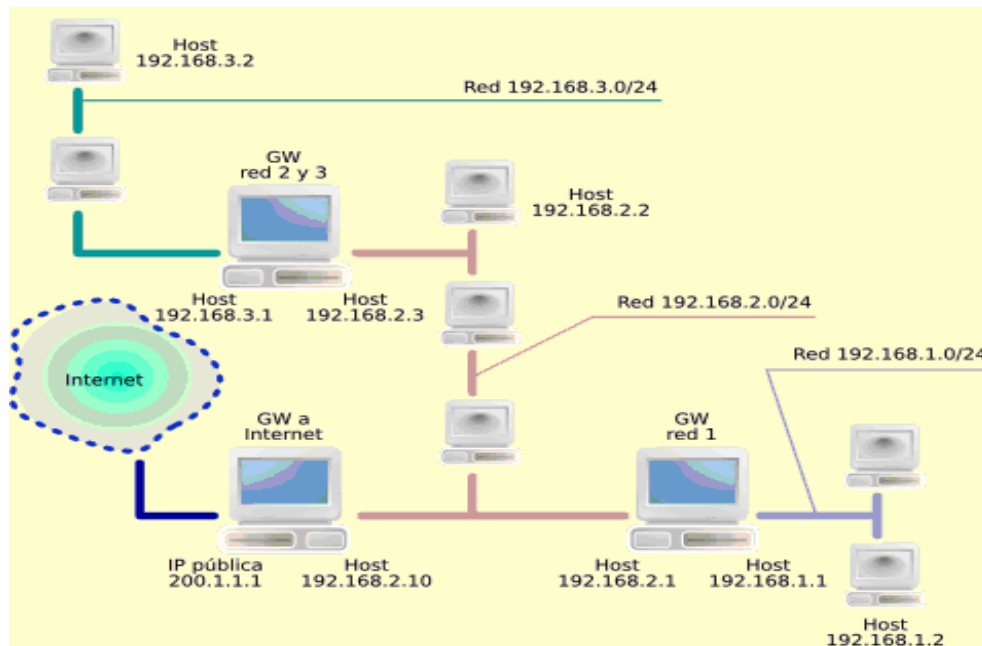


Figura 17. Redes Interconectadas. Tomada de:
<http://www.iranon.net/soluciones/imagenes/red06.gif>

La solución adoptada en redes TCP/IP al problema del ruteo es tener, en cada computadora, tenga la suficiente información para encontrar el camino hasta la salida de su propia red y manejarse paso a paso hasta llegar a destino. Pero muy importante saber que todo este proceso se lleva a cabo mediante un conjunto de protocolos de red y de ruteo.

3.2 Protocolos de red

Los protocolos de red desempeñan una gran variedad de funciones necesarias para la comunicación entre aplicaciones de usuario en dispositivos de origen y destino, y estas funciones pueden variar mucho entre las diversas arquitecturas de protocolos. Los protocolos de red también conocidos como protocolos ruteados son aquellos que se rutean a través de una red. Algunos de dichos protocolos son el protocolo IP (Protocolo Internet), es el encargado de transmitir paquetes desde un host a otro. Además IP proporciona un servicio de entrega que se puede

describir como no fiable o como el mejor posible, porque no existe garantía de entrega. Los paquetes se pueden perder, ser duplicados, sufrir retrasos o ser entregados en un orden distinto al original, pero esos errores surgen sólo cuando las redes subyacentes fallan o cuando los búferes en el destino están llenos.

Posteriormente, el protocolo de ruteado AppleTalk utilizado para interconectar ordenadores Macintosh. El propósito de este protocolo era permitir que varios usuarios compartieran recursos como archivos e impresoras. Los dispositivos que proporcionan estos recursos son los servidores y los que hacen uso de ellos son los clientes; por lo que se puede decir que este protocolo es una de las primeras implementaciones de sistemas distribuidos de conectividad cliente servidor.

NetWare es un NOS (Sistema Operativo de Red) que permite el acceso transparente a archivos y proporciona otros servicios distribuidos de red, entre los que se cuentan el uso compartido de las impresoras y el soporte para las diversas aplicaciones como la transferencia de correo electrónico y el acceso a bases de datos. Además especifica las cinco capas superiores del modelo OSI y, como tal, virtualmente corre en cualquier protocolo de acceso a medios (capa de enlace de datos).

Por otra parte el conjunto de protocolos OSI (Interconexión de Sistemas Abiertos) está compuesto por muchos protocolos estándar basados en el modelo OSI; estos protocolos son parte de un programa internacional para desarrollar protocolos para redes de datos y otros estándares que faciliten la interoperabilidad de equipos de diferentes fabricantes. El programa OSI surgió como respuesta a la necesidad de establecer estándares internacionales de conectividad y está diseñado para facilitar la comunicación entre sistemas de hardware y software a pesar de las diferencias de las arquitecturas en que se basen.

VINES (Servicio de Red Integrada Virtual) utiliza una arquitectura cliente servidor en la que los clientes solicitan determinados servicios a los servidores, como el acceso a archivos e impresoras. El último protocolo ruteado que se hará mención es el XNS (Sistemas de Red de Xerox), que fue diseñado para ser usado en conjunto con una gran variedad de medios de transmisión, procesadores y aplicaciones de oficina.

3.3 Protocolos de ruteo

La responsabilidad del protocolo de ruteo es el intercambio de información, encontrando el camino más confiable para alcanzar el destino deseado teniendo en consideración la distancia, la búsqueda de información en caso de que la conexión falle, recuperación de enlaces caídos gastando el mínimo de potencia de procesamiento y mínimo uso de ancho de banda. Además los protocolos de ruteo son aquellos que implementan algoritmos de ruteo, es decir; los protocolos de ruteo dirigen los protocolos de red a través de una interred. Algunos ejemplos de estos son IGRP (Protocolo de Ruteo de Compuerta Interior), IGRP Mejorado (Protocolo de Ruteo de Compuerta Interior Mejorado), el protocolo OSPF (Algoritmo Abierto de Primero la trayectoria más Corta), BGP (Protocolo de Compuerta Fronteriza), IS-IS (Protocolo de Sistema Intermedio a Sistema Intermedio) y RIP (Protocolo de Información de Ruteo).

En primera instancia el protocolo IGRP (Protocolo de Ruteo de Compuerta Interior) fue diseñado por Cisco Systems y su objetivo primordial era ofrecer un protocolo de ruteo robusto dentro de un AS (Sistema Autónomo). Posteriormente Cisco desarrolló el IGRP Mejorado para mejorar la eficiencia de operación del IGRP, este integra las virtudes de los protocolos basados en estado de enlaces a los protocolos basados en vector de distancia, y ofrece compatibilidad y operación sin barreras con los ruteadores IGRP. Además este protocolo considera las rutas

IGRP como rutas externas y permite que el administrador de la red pueda diseñarlas a la medida.

Por otra parte, el protocolo OSPF (Algoritmo Abierto de Primero la Trayectoria más Corta), analiza los componentes y operación de este protocolo de ruteo de compuerta de enlace interior basado en estado de enlaces; presenta dos características principales, la primera es que es un protocolo abierto, lo que significa que su especificación es de carácter público. La segunda característica es que el OSPF está basado en el algoritmo SPF.

BGP (Protocolo de Compuerta Fronteriza), es un protocolo dedicado a la tarea de determinar la trayectoria en las redes actuales; este desempeña el ruteo entre dominios en las redes que utilizan TCP/IP lo que significa que lleva a cabo el ruteo entre múltiples sistemas autónomos o dominios, e intercambia ruteo e información alcanzable con otros sistemas BGP.

El IS-IS (Protocolo de Sistema Intermedio a Sistema Intermedio), es un protocolo de ruteo jerárquico basado en estado de enlaces de OSI que inunda la red con información de estado de enlaces para construir un panorama consistente de la topología de red.

Por último el RIP (Protocolo de Información de Ruteo). Es un protocolo basado en vector de distancia que utiliza el conteo de saltos como medida, se utiliza ampliamente para el ruteo de tráfico en la red global Internet y es un IGP, lo que significa que realiza el ruteo dentro de un solo sistema autónomo.

Es importante saber en esta investigación como es el mecanismo que permite elegir la ruta por la cual circulará la información, pero esto es posible gracias a los algoritmos de ruteo

3.4 Protocolos LAN

Los protocolos de LAN tienen funcionalidades en los niveles, físico, y enlace de datos, según el modelo de referencia OSI. Algunos de los protocolos de redes utilizados actualmente en las redes de datos son: SSH, HRRP, IRRP, HSRP, RSTP, FTP, Telnet, entre otros. Por lo que a continuación se definirá cada uno muy someramente.

SSH (*Secure SHell*) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

Por otra parte el protocolo HSRP (*Hot Standby Router Protocol*) es un protocolo de enrutamiento de "hot standby", propiedad de Cisco que proporciona una disponibilidad de red de alto desempeño y cambios de topología de red transparentes, evitando en la medida de lo posible la existencia de puntos de fallo únicos en la red. HSRP ofrece tanto rutas de acceso redundantes como equipos redundantes en lugares clave de la red para evitar que cualquier dispositivo cause que los recursos vitales de la red dejen de poder utilizarse.

Posteriormente el protocolo RSTP (*Rapid Spanning Tree Protocol*) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes. RSTP monitorea el estado de todas las trayectorias: si una dirección activa se cae, RSTP activa las direcciones redundantes, configura de nuevo la topología de la red adecuadamente. RSTP es una versión mejorada del STP.

FTP (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de

manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo. El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante puede capturar este tráfico, acceder al servidor, o apropiarse de los archivos transferidos.

Por último, Telnet es un protocolo de red, que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

3.5 Protocolos WAN

Los protocolos WAN tienen funcionalidades de los tres primeros niveles, físico, enlace de datos, y red, según el modelo de referencia OSI. Los protocolos de redes utilizados actualmente en las redes de datos son: RDSI, Frame Relay, ADSL, ATM, y X25. Por lo que a continuación se definirá cada uno muy someramente.

Frame Relay comenzó como un movimiento a partir del mismo grupo de normalización que dio lugar a X.25 y RDSI. Sus especificaciones fueron definidas por ANSI, fundamentalmente como medida para superar la lentitud de X.25, eliminando la función de los conmutadores, en cada salto de la red.

Hasta hace relativamente poco tiempo, X.25 se ha venido utilizando como medio de comunicación para datos a través de redes telefónicas con infraestructuras analógicas, en las que la norma ha sido la baja calidad de los medios de transmisión, con una alta tasa de errores. Esto justificaba los abundantes controles de errores y sus redundantes mecanismos para el control de flujo, junto al pequeño tamaño de los paquetes. En resumen, se trataba de facilitar las retransmisiones para obtener una comunicación segura.

Frame Relay, por el contrario, maximiza la eficacia, aprovechándose para ello de las modernas infraestructuras, de mucha mayor calidad y con muy bajos índices de error, y además permite mayores flujos de información. Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

En la actualidad, X.25 es la norma de interfaz orientada al usuario de mayor difusión en las redes de paquetes de gran cobertura. El servicio que ofrece es orientado a conexión (previamente a usar el servicio es necesario realizar una conexión y liberarla cuando se deja de usar el servicio), fiable, en el sentido de que no duplica, ni pierde ni desordena (por ser orientado a conexión), y ofrece multiplexación, esto es, a través de un único interfaz se mantienen abiertas distintas comunicaciones. El servicio X.25 es un diálogo entre dos entidades ETD Y ECD. Como se ilustra en la siguiente figura.

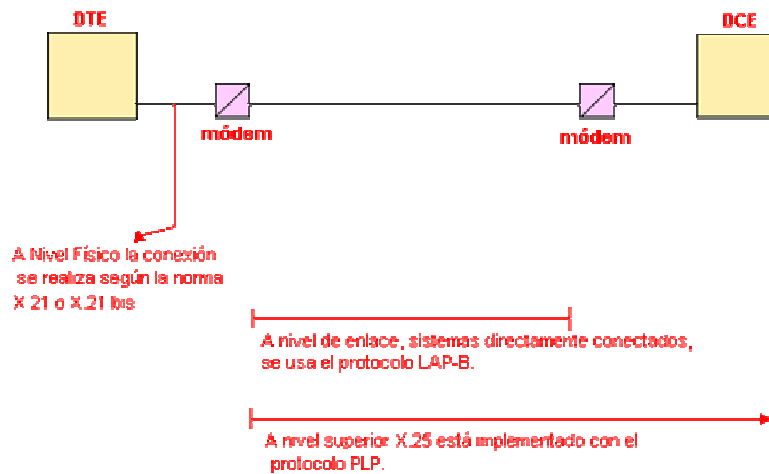


Figura 18. Funcionamiento del protocolo X.25. Tomada de: http://html.redesinformaticas.com/protocolo-de-red-x_25.html

Para que las redes de paquetes y las estaciones de usuario se puedan interconectar se necesitan unos mecanismos de control, siendo el más importante desde el punto de vista de la red, el control de flujo, que sirve para evitar la congestión de la red.

También el ETD ha de controlar el flujo que le llega desde la red. Además deben existir procedimientos de control de errores que garanticen la recepción correcta de todo el tráfico. X.25 proporciona estas funciones de control de flujo y de errores. Además la X.25 se define como la interfaz entre equipos terminales de datos y equipos de terminación del circuito de datos para terminales que trabajan en modo paquete sobre redes de datos públicas.

RDSI (Red Digital de Servicios Integrados) se puede definir como una red que procede por evolución de la red digital integrada (RDI) y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto de interfaces normalizados. Se puede decir entonces que es una red que procede por evolución de la red telefónica existente, que al ofrecer conexiones

digitales de extremo a extremo permite la integración de multitud de servicios en un único acceso, independientemente de la naturaleza de la información a transmitir y del equipo terminal que la genere.

Por otra parte, ADSL (Línea suscriptor digital de abonado) es una técnica de transmisión que, aplicada sobre los abonados de la red telefónica, permite la transmisión de voz y datos a altas velocidades. Para ello utiliza frecuencias más altas que las empleadas en el servicio telefónico y sin interferir en ellas, permitiendo así el uso simultáneo del servicio telefónico y para acceder a servicios de datos a través de ADSL.

Posteriormente, ATM (Modo de Transferencia Asíncrona) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones. Además los conmutadores ATM aseguran que el tráfico de grandes volúmenes es flexiblemente conmutado al destino correcto. Los usuarios aprecian ambas cosas, ya que se cansan de esperar los datos y las pantallas de llegada a sus terminales.

3.6 Algoritmos de ruteo

Se pueden diferenciar a partir de determinadas características fundamentales. Primero, los objetivos particulares del diseñador del algoritmo afectan la operación del protocolo de ruteo resultante. Segundo, hay diferentes tipos de algoritmos de ruteo y cada uno de ellos tiene un impacto diferente en los recursos de la red y del ruteador. Por último, los algoritmos de ruteo utilizan una gran variedad de medidas que afectan el cálculo de las rutas óptimas.¹⁰

¹⁰ FORD, Merilee; SPANIER, Steve; STEVENSON, Tim; LEW, Kim. Tecnologías de Interconectividad de redes. México: Ediciones Pearson, 1998. Pág. 67

Además los algoritmos de ruteo se dividen en dos grupos: estáticos y dinámicos. Los algoritmos estáticos toman las decisiones utilizando información previamente recopilada sobre el estado de la red, en cambio los algoritmos dinámicos utilizan información recopilada en tiempo real sobre el estado de la red que se actualiza constantemente mediante paquetes que intercambian los routers a través de la misma red.

3.6.1 Objetivos de diseño

Los algoritmos de ruteo se diseñan con uno o más de estos objetivos: El diseño óptimo se refiere a la capacidad de un algoritmo de ruteo de seleccionar la mejor ruta, lo cual depende de las medidas y los pesos que se asignen a dichas medidas para realizar el cálculo. Posteriormente están diseñados para que sean lo más simple posible, es decir; el algoritmo de ruteo debe ofrecer su funcionalidad de una manera eficiente, con un mínimo de software y utilización óptima. Además los algoritmos de ruteo deben ser robustos, lo que significa que deben desempeñarse correctamente aun cuando se enfrentan a circunstancias poco comunes e imprevistas, como fallas de hardware, condiciones de carga alta e implementaciones incorrectas. Asimismo los algoritmos de ruteo deben converger rápidamente. La convergencia es el proceso por el cual todos los ruteadores llegan a un acuerdo con respecto a las rutas óptimas. Cuando un evento en la red provoca que las rutas se caigan o estén disponibles, los ruteadores distribuyen mensajes de actualización de ruteo que penetran las redes, estimulando el recalcular de las rutas óptimas y, ocasionalmente, haciendo que todos los ruteadores lleguen a un acuerdo con respecto a esas rutas; y finalmente; los algoritmos de ruteo deben ser flexibles, lo que significa que se deben adaptar rápidamente y con precisión a una gran variedad de circunstancias de la red.

3.7 Métricas de ruteo.¹¹

Las tablas de ruteo contienen información que es utilizada por el software de conmutación para seleccionar la mejor ruta.

La longitud de la trayectoria es la métrica de ruteo más común. Algunos protocolos de ruteo permiten que los administradores de red asignen costos arbitrarios a cada uno de los enlaces de la red; en este caso, la longitud de la trayectoria es la suma de los costos asociados con cada uno de los enlaces por los que se pasa. Otros protocolos de ruteo definen un conteo de saltos, una métrica que especifica el número de veces que un paquete pasa a través de los productos que conforman la red, por ejemplo ruteadores, en su trayecto desde un origen hasta un destino.

La confiabilidad, en el contexto de los algoritmos de ruteo, se refiere a la dependencia de cada enlace de la red. Algunos enlaces de la red pueden caerse con mayor frecuencia que otros. Cuando falla una red, algunos enlaces en la red pueden repararse más fácil o rápidamente que otros. Cualquier factor de confiabilidad se puede tener en cuenta en la determinación del valor de la misma, ya que son valores numéricos arbitrarios asignados generalmente a los enlaces de red por los administradores del sistema.

El retardo de ruteo se refiere al periodo de tiempo que se requiere para transferir un paquete desde un origen hasta el destino a través de la red; el retardo depende de muchos factores entre los cuales se cuenta el ancho de banda de los enlaces intermedios de la red, las colas en los puertos de cada ruteador a lo largo del camino, la saturación de la red en todos sus enlaces intermedios y la distancia física a recorrer.

¹¹ FORD, Merilee; SPANIER, Steve; STEVENSON, Tim; LEW, Kim. Tecnologías de Interconectividad de redes. México: Ediciones Pearson, 1998. Pág. 68

El ancho de banda se refiere a la capacidad del tráfico disponible de un enlace. Si todos los demás parámetros son iguales, sería preferible un enlace Ethernet a 10 Mbps; aunque el ancho de banda es una mediada del rendimiento eficiente total máximo que se puede alcanzar en un enlace, las rutas que pasan a través de enlaces con un ancho de banda mayor no necesariamente son mejores rutas que las que viajan a través de enlaces más lentos.

La carga se refiere a qué tan ocupado está un recurso de la red; la carga se puede calcular de muchas maneras, entre otras la utilización del CPU y el número de paquetes procesados por segundo. La supervisión continua de estos parámetros puede consumir por sí misma muchos recursos.

Los costos de comunicación son otra métrica muy importante, sobre todo porque algunas empresas no les importan tanto el desempeño de una red como los costos de operación de la misma. A pesar de que el retardo de la línea puede ser más grande, enviarán paquetes a través de sus propias líneas en vez de hacerlo por líneas públicas, las cuales tienen un costo asociado en función del tiempo de uso.

[Ver más Información en: FORD, Merilee; SPANIER, Steve; STEVENSON, Tim; LEW, Kim. Tecnologías de interconectividad de redes. México: Ediciones Pearson, 1998. Pág 716]

CAPITULO IV

4. DISEÑO DE REDES

Hoy en día diseñar una red es una tarea un poco complicada debido a la gran variedad de componentes que existen. Por lo que en este documento se darán a conocer las principales metas del diseño de una red, las cuales son prioridades que se adaptan al desarrollo de la red; y aspectos determinantes y útiles al momento de pensar en la realización del diseño de la red, con la finalidad de optimizar, garantizar escalabilizar y reducir costos, para aquellas empresas que desean tener un buen funcionamiento en la red.

1.4 Pasos a tener en cuenta al diseñar una red

- ✓ Tamaño de la red.
- ✓ Topologías a emplear
- ✓ Establecer la lógica del negocio
- ✓ Tipo de negocio.
- ✓ Nivel de seguridad.
- ✓ Nivel de soporte administrativo disponible.
- ✓ Cantidad de tráfico en la red.
- ✓ Necesidades de los usuarios de la red.
- ✓ Presupuesto de la red.

[Ver más información en: Academia de networking de Cisco Systems: Guía del primer año. 2 ed. Pág. 889]

4.2 Diseño de una red

A continuación se darán a conocer algunas preguntas básicas que el diseñador de la red debe siempre preguntarse antes de que empiece la fase del diseño

- ✓ ¿Quién va a usar la red?
- ✓ ¿Qué tareas van a desempeñar los usuarios en la red?
- ✓ ¿Quién va a administrar la red?
- ✓ Igualmente importante ¿Quién va a pagar por ella?

Una vez estas respuestas sean respondidas, las prioridades serán establecidas y el proceso del diseño de la red será mucho más fructífero. Estas prioridades se convertirán en las metas del diseño.

Por lo que a continuación se analizarán algunas metas claves:

4.2.1 Escalabilidad de la red

Las redes están siempre en continuo creciendo; por lo tanto esta es una de las metas más importantes al momento de diseñar una red; el diseñador deberá tener en cuenta el crecimiento de la red en un futuro con el fin de suplir algunas necesidades de las compañías; y a su vez estas no se saturen en un futuro inmediato. Además el diseñador de la red deberá tener en cuenta las siguientes preguntas:

- ✓ ¿Cuántas estaciones de trabajo puede soportar el sistema operativo de red?
- ✓ ¿Si la póliza de precios del vendedor de equipos hace factible la expansión futura?
- ✓ ¿El ancho de banda del medio de comunicación empleado es suficiente para futuro crecimiento de la red?
- ✓ ¿El equipo de comunicaciones tiene puertos disponibles para futuras conexiones?

4.2.2 Desempeño de la red

Los tipos de datos procesados pueden determinar el grado de desempeño requerido; y este se establece de acuerdo al tipo de red a diseñar puesto que el desempeño de la red está directamente relacionado con los costos (desempeño/costo). Se puede decir que existen dos maneras para mejorar el desempeño de la red: aumentar el ancho de banda o hacer que la red sea más eficiente, a través de la tecnología Fast Ethernet, Gigabit Ethernet. La primera hace referencia a una forma de conseguir que la red existente sea más eficiente consiste en añadir algunas características avanzadas, tales como priorización del tráfico. Y la segunda, mejora el rendimiento y elimina los cuellos de botella. Además es una solución para aquellas redes donde se utilicen aplicaciones con mayor ancho de banda o donde haya grandes volúmenes de tráfico.

[Ver más información en: TANENBAUM, Andrew. Redes de computadoras. 3 ed. México: Ediciones Prentice Hall, 1997. Pág 555]

4.2.3 Seguridad de la red

Esta meta algunos diseñadores de red no la tienen mucho en cuenta en el diseño puesto que también está relacionada con los costos. Pero se hace mención de esta porque es una meta muy importante, puesto que se empleará de acuerdo al tipo de negocio para la cual se desea realizar el diseño de red. Por lo tanto el diseñador deberá tener presente las siguientes preguntas:

- ✓ ¿Estarán encriptados los datos?
- ✓ ¿Qué nivel de seguridad en los passwords es deseable?
- ✓ ¿Son las demandas de seguridad lo suficientemente grandes para requerir cable de fibra óptica?
- ✓ ¿Qué tipos de sistema de respaldo son requeridos para asegurar que los datos perdidos siempre puedan ser recuperados?

- ✓ Si la red local tiene acceso a usuarios remotos, ¿Que tipo de seguridad será implementada para prevenir que hackers entren a nuestra red?

4.2.4 Fiabilidad de la red

La fiabilidad esperada de la red es un factor crucial para decidir el diseño de la misma. Para mejorar la fiabilidad se puede usar redundancia en los posibles puntos de fallo de la red. Se distinguen de dos tipos de redundancia: redundancia en medios de transmisión o en equipos

4.2.5 Redundancia en la red

Se emplea más que todo para redes grandes; puesto que sí algún elemento falla, la red por sí misma deberá seguir trabajando. Además el diseñador de la red para emplear redundancia deberá tener en cuenta en primera instancia la lógica del negocio.

4.2.5.1 Redundancia en medios de transmisión o de camino.

Consiste en tener por lo menos dos caminos físicos para llegar al destino, puesto que sí alguno de estos falla, la red por sí misma deberá seguir trabajando. A continuación se observa como es la redundancia en la topología en anillo puesto que esta es la que utiliza redundancia en el cableado.

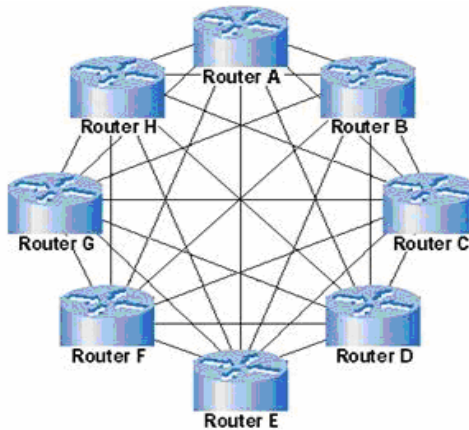


Figura 19. Redundancia en cables. Tomada de:
<http://images.google.com.co/images?gbv=2&hl=es&q=topologias+en+malla>

4.2.5.2 Redundancia en equipos

Consiste en poseer equipos inactivos que puedan sustituir a los que están funcionando en caso de falla. Se puede tener redundancia en el equipo completo o bien en partes del mismo, teniendo en cuenta la lógica del negocio, puesto que la redundancia en la red también está relacionada con los costos. En la siguiente figura se observa que el sistema A no emplea ningún tipo de redundancia a diferencia del segundo sistema B.

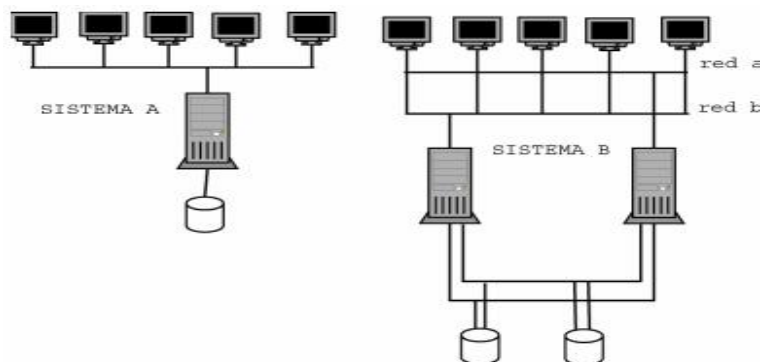


Figura 20. Redundancia en dispositivos. Tomada de:
<http://www.wikilearning.com/imagescc/9756/redundancia.png>

Como se mencionó anteriormente la redundancia se emplea de acuerdo a la lógica del negocio, es decir; si se tienen sistemas críticos que tienen que estar disponibles y funcionando en todo momento, hay que intentar minimizar los fallos que puedan afectar al funcionamiento normal del sistema. Fallos van a ocurrir, pero existen técnicas y configuraciones que ayudan a tener sistemas redundantes, en los que ciertas partes pueden fallar sin que esto afecte al funcionamiento del mismo. Actualmente, existen muchos componentes necesarios para que este funcione, cuantos más componentes, mas probabilidad se tiene que algo falle. Estos problemas pueden ocurrir en el propio servidor, fallos de discos, fuentes de alimentación, tarjetas de red, etc. y en la infraestructura necesaria para que el servidor se pueda utilizar, componentes de red, acceso a Internet, sistema eléctrico entre otros.

4.2.6 Compatibilidad en los dispositivos

Se debe tener en cuenta que tanto hardware como software sean compatibles, tanto hardware como software son una pieza clave también en el diseño de una red. Los sistemas deben ser compatibles para que estos dentro de la red puedan funcionar y comunicarse entre sí, por lo que el diseñador de la red, deberá tener cuidado de seleccionar los protocolos, estándares, sistemas operativos de red, aplicaciones, entre otros.

4.2.7 Compatibilidad entre la organización y la gente

Una vez que la red esté diseñada para ser compatible con el hardware y software existente, sería un gran error si no se considera la organización y el personal de la compañía. A veces ocurre que se tienen sistemas de la más alta tecnología y no se tiene el personal idóneo para utilizar dichos sistemas, o viceversa, se tiene personal con amplios conocimientos y experiencia operando sistemas obsoletos y no tiene la tecnología adecuada.

4.2.8 Costos

El costo que implica diseñar, operar y mantener una red, quizá es uno de los factores por los cuales las redes no tengan la seguridad, redundancia, proyección a futuro y personal adecuado. Por lo que puede ocurrir que las redes se adapten a un escaso presupuesto y todas las metas del diseño anteriores no se puedan implementar. Algunas empresas, muchas veces no tienen idea del alto costo que implica el diseñar una red, que equipos de comunicaciones hay por ejemplo. El costo involucrado siempre será un factor importante para el diseño de una red.

4.3 Normalización

En los primeros inicios de los ordenadores y las redes, las diferentes compañías fabricantes; cada una tenían sus propias arquitecturas y protocolos. Es decir que cada uno desarrollaba sus equipos y los mecanismos de comunicación entre los mismos con tecnología propia, así la comunicación entre dos equipos de diferentes compañías era casi que imposible, no existía un lenguaje común; de esta forma no se podía establecer una red con ordenadores de distintas compañías lo que daba lugar a mercados sujetos, es decir que una vez que se adquiría un ordenador de un fabricante todos los demás debían ser del mismo. Esta restricción provocó la exigencia por parte de los usuarios de que se estableciera una normalización al respecto; la normalización no solamente facilita la comunicación entre equipos construidos por diferentes compañías, sino que también beneficia a los productos que se acogen a la norma ya que el nicho de mercado de dichos productos es mucho más amplio. Se facilita así la producción masiva de equipos, se pueden utilizar técnicas de producción mejores y la tendencia será a disminuir el precio de los productos lo que facilita la penetración de los mismos en el mercado.

CONCLUSIÓN

Para finalizar, se puede decir que las redes son cada vez más indispensables pero sin la interconectividad estas serían un caos ya que la interconectividad en la red sirve para dar servicio de comunicación de datos a los usuarios que lo requieran. Además sirve para aumentar y optimizar los flujos de comunicación, lo cual es de gran ayuda para las grandes redes que necesitan rapidez en cuanto al tráfico de datos.

Por otro lado la arquitectura de red es el medio más efectivo en cuanto a costos para desarrollar e implementar un conjunto de dispositivos que se puedan interconectar; pero para esta interconexión se hace necesaria la presencia de muchos elementos algunos de estos son: los dispositivos y medios de transmisión. Por lo que cabe mencionar que los dispositivos de interconexión de redes han sido un gran avance en la comunicación ya que estos permiten mejorar la comunicación, por que cada uno de estos posee características diferentes que aportan soluciones específicas a la red. Teniendo en cuenta que muchos de estos dispositivos no son compatibles entre sí y por tal motivo hay que tener en cuenta ciertas recomendaciones para no crear conflicto en la red. Asimismo los medios de transmisión es el elemento físico que conecta físicamente las estaciones de trabajo con los servidores y los dispositivos de red. Se pueden usar varios medios físicos para la transmisión real; pero la selección del medio depende de las características de la aplicación en particular ya que cada medio tiene sus propias características costo, facilidad de instalación, ancho de banda, y velocidades de transmisión soportada

Posteriormente la interconectividad de redes es el proceso de comunicación que sucede entre dos o más redes que están conectadas entre sí; asimismo es importante porque permite compartir recursos, el acceso instantáneo a bases de datos compartidas, la insensibilidad a la distancia física y a la limitación en el

número de nodos, permite la administración centralizada de la red y además da una ventaja estratégica en el mercado competitivo global.

Por otra parte el ruteo es el proceso de transferencia de la información a través de una red desde un origen hasta un destino. Pero para que este proceso se pueda llevar a cabo se hace necesaria la presencia de los protocolos de red; estos desempeñan una gran variedad de funciones necesarias para la comunicación entre aplicaciones de usuario en dispositivos de origen y destino, y estas funciones pueden variar mucho entre las diversas arquitecturas de protocolos. Y de los protocolos de ruteo que son aquellos que implementan algoritmos de ruteo, es decir; los protocolos de ruteo dirigen los protocolos de red a través de una interred siendo este un tipo de interconexión de redes.

Hoy en día diseñar una red es una tarea un poco complicada debido a la gran variedad de componentes que existen. Sin embargo al momento que el diseñador de la red vaya a diseñar hay que tener en cuenta quién va a usar la red, qué tareas van a desempeñar los usuarios en la red, quién va a administrar la red, e igualmente importante quién va a pagar por ella, una vez estas respuestas sean respondidas, las prioridades serán establecidas y el proceso del diseño de la red será mucho más fructífero. Estas prioridades se convertirán en las metas del diseño.

Por último, es importante resaltar que las redes no son una ciencia exacta, es decir, que no se tiene un esquema para la realización de la misma, sino cada una se hace diferente, dependiendo la lógica del negocio. Además la tecnología avanza a pasos agigantados no sólo con respecto a las redes sino en todos los campos de la informática. Sólo esperemos que este avance prosiga sin olvidar al hombre como mente creadora y que sin Él todo esto no sería nada.

RECOMENDACIONES

El contenido de la monografía DISEÑO Y ARQUITECTURA DE REDES ENFOCADO EN LA ÍNTERCONNECTIVIDAD, proporciona tanto a estudiantes, docentes, o profesionales dedicados al área de redes y telecomunicaciones una serie de pasos a tener en cuenta al momento de pensar en el diseño de una red; asimismo afianzar algunos conceptos mencionados a lo largo de este documento.

Además como valor agregado a esta investigación se sugiere averiguar e indagar en fuentes distintas a las que contiene este documento, puesto que el tema de esta monografía es bastante extenso, dada a la importancia que hoy en día se le da al diseño de las redes como tal.

Aunque este documento tiene un contenido bastante fructífero se puede complementar con los libros o enlaces que aparecen al final de cada temática.

También se puede investigar un poco más acerca de los dispositivos de interconexión de redes puesto que estos se encuentran en constantes cambios, por lo que tanto proveedores de servicios de Internet o cualquier servicio de montaje de una red, profesionales dedicados a la administración de una red o cualquier persona que necesita estar continuamente actualizado para lograr con éxito su trabajo necesita estar informado acerca de las últimas tendencias de las tecnologías que existan, además este documento será de gran ayuda para aquellas personas que comienzan a explorar el mundo de las redes.

GLOSARIO

ARQUITECTURA DE RED: Las estructuras Hardware y Software que implementan las funciones de comunicación.

APPLETALK: Protocolo de ruteado utilizado para interconectar ordenadores Macintosh.

BGP: (Protocolo de Compuerta Fronteriza) es un protocolo dedicado a la tarea de determinar la trayectoria en las redes actuales.

BRIDGES: Dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

COMPATIBILIDAD: Es la condición que hace que un programa y un sistema, arquitectura o aplicación logren comprenderse correctamente tanto directamente o indirectamente.

DMZ :(Zona Desmilitarizada) se define como una red local que se ubica entre la red interna de una organización y una red externa como Internet.

ETHERNET: Tecnología de redes ampliamente aceptada con conexiones disponibles para PCs, estaciones de trabajo científicas y de alto desempeño.

FIREWALL: Dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra.

GATEWAY: Término inglés que literalmente se refiere a cualquier apertura en una pared que puede cerrarse con una puerta.

HSRP: Es un protocolo de enrutamiento de "hot standby", propiedad de Cisco que proporciona una disponibilidad de red de alto desempeño y cambios de topología de red transparentes, evitando en la medida de lo posible la existencia de puntos de fallo únicos en la red.

IEEE:(Instituto de Ingenieros en Electrónica y Electricidad, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico profesional mundial dedicada a la estandarización, entre otras cosas

IGRP: (Protocolo de Ruteo de Compuerta Interior) fué diseñado por Cisco Systems y su objetivo primordial era ofrecer un protocolo de ruteo robusto dentro de un AS (Sistema Autónomo).

INTERCONECTIVIDAD: Proceso de comunicación el cual ocurre entre dos o más redes que están conectadas entre sí.

INTERRED: Conjunto de redes individuales conectadas por dispositivos intermedios de conectividad de redes que funcionan como una sola gran red.

IP: (Protocolo Internet) es el encargado de transmitir paquetes desde un host a otro.

LAN: Red de datos de alta velocidad, tolerante a fallas, que cubre un área geográfica relativamente pequeña.

MAN: una red de alta velocidad dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo.

MODEM: Es un dispositivo que permite conectar dos ordenadores remotos.

MÚLTIPLEXAJE: es la combinación de múltiples canales de información en un medio común de transmisión de alta velocidad.

NAGIOS: Es un potente y modular sistema de monitorización de red que puede ser usado para monitorizar algunos servicios de red como SMTP, HTTP y DNS en hosts remotos.

NAT: (Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles.

NETWARE: Permite el acceso transparente a archivos y proporciona otros servicios distribuidos de red.

NORMALIZACIÓN: Es la redacción y aprobación de normas que se establecen para garantizar el acoplamiento de elementos construidos independientemente, así como garantizar el repuesto en caso de ser necesario, garantizar la calidad de los elementos fabricados y la seguridad de funcionamiento.

OSI: (Interconexión de Sistemas Abiertos) El modelo de referencia de Interconexión de Sistemas Abiertos lanzado en 1984 fue el modelo de red descriptivo creado por ISO; esto es, un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

OSPF: (Algoritmo Abierto de Primero la trayectoria más Corta) es un protocolo de ruteo, desarrollado para las redes con IP por el grupo de trabajo del IGP (Protocolo de Compuerta Interior) de IETF (Fuerza de Trabajo de la Ingeniería de Internet).

PROTOCOLO: Conjunto de reglas que posibilitan la transferencia de datos entre dos o más computadores.

REDUNDANCIA: Consiste en tener distintos caminos físicos para llegar a un nodo, lo que facilita el cambio de camino ante el fallo en uno de ellos.

RIP: (Protocolo de Información de Ruteo) es un protocolo basado en vector de distancia que utiliza el conteo de saltos como medida.

ROUTERS: Este dispositivo permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

RSTP: Es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes.

RUTEO: Es el acto de transferir información a través de una red desde un origen hasta un destino.

SERVIDOR: Máquina dedicada a la función de intercambio de información dentro de una red LAN, WAN o MAN, bajo ciertos parámetros de restricciones y privilegios.

SNMP: Es un protocolo ampliamente utilizado en la administración de redes para supervisar la salud y el bienestar del equipo de la red, equipo de cómputo y otros dispositivos.

STP: Es un protocolo de red que permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de lazos. STP es transparente a las estaciones de usuario.

TOPOLOGÍA: Mapa en donde se identifican segmentos, puntos de interconexión y los usuarios que van a estar en la red.

VINES: (sistema de red virtual) representaba para algunas personas el patrón más alto en la conectividad interredes y en la seguridad y transparencia de operación.

VPN: (Red privada virtual), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.

VTP: Es un protocolo usado para configurar y administrar VLANs en equipos Cisco. Este opera en 3 modos distintos: cliente, servidor, transparente.

WAN: Son redes que cubren una amplia región geográfica, a menudo un país o un continente. Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales.

BIBLIOGRÁFIAS

COMER, Duglas; STEVENS, David. Interconectividad de redes con TCP/IP: Volumen II diseño e implementación. 3 ed. México: Ediciones Prentice Hall, 2000. Pág. 660

COMER, Duglas. Redes globales de información con internet y TCP/IP: principios básicos, protocolos y arquitectura. 3 ed. México: Ediciones Prentice Hall, 1996. Pág 621

FORD, Merilee; SPANIER, Steve; STEVENSON, Tim; LEW, Kim. Tecnologías de interconectividad de redes. México: Ediciones Pearson, 1998. Pág 716

MOLINA ROBLES, Francisco José. Instalación y mantenimiento de servicios de redes locales. España: Editorial Ra-ma, 2004. 512 p.

TANENBAUM, Andrew. Redes de computadoras. 3 ed. México: Ediciones Prentice Hall, 1997. Pág 813

ABAD DOMINGO, Alfredo. Redes de área local. 3 ed. México: Ediciones McGraw-Hill, 2005. 352 p.

Academia de networking de Cisco Systems: Guía del primer año. 2 ed. Pág. 889

PIÑEROS OROZCO, Karen Cecilia; GONZÁLEZ ZUÑIGA, Darwin. Dispositivos de Interconexión de redes y medios de transmisión. Universidad Tecnológica de Bolívar, Minor en redes y Telecomunicaciones, Facultad de Ingeniería de Sistemas y Electrónica. 2004

Ramírez, A. (2004). Historia de la interconectividad de redes. Edufuturos. [En línea]. N° 36, Recuperado el 5 de junio de 2008, de <<http://www.edufuturo.com/educacion.php?c=4151>>.

Álvarez, Miguel Ángel, (1995, 5 de Mayo). Diseño de redes. Eveliux. [En línea]. N° 85, Recuperado el 3 de junio de 2008, de <http://www.eveliux.com/mx/index.php?option=content&task=view&id=164>

Rivera, N. (2006, 22 de noviembre). Interconexión de redes. Mitecnologico. [En línea]. N° 8, Recuperado 30 de Mayo de 2008, de <<http://www.mitecnologico.com/Main/InterconexionDeRedes>>.

Alcántara, S. (2005 mayo). Tecnologías de interconectividad de redes. [En línea]. N° 36, Recuperado el 5 de junio de 2008, de <<http://biblioteca2.icesi.edu.co/cgi-olub/w21.sh?session=1&infile=details.91007>>

ANEXO 1: Casos prácticos

Proyecto para la realización del Diseño de una red a una entidad Bancaria.

Requerimientos:

- **Cliente:** Entidad Bancaria Las Ameritas
- **Proyecto :** Diseño de un esquema de defensa a profundidad
- **Infraestructura:**
 - ✓ Se cuenta con una red Gigabit Ethernet con 103 PC (50 PC de administración, 25 PC de desarrollo tecnológico, 5 PC de auditoria, 10 PC de operaciones bancarias, 7 PC de Call Center 6 PC de command center(centro de comando para la seguridad física de la corporación)), una granja de servidores compuesta por 2 equipos de alto rendimiento con sistema operativo Windows 2003 Server en Cluster estos se encargan de la gestión de los servicios de red (Exchange Server, DHCP Server, Authentication Server, Active Directory, DNS Server)
 - ✓ Se cuenta con 9 servidores de acceso publico:
 - ✓ 3 servidores Web (Apache) montados sobre Windows 2003 Server en Cluster, en estos servidores se encuentran alojadas las aplicaciones de operación bancaria internas a la entidad para su uso dentro de la Extranet de la corporación.
 - ✓ 3 servidores de base de datos (Oracle 9i) montados sobre Windows 2003 Server en Cluster, en estos servidores contienen la información correspondiente a todos los movimientos de la empresa (clientes, cuentas, movimientos, créditos, etc...)
 - ✓ 2 Cisco Access Server AS2511-RJ para la realización de operaciones remotas
 - ✓ Un CheckPoint VPN Server para acceso remoto por parte de los empleados remotos y transacción de información entre las diferentes

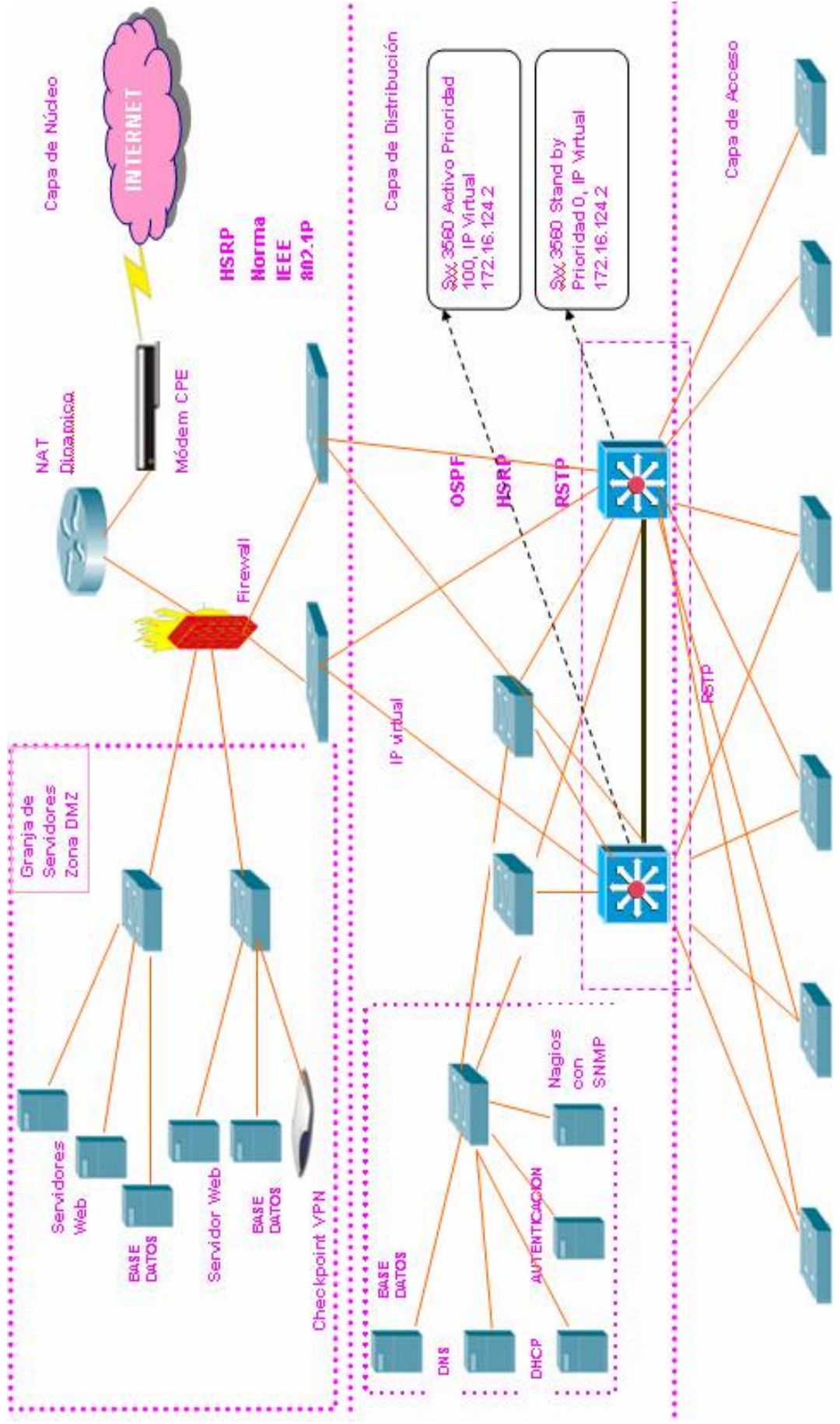
entidades con las que se tiene convenio (DIAN, superintend/encia bancaria, contraloría general de la nación, entidades bancarias extranjeras, etc...).

- ✓ Se cuentan con licencias de las siguientes aplicaciones:
- ✓ Microsoft Windows 2003 Server (Para los servidores privados y públicos)
- ✓ Microsoft Windows XP SP1 (Para las estaciones de trabajo excepto el command center y 5 equipos de desarrollo tecnológico)
- ✓ Linux Red Hat 9.0 (para el command center)
- ✓ Linux White Box (para 20 equipos de desarrollo tecnológico)
- ✓ Microsoft Internet Security and Acceleration (ISA) Server Enterprise Edition (no ha sido usado)
- ✓ Se cuenta con switches Catalyst 3550 y 2950
- ✓ Se cuenta con enrutadores Cisco 2621 y 3620
- ✓ La corporación cuenta con 130 empleados de los cuales 103 tienen acceso a los PC e Internet , el 40% de estos esta de desactualizado en mecanismos para seguridad de la información, 15% de estos desconoce los mecanismos para seguridad de la información y un 45% esta actualizado y conoce los mecanismos para seguridad de la información.
- ✓ Se cuenta con el siguiente rango de direcciones publicas 200.21.130.1/24 – 200.21.130.20/24

- **La entidad requiere un replanteamiento de su esquema de defensa a profundidad con los siguiente requerimientos:**

- ✓ El diseño del perímetro y la red interna deberá contar con las características básicas para el desarrollo de un modelo de defensa a profundidad.
- ✓ Se deberá crear un plan para adecuar el factor humano a los requerimientos mínimos de seguridad que exige una corporación bancaria.

- ✓ Se requiere la creación de zonas de seguridad bien definidas según la función de los equipos y su grado de importancia para el proceso productivo de la corporación.
- ✓ Se requiere la implementación VLAN dentro de la red interna y en el perímetro de ser necesario.
- ✓ Se requiere la implementación de subredes para las VLAN pertenecientes a la red interna basados en la dirección IP de red 172.16.0.0/ 16.
- ✓ Se requiere un sistema de filtrado de tráfico de altas prestaciones, adaptabilidad y administrabilidad.
- ✓ Se requiere un sistema de notificación de tráfico no deseado con posibilidades de detección en dos sentidos y mútizonas.
- ✓ Se requiere un control de salida a Internet basado en roles y tipo de tráfico.
- ✓ Se necesita un sistema de aceleración de tráfico Web para los usuarios de la red interna.
- ✓ El sistema de seguridad perimetral debe garantizar altos niveles de disponibilidad (alta tolerancia a fallos).
- ✓ Una de las exigencias de la organización es diseñar con base en las plataformas y paquetes informáticos con los que cuenta la misma. En caso de ser necesario se cuenta con un presupuesto de \$15.000 U.S., para la adquisición de los dispositivos deberá realizar un análisis técnico en relación de Costo/Beneficio como mínimo con 3 fabricantes y 3 proveedores.



4.4.1 Análisis técnico: CASO I

Capa de acceso

Se utilizaron seis switches Catalyst 2960G-24TC, con la finalidad de que si se cae alguno no se paralizarán totalmente las actividades de la entidad bancaria; además cada switch es responsable de las dependencias asignadas en el diseño. El protocolo utilizado en esta capa fue el RSTP puesto que se utilizaron switches Cisco, además este protocolo reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología, además gestiona enlaces redundantes; también monitorea el estado de todas las trayectorias, es decir, si una dirección activa se cae, RSTP activa las direcciones redundantes.

Capa de distribución

Para el desarrollo de la capa de distribución se utilizaron dos switches Cisco Catalyst 3560G-24TS de 24 puertos, los cuales están conectados entre sí a través de un enlace resilient, con la finalidad de que el tráfico se mantenga fluyendo por medio del enlace activo, mientras que el segundo enlace permanece en standby para que al momento en que ocurra una falla en el enlace activo o primario, este enlace standby se activa de manera de que el tráfico fluya normalmente.

En esta capa se utilizará el protocolo HSRP el cual es un protocolo de enrutamiento de "hot standby", propiedad de Cisco que proporciona una disponibilidad de red de alto desempeño y cambios de topología de red transparentes, evitando en la medida de lo posible la existencia de puntos de fallo únicos en la red. HSRP ofrece tanto rutas de acceso redundantes como equipos redundantes en lugares claves de la red, para evitar que cualquier dispositivo cause que los recursos vitales de la red dejen de poder utilizarse.

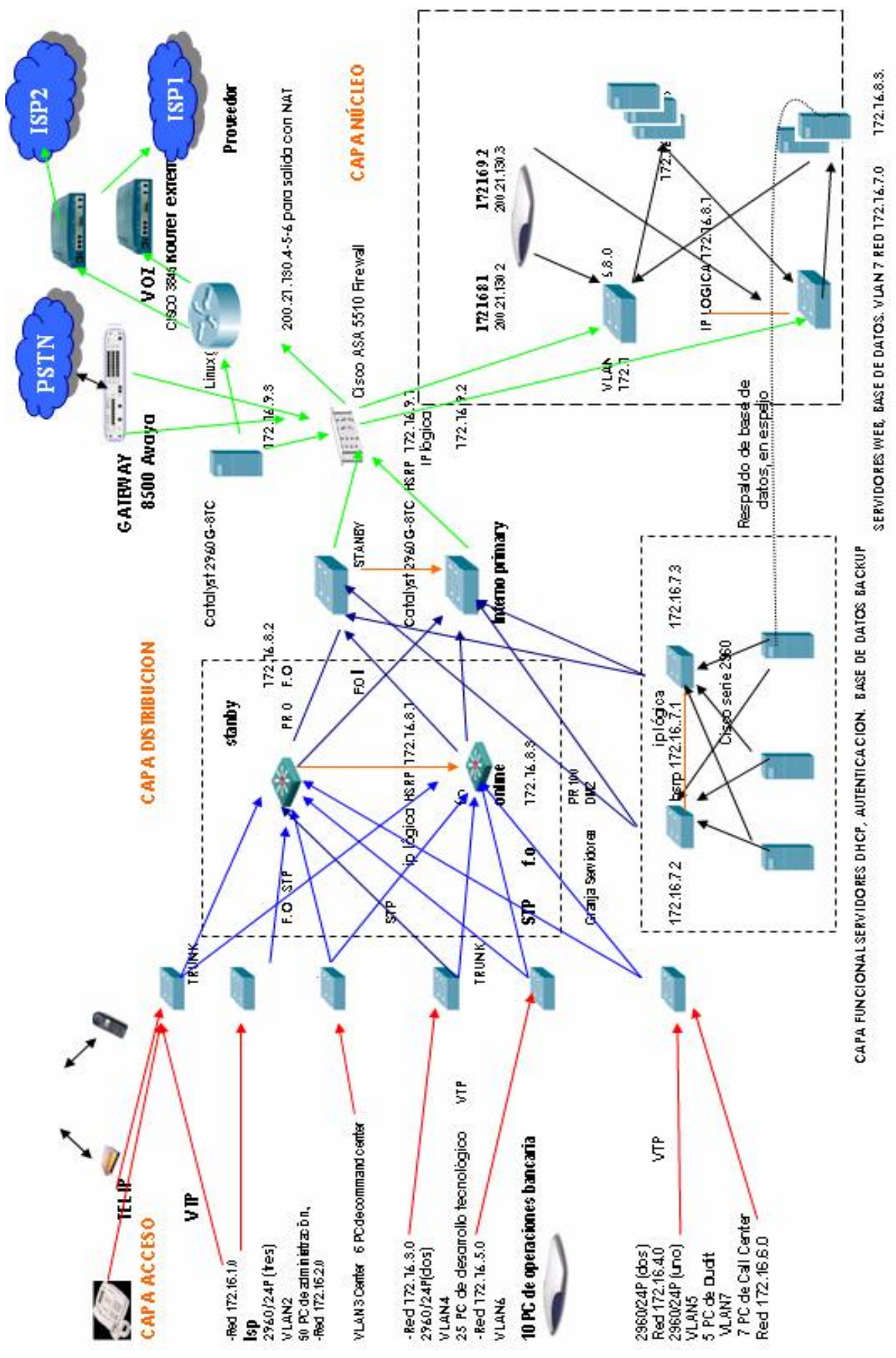
Además, en uno de los switches se conectó un servidor que posee un software Nagios con el protocolo SNMP, el cual sirve para administrar y monitorear colocándole una dirección estática, es decir, los usuarios tienen acceso a lo que el administrador de la red disponga, por seguridad de la red. Cabe resaltar que estos dos switches capa 3 están interconectados a dos switches capa 2 que a su vez se encuentran conectados mediante enlaces redundantes o resilient a los servidores de autenticación, base de datos, DNS y DHCP.

Capa de núcleo

En la capa de núcleo se colocaron dos switches de alto rendimiento enlazados redundantemente, a los switches capa 3 que están en la capa de distribución; los switches de alto rendimiento se conectan a un firewall de Cisco PIX 501 de 4 puertos - EN, Fast EN PIX-501-BUN-K9. El firewall se conecta con un Router Cisco 2851 Security Bundle y dos switches que se encuentran dentro del DMZ, este permite ubicar los servidores públicos como los servicios de e-mail, publicación Web entre otros, en una zona específica destinada a ubicar servicios accesibles directamente desde Internet, por estar destinados a éste fin. Posteriormente en la DMZ hay 3 servidores web y 2 de base de datos, los cuales están conectados a dos switches capa dos para poder llevar el servicio a las dependencias autorizadas. Asimismo se utilizó un Checkpoint VPN, esto es particularmente útil para las empresas que desean conectarse a la administración de impuestos en Colombia (DIAN).

Además un Módem (CPE) que es un equipo que se le proporciona al cliente. Está equipado para conexiones para el PC y el teléfono. Su tamaño es muy similar a un Módem ADSL.

Por otro lado se utilizó el NAT el cual es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos Redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados.



4.2.2 Análisis técnico: CASO II

Capa de acceso a la red

Se utilizaron seis switches Cisco Catalyst 2960 Series con LAN Base de software 24/Ptos Ethernet 10Base-T y Ethernet 100Base-TX. Dentro de sus características técnicas incluye Network Admisión Control (NAC), avanzada calidad de servicio (QoS), y la resistencia, para ofrecer servicios inteligentes de la red de borde. La seguridad de la red a través de una amplia gama de métodos de autenticación, cifrado de datos tecnologías, y el NAC sobre la base de usuarios, puertos y direcciones MAC. Soporta STP. Transfiere sus datos, en 100Mbps con un modo de comunicación semiduplex; Memoria Flash de 8 MB, los protocolo que maneja son el ethernet, fase- ethernet a velocidades de cable. Entre los protocolos de gestión remota que manejan se encuentran el SNMP, RMON, Telnet, HTTP; y su garantía es limitada de por vida. Para la administración de las Vlan se utilizó el protocolo VTP, se calcularon las subredes por Vlan, se instalaron equipos wireless de Voz IP en capa de acceso con el fin que los usuarios que puedan aprovechar la flexibilidad de la red de voz, la redundancia hacia la capa de distribución se realizó con enlaces resailing; apoyados del protocolo *spaning tree* (STP).

Capa de distribución

Esta formada por 2 Switches Cisco Catalyst 3560E-24TD capa tres fabricados por cisco, cantidad de puertos: 24 x Ethernet 10Base-T, Ethernet 100Base-TX, Ethernet 1000Base-T, con una Velocidad de transferencia de datos de 1 Gbps, los Protocolo de interconexión de datos que maneja son Ethernet, Fast Ethernet, Gigabit Ethernet,.Además posee 128 Mb y de memoria Flash 64 MB, el enrutamiento entre las VLANs y subredes por medio del protocolo OSPF, por ser un protocolo de información de enrutamiento que no necesita estar actualizando periódicamente las tablas de enrutamiento a sus vecinos. El protocolo encargado para la tolerancia a fallos es un protocolo creado por Cisco. Este protocolo se denomina HSRP el cual permite la eliminación de lo diferentes puntos únicos de

fallo en el entorno del encaminamiento de la red, es decir que a través de la implementación de este protocolo se aumenta la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. Por ello el objetivo principal de implementar este protocolo en este sistema de red, es porque brinda un esquema eficiente de soporte ante eventuales fallos que se puedan presentar.

En la capa de distribución del modelo jerárquico de 3 capas, el Switch de nombre Online, se configurará con una prioridad de 100, nodo activo, y prioridad 50 a el switch o nodo Stanby, con el fin de definir cual de los dos switch esta soportando el trafico principal. Default gateway de los terminales finales que hacen parte de la capa de acceso, en el diseño de la red construida el gateway de las terminales de la capa de acceso, corresponde a la IP 172.16.8.1. , con el fin que la capa de acceso al momento que se realice la conmutación al switch stanby en una salida de servicio del switch online, estos puedan seguir trabajando sin ningún tipo de afectación de trafico. Para el manejo de la calidad de servicio utilizamos el protocolo de IEEE 802.1P de priorización de trafico, para garantizar calidad de servicio a las aplicaciones que lo requieran de acuerdo a la lógica del negocio.

Capa del Núcleo

Para el diseño del núcleo se utilizó un router externo o de borde, un firewall y dos switches interno. En primera instancia, tanto para EL router externo como para los internos, se utilizaron dispositivos Catalyst 2960G-8TC. Se utilizó NAT dinámico para salida a Internet con tres direcciones IP validas. Se accesarán a los servidores web por medio de las políticas o ACL configurados en el firewall, de forma que desde Internet se puedan realizar peticiones a URL con direcciones públicas asignadas, pero que al momento de entrar en la zona DMZ se realicen translaciones de direcciones válidas a privadas.(NAT firewall natural). El

cortafuego o firewall a utilizar es el Cisco ASA 5510 Firewall edition, por tener una capacidad del cortafuegos de 300 Mbps, una tasa de conexiones de 6000 sesiones bps una memoria RAM instalada de 256 MB y una flash instalada de 64 MB flash. Para el diseño es necesario conocer la lógica del negocio con el fin de politizar el firewall de forma que no se vea afectado las labores de los empleados a causa de una configuración errónea.

Posteriormente, dentro de esta capa de distribución también se encuentran ubicada la granja de servidores la cual esta conformada por dos switches con las siguientes características: Modelo: Cisco Catalyst 2960 serie con LAN base de software24/Ptos. La granja de servidores se encuentra conformada por un cluster de servidores de alto rendimiento, este sistema es la unión de los 2 servidores encargados de la gestión de servicios de red como lo son el DHCP y DNS Server, Exchange y Autenticación Server, Active Directory, entre otros. Este cluster se creó con el fin de que le brinde a la red de la empresa alto rendimiento, alta disponibilidad, equilibrio de carga y escalabilidad. Además al igual que los switches multicapa descritos con anterioridad, se manejará soporte a falla a través del protocolo HSRP.

Por otra parte se encuentra la granja de servidores y aplicaciones web, las cuales manejan todos los accesos y consultas web a los aplicativos de la empresa, se realizó un enlace espejo entre los servidores de base datos de la parte web con los servidores de la base de datos interna. Además la salida a Internet se realiza por medio de NAT dinámico, con el fin de aprovechar las IP entregadas por el proveedor de Internet, en los router de salida a Internet se manejó IP policy para realizar balanceo de carga de la salida a Internet, como también en caso de falla de algún proveedor. Para la solución de telefonía IP se utilizó un gateway Avaya 8500 el cual se encuentra ubicado en la capa de núcleo conectado a la salida de Internet y a la red interna.