UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"METODOLOGÍA PARA LA PLANEACIÓN Y EL DISEÑO DE UNA RED VIRTUAL SIN CONEXIÓN CLNS (CONECTIONLESS NETWORK SERVICE)"

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO EN TELECOMUNICACIONES E INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A N:

VÍCTOR OCTAVIO CID CASTILLO

JUAN CARLOS PÉREZ CRUZ

DIRECTOR DE TESIS: DR. FRANCISCO JAVIER GARCÍA UGALDE

CIUDAD UNIVERSITARIA, OCTUBRE 2004

Agradecimientos:

Papá y mamá, por recordarme con amor e interés la culminación de este ciclo de mi vida, fueron mi motivación en todo momento.

Doctor Francisco J. García Ugalde, por su gran apoyo y ejemplo a lo largo de todo este tiempo de conocerlo, así como la confianza y paciencia que nos brindó para este trabajo.

Marisol, por esos fines de semana que dediqué a este proyecto con tu compañía.

Fito, por tu incondicional apoyo y dedicación en la revisión de cada capítulo..

Amigos, por recordarme en todo momento la satisfacción de concluir esta etapa.

VOCC

Agradecimientos:

A mis Padres, por el apoyo y motivación.

A Ale, por ser mi cómplice y eterna compañera.

A mi hija Carla, por dar un nuevo color a la vida.

Al Doctor Francisco J. García Ugalde, por su apoyo y orientación en la elaboración de esta tesis.

Fito, gracias por tus comentarios.

Vic, gracias por tu apoyo incondicional.

JCPC

Índice

1. Introducción

La evolución que han tomado las redes de telecomunicaciones hasta nuestros días, ha tenido un crecimiento a velocidad impresionante en las últimas tres décadas. Anteriormente las compañías podían tener o rentar redes separadas de voz y datos para el transporte de información entre sus oficinas, lo cual trae consigo inversiones duplicadas, incremento en costos de mantenimiento, rentas, etc. A final de cuentas, estas redes, frente a los nuevos requerimientos, se vuelven obsoletas e incapaces de poder enfrentar las nuevas tecnologías nacientes. Actualmente el punto de convergencia de las redes esta enfocado hacia la capacidad de poder transportar voz, video y datos, sobre una misma infraestructura.

Esta evolución de la redes de telecomunicaciones se ha venido apoyando en gran medida en el aumento de usuarios y en la satisfacción de las múltiples necesidades de comunicación que crecen día con día. Estas dos razones principales requieren implícitamente el poder transportar grandes cantidades de información de manera segura y rápida.

Hoy en día, las más importantes tecnologías de transporte de información de gran capacidad, se encuentran basadas en dispositivos de alto desempeño, los cuales están sincronizados por un reloj común, e interconectados por fibra óptica. Las redes de mayor empleo entre la mayoría de los operadores de redes de telecomunicaciones son las redes basadas en las tecnologías SDH y SONET.

Sin embargo, la operación de una red de telecomunicaciones, no solo debe abarcar el transporte de información, ya que esto resultaría en un servicio de transporte de baja disponibilidad, debido principalmente al hecho de no poder determinar fallas en algún punto de la red en tiempo real. Esto conlleva a la gestión de estas redes mediante un grupo de trabajo dedicado de manera exclusiva a esta tarea, apoyándose en herramientas y esquemas que así lo permitan, con el fin de asegurar la atención oportuna a fallas, o problemas de red, en todo momento; asegurando así una alta disponibilidad en el servicio de transporte de información. Esta gestión resultará proporcional al tamaño y al nivel de criticidad de la red, donde la gestión puede resultar una tarea compleja y grande.

Con base en lo anterior y considerando el manejo del control de la red en forma total, el esquema de gestión se concentra generalmente en un solo sitio, asistiendo de manera remota a los elementos de red bajo observación y requiriendo de técnicas de supervisión para tal efecto. Bajo esta forma de operación centralizada se pueden reducir los tiempos y los costos asociados, como son el tener personal en sitio y su correspondiente coordinación para cualquier evento o contingencia.

El tener un centro de gestión remoto de los equipos en cuestión, requiere analizar la mejor manera de enviar la información de monitoreo y gestión a este centro de gestión. De aquí se origina la filosofía de contar con una red de datos independiente a la red supervisada (SONET[1] o SDH[2]), para asegurar la disponibilidad del servicio de gestión en todo momento.

Por otra parte, la mayoría de los proveedores de equipo de transporte bajo las tecnologías SDH y SONET emplean los protocolos definidos por la Organización Internacional de Estándares (ISO por sus siglas en inglés), para las necesidades de gestión y estas se encuentran directamente basadas en el modelo de referencia OSI. Lo anterior es fundamental al considerar una solución para el transporte de la información de gestión hasta los centros de monitoreo y administración.

[1] SONET: *Synchronous Optical NETwork*
[2] SDH: *Synchronous Digital Hierarchy*

1.1. Justificación para el diseño de la "Red virtual CLNS"

La presente tesis analiza y propone la mejora para el caso particular de la gestión de una red de transporte bajo la tecnología SDH, compuesta de equipos heterogéneos de varios proveedores y que dan este servicio a diferentes regiones del país. La gestión para todos estos elementos se encuentra centralizada en base a sistemas de gestión, ubicados en diferentes sitios a lo largo de una misma red de datos de tipo multiservicos.

Los protocolos de red empleados para la gestión de todos los elementos de red se basan en los definidos por ISO, fundamentalmente: IS-IS[3] y CLNP[4].

La propuesta de mejora, tiene como objeto optimizar el servicio de transporte de información de gestión de los elementos de red SDH, los cuales se encuentran en producción y son administrados por varios sistemas que operan de manera independiente. Tales mejoras abarcan los siguientes aspectos:

- La administración de una sola red para el transporte de información de gestión y monitoreo sobre el principio CLNP, para los sistemas mencionados.
- La creación de una nueva topología que sea sencilla y redundante.
- El aumento de la rapidez en la detección y corrección de fallas.
- El crecimiento sencillo de los sistemas de gestión y monitoreo que se encuentran en producción y la fácil integración de otros nuevos.
- Facilitar el cambio en las ubicaciones de los elementos gestores, gestionados o monitoreados, de cualquier sistema.
- Inversión mínima en la solución, al ser este un desarrollo basado en funcionalidades y tecnologías ya contenidas en los enrutadores empleados, adquiriendo un mínimo de equipamiento para dar robustez y confiabilidad a esta.

El esquema a utilizar en la propuesta se basa en la creación de una red para el transporte de información sobre el protocolo CLNP. Esta red es del tipo privada virtual (VPN), construida sobre una infraestructura de red en operación (recursos actuales). Es decir, en vez de utilizar nuevos enlaces dedicados para conectar redes remotas y crear una red paralela, se utiliza la infraestructura IP actual y una vez que estas redes están conectadas el servicio para los usuarios será transparente.

El servicio de Red Privada Virtual permite conectar diferentes centros de trabajo entre sí desde cualquier parte de la republica. En la modalidad VPN se podrán conectar permanentemente los diferentes sitios que utilicen el protocolo CLPN y acceder a los diferentes recursos de gestión SDH.

La tecnología de Red Privada Virtual está basada en el establecimiento de túneles de comunicación a través de la red IP privada, estos túneles garantizan su seguridad mediante el uso de protocolos que facilitan la interconexión de los equipos CLNP, así como el cifrado de los datos para su transporte dentro de la red IP.

La principal justificación y motivación para la implantación de la Red Privada Virtual VPN, es de orientación financiera: los enlaces dedicados son caros, y tienen un costo de instalación y de renta mensual. Por otro lado existe una red IP, que es una red de alcance nacional y tiene puntos de presencia esparcidos por toda la república. Esto será considerado y explotado en nuestra solución propuesta.

[3] IS-IS: *Intermediate system to intermediate system*
[4] CLNP: *Connectionless Network Protocol*

1.2. Contenido del documento

La presente tesis consta de seis capítulos subdivididos cada uno de ellos en diferentes temas, los cuales estructuran y explican de manera clara los fundamentos y el contenido total de la propuesta de diseño. A continuación se describen de manera general cada uno de estos capítulos:

El presente capítulo expone las razones por las cuales se decidió proponer el diseño de una red virtual para el transporte de información de gestión de elementos SDH basados en el protocolo CLNP, así como la descripción general del contenido de esta tesis.

El segundo capítulo describe los fundamentos y la operación de la tecnología de transporte SDH, o Jerarquía Digital Síncrona, la cual constituye la aplicación a gestionar a través de la propuesta de diseño de Red Virtual de la presente tesis.

El tercer capítulo explica las bases de enrutamiento y los protocolos de capa 3 del modelo de referencia OSI, empleados por las aplicaciones de gestión de elementos SDH y por la Red Virtual propuesta. Asimismo se describen otros protocolos de otras capas, los cuales también son usados en el funcionamiento e implementación de la solución.

El cuarto capítulo expone los criterios y consideraciones que deben tomarse en cuenta a lo largo del diseño de una red de datos. Siendo éstos utilizados para la investigación de la información, el análisis, , el diseño y finalmente la implementación de la red virtual propuesta.

El quinto capitulo cubre en detalle el proceso de creación de la red de gestión, basándose en la definición y conocimiento de los conceptos descritos en los capítulos anteriores. Inicialmente se describe el marco en el cual se desenvolverá la propuesta de diseño, es decir, la estructura de la red física sobre la cual estará montada la Red Virtual. La forma de operación de esta, las políticas de operación y crecimiento de la misma red física, y el funcionamiento actual del servicio de transporte de información de gestión (CLNS[5]). Posteriormente se describen los objetivos que deberá alcanzar el diseño y consecuentemente la propuesta de la red virtual, describiendo la razón de su diseño y su operación. Una vez explicado este diseño se describe su proceso de implementación, constando de adecuaciones a la red física de datos, instalación de nuevos equipos, pruebas de funcionamiento y la migración del actual esquema a la nueva "Red Virtual CLNS". Finalmente se explican las consideraciones de ajuste del diseño con base en su propia operación.

El sexto y ultimo capitulo de la presente tesis expone las conclusiones a las que llegamos a lo largo de la investigación, diseño e implementación de la "Red Virtual CLNS"; así como los ajustes finales al diseño ya implementado.

Esta tesis presupone el entendimiento de los fundamentos básicos en redes de datos por parte del lector para su clara comprensión. Sin embargo, si este no fuese el caso, se ha incluido bibliografía la cual puede usarse como referencia para tal propósito.

[5] CLNS: *Connectionless Network Services*

2. La tecnología SDH

Las primeras generaciones de sistemas de fibra óptica empleadas por las redes de telefonía pública empleaban arquitecturas, códigos de línea, formatos de mutliplexaje y procedimientos de mantenimiento propietarios. Lo anterior originó que los usuarios de estos equipos requirieran de un estándar que permitiera mezclar y combinar equipos de diferentes marcas.

La tarea de crear un estándar fue comenzada en 1984 por la asociación de estándares para compañías telefónicas, ECSA, en los Estados Unidos, y establecer así una conexión entre diferentes sistemas de fibra óptica. En las últimas etapas del desarrollo, la CCITT[6] se involucró desarrollando un estándar internacional para las diferentes redes de telecomunicaciones. El estándar resultante fue nombrado SDH.

El SDH, *Synchronous Digital Hierarchy* fue introducido en 1992, fue diseñado para tasas de alta velocidad usando una señal síncrona multiplexada, que es transportada principalmente a través de un cable de fibra óptica, o bien a través de enlaces de radio, satelitales e interfaces eléctricas.

La creciente demanda en flexibilidad y de ancho de banda en los sistemas de telecomunicaciones, hacen que SDH tenga grandes ventajas en comparación con los sistemas anteriores a este, como PDH. Las principales ventajas se listan a continuación:

- Reducción en la cantidad de equipo e incremento en la confiabilidad de la red.
- La introducción de *bytes* de encabezado y de *bytes* carga útil. Los *bytes* de encabezado permiten la administración de la información transportada y los *bytes* de carga útil individualizan y facilitan el manejo de la misma información bajo un esquema centralizado y regional.
- La definición de un formato de multiplexaje síncrono para transportar señales digitales de bajo nivel, como señales de 2, 34 y 140 Mbps. Lo cual simplifica grandemente la interconexión de conmutadores digitales, equipos de crosconexión digital y multiplexores de inserción y retiro de información.
- La disponibilidad de un conjunto de estándares genéricos, los cuales permiten la interoperabilidad entre diferentes proveedores de equipo.
- La definición de una arquitectura flexible, capaz de soportar aplicaciones futuras con una variedad de tasas de transmisión.

2.1. La sincronización de las señales digitales

Para entender correctamente los conceptos y detalles de SDH, es importante tener claro el significado de los términos síncrono, plesiócrono y asíncrono. A continuación se describen los mismos:

Señales síncronas.- Si comparamos dos señales síncronas, las transiciones digitales entre ambas, suceden exactamente al mismo tiempo. Sin embargo, estas pueden tener una diferencia en la fase, la cual, puede situarse dentro de ciertos límites especificados. Estas diferencias de fase pueden surgir a causa de retardos en la propagación de la señal, o por una interferencia de baja frecuencia en la red de transmisión. En una red síncrona, todos los relojes son alimentados por uno solo de referencia principal, el cual tiene una exactitud de $\pm 1 \times 10^{-11}$ y comúnmente es de cesio.

Señales plesiócronas.- Si dos señales digitales son plesiócronas, sus transiciones suceden casi al mismo tiempo. Esto sucede cuando dos relojes diseñados y fabricados de la misma forma, son usados para generar dos señales independientes; si bien en principio deberían operar a la misma frecuencia, existen diferencias a nivel molecular que producen variaciones en frecuencia entre las señales así generadas.

Esta diferencia de frecuencias es muy pequeña y debe estar dentro de los límites establecidos en la recomendación ITU-T G.811. Por ejemplo si dos redes necesitan ínter operar, sus relojes pueden

[6] Comité Consultativo Internacional de Telefónico y Telegráfico ahora conocido como UIT , Unión Internacional de Telecomunicaciones.

provenir de dos fuentes diferentes. Aunque estos relojes son extremadamente exactos, existe una pequeña diferencia de frecuencia entre uno y otro. Esta diferencia es conocida como plesiócrona.

Señales asíncronas.- para estos casos, las transiciones ente dos señales digitales, no suceden a la misma tasa. El término asíncrono, para este caso, indica que la diferencia entre los relojes es mucho mayor que la diferencia plesiócrona.

A continuación se explica de forma general el funcionamiento y operación del sistema PDH, el cual permitió justificar el desarrollo de la tecnología SDH:

2.2. Jerarquía Digital Plesiócrona, PDH

A principio de los años 70´s, los sistemas de transmisión digital comenzaron a aparecer utilizando un método conocido como PCM, o "modulación por codificación de pulsos". Este permitió que la señal analógica de voz fuera representada de forma binaria a una tasa de transmisión de 64 kbps. De esta forma, los desarrolladores observaron el potencial para producir sistemas de transmisión con un costo mas efectivo combinando varios canales de PCM y transmitiéndolos por el mismo cable, el cual estaba siendo ocupado anteriormente por una sola señal analógica.

De lo anterior, surgieron dos estándares principales de multiplexación por división del tiempo, o TDM, para ordenar la manera en como combinar varios canales de voz en uno de mayor capacidad:

El estándar definido en Estados Unidos propone la multiplexación de 24 canales de 64 Kbps cada uno, para crear un canal de 1544 Kbps. La combinación de estos 24 canales se realiza intercalando 8 bits de cada canal, dando una trama de 192 bits. A esta trama se le agrega un bit que es empleado para efectos de sincronización, dando un total de 193 bits por trama. Si consideramos que se tiene una tasa de transmisión de tramas de 8000 tramas/seg., esto nos da la tasa total de 1544 Kbps, o T1.

El estándar europeo, que consecuentemente fue adoptado en muchos otros países del mundo, combina 30 canales de 64 Kbps junto con dos canales adicionales para información de control y sincronización, para producir uno nuevo a una tasa de transmisión de 2048 Kbps. Cabe mencionar que a lo largo del presente capítulo nos enfocaremos al estándar europeo, dado que es el empleado en el desarrollo de nuestro trabajo.

Conforme creció la demanda telefónica, también sucedió con los niveles de tráfico en la red. Se observó que la señal estándar de 2 Mbps ya no era suficiente para hacer frente a las cargas de tráfico presentes. Entonces, con el objeto de evitar el uso de un gran número de enlaces de 2 Mbps, se decidió crear un nivel superior de multiplexación. El estándar de crecimiento adoptado en Europa involucra la combinación de 4 canales de 2 Mbps, para producir uno solo de 8 Mbps. Este nivel de multiplexación difiere ligeramente de su origen, ya que en el multiplexaje a 2 Mbps las señales entrantes se combinan un *byte* a la vez, en cambio para este nivel se combinan un bit a la vez. Conforme las necesidades de transmisión crecieron, se agregaron niveles superiores, creándose los estándares de 34 Mbps, 140 Mbps y 565 Mbps, para producir una jerarquía completa de tasas de bits, como se observa en la tabla 2.1:

Señal	Tasa de transmisión	Canales
E0	64 Kbps	Un canal de 64 Kbps
E1	2.048 Mbps	32 E0
E2	8.448 Mbps	128E0
E3	34.368 Mbps	16 E1
E4	139.264 Mbps	64 E1

Tabla 2.1 Jerarquía de multiplexación.

La jerarquía de multiplexación descrita anteriormente es sencilla en su principio, sin embargo, presenta ciertas complicaciones en su implementación. Cuando se genera una señal de 8 Mbps, es muy probable que sus canales de origen se hayan creado con piezas de equipo diferentes, con lo que se generan tasas

de transmisión de bits ligeramente diferentes (señales plesiócronas). De esta forma, antes de que los canales sean intercalados para formar la señal de 8 Mbps, estos deben sincronizarse a la misma tasa de transmisión agregando bits de justificación, o de relleno.

Estos bits de justificación son reconocidos cuando se ejecuta la demultiplexación y son descartados para recobrar la señal original. Este proceso se conoce como operación plesiócrona. Los mismos problemas de sincronización, suceden en cada nivel superior de la jerarquía de multiplexación, por lo que el método de agregar bits de justificación se aplica en cada etapa. El uso de la operación plesiócrona a lo largo de la jerarquía, ha logrado que se adopte el término de Jerarquía digital plesiócrona, o PDH.

2.2.1. Limitantes del sistema PDH

El problema principal con un sistema plesiócrono es la falta de flexibilidad, ejemplificándose al considerar que un operador de red está obligado a respetar el orden jerárquico del sistema para poder proporcionar una línea dedicada de 2Mbps.

Así mismo, el uso de bits de justificación en cada nivel dificulta la localización exacta de las tramas de un enlace de 2 Mbps, dentro de los canales superiores.

Por otro lado, cuando se requiere el acceso a una línea de 2 Mbps que se encuentra dentro de un canal de 140 Mbps[7], este debe demultiplexarse completamente en sus 64 enlaces de 2 Mbps, pasando por los niveles respectivos de la jerarquía. Una vez que la línea de 2 Mbps ha sido identificada y extraída, los canales deben ser mulitplexados nuevamente hasta alcanzar 140 Mbps. La figura 2.1 ilustra este procedimiento:

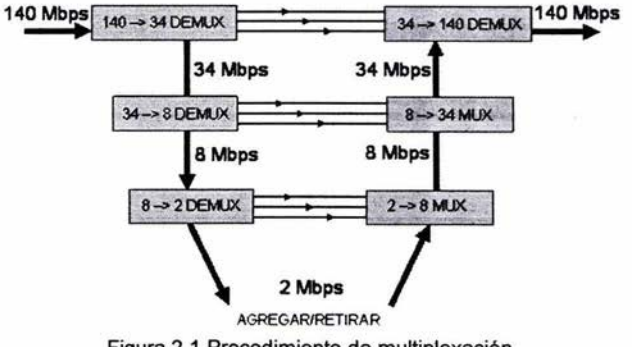

Figura 2.1 Procedimiento de multiplexación.

Obviamente este problema de inserción y retiro de canales, no permite un rápido suministro de servicios, además del costo que representa tener una gran cantidad de equipo para tal efecto.

Otro problema asociado a la cantidad de equipo de multiplexación en la red es el control, ya que una línea dedicada de 2 Mbps puede "viajar" a través de un gran número posible de rutas. La única forma de asegurar el camino correcto es tener un cuidadoso registro de la interconexión de los equipos de transmisión. Sin embargo, a medida que la actividad de reconexiones de canales se incrementa, se dificulta el mantener los registros actualizados y la posibilidad de tener errores aumenta. Tales errores pueden afectar no solo la conexión que se establezca, sino también otras ya existentes.

Finalmente, la operación y mantenimiento de los elementos que forman un sistema PDH, carece de un sistema centralizado de monitoreo y administración.

[7] la tasa de transmisión de 140 Mbps no es múltiplo exacto de 64 señales de 2.048 Mbps debido a que se requiere tener un margen de trabajo para insertar los bits de relleno y así permitir la interoperabilidad entre equipos.

2.3. Sistema de transmisión síncrona, SDH

Como se explicó en la sección anterior, el modo PDH alcanzó un punto donde no fue lo suficientemente flexible y eficiente para cumplir con el incremento de la demanda. Como resultado, las transmisiones síncronas fueron desarrolladas para resolver los problemas asociados con la transmisión plesiócrona, en particular la dificultad que tiene PDH de extraer circuitos individuales de sistemas de alta capacidad, sin tener que demutliplexar todo el arreglo.

La transmisión síncrona es vista entonces como la siguiente etapa de la evolución de los sistemas de transmisión jerárquicos. Los estándares actuales surgen de las recomendaciones de la ITU-T G.707, G.708 y G.709, que cubren la jerarquía digital síncrona SDH[8]. Estas recomendaciones fueron publicadas en el "libro azul" de la CCITT en 1989. En Estados Unidos la ANSI publico su estándar SONET, el cual puede ser considerado como un subconjunto del estándar internacional de SDH.

Adicionalmente a las recomendaciones mencionadas en los párrafos anteriores, se crearon grupos de trabajo para desarrollar otras recomendaciones que cubren otros aspectos de SDH, tales como los requerimientos para las interfaces ópticas y funciones de administración y monitoreo, OA&M (*Operation, Administration & Management*).

Dentro de este sistema, existe una estructura de multiplexaje que permite que una señal de STM-1 (155 Mbps) pueda transportar un número de señales de tasas mas bajas, que se denomina carga útil. De esta manera se permite que las señales de PDH puedan ser transportadas sobre una red síncrona, protegiendo la inversión hecha en los equipos plesiócronos por los operadores de red.

Con la integración de equipos SDH en la redes de transporte, los operadores de estas experimentan ahorros significativos asociados a la reducción del número de equipo en uso, así como un incremento en la eficiencia y confiabilidad de la red, conduciendo a una reducción de costos por mantenimiento y operaciones. Otro resultado es el incremento de la confiabilidad, visualizado en la disminución de la necesidad de mantener equipo de repuesto.

2.3.1. Principios de la Jerarquía Digital Síncrona

A pesar de las ventajas obvias que SDH tiene sobre PDH, su aceptación en la integración de las redes de telecomunicaciones podría haber sido poco probable si no hubiera soportado a las señales entregadas por los sistemas PDH previos. Por esta razón las recomendaciones de CCITT se enfocaron a permitir el transporte de cualquier tasa de transmisión PDH, para ser integrada dentro de una trama de STM-1. En consecuencia, todas las señales plesiócronas ente 1.5 Mbps y 140 Mbps pueden ser acomodadas, de tal forma que pueden ser combinadas para formar una señal STM-1, la cual está definida en la recomendación G.709. La Jerarquia de mulitplexaje SDH se muestra en la siguiente tabla:

Tasa de transmisión	Nomenclatura SDH	Capacidad relativa SDH
51.84 Mbps	STM-0	21 E1
155.52 Mbps	STM-1	63 E1 ó 1 E4
622.08 Mbps	STM-4	252 E1 ó 4 E4
2488.32 Mbps	STM-16	1008 E1 ó 16 E4
9953.28 Mbps	STM-64	4032 E1 ó 64 E4
39813.12 Mbps	STM-256	16128 E1 ó 256 E4

Tabla 2.2 Jerarquía de enlaces SDH.

[8] La presente tesis se enfocará en el estándar internacional, ya que es el empleado por los dispositivos de la propuesta de diseño descrita en el capítulo 4.

Dentro de una red SDH, todos los equipos son sincronizados por un reloj global. Sin embargo, es importante hacer notar que existen retardos asociados con el enlace de transmisión y que pueden variar ligeramente en el tiempo. Como resultado de lo anterior, la ubicación de las señales dentro de una trama de STM-1 no es fija. Estas variaciones son manejadas transportando cada señal en un espacio de tamaño fijo llamado *Contenedor*, dentro del cual la señal puede variar su ubicación. Para conocer donde comienza cada señal dentro de cada contenedor, se añade un apuntador que indica el inicio de la señal dentro del mismo. A esta asociación (Contenedor y apuntador), se le conoce como Contenedor Virtual (VC), el cual a su vez puede variar su ubicación dentro del STM. Asociando un nuevo apuntador con cada VC, se indica la posición del comienzo del mismo en relación a la trama del STM-1. De ser necesario, el valor del apuntador puede ser incrementado, o decrementado, para reubicar la posición del contenedor virtual VC.

2.3.2. Estructura de la Trama de un sistema STM-1

La multiplexación de SDH puede combinar señales digitales de baja velocidad que pueden ir de los 1.5 Mbps, a los 140 Mbps, por lo que es necesario que se tenga cierta información de control durante su transporte. La figura 2.2 muestra la trama de una señal STM-1, la cual está constituida por 9 segmentos de 270 *bytes*. Los primeros 9 *bytes* de cada segmento transportan información de control y los 261 *bytes* restantes llevan al contenedor virtual. La transmisión de esta trama es realizada enviando de manera secuencial los 9 segmentos de izquierda a derecha. La velocidad de transmisión de las tramas es de 8000 tramas/seg.

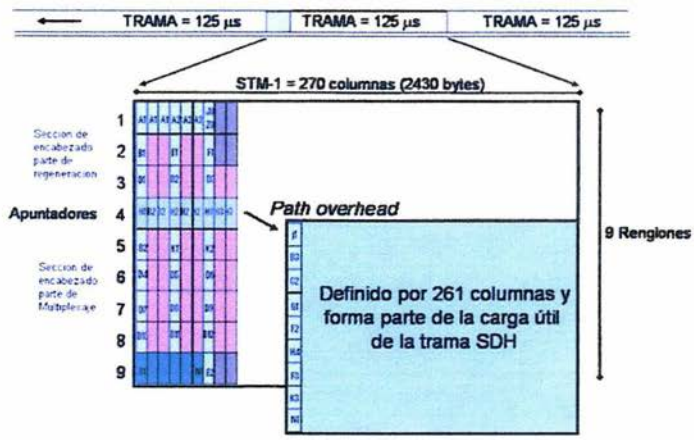

Figura 2.2 Trama STM-1.

Dado que la trama de STM-1 esta formada por dos tipos de información, las primeras 9 columnas (9 primeros *bytes* de los 9 segmentos) son llamadas *section overhead* o SOH, mientras que el resto es llamado contenedor virtual de nivel 4 VC-4. El campo de *section overhead*, está dividido a su vez en tres partes las cuales se explican a continuación, así como su esquema de aplicación mostrado en la siguiente figura:

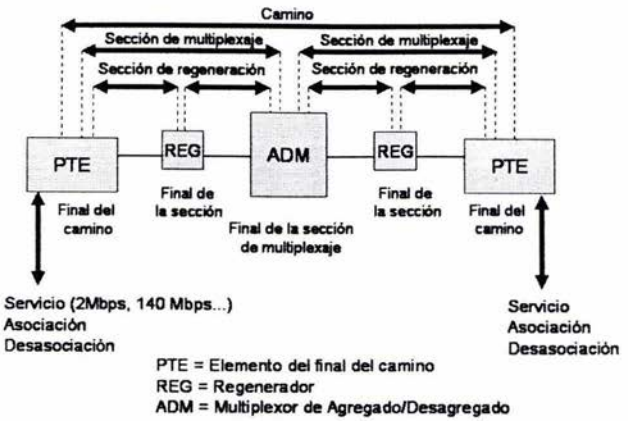

Figura 2.3 Esquema de aplicación del encabezado SDH.

***Regenerator section overhead*, RSOH**- Contiene la información que es requerida por los elementos localizados en los extremos de una sección del trayecto. Estas secciones pueden estar entre dos dispositivos de regeneración de señal, entre un equipo terminal de línea y un regenerador, o entre dos equipos terminales de línea. Es muy importante considerar que dentro de esta sección existen tres *bytes* conocidos como D1, D2 y D3, o *bytes* de canal de comunicación de datos DCC. Estos tres *bytes* crean un canal de mensajes a 192 kbps para suministrar información de Operación, Administración y Mantenimiento (OAM), entre piezas de los equipos terminales de la sección[9]. Este canal puede ser empleado de manera centralizada.

***Multiplexer section overhead*, MSOH**- Contiene la información requerida entre elementos de red consecutivos sin incluir regeneradores.

Apuntadores- Permite localizar diferencias en la fase y frecuencia de un contenedor virtual con respecto a la trama SDH. Estos apuntadores señalan la posición del contenedor virtual localizando el primer *byte* de este.

Contenedor Virtual- Dentro del contenedor virtual de nivel 4 se tiene una columna conocida como *path overhead* de nivel 4, VC-4 POH y el resto de los 260 *bytes* es para los datos. El *path overhead* es empleado para informar de alarmas e información de errores ocurridos dentro de toda la trayectoria.

La recomendación G.709 también define diferentes combinaciones de los contenedores virtuales, los cuales pueden ser usados para llenar el área de datos de una trama de STM-1. El proceso de llenado de los contenedores y la adhesión del encabezado se repite en los niveles superiores de la jerarquía de SDH, resultando el acomodo de pequeños VCs dentro de otro grande. El proceso es repetido hasta que el tamaño mas largo es alcanzado, y es entonces cargado dentro del área de los datos de la trama de STM del nivel correspondiente. Cuando el área de los datos de una trama de STM-1 está llena, son agregados ciertos *bytes* de información de control, para formar el campo *section overhead*. El nombre que se da a los *bytes* del campo *section overhead*, es debido a que permanecen junto al área de los datos, para la sección de fibra entre dos multiplexores síncronos. Su propósito es proporcionar canales de comunicación para funciones tales como OA&M; facilidades, alineación, entre otras funciones.

[9] La información de OAM transportada por este canal, se considera estructurada bajo los protocolos CLNP e IS-IS y es el método mediante el cual la propuesta de diseño de la presente tesis asume su empleo dentro de los arreglos de anillo y bus de los elementos SDH.

2.3.3. Transporte de información a diferentes tasas de transmisión

El transporte de tasas de transmisión de baja velocidad, se realiza bajo la concatenación de contenedores. Lo anterior es una técnica que permite el manejo de múltiples contenedores virtuales de bajo y alto orden como si fuera uno solo.

Para los niveles mas bajos, los contenedores (C) se manejan como entradas a los contenedores virtuales (VC). El propósito de esta función es crear una carga útil o *payload* uniforme del circuito virtual mediante el relleno de bits, para tener a todos los contenedores virtuales a una misma tasa de transmisión y su posterior multiplexado. Los contenedores de bajo nivel pueden ser soportados por la jerarquía SDH al agruparse o alinearse dentro de una unidad tributaria (TU), donde las operaciones de apuntador son usadas.

Estas funciones permiten que la carga útil sea multiplexada en grupos de TU o TUGs. Como se observa en la figura 2.4, la etiqueta xN indica el nivel de multiplexaje empleado para las TU o TUGs. El siguiente paso es el multiplexaje de los TUGs hacia un contenedor virtual de alto nivel, como los TUG-2 y TUG-3 multiplexados en un VC-4.

Estos contenedores virtuales son multiplexados con bits de relleno para formar las unidades de administración AU, las cuales finalmente son multiplexadas en un grupo de unidades de administración AU o AUG. Esta nueva carga útil formada, es multiplexada en los módulos de transporte síncono o STMs.

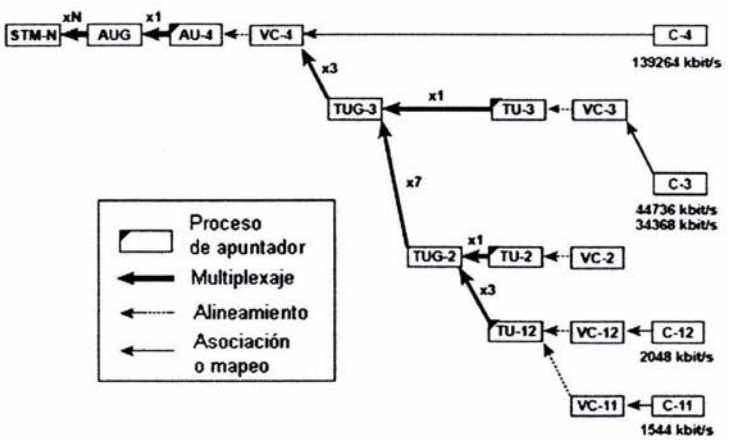

Figura 2.4 Esquema de creación de los módulos de transmisión síncrona.

La creación de tasas de transmisión superiores a un STM-1 dentro de una red síncrona, se logra intercalando *bytes* de las señales constitutivas, es decir, la creación de una tasa de transmisión de 622 Mbps (STM-4) se da intercalando los bytes de 4 señales STM-1 de forma directa. De la misma manera se genera una tasa de 2.4 Gbps (STM-16) intercalando 4 señales de STM-4, como se muestra en la figura siguiente:

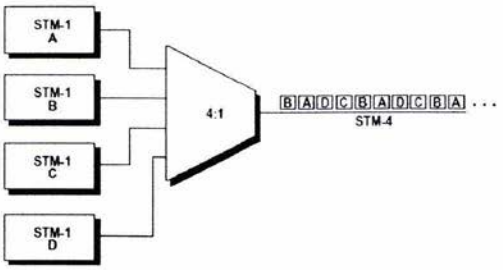

Figura 2.5 Mecanismo de multiplexación.

2.3.4. Beneficios de un sistema Jerárquico Digital Síncrono

La transmisión síncrona permite que la red de transporte se desarrolle para solventar las nuevas demandas. El sistema síncrono ofrece un número de beneficios para los operadores de red y para los usuarios finales, los cuales se describen a continuación:

Simplificación de la red.- Un solo multiplexor síncrono puede desempeñar la función de todo un conjunto de equipos plesiócronos. Permitiendo reducciones importantes en: la cantidad de equipo empleado, de costos de operación, de refacciones, de mantenimiento, en los espacios asignados para la instalación del equipo y finalmente en el consumo de potencia. La función de agregar y retirar canales en la red SDH se vuelve más eficiente, junto con una mejora en la capacidad de administración de la red.

Alta disponibilidad.- El uso de la fibra óptica a través de las redes formadas por elementos de red SDH, permite la posibilidad de monitorear, extremo a extremo, la integridad de la red. Las capacidades de administración de una red síncrona permiten una identificación inmediata de fallas en un enlace, o en un equipo. Utilizando arquitecturas de anillo auto-reparables, la red es automáticamente reconfigurable, permitiendo que el tráfico sea reenrutado de manera inmediata hasta que la falla sea reparada. De esta manera las fallas en los mecanismos de transporte dentro de la red son invisibles en los extremos, ya que no se interrumpe el servicio y permite a los operadores de red tener una alta disponibilidad de los servicios ofrecidos y garantizar altos niveles de desempeño en la red.

Control vía *software*.- El suministro de canales de administración de red dentro de la estructura de la trama de SDH, significa que la red síncrona es controlable completamente mediante aplicaciones de *software*. Los sistemas de administración de red no solo desempeñan funciones de administración tales como el control de alarmas en la red, sino que proporcionan otras funciones como un monitoreo en el desempeño de esta. Permite la administración de configuraciones, de recursos, de seguridad de red, del inventario de equipo, y ofrece herramientas para la planeación y diseño de la red misma. La posibilidad de un abastecimiento remoto y de un mantenimiento centralizado, trae como beneficios grandes ahorros en tiempos de atención a fallas y de inversión.

Ancho de banda por demanda.- En una red síncrona es posible designar dinámicamente la capacidad de red, o ancho de banda, de acuerdo a la demanda. Los usuarios de la red son capaces de solicitar de una manera mas ágil cualquier servicio ofrecido, inclusive aquellos que demanden grandes anchos de banda. Un ejemplo de esto es el caso de "servicio de videoconferencia por marcado".

Soporte de servicios futuros.- La jerarquía digital síncrona permite a los operadores de red contar con una solución para los servicios futuros, mediante la capacidad de actualizar y complementar el *software* existente en cada equipo. Los estándares de SDH también facilitan la interoperabilidad entre los sistemas de transmisión europeos y estadounidenses, ventaja que no es fácil de alcanzar con los sistemas PDH.

3. Protocolos de la capa de red

El presente capítulo trata de explica los conceptos fundamentales en los que se basan los protocolos de enrutamiento. Los temas aquí desarrollados se organizan de acuerdo a los componentes que forman un protocolo de enrutamiento y los algoritmos empleados. Posteriormente se particulariza en la descripción de dos grupos de protocolos: TCP/IP y el grupo de protocolos de ISO, ya que en estos se fundamenta el funcionamiento de nuestra propuesta de diseño.

3.1. Fundamentos de los protocolos de enrutamiento

3.1.1. Concepto de enrutamiento

La función de enrutamiento es la acción de mover datos provenientes de una fuente hacia un destino a lo largo de una red formada por dispositivos llamados enrutadores.

Esta función de enrutamiento es llevada a cabo en la capa 3 del modelo de referencia OSI, empleando direcciones lógicas, que son conservadas a lo largo de toda la trayectoria hasta su destino final.

El tema del enrutamiento ha sido cubierto en la literatura de computación por más de tres décadas, sin embargo este alcanzó gran fuerza a mediados de los años 80s, debido a que anteriormente las redes eran sencillas, de ambientes homogéneos y de cobertura limitada, permitiendo así la comunicación y descubrimiento de los dispositivos a través de técnicas sencillas. Actualmente el enrutamiento toma una importancia fundamental debido al tamaño, cobertura e interacción que se tienen en las redes a escala mundial, con lo cual se requiere de técnicas mas complejas para lograr de manera eficaz la comunicación y descubrimiento entre dispositivos de red.

3.1.2. Componentes de la función de enrutamiento

El enrutamiento esta compuesto de dos actividades básicas:

- Determinación del camino.
- Conmutación o *switching.*

A continuación se explica cada una de estas actividades:

Determinación del camino

Para la evaluación del mejor camino usado en el envío de paquetes, los protocolos de enrutamiento usan diferentes tipos de variables que se encuentran en la red y son llamadas métricas. Estas métricas son estándares de medición, tal como el ancho de banda que se tiene en el camino, y varían en su uso dependiendo del algoritmo de enrutamiento empleado. Durante el proceso de determinar el mejor camino, estos algoritmos crean y mantienen tablas de rutas que contienen los valores de las métricas usadas.

Dentro de las tablas de rutas o de enrutamiento, los algoritmos empleados se encargan de llenarlas con una variedad de información, como asociaciones de direcciones de destino con el "siguiente salto", con las que el enrutador determina que un destino en particular puede ser alcanzado de manera óptima al enviar el paquete a un enrutador determinado y representado como el "siguiente salto".

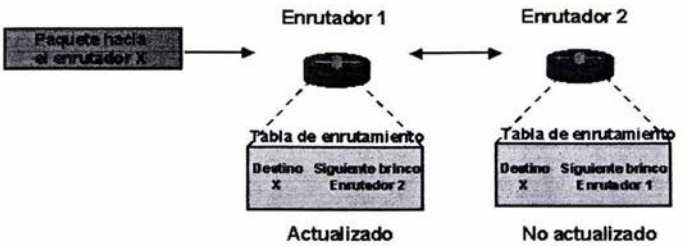

Figura 3.1 Tabla de enrutamiento.

El mantenimiento o actualización de las tablas de enrutamiento se realiza mediante el envío de una variedad de mensajes entre los enrutadores directamente conectados. Estos mensajes de actualización pueden llevar toda, o una parte de la tabla de enrutamiento utilizada. Dentro de cada enrutador estos mensajes de actualización se analizan para construir una topología detallada de la red.

Como parte de los mensajes de actualización existen en particular algunos llamados "anuncios de estado de enlace", los cuales informan de la situación de los enlaces del enrutador que los genera. Esta información de los enlaces también puede ser empleada para construir una imagen completa de la topología de la red, permitiendo a los enrutadores determinar las rutas óptimas a los destinos de la red.

Más adelante se presentarán los tipos de métricas generalmente usados por los diferentes protocolos de enrutamiento.

Conmutación o *Switching*

Los algoritmos empleados para la parte de conmutación son relativamente sencillos y son similares para todos los protocolos de enrutamiento. En la mayoría de los casos el proceso de conmutación se establece cuando un *host* origen determina que debe enviar un paquete a otro *host* de destino. Con el uso de un protocolo en particular para obtener la dirección del enrutador en el cual está directamente conectado, el *host* origen dirige el paquete específicamente a una dirección física o MAC del enrutador, y al mismo tiempo con la dirección de capa de red del *host* de destino. Una vez que el enrutador tiene el paquete a enviar, este examina la dirección de red de destino y determina si sabe como enviarlo. Si procede el envío del paquete, este cambia la dirección física de destino por la del siguiente brinco y transmite el paquete.

El siguiente brinco puede ser el *host* de destino, pero puede ser otro enrutador intermedio el cual ejecuta el mismo proceso de conmutación. Mientras el paquete viaja por la red, la dirección física cambiará, sin embargo la dirección de red permanecerá constante.

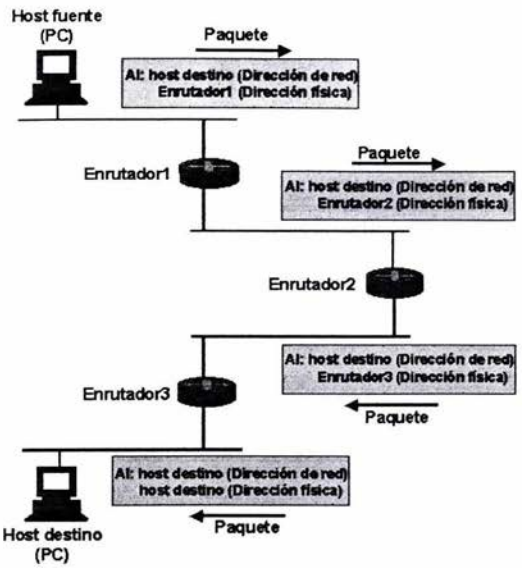

Figura 3.2 Conmutación de un paquete.

3.1.3. Algoritmos de enrutamiento

Estos pueden ser distinguidos con base en ciertas características clave, como son:

- **Los objetivos particulares en el diseño de cada algoritmo**, ya que afectan a la función del protocolo de enrutamiento.
- **Tipos de algoritmos de enrutamiento**, cada uno de estos tiene un impacto diferente en los recursos de la red y de los enrutadores.
- **Métricas**, que son las que afectan directamente el cálculo de las rutas óptimas.

A continuación se analizan estas características de los algoritmos de enrutamiento:

Objetivos de diseño

Los objetivos de diseño para los algoritmos de enrutamiento generalmente usados, se describen brevemente a continuación:

Funcionamiento óptimo. Se refiere a la capacidad del algoritmo de enrutamiento para seleccionar la mejor ruta, la cual depende de los tipos de métricas y del valor que estas tengan. Un ejemplo es cuando un algoritmo de enrutamiento emplea el número de saltos y tiempos de demora (*delay*) como métricas, teniendo el tiempo de demora con un valor más importante en el cálculo.

Sencillez y bajo consumo de recursos. Los algoritmos de enrutamiento deben ser lo mas sencillos posibles, en otras palabras, el algoritmo de enrutamiento debe ofrecer un funcionamiento eficiente, con un mínimo de programación y de utilización de recursos, como procesamiento y memoria.

Robustez y estabilidad. Deben funcionar correctamente en circunstancias imprevistas o poco usuales, como fallas físicas, condiciones de alta demanda e implementaciones incorrectas en la operación. Debido a que los enrutadores están interconectados entre sí, pueden originarse serios problemas si el algoritmo falla. Los mejores algoritmos de enrutamiento son aquellos que pueden soportar pruebas en tiempo y que han probado ser estables bajo una gran variedad de condiciones en la red.

Convergencia rápida. La convergencia es el proceso de concordancia entre todos los enrutadores respecto a la información de las rutas óptimas. Cuando un evento de red origina que las rutas sean creadas o deshabilitadas, los enrutadores distribuyen mensajes de actualización de enrutamiento por toda la red, desencadenando un nuevo cálculo de rutas óptimas y consecuentemente poniendo de acuerdo a todos los enrutadores con estos cambios. Los protocolos de enrutamiento que convergen lentamente pueden causar *loops* de enrutamiento o recesos en la red.

Un *loop* de enrutamiento es un evento que se presenta cuando los paquetes de actualización se mantienen viajando en una trayectoria cerrada. Con base en el ejemplo de la figura 3.3, un paquete de actualización llega al enrutador_1 en el tiempo t1. El enrutador_1 ya ha estado actualizando su información y por lo tanto conoce que la ruta óptima hacia el destino es por el enrutador_2, es decir, su siguiente salto. El enrutador_1 por consiguiente envía la información hacia el enrutador_2, pero debido a que no ha sido actualizado todavía, este cree que el siguiente salto óptimo es el enrutador_1. El enrutador_2 por consiguiente enviará el paquete de regreso al enrutador_1 y el paquete continuará yendo y viniendo entre estos dos enrutadores hasta que el enrutador_2 reciba su actualización de enrutamiento, o hasta que el paquete sea desechado al alcanzar el número de brincos permitidos.

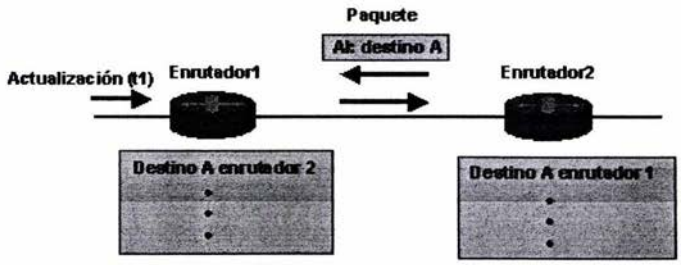

Figura 3.3 *Loop* de enrutamiento.

Flexibilidad. Se refiere a que los algoritmos deben adaptarse rápida y fielmente a una variedad de circunstancias en la red. Un ejemplo sucede cuando un segmento de la red se encuentra fuera de servicio. Debido a esta situación, se pueden dar cuenta del problema diferentes algoritmos de enrutamiento, con lo que estos rápidamente seleccionarán el segundo camino óptimo para todas las rutas que normalmente usan el segmento que está en "falla".

Los algoritmos de enrutamiento pueden adecuarse para adaptarse a cambios en el ancho de banda de la red, en el tamaño de las colas de enrutamiento y en los tiempos de retardo de la red, entre otras variables.

Tipos de algoritmos

Los diferentes algoritmos de enrutamiento pueden ser clasificados de acuerdo a los siguientes tipos:

Estáticos o dinámicos. Los algoritmos de enrutamiento estáticos no son estrictamente algoritmos, sino tablas de asociación establecidas por el administrador de la red antes de comenzar la función de enrutamiento. Estas asociaciones de rutas no son cambiadas a menos que el administrador de red lo haga. Los algoritmos que utilizan enrutamiento estático son sencillos en su diseño y trabajan bien en ambientes donde el tráfico de red es relativamente predecible y donde el diseño de la red es sencillo.

Debido a que los sistemas de enrutamiento estático no reaccionan a los cambios en la red, son considerados generalmente inadecuados para las actuales redes que tienen grandes coberturas y cambios constantes. Los algoritmos de enrutamiento que más dominan son aquellos de tipo dinámico, los cuales realizan ajustes en reacción a los cambios que surjan en la red mediante el análisis de los mensajes de actualización de enrutamiento que se tengan.

Si el mensaje indica que ha ocurrido un cambio en la red, el algoritmo de enrutamiento calcula nuevamente las rutas y envía nuevos mensajes de actualización. Estos mensajes se presentarán en toda la red, originando que todos los enrutadores ejecuten sus algoritmos para actualizar sus tablas de enrutamiento de acuerdo a los cambios ocurridos.

No obstante, los algoritmos de enrutamiento dinámico pueden ser complementados con rutas estáticas donde sea apropiado, y entonces tener un esquema de enrutamiento de tipo híbrido.

Unitrayectoria o multitrayectorias. Algunos protocolos de enrutamiento sofisticados soportan múltiples trayectorias al mismo destino. A diferencia de aquellos de una sola trayectoria, los de múltiples trayectorias permiten multiplexación del tráfico sobre las líneas de transmisión paralelas o con igual métrica que se tengan. Las ventajas de los algoritmos mulitrayectorias son claras, ya que estos pueden proporcionar un mejor desempeño y son más confiables. El proceso de multiplexación de tráfico sobre diferentes líneas es conocido como "balanceo de carga".

Planos o jerárquicos. En los sistemas de enrutamiento planos, todos los enrutadores son iguales en función e importancia dentro de la red.

En un sistema de enrutamiento jerárquico, los enrutadores tienen diferentes funciones dependiendo del nivel de enrutamiento que estos tengan. Estos sistemas de enrutamiento a menudo designan grupos lógicos de nodos llamados dominios, sistemas autónomos o áreas. En los sistemas de enrutamiento jerárquicos, existen dos tipos de comunicación: ínter-dominios, donde ciertos enrutadores de un dominio pueden comunicarse con enrutadores de otros dominios; o bien intra-dominio, donde los enrutadores pertenecientes a un mismo dominio pueden comunicarse entre si.

Debido a que los enrutadores intra-domino solo necesitan saber de otros dentro del mismo dominio, sus algoritmos de enrutamiento son sencillos y como consecuencia el tráfico de actualización de enrutamiento es reducido.

La principal ventaja del enrutamiento jerárquico es que este generalmente empata con la organización de las compañías y por consiguiente soporta los patrones de tráfico de manera óptima. La mayoría de las redes de comunicaciones provienen de pequeñas compañías (dominios). En redes muy grandes este tipo de esquemas de enrutamiento es aconsejable.

Inteligencia de *host* e inteligencia de enrutador. Algunos algoritmos de enrutamiento asumen que los *hosts* extremos determinarán toda la ruta y se refieren usualmente como enrutamiento de fuente. En los sistemas de enrutamiento de fuente, los enrutadores simplemente actúan como dispositivos de reenvío al siguiente salto, sin medidas de cuidado alguno para el paquete. Otros algoritmos asumen que el *host* extremo no sabe de la ruta. En estos algoritmos, los enrutadores determinan el camino por toda la red basándose en sus propios cálculos. En resumen, para el primer algoritmo, los *hosts* tiene la inteligencia de enrutamiento, mientras que en el segundo son los enrutadores los que la tienen.

Intra-dominio e Inter-dominio. Algunos algoritmos de enrutamiento trabajan únicamente dentro de dominios y otros trabajan al mismo tiempo dentro y entre dominios. Debido a que la naturaleza de estos tipos de algoritmos es diferente, el enrutamiento intra-dominio no necesariamente debe ser un enrutamiento inter-domino óptimo.

Estado de enlace y Vector distancia. Los algoritmos de estado de enlace, también conocidos como algoritmos SPF (*Shortest Path First*) hacen que fluya la información de enrutamiento a todos los nodos de la red. Cada enrutador, sin embargo, solo envía la parte de la tabla de enrutamiento que describe el estado de sus propios enlaces. En los algoritmos de estado de enlace, cada enrutador calcula y construye una imagen de toda la red en su tabla de enrutamiento con base en las partes de la tabla de enrutamiento de cada enrutador.

Los algoritmos de "vector distancia", también conocidos como algoritmos Bellman-Ford permiten que el enrutador contacte a todos sus enrutadores vecinos para enviar una parte o toda su tabla de enrutamiento, pero únicamente a ellos. La información contenida en la tabla de enrutamiento está formada básicamente de los parámetros de vector y de distancia. El vector es el número de red y la distancia es el costo que se tiene para alcanzar a ese mismo número de red. Dado que la difusión de esta información es local, los enrutadores dependen de sus vecinos para el cálculo correcto de la distancia.

Debido a que la convergencia es más rápida en los algoritmos de estado de enlace, estos son menos propensos a *loops* de enrutamiento en comparación con los algoritmos de "vector distancia". Sin embargo los algoritmos de "estado de enlace" requieren mayor procesamiento y memoria, que los algoritmos de "vector distancia". Los algoritmos de "estado de enlace" por consiguiente, pueden ser más costosos para implementar y soportarse, sin embargo generalmente son más escalables que los de "vector distancia".

Métricas de enrutamiento

Dentro de las tablas de enrutamiento se tiene información que es utilizada por los algoritmos de enrutamiento para seleccionar la mejor ruta. Esta información es denominada como "métricas". Existen algoritmos sofisticados de enrutamiento que pueden basar su selección de rutas óptimas con múltiples métricas y combinándolas para obtener una sola. Las métricas que a continuación se describen son las que comúnmente se utilizan:

Longitud de la trayectoria. Es la métrica de enrutamiento más utilizada. Algunos protocolos de enrutamiento permiten que los administradores de la red asignen costos o valores arbitrarios a cada enlace. En este caso, la longitud de la trayectoria es la suma de los costos asociados a cada enlace recorrido. Otros protocolos de enrutamiento usan el conteo de brincos, que es una métrica que especifica el paso a través de los dispositivos de red, como enrutadores.

Confiabilidad. Se refiere a la disponibilidad y seguridad de cada enlace de red, usualmente descrita en términos de tasa de error de bit. La confiabilidad es palpable en los enlaces que pueden estar fuera de servicio más a menudo que otros, en la facilidad y rapidez de reparación. Cualquier factor de confiabilidad puede ser tomado en cuenta para la asignación de la tasa de confiabilidad, estos factores son valores numéricos arbitrarios asignados usualmente a los enlaces por los administradores de red.

Tiempo de retardo en el enrutamiento. Se refiere a la cantidad de tiempo requerido para mover un paquete de una fuente hacia un destino a través de la red. El retardo depende de muchos factores, como el ancho de banda de los enlaces de red intermedios, las colas en los puertos de cada enrutador (*buffers*) a lo largo del camino, congestiones en la red de los enlaces intermedios, y la distancia física que debe recorrerse. Debido a que el retardo es un conjunto de variables, es una métrica común y muy utilizada.

Ancho de banda. Se refiere a la capacidad de tráfico disponible en un enlace de red. Por ejemplo, es preferible un enlace *ethernet* de 10 Mbps a una línea dedicada de 64 kbps. A pesar de que el ancho de banda es un valor del máximo desempeño disponible de un enlace, las rutas a través de enlaces con un ancho de banda mayor no necesariamente son las rutas más óptimas. Por ejemplo, si un enlace rápido es muy concurrido, el tiempo requerido para enviar un paquete hacia el destino, podría ser mayor que si se utiliza una ruta de menor capacidad pero que no esta ocupada.

Carga. Se refiere al grado en el cual los recursos de un dispositivo de red, como un enrutador, están ocupados. La carga puede ser calculada en una variedad de formas, incluyendo utilización de CPU, uso de enlaces, y paquetes procesados por segundo. El monitoreo de estos parámetros en una base continua puede consumir recursos de si mismo.

3.2. Protocolos de Internet, IP

Los protocolos de Internet constituyen el grupo de protocolos de sistema abierto o no propietario más popular del mundo, debido a que es empleado para comunicar *hosts* a través de cualquier grupo de redes interconectadas, y está bien adaptado para las comunicaciones en redes tipo WAN y LAN. Dentro de este grupo de protocolos de comunicación, los más conocidos son el protocolo de control de transmisión TCP y el protocolo de Internet IP. Así mismo dentro de este grupo no solo se abarcan los protocolos de las capas más bajas (TCP e IP), sino que también se incluyen aplicaciones comunes, tales como el correo electrónico, la simulación de terminal y la transferencia de archivos.

Los protocolos de Internet fueron desarrollados a mediados de la década de los años 70s cuando la "Agencia de Proyectos de Investigación Avanzada de la Defensa de los EE.UU." (DARPA, por sus siglas en inglés) se interesó en establecer una red de paquetes conmutados que facilitara la comunicación entre diferentes sistemas de computación de instituciones de investigación. Con el objetivo de contar con una conectividad heterogénea, DARPA financió investigaciones en la universidad de Stanford, resultando de este desarrollo a finales de la misma década, el grupo de protocolos de IP.

La figura 3.4 muestra los grupos de protocolos de IP y su posición dentro del modelo de referencia OSI:

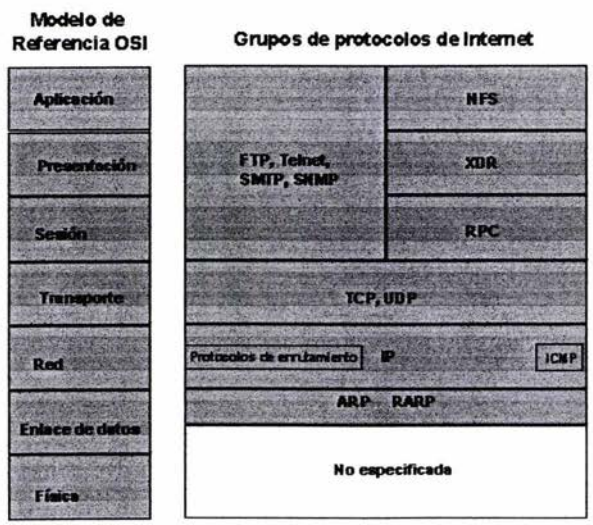

Figura 3.4 TCP/IP en el modelo de referencia OSI.

La presente sección de este trabajo describe de manera general los protocolos y aplicaciones que de este grupo que son empleados por la aplicación de gestión y por la propuesta de diseño.

3.2.1. Protocolo de Internet, IP

El protocolo de Internet o IP, es un protocolo de capa 3 que contiene información de direccionamiento y cierta información de control que permite enrutar a los paquetes. IP está documentado en el RFC 791 y es el principal protocolo de red en su grupo teniendo dos funciones principales:

- Realiza la entrega de paquetes no orientados a conexión mediante el mejor esfuerzo, es decir, no se establece un circuito de comunicación para el transporte de los datos, sino que la información necesaria para su entrega es concentrada dentro de un encabezado sin garantizar que esta llegue de manera integra y ordenada, la responsabilidad de lo anterior se deja a la capa de transporte.
- Permite una fragmentación y reensamblaje de los paquetes para soportar enlaces de datos con diferentes tamaños de "unidades de transmisión máxima" o MTU.

En la siguiente sección se describirá cada parte que conforma un paquete de IP.

3.2.2. Formato del paquete de IP

Un paquete de IP está formado de ciertos campos de información que tiene diferentes funciones. Estos campos se ilustran en la siguiente figura:

Figura 3.5 Paquete de IP.

La función de cada uno de estos campos se presenta a continuación:

- **Versión**. Indica la versión de IP actualmente empleada.
- **Longitud del encabezado IP**. *IHL*- Indica la longitud del encabezado del datagrama.
- **Tipo de servicio**. Especifica la prioridad en la que pueden ser tratados los datagramas.
- **Longitud total**. Especifica la longitud en *bytes* del paquete entero de IP, incluidos los datos y el encabezado.
- **Identificación**. Contiene un entero que identifica a cada datagrama. Este campo es empleado para poder identificar los fragmentos que forman un datagrama, cuando este es segmentado.

- **Banderas**. Consiste de un campo de 3 bits, donde los dos de más bajo orden controlan la fragmentación. El bit de más bajo orden especifica si el paquete puede ser fragmentado, y el bit medio especifica si es el último fragmento de una serie de paquetes. El bit de mayor orden no es utilizado.
- ***Offset* del fragmento**. Indica la posición de los datos del fragmento con relación al comienzo de los datos del datagrama original. De esta forma es posible la reconstrucción del datagrama original en el *host* de destino.
- **Tiempo de vida**. Cada paquete conserva un contador que gradualmente es decrementado hasta cero, con la finalidad de que sea descartado. Este contador corrige el fenómeno de *loops*.
- **Protocolo**. Indica que protocolo de capas superiores recibe el paquete después de que el procesamiento en IP es completado.
- **Detección de errores en el encabezado**. Ayuda a verificar la integridad del encabezado de IP.
- **Dirección fuente**. Especifica el nodo que envía la información.
- **Dirección de destino**. Especifica al nodo que la recibe.
- **Opciones**. Permite a IP soportar varias opciones, como seguridad y determinación de trayectorias.
- **Datos**. Contiene la información de las capas superiores.

3.2.3. Direccionamiento IP

Cada *host* en una red TCP/IP está asociado a una dirección lógica de 32 bits que consta de dos partes fundamentales:

- **Número de red**. Identifica al grupo que pertenece el *host* y es asignado por el Centro de información de la red de Internet, InterNIC, si la red va a formar parte de Internet. Un proveedor de servicio de Internet (ISP) puede obtener bloques de direcciones de red del IterNIC y el mismo puede asignar espacios de direcciones de ser necesario.
- **Número de *host***. Identifica a un *host* dentro de la red y es asignado por el administrador de la red local.

Formato de una dirección IP

La dirección IP de 32 bits se divide bajo 4 partes de 8 bits, cada una separada por puntos y representada en formato decimal. Los bits en cada octeto tienen un peso binario específico (128, 64, 32, 16, 8, 4, 2, 1), generando valores que van desde 0 y hasta 255 por octeto. La siguiente figura 3.6 muestra el formato básico de una dirección IP:

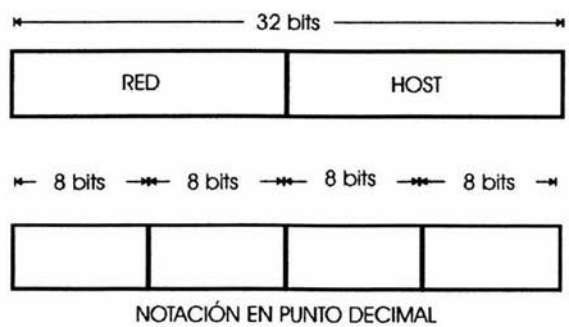

Figura 3.6 formato de una dirección IP.

Clases de direcciones IP

El direccionamiento IP soporta cinco diferentes clases de direcciones: A, B, C, D y E. Únicamente las clases A, B y C están disponibles para uso comercial. La figura 3.7 muestra estos tres tipos de clases:

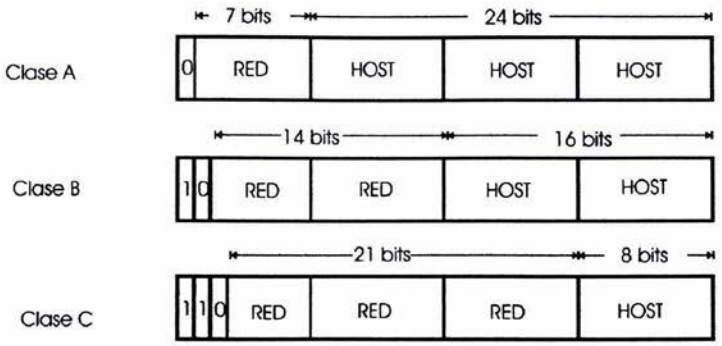

Figura 3.7 Clases de direcciones IP.

Los bits de la extrema izquierda (De alto orden) indican la clase de red. La tabla 3.1 proporciona la información de referencia con relación a las cinco clases.

Clase de Dirección	Formato	Propósito	Bits de alto orden	Rango de direcciones	No. De bits Red/hosts	No. Máximo de hosts
A	N.H.H.H	Organizaciones Grandes	0	1.0.0.0 a 126.0.0.0	8/24	2^{24}-2
B	N.N.H.H	Organizaciones medianas	1,0	128.1.0.0 a 191.254.0.0	16/16	2^{16}-2
C	N.N.N.H	Organizaciones pequeñas	1,1,0	192.0.1.0 a 223.255.254.0	24/8	2^{8}-2
D	-	Grupos de Múlticast	1,1,1,0	224.0.0.0 a 239.255.255.255	-	-
E	-	Uso Experimental	1,1,1,1	240.0.0.0 a 254.255.255.255	-	-

Tabla 3.1 Información de las clases de direcciones IP.

Las clases de direcciones pueden ser determinadas fácilmente si se examina el primer octeto de direcciones y se asocia este valor al rango de clases de la tabla 3.1.

Direccionamiento de subredes IP

Las clases de redes IP pueden ser divididas en redes más pequeñas llamadas subredes. Esta creación de subredes proporciona al administrador de red ciertos beneficios, como lo son una flexibilidad extra en la asignación, un uso mas eficiente de las direcciones de red y la capacidad de incluir tráfico de *broadcast* (El flujo de información de *broadcast* no es permitido por los enrutadores, por omisión).

Una ventaja adicional es que al emplear el concepto de subredes estas se asignan bajo una administración local, con lo que el resto del mundo conoce a la organización que las utiliza como una sola red y no se tiene detalle de su estructura interna.

Una dirección de red dada, puede ser fragmentada en muchas subredes. Por ejemplo: 172.16.1.0, 172.16.2.0, 172.16.3.0 y 172.16.4.0 son subredes dentro de la red 172.16.0.0.

Máscara de subred IP

Para la creación de una dirección de subred se necesita tomar prestados bits del campo asignado para el número de *hosts* y designarlos al campo de la subred. Para identificar cuales bits pertenecen al campo de subred y cuales al número de host, se utiliza la máscara de red. La figura 3.8 muestra un ejemplo de máscara de red y de como los bits son tomados del campo de número de host para crear el campo de dirección de subred a partir de una clase B.

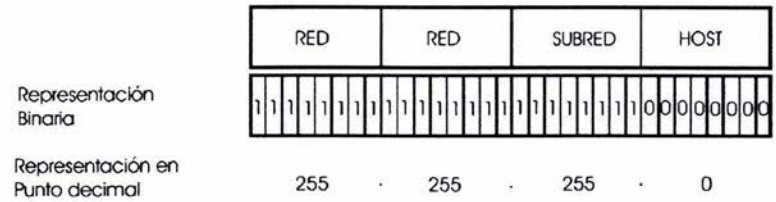

Figura 3.8 Máscara de subred IP.

Las máscaras de subred emplean el mismo formato y técnica de representación de las direcciones IP, sin embargo, solo están compuestas por unos binarios con los que se especifican los campos de red y de subred, y a su vez los ceros binarios especifican el campo de *host*.

El funcionamiento de las mascaras de subred en los enrutadores es mediante el desempeño de varios procesos para determinar la dirección de red, o subred. Inicialmente el enrutador extrae la dirección IP de destino del paquete entrante y toma la mascara de subred de la tabla de enrutamiento. De esta forma se ejecuta una operación lógica AND para obtener el número de red. Esto origina que la parte de *host* de la dirección destino sea removida, mientras que el número de dirección de red de destino permanece. De esta forma el enrutador busca el número de dirección de destino y lo asocia con una interfaz de salida. Finalmente este reenvía la trama hacia el dispositivo de red, o al destino final.

3.2.4 Enrutamiento en IP

Los enrutadores que conforman Internet están organizados de manera jerárquica. Los enrutadores que son usados para el intercambio de información dentro de sistemas autónomos son llamados enrutadores internos, los cuales para cumplir este propósito emplean una variedad de protocolos de "*gateway* internos" o IGPs. RIP es un ejemplo de un IGP.

También existen enrutadores que mueven información entre diferentes sistemas autónomos y son llamados enrutadores externos. Estos enrutadores emplean un protocolo de "*gateway* externo" para intercambiar información entre diferentes sistemas autónomos. BGP es un ejemplo de un protocolo de "*Gateway* externo".

Los protocolos de enrutamiento por definición, son dinámicos, logrando que las rutas sean calculadas automáticamente en periodos regulares dentro de dispositivos de enrutamiento. Lo anterior es contrario al enrutamiento estático, donde las rutas son establecidas por el administrador de red y no cambian hasta que el administrador de red así lo requiera.

Una tabla de enrutamiento de IP, consiste básicamente de dos valores: dirección destino y siguiente brinco, y es empleada para desempeñar el enrutamiento dinámico.

El enrutamiento de IP especifica que los paquetes de IP viajan por la red mediante brincos por la trayectoria. La ruta entera no es conocida desde el comienzo del viaje, por lo que en cada parada, el destino es calculado comparando la dirección dentro del paquete con un valor de entrada en la tabla de enrutamiento del nodo.

Las clasificaciones y características de los protocolos de enrutamiento, se tratan en la sección de Protocolos de enrutamiento del presente documento.

3.2.5. Protocolo de control de mensajes de Internet ICMP

Es un protocolo de la capa de red que genera mensajes para reportar errores e información relativa al procesamiento de los paquetes de Internet y está documentado en el RFC 792. Estos mensajes son variados y si no pueden ser entregados, no se generará un segundo, evitando un flujo infinito de mensajes de ICMP.

Los mensajes que ICMP emplea, se explican a continuación:

Destino inalcanzable - Cuando un mensaje de destino inalcanzable es enviado por un enrutador, este quiere decir que el enrutador es incapaz de enviar el paquete original a su destino final. Para que un destino sea inalcanzable existen dos razones: que el *host* fuente haya especificado una dirección no existente, o que el enrutador no tenga la ruta hacia el destino.

Los mensajes de destino inalcanzable incluyen cuatro tipos básicos:

- Red inalcanzable, generalmente indica que ha ocurrido una falla en el enrutamiento o direccionamiento de un paquete.
- *Host* inalcanzable, indica una falla en la entrega, generalmente debido a una máscara de subred errónea.
- Protocolo inalcanzable, indica que el destino no soporta protocolos de capas superiores a la de red y que se especifica en el paquete.
- Puerto inalcanzable, implica que el *socket* o puerto de TCP no está disponible.

Solicitud y respuesta de Eco - Es generado por el comando *ping* desde cualquier *host* para verificar conectividad hacia el nodo en cuestión a través de la red. El mensaje de respuesta de eco de ICMP indica que el nodo puede ser exitosamente alcanzado.

Redirección de ICMP - Es enviado por el enrutador al *host* fuente para estimular un enrutamiento más eficiente. El mensaje de redirección de ICMP permite que las tablas de enrutamiento del host permanezcan pequeñas debido a que solo es necesario conocer la dirección de un enrutador aún cuando este no proporcione el mejor camino. Incluso después de recibir un mensaje de redirección de ICMP algunos dispositivos deben continuar usando la ruta menos eficiente.

Tiempo excedido de ICMP - Es enviado por el enrutador si el campo de tiempo de vida de un paquete de IP (expresado en brincos o segundos) llega a cero. El campo de tiempo de vida previene a los paquetes de circular continuamente en la red, cuando se tienen *loops* de enrutamiento. Con esto, el enrutador descarta el paquete original.

3.2.6. Protocolo de control de transmisión, TCP

TCP proporciona una transmisión confiable de datos en un ambiente IP y corresponde a la capa de transporte del modelo de referencia OSI. Entre los servicios que TCP proporciona están la transferencia de datos, confiabilidad, un control de flujo eficiente, operación del tipo *full-duplex* y multiplexaje.

Con el flujo de la transferencia de datos, TCP entrega un flujo no estructurado de paquetes identificados por una secuencia de números. Este servicio beneficia a las aplicaciones debido a que estos no tienen que segmentar los datos en bloques antes de manejarlos en TCP. En lugar de eso TCP segmenta a los paquetes y los entrega a IP para su envío.

TCP ofrece confiabilidad proporcionando un servicio orientado a conexión y una entrega de paquetes de extremo a extremo a través de la red. Esto se logra dando una secuencia a los paquetes con un reenvío de números de acuse, que indica lo que espera recibir la fuente del destino con el siguiente paquete. El mecanismo de confiabilidad de TCP permite a los dispositivos trabajar con paquetes perdidos, retrasados, duplicados o mal interpretados. El mecanismo de "tiempo muerto" o *time-out,* permite a los dispositivos detectar perdida de paquetes y generar así la solicitud de retransmisiones.

TCP ofrece un control de flujo eficiente, es decir, cuando se envían de regreso los paquetes de acuse a la fuente, el proceso TCP de recepción indica que el número de secuencia más alto puede ser recibido sin saturar los *buffers* de memoria interna. La operación *full-duplex* indica que los procesos de TCP pueden enviar y recibir al mismo tiempo.

Finalmente el multiplexaje de TCP indica que varias conversaciones simultáneas de capas superiores pueden ser multiplexadas sobre una sola conexión TCP.

Formato del paquete de TCP

La figura 3.9 ilustra los campos y el formato general de un paquete de TCP:

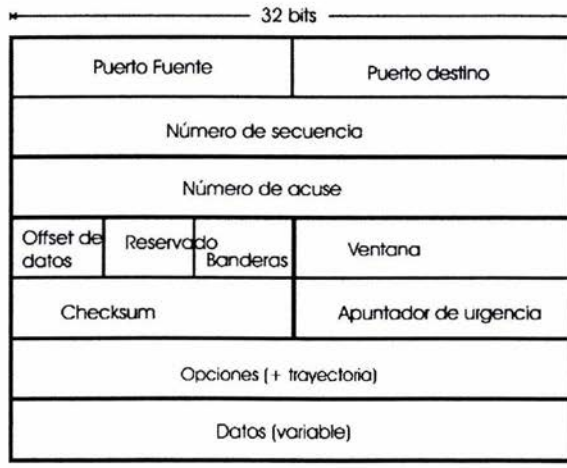

Figura 3.9 Formato del paquete TCP.

A continuación se describe cada campo:

- **Puerto fuente y Puerto de destino-** Estos identifican el tipo de proceso ubicado en las capas superiores del modelo de referencia OSI al cual se necesita acceder.

- **Número de secuencia-** Usualmente especifica el número asignado al primer *byte* de datos del actual mensaje. En la fase de establecimiento de conexión, este campo también puede ser usado para identificar un número de secuencia inicial, para ser usado en una transmisión entrante.
- **Número de acuse-** contiene el número de secuencia del siguiente *byte* de datos, que espera recibir el que envía los paquetes.
- **Compensación de datos-** Indica el número de palabras de 32 bits en el encabezado de TCP
- **Reservado-** Para usos futuros.
- **Banderas-** Transporta una variedad de información de control, incluyendo los bits SYN y ACK utilizados para el establecimiento de conexión, y el bit FIN empleado para la terminación de la conexión.
- **Ventana-** Especifica el tamaño de la ventana de recepción del emisor. (Es decir el espacio disponible en el *buffer* para los datos entrantes).
- ***Checksum-*** Indica si el encabezado fue dañado durante el trayecto.
- **Apuntador de urgencias-** Apunta al primer *byte* de datos urgentes en el paquete
- **Opciones-** Especifica varias opciones de TCP.
- **Datos-** Contiene la información de capas superiores.

3.2.7 Protocolo de Datagramas de Usuario UDP

Es un protocolo de capa de transporte no orientado a conexión que pertenece a la familia de los protocolos de Internet. UDP es básicamente una interfaz entre IP y los procesos de capas superiores. Los puertos del protocolo UDP, diferencian a múltiples aplicaciones que corren en un solo dispositivo.

A diferencia de TCP, UDP no tiene funciones de confiabilidad, control de flujo ni de recuperación de errores para IP. Debido a la simplicidad de UDP, sus encabezados contienen menor número de *bytes* logrando un uso más eficiente del ancho de banda en la red. UDP es útil en situaciones donde los mecanismos de confiabilidad de TCP no son necesarios, como lo son los casos donde los protocolos de capas superiores pueden proporcionar controles de error y de flujo.

UDP es el protocolo de transporte de algunas aplicaciones de protocolos de capas superiores, incluyendo el "Sistema de Archivos de Red" NFS, "Protocolo Único de Administración de Red" SNMP, "Sistema de Dominios de Nombres" DNS y el "Protocolo de Transferencia Trivial de Archivos" TFTP.

El formato del paquete de UDP contiene cuatro campos: puertos fuente y destino, longitud y campos de detección de errores, estos se muestran en la figura 3.10:

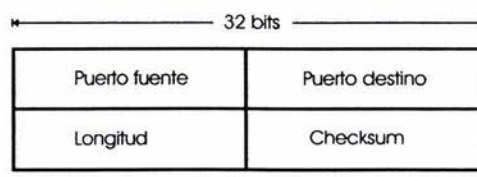

Figura 3.10 Formato del paquete UDP.

Los puertos fuente y de destino contienen los números de puertos de 16 bits usados para identificar a los datagramas recibidos de los procesos de la capa de aplicación. El campo de longitud, especifica la longitud del encabezado de UDP y de los datos. *Checksum* permite revisar la integridad del encabezado y de los datos (opcional).

3.2.8. Protocolos de la capa de aplicación

El grupo de protocolos de Internet incluyen varios protocolos en la capa de aplicación como son los siguientes:

- **Protocolo de Transferencia de Archivos FTP**- Permite mover datos entre dispositivos.
- **Protocolo sencillo de Administración de redes SNMP**- Reporta principalmente condiciones anómalas y valores de umbral de la red.
- **Telnet**- Funciona como un protocolo que simula ser una terminal remota.
- **X Windows**- Funciona como una ventana distribuida, con sistema de gráficos usado para la comunicación entre terminales X y estaciones de trabajo UNÍS.
- **Sistema de Archivos de Red NFS**- Representación externa de datos XDR.
- **Procedimiento remoto RPC**- trabajan juntos para permitir un acceso transparente a los recursos de red remotos.
- **Protocolo sencillo de transferencia de correo SMTP**- Proporciona servicios de correo electrónico.
- **Sistema de dominio de nombres DNS**- Traduce nombres de nodos de red a direcciones de red.

3.3. Grupo de Protocolos de Interconexión de Sistemas Abiertos OSI.

El grupo de protocolos de interconexión de sistemas abiertos OSI esta formado de numerosos estándares de protocolos los cuales están basados en el modelo de referencia OSI. Estos protocolos son parte de un programa internacional de desarrollo de protocolos de redes de datos y otros estándares, que facilitan la interoperabilidad de equipos de diferentes proveedores.

Las especificaciones de OSI fueron concebidas y desarrolladas por dos organizaciones de estándares internacionales, la Organización Internacional de Estandarización (ISO) y la Unión Internacional de Telecomunicaciones, en su Sector de estandarización de Telecomunicaciones. (ITU-T).

A continuación se explica brevemente el funcionamiento de cada protocolo, detallando en el funcionamiento de los protocolos de la capa 3, ya que en estos se fundamenta la propuesta de diseño del presente trabajo:

3.3.1. Protocolos de red con base en el modelo de referencia OSI

La figura 3.11 ilustra el grupo total de protocolos de OSI y su relación con el modelo de referencia OSI.

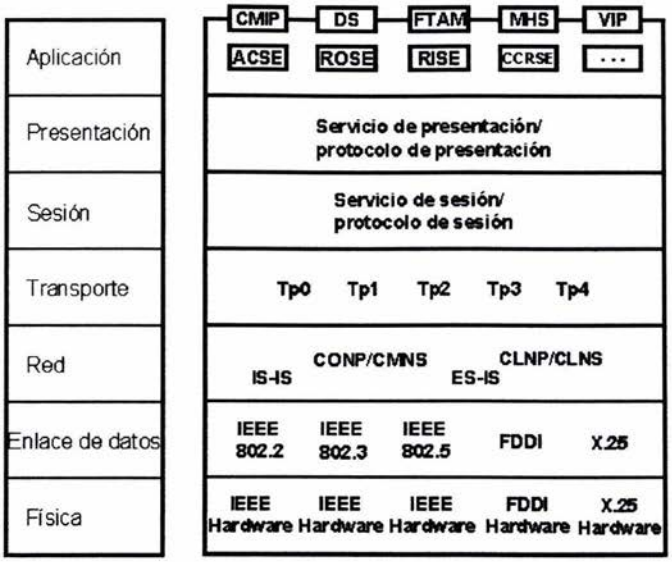

Figura 3.11 Grupo de protocolos de OSI, en relación al modelo de referencia OSI.

Capas física y de enlace de datos de OSI

El grupo de protocolos de OSI soporta numerosos estándares de protocolos de acceso. La gran variedad de estos protocolos soportados permite la convivencia en el mismo medio de otros grupos de protocolos diferentes al OSI. Los protocolos de acceso al medio soportados incluyen IEEE 802.3, *Token Ring*/802.5, *FDDI* y X.25

Capa de Red de OSI[10]

Dentro de esta capa, se especifican dos protocolos de enrutamiento en la capa de red: *End System to Intermediate System* (ES-IS) e *Intermediate System to Intermediate System* (IS-IS). Estos protocolos se tratarán con detalle mas adelante.

Adicionalmente, en esta capa de red, se implementan dos tipos de servicios de red: Servicio no orientado a conexión y el servicio orientado a conexión, los cuales se explican a continuación:

Servicio de red no orientado a conexión de OSI, CLNS.- CLNS (*ConnectionLess Network Service*) describe el servicio que se le ofrece a la capa de transporte, en la cual las solicitudes para la transferencia de datos son realizadas mediante una entrega no garantizada, es decir, el envío de datos podría perderse, dañarse, llegar en desorden, o duplicarse. Con lo anterior, el servicio no orientado a conexión asume que la capa de transporte corregirá, en cada caso, tales problemas.

[10] Debido a que los protocolos más empleados son IS-IS, ES-IS y CLNP, a la capa 3 de este grupo se le conoce comúnmente como CLNS. Por lo anterior en la presente tesis se considerará al nombre CLNS como denominador de la capa 3 de este grupo de protocolos.

Así mismo, CLNS no utiliza ningún tipo de información de conexión o de estado, ni se realiza proceso alguno para el establecimiento de conexiones debido a que los caminos tomados para el envío de la información son independientes, para cada paquete transmitido en la red.

Este servicio se apoya en el uso de CLNP (*ConnectionLess Network Protocol*), el cual es un protocolo no orientado a conexión que permite el transporte de datos e información de errores. Funcionalmente es muy parecido a IP y no cuenta con técnicas de detección y corrección de errores, por lo que se apoya de la capa de transporte para realizar tales funciones. CLNP solo tiene una actividad dentro de su proceso de transmisión, la cual es llamada "transferencia de datos". Debido a que el servicio de transferencia de datos es independiente de otras sesiones, resulta indispensable la información de enrutamiento para la distinción de las sesiones.

Los protocolos CLNP y CLNS son descritos en el estándar ISO 8473.

Servicio de red orientado a conexión de OSI, CMNS.- Este servicio de red en modo de conexión CMNS, es implementado mediante el uso del protocolo de red orientado a conexión CONP y está especificado en los estándares ISO 8208 e ISO 8878. Asimismo CONP está basado en el protocolo de nivel de paquete X.25, para el movimiento de datos e indicadores de error a través de enlaces orientados a conexión. El CMNS realiza funciones relacionadas con el establecimiento explícito de caminos entre entidades de comunicación de la capa de transporte. Estas funciones incluyen el establecimiento, terminación y mantenimiento de conexiones, también proporciona mecanismos de solicitud de calidad de servicio.

Los protocolos de la capa de transporte de OSI

Así como en la capa de red de OSI, se ofrecen los tipos de servicio de transporte orientado a conexión y no orientado a conexión. Actualmente existen cinco protocolos de transporte de OSI que trabajan con el servicio orientado a conexión: TP0, TP1, TP2, TP3 y TP4. El protocolo TP4 trabaja adicionalmente con el servicio no orientado a conexión.

TP0 es el protocolo de transporte más sencillo. Tiene las funciones de la capa de transporte más comunes, es decir, realiza segmentación y reensamblaje de paquetes para la transmisión de datos.

TP1 adicionalmente ofrece una recuperación básica de errores, numera todos los paquetes o PDUs y reenvía aquellos que no son validados. TP1 también reinicia conexiones cuando el número de PDUs no validados son excesivos.

TP2 puede multiplexar y demultiplexar flujos de datos a través de un solo circuito virtual. Esta capacidad en TP2 lo hace particularmente útil sobre redes públicas de datos, donde cada circuito virtual tiene un tipo de tarificación diferente. De la misma forma que TP0 y TP1, TP2 también segmenta y reensambla PDUs.

TP3 combina las funciones de TP1 y TP2.

TP4 es el protocolo de transporte de OSI mas empleado. TP4 es parecido a TCP, ya que está basado en este. Adicionalmente a las funciones de TP3, TP4 proporciona un servicio de transporte confiable, ya que se supone una red sin problemas de medio.

Capa de sesión de OSI

Este protocolo convierte los flujos de datos provenientes de las cuatro capas mas bajas en sesiones con las que se tienen varios mecanismos de control. Estos mecanismos son: conteo, control de la conversación (esto es, determinar cuando y quien se comunica) y negociación de los parámetros de sesión.

El control de la conversación es implementado utilizando un *token*, la posesión de este proporciona el derecho de comunicación. Este *token* puede ser solicitado por las máquinas de los usuarios con diferentes prioridades de uso.

Capa de presentación de OSI

Esta solo tiene un protocolo que permite el la transferencia de la información entre capas adyacentes. Dentro de este protocolo se tiene una función llamada ASN.1 (*Abstract Syntax Notation* 1) que es empleada para convertir el formato de datos, a un formato independiente de cada máquina de usuario. Este permite la comunicación entre aplicaciones de diversas máquinas de usuarios de forma transparente.

Capa de aplicación de OSI

Esta capa contiene *elementos de servicio de aplicación* los cuales permiten una fácil comunicación de las aplicaciones con las capas de OSI mas bajas. Estos *elementos de servicio de aplicación* o ASEs se dividen en tres grupos:

- **Elemento de Servicio de Control Asociado, ACSE.** ACSE asocia los nombres de las aplicaciones con otros en preparación a la comunicación aplicación por aplicación.
- **Elemento de Servicio de Operación Remota, ROSE.** ROSE implementa un mecanismo genérico de solicitud confiable que permite operaciones remotas de forma similar a las llamadas de procedimiento remoto, o RPCs.
- **Elemento de Servicio de Transferencia Confiable, RTSE.** RTSE ayuda a una entrega de la información construyendo una sesión sencilla de usar.

De manera resumida, las principales aplicaciones de OSI son:

Protocolo de Información de Administración Común, CMIP.- Proporciona capacidades de administración de red. Así como SNMP y NetView, CMIP permite la transferencia de información de administración, entre dispositivos finales de usuarios y estaciones de administración.

Servicios de Directorio, DS.- Este fue inspirado de la especificación X.500 de CCITT, que utiliza el servicio de una base de datos distribuida con capacidades de identificación y direccionamiento de los nodos de las capas superiores de OSI.

Transferencia de Archivos, Acceso y Administración, FTAM.- Proporciona el servicio de transferencia de archivos.

Sistemas de Manejo de Mensajes, MHS.- Proporciona un mecanismo fundamental de transporte para aplicaciones de mensajes electrónicos, y de servicios de almacenamiento y envío.

Protocolo de Terminal Virtual, VTP.- Proporciona una emulación de terminal. Es decir permite que un sistema de cómputo situado remotamente parezca estar directamente conectado a una terminal.

3.3.2. Protocolos de enrutamiento de OSI

Como ya se describió anteriormente, la organización de estándares internacionales ISO, desarrolló un grupo completo de protocolos, dentro de los cuales se encuentran los de enrutamiento. Estos protocolos de enrutamiento son llamados IS-IS (*Intermediate system to intermediate system*), ES-IS (*End system to intermediate system*) e IDRP (*Interdomain routing protocol*). La presente sección detalla los primeros dos protocolos de enrutamiento los cuales son requisito para la gestión de los elementos de las redes SDH soportadas por la solución. A continuación se definen algunos términos empleados en el ámbito de las redes ISO:

Terminología para las redes ISO

Para el caso de las redes OSI, es común que se emplee cierta terminología, como la que se define en seguida:

- **Sistema final, ES**.- Se refiere a un nodo de la red que no ejecuta funciones de enrutamiento, como estaciones de trabajo o terminales de monitoreo.
- **Sistema intermedio, IS**.- Son aquellos dispositivos que si ejecutan funciones de enrutamiento.
- **Área**.- Es un grupo de redes contiguas y de *hosts* interconectados, definidos por un administrador de red para constituir un área.
- **Dominio**.- Un grupo de áreas forma un dominio. Los dominios de enrutamiento proporcionan una conectividad completa entre todos los sistemas finales.
- **Enrutamiento de nivel 1**.- Es el enrutamiento que existe dentro de una área.
- **Enrutamiento de nivel 2**.- Es el enrutamiento entre áreas.

Estos términos forman la base de los protocolos IS-IS y ES-IS, siendo la función principal del protocolo ES-IS el permitir que los elementos ES e IS sean descubiertos entre si, mientras que IS-IS proporciona un enrutamiento entre los elementos IS.

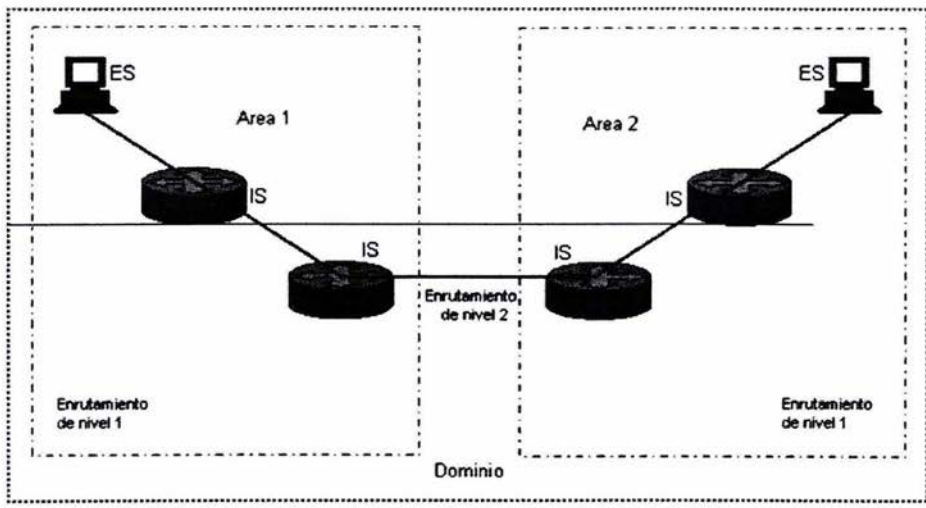

Figura 3.12 Elementos que constituyen una red ISO.

3.3.3. Direccionamiento CLNS

Las direcciones en la arquitectura de una red ISO están referidas con los nombres de "punto de acceso al servicio de red", NSAP o "títulos de entidad de red", NET. Cada nodo en una red OSI puede contar con una, o mas NSAPs o NETs. En un nodo en particular, una dirección NSAP difiere de la NET en relación al valor del último *byte* de esta, que es llamado "selector-n", y su función es similar al número de puerto en TCP/IP. Para una NET el valor es 00 y para una NSAP cualquier otro valor en sistema hexadecimal.

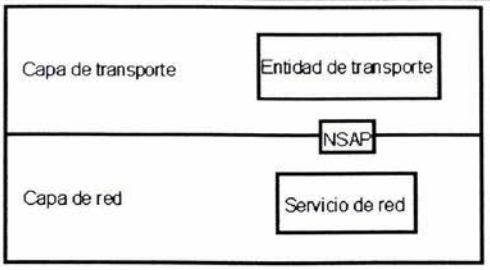

Figura 3.13 Enlace entre una entidad de transporte y un servicio de red

En general, una dirección NSAP está compuesta de dos secciones principales:

- **Parte inicial del dominio, IDP**.- Esta sección está estructurada por un *byte* llamado AFI (identificador de formato y autoridad) y por el campo IDI (Dominio Inicial) de longitud variable. La longitud del campo IDI y el formato de codificación para la segunda sección llamada DSP están basados en el valor del *byte* AFI.
- **Parte específica del dominio, DSP**.- Sección compuesta por los campos "DSP de alto orden", el "identificador de área", el "identificador del sistema" y el *byte* "selector-n".

Sin embargo, para el caso particular del protocolo de enrutamiento IS-IS, una dirección NSAP se divide en dos partes: la dirección de área y el identificador del sistema. El enrutamiento de nivel 2 de IS-IS emplea la dirección de área, mientras que el enrutamiento de nivel 1 emplea el identificador del sistema. En resumen, las direcciones NSAP para el enrutamiento IS-IS están estructuradas como sigue:

- **La dirección de área.-** es la dirección NSAP, sin incluir al identificador del sistema, ni al *byte* "selector-n".
- **El identificador de sistema**.- Ubicado entre la dirección de área y el byte "selector-n".
- **Selector-n.-** Es el último *byte* de la dirección NSAP.

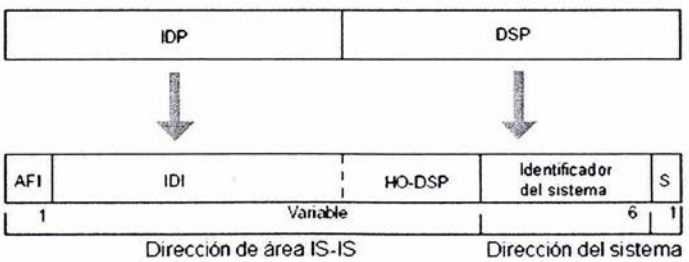

Figura 3.14 Campos que forman una dirección de ISO.

Como se ilustra en la figura anterior, el protocolo de enrutamiento IS-IS interpreta como constitutivos del identificador del área: a los *bytes* desde el campo AFI, hasta el comienzo del campo del identificador del sistema en la sección DSP. El identificador del sistema, ayuda a reconocer al elemento de la red.

Reglas de direccionamiento

Para el correcto direccionamiento de NSAP, se deben respetar las siguientes reglas:

- Dos o más nodos de la red no pueden tener direcciones con la misma NET.
- El protocolo de enrutamiento IS-IS requiere de al menos 8 *bytes* en una dirección: uno para el área, seis para el identificador del sistema y uno para el "selector-n".
- Dos nodos que se encuentren dentro de la misma área, no pueden tener direcciones con el mismo valor en el identificador del sistema.

3.3.4. Protocolo de enrutamiento ES-IS

ES-IS es un protocolo de OSI, que define como los sistemas finales e intermedios se conocen entre si, a través de un proceso llamado "configuración". Esta "configuración" debe realizarse antes de cualquier proceso de enrutamiento entre elementos finales.

Debido a que ES-IS es más un protocolo de descubrimiento que de enrutamiento, este debe distinguir entre tres diferentes tipos de redes:

- **Punto a punto**.- Corresponde a los enlaces seriales, que proporcionan una comunicación uno a uno entre dos elementos de la red.
- ***Broadcast***.- Como *ethernet* e IEEE 802.3, en los cuales se envía un solo mensaje hacia todos los nodos de la red.
- **Topología general**.- Se incluye el protocolo X.25, los cuales soportan un número arbitrario de elementos de red.

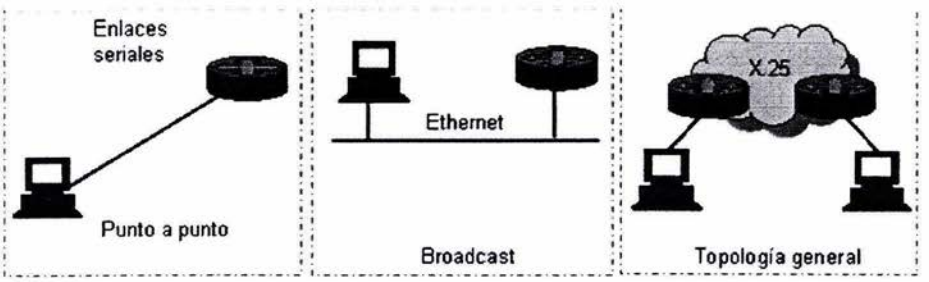

Figura 3.15 Tipos de redes.

Proceso de configuración de ES-IS

Como se mencionó anteriormente, la configuración de ES-IS es el proceso por medio del cual los elementos ES e IS se conocen entre si. La información de configuración ES-IS es transmitida de forma periódica mediante dos tipos de mensajes: Mensajes *ES hello*, o ESH y mensajes *IS hello*, o ISH. Los mensajes ESH son generados por los elementos ES y son enviados a cada elemento IS de la red local. Los mensajes ISH son generados por los elementos IS y son enviados a todos los elementos ES de la red local. Estos mensajes del tipo *hello* son empleados principalmente para transportar las direcciones de capa de red y de subred (capa física) de los sistemas que los generaron.

En las redes tipo *broadcast*, los mensajes tipo *hello* de ES-IS son enviados a todos los elementos IS, a través de direcciones especiales de *multicast* designadas a todos los sistemas finales, mientras que en la operación de una red de topología general, ES-IS generalmente no transmite la información de configuración, debido al alto costo de las transmisiones de *multicast*.

Información de direccionamiento de ES-IS

El protocolo de configuración ES-IS transporta las direcciones tanto de la capa de red, como de la capa física. Las direcciones de capa física de OSI, o "direcciones de punto de conexión a la subred" SNPA, son puntos en los cuales un elemento ES, o IS, está físicamente conectado a una red. La dirección SNPA únicamente identifica a cada sistema conectado en la red. En una red Ethernet, por ejemplo, el SNPA es una dirección de "control de acceso al medio", MAC de 48 bits. Las direcciones de la capa de red de OSI son identificadas mediante la dirección NSAP o mediante la NET. De esta manera, parte de la información de configuración transmitida por ES-IS es la asociación entre las redes NSAP-SNPA, o NET-SNPA.

3.3.5. Protocolo de enrutamiento IS-IS

IS-IS está basado en el protocolo desarrollado por *Digital Equipment Corporation* DEC, y que es llamado DECnet Phase V. Originalmente IS-IS fue desarrollado para enrutar a las redes del tipo "no orientado a conexión" CLNP, sin embargo, posteriormente se desarrolló una versión que soporta tanto redes de este tipo CLNP, como de tipo IP. Esta versión es llamada IS-IS integrado, o IS-IS dual.

IS-IS es un protocolo de enrutamiento jerárquico y de estado de enlace, que inunda a la red con la información de estado de enlace para construir una imagen consistente y completa de la topología de la red.

Con el fin de simplificar el diseño y operación del enrutamiento, IS-IS distingue dos tipos de elementos IS: de nivel 1 y de nivel 2. Los elementos IS de nivel 1 se comunican con otros del mismo nivel dentro de la misma área. Por otro lado, los elementos IS de nivel 2 sirven para el enrutamiento entre áreas de nivel 1 y constituyen el nivel dorsal de enrutamiento interdominio. Mediante esta estructura de enrutamiento jerárquico es posible simplificar el diseño del nivel dorsal debido a que los elementos IS de nivel 1 necesitan saber únicamente como alcanzar al elemento IS de nivel 2 más cercano. Otra ventaja de este esquema jerárquico, es que el protocolo de enrutamiento en el nivel dorsal puede cambiarse sin impactar a los protocolos de enrutamiento intra-área.

Operación de enrutamiento OSI

Con base en lo explicado anteriormente, la operación de enrutamiento se describe a continuación:

Considerando que cada elemento ES existe dentro de una red local, o subred, y que pertenece a un área en particular, el enrutamiento OSI es iniciado cuando un elemento ES descubre al elemento IS mas cercano escuchando los paquetes ISH. Si un ES quiere enviar un paquete a otro ES, este es enviado a uno de los ISs directamente conectados a su subred. Es entonces cuando el elemento IS busca la dirección de destino y envía el paquete por la mejor ruta. Si el ES de destino está dentro de la misma subred, el elemento IS sabrá lo anterior escuchando a los paquetes ESH y consecuentemente reenviará el paquete. Asimismo, el elemento IS también debe proporcionar un mensaje de redirección RD de vuelta a la fuente para indicar que existe una ruta directa y así lograr una comunicación ES a ES. Si la dirección de destino es un elemento ES de otra subred dentro de la misma área, el IS mas cercano tendrá la ruta correcta y enviará consecuentemente el paquete. Si la dirección de destino es un ES de otra área, el IS de nivel 1 envía el paquete al IS de nivel 2 mas cercano. La información se reenviará a través de los IS de nivel 2 hasta que el paquete alcance al IS de nivel 2 del área de destino. Dentro del área de destino, el elemento IS envía el paquete a lo largo del mejor camino hasta que sea alcanzado el ES de destino.

Con la ayuda de los mensajes de actualización de estado de enlace, los elementos IS aprenden acerca de la topología de la red. Estos mensajes son generados por cada IS especificando los ES y los IS que tiene conectados, así como las métricas asociadas. La actualización entonces es enviada a todos los elementos IS vecinos, los cuales reenvían esta información a sus propios vecinos, repitiendo este proceso de manera consecutiva. Con el empleo de estas actualizaciones, cada IS puede construir una topología completa de la red. Si la topología llega a cambiar, son enviadas nuevas actualizaciones.

Consideraciones en la redistribución de áreas de nivel 1

Cuando un dispositivo de enrutamiento tiene conectados a través de una interfaz elementos de red pertenecientes a un área de nivel 1, esta será redistribuida hacia el nivel 2 para su anuncio al resto de la red. Sin embargo, si la interfaz del área de nivel 1 no estuviera en servicio por alguna falla, el dispositivo de enrutamiento seguirá redistribuyéndola no importando la pérdida del enlace. Este fenómeno genera perdida de información, ya que los elementos de otras áreas que quisieran comunicarse con los pertenecientes al área en falla seguirán enviando su información al dispositivo de enrutamiento que la anuncia y finalmente eliminándola al no conocer el destino particular en la tabla de enrutamiento del nivel 1. Para dar solución a este problema, se tienen dos soluciones las cuales se explican a continuación:

Redundancia de equipos interconectados.- Para evitar la pérdida de comunicación de un área, esta deberá tener dos accesos con dos dispositivos de enrutamiento y adicionalmente interconectados de manera directa en su nivel 1. Lo anterior permite que cuando falle uno de los puntos de interconexión al área, el dispositivo de enrutamiento en cuestión actualizará su tabla de enrutamiento de nivel 1, siendo el nuevo camino para alcanzar a los elementos del área la interconexión alterna de nivel 1. La figura 3.16 muestra este esquema:

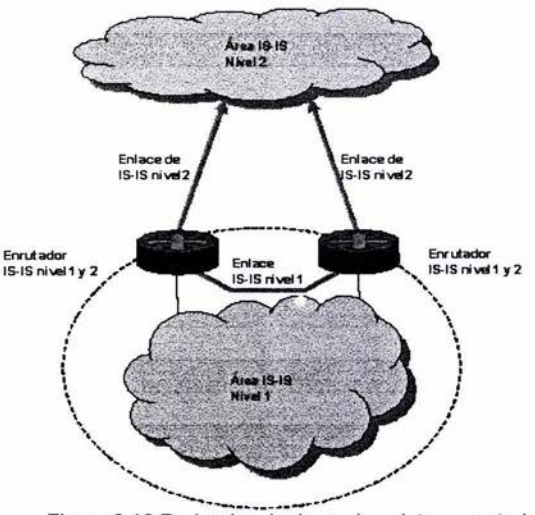

Figura 3.16 Redundancia de equipos interconectados.

La solución anterior se basa en el esquema de reparación de áreas partidas de nivel 1 definida en la especificación de IS-IS 10589, la cual propone establecer un enlace virtual o adyacencia virtual a través del nivel 2 de enrutamiento y anunciándose así el evento de partición de área entre los IS de nivel 1 y 2 mediante un paquete de estado de enlace con el bit, asignado para tal efecto, encendido. De esta, manera la adyacencia virtual se mantiene, evitando pérdida de información. Es importante mencionar, que esta solución no la soporta el proveedor Cisco, por lo que se implementa de manera similar mediante enlaces virtuales o túneles.

Comando de configuración *"partition-avoidance"*.- Este comando para enrutadores Cisco permite detectar de manera automática la perdida de conexión en la interfaz habilitada con el área en cuestión.

Estas dos soluciones se utilizarán en la propuesta de diseño de la presente tesis y se explicará mas adelante bajo que casos se elegirán.

Métricas de IS-IS

IS-IS emplea una sencilla métrica por *default*, con un valor máximo en la trayectoria de 1024, sin embargo esta métrica es arbitraria y la asigna típicamente el administrador de red. Cualquier enlace sencillo puede tener un valor máximo de 64, y la trayectoria total es calculada sumando los valores de los enlaces. Los valores máximos de las métricas fueron asignados a estos niveles para proporcionar la granularidad suficiente para soportar varios tipos de enlaces mientras que al mismo tiempo aseguran que el algoritmo de "trayectoria más corta", SPF, empleado para el cálculo de rutas, sea razonablemente eficiente. IS-IS también define tres métricas opcionales llamadas costos: retardo (*delay*), costo (*expense*) y error. La métrica de retardo, refleja la cantidad de retardo en un enlace. La métrica de costo refleja el costo de comunicación asociado con el uso de un enlace. La métrica de error refleja la tasa de error de un enlace. IS-IS mantiene una relación de estas cuatro métricas, con la opción de calidad de servicio de CLNP que están incluidas en el encabezado. Asimismo, IS-IS emplea esta relación para calcular las rutas a través de la red.

Formatos de paquetes de IS-IS

IS-IS emplea tres formatos básicos de paquetes:

- Paquetes *hello* de IS-IS.
- Paquetes de estado de enlace LSP.
- Paquetes de secuencia de número SNP.

Cada uno de estos tres paquetes de IS-IS tiene un formato complejo con las siguientes tres partes lógicas en común: La primera parte consiste en un encabezado fijo de 8 *bytes*, siendo el mismo para los tres paquetes. La segunda parte es una porción del tipo específico de paquete con un formato fijo. La tercera parte es también un tipo específico de paquete pero de longitud variable. La figura 3.17 ilustra el formato lógico de los paquetes de IS-IS. La figura 3.17 muestra los campos comunes de los encabezados de los paquetes de IS-IS.

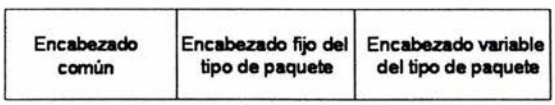

Figura 3.17 Formato lógico de los paquetes de IS-IS.

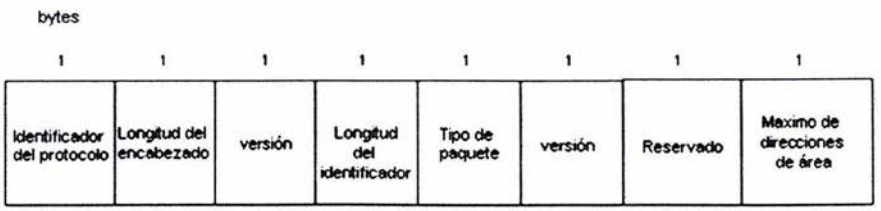

Figura 3.18 Campos comunes de los encabezados de los paquetes de IS-IS.

Las siguientes descripciones resumen los campos mostrados en la figura 3.18:

- **Identificador del protocolo**.- Identifica al protocolo IS-IS y contiene un valor constante de 131.
- **Longitud del encabezado**.- Contiene la longitud del encabezado fijo. La longitud siempre es igual a 8 *bytes*, pero está incluida para que los paquetes IS-IS no difieran significativamente de los paquetes CLNP.
- **Versión**.- Contiene el valor de 1 en la especificación actual de IS-IS.

- **Longitud del identificador**.- Especifica el tamaño de la parte del identificador de una dirección NSAP. Si el campo contiene un valor entre 1 y 8 inclusive, la porción del ID de una dirección NSAP es ese número, en *bytes*. Si el campo contiene un valor de cero, la parte de ID de una dirección NSAP es de 6 *bytes*. Si el campo contiene un valor de 255, la parte del identificador de una dirección NSAP es de cero *bytes*.
- **Tipo de paquete**.- Especifica el tipo de paquete IS-IS (*Hello*, LSP o SNP)
- **Versión**.- Repetida después del campo de tipo de paquete.
- **Reservado**.- Es ignorado por el receptor y es igual a cero.
- **Direcciones de área máxima**.- Especifica el número de direcciones permitida en esa área.

Siguiendo el encabezado común, cada tipo de paquete tiene una parte adicional fija y diferente, seguida por una parte variable.

3.3.6. IS-IS Integrado

Es una versión del protocolo de enrutamiento IS-IS de OSI que emplea un solo algoritmo de enrutamiento para soportar más protocolos de capa de red además de CLNP. IS-IS integrado algunas veces es llamado IS-IS dual por la combinación de soportar redes CLNP e IP en específico. Debido a lo anterior, algunos campos son agregados a los paquetes de IS-IS para permitir que IS-IS soporte protocolos de capa de red adicionales. Estos campos informan a los enrutadores acerca de que tan alcanzable son las direcciones de red de otros grupos de protocolos y su información en particular. Las implementaciones de IS-IS integrado envían un solo grupo de actualizaciones de enrutamiento, logrando ser este proceso más eficiente que el tener dos implementaciones separadas.

IS-IS integrado es la aproximación conocida como *ships in the night*, ya que este enrutamiento evoca el uso de un protocolo de enrutamiento distinto y completamente separado de otros protocolos de red que pudieran tenerse en el mismo dispositivo de enrutamiento. Con lo anterior, múltiples protocolos de enrutamiento esencialmente existen de manera independiente. El enrutamiento integrado tiene la capacidad de enrutar múltiples protocolos de capa de red a través de tablas calculadas por un solo protocolo de enrutamiento, ahorrando algunos recursos del enrutador. IS-IS integrado usa esta aproximación.

3.3.7. Protocolo de enrutamiento interdominios

IDRP (*Interdomain Routing Protocol*), es un protocolo de OSI que especifica como se comunican los enrutadores con otros en diferentes dominios. IDRP fue diseñado para operar de igual forma con CLNP, ES-IS e IS-IS y está basado en el protocolo de enrutamiento interdominios BGP, el cual fue originado dentro de la comunidad de IP.

Dado que IDRP introduce ciertos términos específicos al ambiente en que opera, estos son descritos a continuación:

Terminología de IDRP

- **BIS, *Border intermediate system***.- El "sistema intermedio de frontera", es un elemento IS que opera bajo un mismo conjunto de reglas administrativas y un plan de enrutamiento común.
- **RD, *Routing domain***.- Es un grupo de elementos IS y ES que operan bajo el mismo conjunto de reglas administrativas y que comparten un mismo plan de enrutamiento.
- **RDI, *Routing domain identifier***.- Es un identificador de dominio de enrutamiento, el cual es único.
- **RIB *Routing information base***.- Este contiene el conjunto de rutas elegidas por su uso por un "sistema intermedio de frontera" en particular.
- ***Confederación***.- Es un grupo de dominios de enrutamiento que son vistos como uno solo fuera de la confederación. La topología de una confederación no es conocida fuera del grupo de

dominios de enrutamiento. Asimismo estas pueden estar anidadas entre si, ayudando a reducir el tráfico de red ya que este esquema puede actuar como filtros entre redes.

La figura 3.19 ilustra la relación entre entidades de IDRP:

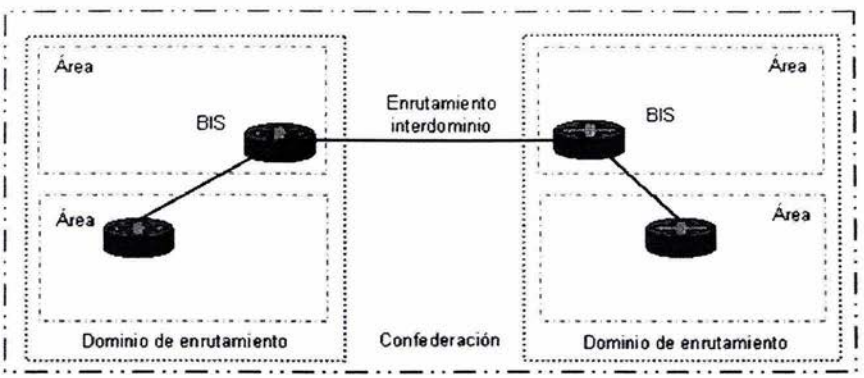

Figura 3.19 Esquema de confederaciones.

A continuación se describe el enrutamiento bajo IDRP:

Enrutamiento IDRP

Una ruta bajo el protocolo IDRP es una secuencia de identificadores de dominios de enrutamiento, los cuales algunos pueden ser de confederaciones. Cada elemento BIS dentro de la ruta, es configurado para tener conocimiento del dominio de enrutamiento y de la confederación a la cual pertenece. El conocimiento de otros BIS, dominios de enrutamiento y confederaciones se realiza a través del intercambio de información entre cada vecino. Únicamente las rutas que satisfacen las políticas locales de los BIS y que han sido seleccionadas para su uso serán enviadas a otro elementos BIS. Por otro lado, si se requiriera de un recálculo de rutas, este es se realiza en forma parcial y ocurre cuando sucede uno de los tres siguientes eventos:

- Al recibir una actualización de enrutamiento por una nueva ruta.
- Cuando un vecino BIS esta fuera de alcance.
- Al establecerse una vecindad con un elemento BIS.

Finalmente, las características del protocolo IDRP incluyen lo siguiente:

- Soporta aspectos de calidad de servicio para CLNP.
- Evita "*loops*" de enrutamiento al conservar la información de todos los dominios de enrutamiento que cruza una ruta en particular.
- Reducción de información de rutas y de procesamiento con el empleo del concepto de confederaciones y por la compresión de información de los dominios de enrutamiento.
- Protocolo confiable al hacer uso de un transporte propio del sistema.
- Seguridad al hacer uso de cifrado en cada paquete.
- Trabaja bajo el empleo de servidores de rutas.

4. Criterios de diseño para una red de datos

El presente capítulo describe los pasos a seguir dentro del proceso general de diseño de una red de datos, por medio del cual se definió la "Red virtual de CLNS" de la presente tesis:

4.1. Premisas de diseño

Como primer paso dentro de los criterios de diseño para una red de datos, se deben considerar ciertos aspectos que el negocio, o el grupo de trabajo interesado, definen para la operación de la red. A continuación se listan tales aspectos:

- El análisis de los requerimientos del cliente, que abarcan tanto sus metas, como las limitaciones del negocio. Las metas de negocios incluyen la capacidad de integrar aplicaciones de red que ayuden a lograr estas metas corporativas. Las limitaciones del negocio, bien pueden ser de presupuesto, de la cantidad del personal de gestión de red, o bien tiempos cortos en la implementación.
- La metodología de diseño que debe estar basada en la medida de lo posible en el modelo OSI, tanto en las funciones de cada nivel, como en la interacción o servicios que se tienen entre ellas. Bajo esta referencia, resulta más ágil la selección de los dispositivos de enrutamiento y de conmutación en la capa de red.
- El análisis de operación de las estructuras de los grupos de trabajo, encargadas de la administración de la red en cuestión, provee información valiosa que se debe considerar en el proceso de diseño.
- Las políticas del negocio resultan imperantes dentro de las consideraciones y lineamientos a seguir durante el diseño de la red.

4.2. Recopilación de Información

Como segundo paso dentro del proceso de diseño, se requiere de la recolección de información necesaria para el análisis del diseño. El contenido de esta información se lista a continuación:

- **Topología actual**.- Que incluye mapas globales, regionales, físicos y lógicos.
- **Equipos**.- Para el caso del rediseño de una red que ya se encuentra en operación, esta información resulta importante y se deben incluir las marcas y modelos de los equipos, versiones de sistema operativo, características de memoria, y tipos de puerto.
- **Enlaces**.- Tipos de enlaces disponibles (Dedicado, *Frame Relay*, conmutado, etc.), el ancho de banda requerido y su trayectoria (origen-destino).
- **Conexiones externas**.- Si existe, o se requiere, interconexión con otras redes, ya sean públicas o privadas.
- **Protocolos de enrutamiento y enrutados**.- Enrutamiento (*OSPF, BGP, EIGRP, RIP, ISIS*) y enrutados (*IP, IPX, Apple Talk, X.25, CLNP*).
- **Desempeño de la red**.- Tiempos de respuesta entre sitios mas críticos, información histórica de la utilización de memoria y CPU (4 meses o mas), información histórica de la utilización de enlaces (4 meses o mas).
- **Información de las aplicaciones**.- Nombre y uso (tarificación, gestión, corporativa, etc.).
- **Equipos y/o usuarios por aplicación** (cantidad y distribución geográfica), flujos de tráfico (magnitud y patrones de tráfico), estatus de la aplicación (nueva o actualización) y protocolos empleados (*IP, IPX, TFTP, ICMP*, etc.).
- **Características de tráfico**.- Horas pico, calendario de uso, sentido de los flujos.

- **Sistema de Gestión**.- Existencia de este, cobertura y tipo (centralizado o distribuido), organización del grupo de gestión.
- **Políticas y restricciones de operación**.- Políticas de uso (quién usa la red, quién la administra, horarios de uso, protocolos de red establecidos y seguridad), políticas de crecimiento de la red (enlaces, equipo y aplicaciones).
- **Tiempo de entrega del proyecto** (etapas y tiempos del proyecto)
- **Presupuesto del proyecto**

4.3. Análisis de la información y propuesta del diseño

De acuerdo a las aplicaciones, es necesario identificar cuales son los flujos de información más importantes considerando su cobertura, la importancia para la empresa, el número de usuarios y/o equipos, así como el volumen de tráfico generado por cada una de ellas.

También es necesario identificar el direccionamiento empleado, abarcando el número y tipo de redes, y la forma de asignación de estas.

Dentro de la propuesta del diseño se establece la topología de la red más recomendable, estableciendo la regionalización de la red, la definición de sitios para los niveles de la red jerárquica, la redundancia de enlaces y equipos en los sitios críticos, y la interconexión de redes externas. La propuesta de diseño debe incluir: la propuesta de topología y enlaces, equipos, sitios críticos, direccionamiento, protocolos de enrutamiento y enrutables, los esquemas de redundancia y los esquemas de seguridad.

De acuerdo a la jerarquía de la red y al costo de ésta, los enlaces se definen de acuerdo a su tipo, al ancho de banda y a su trayectoria.

La propuesta de equipos dependerá del uso de los mismos en la red, así como su costo, además de considerar las marcas y modelos, su sistema operativo (funcionalidades soportadas) y las características de escalabilidad y versatilidad de ellos.

Los sitios críticos deben incluir el tipo de interconexión, los aspectos de seguridad, las características de redundancia y el ancho de banda a utilizar.

El direccionamiento debe ser jerárquico, haciendo uso de subredes y agrupamiento, o "sumarización", de rutas.

Los protocolos de enrutamiento y enrutables, deben definirse como protocolos de bajo consumo de *overhead*, siendo estándares, o abiertos. De ser posible, jerárquicos, escalables y de rápida convergencia.

Las propuestas de esquemas de redundancia deben de incluir la redundancia de enlaces, con diversidad de trayectorias para el flujo de tráfico, redundancia en equipos o en los dispositivos de procesamiento de datos para su enrutamiento y conmutación; la redundancia en la alimentación eléctrica de los equipos y dispositivos también debe ser considerada.

Un punto de suma importancia dentro de la propuesta de diseño es el esquema de seguridad. Desde el control de acceso y la administración de los dispositivos de la red, el filtrado de rutas, el filtrado de tráfico, y el acceso y salida de redes externas, como lo es hacia redes públicas.

4.4. Prueba del diseño

Dentro de las pruebas del diseño, se deben de verificar los esquemas de redundancia y seguridad, realizando la simulación de fallas en equipos y enlaces, así como la simulación de accesos no permitidos (*intrusion detection*), el filtrado de rutas y la verificación de tráficos definidos.

También deben incluirse pruebas de enrutamiento, que abarquen los tiempos de convergencia, el anuncio de rutas en la red, los posibles *loops* de enrutamiento y las métricas obtenidas.

Se deben realizar pruebas de "estrés", las cuales están basadas en la simulación de altos volúmenes de tráfico para verificar la respuesta de la red, y los tiempos de respuesta obtenidos en diferentes puntos de la misma.

Tales pruebas del diseño deberán realizarse en dos etapas, donde la primera será bajo un ambiente controlado, ya sea mediante un simulador de red, o implementando una maqueta que resuma el diseño propuesto. Lo anterior permitirá obtener información necesaria para los posibles ajustes a la propuesta de diseño. Una vez que los resultados de las pruebas al diseño de la red sean satisfactorios. Se procederá a la realización de una prueba piloto dentro de la red en producción. De esta manera se asegurará la correcta implementación y operación del diseño.

4.5. Documentación del diseño

Durante cada etapa del proceso de diseño, es indispensable dejar por escrito la información obtenida. Por lo anterior se deben crear documentos que expongan y expliquen las decisiones tomadas en cada etapa. También deberán quedar asentadas por escrito las nuevas políticas y lineamientos a seguir para la operación en el nuevo diseño de red.

Así mismo, es importante definir el proceso de implementación del diseño, con el fin de evitar afectaciones a los servicios que ya se encuentren en producción y que también permita una ágil y segura implementación del diseño mismo, involucrando e informando a las áreas responsables.

Finalmente, se debe crear un documento ejecutivo que resuma los aspectos más importantes del nuevo diseño, sus ventajas, sus costos de instalación, sus costos de mantenimiento y el tiempo de implementación, así como los requerimientos. Toda esta información debe ser entregada al grupo de trabajo que se encargará de la operación de la red bajo el nuevo diseño.

4.6. Continuidad

Una vez que se encuentre en operación el nuevo diseño de red, es indispensable dar seguimiento al funcionamiento de este, con el fin de detectar posibles ajustes o mejoras, mediante procesos bien definidos de planeación de la capacidad, o ingeniería de tráfico. Tales mejoras pueden ser en puntos particulares de la red, o bien generales, que pueden afectar de manera global al diseño.

5. Análisis de las características de la red y su propuesta de diseño

El presente capítulo describe los aspectos relacionados con la propuesta de diseño que da solución al requerimiento de transporte de información de gestión de elementos SDH. Tales aspectos abarcan los siguientes puntos:

- Características físicas y lógicas de la red de datos en la que se implementará el diseño,
- Características de operación referentes a los sistemas de gestión de elementos SDH.
- Análisis desarrollado para definir la propuesta de diseño, con base en los aspectos descritos anteriormente.
- La solución de diseño, describiendo sus características de funcionamiento.

A continuación se explican las características de las partes en que se deberá basar la propuesta del diseño:

5.1. Marco Inicial de diseño

La propuesta de diseño para dar solución al transporte de información de gestión SDH, se desarrolla sobre una red de datos en operación, razón por la cual se deben realizar los ajustes y modificaciones necesarios en esta basándose en las políticas de desempeño y de crecimiento definidas para esta red de datos, y satisfaciendo plenamente los requisitos para la operación de los sistemas de gestión SDH.

Las políticas de desempeño y crecimiento, las características de operación de los sistemas de gestión SDH, y las características de la red de datos, se describen de forma detallada en las siguientes secciones:

5.1.1 Características de operación de la red de Datos

La propuesta de diseño de la presente tesis está implementada sobre una red corporativa de datos multiservicios, es decir una red que da el servicio de transporte de datos a diferentes aplicaciones empresariales tales como: correo electrónico, acceso a Internet, servicios de impresión, acceso a servidores, transferencia de archivos, transporte de información de alarmas, de información de gestión, de facturación, entre otras.

El diseño de esta red se basa en un modelo jerárquico y redundante, tanto en enlaces, como en equipos de red, permitiendo así un alto grado de disponibilidad para el transporte de información de las aplicaciones y una escalabilidad que permitirá establecer de forma sencilla y oportuna crecimientos sobre la propia red. La siguiente figura muestra el modelo jerárquico utilizado en esta red de datos multiservicio:

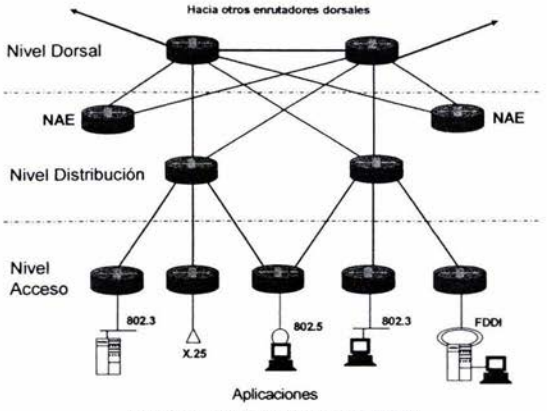

Figura 5.1 Topología jerárquica

Esta topología consiste en definir niveles de servicio a los dispositivos que formarán la red para obtener ventajas en el orden de crecimiento, de atención a fallas y de desempeño. Básicamente se tienen tres niveles los cuales se describen brevemente a continuación:

- **Nivel Dorsal**.- Permite la conmutación de información de manera rápida, segura y en grandes volúmenes entre diferentes regiones, o áreas, definidas para la propia red.
- **Nivel de Distribución**.- Es el nivel donde se concentran todos los dispositivos de enrutamiento que forman parte del nivel de acceso y a su vez se interconecta con el nivel dorsal para el envío de información que tiene como destino otra región. En este nivel se aplican políticas de servicio y de enrutamiento para la operación de la red.
- **Nivel de acceso**.- En este nivel se permite la interconexión de los usuarios y de las aplicaciones, ya sea en forma directa o a través de redes locales, a la red de datos.

Dentro de este modelo jerárquico se desprenden casos especiales de acceso, los cuales son definidos para resguardar las aplicaciones y los servicios críticos para la empresa, ya sea por la importancia del servicio, o por el alto volumen de información que estos generan. Con base en las razones anteriores, estos accesos especiales son conectados directamente al nivel dorsal, asegurando así una mejor y rápida transferencia de la información.

Considerando que la presencia de la empresa es a nivel nacional, la cobertura de la red también lo debe ser, encontrándose organizada en regiones definidas de acuerdo a los intereses de la misma:

Nombres de las regiones	
Región1	Región5
Región2	Region6
Región3	Región7
Región4	Región8

Tabla 5.1 Números de las regiones de la red de datos multiservicios

Cada una de estas regiones se encuentra bajo una estructura jerárquica y las interconexiones entre estas se encuentran mediante arreglos en forma de deltas. Adicionalmente se cuenta con redundancia de enlaces y de dispositivos de red, para el nivel dorsal y el de distribución. Debido a razones de costo, para el caso del nivel de acceso, no se maneja redundancia de equipo ni de enlaces hacia el nivel distribuidor.

La figura 5.2 muestra la topología típica de una región y la figura 5.3 muestra la interconexión de las regiones en el nivel dorsal:

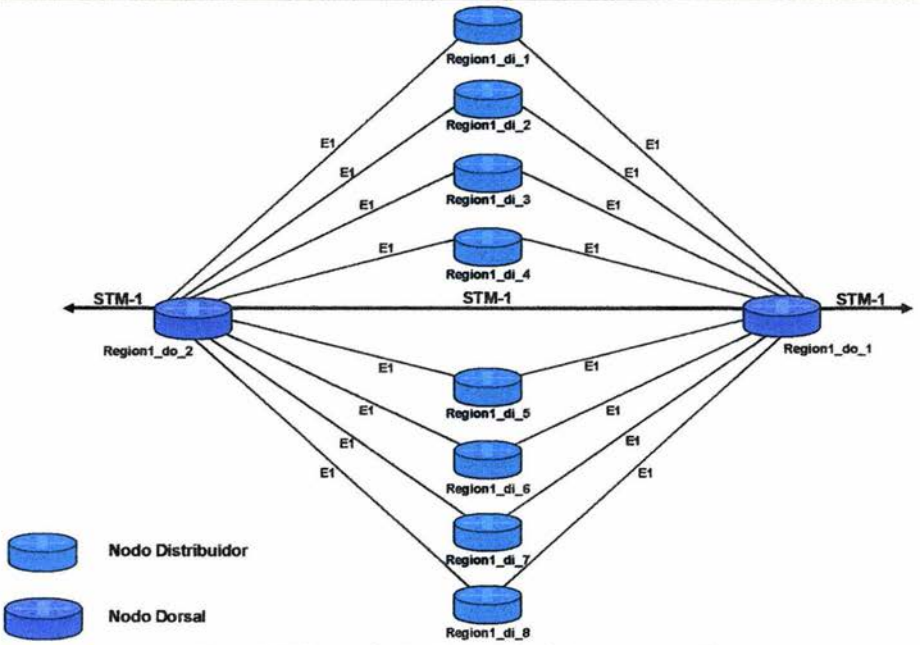

Figura 5.2 Topología de distribución típica de una región

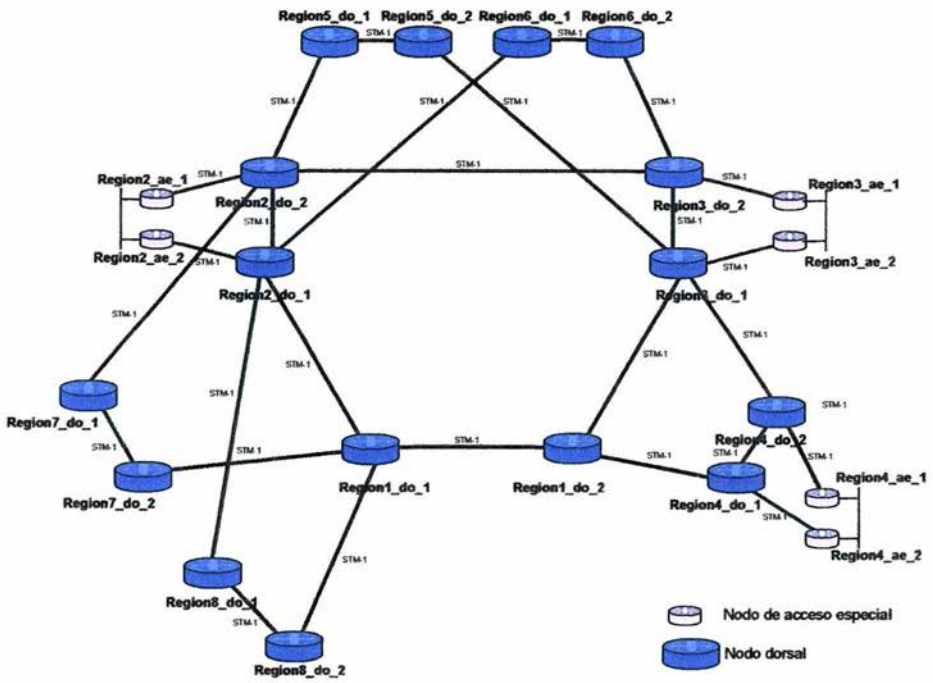

Figura 5.3 Topología del nivel dorsal de la red de datos multiservicio

Es importante observar que en la interconexión de los nodos dorsales existe una "delta principal" en la cual están interconectados otros arreglos en delta. Lo anterior se debe a que en esta se conectan los accesos especiales con mayor terminación y generación de tráfico de la empresa, siendo el resto de las regiones, meros afluentes del tráfico.

Capacidad de los enlaces entre los niveles

La capacidad de los enlaces entre cada uno de los niveles se define de acuerdo a la cantidad de información que se transporte en estos. En particular, la mayoría de la información es enviada, o recibida, por las aplicaciones que residen en los accesos especiales y en una menor proporción, se conserva dentro de la región en cuestión para aplicaciones locales.

El dimensionamiento de ancho de banda requerido entre nodos dorsales se define de acuerdo a las necesidades de velocidad y capacidad de transmisión de datos entre regiones, también este dimensionamiento está muy relacionado con las aplicaciones y nuevas tecnologías que se quieran introducir a la red, tales como Voz sobre IP, Redes Virtuales Privadas, o Aplicaciones bajo *multicast*. Finalmente la elección del tipo de enlace está fuertemente ligada a los costos de instalación, operación y renta. Los enlaces empleados para esta red son del tipo STM-1.

El dimensionamiento y crecimiento de los enlaces que van de los nodos distribuidores a los nodos dorsales, se realiza en múltiplos de enlaces tipo E1 y dependerá de los requerimientos específicos de cada región.
Así como en el caso de los enlaces entre nodos dorsales, el ancho de banda requerido está muy ligado con las aplicaciones y nuevas tecnologías que se requieran en la red. Cuando los requerimientos de la red así lo determinen y de acuerdo a las políticas de crecimiento, es factible emplear enlaces del tipo E3 para conectar nodos distribuidores con nodos dorsales.

Para el caso de los nodos de acceso especial, su interconexión hacia el nivel dorsal se hace mediante enlaces punto a punto de alta capacidad. El número de enlaces y la capacidad de estos varían según los requerimientos de redundancia y volumen de información a transmitir que se tengan, así como de la introducción de nuevas funcionalidades y tecnologías. Los tipos de enlaces empleados pueden ser E1, E3 o STM-1.

El ancho de banda requerido para la conexión de los nodos de acceso al nivel distribución, varía según los requerimientos, tanto de redundancia, como de volumen de información a transmitir. Los principales enlaces empleados son del tipo DS0 (64kps) y E1.

Características físicas de los equipos de red a emplear

Las características físicas de los equipos que forman cada nodo de red están definidas de acuerdo al nivel al que pertenezcan. Asimismo es importante considerar que la marca empleada para los equipos de enrutamiento de la red es "Cisco", ya que satisface de manera amplia con los requerimientos de diseño de cada nivel. A continuación se describen las características más importantes de acuerdo al tipo de nodo:

Nodos Dorsales

De acuerdo a la importancia de las funciones de este nivel, se tienen los siguientes requerimientos:

Concepto	Características
Alta disponibilidad	• Redundancia en tarjetas procesadoras • Redundancia en fuentes de alimentación
Gran capacidad de operación	• Alta densidad de puertos • Gran capacidad de conmutación de paquetes • Retardo mínimo en procesamiento • Soporte de protocolos estándar • Alta disponibilidad en memoria para su funcionamiento
Flexibilidad de crecimiento	• Equipo modular • Fácilmente actualizable en *Hardware* y sistema operativo • Soporte de nuevas tecnologías y funcionalidades

Tabla 5.2 Requerimientos de los enrutadores del nivel dorsal.

Los equipos de enrutamiento comerciales que cumplen con los requerimientos anteriormente listados son los siguientes:

- Cisco serie 7500, modelos Cisco 7507 y 7513

Nodos de Distribución

Los requerimientos para los equipos empleados en este nivel son los siguientes:

Concepto	Características
Alta disponibilidad	• Redundancia en tarjetas procesadoras • Redundancia en fuentes de alimentación
Gran capacidad de operación	• Alta densidad de puertos • Gran capacidad de conmutación de paquetes • Retardo mínimo en procesamiento • Soporte de protocolos estándar • Alta disponibilidad en memoria para su funcionamiento
Flexibilidad de crecimiento	• Equipo modular • Fácilmente actualizable en *Hardware* y sistema operativo • Soporte de nuevas tecnologías y funcionalidades

Tabla 5.3 Requerimientos de los enrutadores del nivel de distribución.

Debido a que estos requerimientos son los mismos para los nodos dorsales, se empleará la serie 7500 de Cisco, modelos Cisco 7507 y 7513.

Nodos de Acceso Especial

Los requerimientos para este tipo de nodos se listan a continuación:

Concepto	Características
Alta disponibilidad	• Redundancia en tarjetas procesadoras • Redundancia en fuentes de alimentación
Gran capacidad de operación	• Versatilidad en puertos (seriales y para red de área local) • Gran capacidad de conmutación de paquetes • Retardo mínimo en procesamiento • Soporte en diversidad de protocolos de redes. • Alta disponibilidad en memoria para su funcionamiento
Flexibilidad de crecimiento	• Equipo modular • Fácilmente actualizable en *Hardware* y sistema operativo • Soporte de nuevas tecnologías y funcionalidades

Tabla 5.4 Requerimientos de los enrutadores de acceso especial.

Las series de enrutadores comerciales de la marca "Cisco" utilizados para este tipo de nodos se listan a continuación:

- Cisco serie 3600, modelo 3660 Telco
- Cisco serie 7500, modelo 7507

Nodos de Acceso

Los modelos de enrutador empleados en este tipo de nodos dependen de las necesidades en los servicios del usuario, sin embargo las características principales que se requieren se listan a continuación:

Concepto	Características
Alta disponibilidad	• No es de carácter crítico.
capacidad de operación	• Versatilidad en puertos (seriales y para red de área local) • Soporte en diversidad de protocolos de redes
Flexibilidad de crecimiento	• Equipo modular • Fácilmente actualizable en *Hardware* y sistema operativo • Soporte de nuevas tecnologías y funcionalidades • Equipos de bajo costo

Tabla 5.5 Requerimientos de los enrutadores del nivel de acceso.

Las plataformas de enrutadores del fabricante "Cisco" que mejor convienen para este tipo de nodos se listan a continuación:

- Cisco 3600, modelo 3620, 3640, 3660 Telco
- Cisco 3700, modelo 3725, 3745
- Cisco 7500, modelo 7507

Características de enrutamiento

Una parte fundamental de la administración y el análisis de una red de datos, es el poder predecir el comportamiento de la misma durante su operación normal y en casos de contingencia. Este comportamiento es derivado, en la mayoría de los casos, del protocolo de enrutamiento en uso, por lo que su elección debe tomar en cuenta principalmente los siguientes criterios:

- Rápida convergencia
- Tráfico generado por actualizaciones de enrutamiento mínimo
- Uso de máscaras IP de longitud variable
- Sumarización de rutas
- Estabilidad del protocolo
- Bajo procesamiento en los equipos de enrutamiento

El protocolo de enrutamiento empleado en esta red de datos bajo los criterios es EIGRP (*Enhanced Interior Gateway Routing Protocol*), siendo utilizado en los niveles dorsal, distribución y nodos de acceso especial. Este protocolo, propietario de "Cisco", ha demostrado ser estable y de rápida convergencia a los cambios suscitados en la red (con tiempos de convergencia menores a 5 segundos), razón por la cual fue elegido para esta red.

Las características más importantes de este protocolo de enrutamiento son las siguientes:

- Protocolo IGP clasificado como un híbrido de los protocolos de "estado de enlace" y de "vector distancia".
- Velocidad de convergencia igual o mejor que la de los protocolos con los cuales compite.
- Soporta máscaras de subred de longitud variada y sumarización de rutas.

Direccionamiento IP de la red

Al ser empleado el protocolo IP en esta red de datos multiservicios, su direccionamiento se basa en el prefijo 10.0.0.0/8, que es el definido para las redes privadas por el IETF bajo el requisito de no anunciar sus rutas a Internet. A esta red se le definen subredes con máscaras de 30 bits para enlaces seriales o WAN, y de 24 a 27 bits para puertos LAN. Asimismo el direccionamiento se desarrolló en forma jerárquica, permitiendo el agrupamiento de rutas por regiones y logrando así: reducir las tablas de enrutamiento, disminuir el procesamiento en los enrutadores debido al cálculo de rutas y aislar problemas por oscilación de enlaces.

Funcionalidades principales del sistema operativo de los enrutadores

El desarrollo de los equipos de enrutamiento de "Cisco", está basado en un crecimiento flexible, que sopote tanto nuevos dispositivos físicos, como software que soporte nuevas funcionalidades y tecnologías. En este último punto, es importante elegir el software o sistema operativo que desempeñe de manera estable y eficiente los requerimientos de cada nodo.

Para el desarrollo del presente diseño se eligieron básicamente 2 versiones de sistema operativo, los cuales cumplen con los requerimientos descritos en las características físicas de los equipos de red a emplear de manera estable:

Versión de sistema operativo	Nodos donde se usan
Cisco IOS 12.0(7)T	Accesos, accesos especiales
Cisco IOS 12.0(23)s3	Dorsales, distribuidores

Tabla 5.6 Versiones de sistema operativo a emplear.

5.1.2. Aspectos lógicos de los sistemas de gestión SDH

Los servicios de transmisión de datos bajo una red de transporte SDH ofrece técnicas de multiplexado y demultiplexado que permiten el envío de información por enlaces digitales de 2 Mbits/s 34 Mbits/s o 155Mbits/s y que son demandadas para la interconexión de redes tipo LAN, acceso de alta velocidad a Internet, videoconferencia y enlaces punto a punto, por citar algunos ejemplos.

La estructura de estas redes SDH utilizan un modelo jerárquico de tres niveles, el cual facilita la elección de las topologías físicas de la red y las técnicas de administración. La siguiente figura muestra este modelo:

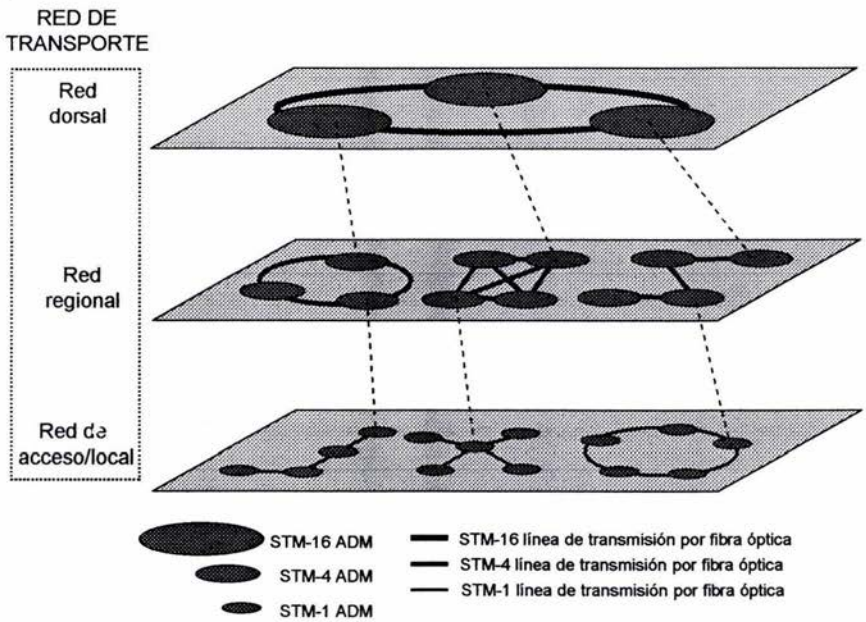

Figura 5.4 Modelo jerárquico de una red SDH.

El nivel dorsal o *backbone*, debe tener la característica de una gran capacidad de transmisión, ya que en este se envían cantidades considerables de tráfico entre regiones. El nivel regional generalmente recolecta el tráfico generado dentro de cada región geográfica. Finalmente el nivel de acceso local, soporta relativamente un bajo volumen de tráfico entre centros urbanos locales o rurales. La selección del equipamiento para formar la estructura de la red de transporte SDH en cada uno de estos tres niveles radica en la velocidad de operación de cada elemento de la red, asimismo el empleo de *software* para la administración de estos elementos resulta flexible para su operación. Con base en esta flexibilidad, se pueden definir los elementos lógicos que conforman un sistema de gestión de una red de transporte SDH, los cuales se listan a continuación:

- El sistema Gestor.
- La red de Comunicación de Datos, ó DCN (*Data Comunication Network*)
- La red de transporte SDH.
- La interfaz usada para integrarse a la DCN.

El sistema de gestión de una red de transporte SDH está basada en el modelo de gestión TMN, *Telecommunication Management Network* . La figura 5.5 muestra la representación esquemática de este modelo:

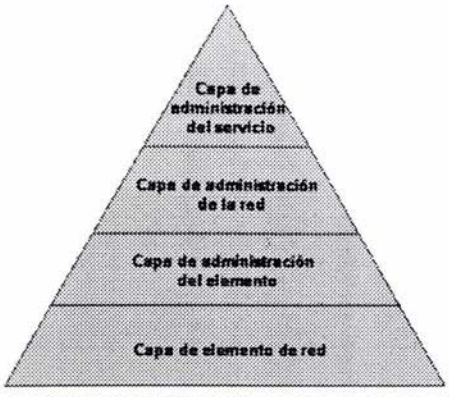

Figura 5.5 Modelo TMN para la gestión de equipos SDH.

Los dispositivos de red para la plataforma SDH comprenden varios tipos de elementos de red llamados NEs (*Network Elements*). Estos NE requieren para su gestión y supervisión de una red alterna de comunicación llamada SDH DCN (*SDH Data Comunication Network*), la cual permite asegurar el acceso remoto a todos los NE para su supervisión de una manera efectiva y segura.

Los protocolos de capa de red recomendados para comunicación entre los NEs y el sistema de gestión están definidos bajo las recomendaciones ISO 10589 para el protocolo de enrutamiento IS-IS, e ISO 8473 para el protocolo de red CLNP.

La figura 5.6 muestra el esquema básico de un sistema de gestión SDH, el cual se encuentra centralizado, es decir, en un extremo se encuentra un solo sistema de gestión, a los usuarios del sistema de gestión y por el otro a los NE que son gestionados.

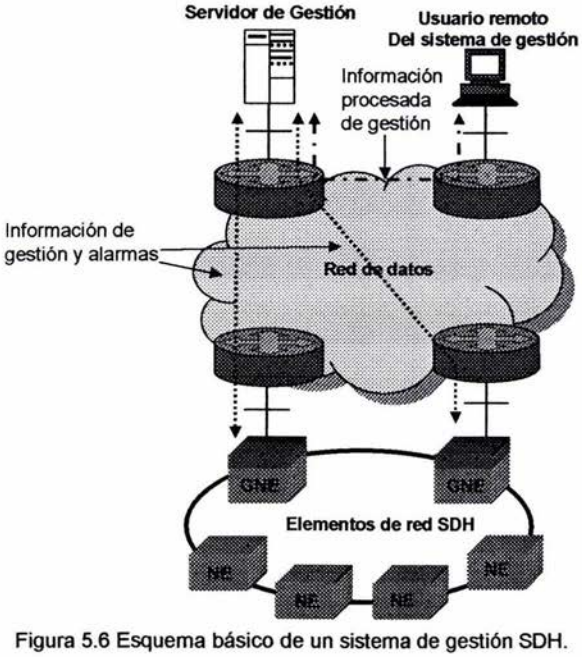

Figura 5.6 Esquema básico de un sistema de gestión SDH.

El arreglo en que se encuentran interconectados los elementos de red puede ser en anillo o en bus, y la cantidad de estos puede variar de entre 18 y 128 elementos dependiendo del tamaño del anillo, cobertura y especificaciones del fabricante. La comunicación hacia el sistema de gestión para cada NE es a través de sus propios vecinos NE, contando con un máximo de 128 saltos o vecinos por cruzar. Este valor es considerado como el número máximo de elementos dentro de un anillo y se encuentra definido por la norma ISO 10589.

La interconexión del arreglo de elementos de red con la red de datos, se realiza con la elección de un NE el cual tendrá la capacidad de conocer la ubicación y de alcanzar a sus vecinos de área. Tales dispositivos son llamados *Gateways Network Elements* (GNE), contando con dos de ellos por arreglo para efectos de redundancia en al acceso a la red de datos. Cada GNE sólo puede atender a un número determinado de NEs de su propia área, y depende tanto del fabricante, como del sistema de gestión utilizado. Adicionalmente, la comunicación de los GNE con la DCN puede estar basada en direccionamiento estático o dinámico de CLNP.

El intercambio de la información de monitoreo y administración de los NEs con su sistema gestor dentro del anillo, se realiza mediante la trama de SDH. Dentro de esta trama se encuentran los campos D1,D2 y D3 que son los responsables de transportar esta información. Cuando la información llega al GNE este la envía a través de la red de datos hacia el sistema de gestión. Una vez que se identifica al NE y se establece la comunicación con el sistema de gestión, se igualan las bases de datos del NE y del sistema de gestión para que la información sea la misma en ambos extremos. Finalmente el elemento será censado regularmente por el sistema para recopilar sus "signos vitales" y de esta forma cualquier problema que se presente se reflejará en el sistema de gestión prácticamente en tiempo real.

Como ya se mencionó, el sistema de gestión de elementos SDH, trabaja mediante un esquema centralizado, visualizando esta información a través de estaciones de trabajo o de PCs bajo un ambiente gráfico detallado de la red y de los equipos que ofrece un software de emulación de terminal. Por lo general se utiliza el protocolo TCP/IP para la comunicación entre el servidor de gestión y las terminales de usuario en un ambiente de red local. De esta manera se logra un control pleno de cada elemento de la red.

Las principales funciones que el sistema de gestión realiza se pueden resumir en la siguiente lista:

- La configuración del equipo, de sus recursos de transmisión, de sus puertos.
- Visualización del estado de gestión de cada elemento.
- La gestión de alarmas y fallas:
    - Indicación de alarmas en vista de alto nivel,
    - Despliegue gráfico del estado de las alarmas en los elementos de la red,
    - Lista activa de alarmas,
    - Almacenamiento de registros en bitácoras.
- Gestión del *software* del elemento de red.

Para el caso particular de la presente propuesta de diseño, la residencia de todo un sistema de gestión, servidor y terminales de usuario, será dentro de un nodo de acceso especial (el cual se detalla mas adelante), ofreciendo ventajas de mayor velocidad en la interconexión con la red de datos y redundancia tanto en enlaces como en equipos de enrutamiento y de conmutación de capa 2.

5.1.3 Políticas de operación y crecimiento de la red de datos

Adicional a la estructura y operación de una red de datos, es fundamental contar con ciertas reglas que regulen el funcionamiento y crecimiento de esta con base en los intereses propios de la empresa y permitiendo una fácil adaptación de la red a las nuevas tecnologías y servicios. La red de datos en la que operará la propuesta de diseño de la presente tesis, no es la excepción, por lo que en la presente sección se establecen las políticas de operación y crecimiento de la red corporativa multiservicios. A continuación se listan las políticas usadas en esta red:

Políticas de operación

De organización empresarial

- La red dará servicios de transporte de datos a las aplicaciones y servicios propios de la empresa.
- La estructura física de la red será basada en un modelo jerárquico de tres niveles, contando con redundancia tanto en equipos como de enlaces en todos sus niveles.
- La forma de organización de la red será regional, siendo definidas estas por la empresa de acuerdo a su operación y requerimientos.
- La implantación de nuevas tecnologías y servicios requerirá de un análisis y pruebas de funcionamiento previo, así como de la definición de un proceso de implementación.
- Cualquier modificación de las presentes políticas podrán realizarse siempre y cuando sean en mejora de la operación de la red o por decisiones a nivel dirección.

De equipos

- La elección de equipos para los esquemas de red WAN y LAN deberá basarse sobre estándares vigentes, así como en el desempeño y valor agregado de los equipos seleccionados.
- La elección de los equipos requeridos para cada unos de los niveles que estructuran la red, se basará en las políticas de crecimiento de equipos.
- Las redes locales deberán estar integradas por switches de capa 2 y evitar la utilización de *hubs*, repetidores ó *bridges*.
- El número de versiones de sistemas operativos empleadas en los enrutadores y switches de la red podrán ser hasta 5, a fin de reducir el número de variables durante situaciones de falla.

De la red

- Solo se podrá utilizar el protocolo IP para la operación de la red.
- Si se requiere el uso de otros protocolos de capa de red, estos deberán ser encapsulados en IP en los niveles de acceso de la jerarquía de la red para su transporte a través de los niveles de distribución y dorsal.
- El protocolo de enrutamiento IP a emplearse en la red será EIGRP.
- El número de red empleado será una red clase A (10.0.0.0), con máscara de red 255.0.0.0
- El direccionamiento aplicado en la red deberá ser jerárquico realizando subredes y usando el concepto de sumarización.

De administración

- Deberá contarse con un grupo de personas encargados del monitoreo de la red y la atención a fallas de primer nivel las 24 hrs. los 365 días del año.
- Se contará con un grupo de trabajo para la administración de equipos y enlaces propios de la red.
- Deberá contarse con un grupo de personas encargados la atención a fallas de segundo nivel en el momento que sea requerido.
- Se deberán realizar funciones de planeación de la capacidad de la red, con el fin de asegurar el óptimo funcionamiento de la red.

Políticas de crecimiento

De Enlaces

Estas políticas se basan en el manejo de dos tipos de umbrales, los cuales se explican a continuación:

Umbral de advertencia. Se define como el valor promedio de tráfico sobre un enlace durante una semana, que al ser alcanzado indicará que este entrará en etapa de observación. Para fines prácticos, se considera que el enlace no tiene saturación moderada si el tráfico cursante no ha llegado al umbral de advertencia.

Umbral de crecimiento inmediato. Se define como el valor promedio de tráfico sobre un enlace durante una semana, que al ser alcanzado indicará que este requerirá de crecimiento inmediato. Para fines prácticos, se considera que el enlace tiene saturación alta si el tráfico cursante ha llegado al umbral de crecimiento.

Enlaces entre dorsales

Para este caso se considera:

- Umbral de advertencia: 35 % de ocupación del enlace
- Umbral de crecimiento: 40 % de ocupación en el enlace

Lo anterior se basa en el caso de falla de alguno de los enlaces de la dorsal, ya que el tráfico deberá ser redireccionado y consecuentemente cargando los enlaces de la nueva trayectoria. Suponiendo que todos los enlaces de la dorsal se encontraran al 40 % de su ocupación (umbral de crecimiento) y un cierto enlace tuviera que respaldar a un enlace que ha quedado fuera de operación, el primero tendría que soportar un 40 % adicional (si ambos enlaces son de la misma capacidad) esto nos daría un total del 80% de ocupación del enlace, el 20% restante sirve como de margen de crecimiento, que permitirá soportar el incremento de tráfico que se dé en la red mientras se toman las acciones necesarias y mantendrá bajos los tiempos de respuesta de este nivel. Este margen del 20 % es muy importante dada la importancia de la dorsal para la operación de la red.

Enlaces dorsal-distribución, distribución-distribución y dorsal-accesos especiales

Para este caso se considera:

- Umbral de advertencia: 40 % de ocupación del enlace
- Umbral de crecimiento: 45 % de ocupación del enlace

En caso de falla de alguno de los dos enlaces que interconectan a un nodo distribuidor con el nivel dorsal el enlace que aún este en operación deberá soportar su propio tráfico y el del otro enlace. En caso de que ambos enlaces hubieran alcanzado su umbral de crecimiento, el enlace que soportaría todo el tráfico del nodo distribuidor estaría ocupado al 90 % de su capacidad, lo que nos da un margen de crecimiento del 10 % contra incrementos en la cantidad de tráfico cursado a por el mismo enlace durante el tiempo que tardará en implementarse una solución.

Enlaces entre acceso y distribución

Para este caso se considera un solo enlace sin redundancia con los siguientes umbrales:

- Umbral de advertencia: 65 % de ocupación del enlace
- Umbral de crecimiento: 75 % de ocupación del enlace

Dado que los accesos tienen una sola conexión al nivel de distribución, no hay forma de que pudieran ser enlaces de tránsito de otros, por lo que si este quedara fuera de operación su propio tráfico tampoco tiene posibilidad de tomar rutas alternas. Por ello se soporta un umbral de crecimiento mayor en estos enlaces.

Existe la posibilidad de que en el nodo de acceso afectado se corra alguna aplicación que vea afectado negativamente su desempeño al aumentar la ocupación del enlace, inclusive antes de llegar al 65 %, este hecho sería un catalizador para llevar a cabo un crecimiento en la capacidad de este enlace.

De Equipos

Las decisiones de crecimiento y sustitución de equipos se basan en las siguientes consideraciones:

- Incremento en el número de nodos de acceso conectados a los nodos distribuidores
- Incremento del volumen de tráfico en los enlaces
- Soporte de nuevas funcionalidades y tecnologías requeridas para nuevos servicios
- Terminación del tiempo de vida del equipo
- Requerimiento de un mayor desempeño en los equipos

El esquema general de crecimiento de equipos para cada nivel se muestra a continuación, pero cabe aclarar que cada caso debe analizarse de manera puntual.

Crecimiento de equipo Dorsal y distribución		
Modelo actual	**Necesidad**	**Equipo sustituto**
Cisco 7507	Densidad de puertos E1	Cisco 7513
	Densidad de puertos STM-1	Cisco 12012
	Desempeño	Cisco 12012
	Fin de su tiempo de vida	Cisco 12012
Cisco 7513	Densidad de puertos E1	Cisco 12012
	Densidad de puertos STM-1	Cisco 12012
	Desempeño	Cisco 12012
	Fin de su tiempo de vida	Cisco 12012
Crecimiento de equipo de acceso		
Modelo actual	**Necesidad**	**Dispositivos sustitutos**
Cisco 3620	Capacidad de puertos Soporte de nuevas tecnologías y funcionalidades Fin de su tiempo de vida	Cisco 3640
Cisco 3640		Cisco 3660
Cisco 3660		Cisco 7507

Tabla 5.7 Plataformas de equipos elegidas para crecimiento.

5.2. Análisis y propuesta del diseño de la "red virtual CLNS"

La presente sección explica los requisitos generales, el análisis y la propuesta de diseño que permiten dar solución a la necesitad de transportar la información de gestión de los elementos SDH hacia su sistema de gestión centralizado, utilizando la infraestructura de la red que ya se tiene en operación. Es importante definir que se denominará como "aplicación" al conjunto de elementos SDH, junto con su sistema de gestión, y que son pertenecientes al mismo proveedor de equipo. Finalmente la presente solución satisface el transporte de tráfico de más de una aplicación dentro de la red corporativa multiservicios.

5.2.1 Requisitos de la propuesta de diseño

Para poder otorgar el servicio de transporte de información de gestión de los elementos SDH se deben cumplir ciertos requisitos, los cuales son listados a continuación:

- Aprovechar la infraestructura de transporte de datos que actualmente se tiene en operación con el fin de no generar grandes costos de inversión.
- Respetar las políticas de operación de la red de datos al implementar la solución.
- Considerar las recomendaciones de los proveedores de equipos para el uso de estos.
- El diseño debe permitir un fácil crecimiento de las aplicaciones a las que se dará el servicio, y una integración sencilla de aquellas que se requieran en un futuro.
- Deberá proporcionarse el servicio de transporte donde sea requerido.
- La solución dará servicio de manera general a todas las aplicaciones que así lo requieran.
- El servicio deberá ser confiable y de una alta disponibilidad.

Con base en los requisitos listados anteriormente, en los criterios de diseño de una red de datos del capítulo 4, y en los aspectos de la red de datos descritos en la sección 5.1 del marco inicial de diseño, a continuación se describe el análisis desarrollado para lograr la propuesta de diseño.

5.2.2 Análisis del servicio

El servicio de transporte de la presente propuesta, se concibe de acuerdo a las características que tienen en común las aplicaciones. En el contexto de la tesis estas características fueron analizadas para equipos marca Alcatel, Ericsson, Nortel y Nec, los cuales fueron elegidos por la empresa ya que cumplen con los requerimientos definidos por la misma. La lista de las aplicaciones beneficiadas con la propuesta se muestra a continuación:

APLICACIÓN	COBERTURA
TN1X/TNMS-NACIONAL NORTEL	NACIONAL
1353SH/1354/RM-NACIONAL ALCATEL	NACIONAL
1353NX-NACIONAL ALCATEL	NACIONAL
ETNA-NEM-1 ERICSSON	REGION 1
1353SH/1354/RM-1 ALCATEL	REGION 1
PRESIDE-1 NORTEL	REGION 1
INC-100-1 NEC	REGION 1
ETNA-NEM-2 ERICSSON	REGION 2
1353SH/1354/RM-2 ALCATEL	REGION 2
ERION-2 ERICSSON	REGION 2
TN1X/TNMS-2 NORTEL	REGIÓN 2
INC-100-3 NEC	REGION 3
ETNA-NEM-4 ERICSSON	REGION 4
1353SH/1354/RM-4 ALCATEL	REGION 4
PRESIDE-4 NORTEL	REGION 4
INC-100-5 NEC	REGION 5
INC-100-6 NEC	REGION 6
INC-100-7 NEC	REGION 7
ETNA-NEM-7 ERICSSON	REGION 7
PRESIDE-7 NORTEL	REGION 7
PRESIDE-8 NORTEL	REGION 8
1353SH/1354/RM-8 ALCATEL	REGION 8
ETNA-NEM-8 ERICSSON	REGION 8
TN1X/TNMS-56 NORTEL	REGIÓNES 5 Y 6
TN1X/TNMS-78 NORTEL	REGIÓNES 7 Y 8

Tabla 5.8 Aplicaciones de gestión y su cobertura.

Las aplicaciones anteriormente listadas, cuentan con las siguientes características en común:

- Están constituidas por elementos de transporte SDH, los cuales son gestionados en forma centralizada a través de un sistema particular.
- Los elementos SDH están conformados en anillos y/o *buses* ya sea a escala nacional o regional, y tienen asignada un área CLNS única por arreglo, así como para su centro o sistema de gestión.
- Los anillos, *buses* y sistemas de gestión, por estar dispersos de manera nacional y regional requieren de una comunicación remota entre si.
- La comunicación e interacción entre las diferentes aplicaciones de gestión no existen, por lo que pueden considerarse independientes.
- Pueden existir sitios donde se tengan dos o más áreas de diferentes aplicaciones, es decir, que dos anillos o buses de elementos SDH que dan servicio a diferentes zonas y que son de diferentes aplicaciones tengan como interconexión a la red de datos el mismo enrutador de acceso.
- Todas las aplicaciones trabajan bajo el mismo protocolo de capa de red, CLNP.

Topología de las aplicaciones

La topología de cada aplicación es en todos los casos del tipo estrella, en donde su centro es el sistema de gestión y en los extremos se encuentran los elementos SDH que se van a gestionar bajo arreglos en anillo, o en *bus*. La figura 5.7 muestra un ejemplo de esta topología.

Existen anillos y buses de elementos SDH que por su tamaño tienen más de una conexión hacia su sistema de gestión, lo anterior permite asegurar la comunicación en caso de fallar una de las interconexiones a la red de datos.

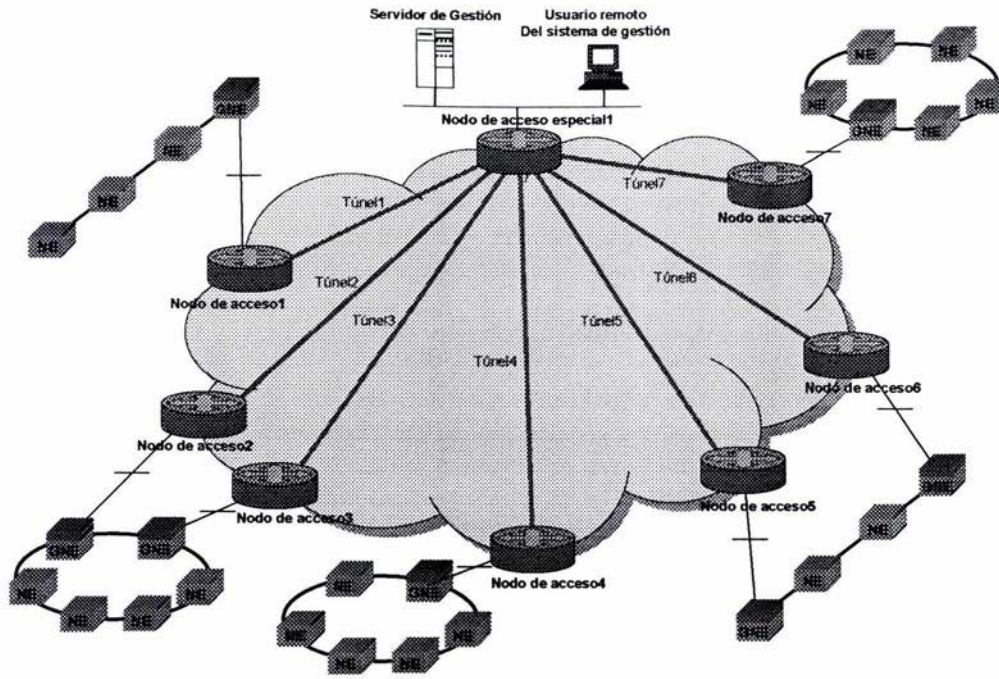

Figura 5.7 Topología típica de una aplicación de gestión.

Protocolo de enrutamiento

Las aplicaciones de gestión utilizadas pueden dividirse en dos grupos, de acuerdo a los protocolos de enrutamiento usados:

- **Aplicaciones con enrutamiento dinámico**. Son aquellas que trabajan con el protocolo de enrutamiento IS-IS de nivel 1, dentro de cada área (cada anillo, *bus* y sistema de gestión tiene un área asignada), y de nivel 2 para la comunicación entre áreas diferentes (por ejemplo: la comunicación del sistema de gestión con los elementos SDH de cada anillo o área).
- **Aplicaciones con enrutamiento estático**. Para el caso particular de la presente tesis, la aplicación 1353NX es la única que trabaja bajo un esquema de enrutamiento ISO estático.

Direccionamiento CLNP

El esquema de direccionamiento para las aplicaciones bajo el protocolo CLNP será respecto a cada una de ellas. Es decir, se asignará un valor diferente de la parte de dominio a cada aplicación, y se repartirá de manera consecutiva la parte de área a cada grupo anillo o bus de elementos SDH o de servidores de gestión como se indica a continuación:

APLICACIÓN	Parte de DOMINIO	Parte de AREA (rango)
TN1X/TNMS-NACIONAL NORTEL	0001	0001 - FFFE
1353SH/1354/RM-NACIONAL ALCATEL	0002	0001 - FFFE
1353NX-NACIONAL ALCATEL	0003	0001 - FFFE
ETNA-NEM-1 ERICSSON	0004	0001 - FFFE
1353SH/1354/RM-1 ALCATEL	0005	0001 - FFFE
PRESIDE-1 NORTEL	0006	0001 - FFFE
INC-100-1 NEC	0007	0001 - FFFE
ETNA-NEM-2 ERICSSON	0008	0001 - FFFE
1353SH/1354/RM-2 ALCATEL	0009	0001 - FFFE
ERION-2 ERICSSON	000A	0001 - FFFE
TN1X/TNMS-2 NORTEL	000B	0001 - FFFE
INC-100-3 NEC	000C	0001 - FFFE
ETNA-NEM-4 ERICSSON	000D	0001 - FFFE
1353SH/1354/RM-4 ALCATEL	000E	0001 - FFFE
PRESIDE-4 NORTEL	000F	0001 - FFFE
INC-100-5 NEC	0010	0001 - FFFE
INC-100-6 NEC	0011	0001 - FFFE
INC-100-7 NEC	0012	0001 - FFFE
ETNA-NEM-7 ERICSSON	0013	0001 - FFFE
PRESIDE-7 NORTEL	0014	0001 - FFFE
PRESIDE-8 NORTEL	0015	0001 - FFFE
1353SH/1354/RM-8 ALCATEL	0016	0001 - FFFE
ETNA-NEM-8 ERICSSON	0017	0001 - FFFE
TN1X/TNMS-56 NORTEL	0018	0001 - FFFE
TN1X/TNMS-78 NORTEL	0019	0001 - FFFE

Tabla 5.9 Asignación de áreas CLNP por aplicación

Si el rango de la parte de área de alguna aplicación fuera agotado, se deberá asignar tanto una nueva parte de dominio como un nuevo rango de la parte de área de manera consecutiva.

La estructura final del direccionamiento se ejemplifica a continuación:

47.0005.8000.0000.0000.*DOMINIO.AREA. IDENTIFICADOR.DEL.SISTEMA*.00
Parte inicial del dominio Parte especifica del dominio

Los valores de la parte de dominio y área 0000 y FFFF serán reservados para efectos de crecimiento del nivel dorsal de la "Red virtual CLNS".

Flujos de tráfico

El flujo de información de todas las aplicaciones se desempeña de manera centralizada, es decir, los elementos gestionados tienen comunicación directa a sus sistemas de gestión, por lo tanto, el único tipo de flujo de tráfico es el que existe entre los anillos y *buses*, con el sistema de gestión respectivo. No existe comunicación entre aplicaciones, entre sistemas de gestión, o entre *buses* y anillos con sistemas de gestión de aplicaciones diferentes.

Políticas de implementación de protocolos sobre la Red Corporativa

De acuerdo a las políticas de operación descritas en la sección 4.1.3, se establece el uso del protocolo IP como el único a ser enrutado sobre la Red Corporativa, por lo que los protocolos CLNP e IS-IS en sus dos niveles deberán ser encapsulados. Este encapsulamiento se realizará a través de circuitos lógicos, o túneles que son configurados entre los enrutadores de interés formándose de esta manera la red virtual.

5.2.3. Propuesta del diseño

La presente sección describe en dos partes la propuesta de diseño realizada en esta tesis: El esquema de interconexión WAN y el esquema de interconexión LAN. Así mismo se explica el proceso de implementación del diseño y las actividades posteriores a la implementación del diseño que permiten optimizar al servicio de transporte.

Esquema de interconexión WAN

La propuesta de diseño, que en lo subsiguiente se le denominará como "red virtual CLNS", se describe a continuación bajo los siguientes puntos:

- Modelo de red.
- Topología.
- Protocolo de enrutamiento.
- Procesos de enrutamiento IS-IS.
- Flujos de tráfico.
- Direccionamiento.
- Versión IOS a emplear.

Modelo de red

El modelo de red empleado se basa en el enrutamiento jerárquico IS-IS en sus dos niveles: IS-IS nivel 1 (intra área) e IS-IS nivel 2 (inter área).

El nivel 1 del enrutamiento IS-IS permite la comunicación de los elementos SDH con el enrutador de acceso de la red de datos ya que todos estos pertenecen a una misma área. Una vez que la información de gestión se encuentra en el enrutador de acceso, esta se reenviará hacia el área donde se encuentra el sistema de gestión correspondiente mediante el uso del protocolo de enrutamiento IS-IS de nivel 2. Las solicitudes de información provenientes del sistema de gestión serán enviadas de la misma forma, es decir, haciendo uso de los niveles 1 y 2 del protocolo de enrutamiento IS-IS.

Es importante tomar en cuenta que en el nivel 2 se conocen todas las áreas de nivel 1 de todas las aplicaciones de gestión de elementos SDH. El modelo de red empleado se muestra en la siguiente figura:

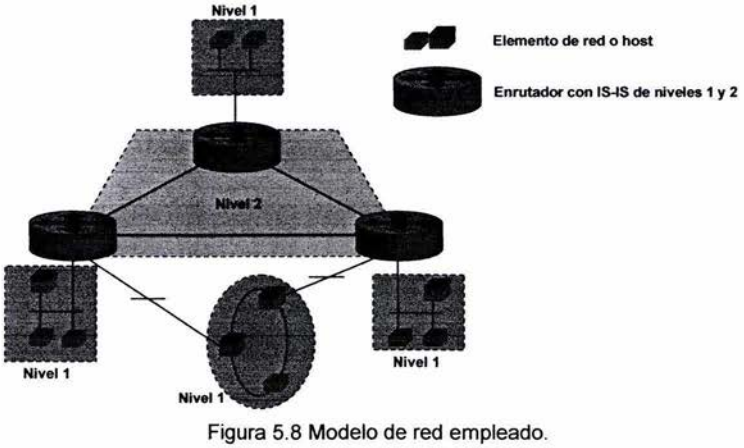

Figura 5.8 Modelo de red empleado.

Topología

La siguiente figura muestra la topología lógica de la "Red virtual de CLNS":

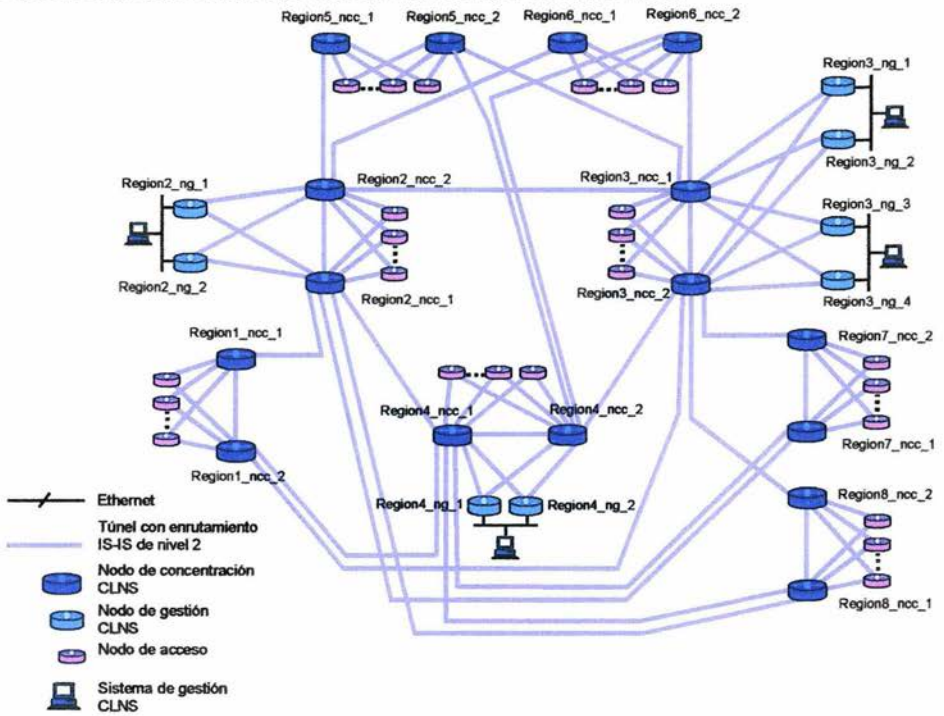

Figura 5.9 Topología lógica de la "red virtual CLNS"

La "red virtual CLNS" se estructura bajo una jerarquía de dos niveles llamados: "Dorsal" y de "acceso", así como por los tipos de nodos que los conforman: "nodos de acceso" para el nivel de acceso, "nodos de concentración CLNS" y "Nodos de Gestión CLNS" para el nivel "dorsal", los cuales tienen las siguientes características:

- Nodos de acceso. Proporcionan la conexión de los elementos SDH mediante un puerto de red local (802.3) con la red de datos. Pueden concentrar más de un grupo de elementos SDH por puerto de red local y de diferentes aplicaciones. Su interconexión con el resto de la "Red virtual CLNS" es con los dos "nodos de concentración CLNS" pertenecientes a su región.

- Nodos de concentración CLNS. Agrupa a los "nodos de acceso" con aplicaciones de CLNS y para algunos casos, a los "nodos de gestión". Por cuestiones de redundancia se tienen dos de estos por región y a su vez se encuentran interconectados con otros NCCs de otras regiones

- Nodos de Gestión CLNS. En ellos se encuentran resguardados los sistemas de gestión SDH basados en CLNP. Utilizan un esquema seguro de interconexión física a nivel LAN y se encuentran interconectados con los "nodos de concentración CLNS" de la Divisional correspondiente.

La interconexión entre todos los nodos que forman parte de la "Red virtual CLNS" es mediante circuitos lógicos o túneles, los cuales encapsulan en IP la información de gestión basada en CLNP e IS-IS. La implementación de estos túneles son creados mediante interfaces lógicas o *loopbacks*, las cuales proporcionan una mayor disponibilidad en el servicio

Es importante observar de la figura 5.9 que los "nodos de concentración CLNS" o NCC son interconectados formando deltas entre diferentes divisionales, siendo la delta principal, o dorsal, la formada entre las regiones 1, 2 y 4, ya que en estas se concentran todos los sistemas de gestión SDH y por contar en estos lugares con una alta disponibilidad bajo las siguientes características:

- Capacidad en troncales digitales
- Esquema confiable de seguridad de acceso físico a la central
- Alta disponibilidad de energía eléctrica
- Concentración directa de enlaces de larga distancia

Cabe señalar que este diseño soporta de manera sencilla la reubicación de los sistemas de gestión CLNS o de los nodos de acceso en caso de que así se requiriera, ya que las modificaciones se realizarían de manera lógica, es decir modificando configuraciones de los enrutadores en cuestión.

El criterio de agrupación de los nodos de acceso y de gestión para cada región se hará de acuerdo al siguiente criterio:

Nombre de Región	Nodos de concentración CLNS
Región 1	region_1_ncc_1 región_1_ncc_2
Región 2	region_2_ncc_1 región_2_ncc_2
Región 3	region_3_ncc_1 región_3_ncc_2
Región 4	region_4_ncc_1 región_4_ncc_2
Región 5	region_5_ncc_1 región_5_ncc_2
Región 6	region_6_ncc_1 región_6_ncc_2
Región 7	region_7_ncc_1 región_7_ncc_2
Región 8	region_8_ncc_1 región_8_ncc_2

Tabla 5.10 Nombre de los NCCs por región.

La topología física en la que se monta la "Red virtual CLNS" se muestra en la siguiente figura:

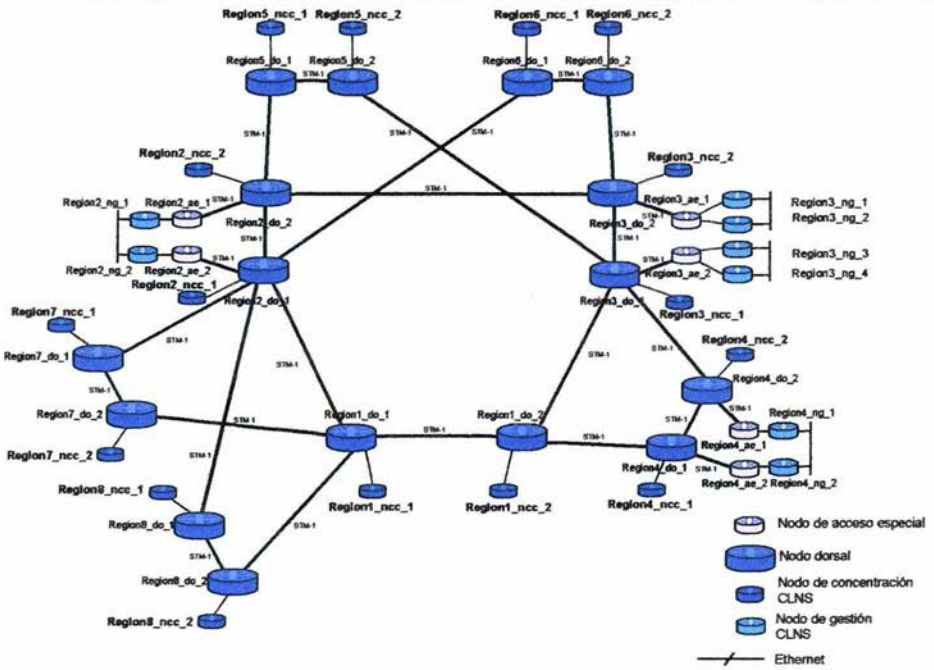

Figura 5.10 Topología física de la red de datos donde se "monta" la red virtual CLNS

Protocolos de enrutamiento

Los protocolos de enrutamiento a usarse en la "Red virtual CLNS" son los siguientes:

- IS-IS NIVEL 1. Utilizado dentro de cada área para la comunicación de los elementos SDH con el "nodo de acceso".
- IS-IS NIVEL 2. Empleado para la comunicación entre áreas, específicamente entre las áreas de los elementos SDH y su sistema de gestión. Este enrutamiento es aplicado en los túneles que interconectan a las diferentes áreas.
- ESTÁTICO. La aplicación 1353NX NACIONAL ALCATEL trabaja con enrutamiento estático, por lo cual este será empleado y redistribuido al protocolo IS-IS de nivel 2 para su comunicación.

Flujos de tráfico

El flujo de los datos se realizará de una forma jerárquica, es decir, la información proveniente de los elementos gestionados de SDH será recopilada por los nodos de acceso y posteriormente agrupada en los nodos de concentración correspondientes de su región. Finalmente los datos serán transportados hacia su nodo gestor.

Los dos flujos principales de información sobre la red son:

- Tráfico intra-divisional. Los datos provenientes de una divisional serán enviados a los sistemas de gestión pertenecientes a la misma.
- Tráfico Inter-divisional. Los datos provenientes de una divisional serán enviados a los sistemas de gestión situados fuera de ella.

Cabe mencionar que la presente propuesta está preparada para la transferencia de información entre cualquier área, usando la red dorsal en caso de que alguna aplicación futura así lo requiera.

Direccionamiento

El direccionamiento empleado será el mismo que está definido en el punto direccionamiento CLNP de la sección 4.2.2 Análisis de servicio.

Versión IOS a utilizar

La versión de sistema operativo IOS empleada para los enrutadores usados en la propuesta de diseño es la 12.0(7)T *Enterprise*, y la versión 12.1(1)T *Telco Enterprise* para los modelos 3660, ya que soportan los requisitos tanto para la red de datos multiservicios, como para la "Red virtual de CLNS".

Políticas y recomendaciones de conexión y crecimiento

Con el objeto de mantener una topología sencilla, eficiente y flexible para el crecimiento futuro de la "red virtual CLNS", es importante que se cumplan las siguientes políticas y recomendaciones:

- Crecimiento de áreas. Se recomienda que el número máximo de NEs del arreglo correspondiente a un área sea de acuerdo las siguientes recomendaciones:

Proveedor	Elementos por área
Alcatel	50
Ericsson	50
Nortel	50
Nec	50

Tabla 5.11 Recomendación del número de elementos por área.

Una vez que sea alcanzado el número máximo de NEs del área en cuestión y sea imperante su crecimiento, deberá realizarse la creación de una nueva área como vía de crecimiento.

- Áreas por enrutador. El número máximo de áreas soportadas por enrutador será 12 de nivel 1 y una de nivel 2.

- Crecimiento de enrutadores por número de áreas. Si un enrutador alcanza un nivel de procesamiento del 50% o tiene el número máximo de áreas, se instalará un nuevo enrutador y se conectará de acuerdo a la secuencia de la figura 5.11 como parte del crecimiento:

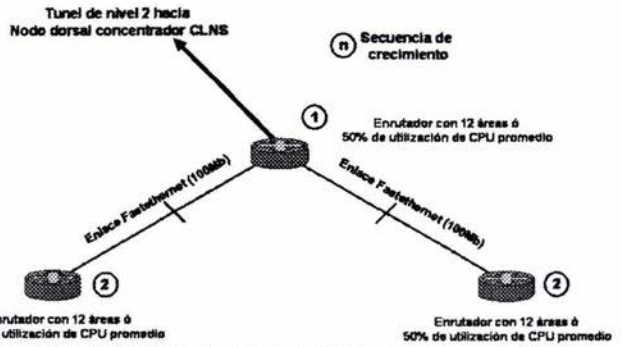

Figura 5.11 Crecimiento de enrutadores por número de áreas

La selección del enrutador nuevo dependerá de la capacidad de soportar la versión IOS 12.0(7)T o superior, de la cantidad y tipo de puertos requeridos para la conexión de áreas y enrutadores.

- **Interconexión de nodos de acceso y de gestión**. Estos nodos tendrán un túnel con enrutamiento IS-IS de nivel 2 hacia cada uno de sus "nodos concentradores CLNS" de la región, no importando el número de aplicaciones CLNS que este tenga conectado.

- **Redundancia de acceso al área debido a partición de esta o por falla en su interconexión**. Con objeto de dar redundancia al área en caso de fallas en el puerto de red local, o debido a que el anillo o *bus* quedara dividido en dos segmentos, los enrutadores que sean acceso de esa misma área serán interconectados entre sí a través de un túnel con enrutamiento IS-IS de nivel 1.

Esquema de interconexión LAN

Las aplicaciones de gestión de los diferentes proveedores comparten una estructura de interconexión muy similar, la cual se puede resumir en los siguientes puntos:

- Plataforma de operación
- Protocolos
- Interacción con los usuarios locales y remotos
- Integración a la DCN.

A continuación se describen cada uno de estos puntos:

Plataforma de operación

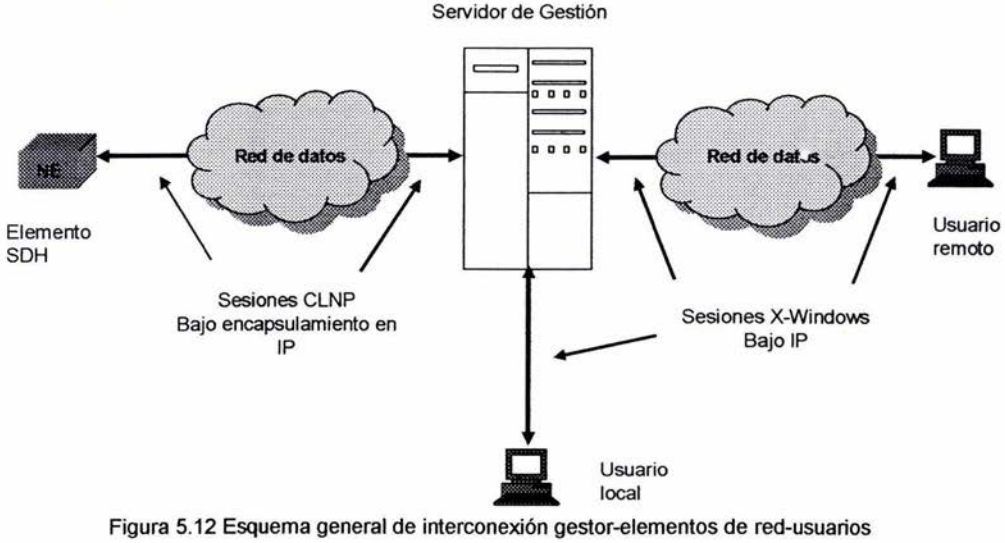

Figura 5.12 Esquema general de interconexión gestor-elementos de red-usuarios

La figura anterior muestra una conexión típica entre el servidor de gestión, un elemento de red y el usuario que opera la gestión de estos elementos. En los servidores de gestión o gestores reside el sistema de gestión en si y la base de datos del mismo donde se guarda la información de todos los elementos gestionados. Estos servidores son accesados por usuarios en forma remota o local para consultar, configurar y supervisar a los elementos de red.

Protocolos

La manera en como se logra establecer la conectividad entre usuarios y elementos es mediante el uso de los protocolos IP y CLNP para todas las aplicaciones de gestión.

Usuarios locales y remotos

La comunicación existente de los usuarios de gestión con los elementos de red, se puede dividir en dos partes:

- Comunicación Elemento de red-Gestor. Esta es a través del protocolo CLNP de punto a punto (totalmente remota), es decir los elementos de red no se encuentran en el sitio del gestor.
- Comunicación Gestor-Usuario. Se lleva a cabo a través de TCP/IP y establece comunicación local y/o remota hacia los usuarios de la aplicación de gestión.

Integración a la DCN

La conexión más sencilla entre los gestores y enrutadores de la red de datos es aquella que es directa a través de una conexión de red local tipo 802.3/*Ethernet*. La figura 5.13 representa este esquema típico de integración:

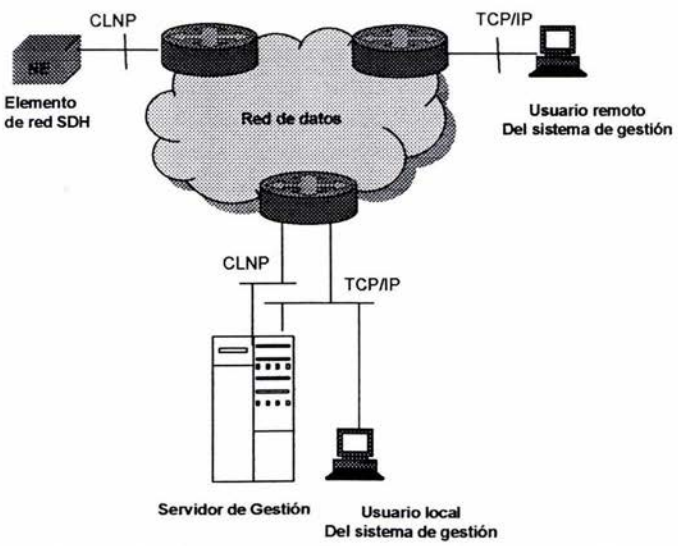

Figura 5.13 Esquema general de integración de gestores SDH

Debido a la importancia de estos elementos de red, es imperante tener una alta disponibilidad para mantener siempre la comunicación entre los elementos de red, los servidores de gestión y usuario de gestión, por lo que el esquema de la figura 5.13, no es el indicado al no contar con un esquema de redundancia, para situaciones de falla de un enlace o de un enrutador de interconexión con la red de datos. Para solventar esta falta de continuidad en el servicio se consideran en la propuesta de diseño dos esquemas para la integración de los servidores de gestión y los elementos de red SDH: por un lado tendremos la topología para los gestores y por el otro se tendrá la topología de integración de elementos de red y usuarios. Los usuarios de gestión también serán interconectados mediante un esquema seguro igual al implementado para los gestores. El esquema para la red de datos ya se explicó en detalle en la sección de "Esquema de interconexión WAN".

Criterios importantes para el diseño LAN

La infraestructura LAN para los dispositivos que utilizan el protocolo CLNP será a través de conmutadores de capa dos o *switches* LAN dedicados de manera exclusiva al transporte de este protocolo y serán conocidos como "*switches* CLNS", contando con puertos del tipo *Fastethernet*. (100 Mbps de velocidad).

Los usuarios que utilizan el protocolo IP serán interconectados a través de *switches* LAN dedicados también de manera exclusiva para este protocolo y serán conocidos como "*switches* IP", contando con puertos del tipo *Fastethernet* (100 Mbps de velocidad).

Con base en las facilidades de los enrutadores y *switches* LAN, es posible crear subinterfaces de los puertos tipo *FastEthernet* en los enrutadores, asociando estas a diferentes dominios de *broadcast* (*VLANs*) en los *switches* LAN. Considerando estas facilidades se configurarán subinterfaces exclusivas para los protocolos de CLNP e IP en puertos tipo *FastEthernet*.

Para cada subinterfaz creada en los enrutadores, su número de identificación deberá ser el mismo para la VLAN asociada, por ejemplo; la subinterfaz 2 del puerto *Fastethernet* 0/1 (en el enrutador se visualiza como subinterfaz 0/1.2) tendrá asociada la VLAN con número 2. De lo anterior se define que cada una de las aplicaciones, será integrada en una VLAN exclusiva para su operación. La VLAN con número 1 será reservada para efectos de administración de los *switches*, siendo utilizable la numeración de la VLAN 2 en adelante.

Con objeto de facilitar la administración y la atención a fallas, a cada aplicación de gestión se le asignará un número específico de VLAN, no importando si se tiene conectado a los servidores de gestión o arreglos de elementos de red SDH, ni el lugar donde se encuentren. La asignación de los números de VLAN de acuerdo a la aplicación es la siguiente:

APLICACIÓN	Número de VLAN
TN1X/TNMS-NACIONAL NORTEL	1
1353SH/1354/RM-NACIONAL ALCATEL	2
1353NX-NACIONAL ALCATEL	3
ETNA-NEM-1 ERICSSON	4
1353SH/1354/RM-1 ALCATEL	5
PRESIDE-1 NORTEL	6
INC-100-1 NEC	7
ETNA-NEM-2 ERICSSON	8
1353SH/1354/RM-2 ALCATEL	9
ERION-2 ERICSSON	10
TN1X/TNMS-2 NORTEL	11
INC-100-3 NEC	12
ETNA-NEM-4 ERICSSON	13
1353SH/1354/RM-4 ALCATEL	14
PRESIDE-4 NORTEL	15
INC-100-5 NEC	16
INC-100-6 NEC	17
INC-100-7 NEC	18
ETNA-NEM-7 ERICSSON	19
PRESIDE-7 NORTEL	20
PRESIDE-8 NORTEL	21
1353SH/1354/RM-8 ALCATEL	22
ETNA-NEM-8 ERICSSON	23
TN1X/TNMS-56 NORTEL	24
TN1X/TNMS-78 NORTEL	25

Tabla 5.12 Asignación de números de VLAN de administración por gestión.

El tipo de encapsulamiento a utilizar para la asociación de una VLAN con su subinterfaz en cuestión deberá estar basado en el estándar IEEE 802.1q[10]

[10] Para mayor información, consultar la siguiente liga: http://www.marconi.ca/media/vlan100.pdf

Una vez definidos los criterios de diseño, a continuación se explicarán los dos esquemas fundamentales a nivel de acceso que se requieren para resguardar a los servidores de gestión y los elementos de red:

Esquema de red local para los servidores de gestión

La ubicación de los servidores de gestión será dentro de edificios que permiten evitar la interrupción de energía eléctrica y clima cuentan con un estricto acceso a sus salas y diversidad física de caminos para los enlaces de datos que llegan a estos.

La figura 5.14 muestra el esquema empleado para el resguardo de los servidores de gestión y de los usuarios de gestión:

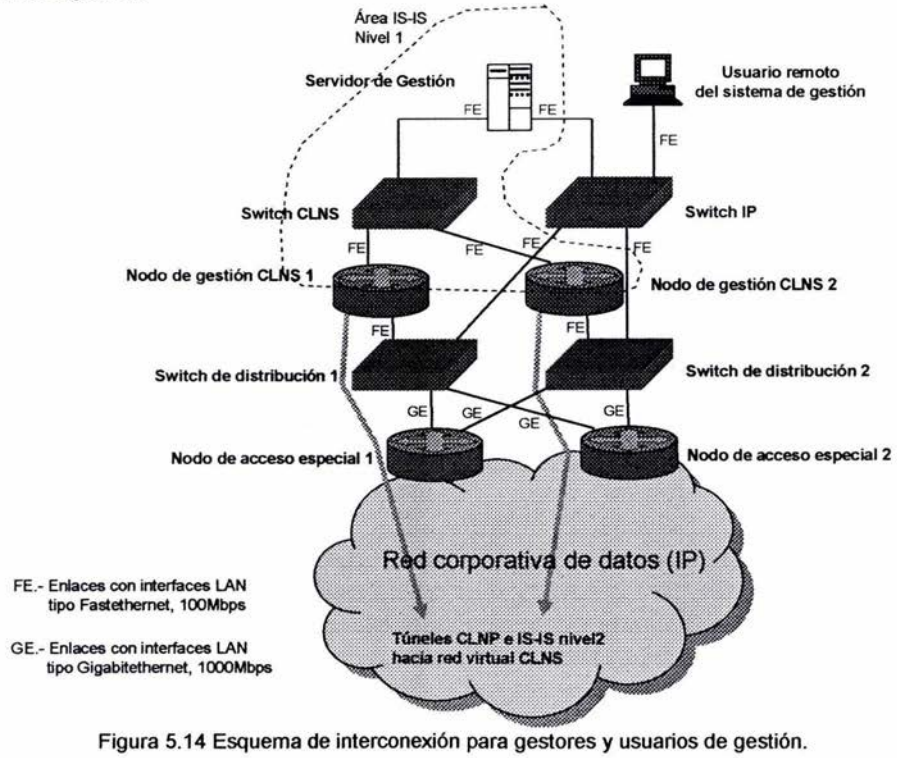

Figura 5.14 Esquema de interconexión para gestores y usuarios de gestión.

De la figura anterior se puede observar la redundancia en enlaces y equipos del esquema de interconexión LAN para el servidor de gestión y usuarios de gestión. Como interconexión directa, se tiene al servidor de gestión conectado de manera separada a través de puertos de red local del tipo *fastethernet* al "*switch* IP" y al "*switch* CLNS". En estos *switches* se tiene asociada una VLAN diferente tanto para la información transportada sobre IP, como por CLNP. En esta parte, los *switches* de IP y CLNP se conectan de manera diferente. Para el caso del CLNP, este *switch* se conecta a dos enrutadores que serán dedicados de manera exclusiva para el transporte de la información de gestión de los elementos SDH en el nivel WAN. Para el "*switch* IP" y los enrutadores de gestión CLNS, tendrían una interconexión a dos *switches* denominados de distribución, los cuales concentrarán a otros (*switches* y enrutadores) que pertenezcan a otras aplicaciones de la empresa.

Finalmente los *switches* de distribución estarán conectados de manera redundante y a través de interfaces de red local *Gigabit ethernet*[11] hacia dos enrutadores que definen la frontera de este nodo de alta seguridad y que son conocidos como accesos especiales. Este tipo de interfaz fue seleccionado, debido a su gran velocidad de transmisión y por operar de manera idéntica al estándar 802.3, ya que en estos enlaces se concentra el tráfico de todas las aplicaciones que residen en los nodos de acceso especial.

Es importante hacer notar que los enrutadores denominados "nodos de gestión CLNS", son los que se encargarán de redistribuir la información de IS-IS de nivel 1 a nivel 2, y de su correspondiente encapsulamiento de la información en CLNP e IS-IS a través de túneles. Para el caso de las aplicaciones de gestión de elementos SDH, la información en IP serán las consultas de los usuarios de gestión al servidor que pueden ser tanto de manera local al nodo, como remota.

Esquema de red local para los elementos de red SDH

La forma de interconexión de los arreglos de elementos SDH con la Red corporativa de datos para su gestión, se muestra en la siguiente figura:

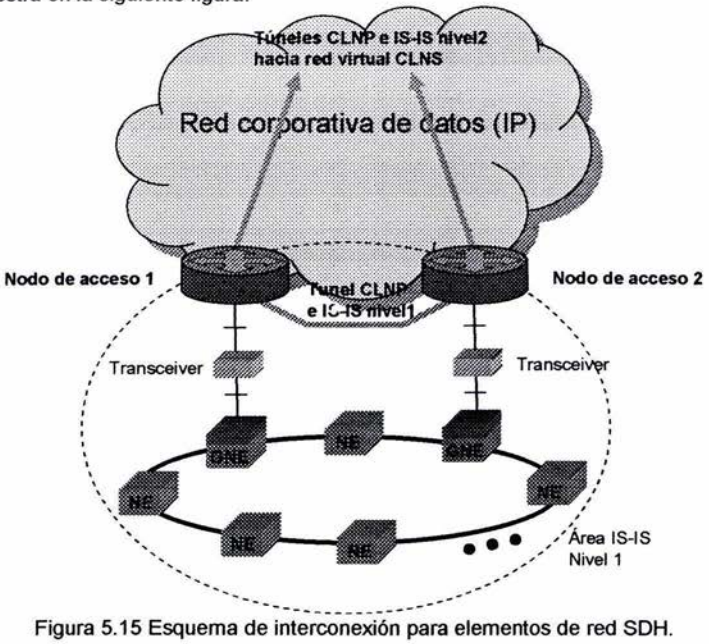

Figura 5.15 Esquema de interconexión para elementos de red SDH.

Debido al número de elementos que conforman estos arreglos, es importante contar con dos interconexiones a la red de datos, como medida de redundancia en caso de falla en alguno de ellos. Estos puntos de interconexión serán a través de interfaces de red local del tipo ethernet/ 802.3 10BaseT del lado del enrutador llamado nodo de acceso y del lado de los elementos de red SDH con interfaces *ethernet*/ 802.3 10Base5. Este tipo de estándar fue elegido por los proveedores de equipo ya que el cable coaxial tiene una mayor resistencia a las interferencias, siendo muchas por razones de temperatura en el equipo. Para poder lograr la interconexión entre estos dos dispositivos, se requerirá del empleo de un "*transceiver*", el cual permite la conversión física y de señalización de capa 1 entre ellos.

La parte lógica de este esquema está formada de la interconexión directa de los dos nodos de acceso a través de un túnel de nivel 1, con el fin de evitar las consideraciones en la redistribución de áreas de nivel

[11] El estándar de esta tecnología es IEEE 802.3ab. El detalle del funcionamiento se encuentra en la siguiente liga: http://www.10gea.org/GEA1000BASET1197_rev-wp.pdf

1 descritas en la sección 3.3.5 "protocolo de enrutamiento IS-IS". Asimismo este esquema permite dar solución a la situación de partición de área, es decir, si se presentara el caso en que el arreglo de elementos de red se fragmentara en dos partes y cada una tuviera salida por un nodo de acceso diferente. Con este túnel de nivel 1 los elementos de red de las dos partes se conocerán en su totalidad en los nodos de acceso, evitando la perdida de comunicación o de información al llegar esta al enrutador de la parte segmentada no correspondiente.

De los esquemas anteriores, en la figura siguiente se presenta de manera integral la forma de interconexión típica de una aplicación de gestión de elementos SDH.

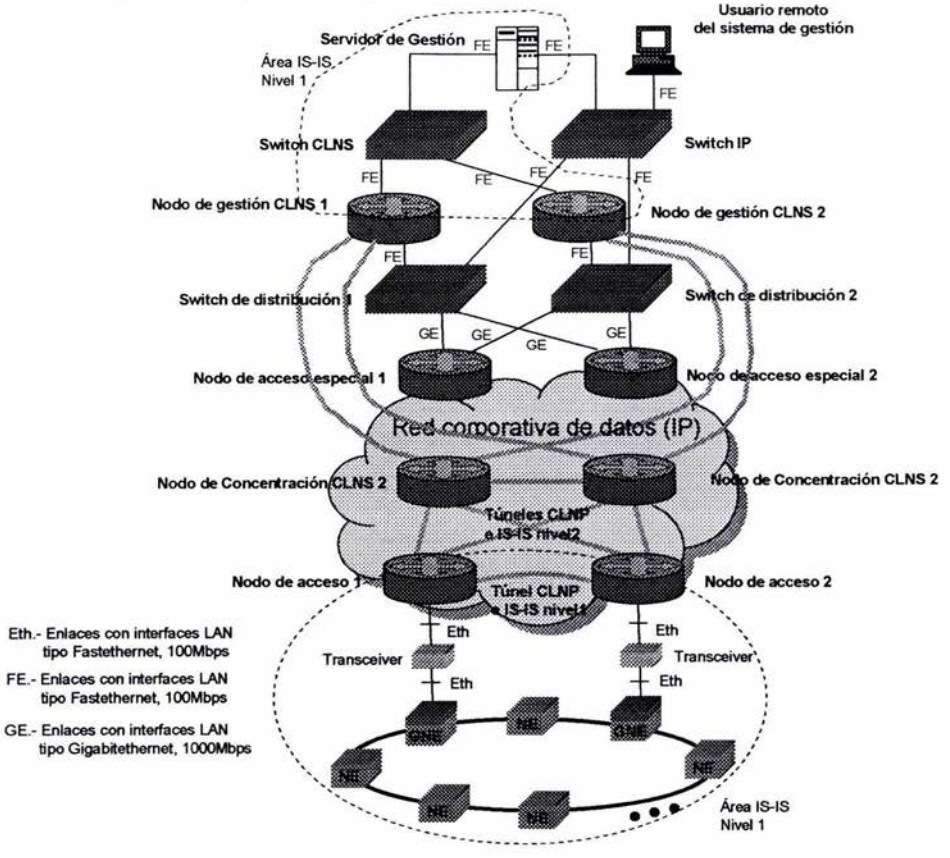

Figura 5.16 Esquema general de interconexión de aplicaciones de gestión SDH.

5.3. Proceso de implementación de la propuesta de diseño de la "red virtual CLNS"

En la presente sección se enlista y proporciona una explicación somera de las etapas que se deberán realizar para la implementación de la "red virtual CLNS". El conjunto de etapas que se deben llevar a cabo son las siguientes:

Secuencia	Etapa
1	Implementación de los esquemas de red local
2	Instalación de los "nodos de concentración CLNS"
3	Implementación del nivel dorsal de la "red virtual de CLNS"
4	Pruebas de enrutamiento y conectividad del nivel dorsal
5	Interconexión de los nodos de gestión al nivel dorsal
6	Prueba piloto de interconexión de accesos a la "red virtual CLNS"
7	Interconexión masiva de los accesos hacia la "red virtual CLNS"
8	Actividades de ajuste fino a la "red virtual CLNS"

Tabla 5.13 Etapas del proceso de migración.

5.3.1. Implementación de los esquemas de red local

Para la implementación de la "red virtual CLNS" nuestro diseño define dos tipos de esquema de red local:

- Esquema de red local para servidores de gestión.
- Esquema de red local para elementos de red SDH.

El esquema de red local para servidores de gestión

Este tipo de esquema es el que se explica en la sección anterior de esquema de interconexión LAN, y será implementado de acuerdo a la disponibilidad de trasladar los actuales sistemas de gestión en operación. La ubicación final de estos sistemas se muestra en la siguiente tabla:

APLICACIÓN	Actual	Ubicación final
TN1X/TNMS-NACIONAL NORTEL	Región 4	Región 4, Región 2
1353SH/1354/RM-NACIONAL ALCATEL	Región 4	Región 4, Región 2
1353NX-NACIONAL ALCATEL	Región 4	Región 4, Región 2
ETNA-NEM-1 ERICSSON	Región 1	Región 3
1353SH/1354/RM-1 ALCATEL	Región 1	Región 3
PRESIDE-1 NORTEL	Región 1	Región 3
INC-100-1 NEC	Región 1	Región 3
ETNA-NEM-2 ERICSSON	Región 2	Región 3
1353SH/1354/RM-2 ALCATEL	Región 2	Región 3
ERION-2 ERICSSON	Región 2	Región 3
TN1X/TNMS-2 NORTEL	Región 2	Región 3
INC-100-3 NEC	Región 3	Región 3
ETNA-NEM-4 ERICSSON	Región 4	Región 3
1353SH/1354/RM-4 ALCATEL	Región 4	Región 3
PRESIDE-4 NORTEL	Región 4	Región 3
INC-100-5 NEC	Región 5	Región 3
INC-100-6 NEC	Región 6	Región 3
INC-100-7 NEC	Región 7	Región 3
ETNA-NEM-7 ERICSSON	Región 7	Región 3
PRESIDE-7 NORTEL	Región 7	Región 3
PRESIDE-8 NORTEL	Región 8	Región 3
1353SH/1354/RM-8 ALCATEL	Región 8	Región 3
ETNA-NEM-8 ERICSSON	Región 8	Región 3
TN1X/TNMS-56 NORTEL	Región 5	Región 3
TN1X/TNMS-78 NORTEL	Región 7	Región 3

Tabla 5.14 Ubicación final de los servidores de gestión.

La interconexión de los sistemas de gestión con los nodos de acceso especial de la red corporativa de datos se muestra en la siguiente figura:

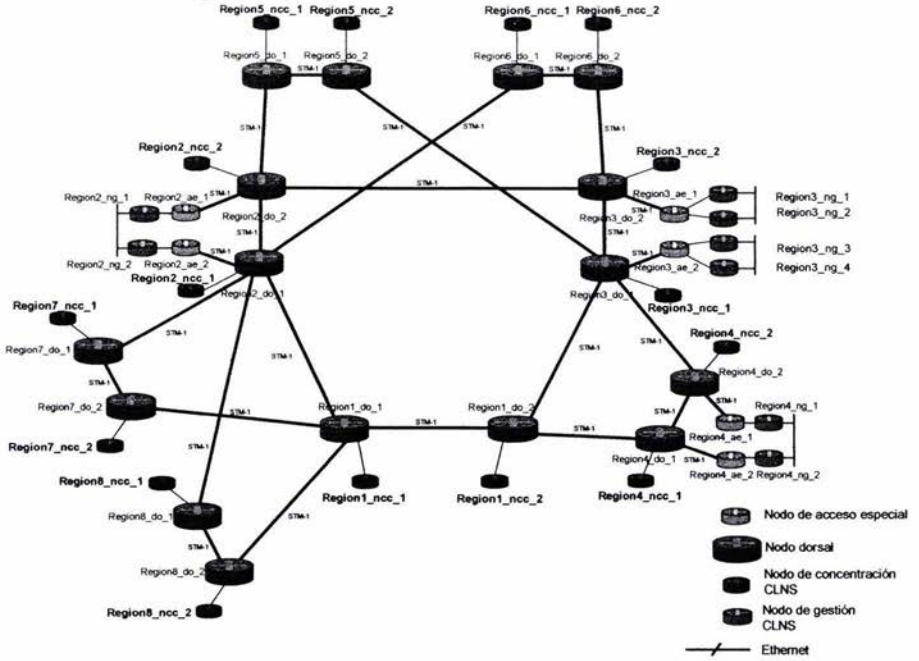

Figura 5.17 Topología física de la red de datos, NCCs y nodos de gestión CLNS.

Las características de cada uno de los nodos de acceso dedicados a los sistemas de gestión para la interconexión de los gestores se indican a continuación:

Modelo	Cisco 3662-DC-CO
Módulos adicionales instalados en el enrutador	Dos módulos NM-1FE-TX (1 puerto Ethernet 100BaseT por cada módulo)
Alimentación	2 circuitos de 10A y -48V DC cada uno
Memoria	Tipo flash 8 MB para almacenamiento de información y tipo DRAM 32 MB para procesamiento
Tipo de procesador	RISC a 80 Mhz
Versión de sistema operativo	Cisco IOS 12.1(1)T

Tabla 5.15 Equipamiento para los nodos de gestión CLNS.

Es importante considerar que la culminación en la implementación de este esquema no es requisito para iniciar las siguientes etapas, pero si debe completarse para continuar la etapa 5 que es la Interconexión de los nodos de gestión al nivel dorsal.

Esquema de red local para elementos de red SDH

Este tipo de esquema es el que se explica en la sección anterior de esquema de interconexión LAN, y será implementado en la fase 7 de Interconexión masiva de los accesos hacia la "red virtual CLNS".

5.3.2. Instalación de los "nodos de concentración CLNS"

Para efectos de contar con redundancia de equipo para este tipo de nodos, se instalarán dos nodos de concentración CLNS por región, siendo por razones de homogeneidad del mismo modelo y con las mismas características físicas cada uno de ellos, las cuales se enlistan en la siguiente tabla:

Modelo	Cisco 3662-DC-CO
Módulos adicionales instalados en el enrutador	1 NM-2CE1U, Módulo de dos puertos seriales tipo E1 canalizado.
Alimentación	2 circuitos de 10A y -48V DC cada uno
Memoria	Flash 8 MB para almacenamiento de información y DRAM 32 MB para procesamiento
Tipo de procesador	RISC a 80 Mhz
Versión de sistema operativo	Cisco IOS 12.1(1)T

Tabla 5.16 Equipamiento para los nodos de concentración CLNS.

La interconexión de cada uno de estos nodos será a través de un enlace serial de tipo E1 local, o *back to back* con el nodo dorsal del sitio correspondiente. La siguiente figura muestra el esquema a emplear:

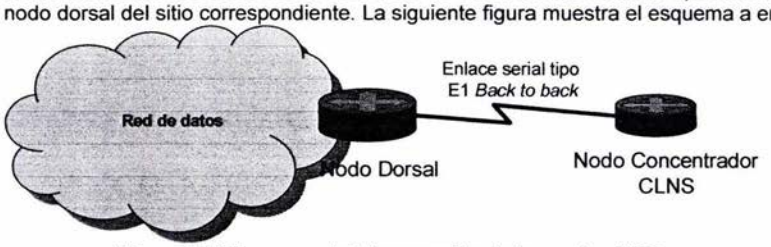

Figura 5.18 Esquema de interconexión de los nodos NCC

Para la instalación física de estos nodos y la configuración de los protocolos IP y EIGRP, no es necesario seguir un orden, sin embargo, la configuración de los protocolos CLNP e IS-IS se realizará bajo un orden establecido en la siguiente etapa del proceso.

5.3.3. Implementación del nivel dorsal de la "Red virtual CLNS"

La implementación del nivel dorsal de la "red virtual CLNS" consiste de la interconexión lógica entre todos los "nodos concentradores CLNS", como lo muestra la siguiente figura:

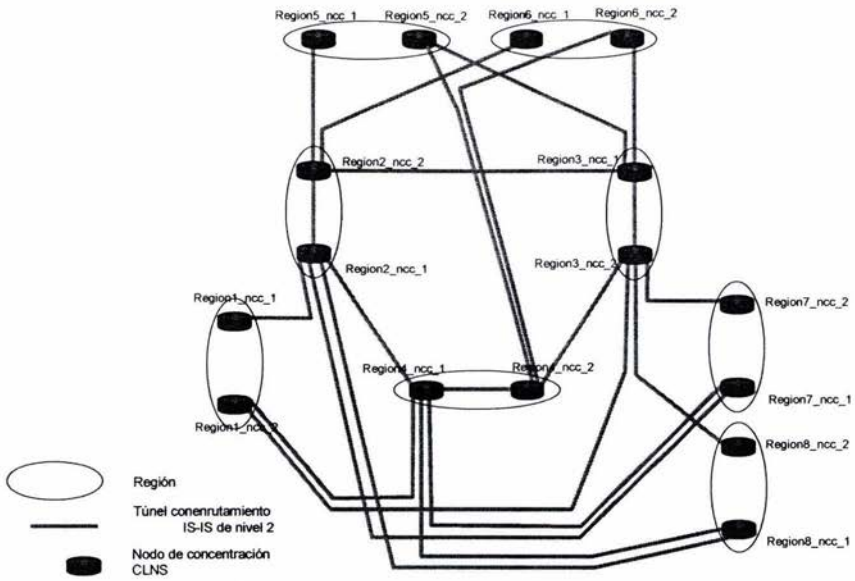

Figura 5.19 Topología del nivel dorsal de la red virtual CLNS.

Esta interconexión entre NCCs será mediante la creación de túneles para IS-IS y CLNP. El establecimiento de estos túneles tendrá asociado el uso de interfaces lógicas o *loopbacks* con direccionamiento IP de red 10.0.0.0. Asimismo el enrutamiento para CLNP será IS-IS de nivel 2.

Configuración de los nodos involucrados

La configuración de cada "nodo de concentración CLNS" será de acuerdo al orden establecido a continuación y el cual pretende mantener un control en el proceso de configuración, para poder identificar de manera rápida errores de configuración y de operación durante la ejecución del mismo:

Secuencia de configuración	Nombre del nodo dorsal concentrador a configurar	Región a la que pertenece el nodo dorsal concentrador
1	Region_1_ncc_1	Region_1
2	Region_1_ncc_2	
3	Region_2_ncc_1	Region_2
4	Region_2_ncc_2	
5	Region_3_ncc_1	Region_3
6	Region_3_ncc_2	
7	Region_4_ncc_1	Region_4
8	Region_4_ncc_2	
9	Region_5_ncc_1	Region_5
10	Region_5_ncc_2	
11	Region_6_ncc_1	Region_6
12	Region_6_ncc_2	
13	Region_7_ncc_1	Region_7
14	Region_7_ncc_2	
15	Region_8_ncc_1	Region_8
16	Region_8_ncc_2	

Tabla 5.17 Secuencia de configuración de los nodos de concentración CLNS.

La configuración de los NCCs, bajo la lógica de programación del proveedor "Cisco" se lista y se explica con el siguiente ejemplo:

Región1_ncc_2	
interface loopback666 ip address 10.1.1.1 255.255.255.255	Interfaz lógica usada para la construcción de túneles.
Router eigrp 124 network 10.0.0.0	Protocolo de enrutamiento IP, número de sistema autónomo perteneciente y número de red empleado en este nodo.
Ip classless	Comando que especifica el uso del concepto de subred.
Router isis DORSAL net 49.0001.0001.0001.0001.ffff.ffff.0001.234.5678.00 is-type level-2-only	Proceso de enrutamiento IS-IS de nivel 2 y dirección CLNP empleados por el enrutador "región1_ncc_2"
interface Tunnel300 description TUNEL CLNS DORSAL REGION1_NCC_2 <---> REGIÓN5_NCC_1 ip mtu 1500 clns mtu 1480 clns router isis DORSAL tunnel source loopback 666 tunnel destination 10.1.1.2 tunnel mode eon	Configuración del túnel número 300 que tiene como punta extrema al nodo "region5_ncc_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2. Así mismo se fijan los tamaños de los paquetes IP y CLNP[12] a los valores en bytes especificados en la configuración.
Interface Tunnel301 description TUNEL CLNS DORSAL REGION1_NCC_2 <-> REGION3_NCC_1 ip mtu 1500 clns mtu 1480 clns router isis DORSAL tunnel source loopback 666 tunnel destination 10.1.1.3 tunnel mode eon	Configuración del túnel 301 que tiene como punta extrema al nodo "region3_ncc_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2. Así mismo se fijan los tamaños de los paquetes IP y CLNP a los valores en bytes especificados en la configuración.

Continúa...

[12] Se toman estos valores a fin de asegurar que el tamaño de unidad máxima de transferencia sea el mismo para IP y CLNS, ya que se pueden encontrar diferencias al respecto entre versiones de sistema operativo y de plataformas.

Configuración de Región1_ncc_2...

Interface Tunnel302 shutdown Description TUNEL CLNS DORSAL REGION1_NCC_1 <-> REGION1 _NG _1 ip mtu 1500 clns mtu 1480 clns router isis DORSAL tunnel source loopback 666 tunnel destination 10.1.2.1 tunnel mode eon	Configuración del túnel 302 que tiene como punta extrema al nodo "región1_ng_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2. Adicionalmente se encuentra deshabilitado con el comando *shutdown*. Así mismo se fijan los tamaños de los paquetes IP y CLNP a los valores en bytes especificados en la configuración.
interface Tunnel303 shutdown description TUNEL CLNS DORSAL REGION1_NCC_1 <--> REGION1 _NG _2 ip mtu 1500 clns mtu 1480 clns router isis DORSAL tunnel source loopback 666 tunnel destination 10.1.2.2 tunnel mode eon	Configuración del túnel 303 que tiene como punta extrema al nodo "región1_ng_2", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2. Adicionalmente se encuentra deshabilitado con el comando *shutdown*.

Tabla 5.18 Ejemplo de configuración de un nodo de concentración CLNS.

Como se observa en la tabla anterior, los túneles de interconexión con nodos gestores, se configurarán en esta etapa y se mantendrán desactivados (*shutdown*) hasta ser completada esta fase.

Supervisión del funcionamiento del nivel dorsal

Terminada la tercera fase, se procederá a la activación de los túneles del nivel dorsal. A lo largo de esta nueva fase se utilizarán los siguientes comandos a fin de verificar su correcta operación:

Comando	Descripción de la operación
Show clns protocol	Muestra las NETs configuradas, así como las interfaces en las cuales se tienen habilitados los procesos de IS-IS en el enrutador.
Show clns neighbors	Muestra los vecinos de IS-IS conocidos por las interfaces habilitadas con este protocolo.
Show clns interface	Muestra los parámetros habilitados de CLNS que tienen las interfaces en cuestión.

Tabla 5.19 Comandos de supervisión para el protocolo CLNP.

Una vez implementado el nivel dorsal, se procederá a desarrollar la cuarta fase que consiste en realizar pruebas de enrutamiento y de conectividad.

5.3.4. Pruebas de enrutamiento y conectividad del nivel dorsal

El propósito de esta fase de pruebas es verificar el correcto flujo de tráfico y que los tiempos de respuesta sean los adecuados dentro de la red. Lo anterior es con el fin de verificar el óptimo servicio de comunicación durante y después de la etapa de migración de las aplicaciones de gestión de elementos SDH. Estas pruebas consistirán de cuatro partes:

Prueba	Descripción general de la prueba
1. Matriz de tiempos de respuesta	Elaborar una matriz de tiempos de respuesta para todos los puntos de la red con base en *PINGS* de CLNS.
2. Flujos de tráfico	Verificar que los flujos de tráfico entre todos los puntos de la red sean los esperados.
3. Redundancia en los "nodos concentradores CLNS"	Verificar que el servicio no sea interrumpido a causa de la falla de uno de los "nodos concentradores CLNS".
4. Revisar características del protocolo IS-IS	Verificar que el funcionamiento del protocolo IS-IS sea estable revisando algunas de sus características de funcionamiento.

Tabla 5.20 Secuencia de las pruebas en el nivel dorsal.

Los requerimientos y el desarrollo de cada una de estas partes se exponen a continuación:

Preparativos de las pruebas

Para el desarrollo de esta etapa de prueba se deberán configurar áreas temporales[13] de prueba de nivel 1 de IS-IS, las cuales se listan a continuación y se muestra su ubicación en la figura 5.20:

Nodo .- Nombre y dirección IP	Configuración del nodo.- De los procesos de enrutamiento IS-IS de nivel 1 y de las direcciones CLNP de los enrutadores en cuestión.
Region1_ncc_1 10.1.1.1	Router isis 11 Net 49.00001.0001.0001.0001.1111.1111.0005.3204.1580.00
Region1_ncc_2 10.1.1.2	Router isis 22 Net 49.00001.0001.0001.0001.2222.2222.0004.c14c.ba10.00 Router isis 11 Net 49.00001.0001.0001.0001.1111.1111.0004.c14c.ba10.00
Region2_ncc_1 10.1.1.3	Router isis 33 Net 49.00001.0001.0001.0001.3333.3333.0005.3204.1200.00
Region2_ncc_2 10.1.1.4	Router isis 44 Net 49.00001.0001.0001.0001.4444.4444.0005.3203.fe50.00 Router isis 33 Net 49.00001.0001.0001.0001.3333.3333.0005.3203.fe50.00
Region3_ncc_1 10.1.1.5	Router isis 55 net 49.00001.0001.0001.0001.5555.5555.0004.c1b5.28c0.00
Region3_ncc_2 10.1.1.6	Router isis 66 net 49.00001.0001.0001.0001.6666.6666.0005.3204.1120.00 Router isis 55 net 49.00001.0001.0001.0001.5555.5555.0005.3204.1120.00
Region4_ncc_1 10.1.1.7	Router isis 77 net 49.00001.0001.0001.0001.7777.7777.0005.3204.4840.00
Region4_ncc_2 10.1.1.8	Router isis 88 Net 49.00001.0001.0001.0001.8888.8888.0005.3204.4ae0.00 Router isis 77 Net 49.00001.0001.0001.0001.7777.7777.0005.3204.4ae0.00
Region5_ncc_1 10.1.1.9	Router isis F0 Net 49.00001.0001.0001.0001.FFFF.0000.0005.3204.48b0.00
Region_5_ncc_2 10.1.1.10	Router isis 0F Net 49.00001.0001.0001.0001.0000.FFFF.0005.9b87.4fa0.00 Router isis F0 Net 49.00001.0001.0001.0001.FFFF.0000.0005.9b87.4fa0.00
Region7_ncc_1 10.1.1.11	Router isis 99 net 49.00001.0001.0001.0001.9999.9999.0004.c14c.87c0.00
Region7_ncc_2 10.1.1.12	Router isis AA net 49.00001.0001.0001.0001.AAAA.AAAA.0005.3204.00f0.00 Router isis 99 net 49.00001.0001.0001.0001.9999.9999.0005.3204.00f0.00
Region8_ncc_1 10.1.1.13	Router isis BB net 49.00001.0001.0001.0001.BBBB.BBBB.0005.3203.ffa0.00
Region8_ncc_2 10.1.1.14	router isis CC net 49.00001.0001.0001.0001.CCCC.CCCC.0005.3204.1040.00 router isis BB net 49.00001.0001.0001.0001.BBBB.BBBB.0005.3204.1040.00
Region6_ncc_1 10.1.1.15	router isis DD net 49.00001.0001.0001.0001.DDDD.DDDD.0004.c14c.b9a0.00
Region6_ncc_12 10.1.1.16	router isis EE net 49.00001.0001.0001.0001.EEEE.EEEE.0005.3203.fec0.00 router isis DD net 49.00001.0001.0001.0001.DDDD.DDDD..0005.3203.fec0.00

Tabla 5.21 Asignación de las áreas de prueba.

[13] La selección del número de estas áreas solo tiene como fin el identificarlas de manera sencilla durante el desarrollo de las pruebas. La estructura de las direcciones se explica en el capítulo 3.3 Protocolos de enrutamiento OSI.

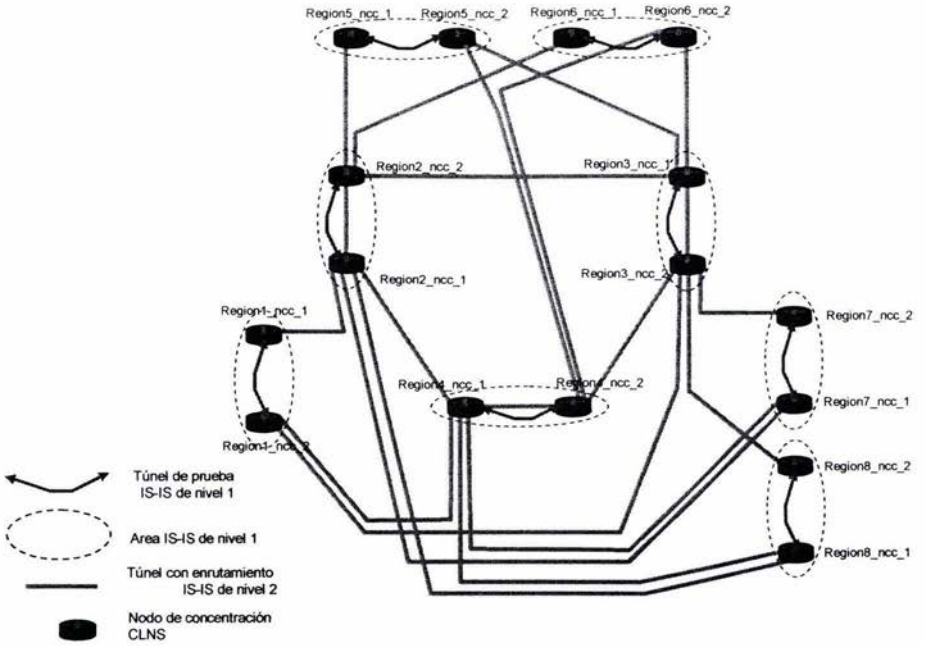

Figura 5.20 Ubicación de las áreas de prueba.

Prueba 1. Obtención de una matriz de tiempos de respuesta

La presente prueba pretende obtener los tiempos de respuesta (en milisegundos) entre cada uno de los nodos concentradores CLNS que forman el nivel dorsal (ver figura 5.20) con el fin de presentar a los usuarios de la "Red virtual CLNS" los tiempos promedio que ofrece esta y comprometer de esta forma un nivel de servicio.

La ejecución de esta prueba será mediante *pings* de tipo CLNS extendido con direcciones fuente y de destino de las áreas de prueba. El número de paquetes es de 100 con un tamaño de 900 Bytes[14].

La matriz empleada, así como sus resultados se muestra en la siguiente tabla:

[14] Estos valores fueron seleccionados ya que representan un tamaño promedio de los paquetes bajo CLNP en operación normal y el envío de 100 paquetes ofrece un valor de tiempo de respuesta promedio estable.

Tiempos en milisegundos	Region1_ncc_1 1111.1111	Region1_ncc_2 2222.2222	Region2_ncc_1 3333.3333	Region2_ncc_2 4444.4444	Region3_ncc_1 5555.5555	Region3_ncc_2 6666.6666	Region4_ncc_1 7777.7777	Region4_ncc_2 8888.8888	Region5_ncc_1 FFFF.0000	Region5_ncc_2 0000.FFFF	Region7_ncc_1 9999.9999	Region7_ncc_2 AAAA.AAAA	Region8_ncc_1 BBBB.BBBB	Region8_ncc_2 CCCC.CCCC	Region6_ncc_1 DDDD.DDDD	Region6_ncc_2 EEEE.EEEE
Region1_ncc_1 1111.1111		131	143	109	88	109	52	83	82	64	107	120	138	127	119	104
Region_1_ncc_2 2222.2222	131		98	124	43	63	79	98	95	133	94	136	125	142	134	91
Region2_ncc_1 3333.3333	143	98		136	62	75	91	110	106	146	106	148	137	154	146	102
Region2_ncc_2 4444.4444	109	124	136		81	103	45	76	76	57	101	114	131	120	112	97
Region3_ncc_1 5555.5555	88	43	62	81		21	36	55	51	91	51	93	82	99	91	48
Region_3_ncc_2 6666.6666	109	63	75	103	21		56	76	32	50	32	114	62	121	112	28
Region4_ncc_1 7777.7777	52	79	91	45	36	56		20	100	89	87	57	118	63	55	83
Region4_ncc_2 8888.8888	83	98	110	76	55	76	20		49	44	74	38	105	44	36	71
Region5_ncc_1 FFFF.0000	82	95	106	76	51	32	100	49		49	24	87	56	94	85	22
Region5_ncc_2 0000.FFFF	64	133	146	57	91	50	89	44	49		43	69	74	76	67	40
Region_7_ncc_1 9999.9999	107	94	106	101	51	32	87	74	24	43		112	84	119	110	47
Region7_ncc_2 AAAA.AAAA	120	136	148	114	93	114	57	38	87	69	112		143	82	74	109
Region8_ncc_1 BBBB.BBBB	138	125	137	131	82	62	118	105	56	74	84	143		150	141	80
Region8_ncc_2 CCCC.CCCC	127	142	154	120	99	121	63	44	94	76	119	82	150		81	116
Region6_ncc_1 DDDD.DDDD	119	134	148	112	91	112	55	36	85	67	110	74	141	81		107
Region6_ncc_2 EEEE.EEEE	104	91	102	97	48	28	83	71	22	40	47	109	80	116	107	

Tabla 5.22 Tiempos de respuesta de la "red virtual CLNS"

Los tiempos mostrados en la tabla anterior están dados en milisegundos. Los que se encuentran sombreados son los mas cortos para llegar a los sitios donde se encuentran los centros de gestión, siendo los caminos mas directos y consecuentemente los naturales.

Prueba 2. Flujos de tráfico

En esta prueba se pretenden verificar los flujos de tráfico esperados, de acuerdo a la ubicación final de los sistemas de gestión. Debido a los intereses particulares de la empresa, todos los sistemas de gestión estarán concentrados en las regiones 3, 4 y 5. Por lo anterior, en la presente prueba ejecutará el comando "*trace route*" de modo extendido para CLNS desde los nodos definidos como "punta A", con las áreas de CLNP y siguiendo la secuencia definida a continuación:

Secuencia	Punta A: Nombre del nodo y área	Punta B: Nombre de nodo y área
1	Region2_ncc_2 5555.5555	Region5_ncc_1 1111.1111
2	Region2_ncc_2 5555.5555	Region6_ncc_1 3333.3333
3	Region2_ncc_2 5555.5555	Region3_ncc_1 7777.7777
4	Region2_ncc_1 5555.5555	Region8_ncc_1 9999.9999
5	Region2_ncc_1 5555.5555	Region7_ncc_1 BBBB.BBBB
6	Region2_ncc_1 5555.5555	Region1_ncc_1 DDDD.DDDD
7	Region2_ncc_1 5555.5555	Region4_ncc_1 FFFF.0000
8	Region3_ncc_1 7777.7777	Region6_ncc_2 3333.3333
9	Region3_ncc_1 7777.7777	Region5_ncc_2 1111.1111
10	Region3_ncc_2 7777.7777	Region8_ncc_2 9999.9999
11	Region3_ncc_2 7777.7777	Region7_ncc_2 BBBB.BBBB
12	Region3_ncc_2 7777.7777	Region1_ncc_2 DDDD.DDDD
13	Region3_ncc_2 7777.7777	Region2_ncc_2 FFFF.0000
14	Region4_ncc_2 FFFF.0000	Region5_ncc_2 1111.1111
15	Region4_ncc_2 FFFF.0000	Region6_ncc_2 3333.3333
16	Region4_ncc_1 FFFF.0000	Region8_ncc_1 DDDD.DDDD
17	Region4_ncc_1 FFFF.0000	Region7_ncc_1 BBBB.BBBB
18	Region4_ncc_1 FFFF.0000	Region1_ncc_1 9999.9999

Tabla 5.23 Secuencia de pruebas de flujos de tráfico.

La figura 5.21, muestra los flujos de tráfico obtenidos en la prueba y que fueron los esperados por ser las trayectorias mas cortas:

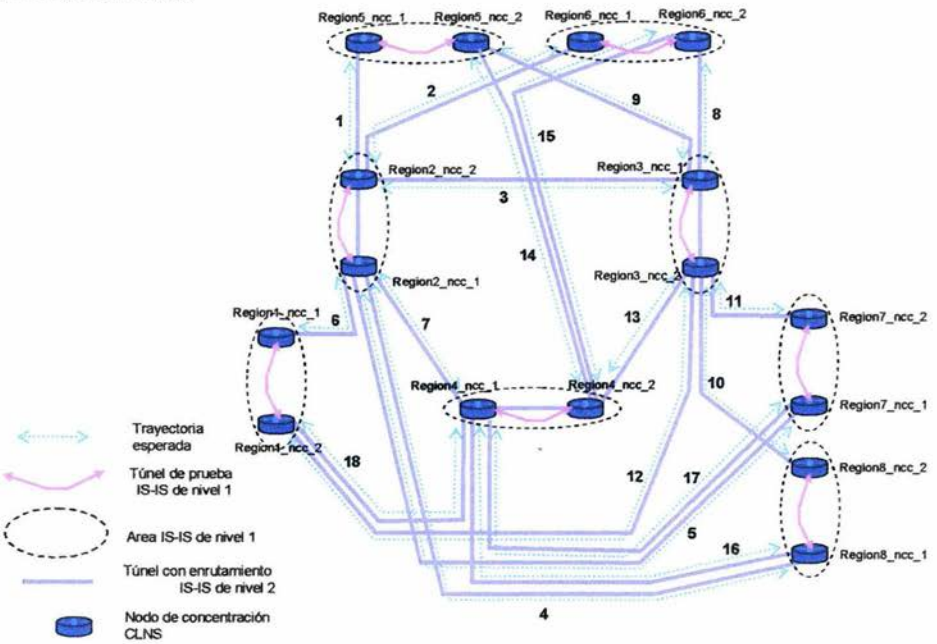

Figura 5.21 Flujos de información esperados.

Prueba 3. Redundancia en los nodos de concentración CLNS

Después de las trayectorias verificadas en la prueba anterior, la presente prueba pretende verificar que las trayectorias tomadas en diferentes casos de falla son las esperadas por ser las segundas mas cortas.

El desarrollo de esta prueba consiste en dar de baja los enlaces que conectan a los nodos concentradores CLNS con los nodos dorsales, y de esta forma verificar su correcto enrutamiento.

La secuencia, desarrollo y resultado de estas pruebas se muestra a continuación:

Sec	Sitio	Simulación de falla	Resultado esperado
1	Region1_ncc_2	Enlace serial en *shutdown* en el nodo region1_doc_2	Cambio de trayectoria. Ver figura 5.23
	Actividades a desarrollar		
	Trace route de CLNS extendido *Ping* de CLNS extendido de 10000 paquetes con un tamaño de 900 Bytes. fuente 49.0001.001.0001.0001.1111.1111.0005.3204.1580.00 destino 49.00001.0001.0001.0001.7777.7777.0005.3204.4ae0.00		
	Comentarios de los resultados		
	El resultado fue satisfactorio, ya que el flujo de datos se reenrutó por el camino estimado de manera inmediata.		
2	Region7_ncc_1	Enlace serial en *shutdown* en el nodo region7_do_1	Cambio de trayectoria. Ver figura 5.23
	Actividades a desarrollar		
	Trace route de CLNS extendido *Ping* de CLNS extendido de 10000 paquetes con un tamaño de 900 Bytes. fuente 49.00001.0001.0001.0001.DDDD.DDDD..0005.3203.fec0.00 destino 49.00001.0001.0001.0001.7777.7777.0005.3204.4ae0.00		
	Comentarios de los resultados		
	El resultado fue satisfactorio, ya que el flujo de datos se reenrutó por el camino estimado de manera inmediata.		
3	Region3_ncc_1	Enlace serial en *shutdown* en region3_doc_1	Cambio de trayectoria. Ver figura 5.23
	Actividades a desarrollar		
	Trace route de CLNS extendido *Ping* de CLNS extendido de 10000 paquetes con un tamaño de 900 Bytes. fuente 49.00001.0001.0001.0001.9999.9999.0005.3204.1040.00 destino 49.00001.0001.0001.0001.5555.5555.0005.3204.1120.00		
	Comentarios de los resultados		
	El resultado fue satisfactorio, ya que el flujo de datos se reenrutó por el camino estimado de manera inmediata.		

Tabla 5.24 Pruebas de redundancia del nivel dorsal.

Las trayectorias de los flujos de información esperados en los casos de falla se muestran en la siguiente figura:

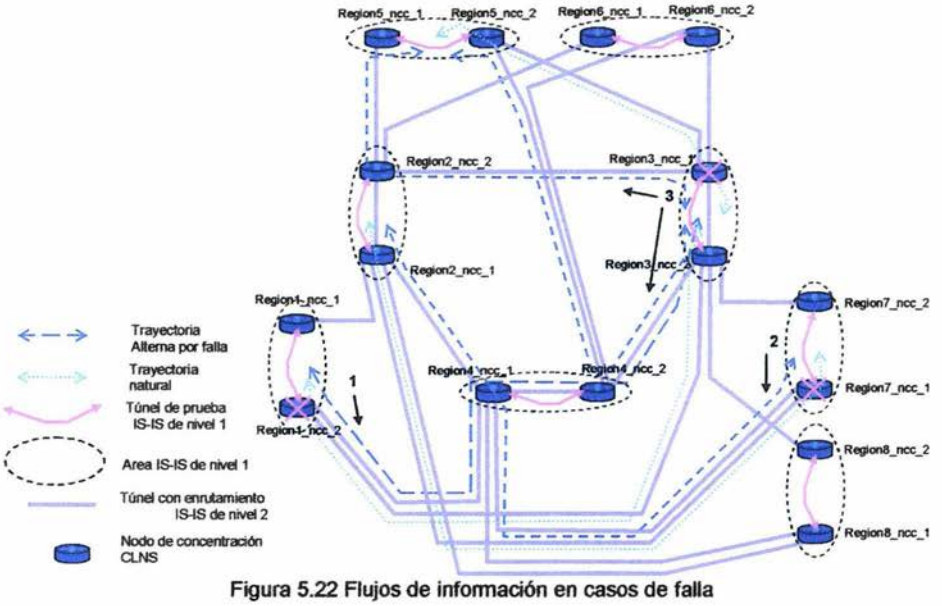

Figura 5.22 Flujos de información en casos de falla

Prueba 4. Revisión de características del protocolo IS-IS

Como parte informativa en el desarrollo de las pruebas, se revisarán las características del comportamiento del protocolo IS-IS en su nivel 2. Los datos más importantes a verificar en cada enrutador son los siguientes:

- Vecinos de nivel 2 de IS-IS en cada equipo.
- Tamaño de MTU o unidad máxima de transferencia en las interfaces *FastEthernet* y túnel.
- Número de áreas que se anuncian en la tabla de enrutamiento del nivel dorsal.
- Eventos ocurridos dentro del nivel dorsal.

Una vez revisado el correcto funcionamiento del nivel dorsal de la "red virtual CLNS", se podrá iniciar la etapa de interconexión de los sistemas de gestión de las aplicaciones al nuevo esquema.

Si en alguna de las etapas no se hubiera obtenido el resultado esperado, se hubiera detenido el desarrollo de las etapas posteriores hasta analizar la causa y dar solución a esta, pudiéndose hacer entonces un cambio en las configuraciones, en el sistema operativo de los enrutadores (por errores en este), o considerar un rediseño a la "red virtual CLNS".

5.3.5. Interconexión de los sistemas de gestión al nivel dorsal

Una vez implementado el nivel dorsal de la "red virtual CLNS" y verificado el correcto funcionamiento de este, se procede con la siguiente fase dentro del proceso general de implementación de la VPN, el cual consiste en integrar al nuevo esquema los enrutadores donde se encontrarán conectados los sistemas de gestión de las aplicaciones que operan bajo CLNP.

Proceso de Integración

La integración de los sistemas de gestión a la "Red Virtual CLNS" se realizará de acuerdo al diagrama siguiente:

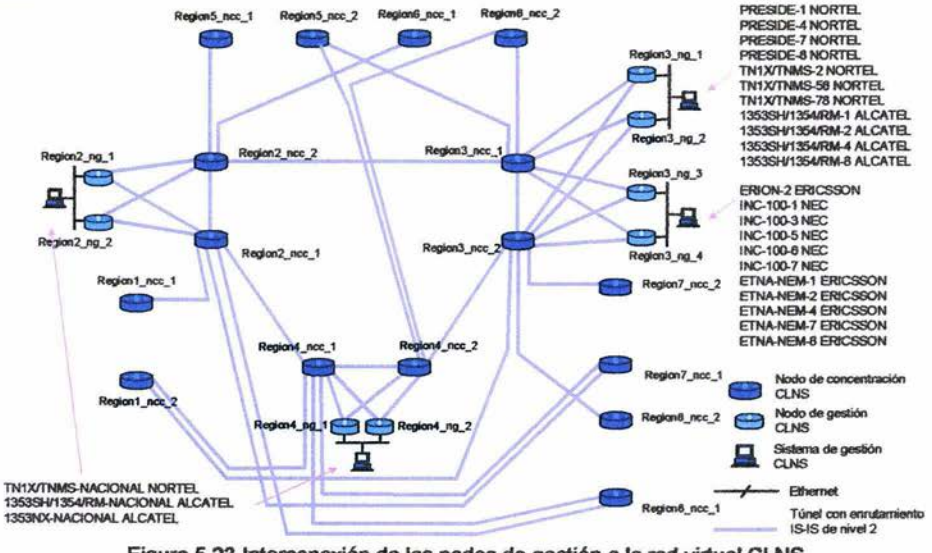

Figura 5.23 Interconexión de los nodos de gestión a la red virtual CLNS

La interconexión de los "nodos gestores" a la "Red virtual CLNS" se realiza mediante túneles con enrutamiento IS-IS de nivel 2 hacia los "nodos concentradores CLNS" de la región correspondiente, asimismo su implementación será mediante interfaces *loopback* con direccionamiento IP de red 10.0.0.0.

Configuración de los nodos involucrados

Los nodos de gestión que se integrarán al nivel dorsal de "Red virtual CLNS", así como su secuencia de configuración, se muestra a continuación:

Secuencia	Nombre del nodo	Región afectada
1	Region2_ng_1	Región 2
2	Region1_ng_1	Región 1
3	Region1_ng_2	
4	Region3_ng_1	Region 3
5	Region3_ng_2	
6	Region3_ng_3	
7	Region3_ng_3	
8	Region5_ng_1	Region 5
9	Region5_ng_2	
10	Region6_ng_1	Region 6
11	Region6_ng_2	
12	Region4_ng_1	Region 4
13	Region4_ng_2	
14	Region4_ng_3	
15	Region4_ng_3	
16	Region4_ng_4	
17	Region4_ng_5	
18	Region4_ng_6	

Tabla 5.25 Secuencia de integración de los nodos de gestión.

El ejemplo de configuración en estos enrutadores se enlista a continuación:

Region2_ng_1, 13.38.4.85	
router isis DORSAL net 49.0001.0001.0001.0001.FFFF.FFFF.0005.3204.2354.00 is-type level-2-only	Proceso de enrutamiento IS-IS de nivel 2 y dirección CLNP empleados por el enrutador "región2_ng_1" para la comunicación con el resto de las áreas de la "red virtual CLNS"
router isis AREA12344321 net 49.0001.0001.0001.0001.1234.4321.0005.3204.2354.00 is-type level-1	Proceso de enrutamiento IS-IS de nivel 1 y dirección CLNP empleados por el enrutador "región2_ng_1" para la comunicación de este con los elementos del sistema de gestión.
Interface ethernet 1 Description SISTEMA DE GESTION DE LA APLICACION 1353SH REGIÓN2 clns router isis AREA12344321	Interfaz ethernet donde se conectará la red local de los elementos del sistema de gestión , la cuál está asociada al proceso de enrutamiento IS-IS de nivel 1.
interface Tunnel300 description TUNEL DORSAL REGION2_NG_1 <---> REGION2_NCC_1 ip mtu 1500 clns mtu 1480 clns router isis DORSAL tunnel source loopback 0 tunnel destination 10.1.1.3 tunnel mode eon	Configuración del túnel número 300 que tiene como punta extrema al nodo "región2_ncc_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2. Así mismo se fijan los tamaños de los paquetes IP y CLNP a los valores en bytes especificados en la configuración[15].
interface Tunnel301 description TUNEL DORSAL REGION2_NG_1 <---> REGION2_NCC_2 ip mtu 1500 clns mtu 1480 clns router isis DORSAL tunnel source loopback 0 tunnel destination 10.1.1.4 tunnel mode eon	Configuración del túnel 301 que tiene como punta extrema al nodo "región2_ncc_2", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2 (túnel redundante). Así mismo se fijan los tamaños de los paquetes IP y CLNP a los valores en bytes especificados en la configuración.

Tabla 5.26 Ejemplo de configuración de un nodo gestor

Como se había establecido en la etapa de implementación del nivel dorsal, las puntas de los túneles del lado de los nodos concentradores CLNS se activarán una vez terminada la configuración anteriormente listada y de acuerdo a la secuencia de configuración siguiente:

Secuencia	Enrutador	Región
1	Region2_ncc_1	Region 2
2	Region2_ncc_2	
3	Region1_ncc_1	Region 1
4	Region1_ncc_2	
5	Region2_ncc_1	Region 3
6	Region2_ncc_2	
7	Region5_ncc_1	Region 5
8	Region5_ncc_2	
9	Region4_ncc_1	Region 6
10	Region4_ncc_2	
11	Region3_ncc_1	Region 4
12	Region3_ncc_2	

Tabla 5.27 Secuencia de activación de túneles

[15] Se toman estos valores a fin de asegurar que el tamaño de unidad máxima de transferencia sea el mismo para IP y CLNS, ya que se pueden encontrar diferencias al respecto entre versiones de sistema operativo y de plataformas.

El ejemplo de configuración en los nodos concentradores CLNS se lista a continuación:

Region2_ncc_1	
interface Tunnel301 description TUNEL CLNS REGION2 _NCC_1 <---> REGION2_NG_1 no shutdown	Activación del túnel número 301 en el nodo "region2_ncc_1" configurado en la etapa 3 de implementación del nivel dorsal.

Tabla 5.28. Ejemplo de configuración posterior de un "nodo concentrador CLNS"

Una vez terminada la interconexión de cada "nodo gestor" a la "Red virtual CLNS" se procederá a realizar la siguiente fase que consiste en una serie de pruebas en sitio para verificar la operación de la gestión de elementos SDH en un caso real.

5.3.6. Prueba piloto de interconexión de accesos a la "Red virtual de CLNS"

Como parte previa a la migración masiva de todos los nodos de acceso que trabajarán con CLNP al esquema de la "Red virtual CLNS", se realizará una serie de pruebas de conectividad y desempeño en algunos equipos previamente definidos con el fin de asegurar la correcta migración durante y después del proceso masivo. La figura 5.24 muestra los sitios involucrados durante esta prueba piloto:

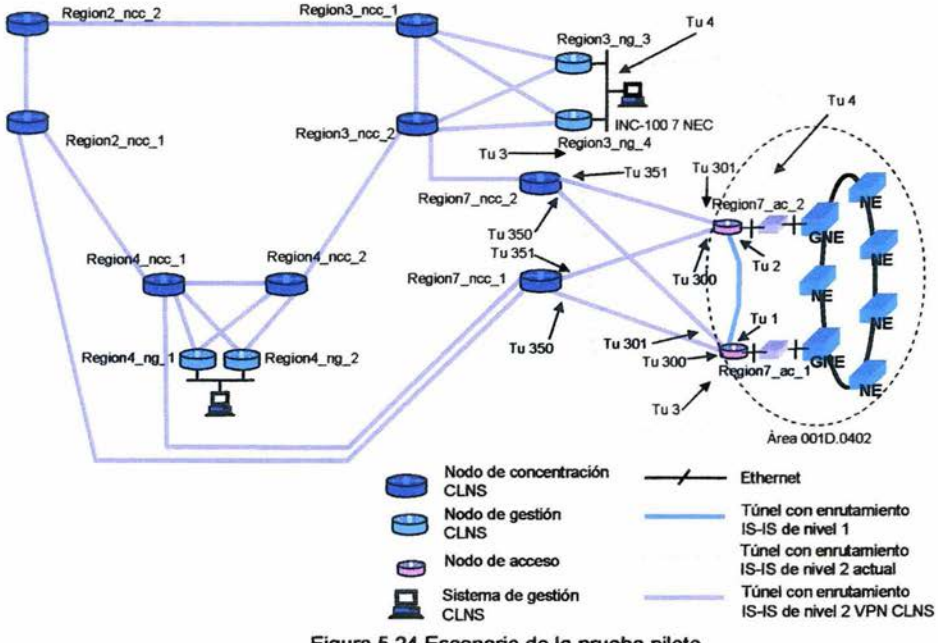

Figura 5.24 Escenario de la prueba piloto.

Los nodos de acceso que participarán en la prueba se listan a continuación:

Enrutador	Área	Aplicación	Gestor
region7_ac_1	001D.0402	INC-100 7 NEC	Region3_ng_3
region7_ac_2	001D.0402	INC-100 7 NEC	Region3_ng_4

Tabla 5.29 Nodos de acceso que participan en la prueba.

El desarrollo de las pruebas se dividirá en 2 etapas las cuales se describen a continuación:

Etapa	Nombre de la Prueba	Descripción de la prueba
1	Migración	El objetivo de esta etapa es asegurar que la gestión de los elementos SDH sea afectada lo menos posible durante la migración de los nodos de acceso al esquema de la "red virtual de CLNS".
2	Redundancia y desempeño	Se pretende verificar que el transporte de información de gestión llegue a su destino de acuerdo a diferentes situaciones de falla en la red corporativa de datos.

Tabla 5.30 Etapas de la prueba.

Etapa 1. Migración

La prueba que define el proceso de migración deberá aplicarse para cada nodo de acceso que sea migrado, es decir, se ejecutará bajo el siguiente orden para los dos nodos en cuestión:

1. region_7_ac_1
2. region_7_ac_2
3. Deshabilitar los túneles directos a los nodos gestores

Y para cada acceso migrado se realizarán las siguientes actividades:

Acción	Comandos a emplear
Configurar túneles al nivel dorsal de la "red virtual de CLNS" y activarlos (enrutador de acceso – NCC)	Ver sección de Configuraciones a emplear
Verificar la comunicación punto a punto (Enrutador de acceso y NCC) durante cada nodo migrado.	*Show clns route.*- Muestra los elementos de la tabla de enrutamiento de IS-IS de nivel 2. *Show isis route.*- Muestra los elementos de la tabla de enrutamiento de IS-IS de nivel 1. *Show clns neighbors.*- Muestra los vecinos de IS-IS de nivel 1 y 2 del enrutador en cuestión. *Ping clns XXXX.....*- Verifica la conectividad a nivel CLNP. Verificar la gestión correcta de la aplicación a través del propio sistema.

Tabla 5.30 Actividades a realizar en cada nodo de acceso.

Configuraciones a emplear

Las configuraciones utilizadas bajo secuencia en los enrutadores involucrados en las pruebas, así como su explicación se listan a continuación:

Primera etapa

Region7_ac_1, Paso 1	
interface loopback666 ip address 10.1.3.1 255.255.255.255	Interfaz lógica empleada para la construcción de los túneles.
Router eigrp 124 network 10.0.0.0 no auto-summary	Protocolo de enrutamiento IP y número de red empleados en este nodo.
Ip classless	Comando que especifica el uso del concepto de subred.
Router isis DORSAL net 49.00001.0001.0001.0001.ffff.ffff.0005.3204.1681.00 is-type level-2-only	Proceso de enrutamiento IS-IS de nivel 2 y dirección CLNP empleados por el enrutador "región7_ac_1" para su comunicación con el área del sistema de gestión
router isis AREAABABABAB net 49.00001.0001.0001.0001.ABAB.ABAB.0005.3204.1681.00 is-type level-1	Proceso de enrutamiento IS-IS de nivel 1 y dirección CLNP empleados por el enrutador "región7_ac_1" para la comunicación de este con los elementos SDH.
Interface ethernet 1 Description APLICACIÓN INC-100 7 NEC Clns router isis AREAABABABAB	Interfaz ethernet donde se conectará la red local de los elementos SDH, la cual y está asociada al proceso de enrutamiento IS-IS de nivel 1.
Interface tunnel 300 Description TUNEL DORSAL region7_ac_1 <-> Region7_NCC_1 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.1.13 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 300 que tiene como punta extrema al nodo "región7_ncc_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2.
Interface tunnel 301 Description TUNEL DORSAL region7_ac_1 <---> Region7_NCC_2 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.1.14 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 301 que tiene como punta extrema al nodo "región7_ncc_2", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2 (túnel redundante).
Interface tunnel 1 Description TUNEL DORSAL region7_ac_1 <---> Region7_ac_2 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.3.2 Tunnel mode eon Clns router isis AREAABABABAB	Configuración del túnel 100 que tiene como punta extrema al nodo "región7_ac_2", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "AREAABABABAB" de nivel 1 (túnel de redundancia en caso de partición de área, como se indica en la sección 3.3.5 Protocolo de enrutamiento IS-IS).

Tabla 5.32 Configuración en el nodo de acceso region_7_ac_1.

region7_ncc_1, Paso 2	
Interface tunnel 350 Description TUNEL DORSAL Region7_NCC_1<---> region7_ac_1 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.3.1 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 350 que tiene como punta extrema al nodo "región7_ac_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2.

Tabla 5.33 Configuración en el nodo region_7_ncc_1.

region7_ncc_2, Paso 3	
Interface tunnel 350 Description TUNEL DORSAL Region7_NCC_1<---> region7_ac_1 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.3.1 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 350 que tiene como punta extrema al nodo "región7_ac_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2 (túnel redundante).

Tabla 5.34 Configuración en el nodo region_7_ncc_2.

Segunda etapa

region7_ac_2, Paso 1	
interface loopback666 ip address 10.1.3.2 255.255.255.255	Interfaz lógica empleada para la construcción de los túneles.
router eigrp 124 network 10.0.0.0 no auto-summary	Protocolo de enrutamiento IP y número de red empleados en este nodo.
Ip classless	Comando que especifica el uso del concepto de subred.
router isis DORSAL net 49.00001.0001.0001.0001.ffff.ffff.0005.3204.1231.00 is-type level-2-only	Proceso de enrutamiento IS-IS de nivel 2 y dirección CLNP empleados por el enrutador "región7_ac_2" para su comunicación con el área del sistema de gestión
router isis AREAABABABAB net 49.00001.0001.0001.0001.ABAB.ABAB.0005.3204.1231.00 is-type level-1	Proceso de enrutamiento IS-IS de nivel 1 y dirección CLNP empleados por el enrutador "región7_ac_2" para la comunicación de este con los elementos SDH.
Interface ethernet 1 Description APLICACIÓN INC-100 7 NEC Clns router isis AREAABABABAB	Interfaz ethernet donde se conectará la red local de los elementos SDH, la cual está asociada al proceso de enrutamiento IS-IS de nivel 1.
Interface tunnel 300 Description TUNEL DORSAL region7_ac_2 <---> Region7_ncc_1 ip mtu 1500 clns mtu 1480 Tunnel source loopback 0 Tunnel destination 10.1.1.13 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 300 que tiene como punta extrema al nodo "región7_ncc_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2.
Interface tunnel 301 Description TUNEL DORSAL region7_ac_2 <---> Region7_ncc_2 ip mtu 1500 clns mtu 1480 Tunnel source loopback 0 Tunnel destination 10.1.1.14 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 301 que tiene como punta extrema al nodo "región7_ncc_2", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2 (túnel redundante).
Interface tunnel 2 Description TUNEL DORSAL region7_ac_2 <---> Region7_ac_1 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.3.1 Tunnel mode eon Clns router isis AREAABABABAB	Configuración del túnel 100 que tiene como punta extrema al nodo "región7_ac_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "AREAABABABAB" de nivel 1 (túnel de redundancia en caso de partición de área, como se indica en la sección 3.3.5 Protocolo de enrutamiento IS-IS).

Tabla 5.35 Configuración en el nodo de acceso region_7_ac_2.

region7_ncc_1, Paso 2	
Interface tunnel 351 Description TUNEL DORSAL Region7_NCC_1<---> region7_ac_1 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.3.2 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 350 que tiene como punta extrema al nodo "región7_ac_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2.

Tabla 5.36 Configuración en el nodo de acceso region_7_ncc_1.

region7_ncc_2, Paso 3	
Interface tunnel 351 Description TUNEL DORSAL Region7_NCC_2<---> region7_ac_2 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.1.2 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 350 que tiene como punta extrema al nodo "región7_ac_2", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2 (túnel redundante).

Tabla 5.37 Configuración en el nodo de acceso region_7_ncc_2.

Tercera etapa

region7_ac_1, Paso 1	
Interface tunnel 3 Description TUNEL Region3_ng _4<---> region7_ac_1 shutdown	Desactivación del túnel 3 dirigido hacia el nodo Region3_ng _4 (únicamente durante la fase de pruebas)

Tabla 5.38 Configuración en el nodo de acceso region7_ac_1.

region7_ac_2, Paso 2	
Interface tunnel 4 Description TUNEL Region3_ng _3<-> region7_ac_2 shutdown	Desactivación del túnel 4 dirigido hacia el nodo Region3_ng _3 (únicamente durante la fase de pruebas)

Tabla 5.39 Configuración en el nodo de acceso region7_ac_2.

region3_ng_4, Paso 3	
Interface tunnel 3 Description TUNEL Region3_ng _4<---> region7_ac_1 shutdown	Desactivación del túnel 3 dirigido hacia el nodo region7_ac_1 (únicamente durante la fase de pruebas)

Tabla 5.40 Configuración en el nodo de acceso region3_ng_4.

region3_ng_3, Paso 4	
Interface tunnel 4 Description TUNEL Region3_ng _3<---> region7_ac_1 shutdown	Desactivación del túnel 4 dirigido hacia el nodo region7_ac_2 (únicamente durante la fase de pruebas)

Tabla 5.41 Configuración en el nodo de acceso region3_ng_3.

Resultado de la etapa de migración

El resultado de esta etapa de prueba resultó satisfactorio, ya que la gestión de los elementos SDH fue lograda de manera inmediata, una vez que los túneles fueron habilitados. Asimismo fueron verificadas que las trayectorias de los flujos de información fueran las esperadas.

Etapa 2. Redundancia y desempeño

Las pruebas a realizarse en esta etapa consistirán en los siguientes puntos:

- Simular fallas en algunos de los enrutadores para verificar que las trayectorias alternas sean las previstas para estos casos.
- Asegurar el funcionamiento de los túneles de redundancia para los casos de una partición de anillo, o de falla en el enlace entre el enrutador de acceso y el elemento SDH inicial (GNE).

Si en alguna de las etapas no se obtuviera el resultado esperado, se deberá detener el desarrollo de las etapas posteriores hasta analizar la causa y dar solución a esta, pudiendo hacerse entonces un cambio en las configuraciones, en el sistema operativo de los enrutadores (por errores en este), o considerar un rediseño en la "red virtual CLNS".

La figura 5.25 muestra las trayectorias naturales y alternas debido a las contingencias enumeradas en la etapa de pruebas:

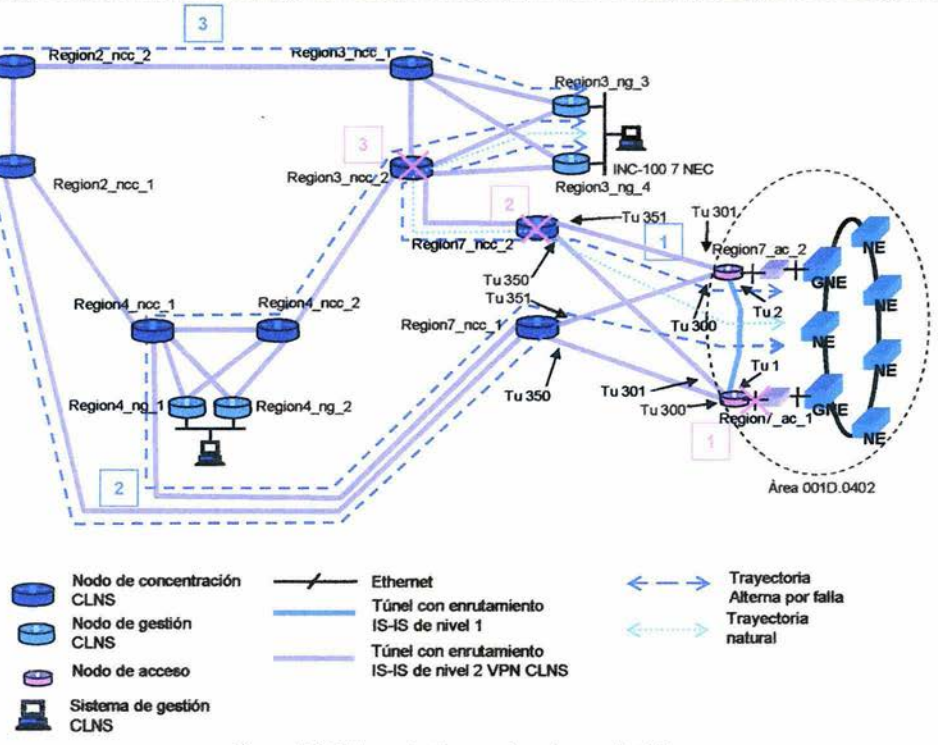

Figura 5.25 Trayectorias en situaciones de falla.

No. de prueba	Acción	Resultado esperado
1	Dar de baja conexión ethernet en region7_ac_1	Reenrutamiento de la trayectoria sin pérdida de gestión (Ruta alterna 1)
2	Dar de baja serial en region7_ac_1	Reenrutamiento de la trayectoria sin pérdida de gestión (Rutas alternas 2)
3	Dar de baja serial en region4_doc_2	Reenrutamiento de la trayectoria sin pérdida de gestión (Ruta alterna 3)

Tabla 5.42 Secuencia de pruebas.

Para cada una de estas pruebas se utilizarán los siguientes comandos para verificar los resultados esperados:

Comando	Función del comando
Show clns route NET	Muestra la información de enrutamiento IS-IS de nivel 2 de la NET deseada.
Show isis route SYSTEM ID	Muestra la información de enrutamiento IS-IS de nivel 1 del Identificador de sistema *(SYSTEM ID)* deseado.
Show clns neighbor	Muestra los vecinos de IS-IS de nivel 1 y nivel 2 que se tienen a través de las interfaces habilitadas con IS-IS.
Trace clns XX.XXXX...	Verificar la trayectoria tomada para un destino *XX.XXXX...* de CLNP en particular.

Tabla 5.43 Comandos de supervisión de los protocolos CLNP e IS-IS.

Resultado de la etapa de redundancia y desempeño

El resultado en esta etapa de pruebas fue satisfactorio ya que los flujos de información alternos (al presentarse la simulación de las fallas) fueron los esperados de acuerdo a la figura 5.25.

Una vez terminadas las pruebas se procederá a regresar a las configuraciones iniciales verificando la correcta operación de las aplicaciones afectadas y validando el servicio por el usuario mismo.

5.3.7. Interconexión masiva de los accesos hacia la "red virtual de CLNS"

Dado que los nodos de acceso son la interfaz entre la red de datos con el usuario final, estos tienen una gran variedad de aplicaciones y de redes locales conectados a ellos, no siendo la excepción las aplicaciones de gestión de elementos SDH.

Para el caso particular de estas aplicaciones, se deberá cambiar la forma de conexión lógica para poder integrarlas a la "Red virtual CLNS", explicando la presente sección este proceso y sus configuraciones relacionadas que permiten reducir el tiempo de afectación al servicio durante esta migración.

El esquema de interconexión explicado en la sección de Esquema de red local para los elementos de red SDH es el empleado para todos los nodos de acceso y se muestra en la siguiente figura:

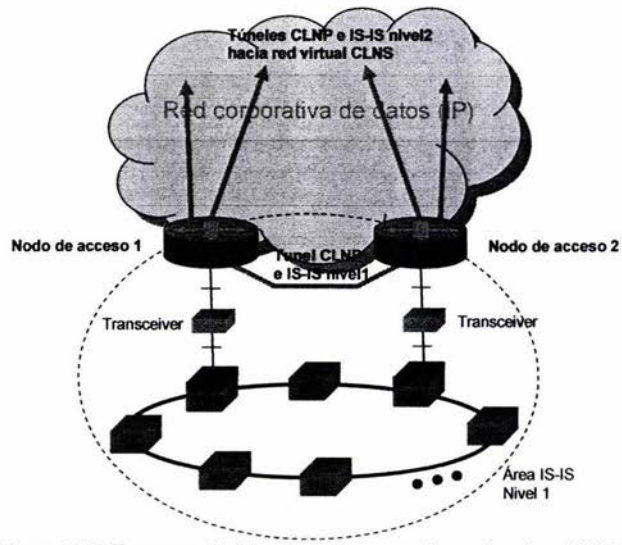

Figura 5.26 Esquema de interconexión para elementos de red SDH.

Pueden existir casos para los nodos de acceso en los que se tengan más de un anillo de elementos SDH interconectados y que sean de diferentes sistemas de gestión.

Proceso de migración de los nodos de acceso

Con base en lo anterior, y con el fin de reducir tiempos de afectación se tiene definido el siguiente proceso de migración

Escenario en servicio.- el nodo de acceso tiene conectado uno o más anillos de elementos de SDH pertenecientes a diferentes aplicaciones de gestión, y teniendo túneles directos hacia los centros de gestión de cada aplicación, como se explica en la sección de análisis del servicio en parte de topología de las aplicaciones.

Proceso.-

1. Configuración de los túneles que van de los nodos de acceso a migrar en la intervención hacia los dos nodos de concentración CLNS de la región perteneciente, manteniéndolos desactivados.
2. Activación de los dos túneles del nodo de acceso a migrar.
3. Verificar conectividad lógica de CLNP y servicio de gestión desde los elementos SDH hacia el servidor de gestión.
4. Deshabilitar los túneles directos del nodo de acceso a los centros de gestión correspondientes a cada aplicación
5. Verificar el reenrutamiento de la información de gestión de los elementos SDH migrados a la red virtual CLNS, verificar que el servicio de monitoreo y que los tiempos de respuesta sean los esperados.

Este proceso será aplicado en grupos de 15 nodos de acceso por intervención diaria y que pertenecerán a una misma región. Una vez terminada esta región se procederá a una siguiente de acuerdo al siguiente orden:

Orden de migración	Región por migrar
1	Región 8
2	Región 7
3	Región 6
4	Región 5
5	Región 4
6	Región 3
7	Región 2
8	Región 1

Tabla 5.44 Secuencia de migración de regiones.

Tal orden se basa en el número de anillos que se tienen en cada región, siendo los menores en cantidad e importancia los primeros en ser migrados, con el fin de reducir aun más alguna afectación al servicio en caso de una contingencia.

Configuraciones empleadas en los nodos de acceso

A continuación se lista y explica un ejemplo de configuraciones empleadas para el caso del nodo de acceso region7_ac_2 el cual es aplicable para cualquier otro nodo de acceso:

region7_ac_2	
interface loopback666 ip address 10.1.3.2 255.255.255.255	Interfaz lógica empleada para la construcción de los túneles.
router eigrp 124 network 10.0.0.0 no auto-summary	Protocolo de enrutamiento IP y número de red empleados en este nodo.
Ip classless	Comando que especifica el uso del concepto de subred.
router isis DORSAL net 49.00001.0001.0001.0001.ffff.ffff.0005.3204.1231.00 is-type level-2-only	Proceso de enrutamiento IS-IS de nivel 2 y dirección CLNP empleados por el enrutador "región7_ac_2" para su comunicación con el área del sistema de gestión
router isis AREAABABABAB net 49.00001.0001.0001.0001.ABAB.ABAB.0005.3204.1231.00 is-type level-1	Proceso de enrutamiento IS-IS de nivel 1 y dirección CLNP empleados por el enrutador "región7_ac_2" para la comunicación de este con los elementos SDH.
Interface ethernet 1 Description APLICACIÓN 1353SH-8 ALCATEL Clns router isis AREAABABABAB	Interfaz ethernet donde se conectará la red local de los elementos SDH y está asociada al proceso de enrutamiento IS-IS de nivel 1.
Interface tunnel 300 Description TUNEL DORSAL region7_ac_2 <---> Region4_ncc_1 ip mtu 1500 clns mtu 1480 Tunnel source loopback 0 Tunnel destination 10.1.1.1 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 300 que tiene como punta extrema al nodo "región4_ncc_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2.
Interface tunnel 301 Description TUNEL DORSAL region7_ac_2 <---> Region4_ncc_2 ip mtu 1500 clns mtu 1480 Tunnel source loopback 0 Tunnel destination 10.1.1.2 Tunnel mode eon Clns router isis DORSAL	Configuración del túnel 301 que tiene como punta extrema al nodo "región4_ncc_2", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "DORSAL" de nivel 2 (túnel redundante).
Interface tunnel 2 Description TUNEL DORSAL region7_ac_2 <---> Region7_ac_1 ip mtu 1500 clns mtu 1480 Tunnel source loopback 666 Tunnel destination 10.1.3.1 Tunnel mode eon Clns router isis AREAABABABAB	Configuración del túnel 100 que tiene como punta extrema al nodo "región7_ac_1", habilitando el encapsulamiento de CLNP sobre IP y trabajando bajo el proceso IS-IS "AREAABABABAB" de nivel 1 (túnel de redundancia en caso de partición de área, como se indica en la sección 3.3.5 Protocolo de enrutamiento IS-IS).

Tabla 5.45 Ejemplo de configuración de un nodo de acceso especial.

Durante esta etapa del proceso de migración se deberá monitorear de manera constante el uso de los recursos de los enrutadores involucrados, como por ejemplo uso del procesador y consumo de memoria en los enrutadores, utilización del ancho de banda y verificación con el usuario del funcionamiento de las aplicaciones.

5.3.8. Actividades posteriores de ajuste a la "Red Virtual CLNS"

En cualquier propuesta de diseño, durante la etapa de implementación o al final de esta, es factible realizar ciertos ajustes con el fin de mejorar el desempeño y consecuentemente el servicio ofrecido al usuario. La propuesta de diseño presentada en la presente tesis también cubre esta actividad, listando las actividades a realizar para poder llevar a cabo un análisis que permita posibles modificaciones a la propuesta:

- **Monitoreo de la utilización de enlaces.** Aún cuando se estime la utilización de los enlaces, es posible que estos alcancen los umbrales definidos en las políticas de operación, por lo que se deberá realizar un crecimiento con base en las políticas de crecimiento de enlaces.

- **Utilización de memoria en los enrutadores involucrados.** El número de elementos de red y de las áreas que manejen los enrutadores, asi como la memoria empleada para el procesamiento de la información pueden alcanzar ciertos niveles que puedan afectar el desempeño mismo del equipo. Si es el caso, se deberá analizar el crecimiento de la memoria o en su defecto contemplar un nuevo enrutador con mayor capacidad.

- **Uso de las colas de salida y de entrada en las interfaces de los enrutadores involucrados o *buffers*.** La cantidad de paquetes que un enrutador recibe o envía por sus interfaces físicas, puede ser tal que los *buffers* se saturen y se comience a desecharlos. Las posibles mejoras a esto es modificando el tamaño de los *buffers*, ya sea por configuración o incrementando la memoria utilizada para esto.

- **Utilización del procesamiento en los enrutadores involucrados.** El proceso de enrutamiento tanto para el protocolo de IP como de CLNP, asi como las funciones de encapsulamiento pueden incrementar el uso del procesador principal y alcanzar los umbrales definidos por las políticas de operación de la red. Las posibles acciones a tomar serían el uso de funcionalidades de distribución de procesamiento (*Distributed Cisco Express Forwarding, fast-switching*), cambio del tipo de encapsulamiento o el cambio de enrutador por un modelo con mayor capacidad de procesamiento.

- **Tiempos de respuesta desde el punto de vista del usuario.** La lentitud percibida por el usuario puede ser originada por varias causas, como saturación de enlaces, un procesamiento elevado, o situaciones propias de la aplicación. Las acciones a tomar se describen en los puntos anteriormente citados, o en su defecto se requerirá de un análisis mas detallado de la operación de la aplicación.

- **Convergencia de las actualizaciones de la tabla de enrutamiento para el protocolo IS-IS.** Al momento de surgir un evento como la falla de un elemento, en la "Red virtual CLNS", este debe ser anunciado a los elementos pertenecientes a este de manera inmediata. Si no fuera el caso, se deberán analizar las causas de este fenómeno que bien puede ser por oscilaciones de enlaces, enrutadores con fallas en sus interfaces, o modo de operación del protocolo de enrutamiento para IP.

- **Balanceo de tráfico.** La utilización de los enlaces que van dirigidos hacia un mismo sitio pueden no estar balanceados entre si y originar saturación, lentitud y pérdida de información del usuario. Tales circunstancias pueden ser atendidas realizando modificaciones a la topología de la red o haciendo uso del concepto de ingeniería de tráfico.

Los puntos anteriormente descritos, son los más comunes y posiblemente puedan surgir durante y al final de la implementacion de la "Red Virtual CLNS". Sin embargo pueden existir otros que requerirán de un análisis detallado con base en la información que proporcionen los dispositivos utilizados en la solución, herramientas de monitoreo, y por el usuario mismo.

6. Conclusiones

El diseño de una red de telecomunicaciones puede ser realizado bajo diferentes tipos de procesos o metodologías. Dentro de estas pueden encontrarse procesos generales o particulares, dependiendo del tipo de red que esta sea.

Para el caso particular de redes de datos, pueden existir dos líneas de diseño a seguir:

- Experiencia particular del diseñador: La cual se basa en el conocimiento propio de la red de datos, de la operación de las aplicaciones y de los procedimientos seguidos por los grupos de trabajo. Las propuestas pueden ser bien implementadas mientras se tenga un perfecto conocimiento y control en la operación de la red misma.
- Metodologías generales de diseño: Enfocadas tanto para redes del tipo LAN, como del tipo WAN . Los usos de los lineamientos a seguir dentro de estos procesos resultan efectivos y aseguran el control de la operación de la red, aun cuando el conocimiento inicial de esta sea mínimo. Este tipo de metodologías sugiere que sean utilizados en redes donde su tamaño conlleve una administración compleja.

Dentro de nuestro trabajo hicimos uso del proceso de diseño conocido como "*Top-Down*"[16] desarrollado por Priscilla Oppenheimer, el cual tiene como origen la metodología de programación estructurada iniciada a finales de la década de los 70's. Esta metodología fue elegida ya que se enfoca esencialmente en las aplicaciones de los clientes, los objetivos técnicos y las metas del negocio, ayudando a diseñar una visión lógica de la red. Se enfatiza en la planeación, antes que en la implementación y es iterativo, ya que ajusta al diseño inicial cuando se conocen detalles y requerimientos específicos.

Sin embargo, dado que este proceso de diseño tiene como alcance cualquier red de datos, lo adecuamos por nuestra parte, a fin de enfocarlo a los requerimientos del diseño, dando como resultado la metodología explicada en el capítulo 4. Lo anterior nos resultó justificable al no requerirse de la recopilación y análisis de información inexistente, o poco valiosa, para la solución que dimos.

Al realizar la parte de análisis dentro de la metodología, nos dimos cuenta que existen diferentes formas de transportar la información de gestión, como contar con una red dedicada, o solicitar este mismo servicio de transporte a un tercero. Sin embargo cada una de estas alternativas tiene implicaciones en el costo, o que se ponga en riesgo la confidencialidad de la información. Por tal razón, nuestra propuesta de diseño la consideramos como un híbrido de las formas anteriormente mencionadas, ya que existe la oportunidad de utilizar la red de datos de la misma empresa, dueña de la infraestructura de la red SDH, para el transporte de la información, y que otorga el mismo servicio a diferentes aplicaciones y usuarios, propiedad de la misma empresa, conservando la confidencialidad de la información y compartiendo costos con el resto de los usuarios. Asimismo, al emplear el concepto de red virtual, se refuerza aun mas el grado de confidencialidad de los datos, al ser difundidos exclusivamente entre los dispositivos interesados.

Al dar fin a la etapa de implementación de nuestra propuesta, se ha mantenido una observación constante del funcionamiento y comportamiento de la solución. Con lo anterior podemos concluir que los requisitos y objetivos para el funcionamiento de esta red virtual fueron cumplidos en su totalidad. Estos requisitos y objetivos cumplidos se enlistan a continuación:

[16] Top-Down Network Design , Priscilla Oppenheimer Cisco Press.

- El empleo de la infraestructura de transporte de datos que actualmente se tiene en operación con el fin de mantener los costos de inversión al mínimo.
- Estar bajo el acato de las políticas de operación de la red de datos.
- Considerar las recomendaciones por parte de los proveedores de equipo.
- Se permite un fácil crecimiento de las aplicaciones actuales, y una integración sencilla de aquellas que se requieran a futuro.
- Dada la flexibilidad de esta red virtual, el servicio de transporte puede ser soportado donde sea requerido.
- Se da el servicio a todas las aplicaciones de manera integrada.
- La "Red virtual de CLNS" es confiable y de alta disponibilidad.

Cabe mencionar que adicionalmente, se obtuvo una mejor administración al servicio de transporte ofrecido a las aplicaciones de gestión de los elementos SDH, bajo el protocolo CLNP, ya que se cuenta con una infraestructura en común para tal fin y se cuenta con una topología sencilla bajo esta red virtual. De la misma manera se pudo optimizar el tiempo en la atención a fallas, reducir el número de estas. Optimizar también la activación de nuevos servicios y el orden de crecimiento de la propia red virtual, al tener un esquema en común de operación y de interconexión a la red para todas las aplicaciones. En resumen una mejora en la administración del servicio. También observamos que la planeación de la capacidad de la red fue beneficiada al contar con equipos exclusivos para la estructura dorsal de la red virtual, ya que de esta manera se pueden realizar mejoras o ajustes a este nivel, sin afectar a otras aplicaciones o servicios prestados por la misma red (corporativa multiservicios).

Comparando el esquema original del servicio con la nueva red virtual, observamos que las trayectorias ya no son directas entre los elementos SDH gestionados y sus sistemas de gestión correspondientes. Si bien lo anterior origina que los tiempos de respuesta para el servicio de transporte sean incrementados (ya que los procesos de encapsulamiento y desencapsulamiento de los paquetes de CLNP en IP, se realizaran en cada uno de los enrutadores que forman la trayectoria en cuestión), los tiempos de recorrido total pueden garantizarse en todo momento ya que las trayectorias se encuentran bien definidas y dentro de los tiempos recomendados por los proveedores para una correcta operación.

Con la culminación de la migración total del servicio de transporte de información de gestión al nuevo esquema de la "Red virtual CLNS", observamos crecimientos importantes en el procesamiento de algunos nodos de concentración CLNS. Analizando lo anterior, concluimos que esto se origina por la cantidad de tráfico que se procesa en estos. Las acciones a tomar se realizaron como parte de la etapa de actividades posteriores de ajuste, y consisten en sustituir los actuales modelos de enrutadores, por otros con una capacidad de procesamiento mayor, como lo son los modelos Cisco 7206. Asimismo, al considerar disminuir el procesamiento en los enrutadores, o reduciendo el uso de memoria en estos, al optimizar el número de áreas CLNP dentro de las tablas de enrutamiento de IS-IS de nivel 2, buscando otras técnicas de encapsulamiento y evaluando diferentes técnicas de conmutación de paquetes CLNP dentro de los enrutadores, se mantiene una constante observación y análisis del comportamiento general de la "Red virtual CLNS", con el fin de mejorar aun mas su desempeño.

Respecto al procedimiento de implementación del diseño, se demostró que fue el óptimo en su totalidad ya que durante todas sus etapas la afectación al servicio fue mínima o nula, lográndose de esta manera acelerar los trabajos correspondientes y consecuentemente acortar la fecha estimada de terminación del proyecto.

Finalmente, los costos generados para operación del nuevo esquema, resultaron ser mínimos, dado que solamente se adquirió el equipo dedicado al nivel dorsal de la "red virtual CLNS" y el equipamiento relacionado a la interconexión con los nodos dorsales. Respecto al equipamiento requerido en los esquemas de red local, empleados para la interconexión de los elementos de red SDH, así como de los servidores de gestión y usuarios remotos, este fue absorbido por parte del dueño de la aplicación. En resumen, para los esquemas locales la inversión se compartió con otros servicios ofrecidos por la misma red corporativa multiservicios.

Referencias

Libros

Stalling, William
Local & Metropolitan Area Network, 5a Edición
Prentice Hall

Abe Martey
IS-IS Network Design Solutions
Cisco Press

Darren L. Spohn
Data Network Design
Mc Graw-Hill on Computer Comunications.

Diane Teare
Designing Cisco Networks
Cisco Press

Priscilla Oppenhimer
Top-Down Network design
Cisco Press

Allan Leinwand, Bruce Pinsky
Cisco Router Configuration
Cisco Press

Merilee Ford, H. Kim Lew
Internetworking Technologies Handbook 2a Edición.
Cisco Press

Howard C. Berkowitz
Designing Routing and Switching Architectures for Enterprise Networks
MacMillan technical Publishing

William Stallings
Local & Metropolitan Area Networks
Prentice Hall

Cisco IOS Configuration Fundamentals
Cisco Press

John J Roese
Switched LANs
McGraw-Hill Series on Computer Communication

Cursos

Curso de Instalación de sistemas de cableado estructurado
Centec México

Troubleshooting TCP/IP Networks
Global Knowledge

Building Cisco Multilayer Switched Networks
Cisco

Designing Cisco Networks
Cisco

Referencias electrónicas.

http://www.itu.int/telecom-wt99/auth/backgrounders/packets_circuits-next-es.html

http://www.techfest.com/networking/index.htm

http://www.cellsoft.de/telecom/dcn.htm

http://www.protocols.com/pbook/iso.htm

http://www.dcbnet.com/notes/9611t1.html

http://www.ietf.org/rfc/rfc1195.txt

http://www.marconi.ca/media