UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERIA

REINGENIERIA DE UNA RED DE DATOS DE SERVICIO MULTIPLE

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO ELECTRICO – ELECTRÒNICO

P R E S E N T A:

ALMA LINDA DIAZ ORTEGA
CHRISTIAN YAIR CONTRERAS FALCÒN

TUTOR: ING. ALEJANDRO SOSA FUENTES

MÉXICO, D.F. **2009**

DEDICADA:
A MI MAMI
SRA ELOY ORTEGA
A MI PAPI ING. JAIME DIAZ
A MIS HERMANOS
ADRIANA, JAIME, JAVIER

ALMA LINDA DIAZ ORTEGA

AGRADECIMIENTOS

Quiero agradecer a la Universidad Nacional Autónoma de México, a la Facultad de Ingeniería por la oportunidad y apoyo brindado durante toda mi formación académica.

Agradezco a mi tutor de tesis Ing. Alejandro Sosa Fuentes por la disponibilidad y dirección en el presente trabajo.

A los miembro del jurado Ing. Rodolfo Arias Villavicencio, Dra. Fátima Moumtadi, Ing. Jesús Reyes García, Ing. Héctor Raúl Mejía Ramírez, por su incondicional apoyo.

Al Ing. Víctor Cid Castillo por las enseñanzas y asesoramiento en el campo de las redes.

A mis padres y mis hermanos por darme la estabilidad emocional, económica y por confiar siempre en mi, definitivamente no hubiese podido ser realidad sin ustedes. Madre, serás siempre mi inspiración para alcanzar mis metas.

A mis tíos y primos Ezequiel, Ebelia, Estela, Silvestre, Celia, Octavio, Pepe, Alfredo, Brenda y Diana por hacerme sentir feliz y con fuerza.

A mis amigos Jonathan, Christian, Luís, Gaby, Jose, Ivonne, Miguel y Roberto por ayudarme a crecer y madurar como persona y por estar siempre conmigo apoyándome.

ALMA LINDA DIAZ ORTEGA

DEDICADA:
A MI MAMÁ
SRA SANTA TERESITA FALCÓN
A MI PAPÁ SR. JULIO
CONTRERAS
A MI HERMANA Y SOBRINOS
NALLELY, DIDIER, HECTOR

CHRISTIAN YAIR CONTRERAS FALCÓN

AGRADECIMIENTOS

Quiero agradecer a la Universidad Nacional Autónoma de México, a la Facultad de Ingeniería por la oportunidad y apoyo brindado durante toda mi formación académica.

Agradezco a mi tutor de tesis Ing. Alejandro Sosa Fuentes por la disponibilidad, paciencia y dirección en el presente trabajo.

A los miembro del jurado Ing. Rodolfo Arias Villavicencio, Dra. Fátima Moumtadi, Ing. Jesús Reyes García, Ing. Héctor Raúl Mejía Ramírez, por su incondicional apoyo.

Al Ing. Víctor Cid Castillo por las enseñanzas y asesoramiento en el campo de las redes.

A mis padres y hermana por darme la estabilidad emocional, económica y por confiar siempre en mí, definitivamente sin su apoyo este sueño no hubiese podido ser realidad. Mamá y Papá, siempre serán mi inspiración para alcanzar mis metas y ser mejor cada día.

A mis tíos y primos por brindarme su apoyo y hacerme sentir feliz y con fuerza.

A mis amigos Alma y Miguel por ayudarme a crecer, a creer en la amistad, a madurar como persona y por estar siempre conmigo apoyándome.

CHRISTIAN YAIR CONTRERAS FALCÓN

INDICE

INTRODUCCION

Desde tiempos muy remotos el hombre siempre ha tenido una gran necesidad de comunicarse entre si, esta necesidad ha venido evolucionando ya que primero fueron las señales de humo, pinturas rupestres, después el papel y la tinta, hasta que surgió un medio mucho mas poderoso tanto para almacenar información como para transmitirla, estos son los microprocesadores o CPU como se les conoce actualmente.

Durante el siglo XX y los comienzos del XXI la tecnología clave ha sido la recolección, procesamiento y distribución de información. Entre otros desarrollos, hemos asistido a la instalación de redes telefónicas en todo el mundo, a la invención de la radio y la televisión, al nacimiento y crecimiento sin precedente de la industria de las computadoras, así como a la puesta en orbita de los satélites de comunicación. A medida que crece nuestra habilidad para recolectar, procesar y distribuir información, la demanda de más sofisticados procesamientos de información crece todavía con mayor rapidez.

La industria de las computadoras ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener una sola computadora para satisfacer todas las necesidades de calculo de una organización, institución o empresa se esta reemplazando con rapidez por otro que considera un numero grande de computadoras interconectadas, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de computadoras.

Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas. Se utilizaron líneas telefónicas, ya que estas permitían un traslado rápido y económico de los datos. Se utilizaron procedimientos y protocolos ya existentes para establecer la comunicación y se incorporaron moduladores y demoduladores para que, una vez establecido el canal físico, fuera posible transformar las señales digitales en analógicas adecuadas para la transmisión por medio de un modem.

Posteriormente, se introdujeron equipos de respuesta automática que hicieron posible el uso de redes telefónicas publicas conmutadas para realizar las conexiones entre las terminales y la computadora.

A principios de los años 70 surgieron las primeras redes de transmisión de datos destinadas exclusivamente a este propósito, como respuesta al aumento de la demanda del acceso a redes a través de terminales para poder satisfacer las necesidades de funcionalidad, flexibilidad y economía. Se comenzaron a considerar las ventajas de permitir la comunicación entre computadoras y entre grupos de terminales, ya que dependiendo de el grado de similitud entre computadoras es posible permitir que compartan recursos en mayor o menor grado.

Las redes en general, consisten en “compartir recursos”, y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 kilómetros de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. Por ejemplo todos los archivos podrían duplicarse en dos o tres maquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias. Además la presencia de múltiples CPU significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Una red de computadoras no solo se compone de CPU sino también de otros dispositivos electrónicos (routers, switches, bridges, etc.) que ayudan a una mayor eficiencia en la transmisión de información, lo cual origina que estas sean cada vez mas complejas en cuanto a su funcionamiento y puede provocar una posibilidad mayor de tener errores en el envío de información, para esto se hace uso de protocolos de enrutamiento los cuales le dicen a los equipos que conforman la red por donde deben enviar la información .

Hoy en día las redes pueden llegar a ser tan complejas como nuestras necesidades nos lo marquen lo cual trae consigo algunos problemas para efectuar la transmisión de información, referente a la saturación de enlaces, problemas con el enrutamiento, mayor tiempo de convergencia, saturación del ancho de banda debido al crecimiento del numero de usuarios y crecimiento de los nodos de la red.

En esta tesis consideramos una red cuyas características nos brinda la oportunidad de analizarla y redisenarla ya que esta red actual no cumple con las características necesarias para el buen funcionamiento ya que tiene una mala administración, no utiliza un sistema redundante el protocolo de enrutamiento no esta aplicado en su totalidad ya que el direccionamiento no permite sumarizaciones, no es escalable durante un tiempo considerable y el ancho de banda es muy limitado.
Por todas estas características de esta red actual proponemos una reingeniería que me permita tener una buena administración de la red, que el direccionamiento y el protocolo propuesto cumpla con los requerimientos futuros, calcular el ancho de banda requerido tomando en cuenta usuarios futuro y utilizando un sistema redundante.

A lo largo del desarrollo de la tesis determinamos que cambios tenemos que realizar para rediseñar la red actual.

Nuestra tesis consta de 5 capítulos, los cuales nos dan las herramientas necesarias para realizar la reingeniería de la red actual que nos brinde una buena administración y oportunidad de crecimiento futuro.

En el primer capitulo se explicarán a detalle los conceptos básicos necesarios que se utilizarán para entender como se realizará la reingeniería.

En el segundo capitulo analizamos el estado actual de la red y realizamos un diagrama completo de la topología de la red actual, especificando sus características y explicando la problemática que se presenta en dicha red.

En el tercer capitulo analizamos la propuesta de solución, realizamos los cambios necesarios para efectuar la reingeniería en cuanto a direccionamiento, protocolo de enrutamiento, cambio de equipos, redundancia, balanceo de carga, con la cual obtuvimos el diagrama de la red propuesta y además efectuamos el análisis de Costo-beneficio.

En el cuarto capitulo realizamos el proceso de implementación en el cual decidimos como se realiza la instalación de los equipos y enlaces además de explicar como se realiza el cambio de direccionamiento.

El quinto capitulo son las conclusiones en las cuales se explica las ventajas de la reingeniería y además la experiencia obtenida a lo largo de esta tesis.

CONCEPTO GENERAL DE REINGENIERÍA

La reingeniería requiere que los procesos fundamentales sean observados desde la satisfacción del cliente.

Para adoptar este concepto, se tiene que estar abierto a cambios drásticos que nos lleve a ser más eficiente un servicio, también se puede ver como comenzar de nuevo o el abandono de viejos procedimientos y la búsqueda de nuevos procesos para brindar un mejor servicio.

La reingeniería se basa en crear procesos que agreguen el mayor valor a la empresa.

Estas palabras son claves:

1. Una reingeniería buscará el porqué se está realizando
2. Los cambios en el diseño deberán ser radicales (desde la raíz y no superficiales).
3. Las mejoras esperadas deben ser dramáticas (no de unos pocos porcentajes).
4. Los cambios se deben enfocarse únicamente sobre los procesos.

Se puede decir que una reingeniería es un cambio dramático en el proceso y que como efecto de esto se tendrá un rompimiento en la estructura y la cultura de trabajo. La gente tiene que acceder a deshacerse de las anticuadas reglas y suposiciones básicas de los procesos en la organización.

El objeto de la reingeniería lo constituyen aquellos procesos que son a la vez estratégicos y de valor agregado.

En general solo el 50% de los procesos son estratégicos y agregan valor.

La reingeniería se mide en términos de resultados del negocio, incremento de rentabilidad, participación del mercado, ingresos y rendimiento sobre la inversión.

La reingeniería en general debe ser rápida porque los ejecutivos esperan resultados en tiempos muy cortos, además debe ser radicales para que logren resultados notables y sorprendentes. Además debe rediseñar los procesos que agreguen valor y desechar los demás.

La reingeniería no es reparar o mejorar lo que ya existe para que funcione mejor, lo que pretende la reingeniería es abandonar los procedimientos establecidos y examinar nuevamente el trabajo que se requiere para crear el producto o servicio y entregar un producto que cumpla con los requisitos exigidos por el cliente. La reingeniería también implica rediseñar esto es volver a empezar e inventar una manera mejor de hacer el trabajo, haciendo un lado sistemas viejos y empezando de nuevo, con esto hay mejoras espectaculares en costos, calidad, servicio y rapidez.

La reingeniería empieza sin ningún concepto previo, es decir, se concentra en lo que se pretende lograr y como es la manera óptima de lograrlo.

Se debe apelar a la reingeniería únicamente cuando exista la necesidad de cambiar todo y empezarlo de nuevo. Debido a esto es que la reingeniería apunta a una visión global de lo que se quiere obtener como resultado.

Debido a que la red actual no cumple con las características necesarias para el buen funcionamiento ya que tiene una mala administración, no utiliza un sistema redundante no es escalable durante un tiempo considerable y el ancho de banda es muy limitado.
Se tiene que realizar una reingeniería ya es la única manera de obtener los resultados deseados y la satisfacción del cliente.
Este cambio nos brinda el tener una buena administración de la red, un direccionamiento eficiente, que el protocolo y el ancho de banda propuesto cumpla con los requerimientos futuros.

Capitulo l. Conceptos básicos de redes de datos.

1.1 Concepto de Red de Datos

Una red de datos es una agrupación de computadoras, impresoras, routers, switches y dispositivos que se pueden comunicar entre si a través de un medio de transmisión, es una conexión de equipos de manera intrincada. La interconexión tiene como finalidad transmitir y compartir información, recursos, espacio en disco, conexión paralela de equipos (Figura 1.1). Su ventaja es el acceso a equipos que están separados incluso a grandes distancias, y el acceso se da de forma casi instantánea.

Las redes de datos surgieron como una necesidad que las empresas tenían para compartir archivos o información entre sus equipos. Las empresas tenían computadoras que eran dispositivos independientes que no se comunicaban con las demás computadoras, se vio que esta no era una manera eficiente ni rentable para operar en el medio empresarial, entonces se dieron cuenta que podían ahorrar mucho dinero y aumentar su productividad con la tecnología *Networking*, esto llevo a que las empresas tuvieran su propia red, pero surgió el problema de que cada empresa usaba una tecnología diferente de *hardware* y *software* lo cual era un factor muy importante de incompatibilidad e hizo que se volviera cada vez mas difícil la comunicación entre redes que usaban distintas especificaciones.

Una de las primeras soluciones a estos problemas fue la creación de *redes de área local (LAN – Local Area Network)*. Las cuales permitían conectar todas las estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos ubicados dentro de un mismo edificio, las *LAN* permitieron que las empresas utilizaran la tecnología informática para compartir de manera eficiente archivos e impresoras. A medida que el uso de computadoras en las empresas aumentaba, pronto se vio como resultado que las *LAN* no eran suficientes y además cada departamento o empresa, era una especie de isla electrónica.

Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino de una empresa a otra. Entonces, la solución fue la creación de *redes de área metropolitana (MAN – Metropolitan Area Network)* y *redes de área amplia (WAN – Wide Area Network).* Las *WAN* podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias.

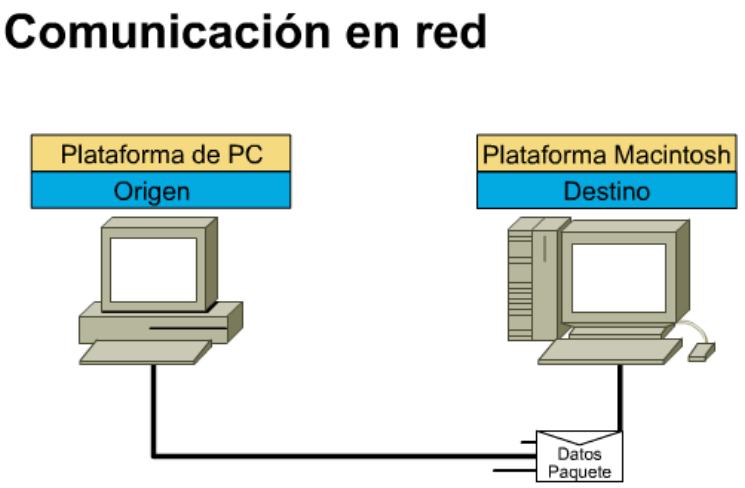


Fig.1.1 Se muestra como se realiza la comunicación de paquetes entre 2 equipos (hosts)

1.2 Modelo de Referencia OSI (Open Systems Interconection)

A mediados de los 70 diversos fabricantes desarrollaron sus propios sistemas de redes locales. El principal inconveniente de estos sistemas de comunicación en red fue que cada uno de ellos era propietario de una empresa particular, siendo desarrollados con hardware y software propios. Como consecuencia de esto, la comunicación entre computadoras pertenecientes a distintas redes era imposible. Para que se pudiera comunicar redes situadas en diferentes lugares, con implementaciones particulares, necesitaban salir de sistemas de networking propietarios, se optó por una arquitectura de red con un modelo común que hiciera posible interconectar varias redes sin problemas.

Para solucionar este problema, la Organización Internacional para la Normalización (ISO) realizó varias investigaciones acerca de los esquemas de red. La ISO reconoció que era necesario crear un modelo que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, elaboraron el modelo de referencia OSI en 1984. Este modelo proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial.

Los fabricantes consideran que es la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

La división de las funciones de *networking* se denomina *división en capas*. Si la red se divide en estas siete capas, se obtienen las siguientes ventajas:

- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.

- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, para que se puedan desarrollar con más rapidez.
- La comunicación de la red se divide en partes más pequeñas y sencillas que permiten simplificar el aprendizaje.

Esta división en 7 capas la podemos ver con más detalle en la Figura 1.2.

Figura1.2. Modelo OSI dividido en siete capas cada una desarrollando funciones distintas.

Capa 1: Capa Física

La capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son movidos. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares se definen a través de las especificaciones de la capa física. Sus principales funciones se resumen en:

- Definir las características físicas (componentes y conectores mecánicos) y eléctricas (niveles de tensión).
- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).
- Transmitir el flujo de bits a través del medio.
- Manejar voltajes y pulsos eléctricos.
- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.
- Garantizar la conexión, pero no la fiabilidad de esta.

Para recordar más rápidamente a esta capa podemos pensar en señales y medios.

Capa 2: Capa de Enlace de Datos

La capa de enlace proporciona sus servicios a la capa de red, suministrando un transito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico), la topología de red, el acceso a la red, la notificación de errores, formación y entrega ordenada de tramas y control de flujo. Por lo tanto, su principal misión es convertir el medio de transmisión en un medio libre de errores de cualquier tipo. Sus principales funciones son:

- Establecer los medios necesarios para una comunicación confiable y eficiente entre dos maquinas en red.
- Agregar una secuencia especial de bits al principio y al final del flujo inicial de bits de los paquetes, estructurando este flujo bajo un formato predefinido llamado trama o marco.
- Sincronizar el envió de las tramas, transfiriéndolas de una forma confiable libre de errores. Para detectar y controlar los errores se añaden bits de paridad, se usan Códigos Cíclicos Redundantes y envió de acuses de recibo positivos y negativos, y para evitar tramas repetidas se usan números de secuencia en ellas.
- Enviar los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Controlar la congestión de la red.
- Regular la velocidad de tráfico de datos.
- Controlar el flujo de tramas mediante protocolos que prohíben que el remitente envíe tramas sin la autorización explicita del receptor, sincronizando así su emisión y recepción.
- Se encarga de la secuencia del enlace lógico y de acceso al medio (soportes físicos de la red).

Para recordar más rápidamente a esta capa podemos pensar en tramas y control de acceso al medio.

Capa 3: Capa de Red

La capa de red proporciona sus servicios a la capa de transporte, siendo una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Se ocupa de aspectos de confiabilidad de paquetes.

Es la responsable de las funciones de conmutación y enrutamiento de la información, proporcionando los procedimientos precisos necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red, con objeto de determinar la ruta más adecuada.
Las funciones de esta capa se pueden resumir en los siguientes puntos:

- Dividir los mensajes de la capa de transporte en unidades mas complejas, denominadas paquetes, y los ensambla al final.

- Conocer la topología de la subred y manejar el caso en que la fuente y el destino están en redes distintas.
- Envía la información a través de la subred, viendo las direcciones del paquete para determinar los métodos de conmutación y enrutamiento.
- Enviar los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Controlar la congestión de la subred.

Para recordar más rápidamente a esta capa podemos pensar en selección de ruta, direccionamiento y enrutamiento.

Capa 4: Capa de Transporte

La capa de transporte proporciona sus servicios a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión. Para ello segmenta los datos originados en el *host* emisor y los reensambla en una corriente de datos dentro del sistema del *host* receptor.

El límite entre la capa de sesión y la capa de transporte puede imaginarse como el límite entre los protocolos de capa de medios y los protocolos de capa de *host*. Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones, las cuatro capas inferiores se encargan del transporte de datos.
Específicamente, temas como la confiabilidad del transporte entre dos *hosts* es responsabilidad de esta capa. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte.
Se conocen con el nombre de circuitos virtuales a las conexiones que se establecen dentro de una subred, y en ellos no hay la necesidad de tener que elegir una nueva para cada paquete, ya que cuando se inicia la conexión se determina una ruta de la fuente al destino, ruta que es usada para todo el tráfico posterior. Las funciones de esta capa se resumen en los siguientes puntos:

- Controlar la interacción entre procesos usuarios.
- Incluye controles de integración entre usuarios de la red para prevenir perdidas o doble procesamiento de transmisiones.
- Controlar el flujo de transacciones y direccionamiento de maquinas a procesos de usuario.
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo.
- Aceptar los datos del nivel de sesión, fragmentándolos en unidades más pequeñas, llamadas segmentos, en caso necesario y los pasa al nivel de red.
- Realizar funciones de control y numeración de unidades de información, fragmentación y reensamblaje de mensajes.
- Se encarga de garantizar la transferencia de información a través de la subred.

Para recordar más rápidamente a esta capa podemos pensar en calidad de servicio y confiabilidad

Capa 5: Capa de Sesión

La capa de sesión proporciona sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación en cooperación, organicen y sincronicen su dialogo y procedan al intercambio de datos. Sus principales funciones son:

- Establecer, administrar y finalizar las sesiones entre dos *hosts* que se están comunicando.
- Si por algún motivo una sesión falla por cualquier causa ajena al usuario, esta capa restaura la sesión a partir de un punto seguro y sin perdida de datos o si esto no es posible termina la sesión de una manera ordenada verificando y recuperando todas sus funciones, evitando problemas en sistemas transaccionales.
- Sincronizar el dialogo entre las capas de presentación de los dos *hosts* y administra su intercambio de datos, estableciendo las reglas o protocolos para el dialogo entre maquinas y así poder regular quien habla y por cuanto tiempo o si hablan en forma alterna, es decir, las reglas del dialogo que son acordadas.
- Ofrecer disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.
- Hacer *checkpoints,* que son puntos de recuerdo en la transferencia de datos.

Para recordar más rápidamente a esta capa podemos pensar en diálogos y conversaciones.

Capa 6: Capa de Presentación

La capa de presentación proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro, estableciendo el contexto sintáctico del dialogo. Su tarea principal es aislar a las capas inferiores del formato de los datos de la aplicación, transformando los formatos particulares (ASCII, EBCDIC, etc.) en un formato común de red.

Es también la responsable de la obtención y de la liberación de la conexión de sesión cuando existan varias alternativas disponibles.
Por ello, de ser necesario, la capa de presentación realiza las siguientes operaciones:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida. Para ello convierte los datos desde el formato local al estándar de red y viceversa.
- Definir la estructura de los datos a transmitir. Por ejemplo, en el caso de un acceso a base de datos, definir el orden de transmisión y la estructura de los registros.
- Definir el código a usar para representar una cadena de caracteres ASCII

- Dar formato a la información para visualizarla o imprimirla.
- Comprimir los datos si es necesario.
- Aplicar a los datos procesos criptográficos.

Para recordar más rápidamente a esta capa podemos pensar en un formato de datos común.

Capa 7: Capa de Aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario, y esta relacionada con las funciones de más alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los protocolos usados por las aplicaciones individuales. Es el medio por el cual los procesos de aplicación de usuario acceden al entorno OSI.

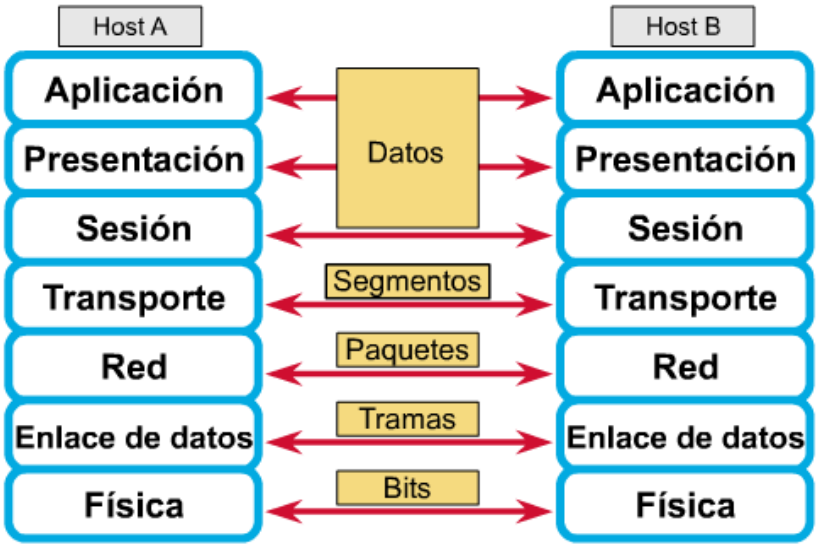
Su función principal es proporcionar los procedimientos precisos que permitan a los usuarios ejecutar los comandos relativos a sus propias aplicaciones.
Los procesos de las aplicaciones se comunican entre si por medio de las entidades de aplicación asociadas, estando estas controladas por protocolos de aplicación, y utilizando los servicios del nivel de presentación.

Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. La capa de aplicación establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre si y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos. Algunos ejemplos de procesos de aplicación son:

- Programas de hojas de cálculo.
- Programas de procesamiento de texto.
- Transferencia de archivos (FTP).
- Login remoto (RLOGIN, TELNET).
- Correo electrónico (MAIL – SMTP).
- Paginas Web (HTTP).

Para recordar más rápidamente a esta capa podemos pensar en navegadores de Web.

La figura 1.3 nos muestra un ejemplo de cómo es la comunicación entre dos equipos a través de las 7 capas que forman el modelo OSI. Cada capa del modelo OSI utiliza un protocolo distinto para comunicarse, los diferentes protocolos que maneja cada capa se muestran en la figura 1.4.



Términos clave:

Bits: La capa física toma los datos binarios de la capa de Enlace de Datos y convierte los 1's y 0's a una señal digital para enviarlos a través de la topología física.

Frames / Tramas: Alojan los paquetes o datagramas enviados desde la capa de Red para ser entregados a un dispositivo en la LAN. Incluye las direcciones físicas.

Paquetes: A veces llamados "datagramas", alojan los segmentos enviados por la capa de Transporte para ser enrutados a través de la red. Incluye las direcciones lógicas.

Segmentos: Se definen en la capa de Transporte. Se trata de la partición del flujo de datos que proviene de las capas superiors hacia el dispositivo de destino.

Figura.1.3 Nos muestra como pasa la información entre las diferentas capas del Modelo OSI

CAPA MODELO OSI		PROTOCOLO
7	Aplicación	http – telnet – SNMP
6	Presentación	JPG – MP3
5	Sesión	NFS – Linux
4	Transporte	TCP – UDP
3	Red	IP – ARP – RIP
2	Enlace de Datos	Ethernet – PPP – HDLC
1	Física	

Figura.1.4. Se puede apreciar los protocolos que se utilizan en cada una de las capas del Modelo OSI.

1.3 Pila TCP/IP

El Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP), inicialmente fueron desarrollados en 1973 por el informático estadounidense Vinton Cerf siendo parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA) del Departamento de Defensa Estadounidense. El proyecto estaba basado en la transmisión de paquetes de información y tenia como principal objetivo la interconexión de redes. De este proyecto surgieron dos redes: Una especializada en investigación, ARPANET y otra que era de uso exclusivamente militar, MILNET. Para poder comunicar a las redes se desarrollaron varios protocolos: El Protocolo de Internet y los Protocolos de Control de Transmisión. Después estos protocolos se englobaron en el conjunto de protocolos TCP/IP.

TCP/IP es el protocolo que la mayoría de las computadoras que se conectan a Internet utilizan para poder comunicarse entre si. En Internet se encuentran conectadas computadoras con *Hardware* y *Software* muy diferentes los cuales en la mayoría de los casos son incompatibles, además de todos los medios y formas posibles de conexión. Una de las grandes ventajas de protocolo TCP/IP es que precisamente este protocolo se encarga de que la comunicación entre todas las computadoras sea posible ya que es compatible con cualquier sistema operativo y con cualquier tipo de *Hardware*.

La función principal de la pila o conjunto de protocolos TCP/IP es la transferencia de información desde un dispositivo de red a otro. (Figura 1.5)

Figura 1.5 Modelo TCP/IP

Algunas ventajas de este Protocolo TCP/IP son:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en maquinas de cualquier tamaño
- Conectividad Universal a través de la red
- Protocolos estandarizados

TCP/IP no es un protocolo único, sino que en realidad es un conjunto de protocolos que cubre los distintos niveles del modelo OSI.

TCP/IP tiene una arquitectura la cual consta de cuatro niveles o capas en las que se agrupan los protocolos, los cuales se relacionan con el modelo OSI. (Figura 1.6)

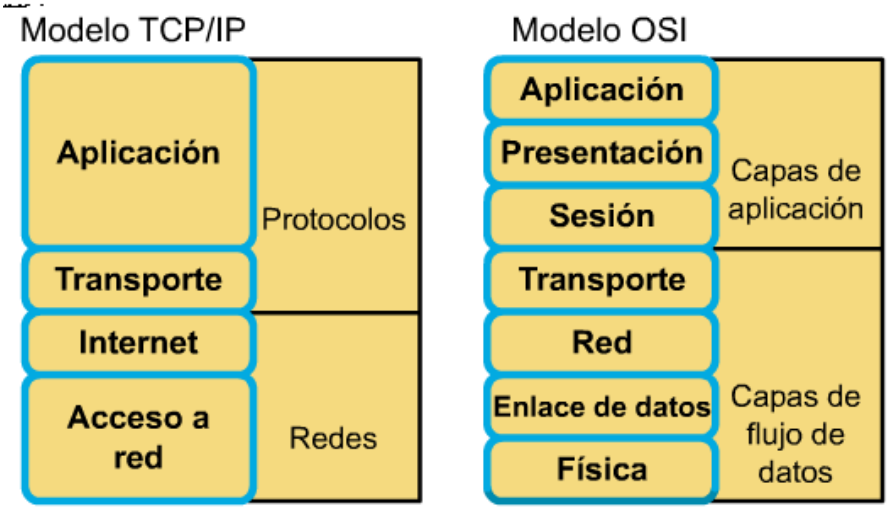


Figura. 1.6 Comparación entre el Modelo TCP/IP y el Modelo OSI

Capa de Aplicación.

Los diseñadores del TCP/IP crearon una capa de aplicación que manejara protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y da por sentado que estos datos están correctamente empaquetados para la siguiente capa. La capa de aplicación del TCP/IP corresponde con el modelo OSI en las capas de aplicación, presentación y sesión. Se encarga de prestar servicios a los usuarios tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET), y otros más recientes como HTTP (Hypertext Transfer Protocol). También soporta los protocolos de la administración de red y de direccionamiento.

*DNS. (Sistema de Denominación de Dominio)***.** Este sistema utilizado en Internet se encarga de transformar los nombres de los dominios y de sus nodos de red en direcciones.

SMTP (Protocolo Simple de Transferencia de Correo). Este es un protocolo que se encarga de la transmisión de correo electrónico a través de las redes de datos. El único soporte que da para la transmisión de datos es el de un texto simple.

SNMP (Protocolo Simple de Administración de Red). Este protocolo tiene la facultad de dar el medio por el cual se puede monitorear y controlar los dispositivos de red y para administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

FTP (Protocolo de Transferencia de Archivos). Este protocolo es un servicio orientado a conexión muy confiable que utiliza TCP para transferir archivos entre sistemas que soportan FTP. También soporta transferencia bidireccional de archivos binarios y archivos ASCII.

*TFTP (Protocolo Trivial de Transferencia de Archivos***).** Este protocolo es no orientado a conexión por lo tanto no es muy confiable, utiliza UDP para transferir archivos entre sistemas que soportan el protocolo TFTP. En algunas LAN llega a ser útil porque opera más rápidamente que FTP en un entorno estable.

*HTTP (Protocolo de Transferencia de Hipertexto***).** Este es el protocolo estándar de Internet por el cual se hace el intercambio de información en la *World Wide Web*, así también para redes internas. Soporta muchos diferentes tipos de archivos incluyendo texto, gráficos, sonido y video. También define el proceso a través del cual los navegadores de la *Web* originan solicitudes de información para enviar a los servidores *Web*.

TELNET. Este es un protocolo estándar de emulación de terminal es utilizado por los clientes para realizar conexiones de terminal remota con los servicios del servidor Telnet, esto permite que los usuarios se conecten de forma remota a los *routers*, con la finalidad de introducir comandos ya sea para configurarlos o para observar su funcionamiento.

NETSTAT. Este tiene la utilidad de dar información acerca de estadísticas TCP/IP, también se puede utilizar para dar información acerca del estado en el que se encuentran las conexiones TCP/IP y resúmenes del ICMP, TCP y UDP.

Capa de Transporte.

Esta capa coincide con la del modelo OSI. Los protocolos que hay en este nivel como UDP y TCP se encargan de manejar los datos y proporcionar la confiabilidad necesaria en el transporte de los mismos. Esta capa permite que un dispositivo de usuario divida en segmentos varias aplicaciones de capas superiores para colocarlas en la misma corriente de datos de la Capa 4 y permite que un dispositivo receptor pueda volver a ensamblar los segmentos de las aplicaciones de las capas superiores. La corriente de datos de Capa 4 es una conexión lógica entre los extremos de una red, y brinda servicios de transporte desde un *host* hasta un destino.

*TCP (Protocolo de Control de Transmisión***.** Es un protocolo orientado a conexión muy confiable; proporciona un control de flujo a través de ventanas deslizantes, y confiabilidad a través de los números de secuencia y acuses de recibo. TCP vuelve a enviar cualquier mensaje que no se reciba y suministra un circuito virtual entre las aplicaciones del usuario final. TCP tiene una gran ventaja que es que proporciona una entrega garantizada de los segmentos.

UDP (User Datagram Protocol). Este es un protocolo que no esta orientado a conexión y por lo tanto no es confiable; aunque tiene la responsabilidad de transmitir mensajes, en esta capa no se suministra ninguna verificación de *software* para la entrega de segmentos. UDP

tiene la ventaja de la velocidad. Como UDP no suministra acuses de recibo, se envía menos cantidad de tráfico a través de la red, lo cual hace más rápido la transferencia.
La pila TCP/IP esta estructurada por diferentes tipos de protocolos, esta estructura principal es mostrada a continuación (Figura 1.7).

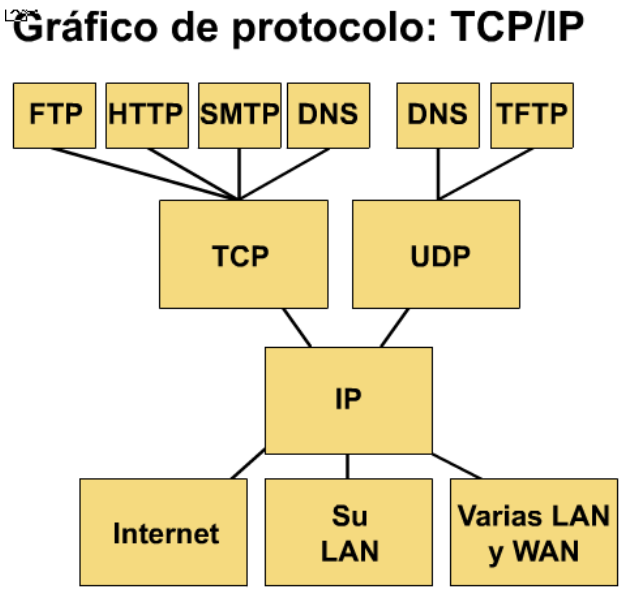


Figura 1.7 Este gráfico ilustra algunos de los protocolos comunes especificados por el modelo de referencia TCP/IP.

Capa de Internet.

Esta capa de la pila TCP/IP corresponde con la capa de Red del modelo OSI. El protocolo IP es parte de esta capa, este se encarga de mandar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte. Esta capa tiene la responsabilidad de transportar los paquetes a través de la red utilizando el direccionamiento por *software.* (Figura 1.8).

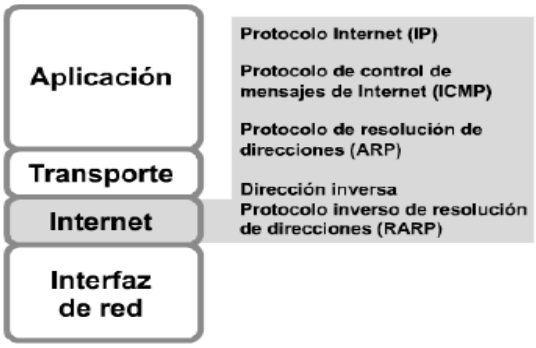


Figura 1.8 TCP/IP y la capa de Internet

IP (Internet Protocol). Este protocolo se encarga del enrutamiento de datagramas y es no orientado a conexión, a este protocolo no le interesa el contenido de los datagramas, solo busca la forma de desplazarlos hasta su destino.

ICMP (Internet Control Message Protocol). Este protocolo proporciona el medio para que el *software* de *hosts* y *gateways* intermedios se comuniquen. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Aporta capacidad de control y mensajeria.

ARP (Address Resolution Protocol). Este protocolo es el encargado de convertir las direcciones IP en direcciones de la red física. El funcionamiento del protocolo ARP es bastante simple. Cuando una máquina desea enviar un mensaje a otra máquina que está conectada a través de una red *ethernet* se encuentra con un problema: la dirección IP de la máquina en cuestión es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por lo que tendrá que encontrar un modo de traducir la dirección IP a la dirección física. Esto se hace con el protocolo ARP.

RARP (Reverse Address Resolution Protocol). Este protocolo es el encargado de determinar las direcciones de red cuando se conocen las direcciones a nivel de la capa de enlace de datos.

Cada capa de la pila TCP/IP proporciona diferentes tipos de servicios y protocolos que ayudan a la transferencia de información desde un dispositivo de red a otro (Figuras 1.9 y 1.11), las cuales tienen una amplia relación con las 7 capas del Modelo de Referencia OSI (Figura 1.10).

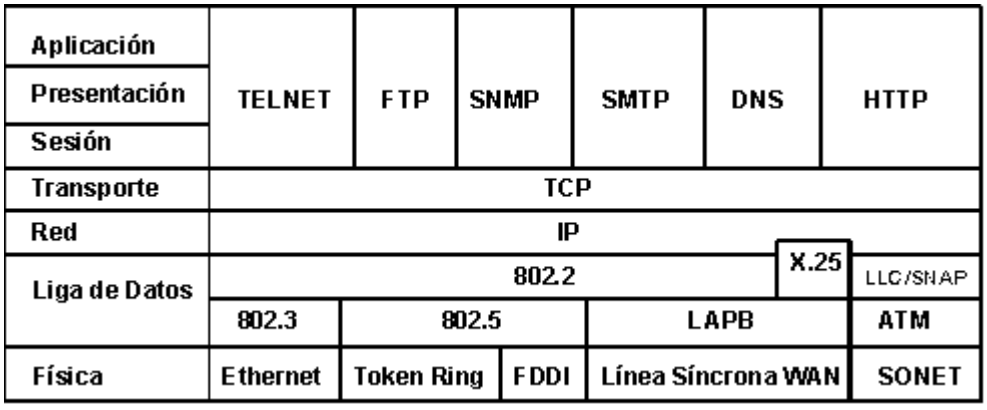


Figura. 1.9 En este gráfico se puede apreciar los servicios que se le brinda a los usuarios tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET), y otros más recientes como HTTP (Hypertext Transfer Protocol).

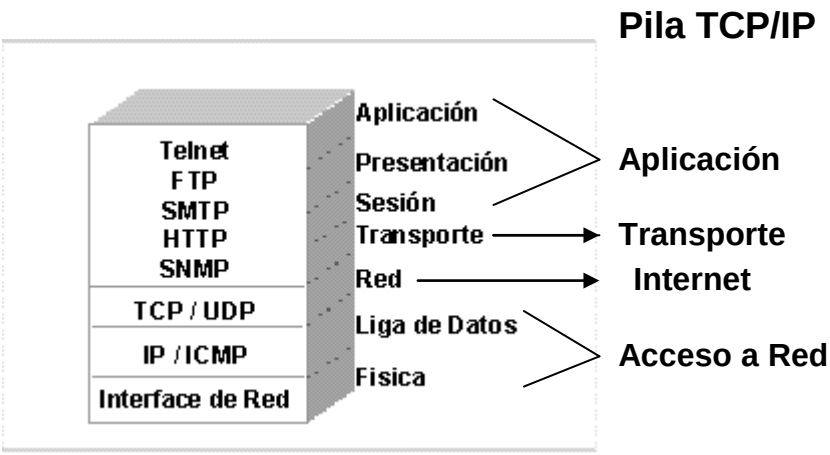


Figura 1.10. Analogía entre las capas del Modelo de referencia OSI y las capas de la pila TCP/IP

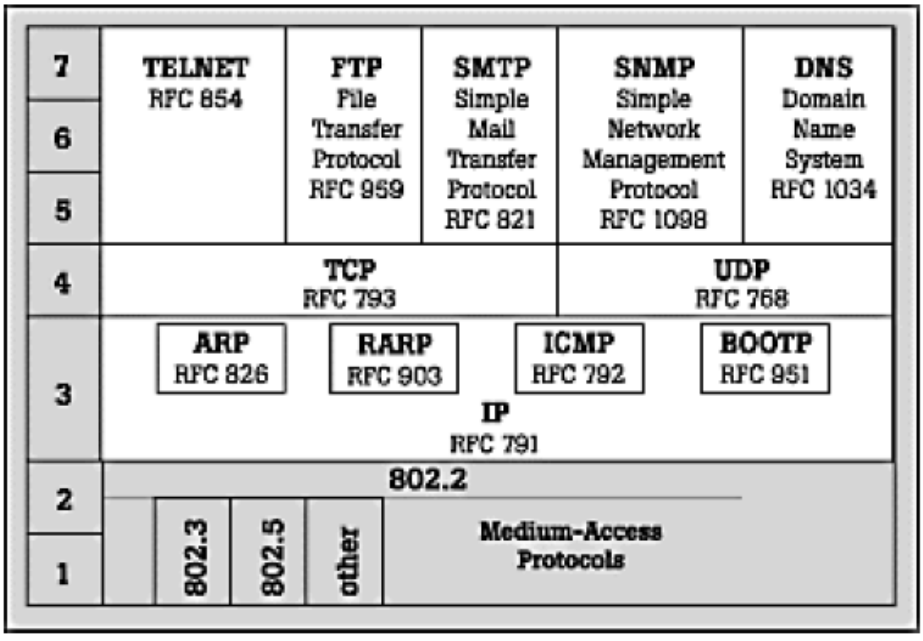


Figura 1.11 Conjunto de protocolos de la pila TCP/IP

Datagrama TCP/IP

El protocolo IP a diferencia de otros protocolos como el X.25 esta basado en la idea de los datagramas de interred los cuales son transportados desde un *host* origen hasta un *host* destino pero no siempre de una manera segura.

El protocolo IP realiza su función de la siguiente manera: La capa de transporte toma los mensajes y los divide en datagramas de hasta 64k cada uno. Cada datagrama se transmite a través de la red desfragmentandose en unidades más pequeñas durante su recorrido. Al llegar los datagramas a su origen final, la capa de transporte se encarga de reensamblarlos para así poder tener el mensaje original.

Un datagrama IP esta constituido por una parte de cabecera y una parte de texto. La cabecera consta de una parte fija de 20 octetos y una parte opcional de longitud variable.

El datagrama IP contiene los siguientes campos:

Versión: Este campo indica a que versión del protocolo pertenece cada uno de los datagramas. Mediante la inclusión de la versión en cada datagrama, no se excluye la posibilidad de modificar los protocolos mientras la red se encuentre en operación.

Opciones: El campo opciones se utiliza para fines de seguridad, informe de errores, enrutamiento fuente, depuración, y otro tipo de información. Esto proporciona básicamente un escape para permitir que las versiones subsiguientes de los protocolos incluyan información que actualmente no esta presente en el diseño original.

Longitud de Cabecera: Debido a que la longitud de cabecera no es constante, este campo permite que se indique la longitud que tiene la cabecera en palabras de 32 bits.

Tipo de Servicio: Este campo le permite al host indicarle a la subred el tipo de servicio que desea. Se pueden tener varias combinaciones con respecto a la seguridad y a la velocidad. Para voz digitalizada, por ejemplo, es más importante la entrega rápida que corregir errores de transmisión. En tanto que, para la transferencia de archivos, resulta más importante tener la transmisión fiable que entrega rápida. También, es posible tener algunas otras combinaciones, desde un tráfico rutinario, hasta una anulación instantánea.

Longitud Total: Este campo incluye todo lo que se encuentra en el datagrama, tanto la cabecera como los datos. La máxima longitud es de 65 536 octetos (bytes).

Identificación: Este campo se necesita para permitir que el host destino determine a que datagrama pertenece el fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación.

DF: Las letras DF quieren decir no fragmentar. Esta es una orden para que las pasarelas no fragmenten el datagrama, ya que el extremo destinatario es incapaz de unir las partes

nuevamente. Por ejemplo, supóngase que se tiene un datagrama que se carga en un micro pequeño para su ejecución; podría marcarse con DF porque la ROM de micro espera el programa completo en un datagrama. Si el datagrama no puede pasarse a través de una red, se deberá encaminar sobre otra red, o bien, desecharse.

MF: Las letras MF significan más fragmentos. Todos los fragmentos, con excepción del último, deberán tener puesto ese bit. Se utiliza como una verificación doble contra el campo de *Longitud total*, con objeto de tener seguridad de que no faltan fragmentos y que el datagrama entero se reensamble por completo.

Desplazamiento de Fragmento: Este campo indica el lugar del datagrama actual al cual pertenece este fragmento. En un datagrama, todos los fragmentos con excepción del último, deberán ser un múltiplo de 8 octetos, que es la unidad elemental de fragmentación. Dado que se proporcionan 13 bits, hay un máximo de 8192 fragmentos por datagrama, dando así una longitud máxima de datagrama de 65 536 octetos, que coinciden con el campo *Longitud total*.

Tiempo de Vida: Este campo es un contador que se utiliza para limitar el tiempo de vida de los paquetes. Cuando se llega a cero, el paquete se destruye. La unidad de tiempo es el segundo, permitiéndose un tiempo de vida máximo de 255 segundos.

Protocolo: Este campo indica a que proceso de transporte pertenece el datagrama. El TCP es efectivamente una posibilidad, pero en realidad hay muchas más. El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino.

Código de Redundancia: Este código de la cabecera es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del *código de redundancia* de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el tiempo de vida**.**

Dirección de Origen: Contiene la dirección del host que envía el paquete. Tamaño 32 bit.

Dirección Destino: Esta dirección es la del *host* que recibirá la información. Los *routers* o *gateways* intermedios deben conocerla para dirigir correctamente el paquete. Tamaño 32 bit.

Formato de segmentos TCP y UDP

Los segmentos TCP contienen los siguientes campos:

- Puerto de Origen. Es el número de origen (puerto) de este segmento.
- Puerto de Destino. Es el número de destino (puerto) de este segmento.

- Numero de Secuencia. Es el número utilizado para asegurar la secuencia correcta de los datos que llegan. Es el número asignado al primer octeto en el campo de datos de usuario.
- Numero de Acuse de Recibo. Es el siguiente octeto TCP esperado.
- Longitud de la Cabecera. Es el número de palabras de 32 bits que hay en la cabecera.
- Reservado. Configurado a 0.
- Bits de Código. Las funciones de control (en el inicio y fin de una sesión).
- Ventana. Es el número de octetos que el emisor espera aceptar.
- Suma de Comprobación. Es la suma de comprobación calculada de los campos de cabecera y datos.
- Puntero de Urgencia. Indicador del final de los datos urgentes.
- Opciones. Tamaño máximo de segmento TCP.
- Datos. Datos del protocolo de capa superior.

(Figuras 1.12 y 1.13)

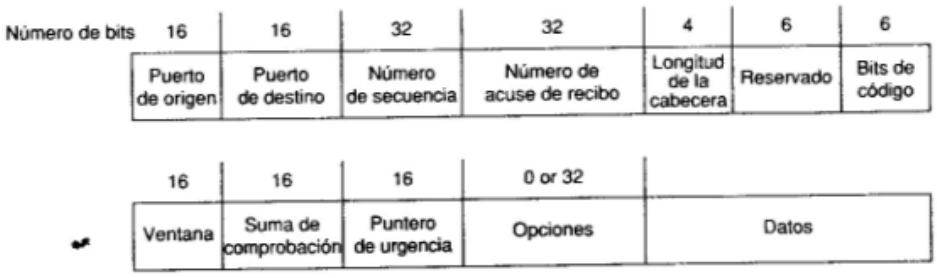


Figura 1.12 El formato del segmento TCP incluye 12 campos

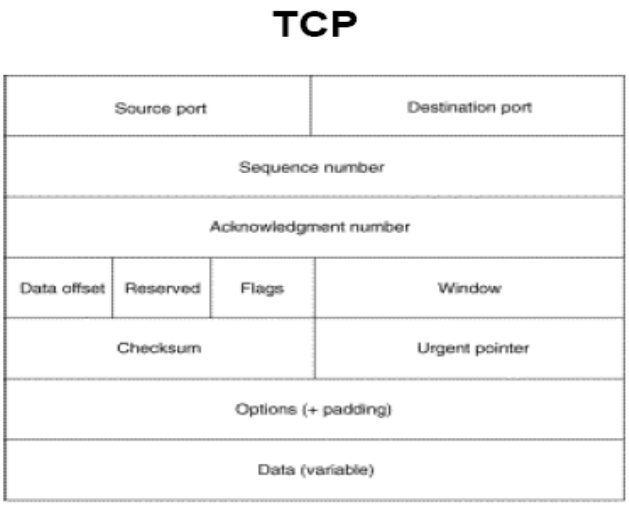


Figura 1.13 Formato de segmentos TCP

Si se utiliza UDP, los protocolos de la capa de aplicación deben proporcionar fiabilidad de ser necesario. UDP no utiliza *windowing* ni acuses de recibo. Esta diseñado para aplicaciones que no necesitan poner secuencias de segmentos juntas (Figuras 1.14 y 1.15).

Los protocolos que utilizan UDP son los siguientes:

- TFTP
- SNMP
- Sistema de archivos de red (NFS).
- Sistema de denominación de dominio (DNS).

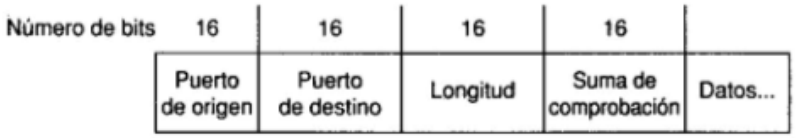


Figura 1.14 UDP no tiene campos de secuencia ni de acuse de recibo.

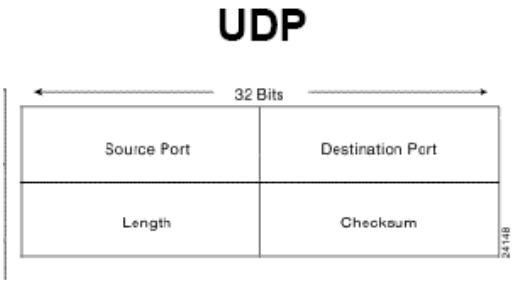


Figura 1.15.- Datagrama UDP

Protocolo de mensajes de control en Internet (ICMP – Internet Control MessageProtocol)

Todos los *host* TCP/IP implementan el Protocolo de mensajes de control en Internet (ICMP). Los mensajes ICMP se transportan en los datagramas IP y se utilizan para enviar mensajes de error y control. ICMP los siguientes tipos de mensajes definidos:

- Destination unreachable (destino inalcanzable).
- Time to Live exceded (tiempo de existencia agotado).
- Parameter problem (problema de parámetro).
- Source quench (origen extinguido).
- Redirect (redireccionar).

- Echo request (solicitud de eco).
- Echo reply (respuesta de eco).
- Timestap reply (solicitud de indicador de hora).
- Information request (solicitud de información).
- Information reply (respuesta de información).
- Adress mask request (solicitud de mascara de dirección).
- Adress mask reply (respuesta de mascara de dirección).

Números de puerto TCP y UDP

- Tanto TCP como UDP utilizan números de puerto para determinar a qué protocolo de capa superior tiene que pasar la información
- Estos puertos vienen definidos en la RFC1700, aunque existen aplicaciones que necesitan su propio número de puerto y no utilizan números de puerto estándar.
- Los puertos están regulados de la siguiente manera:
  0 – 254: Reservados para aplicaciones públicas
  255 – 1023: Reservados a compañías con aplicaciones
  Comerciales
  Superiores a 1024: Puertos no regulados

  (Figura 1.16)

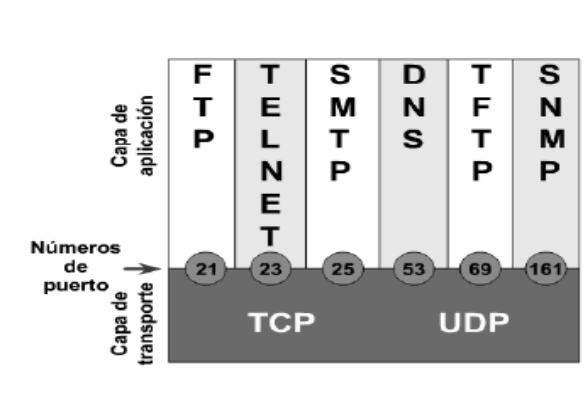


Figura 1.16 Números de puerto TCP y UDP

La Pila TCP/IP tiene una relación muy estrecha con el Modelo de Referencia OSI en cuanto a las capas que los forman así como los protocolos que maneja cada capa (Figura 1.17).

DoD	TCP/IP	OSI	Protocolos
Procesos de Aplicación	Procesos de Aplicación	7- Aplicación 6- Presentación 5- Sesión	Telnet, FTP, LPD, SNMP, TFTP, SMTP, NFS, X WINDOW
Host to Host	Host to Host	4- Transporte	TCP, UDP
Internet	Internet	3- Red	ICMP, BOOTP, ARP, RARP, IP
	Acceso a Red	2- Enlace de datos 1- Física	Ethernet, Fast Ethernet, Token Ring, FDDI

DoD – Modelo desarrollado por el Departamente de Defensa de los Estados Unidos en la década de 1970.

TCP/IP – Suite de protocolos estándar finalmente implementados por la comunidad de ARPANet.

OSI – Modelo estándar desarrollado por la ISO y publicado en el año 1984 a partir de los modelos DecNet, SNA y TCP/IP.

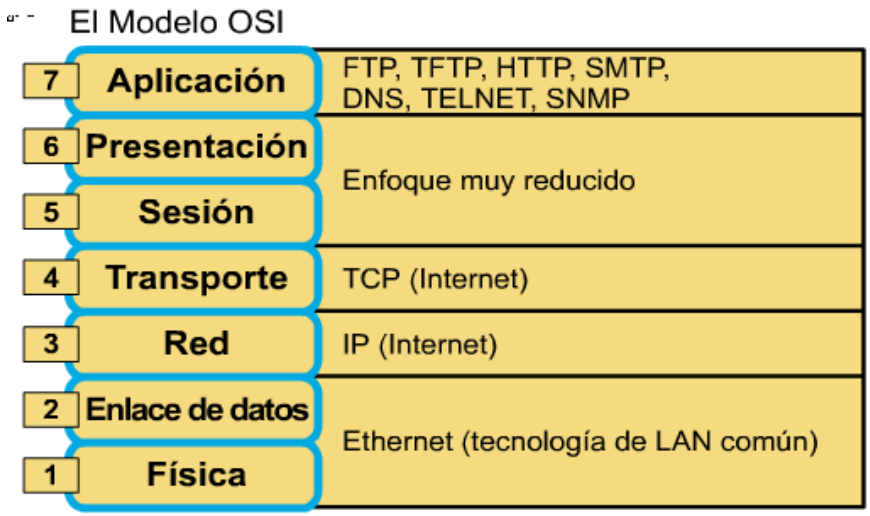


Figura 1.17 Este gráfico nos muestra la relación del Modelo OSI con el Modelo TCP/IP y los protocolos que se ocupan en cada capa.

1.4 Direccionamiento IP

La capa de red se ocupa de la navegación de los datos a través de la red. La función de la capa de red es encontrar la mejor ruta a través de la red. Los dispositivos utilizan el esquema de direccionamiento de capa de red para determinar el destino de los datos a medida que se desplazan a través de la red.

Los protocolos que no tienen capa de red sólo pueden ser usados en redes internas pequeñas. Estos protocolos normalmente sólo usan un nombre (por ejemplo, dirección MAC) para identificar el equipo en una red. El problema que se tiene con este sistema es

que, a medida que la red aumenta de tamaño, se vuelve cada vez más difícil organizar todos los nombres como, por ejemplo, asegurarse de que dos equipos no utilicen el mismo nombre.

Las direcciones de capa de red utilizan un esquema de direccionamiento jerárquico que permite que existan direcciones únicas más allá de los límites de una red, junto con un método para encontrar una ruta por la cual la información viaje a través de las redes. Las direcciones MAC usan un esquema de direccionamiento plano que hace que sea difícil ubicar los dispositivos en otras redes.

Los esquemas de direccionamiento jerárquico permiten que la información viaje por una *internetwork*, así como también un método para detectar el destino de modo eficiente. La red telefónica es un ejemplo del uso del direccionamiento jerárquico. El sistema telefónico utiliza un código de área que designa un área geográfica como primera parte de la llamada (*salto*). Los tres dígitos siguientes representan la central local (segundo salto). Los últimos dígitos representan el número telefónico destino individual (que, por supuesto, constituye el último salto).

Los dispositivos de red necesitan un esquema de direccionamiento que les permita enviar paquetes de datos a través de la *internetwork* (un conjunto de redes formado por múltiples segmentos que usan el mismo tipo de direccionamiento). Hay varios protocolos de capa de red con distintos esquemas de direccionamiento que permiten que los dispositivos envíen datos a través de una red

Existen dos principales razones por las cuales es necesario que existan redes múltiples:

Estas son el aumento de tamaño de cada red y el aumento de la cantidad de redes.

Cuando una LAN, MAN o WAN crece, es aconsejable para el control de tráfico de la red, que ésta sea dividida en porciones más pequeñas denominadas *segmentos de red* (o simplemente segmentos). Esto da como resultado que la red se transforme en un grupo de redes, cada una de las cuales necesita una dirección individual. Por lo tanto es conveniente que estas redes separadas (o sistemas autónomos, en caso de que los maneje una sola administración) se comuniquen entre sí a través de Internet. Sin embargo, esto lo deben realizar mediante esquemas de direccionamiento razonables y dispositivos de red adecuados. De no ser así, el flujo de tráfico de red se congestionaría seriamente y ni las redes locales ni Internet funcionarían.

Los *routers* son dispositivos de red que operan en la Capa 3 del modelo OSI (la capa de red). Los *routers* unen o interconectan segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando con base la información de capa 3

Los *routers* también toman decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red y luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Los *routers* toman paquetes de dispositivos LAN (es decir, estaciones de trabajo), y, basándose en la información de Capa 3, los envían a través de la red. El enrutamiento a veces se denomina *conmutación de Capa 3.*

La determinación de ruta es el proceso que utiliza el *router* para elegir el siguiente salto de la ruta del paquete hacia su destino. Este proceso también se denomina *enrutar el paquete*.
Los *routers* también pueden tomar decisiones basándose en la densidad del tráfico y la velocidad del enlace (ancho de banda).

1.4.1 Clases

Las direcciones IP se expresan como números de notación decimal punteados: se dividen los 32 bits de la dirección en cuatro *octetos* (un octeto es un grupo de 8 bits). El valor decimal máximo de cada octeto es 255 (el número binario de 8 bits más alto es 11111111, y esos bits, de izquierda a derecha, tienen valores decimales de 128, 64, 32, 16, 8, 4, 2 y 1).

Una dirección IP tiene una longitud de 32 bits. Se compone de dos partes principales, un número de red y un número de *host*. Para mucha gente no es fácil recordar 32 bits, debido a esto, las direcciones IP se agrupan de a ocho bits por vez, separados por puntos y representados en formato decimal, no binario. Esto se conoce como "formato decimal separado por puntos". (Figura 1.18)

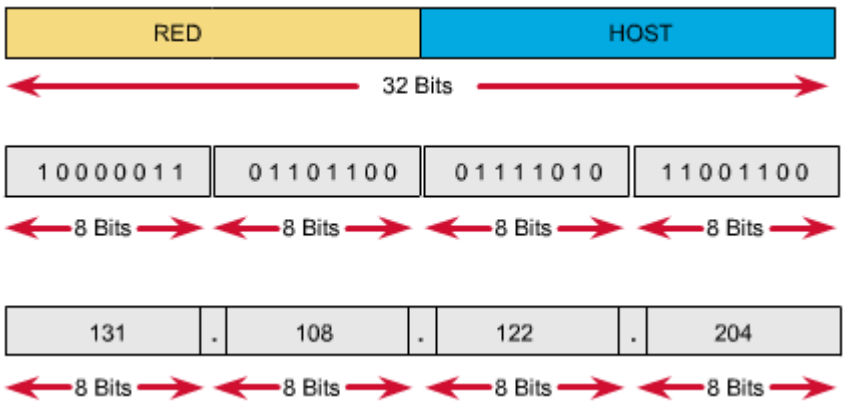


Figura 1.18 Este esquema nos muestra el formato de direccionamiento IP

El número de red de una dirección IP identifica la red a la cual se encuentra conectado un dispositivo. La porción de *host* de una dirección IP identifica el dispositivo específico de esta red. Como las direcciones IP están formadas por cuatro octetos separados por puntos, se pueden utilizar uno, dos o tres de estos octetos para identificar el número de red. De modo similar, se pueden utilizar hasta tres de estos octetos para identificar la parte de *host* de una dirección IP.

Hay tres clases de direcciones IP:

Clase A:

Cuando está escrito en formato binario, el primer bit (el bit que está ubicado más a la izquierda) de la dirección Clase A siempre es 0. Un ejemplo de una dirección IP Clase A es 124.95.44.15. El primer octeto, 124, identifica el número de red asignado por ARIN (Registro Americano de Números de Internet). Los administradores internos de la red asignan los 24 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase A es verificar el primer octeto de su dirección IP, cuyo valor debe estar entre 0 y 126. (127 *comienza* con un bit 0, pero está reservado para fines especiales).

Todas las direcciones IP Clase A utilizan solamente los primeros 8 bits para identificar la parte de red de la dirección. Los tres octetos restantes se pueden utilizar para la parte de *host* de la dirección (Figuras 19 y 20). A cada una de las redes que utilizan una dirección IP Clase A se les pueden asignar hasta 2 elevado a la 24 potencia (2^{24}) (menos 2, se restan dos debido a que la primera dirección por ejemplo 124.0.0.0 es la RED y la ultima dirección por ejemplo la 124.255.255.255 es la dirección de *broadcast,* estas dos direcciones no pueden ser asignadas a ningún *host*), o 16,777,214 direcciones IP posibles para los dispositivos que están conectados a la red.

Clase B

Los primeros 2 bits de una dirección Clase B siempre son 10 (uno y cero). Un ejemplo de una dirección IP Clase B es 151.10.13.28. Los dos primeros octetos identifican el número de red asignado por ARIN. Los administradores internos de la red asignan los 16 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase B es verificar el primer octeto de su dirección IP. Las direcciones IP Clase B siempre tienen valores que van del 128 al 191 en su primer octeto.

Todas las direcciones IP Clase B utilizan los primeros 16 bits para identificar la parte de red de la dirección. Los dos octetos restantes de la dirección IP se encuentran reservados para la porción del *host* de la dirección (Figuras 19 y 20). Cada red que usa un esquema de direccionamiento IP Clase B puede tener asignadas hasta 2 a la 16ta potencia (2^{16}) (menos 2 otra vez), o 65.534 direcciones IP posibles a dispositivos conectados a su red.

Clase C

Los 3 primeros bits de una dirección Clase C siempre son 110 (uno, uno y cero). Un ejemplo de dirección IP Clase C es 201.110.213.28.

Las direcciones IP Clase C siempre tienen valores que van del 192 al 223 en su primer octeto.

Todas las direcciones IP Clase C utilizan los primeros 24 bits para identificar la porción de red de la dirección. Sólo se puede utilizar el último octeto de una dirección IP Clase C para la parte de la dirección que corresponde al *host* (Figuras 1.19 y 1.20). A cada una de las redes que utilizan una dirección IP Clase C se les pueden asignar hasta 2^8 (menos 2), o 254, direcciones IP posibles para los dispositivos que están conectados a la red.

La máscara de subred (término formal: prefijo de red extendida), no es una dirección, sin embargo determina qué parte de la dirección IP corresponde al campo de red y qué parte corresponde al campo de *host.* Una máscara de subred tiene una longitud de 32 bits y tiene 4 octetos, al igual que la dirección IP.

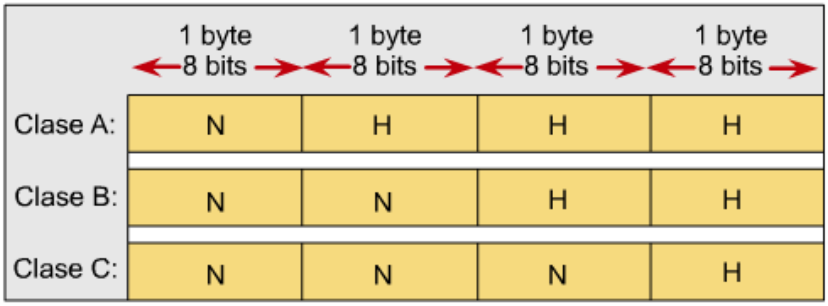


Figura 1.19 Clases de direcciones IP donde ♣ N= Número de red asignado por ARIN ♣H=Número de host asignado por el administrador

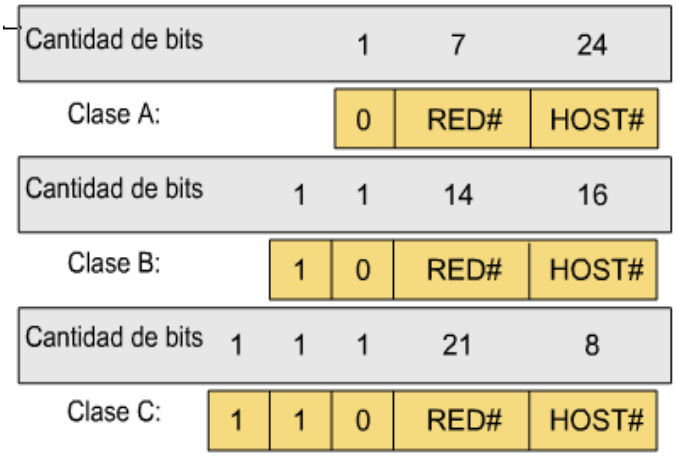


Figura 1.20 Patrones de bit de la dirección IP

1.4.2 Subnetting

A medida que las redes crecen aumentando el número de segmentos, mas direcciones de red (IP) son necesarios ya que cada segmento requiere un número propio. La InterNIC (Network Information Centers cooperation), sin embargo, no puede manejar un numero ilimitado de direcciones de red ya que se están acabando rápidamente debido a la alta demanda proveniente de la comunidad de Internet.

Es por esto que los administradores de redes deberán trabajar con lo poco que tienen para acomodarse mejor a los requerimientos de la red y la reducida oferta de direcciones. Una manera de lograrlo es tomar las direcciones que son asignadas a la red y expandir su capacidad con subredes. *Subnetting* (implementar subredes) permite incrementar el numero de redes disponibles sin solicitar otra dirección IP.

El subnetting es una colección de direcciones IP que permiten definir él número de redes y de host que se desean utilizar en una subred determinada.

La idea principal de las direcciones IP era que cada parte de red identificara exactamente una red física. Pero resulto que esta meta tenia unos cuantos defectos. Por ejemplo, una red implementada en una universidad que tiene muchas redes internas decide conectarse a internet. Para cada red, sin importar cuan pequeña, se necesita una dirección Clase C, por lo menos. Aun peor, para cada red con más de 255 *hosts* se necesitaría una dirección Clase B. Esto representa un gran desperdicio de direcciones, e ineficiencia en la asignación de direcciones IP, sin contar los altos costos.

Peor aun, en dado caso que se llegaran muchas de las direcciones IP en una red Clase B, esto representa un aumento en el tiempo de envío de paquetes ya que la tabla de redireccionamiento de los *routers* aumentaría notablemente, y la búsqueda del destino en esta tabla tomaría mucho tiempo. A medida que se agregan hosts se hace mas grande la tabla de direccionamiento (*routing table*), lo que trae como consecuencia un aumento en los costos de los *routers* y una degradación en el rendimiento del *router*.

Una gran solución a este problema es ofrecida por el s*ubnetting* (implementación de subredes), lo que permite reducir el número total de redes a ser asignadas. La idea es tomar una parte de red de una dirección de IP y asignar las direcciones IP de esa parte de red a varias redes físicas, que serán ahora referidas como subredes. Pero hay que hacer ciertas cosas para que esto funcione. Primero, las subredes deben de estar cerca unas de otras, debido a que a un punto distante en el Internet todas lucirían igual a una sola red, teniendo solo una parte de red en común. Esto significa que un *router* solo estaría habilitado para seleccionar una sola ruta para llegar a cualquiera de las subredes, así que es mejor que se encuentren ubicadas en la misma dirección. No es que no vaya a funcionar si se encuentran muy separadas, solo que funcionara mucho mejor el sistema de subredes si le logra tenerlas en la misma dirección general. Un ejemplo práctico de utilización de subnetting podría ser en una universidad con una red Clase B que tenga muchas redes físicas. Desde afuera de la universidad, todo lo que se necesita saber para alcanzar cualquier subred dentro de la red principal es la dirección del *router* que conecta a la universidad con el resto del Internet.

El mecanismo con el cual se puede lograr compartir un numero de red (parte de red) entre distintas redes involucra la configuración de todos los nodos en cada subnet con una mascara de red, la misma para todos los nodos dentro de una subred. Con las mascaras de redes se logra jerarquizar aun mas la estructura jerárquica de un IP, que como se dijo antes esta constituida por parte de red mas parte de host, incluyendo un nuevo nivel de jerarquía que llamaremos numero de subnet. Como se sabe, todos los hosts en una misma red tienen la misma parte de red, pero ahora todos los host en la misma red física tendrán el mismo numero de subnet, lo que hace que los hosts en la misma red, pero en distintas redes físicas compartan la parte de red pero no el numero de subnet, y esto como se puede notar ayuda notablemente en la transmisión de información, pues se complementa las tablas de direccionamiento con otro campo que ayudara a mejorar la eficiencia de envío de paquetes.
Para entender mejor el funcionamiento de las mascaras de red, supongamos que se quiere dividir una red Clase B en varias redes. Se podría utilizar una mascara de red de la forma 255.255.255.0 (lo que pasado a binario son 1s en los primeros 24 bits y 0s en los últimos 8). Por lo tanto podríamos pensar que ahora los primeros 24 bits de una dirección IP representan la <parte de red> y los últimos 8 la parte de host. Como los primeros 16 bits identifican una red Clase B, podemos pensar que la dirección no tiene dos sino tres partes: la parte de red más parte de subnet más parte de host.

Lo que subnetting significa para un host es que ahora esta configurado con una dirección IP y una mascara de red para la subred a la cual se encuentra conectado. Cuando un host quiere enviar un paquete a una cierta dirección IP, lo primero que hace es realizar un operación de Y (AND) de bits entre su propia mascara de red y la dirección de destino. Si el resultado es igual a la número de subnet del host que envía el paquete, entonces sabe que el host de destino esta en la misma subred y el paquete de entregado directamente a través de la subred. Si el resultado no es igual, el paquete necesita ser enviado a un *router* para ser enviado desde este a otra subred.

Así como el trabajo de envío de un *host* cambia en una subred, también el trabajo de un *router* se ve afectado cuando se introduce la implementación de *subnetting*. Normalmente para satisfacer la estructura jerárquica de parte de red mas parte de host el *router* tiene una tabla de direccionamiento que formada por campos de la forma Numero de Red, Próximo Salto. Para soportar *subnetting* la tabla ahora debe estar conformada por entradas de la forma Número de Subred, Mascara de Subred, Próximo Salto. Para encontrar el lugar correcto en la tabla, el *router* aplica una operación AND entre la dirección de destino del paquete y la Mascara de Subred para cada una de las entradas, y cada vez revisa si el resultado es igual al Número de Subred de la entrada en turno. Si esto sucede, entonces esta es la entrada correcta a utilizar, y el *router* envía el paquete envía el paquete al *router* o a la interfaz especificada en el campo Próximo Salto.

Es bueno aclarar unos ciertos puntos sobre *subnetting*. No es necesario seleccionar una mascara con todos los bits 1s continuos, pero evitar esta estructura acarreará mayores complicaciones administrativas, ya que no será posible ver una parte de una dirección IP y decir ese es el numero de subred. También puede fallar al hacer implementaciones que asumen que nadie utiliza mascara que no-continuas, por esto no es recomendable. También es importante saber que podemos poner múltiplos subredes en una misma red física. El efecto que esto tendría es que se deberá forzar a los hosts en la misma red, pero en

diferentes subredes. Esto puede ser útil para razones administrativas como por ejemplo separar distintos departamentos en una misma LAN, pero acarrea un aumento en los costos de la estructura o topología de la red.

Como habíamos mencionado antes, desde afuera de la red que se encuentra divida en subredes, los *routers* ven a la red como una red física sencilla y única, viendo las colecciones de subredes tan solo por la parte de red del IP, y guardan una entrada en su tabla de direccionamiento para saber como llegar a esa red. Dentro de la red los *routers* necesitan estar capacitados para direccional paquetes a la correcta subred de destino. Es por esta razón que no todas las partes de la internet ven exactamente la misma información de direccionamiento. Por ejemplo, un *router* en una red puede tener información de cómo llegar a otra subred cercana, pero no tiene ninguna entrada sobre otra subred en la red. El envía el paquete al *router* correspondiente (o al router default), y este ultimo se encarga de ver si sabe a donde enviarlo, si no, sigue el envío a otro *router* hasta que se consigue uno que sepa a donde enviarlo.

1.4.3 VLSM

VLSM (Variable Length Subset Masks). Es una técnica que permite dividir subredes en redes más pequeñas pero la regla que hay que tener en consideración siempre que se utilice VLSM es que solamente se puede aplicar esta técnica a las direcciones de redes/subredes que no están siendo utilizadas por ningún host, VLSM permite crear subredes mas pequeñas que se ajusten a las necesidades reales de la red. Para poder usar VLSM, se necesita un protocolo de enrutamiento que lo soporte - básicamente, el protocolo de enrutamiento tiene que enviar tanto la dirección de subred como la máscara de subred en las actualizaciones.

Entre los protocolos de enrutamiento internos, RIP versión 1 e IGRP no tienen este soporte para VLSM, mientras que RIP versión 2, EIGRP y OSPF sí lo tienen.

En otras palabras, los protocolos CON CLASE como RIP Versión 1 e IGRP, no soportan VLSM, mientras que los protocolos SIN CLASE como EIGRP, RIP Versión 2 y OSPF entre otros, soportan VLSM.

Por ejemplo, si tomamos como base una dirección: 172.16.10.0, al ser esta dirección de clase B, la máscara de red tendrá 16 bits. Cuando llevemos la máscara a 22 bits, lograremos subdividirla en 64 subredes de 1024 direcciones cada una. Si entre nuestras necesidades tenemos que asignar alguna subred de menos de 60 direcciones, podremos utilizar una máscara de 26 bits, es decir: 1024 subredes de 64 direcciones cada una, y todo sin perder la posibilidad de seguir utilizando la máscara anterior de 22 bits para solucionar el problema de alguna subred grande de hasta 1024 hosts que debamos acomodar.

1.4.4 CIDR

Classless Inter-Domain Routing: CIDR

Ejemplo: Qué hacer cuando las direcciones IP asignables están a punto de agotarse y la siguiente versión del estándar simplemente no puede desplegarse a tiempo?. Solución parche: recuperar los millones ya asignadas pero que nunca se usarán. CIDR (RFCs 1466, 1518 y 1519) ha mantenido el crecimiento de Internet, reorganizando las direcciones IP de las cinco clases originales en un sistema sin clases. Antes de CIDR, las direcciones IP se asignaban de acuerdo con el número de direcciones de ``host'' que una compañía u organización necesitaba. Tres de las cinco clases (A, B y C) proporcionaron más de 3 mil millones de hosts utilizables en más de 2 millones de redes, mientras que las restantes eran para multicasting y uso experimental. Sin embargo, a principios de los años 90, esas 2 millones de redes eran devoradas por los ISP que proporcionaban acceso a sus clientes y por compañías que querían conectarse a internet por cuenta propia. Todas las direcciones clase A se habían agotado, y las de clase B sólo se asignaban si se comprobaba su necesidad. Las de Clase C se asignaban a diario, acabándose con tal rapidez que se temía se agotaran en cuestión de meses. Por otro lado, el problema no era sólo la creciente necesidad de direcciones IP, sino que ya se habían asignado y no se utilizaban. Había 125 redes clase A, y todas se subutilizaban. Por ejemplo, America Online era la única compañía del planeta que podía necesitar tal número de direcciones, y sólo si todos sus usuarios estuvieran en línea al mismo tiempo. Con tantas direcciones en manos de tan pocas organizaciones, era preciso hacer algo para liberar algunas y usarlas de modo más eficaz. CIDR utiliza las mismas máscaras de dirección que se emplean en la división en subredes para crear grupos de direcciones clase C, permitiendo la recuperación de porciones sustanciales de las antiguas redes clase A y B, con lo que se podrían formar más de 10 millones de redes clase C. La desventaja de esta reagrupación es el mayor tamaño de las tablas de ruteo centrales debido al mayor número de redes que necesitan que se les identifiquen rutas. Además de esto, el tamaño de las tablas de ruteo se debe al mecanismo de asignación de direcciones que se ha seguido, que ha sido estrictamente cronológico y no existe correspondencia entre la ubicación geográfica de una organización o del ISP y su rango de direcciones, por lo que no es posible resumir las tablas de rutas. Por esto, la información se ha de incluir enumerando una a una todas las redes existentes. Si se siguiera una organización jerárquica de direcciones de acuerdo con criterios geográficos, como ocurre en el direccionamiento de la red telefónica, podría resolverse el problema.

CIDR resuelve estos problemas de dos formas. La primera consiste en establecer una jerarquía en la asignación de direcciones, que en vez de utilizar un criterio puramente cronológico, que desde el punto de vista geográfico o de topología de la red equivale a una asignación aleatoria, los rangos se asignan por continentes. Inicialmente, se ha realizado el reparto de una parte del rango de redes clase C de la manera mostrada en la tabla (Figura 1. 21).

Table: Agrupación de Redes Clase C en Superredes Asignadas Geográficamente.	
Multi regional	192.0.0.0 - 193.255.255.255
Europa	194.0.0.0 - 195.255.255.255
Otros	196.0.0.0 - 197.255.255.255
Norteamérica	198.0.0.0 - 199.255.255.255
Centro y Sudamérica	200.0.0.0 - 201.255.255.255
Anillo Pacífico	202.0.0.0 - 203.255.255.255
Otros	204.0.0.0 - 205.255.255.255
Otros	206.0.0.0 - 207.255.255.255

Figura 1.21 Tabla de Agrupación de Redes Clase C en Superredes Asignadas Geográficamente

Con esta distribución es posible agrupar las entradas en las tablas de ruteo en forma geográfica. Por ejemplo, un router en Chile puede tener una sola entrada en su tabla indicando que todos los paquetes dirigidos a las redes 194.0.0.0 hasta 195.255.0.0 se envíen a la interfaz por la cual accede a Europa, evitando así las 131072 entradas que normalmente harían falta para este rango de direcciones. Sin embargo, este pequeño ``arreglo" no es gratis, pues para que las rutas agrupadas sean posibles de enrutar, es necesario modificar el software de los routers, ya que en principio no considera el rango 194.0.0.0-195.255.0.0 como una sola red sino como 131072 redes distintas. Por esto, se ha extendido el concepto de subred en sentido contrario, es decir la máscara no solo puede crecer hacia la derecha para dividir una red en subredes, sino que puede crecer hacia la izquierda para agrupar varias redes en una mayor, de ahí que a CIDR se le denomine también supernetting. Es decir, la parte de red de la dirección vendrá especificada por la longitud de la máscara únicamente, y la clasificación tradicional en clases no tiene ningún significado, sólo respetándose dicho significado en el caso de las clases D y E. La segunda forma de solucionar el problema original, es una consecuencia de lo anterior, consiste en dar a cada organización la posibilidad de solicitar un rango de direcciones, pero que se ajuste a sus necesidades, dándole siempre un rango contiguo y que tenga una máscara de red común. Por ejemplo, si una empresa requiere una cantidad de 2048 direcciones IP, puede asignársele un grupo de ocho redes clase C consecutivas comenzando en 234.170.168.0 y terminando en 234.170.175.255. Con esto, su dirección de red CIDR será 234.170.168.0 y su máscara 255.255.248.0. Recordar que la máscara por defecto de cada red clase C es 255.255.255.0, de aquí se observa que la máscara se ha corrido hacia la izquierda, perdiendo tres bits.

1.5 Fundamentos de Enrutamiento

El enrutamiento no es otra cosa que instrucciones para ir de una red a otra. Estas instrucciones, también conocidas como rutas, pueden ser dadas a un router por otro de forma dinámica, o pueden ser asignadas al router por el administrador de forma estática.

Un administrador de redes toma en cuenta muchos aspectos al seleccionar un protocolo de enrutamiento dinámico. El tamaño de la red, el ancho de banda de los enlaces disponibles, la capacidad de procesamiento de los routers, las marcas y modelos de los routers de la red y los protocolos que ya se encuentran en uso en la red son todos factores a considerar a la hora de elegir un protocolo de enrutamiento.

El enrutamiento es el proceso usado por el *router* para enviar paquetes a la red de destino. Un *router* toma decisiones en función de la dirección de IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. A fin de tomar decisiones correctas, los routers deben aprender la ruta hacia las redes remotas. Cuando los *routers* usan enrutamiento dinámico, esta información se obtiene de otros *routers*. Cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas (Figura 1.22).

Debido a que las rutas estáticas deben configurarse manualmente, cualquier cambio en la topología de la red requiere que el administrador agregue o elimine las rutas estáticas afectadas por dichos cambios. En una red de gran tamaño, el mantenimiento manual de las tablas de enrutamiento puede requerir de una enorme cantidad de tiempo de administración. En redes pequeñas, con pocos cambios, las rutas estáticas requieren muy poco mantenimiento. Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del enrutamiento dinámico. Aun en redes de gran tamaño, a menudo se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos específicos, junto con un protocolo de enrutamiento dinámico.

La función *determinación de ruta* se produce a nivel de Capa 3 (capa de red). Permite que el *router* evalúe las rutas disponibles hacia un destino y así establecer el mejor manejo de un paquete. Los servicios de enrutamiento utilizan la información de topología de red al evaluar las rutas de red. La determinación de ruta es el proceso que utiliza el router para elegir el siguiente salto de la ruta del paquete hacia su destino. Este proceso también se denomina *enrutar el paquete*.

Los *routers* también pueden tomar decisiones basándose en la densidad del tráfico y la velocidad del enlace (ancho de banda).

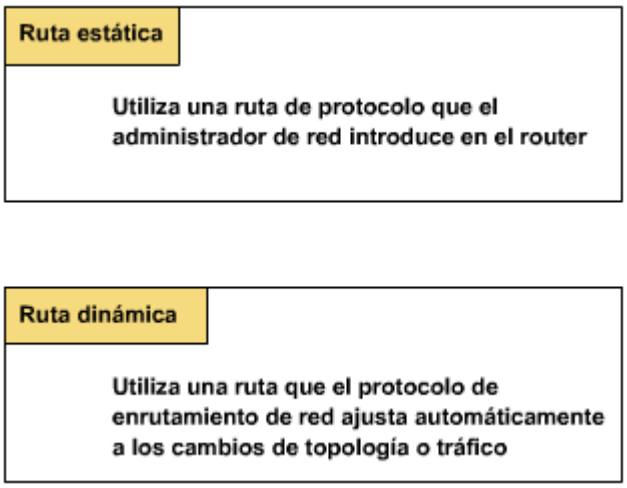


Figura1.22 Diferencian entre enrutamiento Estático y Dinámico.

Algoritmos de Enrutamiento

La capa de Red proporciona la dirección lógica que permite que dos sistemas dispares que se encuentran en redes lógicas diferentes determinen una posible ruta para comunicarse.
En la capa de red es donde residen los algoritmos que implementan los protocolos de enrutamiento.

En la mayoría de las subredes, los paquetes requerirán varias escalas para completar el viaje. La excepción serían las redes de difusión, pero aún aquí es importante el enrutamiento, ya que el origen y el destino pueden no estar en la misma red.

El *algoritmo de enrutamiento* es la parte del *software* de la capa de red encargada de decidir la línea de salida por la que se transmitirá un paquete de entrada.

Si la subred usa datagramas entonces esta decisión debe hacerse cada vez que llega un paquete de datos de entrada, debido a que la mejor ruta podría haber cambiado desde la última vez.

Si la subred utiliza circuitos virtuales internamente, las decisiones de enrutamiento se tomarán sólo al establecerse el circuito y los paquetes seguirán la ruta previamente establecida.

Clasificación de los Algoritmos de Enrutamiento

Algoritmos no adaptables: No basan sus decisiones de enrutamiento en mediciones o estimaciones del tráfico ni en la topología. La decisión de qué ruta tomar de *I* a *J* se calcula

por adelantado, fuera de línea y se cargan en los *routers* al iniciar la red. Éste procedimiento se llama *enrutamiento estáticos.* La desventaja de este tipo de algoritmos es que no es posible responder a situaciones cambiantes como por ejemplo saturación, exceso de tráfico o fallo en una línea.

En un conjunto de redes complejas, se necesita cierto grado de cooperación "dinámica" entre los dispositivos de encaminamiento. En particular se deben evitar aquellas porciones de red que sufren congestión, entendiéndose esto como aquella situación donde hay demasiados paquetes en alguna parte de la subred, y como consecuencia el rendimiento de ésta baja.

Para poder tomar estas decisiones de enrutamiento dinámicas, los dispositivos involucrados en el ruteo deben intercambiar información usando algoritmos de enrutamiento especiales para este propósito. La información que se necesita sobre el estado del conjunto de redes tiene que venir expresada en términos de qué redes son accesibles a través de qué dispositivos y en términos de las características de retardo de varias rutas.

Algoritmos adaptables: En contraste con los algoritmos no adaptables, éstos cambian sus decisiones de enrutamiento para reflejar los cambios de topología y de tráfico. Difieren de los algoritmos estáticos en el lugar de obtención de su información (Ej. localmente, en los routers adyacentes o de todos), el momento del cambio de sus rutas (Ej. cada t seg., o cuando cambia la carga) y la métrica usada para una mejor optimización (Ej. distancia, nº de escalas, tiempo estimado del tránsito). Este tipo de algoritmos no pueden ser demasiado complejos ya que son implementados en los routers y deben ejecutarse en tiempo real con recursos de CPU y la memoria con que el *router* dispone.

1.5.1 Conceptos de Enrutamiento.

Enrutamiento Estático.

Las operaciones con rutas estáticas pueden dividirse en tres partes, como sigue:

El administrador de red configura la ruta.
El *router* instala la ruta en la tabla de enrutamiento.
Los paquetes se enrutan de acuerdo a la ruta estática.
Como las rutas estáticas se configuran manualmente, el administrador debe configurarla en el *router*, mediante el comando *ip route.*

En la Figura 1.23, se muestra como el administrador del router Hoboken necesita configurar las rutas estáticas cuyo destino son las redes 172.16.1.0/24 y 172.16.5.0/24. El administrador puede ejecutar uno de dos comandos posibles para lograr su objetivo. El método de la Figura 1.23 especifica la dirección IP del siguiente salto (hop) del router adyacente. Cualquiera de los comandos instalará una ruta estática en la tabla de enrutamiento del router Hoboken.

La distancia administrativa es un parámetro opcional que da una medida del nivel de confiabilidad de la ruta. Un valor menor de distancia administrativa indica una ruta más confiable. Por lo tanto, es preferible instalar rutas de distancia administrativa menor antes que una ruta idéntica de distancia administrativa mayor. La distancia administrativa por defecto cuando se usa una ruta estática es 1. Cuando una interfaz de salida se configura como el *gateway* de una ruta estática, dicha ruta será desplegada en la tabla de enrutamiento como si estuviera directamente conectada. Esto a veces confunde, ya que la redes directamente conectadas tienen distancia 0. Para verificar la distancia administrativa de una ruta en particular use el comando *show ip route address*, donde la dirección ip de dicha ruta se inserta en la opción *address*. Si se desea una distancia administrativa diferente a la distancia por defecto, se introduce un valor entre 0 y 255 después de la interfaz de salida o el siguiente salto, como se muestra a continuación:

waycross(config)#ip route 172.16.3.0 255.255.255.0 172.16.4.1 130

Si el router no puede llegar a la interfaz de salida que se indica en la ruta, ésta no se instalará en la tabla de enrutamiento. Esto significa que si la interfaz está desactivada, la tabla de enrutamiento no incluirá la ruta.

A veces, las rutas estáticas se utilizan como rutas de respaldo. Es posible configurar una ruta estática en un router, la cual sólo se usará en caso de fallas en la ruta dinámicamente conocida. Para utilizar una ruta estática de esta forma, simplemente fije la distancia administrativa en un valor superior a la proporcionada por el protocolo de enrutamiento dinámico en uso.

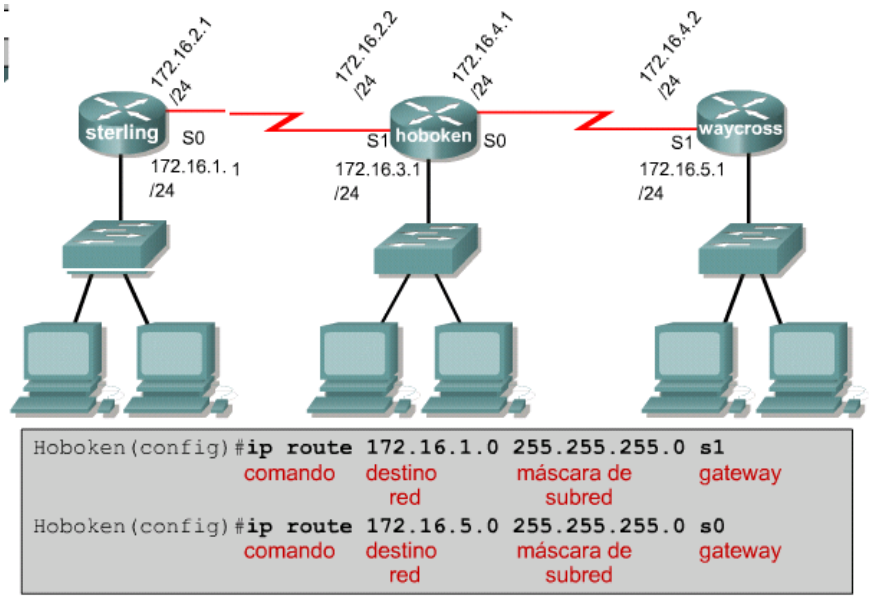


Figura 1.23. Configuración de rutas estáticas especificando la dirección IP del siguiente salto (hop) del router adyacente

Enrutamiento Dinámico

Los protocolos de enrutamiento dinámico pueden ayudar a simplificar la vida del administrador de redes. El enrutamiento dinámico hace innecesario el exigente y prolongado proceso de configurar rutas estáticas. El enrutamiento dinámico también hace posible que los routers se adapten a los cambios de la red y que ajusten sus tablas de enrutamiento en consecuencia, sin intervención del administrador de redes. Sin embargo, el enrutamiento dinámico puede ocasionar problemas.

Introducción a los protocolos de enrutamiento.

Un protocolo de enrutamiento es el esquema de comunicación entre *routers*, permite que un *router* comparta información con otros *routers*, acerca de las redes que conoce así como de su proximidad a otros *routers*. La información que un *router* obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.

Ejemplos de protocolos de enrutamiento (Figura 24):

Protocolo de información de enrutamiento (RIP)
Protocolo de enrutamiento de gateway interior (IGRP)

Protocolo de enrutamiento de gateway interior mejorado (EIGRP)
Protocolo "Primero la ruta más corta" (OSPF)

Un protocolo enrutado se usa para dirigir el tráfico generado por los usuarios. Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

Ejemplos de protocolos enrutados (Figura 1.24):

Protocolo Internet (IP)
Intercambio de paquetes de internetwork (IPX).

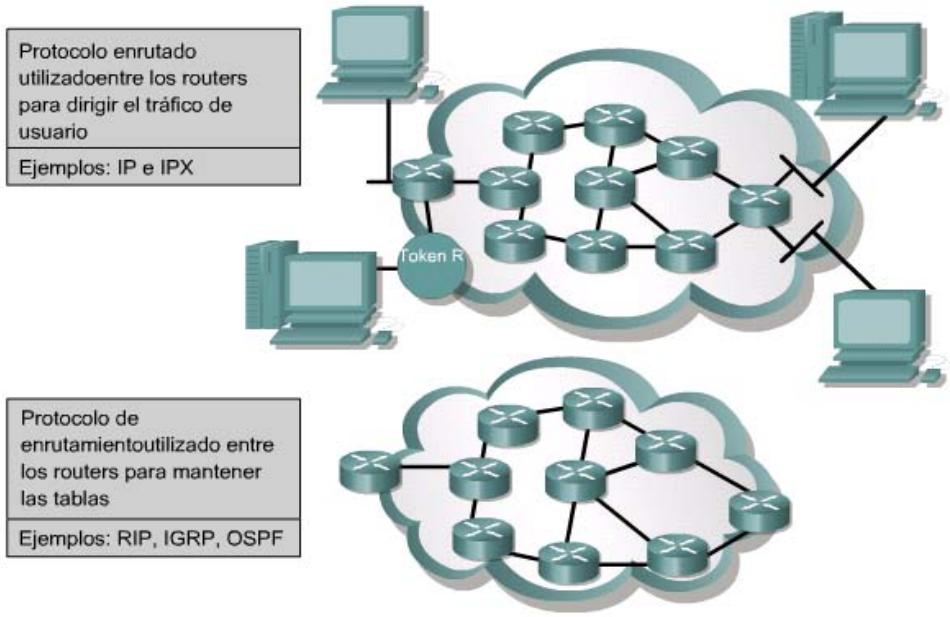


Figura 1.24. Diferencia entre protocolo erutado y de enrutamiento.

Sistema Autónomo

Un sistema autónomo (AS) es un conjunto de redes bajo una administración común, las cuales comparten una estrategia de enrutamiento común. Para el mundo exterior, el AS es una entidad única. El AS puede ser administrado por uno o más operadores, a la vez que presenta un esquema unificado de enrutamiento hacia el mundo exterior.

Los números de identificación de cada AS son asignados por el Registro estadounidense de números de la Internet (ARIN), los proveedores de servicios o el administrador de la red. Este sistema autónomo es un número de 16 bits. Los protocolos de enrutamiento tales como el IGRP de Cisco, requieren un número único de sistema autónomo.

El objetivo de un protocolo de enrutamiento es crear y mantener una tabla de enrutamiento. Esta tabla contiene las redes conocidas y los puertos asociados a dichas redes. Los routers utilizan protocolos de enrutamiento para administrar la información recibida de otros routers, la información que se conoce a partir de la configuración de sus propias interfaces, y las rutas configuradas manualmente.

Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en las tablas de enrutamiento y descartan las rutas que ya no son válidas. El router utiliza la información en la tabla de enrutamiento para enviar los paquetes de datos (Figura 1.25).

El algoritmo de enrutamiento es fundamental para el enrutamiento dinámico. Al haber cambios en la topología de una red, por razones de crecimiento, reconfiguración o falla, la información conocida acerca de la red también debe cambiar. La información conocida debe reflejar una visión exacta y coherente de la nueva topología.

Cuando todos los *routers* de una red se encuentran operando con la misma información, se dice que la red ha hecho convergencia. Una rápida convergencia es deseable, ya que reduce el período de tiempo durante el cual los routers toman decisiones de enrutamiento erróneas.

Los sistemas autónomos (AS) permiten la división de la red global en subredes de menor tamaño, más manejables. Cada AS cuenta con su propio conjunto de reglas y políticas, y con un único número AS que lo distingue de los demás sistemas autónomos del mundo.

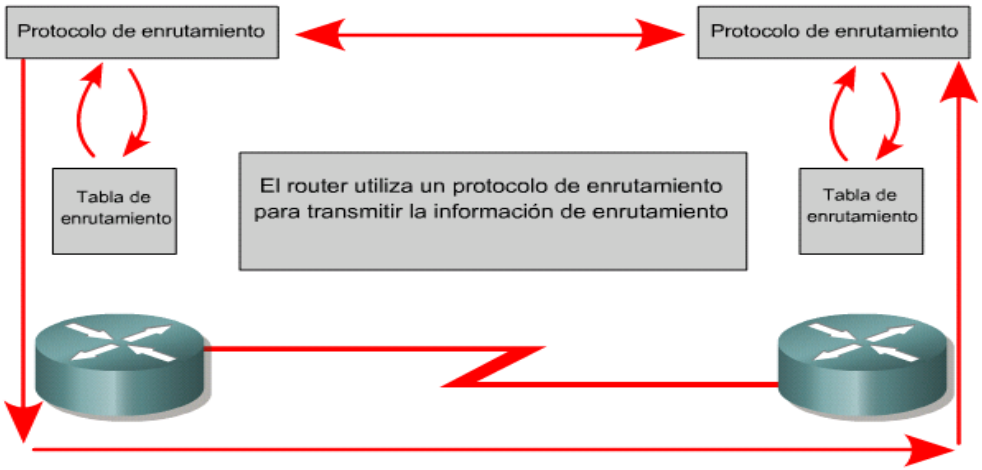


Figura 1.25. Se observa como se transmite a la información entre routers mediante un protocolo de enrutamiento.

1.5.2 Tipos de Protocolos de Enrutamiento.

Un router puede utilizar un protocolo de enrutamiento de paquetes IP para llevar a cabo el enrutamiento. Esto lo realiza mediante la implementación de un algoritmo de enrutamiento específico y emplea la capa de interconexión de redes del conjunto de protocolos TCP/IP.

Los protocolos de enrutamiento tienen varias clasificaciones. De acuerdo al tipo de algoritmo y de acuerdo al tipo de esquema de enrutamiento usado.
En cuanto al esquema de enrutamiento, que involucra la jerarquía en la que se estén empleando se clasifican en:

- IGP's (*Interior Gateway Protocol*)
- EGP's (*Exterior Gateway Protocol*)

Atendiendo al tipo de algoritmo se clasifican como:

- *Distance vector*
- *Link-state*

Los protocolos *vector distancia* son:

- RIP (Sus dos versiones)
- IGRP

Como *estado de enlace* tenemos:

- OSPF
- IS-IS

Como *Path Vector* esta:

- BGP

Y como híbridos esta:

- EIGRP

Atendiendo a la clasificación de IGP's:

- RIP
- IGRP
- OSPF
- IS-IS

Como EGP's tenemos:

- EGP
- BGP

Ahora en cuanto a la información que algunos protocolos de enrutamiento manejan en sus actualizaciones, podemos incluir otra clasificación.

- *Classfull*
    - o IGRP
    - o RIPv1

- *Classless*
    - o RIPV2
    - o OSPF
    - o BGP
    - o EIGRP

Los protocolos que entran en la categoría de *classless* mandan la información de su máscara de red en sus actualizaciones. Esto habilita la posibilidad de manejar VLSM[5], para hacer un mejor uso del espacio de direcciones. Los protocolos *classfull* no mandan información de la máscara de subred de las rutas que anuncian, por lo que no pueden manejar VLSM.
Las redes también entran en esta clasificación. Las subredes que no pertenezcan a clases puras, es decir que no sean de la clase A, B, C o D, se clasifican como *classless*. Por ejemplo la subred 150.185.128.5 con máscara de 255.255.192.0. El término *classfull* define las redes o subredes que pertenecen a una clase pura, es decir, la definida como clase A, B, C o D. Un ejemplo de ella es la 192.168.27.0 con máscara de 255.255.255.

De los protocolos antes mencionados los que se relacionan con la aplicación de la propuesta son los siguientes:

- RIP
- OSPF
- IGRP
- EIGRP (punto 1.5.2.3)

De los cuales hablaremos a continuación mas detalladamente.

RIP (Routing Information Protocol)

Es un protocolo de enrutamiento que esta basado en el bloque de protocolos que emplean los algoritmos vector distancia desarrollados para comparar en forma matemática las distintas rutas disponibles para obtener la mejor hacia el destino final.

Este protocolo específicamente tiene dos versiones: RIP versión 1 y RIP versión 2. La diferencia más importante es que la versión dos tiene una extensión que soporta el envió de información de la máscara de subred en sus mensajes de actualización.

También habilitó el envió de más información en sus mensajes de actualización, por ejemplo a través de esta información permite el uso de un método simple de autentificación con el fin de poder construir tablas de actualización con información confiable, teniendo de esta manera tablas seguras.

RIP es uno de los protocolos que aun se emplean, sin embargo el problema de este protocolo, cuyo algoritmo surgió de algunas investigaciones académicas, es que no es escalable cuando tiene que trabajar en redes grandes, debido a limitantes de alcance.

RIP cuenta con los siguientes procesos y características.
- Actualizaciones de enrutamiento

- Relojes de enrutamiento
- Estabilidad de enrutamiento
- Métricas de RIP

Proceso de actualización de ruta
Los mensajes de actualización de RIP actualizan toda la tabla de enrutamiento de los enrutadores. Estas actualizaciones se realizan con transmisiones de *broadcast* o por difusión ocurriendo en dos tiempos: en intervalos establecidos previamente y cuando un cambio de la topología de la red ha ocurrido.
Cuando un mensaje de actualización de enrutamiento se envía a un *router*, y el mensaje contiene una diferencia con respecto a alguno de los registros de la tabla de enrutamiento donde llegó el mensaje, el *router* realiza el cambio pertinente incrementando el valor de la métrica en 1 y registrando como su próximo salto al *router* que envió el mensaje de actualización. Una característica de RIP es que mantiene exclusivamente la mejor ruta, esto es aquella que tiene la menor métrica hacia el destino final.

Una vez que el *router* ha actualizado su tabla de enrutamiento, este envía mensajes de actualización a los demás enrutadores, aunque aún no sea el momento que tiene programado para enviar mensajes de actualización de ruta.

Relojes de enrutamiento
RIP emplea 3 relojes para manejar el envió información de enrutamiento hacia los otros *routers.*

- Reloj de actualización de enrutamiento
- Reloj de expiración de enrutamiento
- Reloj de vaciado de ruta

El reloj de actualización de enrutamiento establece el intervalo de tiempo en el cual se van a realizar las actualizaciones de las rutas periódicamente. Esta establecido a 30 segundos generalmente y cuenta con un tiempo de más generado aleatoriamente para prevenir posibles congestiones en la red que podrían ser ocasionadas por el intento de todos los *routers* de enviar al mismo tiempo sus actualizaciones.

Ahora, las rutas pueden ser marcadas como inválidas debido al término del tiempo que marca el reloj de expiración del mensaje de actualización, establecido a 180 seg., debido a la falta de un anuncio que indique la presencia de las rutas en cuestión sobre la red. Estas siguen siendo almacenadas por un periodo en la tabla de enrutamiento del *router*. Este último periodo esta marcado por el reloj de vaciado de ruta que después de 240 seg. borra el registro.

Estabilidad de enrutamiento
RIP cuenta con mecanismo para tener cierta estabilidad. Por ejemplo para evitar los *loops*, o que un paquete quede atrapado en la red viajando por “siempre”, se limita el número de saltos que puede dar un paquete para llegar a su destino final. Conociendo que cuando un paquete pasa por un *router* su métrica de salto es incrementada en 1, el destino se marca como inalcanzable cuando esta métrica alcanza el valor de 16, es decir, que el máximo número de saltos permitidos para un paquete antes de llegar al destino final es de 15.

Métrica de enrutamiento de RIP
La métrica que emplea RIP está clasificada como tamaño de ruta y se refiere al número de saltos que tiene que dar el paquete para llegar de un origen a su destino. Es así como conoce la distancia entre los orígenes y destinos, siendo cada sistema intermedio un punto de incremento en la métrica.

Formato de paquete
RIP v1 .-Contiene un encabezado de 24 bytes y esta formado por 9 campos de información del protocolo.

Los campos son los siguientes:

Comando: Indica si se trata de un paquete que transporta una petición o una respuesta.
***Número de versión*:** Indica la versión RIP que se esta usando.
***Cero*:** Fue agregado para hacerlo compatible con las muchas versiones de RIP.
Identificador de la familia de dirección: Dependiendo del protocolo que se este manejando, es el identificador que se le tiene asignado, por ejemplo para el caso de IP es 2. Esto se debe a que RIP fue diseñado para trabajar con distintos protocolos de red.
Dirección: Especifica la dirección de la entrada que será actualizada.
Métrica: Indica cuantos saltos han sido dados durante el viaje hasta el destino.

RIP v2 .-La versión 2 de RIP, contiene mayor información útil en sus paquetes. Igual que RIP v1, el encabezado de RIP v2 ocupa 24 bytes con 9 campos.

Los campos son:
Comando: Este campo indica si se trata de una respuesta o de una petición que lleva información de la tabla de enrutamiento. Cuando se trata de una respuesta puede tratarse de una respuesta a una petición o una actualización de enrutamiento que no se solicito. Como petición pedirá parte o toda la información de la tabla de enrutamiento del *router* solicitado.
Versión: Indica la versión empleada de RIP. Para RIP 2 tiene el valor 2.
Cero: Campo sin emplear.
Identificador de familia de dirección: Como RIP esta diseñado para manejar información de enrutamiento de varios protocolos, el valor de este campo ayuda a definir el tipo de dirección de acuerdo al protocolo que se esta manejando. Para IP es de 2.
Route tag: Ayuda a distinguir que método se empleó para aprender rutas internas o rutas externas.
***Dirección IP*:** Contiene la dirección lógica del paquete que esta entrando.
Máscara de subred: Contiene información de la máscara de subred en conjunto con la dirección IP.
Próximo salto: Contiene la dirección del próximo salto que debe dar el paquete.
Métrica: Contiene el número de saltos que ha dado el paquete en la red, incrementándose este valor al pasar por cada uno de los *routers* por los que tiene que pasar.

OSPF (Open Shortest Path First)

OSPF es un protocolo de enrutamiento desarrollado a mediados de los años 80's para suplir las carencias de otro protocolo de enrutamiento llamado RIP, ante la limitante que tenia este último para trabajar en redes grandes y que no eran homogéneas. Fue desarrollado por el grupo IGP (*Interior Gateway Protocol*) de la IETF (*Internet Engineering Task Force*).

Este protocolo fue desarrollado para trabajar sobre redes IP para usarse en la Internet con el algoritmo SPF (*Shortest Path First*) y fue el resultado de numerosos trabajos previos a este sentido, desarrollados para la ARPANET.

OSPF es un protocolo estándar de enrutamiento de estado de enlace y entra dentro de la clasificación de los protocolos IGP. Los protocolos de estado de enlace envían mensajes de estado de enlace, LSA's (*link-state advertisement*), a los demás *routers*, los cuales son avisos que contienen información acerca de las métricas empleadas, la información referente a las interfaces de los *routers*, además de algunas otras variables de importancia.

Con esta información el algoritmo SPF (*Shortest Path First*), bajo el cual esta construido el protocolo OSPF, calcula lo que sería la ruta más corta a un determinado nodo, además de servir para llenar lo que serían bases de datos de la topología de la red.

Se trata de un algoritmo de enrutamiento multiruta, lo que implica que soporta el conocimiento de más de una ruta hacia un mismo destino. Permite el balanceo de carga sobre enlaces que tienen igual costo y la métrica que emplea esta asociada a un costo.

Soporta el enrutamiento basado en peticiones TOS (*type-of-service*) de capas superiores. Esto es muy útil ya que permite que las aplicaciones puedan especificar una mayor prioridad a sus paquetes avisando a los *routers* que los manejen como urgentes, por ejemplo. Lógicamente, después de determinar la urgencia de estos paquetes, el algoritmo SPF haría el cálculo de la mejor ruta en base a este campo TOS especificado en paquetes IP.

Soporta VLMS (*Variable Lenght Subnet Mask*). Esto se debe a que en los avisos LSA's, se incluye información referente a la máscara de subred IP. Con VLMS se habilita a los administradores de red poder segmentar aún más una subred previamente establecida, permitiendo hacer mucho más flexible el diseño y por tanto la utilización del espacio de IP's que se pueden asignar.

También se caracteriza por ser un protocolo intra-AS o intra-dominio, con la capacidad de poder enviar avisos a *routers* que se encuentren en otros sistemas autónomos. OSPF puede trabajar bajo una estructura jerárquica de enrutamiento.

Cuando hablamos de una jerarquía de enrutamiento, la entidad más grande se denomina como un sistema autónomo (SA). Un sistema autónomo es un conjunto de redes bajo una administración común que comporten las mismas políticas de enrutamiento.

Los sistemas autónomos, también conocidos como dominios, pueden dividirse en lo que se denomina como áreas. Las áreas son redes contiguas en conjunto con los *hosts* que se encuentran junto a ellas.

Una de las ventajas al tener dividido en áreas un sistema autónomo es que se disminuye la información de enrutamiento que los *routers* de cada área tienen que almacenar, siendo esta tan sólo la referente a su propia área, y el como llegar al área que interconecta a todas, es decir, la dorsal principal. Todos los *routers* que tienen varias interfaces pueden ser miembros de varias áreas y se denominan ABR's (*Area Border Routers*), que son los que forman la dorsal principal (área 0). En si, los *routers* de la dorsal principal forman un área OSPF. Cada uno de estos mantiene en forma separada una base de datos de la topología de la red de cada área donde se encuentra adjuntado. La topología de cada área es conocida solo por los *routers* involucrados en dicha área, estando oculta para los *routers* de otras áreas.

Las bases de datos de la topología de la red son básicamente una imagen completa de las ligas que mantienen las redes en relación a los *routers*, y se forman con base a los LSA's (*link-state advertisements*) que envían de forma incremental a los *routers* (es decir, sólo cuando existe un cambio en la red). Ahora como estos avisos son enviados a todos los *routers* que se encuentran dentro de la misma área, estos *routers* tendrán la misma base de datos de la topología de la red.

Con base a está jerarquía, se establecen básicamente dos formas de comunicarse entre los *routers*. La primera se establece si los *routers* involucrados se encuentran en la misma área jerárquica, conociéndose como enrutamiento intraárea. La segunda se forma cuando los *routers* están en áreas distintas, conociéndose como interárea.

El conjunto de todos los ABR's es lo que conforman la dorsal principal, y estos *routers* son los encargados de la distribución de las bases de datos de la topología de las distintas áreas.

Algoritmo SPF

Cuando un *router* configurado para correr OSPF inicia operaciones, lo primero que realiza es iniciar una estructura de datos del protocolo de enrutamiento, para poder almacenar la información de recibirá del estado de los enlaces de los cuales estará al pendiente. Después esperará información de los protocolos de capas inferiores, como la de enlace, que le dirán si las interfaces funcionan adecuadamente y si están listas para trabajar. Una vez establecido que funcionan, SPF empleará el protocolo HELLO de OSPF que servirá para conocer cuales *routers* están en su periferia, es decir sus vecinos. El *router* recién prendido, enviará estos paquetes y sus vecinos le enviarán una respuesta con los mismos paquetes HELLO logrando conocer quienes son sus vecinos. Otro de los objetivos de estos mensajes HELLO es conocer si un *router* vecino se encuentra disponible o no.

Otra de las tareas del protocolo HELLO es determinar el rol de los *routers* cuando estos se localizan en redes que soportan o que están funcionando con más de dos *routers* (por ejemplo en redes tipo ethernet o Frame Relay). Este tipo de redes se denominan como redes multiacceso y existen dos roles que pueden ser asignados a *routers* en este tipo de redes. El

primero es el *router* designado, aludiendo a que esta designado para generar los LSA's de la red multiacceso y de hacer réplicas de los LSA's internos hacia el exterior. El segundo rol es el *router* designado de respaldo.

Al tener un *router* encargado para la generación de los LSA's, esto reducirá cargas de tráfico de información de enrutamiento, ya que no tiene caso que varios *routers* con la misma información repliquen sus datos.

Formato de paquete
Los paquetes OSPF están constituidos por 9 campos comenzando con un encabezado de 24 bytes y terminando con el campo de datos, de tamaño variable.

Los campos son los siguientes:
Numero de versión: Contiene la versión del protocolo OSPF que se esta empleando.
Tipo: Contienen el tipo de paquete OSPF actual.
Tamaño de paquete: Contiene el tamaño en bytes, incluyendo el encabezado.
ID del Router: Contiene el identificador del *router* origen.
ID del Área: Contiene el identificador del área al que pertenece el paquete.
Checksum: Contiene información que ayuda a saber su el paquete sufrió alguna modificación durante su tránsito del origen al destino.
Tipo de autentificación: Parámetro configurable en cada *router* de área.
Autenticación: Contiene la información de la autenticación.
Datos: Contiene los datos.
La autenticación se realiza a través del algoritmo *Hash* MD5.

Algunos ejemplos de protocolos de enrutamiento de paquetes IP s

- **RIP:** Un protocolo de enrutamiento interior por vector-distancia.
- **IGRP:** El protocolo de enrutamiento interior por vector-distancia de Cisco.
- **OSPF:** Un protocolo de enrutamiento interior de estado del enlace
- **EIGRP:** El protocolo mejorado de enrutamiento interior por vector-distancia de Cisco.
- **BGP:** Un protocolo de enrutamiento exterior por vector-distancia

*IGRP (*Interior Gateway Routing Protocol*)*

Es un protocolo propietario de CISCO desarrollado a mediados de los años 80's y su principal objetivo fue proveer un protocolo de enrutamiento robusto que trabajara dentro de los sistemas autónomos. En un inicio se diseño para que trabajara en redes IP, aunque después se implementó para trabajar sobre cualquier ambiente de red lográndose que CISCO lo migrara para que se ejecutase en redes CLNP (*Connectionless-Network Protocol*).

A mediados de los 80's el protocolo IGP más común era RIP, aunque sus mismas limitaciones de alcance fueron creando la necesidad de crear un protocolo de enrutamiento más robusto que satisficiera las necesidades de las redes crecientes en cuanto a tamaño y tecnología y métodos de enrutamiento.

Características de IGRP

IGRP es un protocolo IGP cuyo algoritmo de enrutamiento esta clasificado como *vector distancia.*

Los *router*s que ejecutan el algoritmo *vector distancia*, realizan una comparación matemática de una medida de distancia como primer parámetro para determinar la mejor ruta. Esta medida de distancia se denomina como vector distancia. Los *routers* también deben de enviar información referente a su tabla de enrutamiento, ya sea una parte o toda su tabla en sus mensajes de actualización de enrutamiento hacia sus vecinos, exclusivamente. Soporta enrutamiento multiruta, es intradominio y es dinámico, además de tener una métrica compuesta.

La métrica compuesta se calcula en base a valores matemáticos que son tomados como factores de peso para la carga, el ancho de banda, la confiabilidad y el retardo de la red. Cada una de estas métricas puede tomar los valores que se muestran en la siguiente tabla (Figura 1.26).

Mínimo		Máximo
Retardo	1	2^{24}
Ancho de banda	1.2kbps	10Gbps
Confiabilidad	1	255
Carga	1	255

Figura.1.26 Tabla Métricas de IGRP

Estas métricas son complementadas por constantes que pueden ser definidas en forma manual. Estas constantes se mapean contra cada una de las métricas produciendo lo que sería una métrica compuesta.

Los valores de las métricas y el de las constantes pueden ser establecidos por el administrador, dándole la capacidad de poder influir en la determinación de la ruta escogida. Esto hace que IGRP sea un protocolo de enrutamiento muy flexible. Las actualizaciones se realizan por *broadcast* o difusión y se hace una actualización periódica completa de la tabla de enrutamiento. Se caracteriza por ser un protocolo *classfull*.

Características de estabilidad

Actualizaciones:

- *Holddowns*
- *Split horizon*
- *Poison-reverse*

Holddown

Es el tiempo durante el cual los *routers* mantienen un cambio en alguna ruta al menos hasta que todos los *routers* hayan sido actualizados. El tiempo es un poco mayor al que tomaría a la red completa haber actualizado sus tablas de enrutamiento.

Cuando una ruta se viene abajo en la red, un vecino se entera porque ya no le llegan mensajes de actualización de enrutamiento, entonces, este recalcula las nuevas rutas hacia los destinos que pasaban por la ruta caída y envía sus mensajes de actualización. Como estos mensajes de actualización ocurren en forma repentina (*triggered updates*), puede que no lleguen inmediatamente a todos los nodos de la red. En consecuencia, puede pasar que un *router* que tiene que ser avisado de la caída de alguna ruta, mande sus avisos de actualización de ruta a algún dispositivo que ya había sido avisado de la falla de dicha ruta, por lo que estarían incoherentes en cuanto a la información de enrutamiento. Por esto es necesario que los *routers* mantengan cierto tiempo algunas actualizaciones de rutas hasta que la información de enrutamiento sea coherente en toda la red.

Split horizon

Es un mecanismo que esta basado en la premisa de no enviar ninguna actualización de una ruta por la interfase por donde fue aprendida. Esto con el fin de prever *loops* que pudieran afectar el desempeño de la red.

Por ejemplo teniendo dos *routers*, el A y el B, siendo que el A tiene la red A mas cerca que B. El *router* A envía en sus mensajes de actualización a B que puede alcanzar la red A a través de él mismo. El B no tiene porque enviar en sus actualizaciones hacia A ninguna ruta que involucre la red A, ya que el *router* A esta más cerca que el B por lo que sería innecesario. La situación es esta: si el enlace hacia la red A falla, y si no se tuviera la regla *split horizon*, el *router* B le diría en sus mensajes al *router* A que puede alcanzar la red A a través del mismo *router* A, lo que sería un error. Si se tiene habilitada la regla, el *router* B no avisaría de las rutas que el mismo *router* A conoce y no se producirían *loops* en la comunicación.

Poison-reverse update

Este tipo de actualizaciones son llevadas a cabo para prevenir *loops* en redes grandes, un poco para complementar las reglas de *split horizon* que están para prevenir los *loops* entre *routers* adyacentes. Cuando una ruta de red es aprendida por un *router* a través de otro

router que no esta directamente conectado a dicha red, el primero colocara una métrica infinita hacia el *router* que no esta directamente conectado a la red.

Timers

IGRP mantiene una serie de variables y temporizadores que le ayudan a controlar sus procedimientos como las actualizaciones periódicas que realiza, entre otras cosas. El primer temporizador se llama de actualización, y especifica el periodo en el que debe de enviarse un mensaje de actualización de enrutamiento a los *routers* vecinos. Por omisión tiene un valor de 90 segundos. El siguiente temporizador se denomina de ruta inválida y determina el tiempo que debe de esperar un *router* por algún mensaje de actualización de una ruta antes de declararla inválida. El valor para esta variable es por defecto de tres veces el tiempo de la variable de actualización, o sea 270 segundos. Existe una tercera variable que determina el tiempo de *holddown*, por defecto es de tres veces el periodo de actualización mas 10 segundos, se llama *hold-time*. Por último el temporizador de flujo, que determina cuanto tiempo debe pasar para eliminar una ruta de la tabla de enrutamiento, vale 630 seg.

Tipos de rutas IGRP

IGRP anuncia tres tipos de rutas: internas, externas y de sistema. Las rutas internas son rutas de las subredes que están en la red adjunta a la interfase del *router*. Las rutas externas son aquellas que no pertenecen al sistema autónomo al que pertenece el *router*. Las rutas de sistema son rutas que están dentro del sistema autónomo. Las rutas de sistema no incluyen información de las subredes.

Formato de paquete

El paquete de IGRP consta de 8 campos. Un mismo paquete puede contener múltiples entradas, máximo hasta 104. Las entradas siguen inmediatamente de este encabezado de paquete.

Los campos son:

Versión: Actualmente con valor 1.

Código OP: Cuando son paquetes de petición IGRP vale 1 y cuando son de actualización IGRP es 2.

Edición: Este campo evita aceptar una actualización anterior a la más reciente. Su valor siempre se incrementa cuando ocurre un cambio en la información de enrutamiento.

Número de Sistema Autónomo: Se refiere al ID (identificador) del proceso IGRP. Permite que múltiples procesos IGRP intercambien información empleando un mismo enlace de datos común.

Número de Rutas Interiores: Número de entradas en la actualización que son subredes de una red conectada directamente.

Número de Rutas del Sistema: Número de rutas de redes que no están conectadas directamente. Por ejemplo rutas que han sido sumarizadas por un *router* de frontera.

Número de Rutas Exteriores: Número de rutas de redes que han sido identificadas como redes por *default*.

Checksum: Se calcula sobre el encabezado IGRP y todas las entradas empleando complemento a uno de 16 bits de la suma.

BGP (Border Gateway Protocol)

El Protocolo de gateway de frontera (BGP) es un protocolo de enrutamiento exterior (Figura 1.27). Las características claves del BGP son las siguientes:

- Es un protocolo de enrutamiento exterior por vector-distancia.
- Se usa entre ISPs o entre los ISPs y sus clientes.
- Se usa para enrutar el tráfico de Internet entre sistemas autónomos.

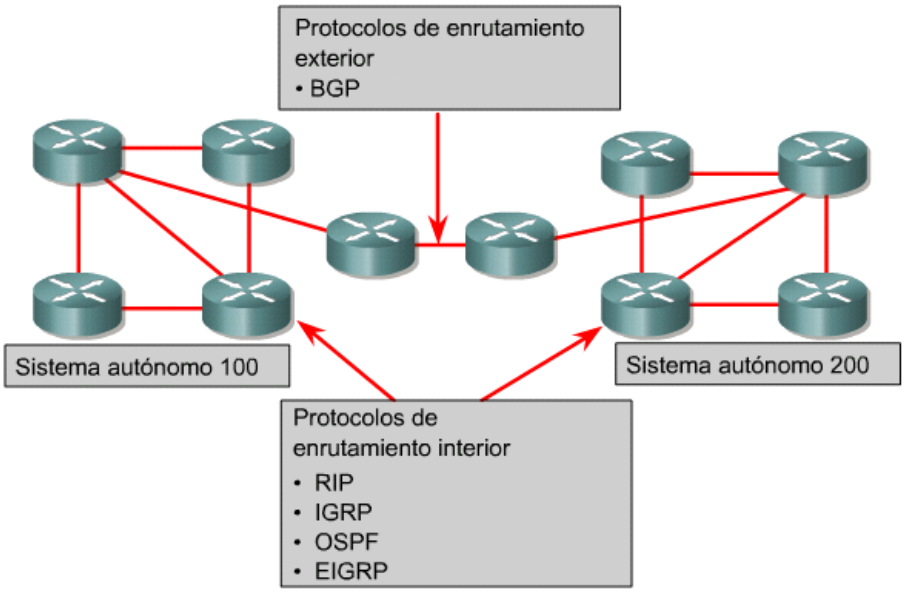


Figura 1.27. Podemos ver los diferentes tipos de protocolos de enrutamiento exterior (BGP – Border Gateway Protocol) e interior.

Los protocolos de enrutamiento interior están diseñados para ser usados en redes cuyos segmentos se encuentran bajo el control de una sola organización. Los criterios de diseño de los protocolos de enrutamiento interior requieren que el protocolo encuentre la mejor ruta a través de la red. En otras palabras, la métrica y la forma en que esta se utiliza es el elemento más importante de un protocolo de enrutamiento interior.

1.5.2.1 Vector Distancia

El método de enrutamiento por vector-distancia determina la dirección (vector) y la distancia hacia cualquier enlace en la red.

Los protocolos de enrutamiento por vector-distancia envían copias periódicas de las tablas de enrutamiento de un router a otro. Estas actualizaciones periódicas entre routers informan de los cambios de topología. Los algoritmos de enrutamiento basados en el vector-distancia también se conocen como algoritmos Bellman-Ford.

Cada router recibe una tabla de enrutamiento de los routers conectados directamente a él. El router B recibe información del router A. El router B agrega un cifra de vector-distancia (por ejemplo: el número de saltos), la cual aumenta el vector-distancia. Luego el router B pasa esta nueva tabla de enrutamiento a su otro vecino, el router C. Este mismo proceso, paso a paso, se repite en todas direcciones entre routers vecinos.

El algoritmo finalmente acumula información acerca de las distancias de la red, las cual le permite mantener una base de datos de la topología de la red. Sin embargo, los algoritmos de vector-distancia no permiten que un router conozca la topología exacta de una red, ya que cada router solo ve a sus routers vecinos.

Cada router que utiliza el enrutamiento por vector-distancia comienza por identificar sus propios vecinos (Figura 1.28) La interfaz que conduce a las redes conectadas directamente tiene una distancia de 0. A medida que el proceso de descubrimiento de la red avanza, los routers descubren la mejor ruta hacia las redes de destino, de acuerdo a la información de vector-distancia que reciben de cada vecino. Por ejemplo, el router A aprende acerca de otras redes según la información que recibe del router B. Cada una de las redes de destino en la tabla de enrutamiento tiene una cifra total de vector-distancia, la cual indica la distancia a la que se encuentra dicha red por una ruta determinada.

Las actualizaciones de las tablas de enrutamiento se producen al haber cambios en la topología. Al igual que en el proceso de descubrimiento de la red, las actualizaciones de cambios de topología avanzan paso a paso, de un router a otro. Los algoritmos de vector-distancia hacen que cada router envíe su tabla de enrutamiento completa a cada uno de sus vecinos adyacentes. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta (definido por su métrica) y la dirección lógica del primer router en la ruta hacia cada una de las redes indicadas en la tabla.

Una analogía del vector-distancia podría ser los carteles que se encuentran en las intersecciones de las autopistas. Un cartel indica el destino e indica la distancia hasta el

destino. Más adelante en la autopista, otro cartel indica el destino, pero ahora la distancia es mas corta. A medida que se acorta la distancia, el tráfico sigue la mejor ruta.

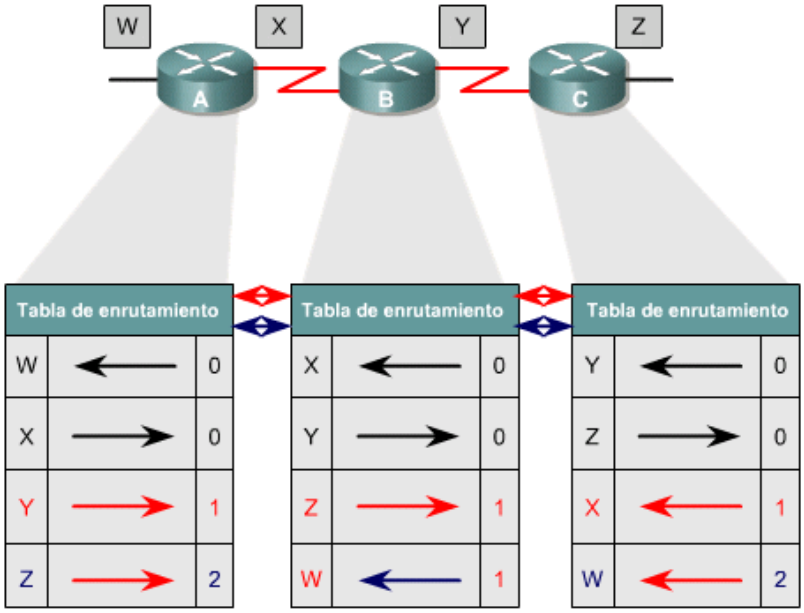


Figura 1.28. Descubrimiento de la red por vector-distancia.

1.5.2.2 Estado de Enlace

El método de estado del enlace, también denominado "primero la ruta más corta", recrea la topología exacta de toda la red.

El segundo algoritmo básico que se utiliza para enrutamiento es el algoritmo de estado del enlace. Los algoritmos de estado del enlace también se conocen como algoritmos Dijkstra o SPF ("primero la ruta más corta"). Los protocolos de enrutamiento de estado del enlace mantienen una base de datos compleja, con la información de la topología de la red. El algoritmo de vector-distancia provee información indeterminada sobre las redes lejanas y no tiene información acerca de los routers distantes. El algoritmo de enrutamiento de estado del enlace mantiene información completa sobre routers lejanos y su interconexión.

El enrutamiento de estado del enlace utiliza:

- **Publicaciones de estado del enlace (LSA):** una publicación del estado del enlace (LSA) es un paquete pequeño de información sobre el enrutamiento, el cual es enviado de *router* a *router*.
- **Base de datos topológica:** una base de datos topológica es un cúmulo de información que se ha reunido mediante las LSA.
- **Algoritmo SPF:** el algoritmo "primero la ruta más corta" (SPF) realiza cálculos en la base de datos, y el resultado es el árbol SPF.
- **Tablas de enrutamiento:** una lista de las rutas e interfaces conocidas.

Proceso de descubrimiento de la red para el enrutamiento de estado del enlace:

El intercambio de LSAs se inicia en las redes conectadas directamente al router, de las cuales tiene información directa. Cada router, en paralelo con los demás, genera una base de datos topológica que contiene todas la información recibida por intercambio de LSAs.

El algoritmo SPF determina la conectividad de la red. El *router* construye esta topología lógica en forma de árbol, con él mismo como raíz, y cuyas ramas son todas las rutas posibles hacia cada subred de la red. Luego ordena dichas rutas, y coloca las ruta más cortas primero (SPF). El *router* elabora una lista de las mejores rutas a las redes de destino, y de las interfaces que permiten llegar a ellas. Esta información se incluye en la tabla de enrutamiento. También mantiene otras bases de datos, de los elementos de la topología y de los detalles del estado de la red. (Figura 1.29)

El *router* que primero conoce de un cambio en la topología envía la información al resto de los routers, para que puedan usarla para hacer sus actualizaciones y publicaciones.(Figura 1.30) Esto implica el envío de información de enrutamiento, la cual es común a todos los routers de la red. Para lograr la convergencia, cada router monitorea sus *routers* vecinos, sus nombres, el estado de la interconexión y el costo del enlace con cada uno de ellos. El *router* genera una LSA, la cual incluye toda esa información, junto con información relativa a nuevos vecinos, los cambios en el costo de los enlaces y los enlaces que ya no son válidos. La LSA es enviada entonces, a fin de que los demás *routers* la reciban.

Cuando un *router* recibe una LSA, actualiza su base de datos con la información más reciente y elabora un mapa de la red con base en los datos acumulados, y calcula la ruta más corta hacia otras redes mediante el algoritmo SPF. Cada vez que una LSA genera cambios en la base de datos, el algoritmo de estado del enlace (SPF) vuelve a calcular las mejores rutas, y actualiza la tabla de enrutamiento.

Puntos de interés acerca del estado del enlace

- Carga sobre el procesador.
- Requisitos de memoria.
- Utilización del ancho de banda.

Los *routers* que usan protocolos de estado del enlace requieren de más memoria y exigen mas esfuerzo al procesador, que los que usan protocolos de enrutamiento por vector-distancia. Los *routers* deben tener la memoria suficiente para almacenar toda la

información de las diversas bases de datos, el árbol de topología y la tabla de enrutamiento. (Figura 1.31) La avalancha de LSAs que ocurre al activar un router consume una porción del ancho de banda. Durante el proceso de descubrimiento inicial, todos los routers que utilizan protocolos de enrutamiento de estado del enlace envían LSAs a todos los demás routers. Esta acción genera un gran volumen de tráfico y reduce temporalmente el ancho de banda disponible para el tráfico enrutado de los usuarios. Después de esta disminución inicial de la eficiencia de la red, los protocolos de enrutamiento del estado del enlace generalmente consumen un ancho de banda mínimo, sólo para enviar las ocasionales LSAs que informan de algún cambio en la topología.

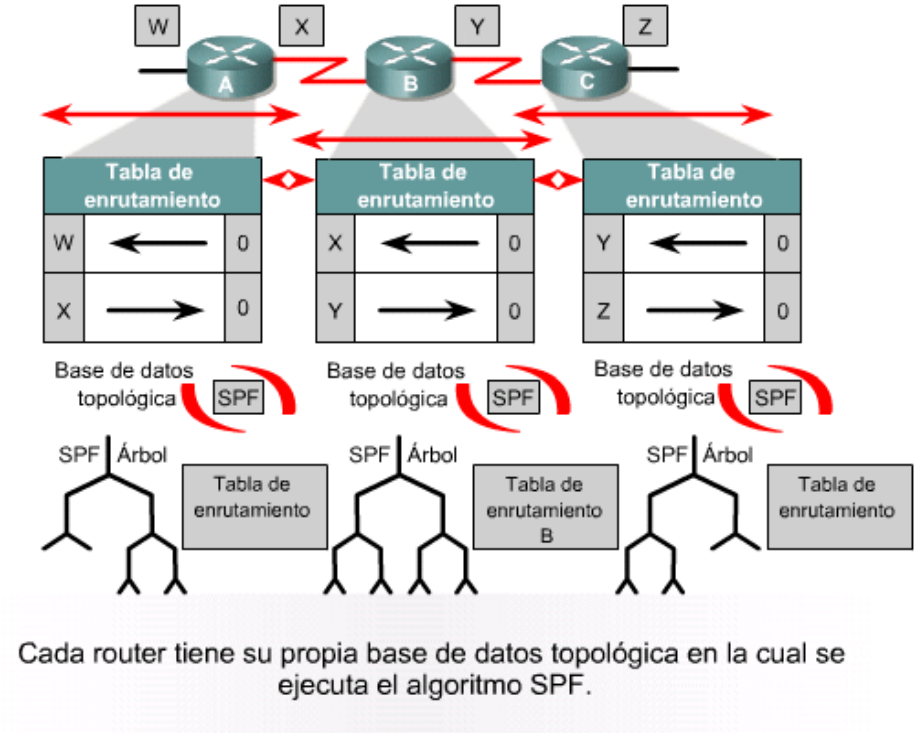


Figura 1.29 Detección de red por estado de enlace.

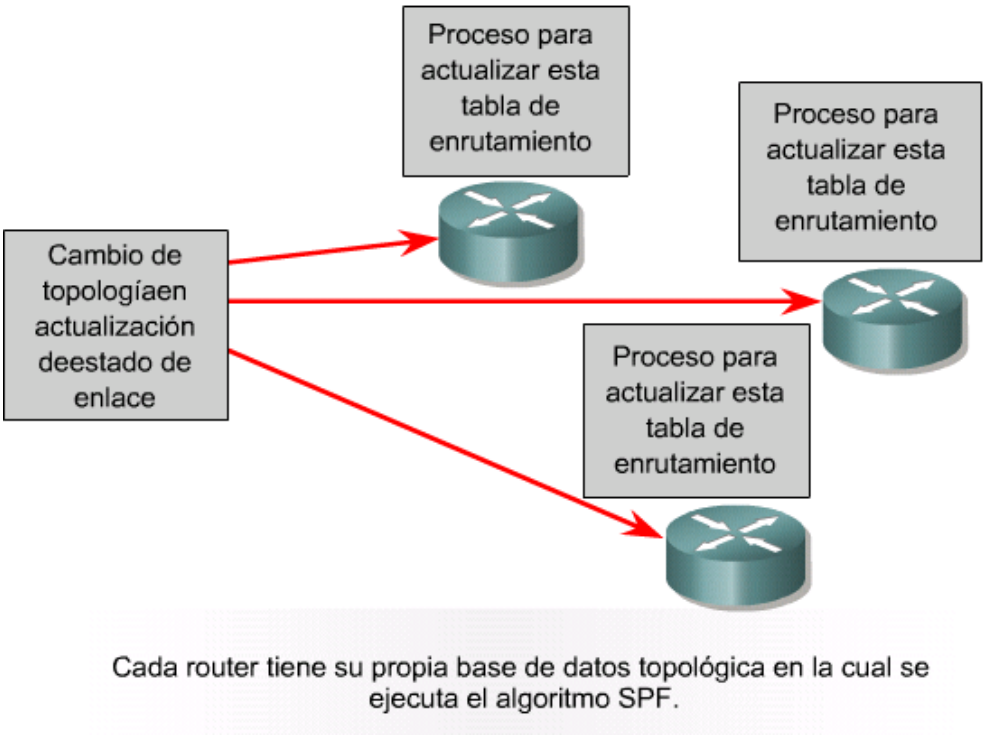


Figura. 1.30 Cambios de la topología de estado de enlace.

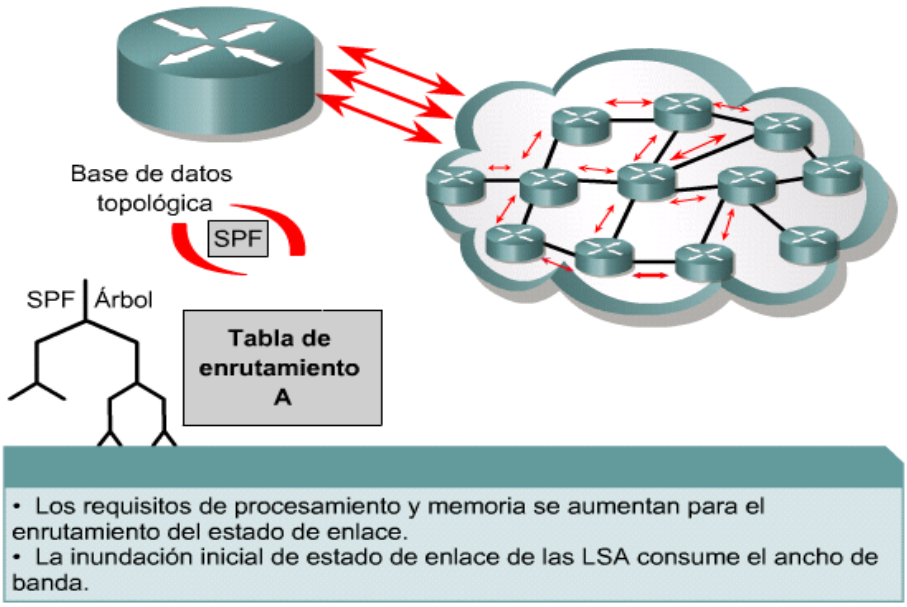


Figura. 1.31 Cuestiones del estado de enlace.

1.5.2.3 Híbrido

Además de los protocolos de estado del enlace y de los protocolos de vector distancia también disponemos de los protocolos de enrutamiento híbridos equilibrados.

Estos protocolos utilizan la métrica de los protocolos vector distancia como métrica, sin embargo utiliza en las actualizaciones de los cambios de topología bases de datos de topología, al igual que los protocolos de estado del enlace.
Un ejemplo de protocolo híbrido sería EIGRP.

*EIGRP (*Enhanced Interior Gateway Routing Protocol*)*

EIGRP fue el resultado del constante cambio en cuanto a la diversidad y el tamaño de las redes actuales. Su arquitectura esta basada en módulos y soporta por si mismo múltiples protocolos de capa de red existentes. Sus capacidades y eficiencia se ve mejorada al implementar los beneficios de los algoritmos *link-state* junto con los *vector-distancia*, clasificándose como híbrido.

EIGRP es la versión actualizada de IGRP, agrega mas funcionalidades que lo hacen un protocolo de enrutamiento sumamente robusto y estable, y tiene una excelente compatibilidad con su antecesor IGRP. Las rutas son fácilmente importables y exportables de IGRP a EIGRP y viceversa. Las métricas pueden emplearse indistintamente para ambos protocolos ya que son fácilmente trasladables, si es que son empleadas por *routers* dentro de un mismo sistema autónomo.

EIGRP posee un conjunto de protocolos adicionales que le hacen ser un protocolo de enrutamiento más eficiente en comparación con los basados en algoritmos vector-distancia.

Características de EIGRP

Las principales capacidades que provee EIGRP que sobresalen en comparación con los otros protocolos de enrutamiento son:

- Rápida convergencia
- Soporte de VLMS
- Actualizaciones parciales
- Soporte para múltiples protocolos de capa de red

Para ciertos tipos de paquetes que maneja EIGRP, se manejan lo que son transmisiones *multicast* en lugar de *unicast*. Esto permite que varias entidades puedan recibir en una única transmisión información referente al estado de los vecinos, lo que ocasiona un tiempo de convergencia menor que otros protocolos de enrutamiento. El soporte de VLMS permite que las rutas puedan ser sumarizadas, lo que provoca que las tablas de rutas sean de menor tamaño y que cierta información de enrutamiento sea menos densa. Los *routers* que corren EIGRP almacenan las tablas completas de enrutamiento de sus vecinos, lo que les permite fácilmente encontrar rutas alternas y si no las encuentran lanzan peticiones a sus vecinos solicitando información sobre rutas alternas. Las actualizaciones de información de

enrutamiento son parciales y ocurren solo cuando la métrica de una ruta ha cambiado. Las actualizaciones son parciales para no enviar información que puede estar ya contenida en los demás *routers*, lo que ahorra consumo en ancho de banda, y se limita sólo a aquellos *routers* que necesitan ser actualizados. La capacidad de EIGRP para trabajar con múltiples protocolos de red lo hacen sumamente escalable, además de que puede adaptarse para trabajar con nuevos protocolos de capa de red desarrollados por distintas entidades de acuerdo a sus necesidades.

Las tecnologías que permiten que EIGRP soporte múltiples protocolos de red, además de mejorar los tiempos de convergencia y de soportar solo actualizaciones periódicas son descritas en seguida.

Tecnologías fundamentales de EIGRP

Las cuatro tecnologías que permiten un mejor desempeño de EIGRP sobre los demás protocolos de enrutamiento son:

- *Neighbor discovery/recovery*
- RTP (*Reliable Transport Protocol*)
- *DUAL finite-state machine*
- *Protocol-dependent modules*.

Neighbor discovery/recovery

Este mecanismo se basa en el envió de pequeños mensajes *hello*. Estos son enviados periódicamente a los vecinos. Una vez recibidos, el *router* lo interpreta como una señal que indica que están listos para intercambiar información. Este mecanismo habilita a los *routers* para conocer si un vecino es alcanzable y esta funcionando, permitiéndoles aprender dinámicamente acerca de otros *routers* que se encuentran directamente conectados a su red.

RTP (Reliable Transport Protocol)

Este mecanismo es el encargado de garantizar que los paquetes EIGRP sean entregados a todos los vecinos. Este protocolo será el responsable de que los tiempos de convergencia sean bajos. Cuando estamos en un medio donde hay soporte *multicast*, como es el caso de la tecnología *Ethernet*, RTP aprovecha esta capacidad para enviar solo un paquete *multicast* del tipo *hello* en lugar de transmitir paquetes *unicast* hacia los *routers* vecinos en forma individual. Este tipo de paquetes son los que no se requiere que sean entregados en forma confiable, por cuestiones de eficiencia. En cambio algunos otros paquetes EIGRP necesitan ser enviados en forma confiable como es el caso de los paquetes de actualización. Cuando se envían paquetes EIGRP en forma no confiable, el paquete contiene un indicador que le informa al receptor que no es necesario hacer un reconocimiento de dicho paquete. En cambio, cuando se envía un paquete en forma confiable, este indicador le dice al receptor que debe existir un reconocimiento de dicho paquete.

DUAL finite-state machine

Este algoritmo involucra el proceso de cálculo relacionado con todas las rutas advertidas por todos los *routers* vecinos. Emplea información de distancia para seleccionar rutas libres de *loops* y para elegir aquellas rutas que han de ser agregadas a las tablas de enrutamiento a través de los *feasible successors*.

Los *feasible successors* son *routers* que se encargan del envío de paquetes a través de las rutas con el menor costo hacia un destino, garantizando que la ruta elegida no forma parte de un camino con *loops*. Estos son empleados para evitar hacer recálculos de las rutas cuyas métricas han cambiado. Esto es, cuando la métrica de una ruta cambia, el algoritmo de actualización por difusión (DUAL) revisa si existe un *routers feasible sucesor*, si sí, no se realiza el recálculo para encontrar la mejor ruta. Si no existe un *feasible sucesor*, el recálculo es obligatorio para determinar el nuevo *feasible sucesor*. Este recálculo se llama cálculo por difusión y comienza con el envió de un paquete de petición de un *router* hacia todos sus vecinos. Cada uno de estos vecinos puede enviar dos tipos de respuestas: la primera para indicar que tiene un *feasible successor* disponible para la ruta y la segunda que indicaría que esta participando en el recálculo. Después de recibir respuesta de cada uno de los vecinos, el *router* puede alterar la información del destino en la tabla de enrutamiento y elegir un nuevo *feasible successor*.

Protocol-dependent modules

Estos módulos son los encargados de cumplir los requisitos específicos de cada protocolo de capa de red. Los protocolos más comunes para los cuales provee soporte son IPv4, AppleTalk e IPX.

Componentes de enrutamiento para EIGRP

Para poder desempeñarse como protocolo de enrutamiento, EIGRP se basa en cuatro conceptos fundamentales.

Tablas de vecinos

Cuando un nuevo vecino es encontrado, la información referente a su interfase y su dirección es almacenada en la tabla. También se almacena información que emplea el RTP. Esta información son números de secuencia que sirven para llevar un control de los reconocimientos y los paquetes. Para poder detectar cuando los paquetes están en desorden, se almacena el último número de secuencia enviado por un *router*. Por cada modulo de dependencia de protocolo de red existe una tabla de vecino. Cuando un paquete *hello* se envía, lleva asociado un tiempo que determinará el tiempo que un vecino considerará alcanzable y funcional al *router* emisor. Si durante este tiempo no es recibido algún otro paquete *hello*, entonces el emisor se determina inalcanzable y automáticamente este cambio en la topología de la red es informado al algoritmo de actualización por difusión.

Tablas de la topología
Estas tablas contienen todos los destinos anunciados por los *router* vecinos además de una lista de los vecinos que han anunciado dichos destinos y las métricas por cada vecino. En cuanto a la métrica, se anunciará la menor resultante de sumar la ruta advertida de todos los vecinos más el costo de la interfase por donde se aprendió dicha ruta.

Estados de ruta
Indican el estado en que se encuentra una ruta hacia un destino. Cuando un *router* no realiza un recálculo referente a un destino se dice que la ruta esta en estado pasivo. Cuando se realiza el recálculo, se dice que esta en estado activo. Evidentemente cuando existe un *feasible successor*, las rutas estarán en estado pasivo.

Etiquetado de ruta

EIGRP soporta rutas internas y rutas externas. Las rutas internas serán aquellas asociadas a dispositivos que se encuentren conectados directamente a los dispositivos de red que estén configurados para ejecutar EIGRP dentro del sistema autónomo EIGRP. Las rutas externas serán las aprendidas por otros protocolos de enrutamiento o aquellas rutas estáticas que residan en las tablas de enrutamiento.

Las rutas externas son etiquetadas con la siguiente información:

- ID del *router* EIGRP que distribuyo la ruta
- Número del sistema autónomo del destino
- Etiqueta de administrador configurable
- Identificador del protocolo externo
- Métrica del protocolo externo
- Bit como bandera para enrutamiento por defecto.

El etiquetado de las rutas permite a los administradores personalizar y tener control sobre las políticas de enrutamiento.

Tipos de paquetes EIGRP

Los tipos de paquetes que emplea EIGRP son:
- *Hello*
- *Acknowledge*
- *Update*
- *Query* y *reply*

Los paquetes *hello* son empleados por el mecanismo de *neighbor discovery/recovery* y no requieren de un reconocimiento. Son enviados en transmisiones *multicast*.

Los paquetes Acknowledge es un paquete *hello* pero sin datos. Siempre son enviados en transmisiones *unicast.*

Los paquetes *update* se emplean para indicar el grado de alcance de un destino. Siempre son enviados en forma confiable y cuando se ha descubierto un vecino nuevo, son enviados en transmisiones *unicast* para que puedan construir sus tablas de topología.

Los paquetes *query* son enviados en forma confiable y siempre son *multicast*.

Los paquetes *reply* son enviados en forma confiable y se envían para indicar al *router* que origino un query que no recalcule una ruta si es que existe un *feasible successor*. Son paquetes *unicast* dirigidos al *router* que realizó el *query*.

Formato de paquete

Consta de un encabezado de 7 campos con un tamaño de 20 bytes más un campo TLV de tamaño variable.

Los campos significan:
Versión: Vale 1.
Código OP: Indica el tipo de paquete.

1. *Update*
2. *Query*
3. *Reply*
4. *Hello*
5. IPX SAP

Checksum: Se calcula sobre la porción completa de EIGRP del datagrama IP.
Banderas: El bit *INIT*, cuando vale 1, significa que la ruta contenida en ese paquete es la primera de una nueva relación de vecinos. El bit *Condicional Receive*, cuando vale 2, es empleado por el algoritmo de *Multicast Reliable* de CISCO.
Secuencia: Un número de secuencia de 32 bits que usa RTP.
ACK: La última secuencia de 32 bits que fue escuchada de un vecino. Por ejemplo, un paquete *hello* con un valor distinto de cero es un ACK.
Número de Sistema Autónomo: El número de SA del dominio EIGRP.
TLV (Type/Length/Value): Existen varios tipos de TLV's, pero todos comienzan por un campo de 2 bytes denominado Tipo seguido de un campo de 2 bytes que indica tamaño.

Los campos que siguen dependen del valor del campo Tipo, clasificándose como sigue:
TLV's generales:

Tipo
0x0001: Parámetros EIGRP generales.
0x0003: Secuencia (Usado por *Reliable Multicast* de CISCO)
0x0004: Versión del *software* EIGRP.
0x0005: Próxima secuencia *multicast* (Usado por *Reliable Multicast* de CISCO)
TLV's IP:
Tipo
0x0102: Rutas internas IP
0x0103: Rutas externas IP
TLV's Apple Talk
Tipo
0x0202: Rutas internas *Apple Talk*
0x0203: Rutas externas *Apple Talk*
0x0204: Configuración de cable *Apple Talk*
TLV's IPX
Tipo
0x0302: Rutas internas IPX
0x0303: Rutas externas IPX

En resumen el protocolo híbrido (EIGRP) contiene las principales características de los algoritmos Vector Distancia y Estado del Enlace (Figura 1.32).

PROTOCOLO HIBRIDO	
Vector Distancia	**Estado del Enlace**
Vista de la topología de la red desde la perspectiva del vecino	Consigue una vista común de toda la topología de la red
Añade vectores de distancias de router a router	Calcula la ruta más corta hasta otros routers
Frecuentes actualizaciones periódicas, convergencia lenta	Actualizaciones activadas por eventos, convergencia rápida
Pasa copias de la tabla de enrutamiento a los routes vecinos	Pasa las actualizaciones de enrutamiento de estado del enlace a los otros routers

Figura. 1.32. El Protocolo híbrido tienes las principales características de Vector Distancia y Estado de Enlace

1.6 Metodología de diseño de una red de datos

Dada la complejidad que conlleva realizar la reingeniería de una red de servicios múltiples, es necesario desarrollar una metodología, la cual nos va a servir para realizar paso por paso el nuevo diseño de la red.
En términos generales la metodología para el diseño de una red de datos, se compone de diferentes etapas y cada etapa comprende diferentes puntos, la metodología propuesta por nosotros en el índice de la tesis, coincide perfectamente con las etapas marcadas de forma general en el diseño de una red, a continuación veremos cada una de estas etapas y así mostraremos que cada una de ellas encaja perfectamente en cada capitulo de nuestra tesis.

Etapas de metodología de diseño de una red de servicio múltiple en términos generales:

- Etapa1. Recopilación de información.
- Etapa 2. Análisis y propuesta del diseño.
- Etapa 3. Prueba piloto.
- Etapa 4. Implementación masiva.
- Etapa 5. Entrega de documentación.

Etapa 1. Recopilación de Información.

En esta etapa nos encargaremos de buscar la información necesaria que nos llevo a obtener los aspectos principales y más importantes que componen a la red de datos, los cuales se enuncian a continuación:

- Topología
- Cobertura o distribución.
- Cantidad y tipo de enlaces
- Cantidad y tipo de equipos
- Esquemas de red local
- Protocolos utilizados
- Redundancia
- Direccionamiento
- Interconexión con otras redes
- Funcionamiento
- Fechas de puesta en operación

Etapa 2. Análisis y propuesta del diseño.

En esta etapa nos encargamos de analizar la información recopilada para poder llegar así a proponer un nuevo diseño de la red el cual contempla los siguientes aspectos:

- Topología
- Capacidad, cantidad y tipos de enlace
- Cantidad y tipos de equipo
- Protocolos a emplear
- Esquemas de redundancia
- Esquemas de calidad de servicio
- Direccionamiento

- Esquemas de interconexión con otras redes
- Esquemas de red local
- Esquemas de seguridad
- Funcionalidades y tecnologías para optimizar el desempeño

Etapa 3. Prueba Piloto

En esta etapa, analizaremos aspectos que nos sirven para saber si la red va a funcionar de una manera adecuada, y si va a poder cubrir nuestras necesidades futuras, estos puntos son los siguientes:

- Definición del lugar
- Análisis del impacto de la prueba
- Definición del proceso de implantación
- Desarrollo de pruebas definidas
- Periodo de observación

Etapa 4. Implementación Masiva

Esta es una etapa en la que el nuevo diseño de la red se lleva al plano real, y en la que analizamos cada aspecto para saber cual es la mejor manera de implementar la red, estos aspectos son los siguientes:

- Elaborar procesos de implementación
- Tiempos de compra y entrega de equipo
- Tiempo de solicitud e instalación de enlaces
- Tiempos de instalación de equipo
- Tiempos de adecuamiento del lugar
- Tiempos de configuración de equipos
- Tiempos de integración de aplicaciones y usuarios
- Fecha de entrega del proyectos

Etapa 5. Entrega de Documentación

Esta ya es la etapa final en que todos los aspectos técnicos y de funcionamiento de la red se documentan, para así poder tener un respaldo escrito de los aspectos que componen nuestra red, los cuales son los siguientes:

- Memoria técnica
- Topología
- Parámetros de salud (procesamiento, tiempos de respuesta, utilización de enlaces)
- Índices de disponibilidad de la red
- Configuraciones
- Costos

Capitulo II. Escenario de la Red Actual

2.1 Análisis y Características del Estado de la Red Actual

En el presente capitulo se expondrán las características de la red actual y en la cual nos basaremos para realizar la red propuesta.
Cabe mencionar que esta red actual cuenta con múltiples errores en cuanto a su estructura y lógica (topología y direccionamiento).

Actualmente la red cuenta con 3 regiones (Región 4 Monterrey, Región 5 Guadalajara, Región 6 Metropolitana y un backbone), las cuales tienen su infraestructura de datos propia, ocupando un direccionamiento estático en cada una de estas regiones y el backbone, las cuales describirán a continuación.

Características de la Región 4 (Monterrey)
Segmento IP: 192.4.0.0/16

Cantidad y tipo de equipos:
2 *routers* 7507 (MTY_R_1) y (MTY_R_2).
2 *routers* 2514 (MTY_R_4) y (MTY_R_3)
1 *router* 3745 (MTY_R_5).

Interfaz Loopback:
MTY_R_1 : 192.168.200.1/32
En esta regiòn solo un equipo contaba con loopback

Segmentos Lan:
Lan 1: 192.4.102.0/24
25 usuarios administrativos

Lan 2: 192.4.221.0 /24
30 usuarios administrativos

Lan 3: 192.4.104.0/24
35 usuarios administrativos

Lan 4: 192.4.204.0/24
10 usuarios administrativos

En la figura 2.1 se muestra la topología de la región 4

TOPOLOGÍA ACTUAL DE LA REGIÓN 4 (MONTERREY)

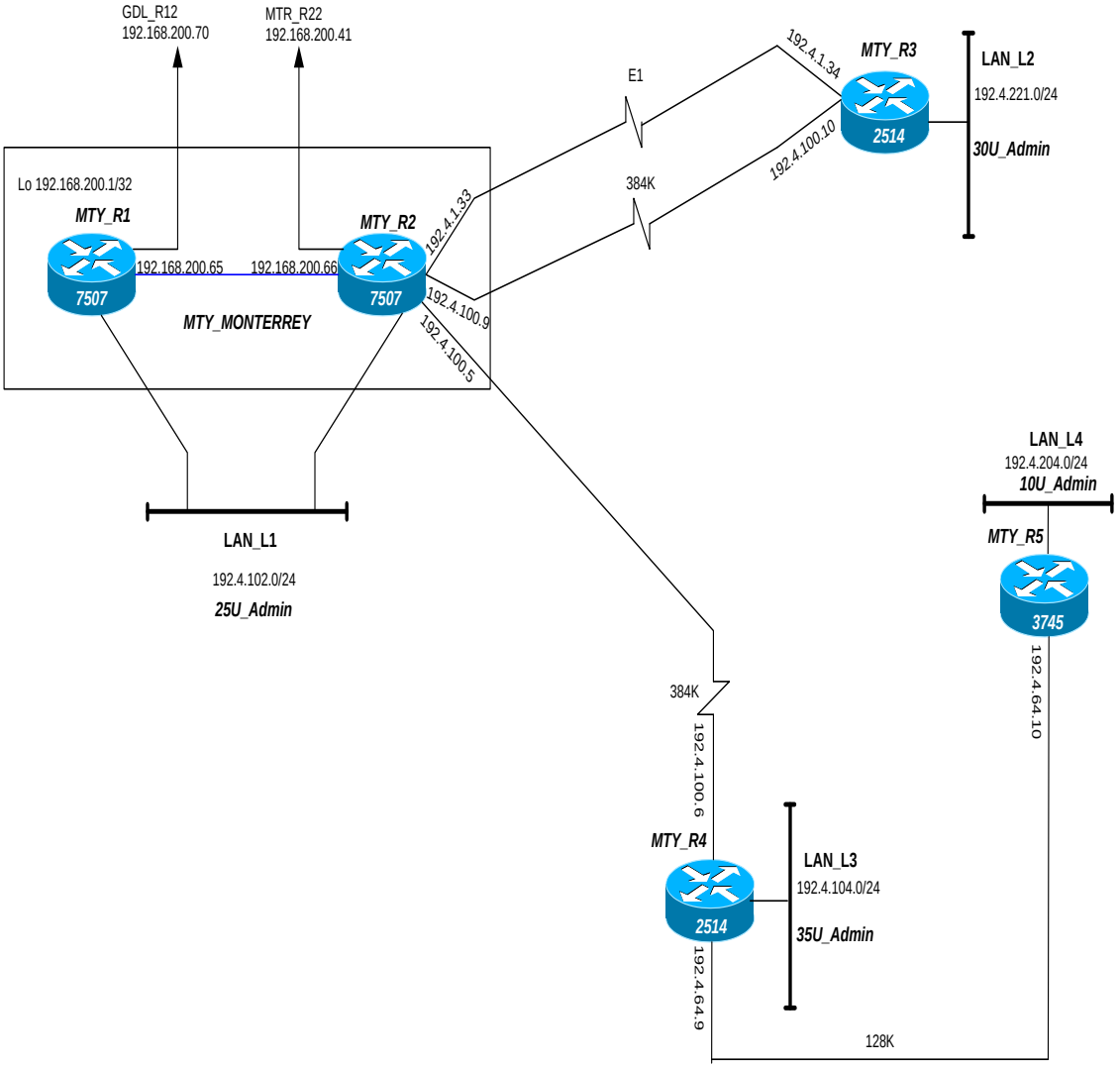


Figura 2.1 Topología de la región 4

Esta región consta de 2 *routers* 7507 (MTY_R_1 y MTY_R_2), estos están unidos por un enlace serial, tienen conexión hacia un segmento *Lan* 1, estos equipos tienen conexión a otros dorsales los cuales son Guadalajara (GDL_R_{12}) y Metropolitana (MTR_R_{22}).
El *router* MTY_R_2 esta unido mediante dos enlaces (E1 y 384 *Kbps*) con el *router* MTY_R_3, también esta unido por un enlace de 384 *Kbps* a el *router* MTY_R_4.
A su vez el *router* MTY_R_4 esta unido por un enlace de 128 *Kbps* al *router* MTY_R_5.
No es correcto tener en serie varios equipos ya que en este caso si el router MTY_R_4 fallara, quedarían sin servicio los usuarios de las *Lan* 3 y 4.

Características de la Región 5 (Guadalajara)
Segmento IP: 192.5.0.0/16

Cantidad y tipo de equipos:
2 *routers* 7507 (GDL_R_{11}) y (GDL_R_{12}).
3 *routers* 3745 (GDL_R_{13}), (GDL_R_{14}) y el (GDL_R_{15}).

Interfaz Loopback:
GDL_R_{11} : 192.168.200.2/32
En esta regiòn solo un equipo contaba con loopback

Segmentos Lan:
Lan 5: 192.5.11.0/24
16 usuarios administrativos

Lan 6: 192.5.68.0/24
12 usuarios administrativos

Lan 7: 192.5.220.0/24
25 usuarios administrativos

Lan 8: 192.5.222.0/24
38 usuarios administrativos

En la Figura 2.2 se muestra la topología de la Región 5

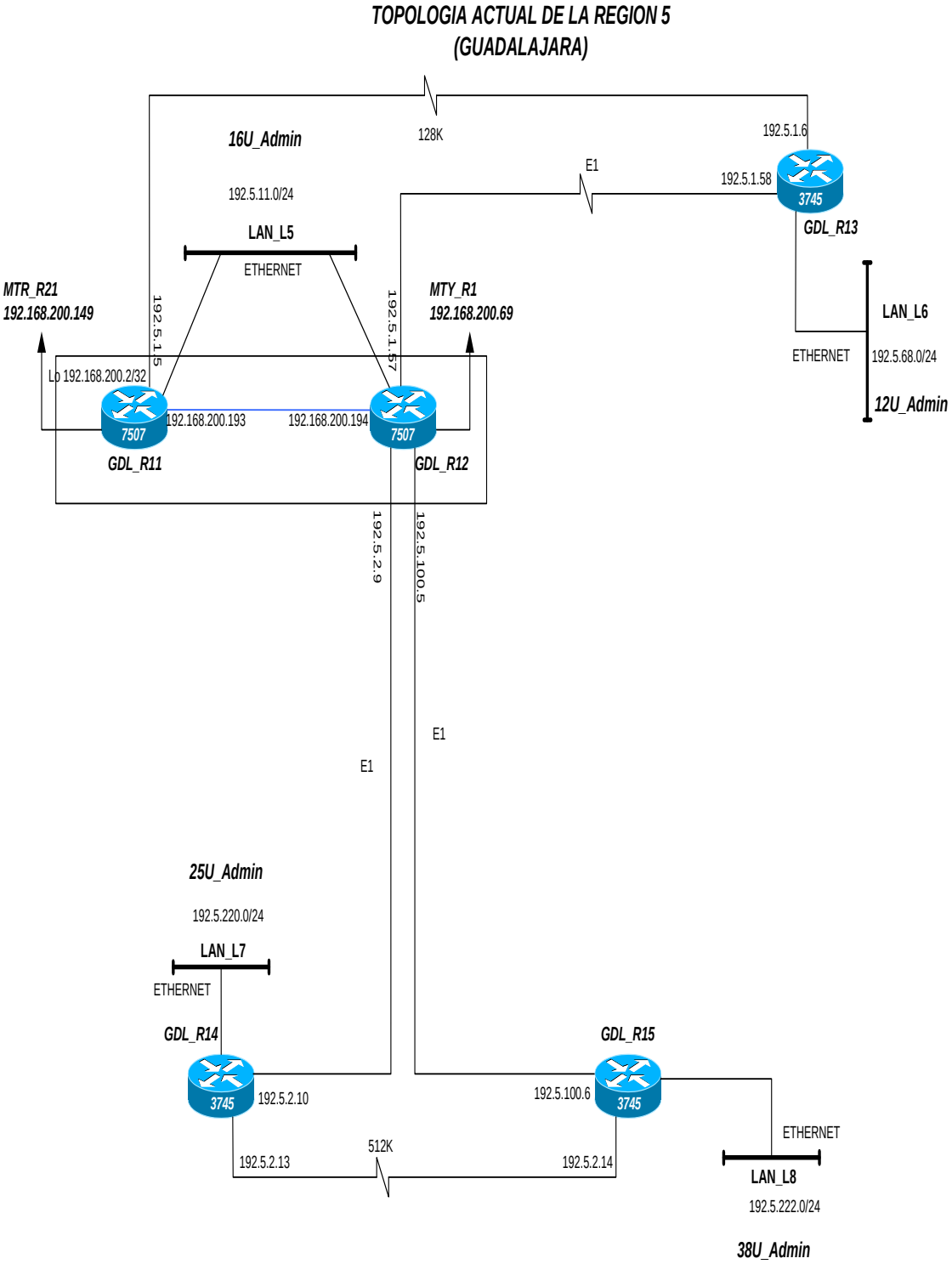


Figura 2.2 Topología de la región 5

Esta región consta de 2 *routers* GDL_ R_{11} y GDL_ R_{12}, estos están unidos por un enlace serial, tienen conexión hacia un segmento *Lan* 5, también tienen conexión a otros dorsales los cuales son Monterrey (MTY_ R_1) y Metropolitana (MTR_ R_{21}). El *router* GDL_ R_{12} tiene una conexión E1 hacia el router GDL_ R_{13}, y este a su vez tiene una conexión de 128 kbps hacia el router GDL_ R_{11}. El router GDL_ R_{12} esta conectado mediante un enlace E1 al router GDL_ R_{15} y mediante otro enlace E1 hacia el router GDL_ R_{14}, existe un enlace de 512 k entre los routers GDL_ R_{14} y GDL_ R_{15}.

Características de la Región 6 (Metropolitana)
Segmento IP: 192.6.0.0/16

Cantidad y tipo de equipos:
2 routers 7507 (MTR_ R_{21}) y el (MTR_ R_{22}).

Interfaz Loopback:
MTR_ R_{21} : 192.168.200.3/32
En esta regiòn solo un equipo contaba con loopback

Segmentos Lan:
Lan 9: 192.6.218.0/24
35 usuarios administrativos

Lan 10: 192.6.219.0/24
7 usuarios administrativos

En la Figura 2.3 se muestra la topología de la Región 6

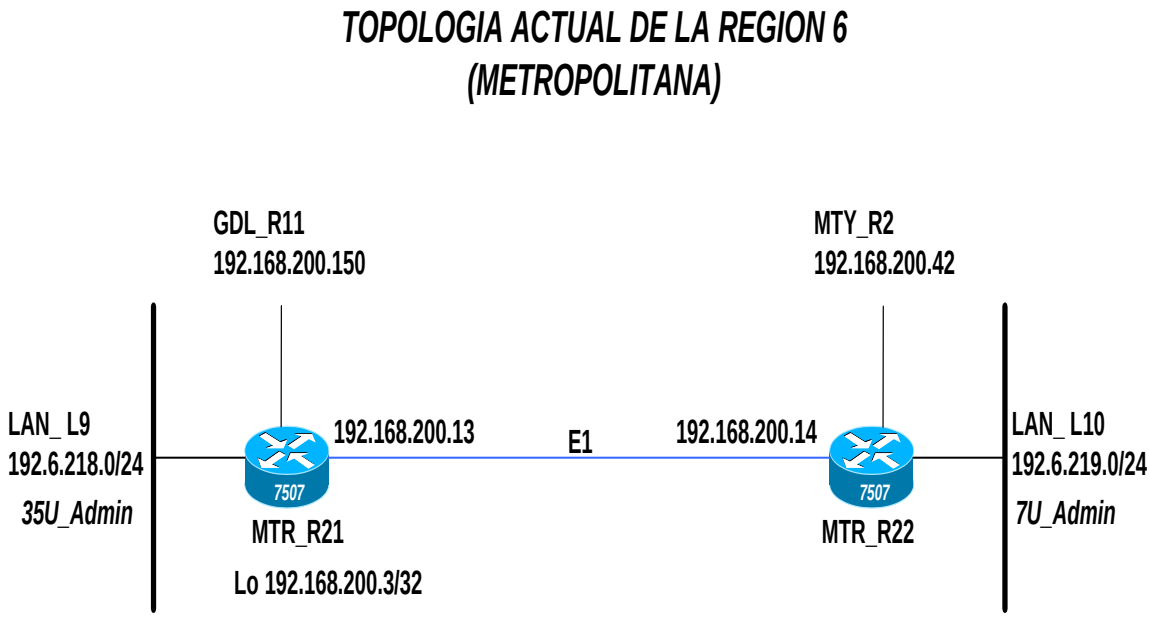


Figura 2.3 Topología de la región 6

Esta región consta de 2 *routers* MTR_R_{21} y MTR_R_{22}, los cuales están unidos por un enlace E1 y cada uno de estos routers tiene un segmento conectado LAN 9 y LAN10 respectivamente, también están conectados a los equipos dorsales MTY_R_2 y GDL_R_{11}.

Características del Backbone

El backbone consta de los equipos mas robustos de cada región (routers 7507), en la región 4 (Monterrey) lo conforman MTY_R_1 y MTY_R_2, en la región 5 (Guadalajara) los routers GDL_R_{11} y GDL_R_{12} y en la región 6 (Metropolitana) el MTR_R_{21} y MTR_R_{22}.

Los routers MTY_R_1 y MTY_R_2 están unidos por un enlace E1, en el router MTY_R_2 se encuentra conectado a su LAN un servidor (*SERV_MTY*), el equipo MTY_R_1 a su ves se encuentra conectado por un enlace E1 al router GDL_R_{12} el cual se encuentra conectado por un enlace El al router GDL_R_{11} el cual tiene conectado a su LAN un servidor (*SERV_GDL*).

El equipo GDL_R_{11} esta conectado por un enlace E1 hacia el router MTR_R_{21} el cual tiene conectado a su LAN un servidor (*SERV_MTR*) este mismo router esta conectado por un enlace E1 al router MTR_R_{22}, el cual a su vez esta conectado por un enlace E1 hacia el router MTY_R_2

En el backbone se esta utilizando un protocolo dinámico el cual es EIGRP (*Enhanced Interior Gateway Routing Protocol)* que es propietario de CISCO, este protocolo solo se esta utilizando para anunciar los segmentos dinámicos y las loopbacks pertenecientes a un equipo de cada región.

Esto se muestra en la figura 2.4

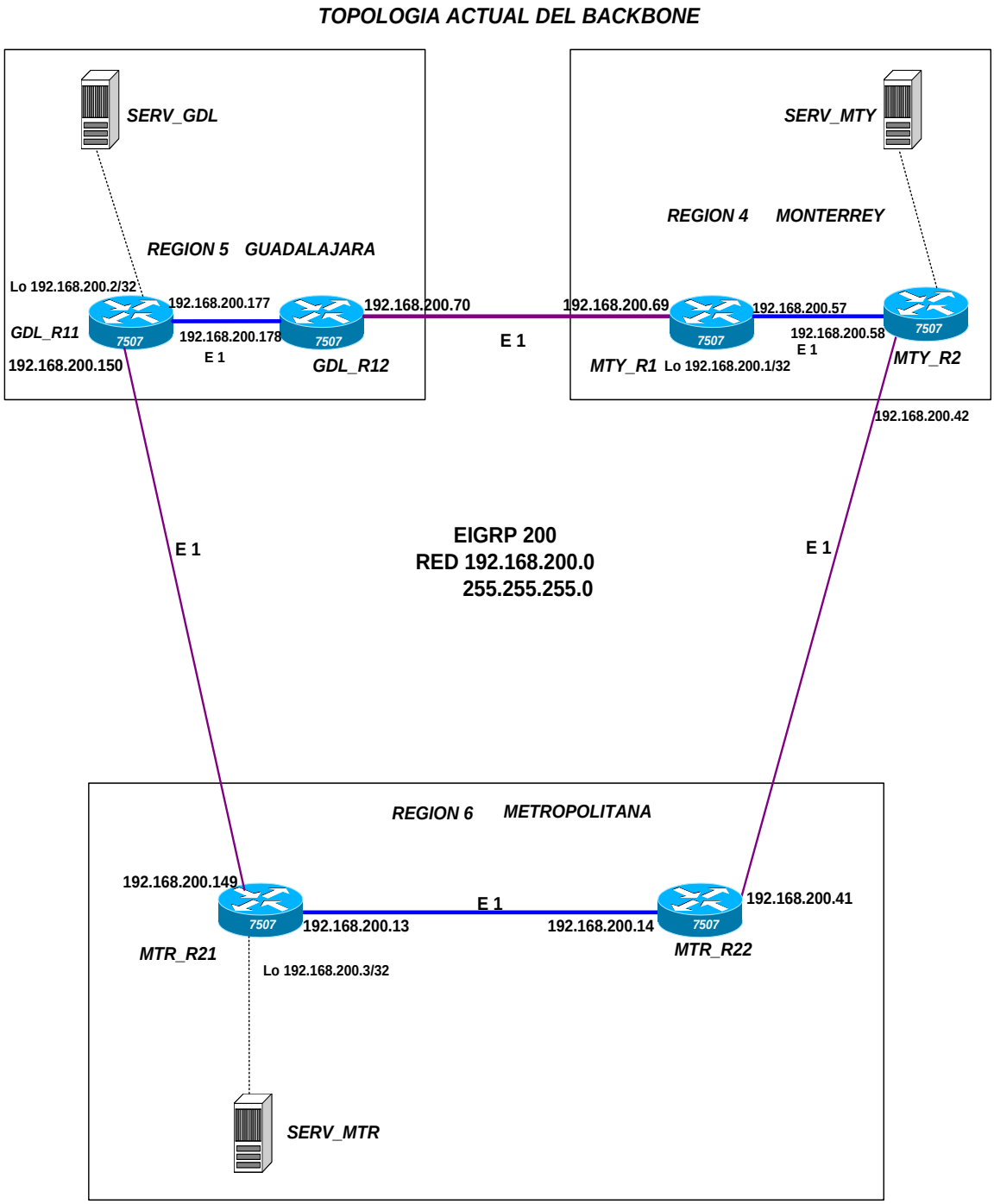


Figura 2.4 Topología del nivel dorsal de la red.

2.2 Problemática de la Red Actual

La red de datos actual tiene la problemática siguiente:

1.- La topología de la red ha crecido por demanda de usuarios.
Esto significa que a la red se le han estado aumentando enlaces sin ningún tipo de política, ejemplo: se puede apreciar en la región 4 que tenemos un enlace de 384 *Kbps.* Por demanda de usuarios, se aumento en paralelo otro enlace E1.

2.-No hay esquema de redundancia en varios puntos de la red.
Si se cae un equipo o enlace se pierde la comunicación con lo que esté conectado ya sea un segmento *LAN* u otro equipo o ambos. Ejemplo, en la región 4 se tienen 2 enlaces hacia un mismo *router* pero sin existir una redundancia, esto quiere decir que en el momento que deje de funcionar el *router* el segmento *LAN* conectado a este quedaría fuera de servicio.
Por razones de costo el esquema de redundancia solo se debe aplicar en sitios críticos.

3.- El ancho de banda no es suficiente pensando en las aplicaciones futuras del usuario.
Se tienen enlaces de poco ancho de banda *(*alrededor de 384 *Kbps).* Esto es muy poco pensando que en aplicaciones futuras como *Internet* o telefonía, en las que el usuario va a demandar un mayor ancho de banda.

4.-Existen conexiones seriales entre nodos.
Si se cae el *router* 1 se cae también el *router* 2 que este en serie, Este tipo de conexiones deben evitarse en una red ya que si cualquiera de los *routers* en serie deja de funcionar, también se quedarán sin servicio los segmentos *LAN* que están conectados a dicho *router.*

5.- No hay un control en la asignación de direccionamiento.
No se tiene una asignación eficiente de direcciones *IP*, ocasionando que no puedan sumarizarse los segmentos.

6.- No existe una administración en las configuraciones de enrutamiento.
Esto se debe a que no se tiene un control tanto de equipo, tarjetas, enlaces y usuarios.

7.-Existen nodos que se vuelven altamente críticos debido a que concentran diferentes funciones. Como no es una red jerárquica, no se tiene un claro control de las funciones que deben de tener cada uno de los equipos, por ejemplo en algunos routers dorsales se tienen conectados segmentos LAN esto es un problema ya que si uno de estos equipos llegase a fallar todos los usuarios conectados a este quedarían sin servicio.

8.- En cada región podemos observar que se están utilizando segmentos de direccionamiento de mascara de 24 para cada una de las LAN's, lo cual significa un gran desaprovechamiento de direcciones ya que se tienen muy pocos usuarios por cada LAN. Además esto dificulta una sumarizaciòn eficiente cuando se quiera aplicar un protocolo de enrutamiento dinámico para cada una de estas regiones.

Capitulo III. Análisis de la propuesta de solución.

La productividad de una compañía depende en gran medida de la eficiencia con que son colectados, procesados y distribuidos los datos. Si una red de datos falla, una compañía entera se puede colapsar por la incapacidad de poder recabar, procesar y distribuir su información.
Para el proceso de tratamiento de la información en la Red propuesta, podemos definir tres diferentes componentes que interactúan entre si.
• Infraestructura de Aplicaciones, que define los servicios de software utilizados.
• Infraestructura de cómputo. Proporciona la capacidad de procesamiento de las aplicaciones servidores, PC´s y terminales.
• Infraestructura de Red. Debe proporcionar la confiabilidad y eficiencia en el transporte de datos entre los usuarios y las aplicaciones.
Las aplicaciones dependen de la capacidad de cómputo y también dependen de la confiabilidad de la estructura de la red de datos. Por lo tanto, mientras los usuarios de las aplicaciones cliente-servidor se sigan expandiendo y encontrándose más dispersos, se tendrá que contar con una estructura con alta eficiencia y disponibilidad de la red.
Para cumplir con dichos requerimientos, la Red propuesta ha sido implementada de tal forma que cumpla con los más altos índices de calidad, empleando un diseño jerárquico que permita escalar a otras tecnologías, simplificar la administración y agilizar la solución de fallas.

3.1 Propuestas de los cambios a la red actual.

Ya que en la red actual no se está manejando un sistema jerárquico, el direccionamiento no está sumarizado. No se está utilizando un protocolo de ruteo en su totalidad y además tenemos redes LAN conectadas a los dorsales. Todo esto provoca que nuestra red sea poco escalable y no tenga una buena administración. Por estas razones se propone un sistema jerárquico de 2 niveles los cuales son Dorsal/Distribución y Acceso, ya que estos niveles tienen funciones específicas como son:
Nivel Dorsal/Distribución: Constituye la parte de la red que se encarga del transporte de datos a alta capacidad. Dada su importancia para la conectividad en la empresa cuenta con componentes redundantes, es altamente confiable y es capaz de adaptarse a cambios rápidamente.
El diseño de la dorsal/distribución debe ser capaz de integrar nuevos enrutadores en el nivel de acceso sin necesidad de incrementar su tamaño y capacidad.
Nivel de Acceso: Concentra, distribuye y enruta la información del usuario a la red. Permite la aplicación de políticas de administración y enrutamiento de tráfico sin comprometer el desempeño global de la red. Es el punto de conexión del usuario o de las aplicaciones a la red.

Se propone integrar nuevos equipos en los cuales se conectarán las diferentes redes locales que antes estaban conectadas a los equipos dorsales/distribución. Se realizarán cambios de plataforma ya que al analizar las características futuras de cada región (región 4, 5 y 6) éstas no cuenta con la capacidad de soportar el crecimiento de usuarios.

En cuanto a los enlaces se realizaron predicciones a 3 años y se encontró que en algunas regiones se tiene que incrementar su ancho de banda para cumplir con la demanda requerida. En cuanto a los usuarios se esta añadiendo un servicio nuevo, que es el de atención telefónica.

En lo que respecta al direccionamiento se define utilizar una red clase B debido a que las diferentes clases C que se están utilizando actualmente en cada una de las LAN`s no es suficiente para el crecimiento de la red, la clase B nos proporcionará una administración mas eficiente ante el crecimiento de usuarios, la demanda de enlaces e incremento de equipos. En cuanto al protocolo de enrutamiento que se está manejando actualmente en el backbone es EIGRP, pero no se está utilizando en su totalidad por lo que al cambiar el direccionamiento esto trae consigo que exista una buena sumarización y se pueda implementar en su totalidad este protocolo. Se va a mantener el protocolo de enrutamiento en esta propuesta ya que se tiene la característica de utilizar solo equipos Cisco, teniendo un impacto menor si se compara con un cambio de protocolo. Sin embargo se tiene entendido que este protocolo es propietario y conlleva restricciones en cuanto a no poder implementar equipos de otros proveedores.

En la red actual los enrutadores dorsales tienen conectados directamente los segmentos LAN lo que trae como consecuencia en estos equipos se afecte su desempeño. A si mismo tiene como consecuencia que si uno de los equipos falla dejaría sin servicio a los usuarios de esta LAN. Este esquema ha sido modificado en la red propuesta ya que en los casos donde se tenía el segmento LAN conectado directamente a los routers dorsales se integró nuevo equipo que servirá como acceso para conectar al segmento LAN y mejorar el funcionamiento de los routers dorsales.

3.2 Cambios necesarios para efectuar la propuesta

A continuación veremos todos los cambios que se necesitan realizar para obtener una red jerárquica, redundante, altamente confiable y escalable a un tiempo estimado de tres años.

3.2.1 Cambio de tarjetas equipos y enlaces.

Como ya se menciono se tienen dos tipos de usuarios:
Usuarios Tipo A (Operadoras) las cuales manejan voz y datos y los usuario Tipo B (Administrativos) los cuales solo manejan datos.

Región 4 (Monterrey)

De acuerdo a la figura 3.1 la LAN_LI que esta conectada al router MTY_R_6, cuenta con 25 usuarios administrativos y 20 operadoras, de los cuales se obtiene un ancho de banda de 990 kbps, para esto se realizaron los siguientes cálculos:

LAN_L1 Codec G.703 = 30 kbps
(20 usuarios-operadoras, 25 usuarios-administrativos)

A

Operadoras/Voz = 20 (30 kbps) = 600 kbps
Concurrencia: Operadoras/voz = 90%
90% = (600 kbps) (0.9) = 540 kpbs

Datos **300 kbps = 20 usuarios = 15 kbps por usuario**

Operadoras/Datos = 20 (15 kbps) = 300 kbps
Concurrencia: Operadoras/datos = 90%
90% = (300 kbps) (0.9) = 270 kbps

B

600 kbps = 25 usuarios = 24 kbps por usuario

Administrativos/Datos = 25 (24 kbps) = 600 kbps
Concurrencia: Administrativos = 30%
30% = (600 kbps) (0.3) = 180 kbps

540 kbps + 270 kbps + 180 kbps = 990 kbps
990 kbps

El 50% de 1984 kbps = 992 kbps
El 45% de 1984 kbps = 892.8 kbps
El 40% de 1984 kbps = 793.6 kbps

Por cuestiones de ruteo, podemos enviar la mitad del tráfico (25%) por una interfaz y el otro 25% por la otra interfaz. En dado caso que alguna de las interfaces dejara de funcionar, quedaría la otra interfaces al 50% de su capacidad y este trafico estaría soportado por el enlace Figura 3.1

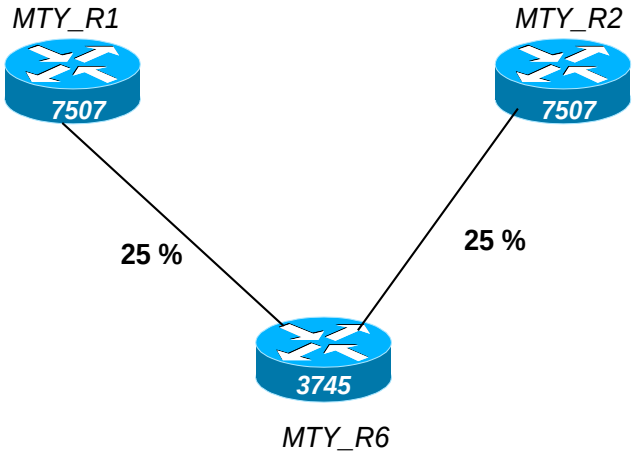


Figura 3.1

Considerando los cálculos para un tiempo estimado de tres años se tendría lo siguiente:
Se hace una estimación considerando que en tres años estos usuarios puedan crecer al doble y todavía tener capacidad los enlaces, para soportar más tráfico. Tomando en cuenta esta consideración se propone lo siguiente:

40 Usuarios – Operadoras
50 Usuarios – Administrativos
La suma de usuarios nos da 90 usuarios

Para dar servicio a esta LAN_L1 se integró un nuevo equipo, el modelo 3745, ya que esta LAN estaba anteriormente conectada a los routers dorsales, ahora se conectó a este router de acceso el cual a su ves esta conectado a los routers dorsal/distribución, a este equipo 3745 se le configuro tres subinterfaces:

VLAN 2 = Operadoras
VLAN 3 = Administrativos
VLAN 4 = Gestión de equipos

Este equipo ira conectado a 1 switch de distribución y 4 switches de acceso, ya que cada switch puede dar servicio a 23 usuarios.

Para la consideración de crecimiento al doble de usuarios en un tiempo estimado de 3 años donde tenemos que hay 40 usuarios operadoras y 50 usuarios administrativos, se obtiene que el ancho de banda de los enlaces será de 1980 kbps, lo cual implica que si un enlace dejara de funcionar, el otro enlace estaría al 100% de su capacidad, al ocurrir esto el enlace no podrá soportar el trafico demandado por lo tanto se tendrá que integrar un nuevo enlace (Figura 3.2).

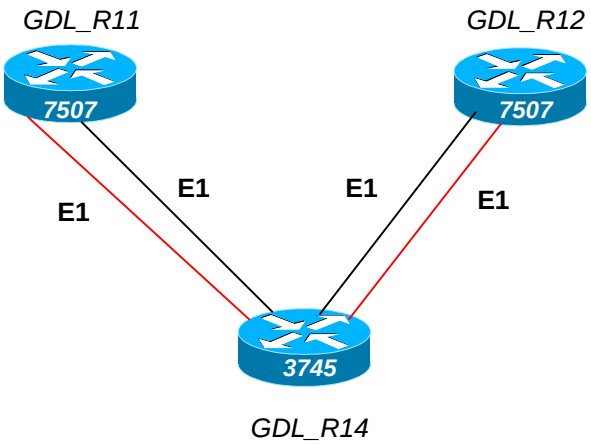


Figura 3.2

Por lo tanto este nuevo equipo requiere de 4 puertos seriales más un puerto Fast Ethernet para los usuarios de la LAN_L1.

Debido a que se van a necesitar 4 enlaces Seriales necesitamos contar con una tarjeta 2FE(TX)-3W y otra tarjeta NM-2CE1T1-PRI, con estas dos tarjetas tendríamos dos fast ethernet y cinco seriales con lo cual se cubre perfectamente los requerimientos a un tiempo de tres años. Por lo tanto el equipo que cumple con las características necesarias es un 3745, el cual tiene 4 slots, DUAL FE, 32F/256D. Como se ve en la figura 3.2 se necesitan 4 enlaces E1 en el nodo de acceso para cumplir con la demanda de usuarios.

En la LAN_L2 que esta conectada al router MTY_ R_3, se tienen 30 operadoras, de los cuales se obtiene un ancho de banda de 1215 kbps, para esto se realizaron los siguientes cálculos:

Lan_L2 (30 usuarios – Operadoras)
Codec G.703 = 30 kbps

A

Operadoras/Voz = 30 (30 kbps) = 900 kbps

Concurrencia: Operadoras/voz = 90%
90% = (900 kbps) (0.9) = 810 kpbs

Datos **300 kbps = 20 usuarios = 15 kbps por usuario**

Operadoras/Datos = 30 (15 kbps) = 450 kbps

Concurrencia: Operadoras/datos = 90%
90% = (450 kbps) (0.9) = 405 kbps

810 kbps + 450 kbps = 1215 kbps; 1215 kbps ≈ E 1

El 50% de 1984 kbps = 992 kbps
El 60% de 1984 kbps = 1190 kbps
El 70% de 1984 kbps = 1388 kbps

Si un enlace dejara de funcionar, el enlace restante estaría al 70% de su capacidad ya que el E1 son 1984 kbps y solo se tienen 1215 kbps, por lo tanto no será necesario otro enlace E1 para esta cantidad de usuarios.

En el caso de la LAN_L2 no tendrá crecimiento de usuarios de operadoras por lo que seguirá siendo el mismo ancho de banda el que se va a utilizar a un tiempo estimado de tres años (Figura 3.3).

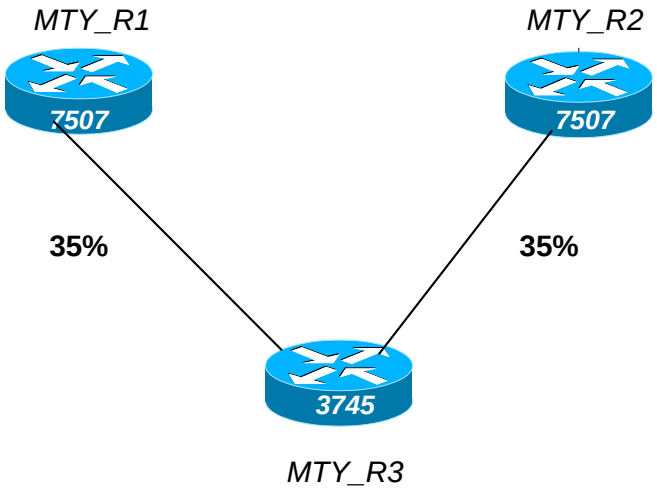


Figura 3.3

Para dar servicio a esta LAN_L2 se ocupo el equipo modelo 3745, al cual se le configuró dos subinterfaces:

VLAN 2 = Operadoras
VLAN 4 = Gestión de equipos

Este equipo se conecto a 2 switches de acceso y un switch de distribución, ya que cada switch puede dar servicio a 23 usuarios. Considerando también una Loopback del equipo MTY_R_3 .

Para este nodo de acceso no habrá crecimiento de operadoras. Por lo tanto con dos enlaces E1 será suficiente para esta cantidad de operadoras.

Debido a que se van a necesitar 2 enlaces Seriales necesitamos tener una tarjeta 2FE(TX)-3W. Con esta tarjeta tendríamos dos fast ethernet y 3 seriales con lo cual se cubre perfectamente los requerimientos a un lapso de tres años. De lo anterior el equipo que cumple con las características necesarias es un enrutador Cisco modelo 3745.

En la LAN_L3 que esta conectada al router MTY_ R_4, se tienen 70 administrativos, de los cuales se obtiene un ancho de banda de 504 kbps, para esto se realizaron los siguientes cálculos:

Lan_ L3 (70 usuarios – Administrativos)

B Administrativos/Datos = 70 (24 kbps) = 1680 kbps
Concurrencia: Administrativos = 30%
30% = (1680 kbps) (0.3) = 504 kbps

600 kbps = 25 usuarios = 24 kbps por usuario

El 10% de 1984 kbps = 198.4 kbps
El 20% de 1984 kbps = 396.8 kbps
El 30% de 1984 kbps = 595.2 kbps
El 40% de 1984 kbps = 793.6 kbps

Si un enlace dejara de funcionar el enlace restante estaría al 30% de su capacidad ya que el E1 son 1984 kbps y solo se tienen 504.5 kbps, por lo tanto con un E1 seria suficiente para esta cantidad de usuarios.

Se hace una estimación considerando que en tres años estos usuarios puedan crecer al doble y todavía tener capacidad los enlaces, para más usuarios. Tomando en cuenta esta consideración se propone lo siguiente:

140 Usuarios – Administrativos

Para dar servicio a esta LAN_L3 se ocupo el equipo Cisco modelo 3745, al cual se le configuro dos subinterfaces:

VLAN 3 = Administrativos
VLAN 4 = Administración de equipos

Este equipo se conecto a 6 switches de acceso y un switch de distribución / acceso, ya que cada switch puede dar servicio a 23 usuarios.
Al igual que en el equipo anterior, ya se calculo previamente el ancho de banda al cual deberán estar los enlaces conectados a este equipo, obteniendo los siguientes resultados.

Para el caso donde solo se tienen 70 usuarios administrativos, si un enlace dejara de funcionar se obtiene que el ancho de banda es de 504.5 kbps, lo cual implica que el enlace E1, estará aproximadamente a un 30% de su capacidad (Figura 3.4).

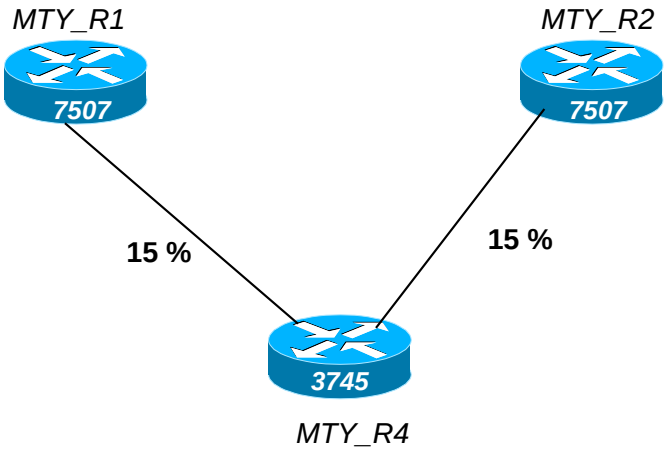


Figura 3.4

Para la consideración de crecimiento al doble de usuarios en un tiempo estimado de 3 años donde tenemos que hay 140 usuarios administrativos, si uno de los enlaces dejara de funcionar se obtiene que el ancho de banda de los enlaces será de 1009 kbps, lo cual implica que el enlace E1, esta al 60% de su capacidad.

Por lo tanto para este equipo se necesitó 2 puertos seriales, más un puerto Fast Ethernet para los usuarios de la LAN_L3.

Debido a que se van a necesitar 2 enlaces Seriales necesitamos tener una tarjeta 2FE(TX)-3W.. Por lo tanto el equipo que cumple con las características necesarias es un 3745, el cual tiene 4 slots, DUAL FE, 32F/256D.

En la LAN_L4 que esta conectada al router MTY_R_5, se tienen 35 operadoras, de los cuales se obtiene un ancho de banda de 1350 kbps, para esto se realizaron los siguientes cálculos:

LAN_L4 (35 usuarios – Operadoras)
Codec G.703 = 30 kbps

A

Operadoras/Voz = 35 (30 kbps) = 1050 kbps
Concurrencia: Operadoras/voz = 90%
90% = (1050 kbps) (0.9) = 945 kpbs

Operadoras/Datos = 30 (15 kbps) = 450 kbps
Concurrencia: Operadoras/datos = 90%
90% = (450 kbps) (0.9) = 405 kbps

945 kbps + 405 kbps = 1350 kbps

El 60% de 1984 kbps = 1190 kbps
El 70% de 1984 kbps = 1388 kbps

Si un enlace dejara de funcionar el enlace restante estaría al 70% de su capacidad ya que el E1 son 1984 kbps y solo se tienen 1350 kbps, por lo tanto no será necesario otro enlace E1 para esta cantidad de usuarios.

Este nodo de acceso no tendrá crecimiento de usuarios de operadoras por lo tanto podemos decir que seguirá siendo el mismo ancho de banda el que se va a utilizar a un tiempo estimado de tres años.

Para dar servicio a esta LAN_L4 se ocupo el equipo modelo 3745, al cual se le configuró dos subinterfaces:

VLAN 2 = Operadoras
VLAN 4 = Administración de equipos

Este equipo se conecto a un switch de acceso y un switch de distribución / acceso, ya que cada switch puede dar servicio a 23 usuarios. Considerando también una Loopback del equipo MTY_R_5.

Para este nodo de acceso no habrá crecimiento de operadoras. Por lo tanto con dos enlaces E1 será suficiente para esta cantidad de operadoras.

Debido a que se van a necesitar 2 enlaces Seriales necesitamos tener una tarjeta 2FE(TX)-3W.. Por lo tanto el equipo que cumple con las características necesarias es un enrutador Cisco modelo3745, el cual tiene 4 slots, DUAL FE, 32F/256D.

Routers MTY_R_1 y MTY_R_2, estos son equipos dorsales modelo 7507, a cada uno irán conectados los equipos MTY_R_3, MTY_R_4, MTY_R_5 Y MTY_R_6, por lo tanto necesitaran 9 enlaces seriales E1 cada uno, haciendo la consideración de que a tres años

estamos creciendo al doble de usuarios en algunos nodos, por lo tanto se necesitaran 18 enlaces seriales.

En esta tabla (Figura 3.5) resume la cantidad de tarjetas y enlaces utilizados para cada router de la Región 4 y así definir la plataforma a utilizar

TIPO DE TARJETAS, EQUIPO Y ENLACES

Equipo por Región	Tarjetas	Plataformas R y SW	Enlaces
Región 4 MTY_R6	2FE(TX)-3W, NM-2CE1T1-PRI	3745 y 3550	4 E1
Región 4 MTY_R3	2FE(TX)-3W	3745	2 E1
Región 4 MTY_R4	2FE(TX)-3W,	3745 y (3)3550	2 E1
Región 4 MTY_R5	N / A	N / A	2 E1

Figura 3.5

Región 5 (Guadalajara)

Para la Región 5 en la LAN_L5 que esta conectada al router GDL_ R_{16}, se tienen 25 usuarios administrativos y 25 operadoras, de los cuales se obtiene un ancho de banda de 1192.5 kbps, para esto se realizaron los siguientes cálculos:

LAN_L5 (25 usuarios- Operadoras; 25 usuarios – Administrativos)
Codec G.703 = 30 kbps

Operadoras/Voz = 25 (30 kbps) = 750 kbps
Concurrencia: Operadoras/voz = 90%
90% = (750 kbps) (0.9) = 675 kpbs

A

Datos 300 kbps = 20 usuarios
15 kbps = por cada usuario

Operadoras/Datos = 25 (15 kbps) = 375 kbps
Concurrencia: Operadoras/datos = 90%
90% = (375 kbps) (0.9) = 337.5 kbps

600 kbps = 25 usuarios
24 kbps = por cada usuario

B

Administrativos/Datos = 25 (24 kbps) = 600 kbps
Concurrencia: Administrativos = 30%
30% = (600 kbps) (0.3) = 180 kbps

675 kbps + 337.5 kbps + 180 kbps = 1192.5 kbps

El 50% de 1984 kbps = 992 kbps
El 60% de 1984 kbps = 1190 kbps
El 70% de 1984 kbps = 1388 kbps

Si un enlace dejara de funcionar el enlace restante estaría al 60% de su capacidad ya que el E1 son 1984 kbps y solo se tienen 1192.5 kbps, por lo tanto no será necesario otro enlace E1 para esta cantidad de usuarios.

Este nodo de acceso no tendrá crecimiento de usuarios por lo tanto podemos decir que seguirá siendo el mismo ancho de banda el que se va a utilizar a un tiempo estimado de tres años.

Para dar servicio a esta LAN_L5 se ocupo el equipo modelo 3745, al cual se le configuró tres subinterfaces:

VLAN 2 = Operadoras
VLAN 3 = Administrativos
VLAN 4 = Gestión de equipos

Este equipo se conecto a 1 switch de distribución /acceso y 2 switches de acceso, ya que cada switch puede dar servicio a 23 usuarios.

Para la LAN_L6 que esta conectada al router GDL_ R_{13} , se tienen 90 usuarios administrativos, de los cuales se obtiene un ancho de banda de 648 kbps, para esto se realizaron los siguientes cálculos:

Lan_L6 (90 usuarios – Administrativos)

600 kbps = 25 usuarios
24 kbps = por cada usuario

B

Administrativos/Datos = 90 (24 kbps) = 2160 kbps
Concurrencia: Administrativos = 30%
30% = (2160 kbps) (0.3) = 648 kbps

El 30% de 1984 kbps = 595.2 kbps
El 40% de 1984 kbps = 793.6 kbps

Si un enlace dejara de funcionar, el enlace restante estaría al 40%, por lo tanto no se requiere de otro enlace.

Se hace una estimación considerando que en tres años estos usuarios puedan crecer al doble y todavía tener capacidad para más usuarios. Tomando en cuenta esta consideración se propone lo siguiente:

180 Usuarios – Administrativos

Para dar servicio a esta LAN_L6 se ocupo el equipo modelo 3745, al cual se le configuró dos subinterfaces:

VLAN 3 = Administrativos
VLAN 4 = Gestión de equipos

Este equipo se conecto a 8 switches de acceso y un switch de distribución , ya que cada switch puede dar servicio a 23 usuarios.

Para la consideración de crecimiento al doble de usuarios en un tiempo estimado de 3 años donde tenemos que hay 180 usuarios administrativos, si un enlace dejara de funcionar el enlace restante tendrá un ancho de banda de los enlaces será de 1587.2 kbps, lo cual implica que el enlace E1, esta al 80% de su capacidad, por lo tanto no se necesitara un nuevo enlace..

Debido a que en este nodo ya se tienen el equipo y la tarjeta no se va a tener que invertir en este nodo de acceso.

Para la LAN_L7 que esta conectada al router GDL_ R_{14} , se tienen 28 usuarios operadoras, de los cuales se obtiene un ancho de banda de 1134 kbps, para esto se realizaron los siguientes cálculos:

Lan_L7 (28 usuarios – Operadoras)
Codec G.703 = 30 kbps

Operadoras/Voz = 28 (30 kbps) = 840 kbps
Concurrencia: Operadoras/voz = 90%
90% = (840 kbps) (0.9) = 756 kpbs

A

Datos 300 kbps = 20 usuarios
15 kbps = por cada usuario

Operadoras/Datos = 28 (15 kbps) = 420 kbps
Concurrencia: Operadoras/datos = 90%
90% = (420 kbps) (0.9) = 378 kbps

756 kbps + 378 kbps = 1134 kbps

El 50% de 1984 kbps = 992 kbps
El 60% de 1984 kbps = 1190 kbps
El 70% de 1984 kbps = 1388 kbps

Si un enlace dejara de funcionar el enlace restante estaría al 60% de su capacidad ya que el E1 son 1984 kbps y solo se tienen 1134 kbps, por lo tanto no será necesario otro enlace E1 para esta cantidad de usuarios, ya que si un enlace deja de funcionar el otro enlace restante si podrá soportar el tráfico demandado.

Este nodo de acceso no tendrá crecimiento de usuarios por lo tanto podemos decir que seguirá siendo el mismo ancho de banda el que se va a utilizar a un tiempo estimado de tres años.

Para dar servicio a esta LAN_L7 se ocupo el equipo modelo 3745, al cual se le configuró dos VLAN:

VLAN 2 = Operadoras
VLAN 4 = Gestión de equipos

A este equipo se le conecto dos switches de acceso y un switch de distribución, ya que cada switch puede dar servicio a 23 usuarios.

Para la LAN_L8 que esta conectada al router GDL_R_{15}, se tienen 95 usuarios administrativos, de los cuales se obtiene un ancho de banda de 684 kbps, para esto se realizaron los siguientes cálculos:

Lan_L8 (95 usuarios – Administrativos)

B

600 kbps = 25 usuarios
24 kbps = por cada usuario

Administrativos/Datos = 95 (24 kbps) = 2280 kbps
Concurrencia: Administrativos = 30%
30% = (2280 kbps) (0.3) = 684 kbps

El 30% de 1984 kbps = 595.2 kbps
El 40% de 1984 kbps = 793.6 kbps

Si un enlace dejara de funcionar, el enlace restante estaría al 40% de su capacidad**,** por lo tanto no se necesita otro enlace.

Se hace una estimación considerando que en tres años estos usuarios puedan crecer al doble y todavía tener capacidad para más usuarios. Tomando en cuenta esta consideración se propone lo siguiente:

190 Usuarios – Administrativos

Para dar servicio a esta LAN_L8 se ocupó el equipo modelo 3745, al cual se le configuró dos subinterfaces:

VLAN 3 = Administrativos
VLAN 4 = Gestión de equipos

Este equipo se conecto a 8 switches de acceso y un switch de distribución / acceso, ya que cada switch puede dar servicio a 23 usuarios.

Para la consideración de crecimiento al doble de usuarios en un tiempo estimado de 3 años donde tenemos que hay 190 usuarios administrativos, si uno de los enlaces dejara de funcionar el enlace restante tendría un ancho de banda de los enlaces será de 1587.2 kbps, lo cual implica que el enlace E1, esta al 80% de su capacidad, por lo tanto no se requiere de otro enlace.

Para los Routers GDL_R_{11} y GDL_R_{12}, estos son equipos dorsales modelo 7507, a cada uno de los dorsales irán conectados los equipos GDL_R_{13}, GDL_R_{14}, GDL_R_{15} Y GDL_R_{16}, se tienen por lo tanto necesitarón 8 enlaces seriales E1 cada uno, haciendo la consideración de que a tres años estamos creciendo al doble de usuarios en algunos nodos, por lo tanto se necesitaran 16 enlaces seriales.

En esta tabla (Figura 3.6) resume la cantidad de tarjetas y enlaces utilizados para cada router de la Región 5 y así definir la plataforma a utilizar

TIPO DE TARJETAS, EQUIPO Y ENLACES

Equipo por Región	Tarjetas	Plataformas	Enlaces
Región 5 GDL_R16	2FE(TX)-3W	3745 y 3550	2 E1
Región 5 GDL_R13	N / A	(7)3550	2 E1
Región 5 GDL_R14	N / A	N / A	2 E1
Región 5 GDL_R15	N / A	(3)3550	2 E1

Figura 3.6

Región 6 (Metropolitana)

Para la Región 6 en la LAN_L9 que esta conectada al router MTR_ R_{23}, se tienen 92 usuarios administrativos, de los cuales se obtiene un ancho de banda de 662.4 kbps, para esto se realizaron los siguientes cálculos:

Lan_L9 (92 usuarios – Administrativos)

B

600 kbps = 25 usuarios
24 kbps = por cada usuario

Administrativos/Datos = 92 (24 kbps) = 2208 kbps
Concurrencia: Administrativos = 30%
30% = (2208 kbps) (0.3) = 662.4 kbps

El 30% de 1984 kbps = 595.2 kbps
El 40% de 1984 kbps = 793.6 kbps

Si un enlace dejara de funcionar el enlace restante estaría al 40% de su capacidad por lo tanto no será necesario otro enlace.

Se hace una estimación considerando que en tres años estos usuarios puedan crecer al doble y todavía tener capacidad para más usuarios. Tomando en cuenta esta consideración se propone lo siguiente:

184 Usuarios – Administrativos

Para dar servicio a esta LAN_L9 se metió un nuevo equipo modelo 3745, ya que anteriormente esta LAN estaba conectada directamente al router MTR_ R_{21} lo cual implicaba que si este router fallaba se dejaría de dar servicio a la LAN, a este nuevo equipo se le configurará dos subinterfaces:

VLAN 3 = Administrativos
VLAN 4 = Gestión de equipos

Este equipo ira conectado a 8 switches de acceso y un switch de distribución, ya que cada switch puede dar servicio a 23 usuarios.

Para la consideración de crecimiento al doble de usuarios en un tiempo estimado de 3 años donde tenemos que hay 184 usuarios administrativos, si un enlace dejara de funcionar, el

enlace restante tendría ancho de banda de 1324 kbps, lo cual implica que el enlace E1, esta al 80% de su capacidad y no se requiere de un enlace adicional.

Para la LAN_L10 que esta conectada al router MTR_R_{24}, se tienen 7 usuarios administrativos y 20 operadoras, de los cuales se obtiene un ancho de banda de 860.4 kbps, para esto se realizaron los siguientes cálculos:

Lan_L10 (20 usuarios- Operadoras; 7 usuarios – administrativos)
Codec G.703 = 30 kbps

A

Operadoras/Voz = 20 (30 kbps) = 600 kbps
Concurrencia: Operadoras/voz = 90%
90% = (600 kbps) (0.9) = 540 kpbs

Datos 300 kbps = 20 usuarios
15 kbps = por cada usuario

Operadoras/Datos = 20 (15 kbps) = 300 kbps
Concurrencia: Operadoras/datos = 90%
90% = (300 kbps) (0.9) = 270 kbps

B

600 kbps = 25 usuarios
24 kbps = por cada usuario

Administrativos/Datos = 7 (24 kbps) = 168 kbps
Concurrencia: Administrativos = 30%
30% = (168 kbps) (0.3) = 50.4 kbps

540 kbps + 270 kbps + 50.4 kbps = 860.4 kbps

El 40% de 1984 kbps = 793.6 kbps
El 50% de 1984 kbps = 992 kbps

Si un enlace dejara de funcionar el enlace restante estaría al 43% de su capacidad por lo tanto no será necesario otro enlace.

Se hace una estimación considerando que en tres años estos usuarios puedan crecer al doble y todavía tener capacidad para más usuarios. Tomando en cuenta esta consideración se propone lo siguiente:

40 Usuarios – Operadoras
14 Usuarios – Administrativos
La suma de usuarios nos da 54 usuarios

Para dar servicio a esta LAN_L10 se meterá un nuevo equipo, el modelo 3745, ya que esta LAN estaba anteriormente directamente conectada a un equipo dorsal, ahora se conecto a un router de acceso, a este equipo se le configurara tres subinterfaces:

VLAN 2 = Operadoras
VLAN 3 = Administrativos
VLAN 4 = Gestión de equipos

Este equipo ira conectado a 1 switch de distribución/acceso y 3 switches de acceso, ya que cada switch puede dar servicio a 23 usuarios.

Para la consideración de crecimiento al doble de usuarios en un tiempo estimado de 3 años donde tenemos que hay 40 usuarios operadoras y 14 usuarios administrativos, se obtiene que el ancho de banda de los enlaces será de 1720.8 kbps, lo cual implica que si un enlace dejara de funcionar el enlace restante estaría al 86% de su capacidad, para lo cual es necesario adicionar otro enlace (Figura 3.7).

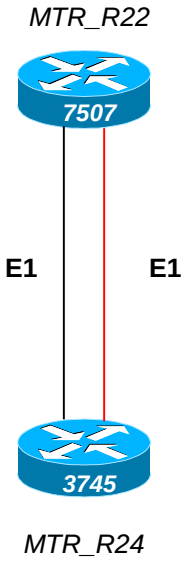


Figura 3.7

En esta tabla (Figura 3.8) resume la cantidad de tarjetas y enlaces utilizados para cada router de la Región 6 y así definir la plataforma a utilizar

TIPO DE TARJETAS, EQUIPO Y ENLACES

Equipo por Región	Tarjetas	Plataforma	Enlaces
Región 6 MTR_R23	2FE(TX)-3W	3745 y (6)3550	1 E1
Región 6 MTR_R24	2FE(TX)-3W	3745 y 3550	2 E1

Figura 3.8

3.2.2 Calculo de direccionamiento

Región 4 (Monterrey)

Para esta región se necesitan 4 segmentos de 254 host válidos, este valor se obtiene de la siguiente tabla Figura 3.9

DIRECCIONAMIENTO

Equipo por Region	Mascara 24	Mascara 25	Mascara 26	Mascara 27	Mascara 28	Total de Segmentos
Region 4 MTY_R6			2		1	
Region 4 MTY_R3			1		1	
Region 4 MTY_R4	1				1	
Region 4 MTY_R5		1			1	
Seriales			1			
Loopbacks					1	
Total	1	1	4		5	4 segmentos de 254 host

Figura 3.9

Región 5 (Guadalajara)

Para esta región se necesitan 4 segmentos de 254 host válidos, este valor se obtiene de la siguiente tabla Figura 3.10

DIRECCIONAMIENTO

Equipo por Region	Mascara 24	Mascara 25	Mascara 26	Mascara 27	Mascara 28	Total de Segmentos
Region 5 GDL_R16			2		1	
Region 5 GDL_R13	1				1	
Region 5 GDL_R14			1		1	
Region 5 GDL_R15	1				1	
Seriales			1			
Loopbacks					1	
Total	2	0	4		4	4 segmentos de 254 host validos

Figura 3.10

Región 6 (Metropolitana)

Para esta región se necesitan 4 segmentos de 254 host válidos, este valor se obtiene de la siguiente tabla Figura 3.11

DIRECCIONAMIENTO

Equipo por Region	Mascara 24	Mascara 25	Mascara 26	Mascara 27	Mascara 28	Total de Segmentos
Region 6 MTR_R23	1				1	
Region 6 MTR_R24	1				1	
Seriales			1			
Loopbacks					1	
Total	2	0	1		3	2 segmentos de 254 host validos

Figura 3.11

Por lo tanto de estas tablas obtenemos, que necesitamos diez subredes de 254 host válidos para un crecimiento de usuarios a 3 años.
En la red actual se tiene una clase c para el direccionamiento, pero dado que esta red tiene crecimientos futuro ya no es posible mantener esa clase, es por esto que se migro de una clase c a una clase b que nos brinda un mayor número de subredes.

Con una clase b, a mascara de 22 (172.16.0.0/22) podemos tener 64 subredes con 1022 hosts válidos y con una mascar de 21 podemos tener 32 subredes con 2046 host válidos, para nuestro caso vamos a tomar segmentos de mascara de 21, ya que necesitamos 10 subredes y esta mascara nos brinda 32 subredes con una mayor cantidad de host.

Para la red propuesta se asigno los bloques de direccionamiento siguientes:

1. Seriales y loopbacks = 172.16.8.0/21
2. Usuarios Región 4 y Región 6 = 172.16.16.0/21
3. Usuarios Región 5 = 172.16.24.0/21
4. Backbone = 172.16.32.0/21

3.2.3 Protocolo de Enrutamiento

Debido a que en esta red propuesta estamos utilizando solamente equipos cisco y considerando que es una red pequeña, vamos a utilizar el protocolo EIGRP ya que tiene características como una rápida convergencia, uso eficiente del ancho de banda, compatibilidad con VLSM y CIDR, detección y recuperación de vecinos y usa RTP como protocolo de capa de transporte para garantizar la entrega de información de enrutamiento, establecen relaciones activamente con los vecinos, todas estas características hacen que este sea el protocolo propuesto para la red.
Este protocolo utiliza un comando llamado varianza, el cual se utiliza para balancear trafico a través de múltiples rutas con diferentes métricas a esto se le llama balanceo de carga de costo diferente.

En cuestión de la redundancia, cuando un enlace deja de funcionar todo el tráfico va a poder fluir por el enlace restante, debido a la nueva topología que se implemento y con esto se garantiza un transporte confiable.

3.2.4 Diagrama de la red propuesta

Después de los cambios anteriormente calculados para cada región, queda una propuesta final de direccionamiento para la red propuesta, la cual satisfacerá nuestra demanda presente y proyección de crecimiento futuro a tres años. Como se muestra en las Figuras 3.12, 3.13, 3.14, y 3.15

TOPOLOGÍA PROPUESTA DE LA REGIÓN 4 (MONTERREY)

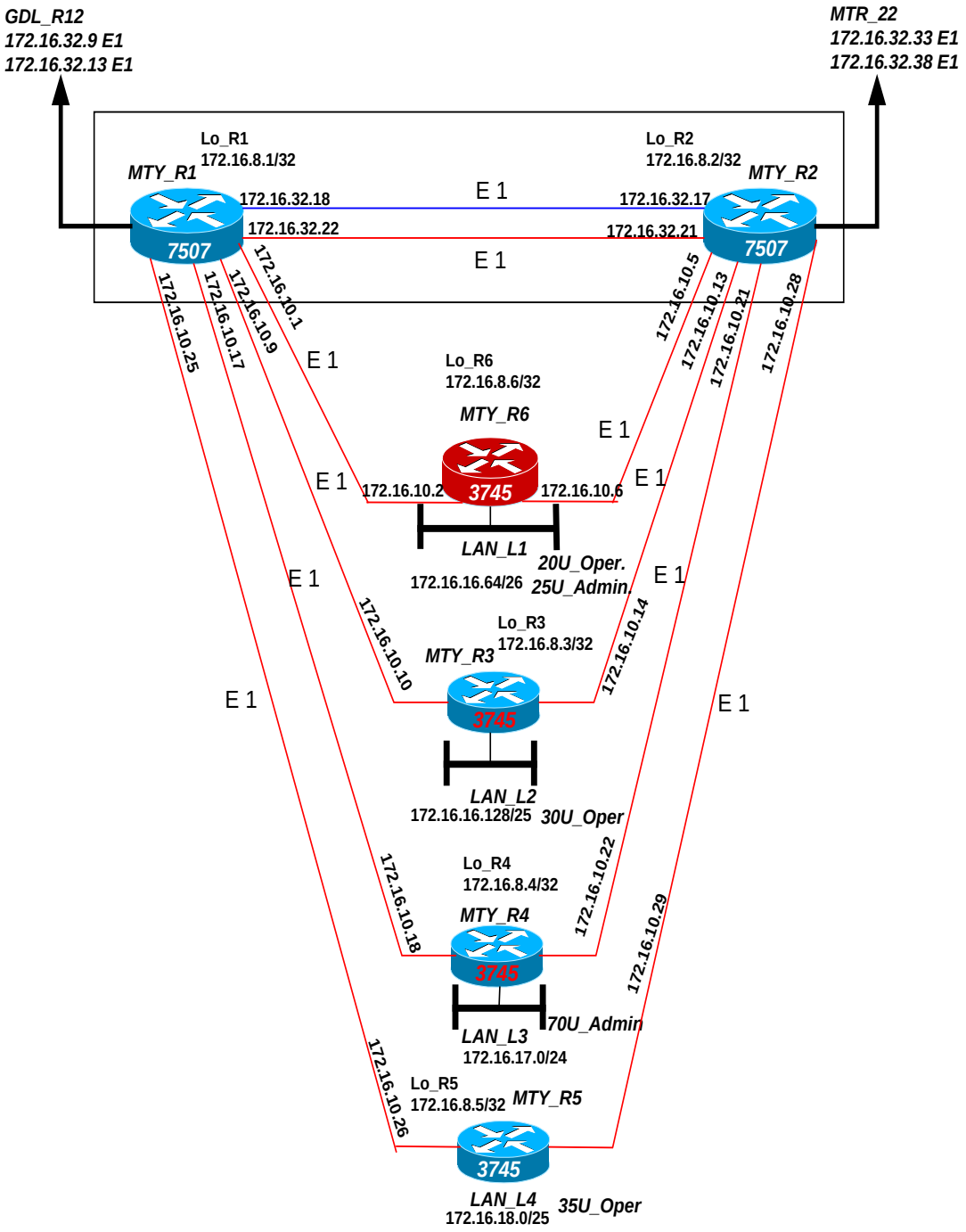


Figura 3.12

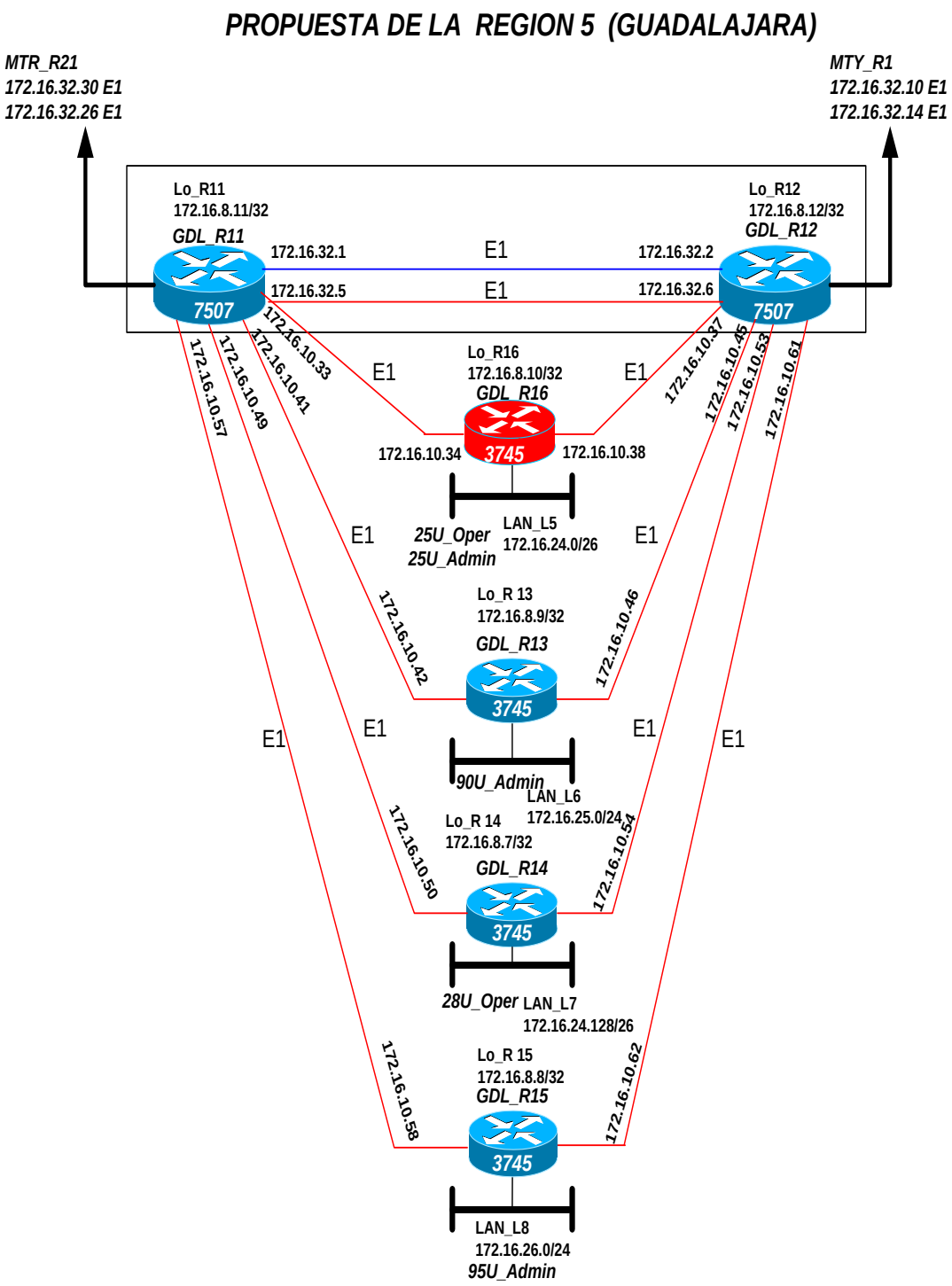

PROPUESTA DE LA REGION 5 (GUADALAJARA)
MTR_R21
172.16.32.30 E1
172.16.32.26 E1
MTY_R1
172.16.32.10 E1
172.16.32.14 E1
Lo_R11
172.16.8.11/32
GDL_R11
Lo_R12
172.16.8.12/32
GDL_R12
172.16.32.1
E1
172.16.32.2
172.16.32.5
E1
172.16.32.6
7507
7507
172.16.10.33
172.16.10.41
172.16.10.49
172.16.10.57
172.16.10.37
172.16.10.45
172.16.10.53
172.16.10.61
E1
Lo_R16
172.16.8.10/32
GDL_R16
E1
172.16.10.34
3745
172.16.10.38
E1
25U_Oper
25U_Admin
LAN_L5
172.16.24.0/26
E1
Lo_R 13
172.16.8.9/32
GDL_R13
172.16.10.42
172.16.10.46
3745
E1
E1
E1
E1
90U_Admin
LAN_L6
172.16.25.0/24
Lo_R 14
172.16.8.7/32
GDL_R14
172.16.10.50
172.16.10.54
3745
28U_Oper
LAN_L7
172.16.24.128/26
Lo_R 15
172.16.8.8/32
GDL_R15
172.16.10.58
172.16.10.62
3745
LAN_L8
172.16.26.0/24
95U_Admin

Figura 3.13

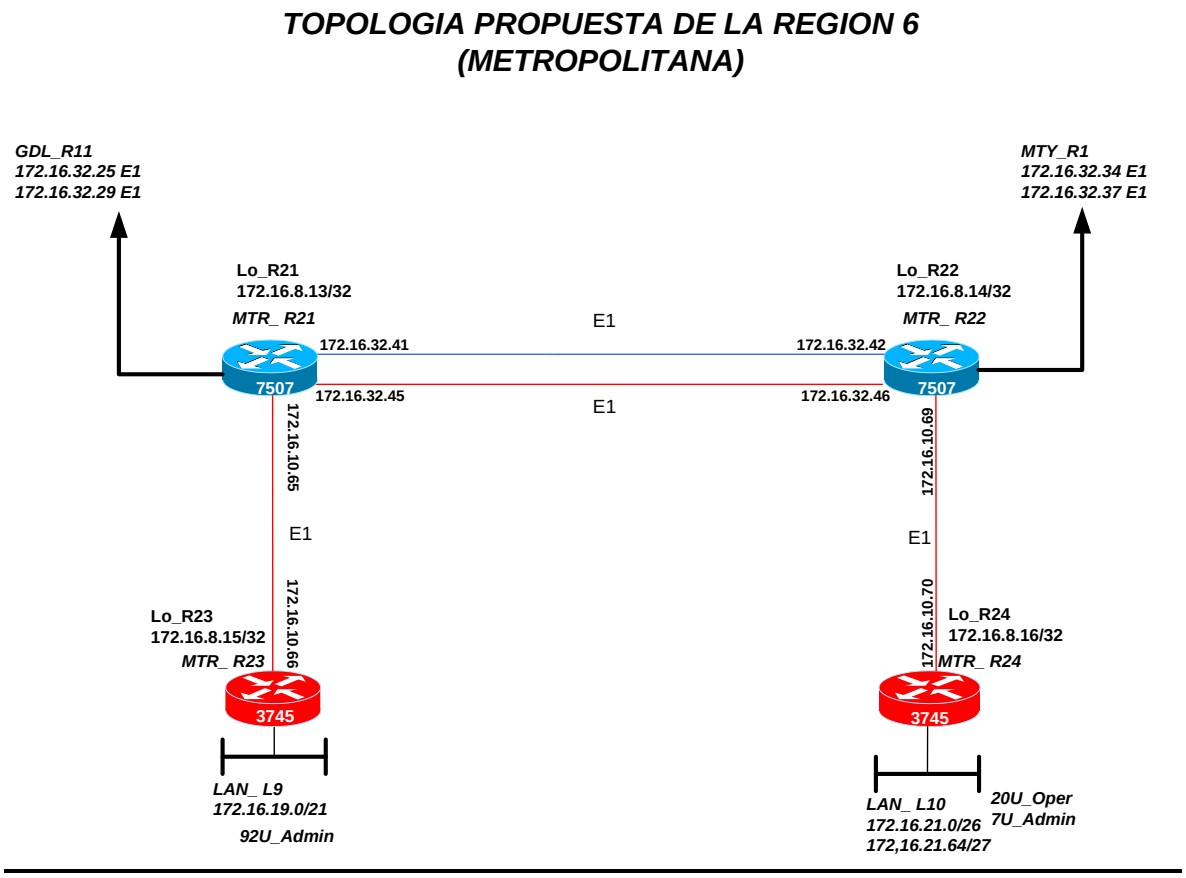

TOPOLOGIA PROPUESTA DE LA REGION 6
(METROPOLITANA)
GDL_R11
172.16.32.25 E1
172.16.32.29 E1
MTY_R1
172.16.32.34 E1
172.16.32.37 E1
Lo_R21
172.16.8.13/32
MTR_ R21
Lo_R22
172.16.8.14/32
MTR_ R22
E1
172.16.32.41
172.16.32.42
7507
7507
172.16.32.45
172.16.32.46
E1
172.16.10.65
172.16.10.69
E1
E1
172.16.10.66
172.16.10.70
Lo_R23
172.16.8.15/32
MTR_ R23
Lo_R24
172.16.8.16/32
MTR_ R24
3745
3745
LAN_ L9
172.16.19.0/21
92U_Admin
LAN_ L10
172.16.21.0/26
172,16.21.64/27
20U_Oper
7U_Admin

Figura 3.14

TOPOLOGIA PROPUESTA DEL BACKBONE

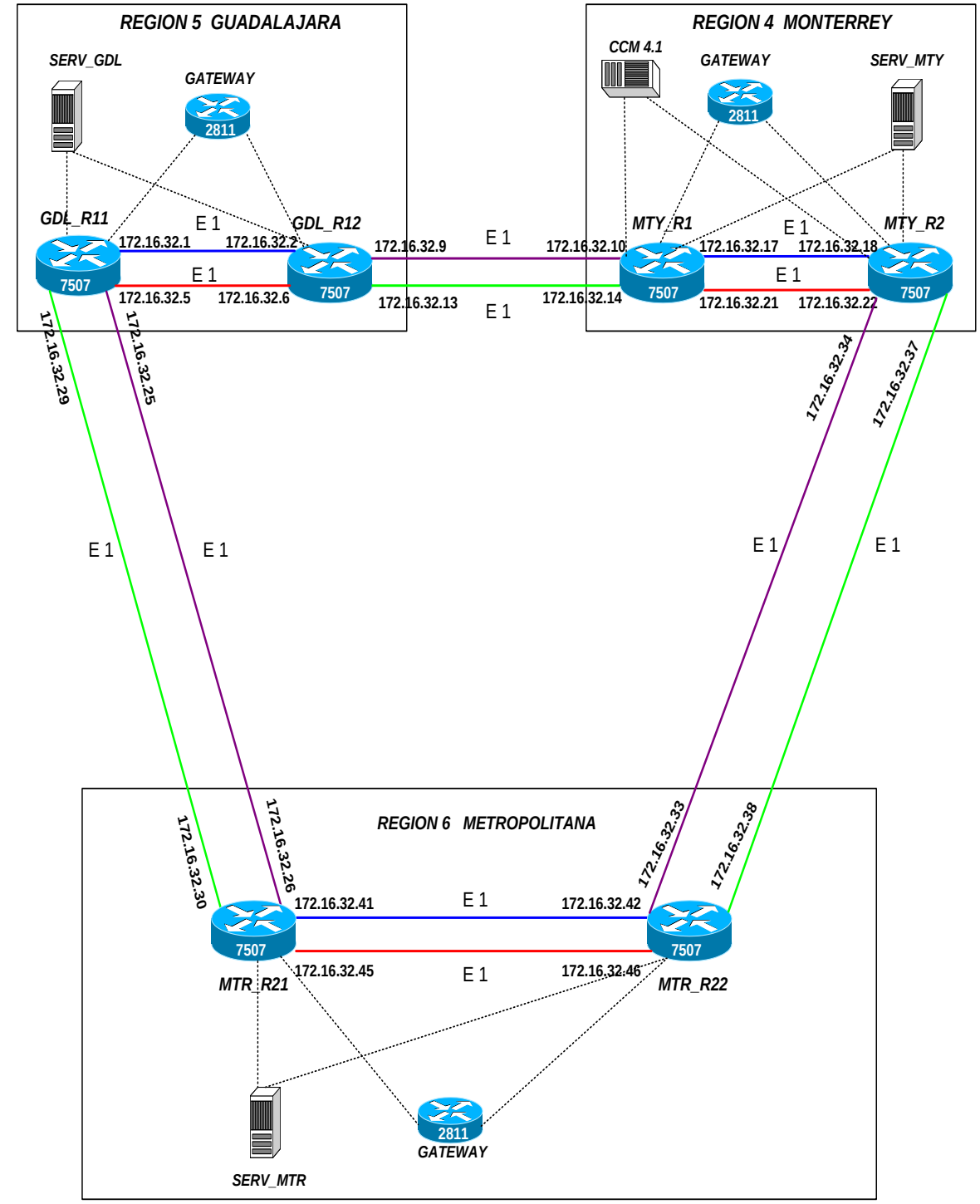


Figura 3.15

3.3 Análisis de costo beneficio

Para poder analizar de una mejor manera el Costo-Beneficio que vamos a obtener al plantear una reingeniería de la red, tenemos que tomar en cuenta algunos factores importantes como lo es, el costo que tiene los equipos nuevos que se agregaran a la nueva topología de la red, así como también el costo de la renta de enlaces nuevos, el tiempo que se va a requerir para la instalación de nuevos equipos y enlaces. Todo esto tiene que comparar contra las ventajas que vamos a obtener al realizar este cambio y la recuperación de la nueva inversión, lo cual implica no solo un tiempo invertido sino también un capital invertido el cual se espera recuperar a corto plazo, el tomar estos factores en cuenta nos va a llevar a saber si el proyecto es viable y rentable a corto plazo.

Los beneficios que obtendremos en la reingeniería de la red de datos la cual implica realizar ciertos cambios tanto en equipo como en enlaces, son diversos, entre estos están dar servicio tanto a usuario administrativos que manejan datos, así como también a operadoras que manejan voz y datos, lo cual amplia la cantidad y el tipo de clientes a los que se les dará servicio, también obtendremos una mayor escalabilidad ya que aunque los usuarios puedan crecer al doble la red siga siendo eficiente y rentable.

En el siguientes subtema veremos con más detalle lo que se tendrá que invertir en la realización de estos cambios y así podremos saber si nuestra propuesta de cambio a esta red de datos es en verdad una opción desde el punto de vista económico.

3.3.1 Costo de equipos y tarjetas

Equipos de la Región 4, 5 y 6

En las tres regiones que estamos manejando Monterrey, Guadalajara y Metropolitana se están utilizando dos clases de plataformas de routers los 7507 (backbone) y los 3745 (nodos de acceso) y switches 3550 de los cuales veremos las características de dichos equipos y su costo dependiendo de las tarjetas que se utilizaran para cubrir la demanda de usuarios.

-Modelo 3745.

- Las características de este equipo son 4 slots, dual fast ethernet, 32F /256D.

El chasis del equipo tiene un costo de 120,000 pesos.

Las tarjetas que puede llevar este equipo son las siguientes:
2FE(TX) – 3W: El costo de esta rajeta es de 30,200 pesos.
NM-2CE1T1-PRI: El costo de esta tarjeta es de 30,000 pesos.

-Modelo 7507

- Las características de este equipo son 7 slots, 2CYBUS, 2RSP4, Dual Power Supply
- RSP4 – 64 M memory
- Flash – 64 M

El chasis del equipo tiene un costo de 340,900 pesos.

Las tarjetas que puede llevar este equipo son las siguientes:
VIP 6-80: El costo de esta tarjeta es de 150,000 pesos.
PA-2FE-TX: El costo de esta tarjeta es de 30,800 pesos.
8 port TI/E1: El costo de esta tarjeta es de 110,600 pesos.

Switch Catalyst 3550 DC SMI
Las características de este equipo son:
- 24 10/100 ports and 2 GBIC-based puertos Gigabit Ethernet
- DC powered
- Installed Standard Multilayer Software Image (SMI), Enhanced Standard Multilayer Software Image (EMI)

El costo del equipo es: $40,495.00

Gateway 2811 DC SMI
Las características de este equipo son:
- 24811W
- AC PWR
- 2 FE, 4 HWICs
- 2 PVDMs(Packet Voice DSP Module)
- IP BASE, 64F/256D

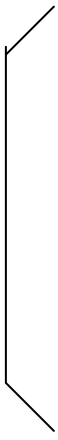
El costo del equipo es: $20,495.00

Call Manager
- CCM 4.1

El costo del equipo es: $70,000.00
Licencia para 10 usuarios es: $5,000.00

Costo de equipos y tarjetas de la Región 4

LAN_L1

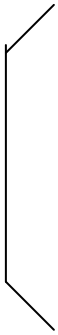


1 switch (3550) = $40,495.00

1 router (3745)=$120,000.00
1 tarjeta 2FE(TX)-3W=$30,200.00
1 tarjeta NM-2CE1T1-PRI=$30,000.00

$40,495.00 + $120,000.00+30,200+30,000 = $220,695.00

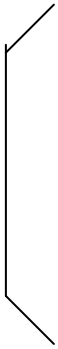
LAN_L2



1 switch (3745) = $120,000.00
1 tarjeta 2FE(TX)-3W=$30,200.00

$120,000.00 +30,200 = $150,200.00

LAN_L3



3 switch (3550) = 3x$40,495.00
1 router (3745)=$120,000.00
1 tarjeta 2FE(TX)-3W=$30,200.00

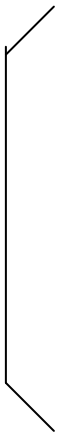
$121,485.00 + $120,000.00+30,200= $271,685.00

1 Gateway=$24,950.00
22 Cables DB15-BNC=22x$350.00 =$7,700.00
1 Call Manager=$70,000.00
Licencia de 10 usuarios= $5,000.00=(180/10)x$5,000

TOTAL: $220,695.00 + $150,200.00+$271,685+24,950+7,700+70,000+90,000= $835,230.00

Costo de equipos y tarjetas de la Región 5

LAN_L5

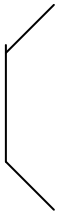


1 switch (3550) = $40,495.00

1 router (3745)=$120,000.00
1 tarjeta 2FE(TX)-3W=$30,200.00

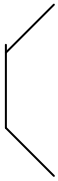
$40,495.00 + $120,000.00+30,200= $190,695.00

LAN_L6



7 switch (3550) = 7x$40,495.00=$283,465.00

LAN_L8



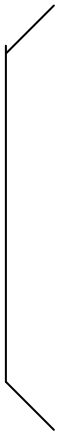
3 switch (3550) = 3x$40,495.00=$121,485.00

1 Gateway=$24,950.00
18 Cables DB15-BNC=$6,300.00

TOTAL: $190,695.00 + $283,465.00+121,485+24,950+6,300= $626,895.00

Costo de equipos y tarjetas de la Región 6

LAN_L9

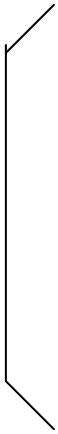


6 switch (3550) = 6x$40,495.00=$242,970

1 router (3745)=$120,000.00
1 tarjeta 2FE(TX)-3W=$30,200.00

$242,970.00 + $120,000.00+30,200= $393,170.00

LAN_L10



1 switch (3550) = $40,495.00

1 router (3745)=$120,000.00
1 tarjeta 2FE(TX)-3W=$30,200.00

$242,970.00 + $120,000.00+30,200= $190,695.00

1 Gateway=$24,950.00
6 Cables DB15-BNC=$2,100.00

TOTAL: $393,170.00 + $190,695.00+2,100+24,950= $610,915.00

En esta tabla (Figura 3.16) se hace un resumen del costo de cada equipo y tarjeta y cables de la Región 4.

COSTOS

Equipo por Región	Costo de equipo y tarjetas	Costo Total en pesos
Región 4 MTY_R6	40,495 + 120,000 + 30,200 +30,000	$220,695
Región 4 MTY_R3	120,000 + 30,200	$150,200
Región 4 MTY_R4	121,485 + 120,000 + 30,200	$271,685
Región 4 MTY_R5	N / A	N / A
Gateway 22Cables Call M Licencia	24,950+7,700+70,000+90,000	$192,650
TOTAL	N / A	$835,230

Figura 3.16

En esta tabla (Figura 3.17) se hace un resumen del costo de cada equipo y tarjeta y cables de la Región 5.

COSTOS

Equipo por Region	Costo de equipo y tarjetas	Costo Total en pesos
Región 5 GDL_R16	40,495 + 120,000 + 30,200	$190,695
Región 5 GDL_R13	283,465	$283,465
Región 5 GDL_R14	N / A	N / A
Región 5 GDL_R15	121,485	$121,485
Gateway 18Cables	24,950+6,300	$31,250
TOTAL	N / A	$626,895

Figura 3.17

En esta tabla (Figura 3.18) se hace un resumen del costo de cada equipo y tarjeta y cables de la Región 6.

COSTOS

Equipo por Región	Costo de equipo y tarjetas	Costo Total en pesos
Región 6 MTR_R23	242,970 + 120,000 + 30,200	$393,170
Región 6 MTR_R24	40,495 + 120,000 + 30,200	$190,695
Gateway 6 Cables	24,950 + 2,100	$27,050
TOTAL	N / A	$610,915

Figura 3.18

3.3.2 Renta de Enlaces

Este es otro factor importante que interviene en el análisis del costo-beneficio que se obtendrá al realizar los cambios a la topología de la red.
Para poder verlo más a detalle obtendremos los costos de los enlaces que intervienen en este proyecto, los cuales veremos a continuación.

Enlaces en la Región 4

Para obtener el costo de la renta de un enlace E1 el cual tiene una velocidad de transmisión de datos de aproximadamente 2 Mbps, debemos considerar la siguiente premisa:

E1 = Gasto de instalación mas una renta mensual por tramo.
Un E1 para llegar de un router origen a un router destino debe pasar por una central de la empresa que renta el enlace para esto se considera que el enlace tendrá dos tramos, el tramo que va del router origen hacia la central mas el tramo que va de la central al router destino.

El esquema tarifario de la empresa que renta el enlace y en el cual nos vamos a basar para sacar los costos de los enlaces es el siguiente (Figura 3.19):

LADA ENLACE DE 2 MBPS.

TARIFAS EN PESOS PARA LADA ENLACE DE 2 MBPS.

	RANGO KM	GASTO DE INSTALACIÓN Por Tramo	RENTA MENSUAL Por Tramo	
			Fijo	Cargo/km
LOCAL	N.A.	$ 90,971	$ 5,321	N.A.
LARGA DISTANCIA NACIONAL	0-81	$ 12,293	$ 9,916	$ 226
	>81-161		$ 20,830	$ 168
	>161-805		$ 39,153	$ 64
	>805		$ 55,228	$ 46
LARGA DISTANCIA INTERNACIONAL	0-81	$ 18,440	$ 16,224	$ 226
	>81-161		$ 27,581	$ 168
	>161-805		$ 46,638	$ 64
	>805		$ 63,356	$ 46
FRONTERIZO	N.A.	$ 90,971	$ 10,289	N.A.

Figura 3.19

PREMISAS DE APLICACIÓN PARA LADA ENLACE DE 2 MBPS.

a) En la contratación de servicios locales se deberá cubrir tanto los gastos de instalación como la renta mensual de dos tramos locales.

Solamente aplicará el cobro de una parte local en la conexión a otros servicios (redes publicas de datos, redes privadas virtuales, etc.) cuando existan servicios de LADA ENLACES con capacidad disponible para ese fin en la otra parte local.

b) En la contratación de servicios nacionales se deberá cubrir tanto los gastos de instalación como la renta mensual de dos tramos locales, más el tramo de larga distancia nacional.

   Solamente aplicará el cobro de una parte local mas el tramo de larga distancia en la conexión a otros servicios (redes públicas de datos, redes privadas virtuales, etc.) cuando existan servicios de LADA ENLACES con capacidad disponible para ese fin en la otra parte local.

c) En la contratación de servicios internacionales se deberá cubrir tanto los gastos de instalación como la renta mensual de un tramo local, más el tramo de larga distancia internacional.

Estos cargos incluyen únicamente la parte México del enlace.

d) En la contratación de servicios fronterizos se deberá cubrir tanto los gastos de instalación como la renta mensual de un tramo fronterizo.

Estos cargos incluyen únicamente la parte México del enlace.

Calculo para obtener el costo de un enlace local:

Por ser un enlace local el costo de la renta mensual del enlace seria de:
$ 90,971 de gasto de instalación, mas $5,321 de renta por tramos.
El costo total de renta mensual seria de $90,971 + $10,642 = $101,613.00
Considerando la renta por todo un año el costo seria de:
$10,642 * 12 + $90,971 = $218,675

Para un enlace larga distancia nacional el costo de la renta mensual del enlace seria de:

Considerando un enlace de una distancia de 810 Km. aproximadamente como el que habría entre la ciudad de Monterrey y la Ciudad de México
$90,971 + $12,293 de gasto de instalación, mas $5,321(2) de dos tramos locales, mas $55,228 de renta mensual, mas $46 por Km.

Gasto de instalación $90,971 + $12,293 = $103,264.00
2 tramos locales: $5,321(2) = $10,642
Tramo de larga distancia nacional: $55,228 + $46 (810 Km.) = $92,488.00

El costo total de renta mensual seria de $103,264 + $92,488 + $10,642 = $206,394
Considerando la renta por todo un año el costo seria de:

($92,488 + $10,642) * 12 + $103,264 = $1,340,824.00
Para el enlace de Monterrey a la Ciudad de México el costo por un año seria de:
($92,488 + $10,642) * 12 = 1, 237,560.00

Considerando un enlace de una distancia de 862 Km. aproximadamente como el que habría entre la ciudad de Guadalajara a Monterrey.
$90,971 + $12,293 de gasto de instalación, mas $5,321(2) de dos tramos locales, mas $55,228 de renta mensual, mas $46 por Km.

Gasto de instalación $90,971 + $12,293 = $103,264.00
2 tramos locales: $5,321(2) = $10,642
Tramo de larga distancia nacional: $55,228 + $46 (862 Km.) = $94,880.00

El costo total de renta mensual seria de $103,264 + $94,880 + $10,642 = $208,786.00
Considerando la renta por todo un año el costo seria de:
($94,880 + $10,642) * 12 + $103,264 = $1,369,528.00

Para el enlace de Guadalajara a Monterrey el costo por un año seria de:
($92,488 + $10,642) * 12 = $1, 266,264.00

Considerando un enlace de una distancia de 552 Km. aproximadamente como el que habría entre la ciudad de Guadalajara a la Ciudad de México.
$90,971 + $12,293 de gasto de instalación, mas $5,321(2) de dos tramos locales, mas $55,228 de renta mensual, mas $64 por Km.

Gasto de instalación $90,971 + $12,293 = $103,264.00
2 tramos locales: $5,321(2) = $10,642
Tramo de larga distancia nacional: $55,228 + $64 (552 Km.) = $90,556.00

El costo total de renta mensual seria de $103,264 + $90,556 + $10,642 = $204,462.00
Considerando la renta por todo un año el costo seria de:
($90,556 + $10,642) * 12 + $103,264 = $1,317,640.00

Para el enlace de Guadalajara a Monterrey el costo por un año seria de:
($90,556 + $10,642) * 12 = $1, 214,376.00.

Lo anterior se resume en la siguiente tabla (Figura 3.20)

COSTOS

Tramo	Costo de enlaces a un año
MTY – MTR (Considerando el costo de instalación)	$1,340,824.00
MTY – MTR (Sin Considerar el costo de instalación)	$1, 237,560.00
GDL – MTY (Considerando el costo de instalación)	$1,369,528.00
GDL – MTY (Sin Considerar el costo de instalación)	$1, 266,264.00
GDL – MTR (Considerando el costo de instalación)	$1,317,640.00
GDL – MTR (Sin Considerar el costo de instalación)	$1, 214,376.00

Figura 3.20

Capitulo 4. Proceso de Implementación.

En este capitulo veremos la manera en la que se realiza el proceso de implementación de los equipos, enlaces y direccionamiento para la red propuesta, esto nos lleva a tomar en cuenta el tiempo y algunos factores que se consideraran para llevar a cabo el cambio de equipos, instalación de nuevos equipos, instalación de enlaces y migración de red.
A continuación se verán cada uno de estos aspectos para las 3 regiones o nodos que forman la red propuesta.

4.1 Instalación y cambio de Equipos.

Región 4 (Monterrey)

En la Región 4 se va a instalar un nuevo equipo para los usuarios de la LAN_ L1, el cual es un router modelo 3745 (MTY_ R_6), el tiempo que se tarda desde la solicitud de este equipo hasta la configuración del mismo es aproximadamente una semana y para los 5 switches 3550 (distribución y 2 acceso) el tiempo es de cinco semanas.
En esta Región 4 se realizaran dos cambios de equipo los cuales corresponden a los routers modelo 2514 (MTY_ R_3 y MTY_ R_4) los cuales dan servicio a los usuarios de la LAN_L2 y la LAN_L3 respectivamente, estos serán sustituidos por dos routers modelo 3745 respectivamente, para esto se llevara un tiempo aproximado de una semana por cada equipo. Para la LAN_L2 se van a necesitar 3 switches (distribución y 2 acceso) el tiempo que se empleara desde la configuración hasta la instalación es de tres semanas. Para la LAN_L3 se va a necesitar un switch de distribución/acceso y seis switches de acceso, el tiempo que se empleara desde la configuración hasta la instalación es de siete semanas. Para la LAN_L4 se van a necesitar un equipo 3745 el tiempo de instalación de este equipo es de una semana y 2 switches (distribución/acceso y uno de acceso) el tiempo que se empleara desde la configuración hasta la instalación es de dos semanas.
En cuanto a los routers MTY_ R_1, MTY_ R_2 seguirán funcionando normalmente ya que estos equipos no se sustituirán. El tiempo puede variar dependiendo de los contratiempos que en algún determinado momento pueden ocurrir haciendo que este tiempo se prolongue un poco mas, algunos de estos contratiempos serian el mal funcionamiento de los equipos debido a el mal funcionamiento de la fuente de poder o de alguna de las tarjetas que integran el equipo. Se instalará un Call Manager 4.1 y un Gateway 2811 para dar servicio a las operadoras. Lo anterior se muestra en la Figura 4.1.

INTALACIÓN DE EQUIPOS E INTERVENCIÓN R4

CAN	Articulo	Descripción	Nombre del equipo_LAN	Region	Proyecto	Fecha de Solicitud de instalacionde	Fecha Programada
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	MTY_R6_LAN-L1	4	OPER , ADMIN	30-Mar-09	3-Abr-09
5	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	MTY_R6_LAN-L1	4	OPER , ADMIN	6-Abr-09	8-May-09
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	MTY_R3_LAN-L2	4	ADMIN	11-May-09	15-May-09
3	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	MTY_R3_LAN-L2	4	ADMIN	18-May-09	5-Jun-09
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	MTY_R4_LAN-L3	4	ADMIN	8-Jun-09	12-Jun-09
7	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	MTY_R4_LAN-L3	4	ADMIN	18-May-09	5-Jun-09
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	MTY_R5_LAN-L4	4	OPER	8-Jun-09	12-Jun-09
7	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	MTY_R5_LAN-L4	4	OPER	15-Jun-09	26-Jun-09
1	Gateway 2811 DC	4-slot, Dual FE, Mul service Rauter 32F/ 256D	MTY_R1_R2	4	OPER	29-Jun-09	3-Jul-09
1	Call Manager	CCM 4.1	MTY_R1_R2	4	OPER	6-Jul-09	10-Jul-09

Tabla Región 4 (Figura 4.1)

Región 5 (Guadalajara)

En la Región 5 se va a instalar un nuevo equipo para los usuarios de la LAN_ L5, el cual es un router modelo 3745 (GDL_ R_{16}), el tiempo que se tarda desde la solicitud de este equipo hasta la configuración del mismo es aproximadamente una semana y para los 3 switches 3550 (distribución y 2 acceso) el tiempo es de tres semanas.
Para la LAN_L6, se va a reubicar el equipo (3745) en el edificio donde se encuentran los equipos dorsales de esta región, el tiempo estimado es de una semana. Para conectar a los usuarios de esta LAN se van a necesitar 8 switches (distribución y 7 acceso) el tiempo que se empleara desde la configuración hasta la instalación es de nueve semanas. Para la LAN_L7 se va a reubicar el equipo (3745) en el edificio donde se encuentran los equipos dorsales de esta región, el tiempo estimado es de una semana. Para conectar a los usuarios de esta LAN, se va a necesitar un switch de distribución y dos switches de acceso, el tiempo que se empleara desde la configuración hasta la instalación es de tres semanas. Para la LAN_L8 se va a reubicar el equipo (3745) en el edificio donde se encuentran los equipos dorsales de esta región, el tiempo estimado es de una semana. Para conectar a los usuarios de esta LAN, se van a necesitar 9 switches (distribución/acceso y ocho acceso) el tiempo que se empleara desde la configuración hasta la instalación es de nueve semanas.
En cuanto a los routers GDL_ R_{11}, GDL_ R_{12} seguirán funcionando normalmente ya que estos equipos no se sustituirán. El tiempo puede variar dependiendo de los contratiempos que en algún determinado momento pueden ocurrir. Se instalará un Gateway 2811 para dar servicio a las operadoras. Lo anterior se muestra en la Figura 4.2.

INTALACIÓN DE EQUIPOS E INTERVENCIÓN R5

CAN	Articulo	Descripción	Nombre del equipo_LAN	Region	Proyecto	Fecha de Solicitud de instalacionde	Fecha Programada
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	GDL_R16_LAN-L5	5	OPER , ADMIN	13-Jul-09	17-Jul-09
5	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	GDL_R16_LAN-L5	5	OPER , ADMIN	20-Jul-09	7-Ago-09
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	GDL_R13_LAN-L6	5	ADMIN	10-Ago-09	14-Ago-09
9	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	GDL_R13_LAN-L6	5	ADMIN	17-Ago-09	2-Oct-09
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	GDL_R14_LAN-L7	5	OPER	5-Oct-09	9-Oct-09
3	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	GDL_R14_LAN-L7	5	OPER	12-Oct-09	30-Oct-09
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	GDL_R15_LAN-L8	5	ADMIN	2-Nov-09	6-Nov-09
9	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	GDL_R15_LAN-L8	5	ADMIN	9-Nov-09	8-Ene-10
1	Gateway 2811 DC	4-slot, Dual FE, Mul service Rauter 32F/ 256D	GDL_R11_R12	5	OPER	11-Ene-10	15-Ene-10

Tabla Región 5 (Figura 4.2)

Región 6 (Metropolitana)

En la Región 6 se va a instalar un nuevo equipo para los usuarios de la LAN_ L9, el cual es un router modelo 3745 (MTY_R_{23}), el tiempo que se tarda desde la solicitud de este equipo hasta la configuración del mismo es aproximadamente una semana para dar servicio a los usuarios de esta LAN se necesitan 9 switches 3550 (distribución y 8 acceso) el tiempo de instalación y configuración de estos equipos es de nueve semanas.
Para la LAN_L10, se va a instalar un nuevo el equipo (3745) en el edificio donde se encuentran los equipos dorsales de esta región, el tiempo estimado es de una semana. Para conectar a los usuarios de esta LAN se van a necesitar 3 switches (distribución y 2 acceso) el tiempo que se empleara desde la configuración hasta la instalación es de tres semanas.

En cuanto a los routers MTY_R_{21}, MTY_R_{22} seguirán funcionando normalmente ya que estos equipos no se sustituirán. El tiempo puede variar dependiendo de los contratiempos que en algún determinado momento pueden ocurrir. Se instalará un Gateway 2811 para dar servicio a las operadoras. Lo anterior se muestra en la Figura a 4.3

INTALACIÓN DE EQUIPOS E INTERVENCIÓN R6

CAN	Articulo	Descripción	Nombre del equipo_LAN	Region	Proyecto	Fecha de Solicitud de instalacionde	Fecha Programada
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	MTR_R23_LAN-L9	6	ADMIN	18-Ene-10	22-Ene-10
5	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	MTR_R23_LAN-L9	6	ADMIN	25-Ene-10	26-Mar-10
1	3745	4-slot, Dual FE, Mul service Rauter 32F/ 256D	MTR_R24_LAN-L10	6	OPER , ADMIN	29-Mar-10	2-Abr-10
9	3550	24 10/100 ports and 2 GBIC-based puertos Gigabit	MTR_R24_LAN-L10	6	OPER , ADMIN	5-Abr-10	23-Abr-10
1	Gateway 2811 DC	4-slot, Dual FE, Mul service Rauter 32F/ 256D	MTR_R21_R22	6	OPER	23-Abr-10	30-Abr-10

Tabla Región 6 (Figura 4.3)

4.2 Instalación de Enlaces.

Región 4, 5 y 6 (Monterrey, Guadalajara, Metropolitana)

Para la Región 4, 5 y 6 se va a mandar a construir otro enlace E1, cada E1 desde la fecha de la solicitud de la instalación hasta la fecha programada de la instalación y configuración, se lleva aproximadamente dos semanas.

Para el Backbone se van a mandar a construir otros 3 enlaces para poder dar servicio al incremento de usuarios tanto administrativos como operadoras.

La instalación de los enlaces se programa y calendariza de tal manera que se pueda llevar un control y una bitácora de cuales son los enlaces que se van a instalar y cual será el tiempo aproximado que durara la instalación de cada uno, debe considerarse que estos tiempos marcados son solo aproximados y podrían verse cambiados dependiendo de las fallas que puedan existir en el momento que se esta realizando todo el proceso. Esto lo podemos ver mejor ejemplificado en la siguiente tabla Figura 4.4

INSTALACIÓN DE ENLACES

CAN	Instalacion de enlaces	Descripción	Region		Proyecto	Fecha de Solicitud de instalacion del enlace	Fecha Programada de Instalacion de enlaces
1	E1	enlace entre el router MTY_R1 y MTY_R2	R4	dos semanas	VOIP , ADMIN	30-Abr-09	10-Sep-09
1	E1	enlace entre el router GDL_R11 y GDL_R12	R5	dos semanas	VOIP , ADMIN	13-Sep-09	24-Abr-09
1	E1	enlace entre el router MTR_R21 y MTR_R22	R6	dos semanas	VOIP , ADMIN	27-Abr-09	8-May-09
1	E1	enlace entre el router MTY_R1 y GDL_R12	R4_R5	dos semanas	VOIP , ADMIN	11-May-09	22-May-09
1	E1	enlace entre el router MTY_R2 y MTR_R22	R4_R6	dos semanas	VOIP , ADMIN	25-May-09	5-Jun-09
1	E1	enlace entre el router GDL_R11 y MTR_R21	R5_R6	dos semanas	VOIP , ADMIN	8-Jun-09	19-Jun-09

Figura 4.4

Capitulo 5. Conclusiones.

5.1 Ventajas de la propuesta

- Esta red es una topología jerárquica de dos niveles, los cuales son dorsal/distribución y acceso.

- Los nodos de los segmentos LAN se calcularon considerando un crecimiento a tres años manejando el doble de usuarios.

- Los nodos dorsales tienen una alta capacidad para soportar el tráfico que demandan los nodos de acceso, teniendo además redundancia entre si lo cual nos brinda la seguridad de que si se llega a caer un enlace este tendrá un camino alterno para que la información llegue a su destino.

- Debido a las características de nuestra red, el protocolo que más se adapta a nuestras necesidades es EIGRP (Enhansed Interior Gateway Routin Protocol) ya que solo se esta ocupando equipo Cisco y nuestra red es pequeña.

- El trafico de las regiones cuenta con un sistema redundante con balanceo de carga, esto es que el 50% de la información se va a mandar por primer enlace enlace y el otro 50% por un segundo enlace.

- El direccionamiento que se ocupo en una clase B, la cual nos brinda la capacidad de expansión de la red, considerando que el direccionamiento tanto a segmentos LAN como enlaces WAN y Loopbacks, son suficientes durante un periodo de tres años.

5.2 Aspectos económicos

- El costo de un enlace de 2 Mbps considerando gastos de instalación mas la renta mensual es de aprox. $206,394.

- Se necesitara adicionar 3 enlaces WAN para el crecimiento de la red.

- Por cada región aproximadamente se va a tener un costo de $691,013.00, el costo aproximado por enlace a un año es de $1,200,000.00. Se tiene que considerar que al aprovechar al máximo los recursos ya existentes solo se esta gastando aprox. un 50% para llegar al mejoramiento de la red.

5.3 Experiencia

- El conocer los costos de los equipos y enlaces nos ayuda a dimensionar la inversión necesaria para la reingeniería de una red de datos que brinda varios servicios y a si mismo calcular la recuperación de la inversión, viendo la viabilidad del proyecto.

- Los cambios en la topología utilizando un sistema redundante con balanceo de carga nos brinda la seguridad de que nuestra información siempre va a llegar a su destino en el menor tiempo posible, eficientando la calidad en el servicio.

- El cambio de direccionamiento a una clase mas grande nos brinda mayor administración de segmentos de red, además el tener sumarizada la red nos brinda mayor rapidez en la conmutación de la información haciendo los procesos con mayor velocidad.

Apéndice

10BaseT. Especificación Ethernet de banda base de 10Mbps que utiliza 2 pares de cable de par trenzado (Categoría 3, 4 ó 5): un para para la transmisión de datos y otro para recibirlos. 10 BaseT forma parte de la especificación IEEE 802.3 y tiene una distancia límite de aproximadamente 100 metros por segmento.

100BaseT. Especificación Fast Ethernet de banda base de 100Mbps que utiliza cableado UTP. Al igual que la tecnología 10BaseT en la que se basa, 100BaseT envía impulsos de enlace a través de los segmentos de la red cuando no se detecta tráfico. Sin embargo, estos impulsos de enlace contienen mas información que los utilizados en 10BaseT. Se basa en el estándar IEEE 802.3.

Algoritmo. Regla o proceso bien definido para obtener la solución de un problema. En networking, los algoritmos se utilizan normalmente para determinar la mejor ruta para el tráfico desde un origen particular a un destino en particular.

AM (Amplitud Modulada). Una de las tres formas básicas para agregar información a una señal senoidal, la amplitud de la onda senoidal, o el sistema de transmisión, se modifica de acuerdo a la información a ser transmitida.

Amplificador. Componente electrónico usado para levantar o amplificar señales. El desempeño, también llamado ganancia, se mide en decibeles.

Analógico. Un modo de transmisión en el que los datos se representan por una señal eléctrica de variación continua. Contraste con digital.

Ancho de banda. Diferencia entre las frecuencias mas alta y mas baja disponibles para las señales de red. También se utiliza para describir la capacidad de rendimiento medida de un medio o protocolo de red específico.

ARP (Protocolo de Resolución de Dirección). Un protocolo de control de transmisión/protocolo de Internet (TCP/IP) que mapea una dirección IP a direcciones Ethernet; requerido por TCP/IP para ser usado con Ethernet.

Arquitectura. La manera en la que un sistema (tal como una red o una computadora) o un programa estructurado.

Asíncrono. Una forma de transmisión concurrente de entrada y salida con ninguna relación de tiempo entre las dos señales. Una transmisión asíncrona de baja velocidad requiere de bits de inicio y de parada para evitar dependencia de los relojes de tiempo (10 bits para enviar un byte de 8).

Backbone. Parte de una red que actúa como una ruta primaria para el tráfico que se origina en, y se destina a, otras redes.

Banda Ancha. Un método de transmisión que usa un ancho de banda mayor a los canales de gardo voz y que puede ser capaz de velocidades de transmisión mucho mayores. En transmisión en difusión, múltiples canales accesan un medio (normalmente cable coaxial) que tiene banda ancha, usando módems de radio-frecuencia. Cada canal ocupa (esta modulado a) una ranura de frecuencia diferente en el cable y esta demodulada a su frecuencia original en el lado receptor. La televisión por cable es un ejemplo, con mas de 50 canales ocupando un solo cable coaxial.

Binario. Sistema de numeración caracterizado por unos y ceros (1 = Encendido u On; 0 = apagado u Off).

Bit (Digito Binario). La unidad de información mas pequeña en un sistema binario, un bit puede tener un valor cero ó un uno.

Bps (Bits por segundo). Unidad de medida en la transmisión digital serie.

Buffer. Un dispositivo que almacena datos temporalmente de un dispositivo mas rápido, y después lo envía a un dispositivo esclavo. El dispositivo mas rápido entonces puede irse a realizar otra tarea mientras el dispositivo mas lento esta dedicado al dispositivo esclavo. Un buffer entre su PC y su impresora le permite regresar a trabajar rápidamente después de haber enviado el archivo a imprimir. Los buffers también son llamados spoolers.

Byte. Una unidad de información, usada básicamente para referirse a transferencia de datos, capacidad de semiconductor y almacenamiento de datos; también es referido como carácter; un grupo de ocho (a veces siete) bits usados para representar un carácter.

Cable de fibra óptica. Medio físico capaz de conducir transmisión de luz modulada. Comparado con otros medios de transmisión, el cable de fibra óptica es mas costoso, pero no es susceptible a las interferencias electro magnéticas, también es llamado Fibra óptica.

Cableado de Categoría 3. Uno de los cinco grados de cableado UTP descritos en el estándar EIA / TIA 568B. El cableadote Categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10Mbps.

Cableado de Categoría 5. Uno de los cinco grados de cableado UTP descritos en el estándar EIA / TIA 568B. El cableado de categoría 5 se utiliza para ejecutar CDDI y puede transmitir datos a velocidades de hasta 100Mpbs.

Colisión. En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

Compresión. Una técnica usada para incrementar el numero de bits por segundo enviados por un enlace de datos reemplazando caracteres, arreglos y secuencias de comandos que se repiten frecuentemente con código electrónico. Cuando estos datos comprimidos llegan al lado remoto del enlace de transmisión, los datos codificados son reemplazados con datos reales. También se llama “compactación”.

Concentrador. Dispositivo que sirve como centro de una red de topología en estrella y que conecta las estaciones finales. Opera en la capa 1 del modelo de referencia OSI. Repetidor multipuerto Ethernet.

Congestión. Tráfico que supera la capacidad de la red.

Consola. DTE a través del cual se introducen los comandos en un host.

Control de acceso al medio. La más baja de las 2 subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC manipula el acceso a los medios compartidos, como si se empleara la transmisión de testigos o la contención.

Convergencia. Velocidad y capacidad de un grupo de dispositivos de internetworking que ejecutan un protocolo de enrutamiento específico con el fin de ponerse de acuerdo acerca de la topología de una internetwork después de un cambio en esa topología.

Datagrama IP. Unidad fundamental de información transmitida a través de Internet. Contiene direcciones de origen y de destino junto con datos y un número de campos que definen cosas como la longitud del datagrama, la suma de comprobación de la cabecera e indicadores que señalan si se puede o no fragmentar el datagrama.

DCE. Equipo de comunicación de datos o equipo de terminación de circuito de datos. Los dispositivos y las conexiones de una red de comunicaciones que comprenden el extremo de la red de la interfaz de red del usuario. El DCE proporciona una conexión física a la red., envía tráfico y proporciona una señal de sincronización utilizada para sincronizar la transmisión de los datos entre los dispositivos DCE y DTE. Los módems y las tarjetas de interfaz son ejemplos de DCE.

Desmultiplexación. Separación en varios flujos de salida de varios flujos de entrada que han sido multiplexados en una señal física común.

Dirección IP. Dirección de 32bits asignada a los hosts que utilizan TCP / IP. Una dirección IP pertenece a una de cinco clases (A, B, C, D o E) y se escribe en forma de cuatro octetos separados por puntos. Cada dirección consiste en un número de red, un número opcional de subred y un número de host. Los números de red y de subred unidos se utilizan para enrutar, y el número de host se utiliza para direccional a un host individual dentro de la red o subred. Se utiliza una máscara de subred para extraer información de red y subred de la dirección IP. CIDR proporciona una nueva forma de representar las direcciones IP y las máscaras de subred.

E1. Un circuito digital que corre a 2.048 Mbps.

Ethernet. Especificación LAN de banda base inventada por Seros Corporation y desarrollada conjuntamente por Seros, Intel y Digital Equipment Corp. Las redes Ethernet

utilizan CSMA / CD y funcionan en distintos tipos de cable a 10, 100 y 1000 Mbps. Ethernet es similar a la serie de estándares IEEE 802.3.

Fast Ethernet. Cualquiera de una serie de especificaciones Ethernet de 100Mpbs. Fast Ethernet ofrece una velocidad 10 veces superior a la de la especificación 10BaseT Ethernet mientras mantiene cualidades tales como formato de trama, mecanismos MAC y MTU. Estas similitudes permiten la utilización de las aplicaciones 10BaseT existentes y herramientas de administración de red en redes Fast Ethernet. Se basa en una ampliación de la especificación IEEE 802.3.

Fibra Multimodo. Fibra óptica que soporta la propagación de varias frecuencias de luz.

Frecuencia. Medida en Hertz (Hz), es el número de ciclos de una señal de corriente alterna por unidad de tiempo.

Full duplex (FDX). Capacidad de transmisión simultanea de datos en ambas direcciones.

Gateway. En la comunidad IP un antiguo término que se refiere a un dispositivo de enrutamiento. Hoy se utiliza el término router para describir los nodos que realizan esta función, y gateway se refiere a un dispositivo con un fin especial que realiza una conversión de capa de aplicación de la información desde una pila de protocolo a otra.

Half duplex. (HDX). Transmisión en cualquier dirección, pero no en ambas direcciones simultáneamente.

Hertz (Hz). Una medida de frecuencia o de ancho de banda, 1 Hz es igual a un ciclo por segundo.

Host. Sistema de computadora en una red. Similar a un nodo, excepto que host habitualmente implica un sistema de computadora, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers.

IEEE 802.3. Protocolo LAN del IEEE que especifica la implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza acceso CSMA / CD a distintas velocidades sobre distintos medios físicos.

IGRP. Protocolo de enrutamiento de Gateway Interior, Interior Gateway Routing Protocol. IGP desarrollado por Cisco para tratar los problemas asociados con el enrutamiento en grandes redes heterogéneas.

Interfaz. 1) Conexión entre dos sistemas o dispositivos. 2) En terminología de enrutamiento, conexión de red en el router.

Interoperabilidad. Capacidad de las computadoras fabricadas por distintos vendedores de comunicarse unas con otras satisfactoriamente en una red.

IOS. Sistema Operativo de Internetwork. Software de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes a todos los productos bajo la arquitectura Cisco fusión. El software CISCO IOS permite la instalación y administración centralizadas,

integradas y automatizadas de internetworks mientras aseguras el soporte de una amplia variedad de protocolos, medios, servicios y plataformas.

ISDN. Red Digital de Servicios Integrados.

ISO. Organización Internacional responsable de un amplio abanico de estándares incluidos los referidos a internetworking. ISO desarrolló el modelo de referencia OSI un popular modelo de referencia de networking.

LAN. Red de Area Local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña. Las LAN conectan estaciones de trabajo, periféricos, terminales, y otros dispositivos en un solo edificio u otra área limitada geográficamente.

Malla. Una topología de red donde los dispositivos están organizados de un modo manejable y segmentad, con muchas interconexiones colocadas estratégicamente entre los nodos de red.

Multiplexaje. Técnica para la cual es posible dividir un canal de transmisión, ya sea en tiempo o en frecuencia, con el interés de crear varios canales y transmitirlos en forma simultanea.

OSI (Open Systems Interconnection). Estructura lógica para operaciones en red estandarizado por la ISO. Una arquitectura de red de siete capas de OSI define y estandariza los protocolos de comunicación, permitiendo que cualquier sistema computarizado compatible con OSI se comunique con cualquier otro dispositivo que cumpla también con los mismos estandares y pudiendo así manejar una amplia gama de intercambio de información.

PAM (Pulse Amplitud Modulation). Tipo de modulación en la cual la amplitud de la señal portadora (transmitida) varia en función de la señal de información.

PBX (Prívate Branco Exchange). Termino genérico utilizado al referirse a los conmutadores telefónicos privados; también se le conoce como PABX.

Pleosincrono. Termino que se refiere a señales sincronías digitales que tienen tasas muy similares, con variaciones acotadas por limites muy específicos alrededor de un mismo valor nominal.

Bibliografía.

Guía del primer año.
CCNA 1 y 2.
Tercera Edición.
Cisco Systems

Programa de estudios autorizados por la academia de networking de Cisco
Guía del Segundo Año.
Segunda Edición.

http://www.eveliux.com/telecom/servdig.html

http://www.cisco.com/en/US/tech/tk1330/tsd_technology_support_technical_reference_chapter09186a00807596d3.html#wp1020617

http://www.cisco.com/en/US/tech/tk1330/tsd_technology_support_technical_reference_chapter09186a00807598ad.html

http://www.cisco.com/en/US/tech/tk1330/tsd_technology_support_technical_reference_chapter09186a0080759837.html

http://www.cisco.com/en/US/tech/tk1330/tsd_technology_support_technical_reference_chapter09186a0080759781.html#wp1020627

http://cisco.netacad.net

http://www.cisco.com/en/US/products/hw/routers/ps282/products_quick_start09186a008007e2fb.html

http://www.cisco.com/en/US/products/hw/routers/ps359/products_quick_start09186a00800dc779.html