UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

CONVERGENCIA DE SERVICIOS DE VOZ Y DATOS SOBRE REDES DE ACCESO METRO E INALÁMBRICO Y ENLACES DE RESPALDO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ROBERT SAMUEL SANCHEZ BLAS

PROMOCIÓN
2000 - I

LIMA – PERÚ
2010

CONVERGENCIA DE SERVICIOS DE VOZ Y DATOS SOBRE REDES DE ACCESO METRO E INALÁMBRICO Y ENLACES DE RESPALDO

DEDICATORIA

A mi madre Yadira, por su entereza, por su dedicación a esposo, hijos y nietos, por su lucha en la vida a pesar de las circunstancias que enfrentó, el ejemplo que quiero seguir.

SUMARIO

El mundo de la integración de servicios de datos y voz a nivel corporativo o empresarial, hace que dichas organizaciones crean la necesidad de interactuar con sus oficinas y/o sedes a través de una red privada virtual; y para ello implementan su propia infraestructura de telecomunicaciones o establecen un socio tecnológico que en la mayoría de las veces, por un factor económico, es un proveedor de servicios de telecomunicaciones. Éste último ofrece una infraestructura de red de datos quebrinda servicios y soluciones de conectividad. Lo más importante a través del uso de nuevas tecnologías, es la capacidad de segmentar en forma segura múltiples sedes, servicios y aplicaciones mientras operan en una simple red basada en técnicas de conmutación y enrutamiento de un protocolo de comunicaciones dado, en este caso el Protocolo de Internet.

ÍNDICE

INTRODUCCIÓN

En la actualidad las necesidades de las empresas en sus telecomunicaciones son imprescindibles debido a sus requerimientos de información comoactualizacióne intercambio entre aéreas internas y externas de voz y datos, es por este motivo que se tiene la necesidad de contar con garantías en la calidad del servicio y alta disponibilidad en elenvío y recepción de las mismas, se pueden elegir diversas soluciones a estas necesidades de acuerdo a las características de la infraestructura de la red de la empresa.

Se tienen diversos modelos que se pueden adaptar a las necesidades de la empresa para brindar una solución que tenga respaldo y priorizar determinados servicios de acuerdo a una regla determinada porla empresa y/o los usuarios con el fin de mantener un adecuado servicio de acuerdo a los requerimientos, para el presente informe se implementará, desarrollará y analizará un proyecto para brindar la solución indicada, diferenciando los elementos que intervienen tanto físicamente como lógicamente.

En el primer capítulo se realiza la presentación, objetivo, análisis y consideraciones el proyecto también la topología de red, protocolos de comunicaciones que se usan para manejar diversas funciones entre capas las cuales proporcionan o con la cual es posible la comunicaciones entre servicios.

En el segundo capítulonos centraremos endesarrollar y entender los conceptos que proporcionan la tecnología tanto en la parte teórica comoen los elementosfísicos utilizados como medio de transportes Fibra Óptica, enlaces inalámbricos, enlaces de Cobre y dispositivos de capa física, la interacción entre estos elementos, las tecnologías usadas para este fin y las técnicas y estándares utilizadas, los protocolos de la capa de acceso a la red, los protocolos de la capa de red y la forma en que las aplicaciones finales interactuaran con estos elementos.

En el tercer capítulo se desarrollaráel planteamiento del problema y la solución de la misma describiendo los enlaces de respaldo y los tipos de protocolos usados para este

fin, se detallara las tecnologías para aplicar calidad de servicio para garantizar la transmisión de ciertos tipos de datos en un tiempo determinado, sobre los diferentes medios de transmisión y la convergencia de los servicios en un determinado medio, todo esto soportado sobre la infraestructura de red a nivel transporte, enrutamiento y servicio de voz e interconexión entre locales remotas local y nacional brindados por un determino proveedor local.

Finalmente en el cuarto capítulo se realiza un análisis del desarrollo de este proyecto, mostrando las cualidades de la solución en toda la red, tanto del cliente como del proveedor de servicios.

Este informe tiene como propósito la puesta en operación de un enlace de datos para brindar un servicio corporativo, con altas prestaciones, tratando los medios empleados tanto en recursos económicos, mano de obra y aplicación de las tecnologías existentes en nuestro medio, ajustando estos parámetros para un eficaz uso de los recursos, se realizará un análisis del comportamiento de todos los servicios implementados comparando valores como tiempo de implementación e instalación, tiempo de respuesta de los servicios de datos y voz, acuerdo de nivel de servicio, tiempo de convergencia en caso de averías.

CAPITULO I
OBJETIVOS Y DESCRIPCIÓN DE LA PROBLEMÁTICA

1.1. Presentación

Se presenta el caso para implementar los servicios para de una corporación donde tienen la necesidad de habilitar enlaces de voz y datos con altas prestaciones que para este caso son calidad de servicio y alta disponibilidad para el envió de datos, se tiene el escenario con tres sedes alejadas geográficamente, una sede está definida como sede principal y dos como sedes remotas (Figura 1.1), se tiene la necesidad de tener enlaces de contingencia para cada una de las tres sedes, a nivel de enlace físico y también enlace lógico tomando en cuenta el respaldo a nivel de enlace con conmutación y a nivel de red con protocolos de enrutamiento, todo esto será completamentetransparente a las funciones que se realizan en las tres sedes, según esto todas las sedesmantendrán internamente y externamente comunicación y no percibirán evento alguno sobre sus servicios.

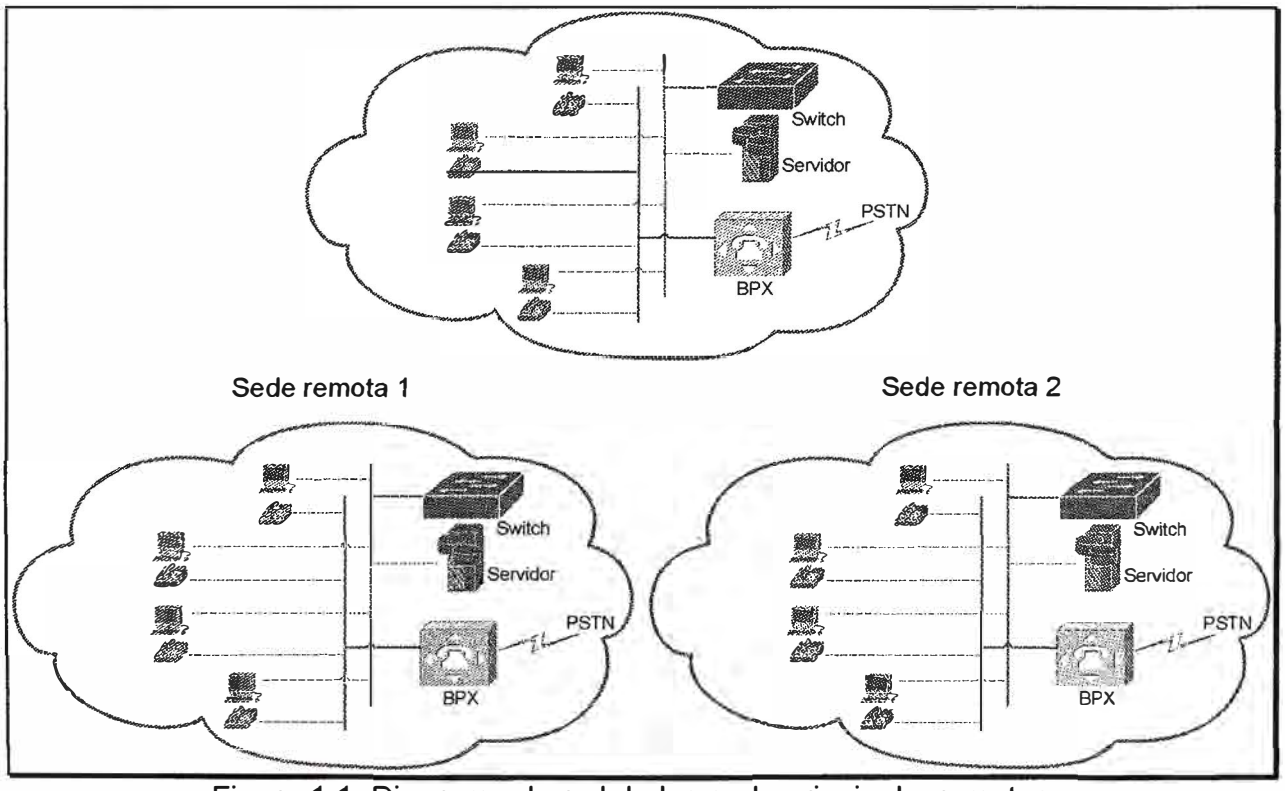

Figura 1.1. Diagrama de red de las sede principal y remotas.

Las sedes principal y remotas cuentan independientemente con servicios de Internet, Datos a nivel LAN, y servicio de telefonía analógica corporativa conectado a la red PSTN,

el problema presentado es la falta de interacción directa entre las sedes para sus servicios tanto de datos como de VOZ, a la vez que presenta servicios de Internet para cada sede lo cual eleva el costo por cada sede remota.

1.2. Objetivos del trabajo

Diseñar una solución viable de acuerdo a las necesidades de la empresa con las tecnologías presentes en la localidad y en los proveedores de servicio, implementar el diseño desarrollado ajustándose a las condiciones físicas y económicas de la empresa, los equipo y las tecnologíasutilizadas para este proyecto deben superar los servicios actuales brindando mayor rendimiento y comodidad, reflejándose en disminución de costos y horas hombre.

1.3. Análisis del sistema planteado

Para este proyecto se utiliza un modelo ya implementado en soluciones para redes de datos y áreas de trabajo con enlaces entre estaciones de trabajo que requieren enlaces con respaldo aplicando protocolos de enrutamiento dinámico, para este caso protocolo de enrutamiento BGP (Border Gateway Protocol), se realizará un estudio de los tipos de dispositivos a utilizar como router, switch y concentradores (Hub), los servicios de voz que brinda el proveedor de servicios, revisando sus especificaciones y las recomendaciones de los fabricantes y los requerimientos de la empresa para sus servicios, se tomara en cuenta los ancho de banda requerido según las necesidades de la empresa, la cantidad de usuarios en cada sede tanto principal y remotas, se realizará el diseño y la implementación revisando estos datos, realizando pruebas con los servicios implementados garantizando el correcto funcionamiento de los mismos.

1.4. Consideraciones del proyecto

Se implementa la solución planteada utilizando una arquitectura basado en enlaces con tecnología MetroEthernet, wireless en este caso WiMAX, última milla con fibra óptica utilizando un conversor de medios, los enlaces entre los diferentes locales serán brindados por un proveedor de enlace de datos con el siguiente esquema, cada sede tanto principal como remota tendrá dos enlaces, un primer enlace con fibra óptica como última milla y un segundo enlace inalámbrico, por un mismo medio físico se brindaran los diferentes servicios separándolos con enlaces lógicos utilizando sub interfaces lógicas, en los dispositivos locales se realizará una configuración a nivel de ruteo utilizando protocolos de enrutamiento dinámicos, estos protocolos serán los que redireccionen el tráfico hacia los enlaces lógicos o las interfaces lógicas, proporcionando contingencia a nivel de capa de red.

Se estudiara el protocolo de enrutamiento dinámico aplicado, revisando y comparando con otros protocolos y las razones por el cual se eligió este protocolo, se revisara la infraestructura de red del proveedor de servicios las razones para su elección y cuál es el impacto de esta red sobre la red de la empresa, los beneficios y perjuicio del mismo sobre la red de la empresa, en la implementación también se tomara en cuenta la aplicación de políticas para garantizar alto rendimiento de cierto tipo de servicio como por ejemplo las comunicaciones de voz y ciertos datos críticos, finalmente la aplicación de los enlaces de respaldo en la red de la empresa y en la red del proveedor de servicios de datos.

1.5. Topología de la red

Se da el caso con tres sede remotas (una considerada principal) la topología inicial antes de implementar el proyecto es de tres redes de área local separada e independientes cada una de otra, en cada sede se tiene las estaciones de trabajo conectadas a un switch por lo que la topología sería Bus, esto lo detallamos en la figura 1.2.

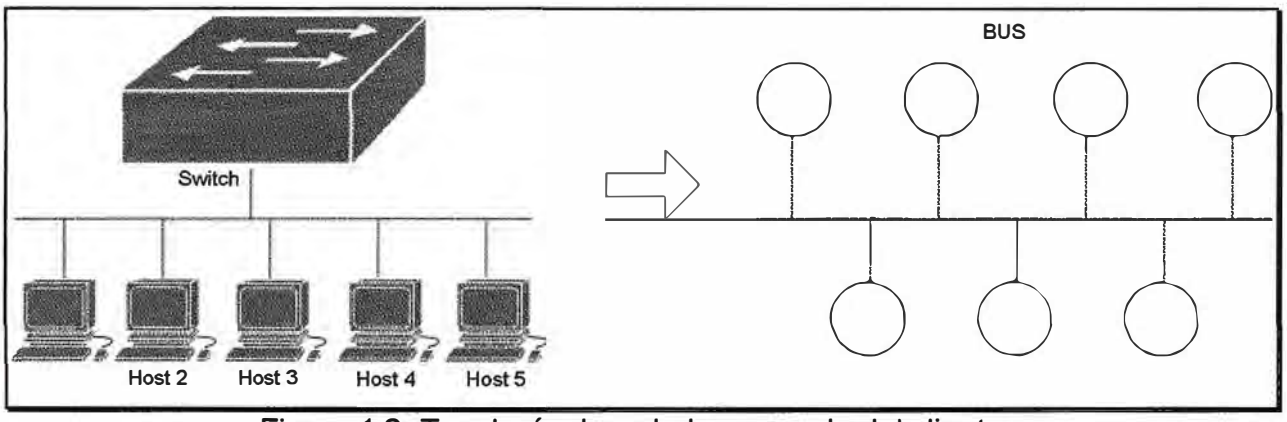

Figura 1.2. Topología de red de una sede del cliente.

La nueva topología implementada de lado del cliente será mixto, mezcla entre topología Bus y Conexa, el cual detallaremos en la figura 1.3.

Revisandola topología en modo global teniendo en cuenta la infraestructura de red del proveedor de servicios, la topología seria también mixta pero mucho más compleja el cual trataremos de resumir de modo de podamos utilizar para nuestro caso para el análisis, cuestionamientos y finalmente para las conclusiones, se debe resaltar los enlaces en la sede principal serian doble conexiones inalámbricas y doble conexiones alámbricas, el enlace entre las sedes a nivel de capa de enlace de datos y protocolo de red serán netamente por la red del proveedor de servicio de datos, figura 1.4.

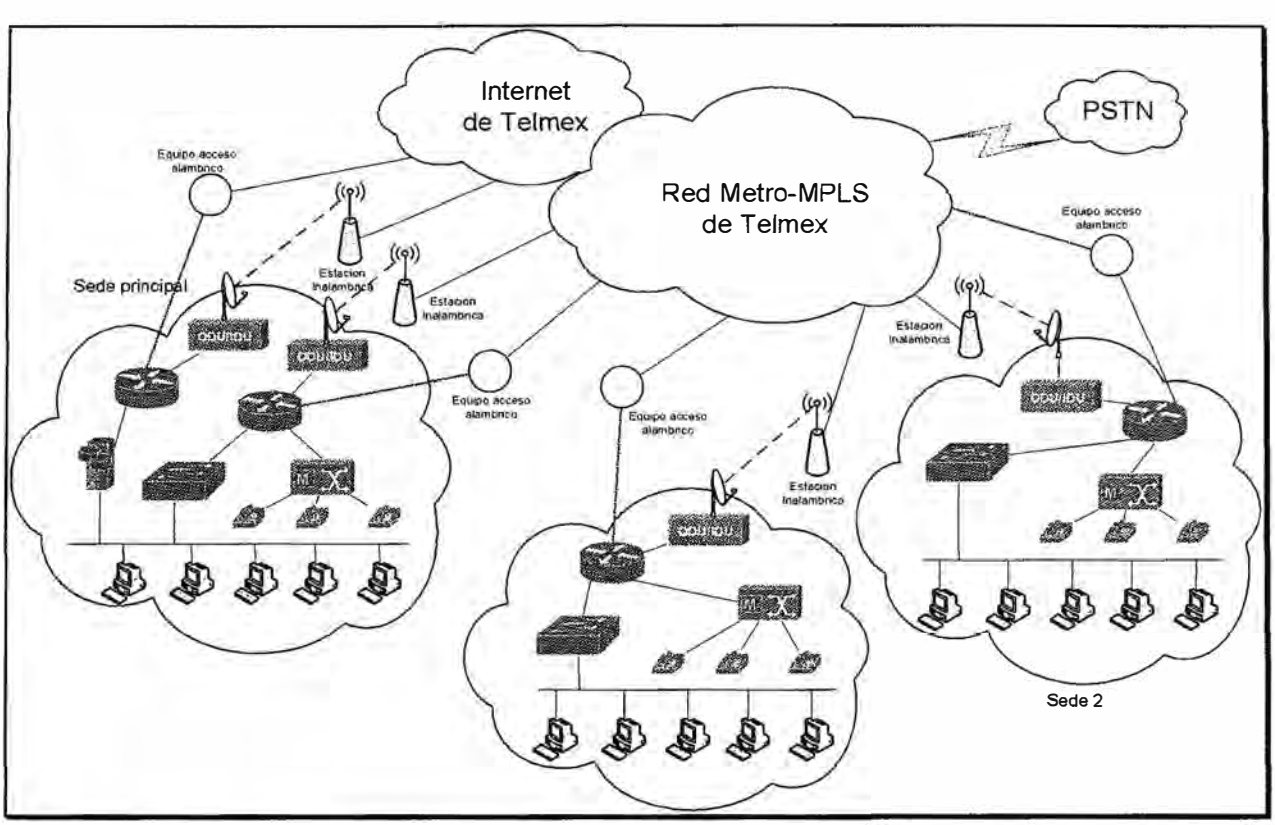

Figura 1.3. Topología de red del cliente.

1.6 Protocolo de las capas enlace de datos y de red

Siguiendo el esquema del modelo OSI se crearon numerosos protocolos, el advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano.Se detallará los protocolos usados en este proyecto, iniciando con el protocolo de la capa de enlace de datos y luego los protocolos de la cada de red.

1.6.1. Capa de enlace de datos

La Capa de Enlace de Datos es la responsable del intercambio de datos entre un host cualquiera y la red a la que está conectado, permitiendo la correcta comunicación y trabajo conjunto entre las capas superiores (Red, Transporte y Aplicación) y el medio físico de transporte de datos.Tiene como objetivo convertir la corriente de bits en bruto en una corriente de marcos o tramas y enviandola información o flujo de datos sin errores entre dos dispositivos conectados directamenteusando direcciones de Hardware y traducirán los mensajes de la capa de red en bits para que la capa física los transmita.

1.6.2. Capa de red

La capa de red, según la normalización OSI, es una capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es

conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones.

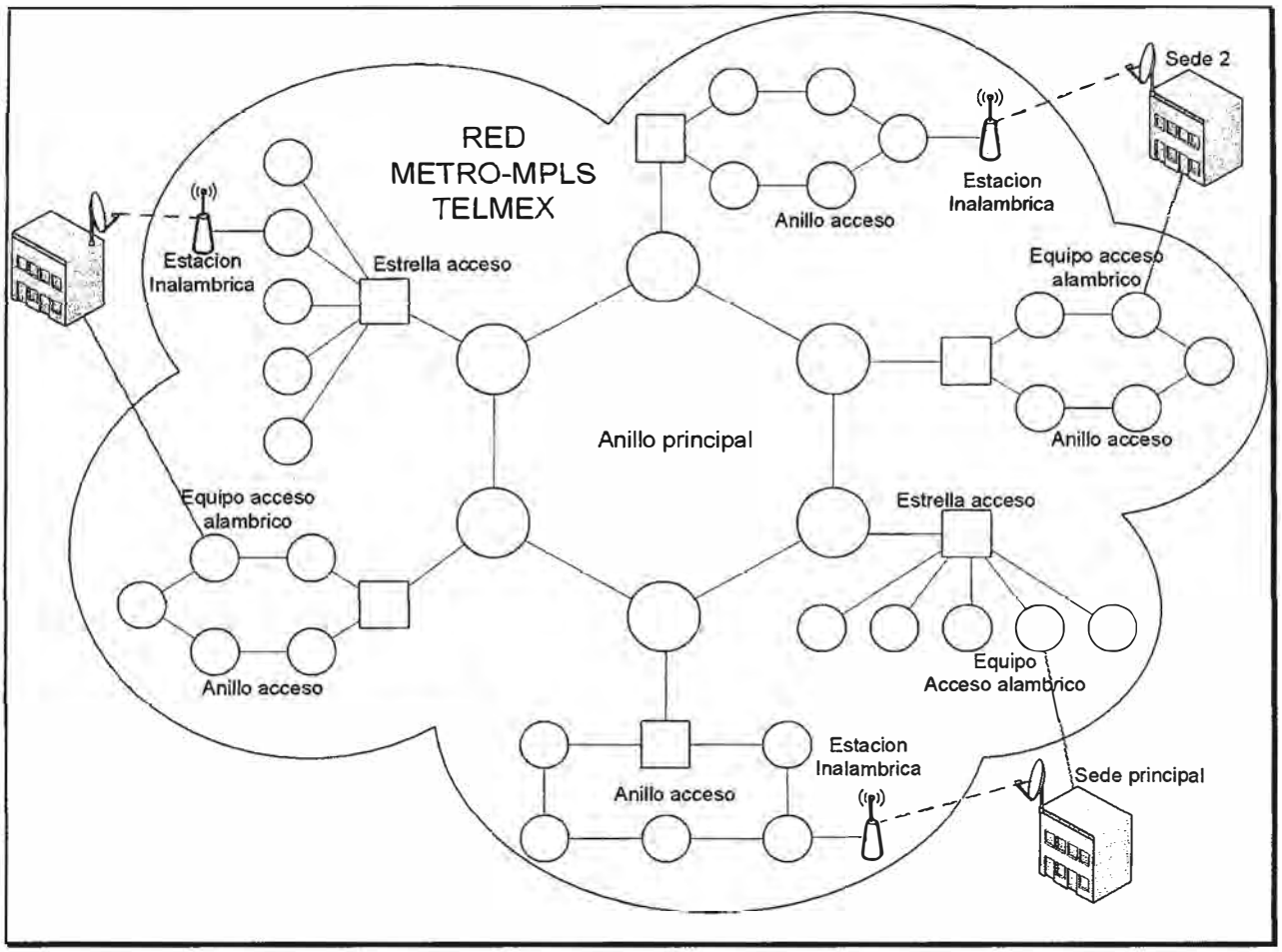

Figura 1.4. Topología de red del proveedor de servicio.

Para la consecución de su tarea, puede asignar direcciones de red únicas, interconectar subredes distintas, encaminar paquetes, utilizar un control de congestión y control de errores.

CAPITULO II
MARCO TEÓRICO CONCEPTUAL

2.1. Definiciones y funciones de la capa de enlace de datos

La capa de enlace de datos (data link layer) usa unidades de datos llamadas frames; y se construyen con el encabezado que contiene las direcciones físicas o de hardware de destino y de origen. Esta información encapsula el mensaje original para que el viaje por la red local pueda ser exitoso.

La capa de enlace de datos se divide en dos partes:

a. La de Media Access Control (MAC), que es la que interactúa con la capa física, y que se define por los estándares 802.5 (token ring) y 802.3 (ethernet), y define como se sitúan los paquetes en el medio de transmisión, es decir, controla la entrada al medio. También define las direcciones físicas y la topología lógica. También se tienen la disciplina de línea, notificaciones de error (pero no corrección), entrega ordenada de frames, y control de flujo opcional.

b. Y la de Logical Link Control (LLC) definida por el estándar IEEE 802.2. Identifica los protocolos de la capa de red y los encapsula con la información de la capa de enlace de datos para construir el frame. También hace el control de flujo y la secuencia de los bits de control.

La cabecera de una trama de red de área local (LAN) contiene las direcciones físicas del origen y el destino de la LAN. La cabecera de una trama que se transmite por una red de área extensa (WAN) contiene un identificador de circuito en su campo de dirección, figura 2.1.

La capa de enlace de datos es responsable de la transferencia fiable de información a través de un Circuito eléctrico de transmisión de datos. La transmisión de datos lo realiza mediante tramas que son las unidades de información con sentido lógico para el intercambio de datos en la capa de enlace. También hay que tener en cuenta que en el modelo TCP/IP se corresponde a la segunda capa.

Sus principales funciones son:

a. Iniciación, terminación e identificación.
b. Segmentación y bloqueo.

c. Sincronización de octeto y carácter.
d. Delimitación de trama y transparencia.
e. Control de errores.
f. Control de flujo.
g. Recuperación de fallos.
h. Gestión y coordinación de la comunicación.

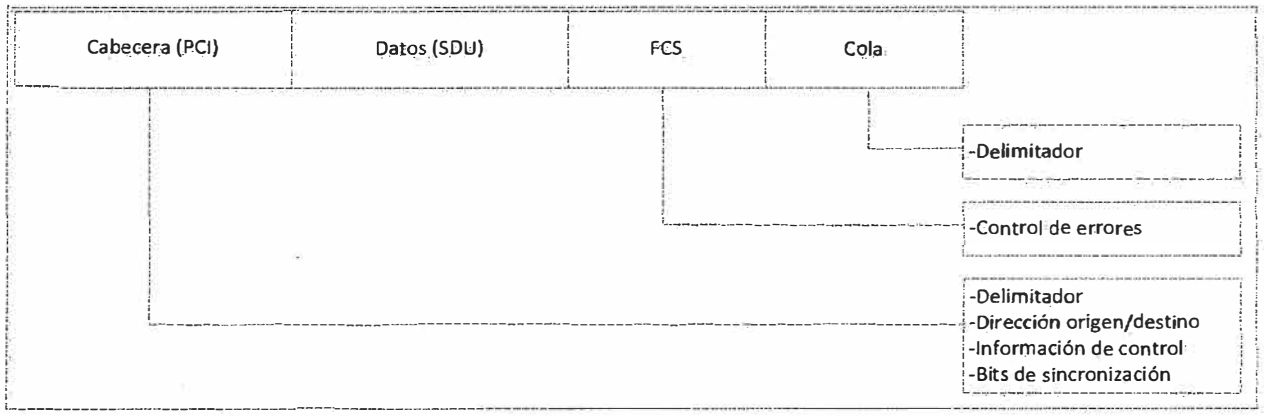

Figura 2.1. Trama de la capa de enlace de datos.

2.2. Protocolo IEEE 802.1Q

El protocolo IEEE 802.1Q fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking). Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet.

802.1Q en realidad no encapsula la trama original sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

Debido a que con el cambio del encabezado se cambia la trama, 802.1Q fuerza a un recálculo del campo "FCS".

El punto 9 del estándar define el protocolo de encapsulamiento usado para multiplexar varias VLAN a través de un solo enlace, e introduce el concepto de las VLAN nativas. Las tramas pertenecientes a la VLAN nativa no se etiquetan con el ID de VLAN cuando se envían por el trunk. Y en el otro lado, si a un puerto llega una trama sin etiquetar, la trama se considera perteneciente a la VLAN nativa de ese puerto. Este modo

de funcionamiento fue implementado para asegurar la interoperabilidad con antiguos dispositivos que no entendían 802.1Q.

La VLAN nativa es la vlan a la que pertenecía un puerto en un switch antes de ser configurado como trunk. Sólo se puede tener una VLAN nativa por puerto.

Para establecer un trunking 802.1q a ambos lados debemos tener la misma VLAN nativa porque la encapsulación todavía no se ha establecido y los dos switches deben hablar sobre un link sin encapsulación (usan la nativa VLAN) para ponerse de acuerdo en estos parámetros. En los equipos de Cisco Systems la VLAN nativa por defecto es la VLAN 1. Por la VLAN 1 además de datos, se manda información sobre PAgP, CDP, VTP.

2.3. Virtual LAN

Una VLAN (acrónimo de Virtual LAN, 'red de área local virtual') es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del Dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3).

Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. Una de las mayores ventajas de las VLANs surge cuando se traslada físicamente algún ordenador a otra ubicación: puede permanecer en la misma VLAN sin necesidad de cambiar la configuración IP de la máquina.

El protocolo de etiquetado IEEE 802.1Q domina el mundo de las VLANs. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com.

Los primeros diseñadores de redes enfrentaron el problema del tamaño de los dominios de colisión (Hubs) esto se logró controlar a través de la introducción de los conmutadores pero a su vez se introdujo el problema del aumento del tamaño de los dominios de difusión y una de las formas más eficientes para manejarlo fue la

introducción de las VLANs. Las VLANs también pueden servir para restringir el acceso a recursos de red con independencia de la topología física de ésta, si bien la robustez de este método es discutible al ser el salto de VLAN (VLAN hopping) un método común de evitar tales medidas de seguridad.

Las VLANs funcionan en el nivel 2 (enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red).

En el contexto de las VLANs, el término trunk ('troncal') designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o tags) insertadas en sus paquetes. Dichos trunks deben operar entre puertos etiquetados ('tagged ports') de dispositivos con soporte de VLANs, por lo que a menudo son enlaces conmutador a conmutador o conmutador a enrutador más que enlaces a nodos. (Para mayor confusión, el término trunk también se usa para lo que Cisco denomina «canales»; véase agregado de enlaces). Un enrutador (conmutador de nivel 3) funciona como columna vertebral para el tráfico de red transmitido entre diferentes VLANs.

En los dispositivos Cisco, VTP (VLAN Trunking Protocol) permite definir dominios de VLAN, lo que facilita las tareas administrativas. VTP (Cisco) también permite «podar», lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino.

Con las VLANes con pertenencia basada en el puerto de conexión del switch, el puerto asignado a la VLAN es independiente del usuario o dispositivo conectado en el puerto. Esto significa que todos los usuarios que se conectan al puerto serán miembros de la misma VLAN. Habitualmente es el administrador de la red el que realiza las asignaciones a la VLAN. Después de que un puerto ha sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3.

El dispositivo que se conecta a un puerto, posiblemente no tenga conocimiento de la existencia de la VLAN a la que pertenece dicho puerto. El dispositivo simplemente sabe que es miembro de una sub-red y que puede ser capaz de hablar con otros miembros de la sub-red simplemente enviando información al segmento cableado. El switch es responsable de identificar que la información viene de una VLAN determinada y de asegurarse de que esa información llega a todos los demás miembros de la VLAN. El

switch también se asegura de que el resto de puertos que no están en dicha VLAN no reciben dicha información.

Este planteamiento es sencillo, rápido y fácil de administrar, dado que no hay complejas tablas en las que mirar para configurar la segmentación de la VLAN. Si la asociación de puerto-a-VLAN se hace con un ASIC (acrónimo en inglés de Application-Specific Integrated Circuit o Circuito integrado para una aplicación específica), el rendimiento es muy bueno. Un ASIC permite el mapeo de puerto-a-VLAN sea hecho a nivel hardware.

2.4. Conmutación Multi-Protocolo mediante Etiquetas (MPLS)

MPLS (siglas de Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

Es una nueva tecnología de conmutación creada para proporcionar circuitos virtuales en las redes IP, sobre las que introduce una serie de mejoras:

a. Redes privadas virtuales.
b. Ingeniería de tráfico.
c. Mecanismos de protección frente a fallos.

Elementos [editar]LER (Label Edge Router): elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router. Ambos se suelen denominar Edge Label Switch Router ya que se encuentran en los extremos de la red MPLS.

a. LSR (Label Switching Router): elemento que conmuta etiquetas.
b. LSP (Label Switched Path): nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.
c. LDP (Label Distribution Protocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
d. FEC(Forwarding Equivalence Class): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

Cabecera MPLS, figura 2.2.

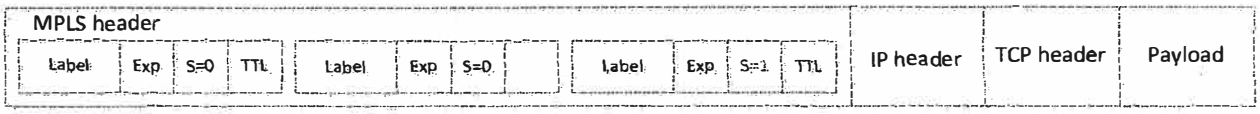

Figura 2.2. Trama de la capa de enlace de datos.

Dónde:

a. Label (20 bits): Es la identificación de la etiqueta.

b. Exp (3 bits): Llamado también bits experimentales, también aparece como QoS en otros textos, afecta al encolado y descarte de paquetes.

c. S (1 bit): Del inglés stack, sirve para el apilado jerárquico de etiquetas. Cuando S=0 indica que hay mas etiquetas añadidas al paquete. Cuando S=1 estamos en el fondo de la jerarquía.

d. TTL (8 bits): Time-to-Live, misma funcionalidad que en IP, se decrementa en cada enrutador y al llegar al valor de 0, el paquete es descartado. Generalmentesustituye el campo TTL de la cabecera IP.

Pila de Etiquetas MPLS, figura 2.3.

Figura 2.3. Trama de la capa de enlace de datos.

MPLS funciona anexando un encabezado a cada paquete. Dicho encabezado contiene una o más "etiquetas", y al conjunto de etiquetas se le llama pila o "stack". Cada etiqueta consiste en cuatro campos:

a. Valor de la etiqueta de 20 bits.

b. Prioridad de Calidad de Servicio (QoS) de 3 bits. También llamados bits experimentales.

c. Bandera de "fondo" de la pila de 1 bit.

d. Tiempo de Vida (TTL) de 8 bits.

Estos paquetes MPLS son enviados después de una búsqueda por etiquetas en vez de una búsqueda dentro de una tabla IP. De esta manera, cuando MPLS fue concebido, la búsqueda de etiquetas y el envío por etiquetas eran más rápido que una búsqueda RIB (Base de información de Ruteo), porque las búsquedas eran realizadas en el switch fabric y no en la CPU.

2.5. Definiciones y funciones de la capa de red

El nivel de red o capa de red, según la normalización OSI, es un nivel o capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden

estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa. Ofrece servicios al nivel superior (nivel de transporte) y se apoya en el nivel de enlace, es decir, utiliza sus funciones.

Para la consecución de su tarea, puede asignar direcciones de red únicas, interconectar subredes distintas, encaminar paquetes, utilizar un control de congestión y control de errores.

2.5.1. Orientación de conexión

Hay dos formas en las que el nivel de red puede funcionar internamente, pero independientemente de que la red funcione internamente con datagramas o con circuitos virtuales puede dar hacia el nivel de transporte un servicio orientado a conexión:

a. Datagramas: Cada paquete se encamina independientemente, sin que el origen y el destino tengan que pasar por un establecimiento de comunicación previo.

b. Circuitos virtuales: En una red de circuitos virtuales dos equipos que quieran comunicarse tienen que empezar por establecer una conexión. Durante este establecimiento de conexión, todos los enrutadores que hayan por el camino elegido reservarán recursos para ese circuito virtual específico.

2.5.2. Tipos de servicio

a. Servicios Conectivos: Sólo el primer paquete de cada mensaje tiene que llevar la dirección destino. Con este paquete se establece la ruta que deberán seguir todos los paquetes pertenecientes a esta conexión. Cuando llega un paquete que no es el primero se identifica a que conexión pertenece y se envía por el enlace de salida adecuado, según la información que se generó con el primer paquete y que permanece almacenada en cada conmutador o nodo.

b. Servicios No Conectivos: Cada paquete debe llevar la dirección destino, y con cada uno, los nodos de la red deciden el camino que se debe seguir. Existen muchas técnicas para realizar esta decisión, como por ejemplo comparar el retardo que sufriría en ese momento el paquete que se pretende transmitir según el enlace que se escoja.

2.5.3. Encaminamiento

Las técnicas de encaminamiento suelen basarse en el estado de la red, que es dinámico, por lo que las decisiones tomadas respecto a los paquetes de la misma conexión pueden variar según el instante de manera que éstos pueden seguir distintas rutas. El problema, sin embargo, consiste en encontrar un camino óptimo entre un origen

y un destino. La bondad de este camino puede tener diferentes criterios: velocidad, retardo, seguridad, regularidad, distancia, longitud media de las colas, costos de comunicación, etc.

Los equipos encargados de esta labor se denominan encaminadores (router en inglés), aunque también realizan labores de encaminamiento los conmutadores (switch en inglés) "multicapa" o "de nivel 3", si bien estos últimos realizan también labores de nivel de enlace.

La capa de red tiene diversos protocolos, para nuestro caso detallaremos el protocolo BGP.

2.5.4. Control de congestión

Cuando en una red un nodo recibe más tráfico del que puede procesar se puede dar una congestión. El problema es que una vez que se da congestión en un nodo el problema tiende a extenderse por el resto de la red. Por ello hay técnicas de prevención y control que se pueden y deben aplicar en el nivel de red.

2.6. Protocolo de enrutamiento de pasarela exterior (BGP)

Los protocolos de enrutamientos externo (BGP: Border Gateway Protocol)son los que se utilizan para interconectar Sistemas Autónomos. En los protocolos de enrutamiento externo la prioridad era buscar rutas optimas atendiendo únicamente al criterio de minimizar la 'distancia' medida en términos de la métrica elegida para la red.

La selección de rutas entre sistemas autónomos plantea un problema diferente,ya que la cuestión no se reduce a la selección de la ruta optima sino que se debe atender a criterios externos de tipo político,económico,administrativo, y otros.

Hasta 1990 se utilizaba como protocolo de enrutamiento externo en la Internet el denominado EGP(Exterior Gateway Protocol). Este protocolo no fue capaz de soportar el crecimiento de la Red y entonces se desarrolló un nuevo protocolo de enrutamiento externo denominado BGP. Desde entonces se ha producido 4 versiones de BGP, las especificaciones ahora vigentes de BGP-4 se encuentran en el RFC 1771.

BGP ES un protocolo de transporte fiable. Esto elimina la necesidad de llevar a cabo la fragmentación de actualización explícita, la retransmisión, el reconocimiento, y secuenciación.

2.6.1. Funciones de BGP

BGP se diseñó para permitir la cooperación en el intercambio de información de encaminamiento entre dispositivos de encaminamiento, llamados pasarelas, en sistemas autónomos diferentes. El protocolo opera en términos de mensajes, que se envían utilizando TCP. El repertorio de mensajes es el siguiente:

a. OPEN
b. UPDATE
c. KEEPALIVE
d. NOTIFICACION

BGP supone tres procedimientos funcionales:

a. Adquisición de vecino.
b. Detección de vecino alcanzable.
c. Detección de red alcanzable.

Dos dispositivos de encaminamiento se considera que son vecinos si están en la misma subred. Si los dos dispositivos de encaminamiento están en sistemas autónomos, podrían desear intercambiar información de encaminamiento. Para este cometido es necesario realizar primero el proceso de adquisición de vecino. Se requiere un mecanismo formal de encaminamiento ya que alguno de los dos vecinos podría no querer participar. Existirán situaciones en las que un vecino no desee intercambiar información esto se puede deber a múltiples factores como por ejemplo que este sobresaturado y entonces no quiere ser responsable del tráfico que llega desde fuera del sistema.

En el protocolo de adquisición de vecino, un dispositivo envía un mensaje de petición al otro, el cual puede aceptar o rechazar el ofrecimiento. El protocolo no indica cómo puede saber un dispositivo la dirección o incluso la existencia de otro dispositivo de encaminamiento. Estas cuestiones se tratan en el momento de establecer la configuración del sistema o por una intervención activa del gestor de la red.

Para llevar a cabo la adquisición de vecino, un dispositivo envía al otro un mensaje OPEN. Si el otro dispositivo acepta la relación, envía un mensaje de KEEPALIVE.

Una vez establecida la relación de vecino, se utiliza el procedimiento de detección e vecino alcanzable para mantener la relación. Este procedimiento consiste en enviarse

entre los dos vecinos periódicamente mensajes de KEEPALIVE para asegurarse de que la relación sigue establecida.

El último procedimiento especificado por BGP es la detección de red alcanzable. Cada dispositivo de encaminamiento mantiene una base de datos con las redes que puede alcanzar y la ruta preferida para llegar hasta esa red. Siempre que se realiza un cambio en esa base de datos, eldispositivo de almacenamientoenvía un mensaje de UPDATE por difusión a todos los dispositivos de encaminamiento que implementan BGP.

2.6.2. Porqué utilizar BGP

Existen situaciones específicas en las que es necesario utilizar BGP:

a. La organización se conecta a múltiples ISPs o ASs, se justifica el coste adicional utilizando estos enlaces reduciendo cuellos de botella y congestión. En este caso se necesitan decisiones de routing basadas en política basadas en el enlace.
b. La política de routing del ISP y el de la organización difieren y es necesario que exista comunicación.
c. El tráfico de la organización necesita diferenciar qué tráfico es de cada ISP.
d. La organización es un ISP, y debido a la naturaleza del negocio es necesario que el tráfico de otros ASs circule por el AS de la organización, funcionando como AS de tránsito.ruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

Por su implementación de políticas de enrutamiento, ya que son:

a. Escalable
b. Estable
c. Simple

2.6.3. eBGP y iBGP

Si un AS tiene múltiplesenrutadores BGP,podrían ser usados para ofrecer un servicio de tránsito para otros AS.

Cuando BGP está funcionando entre 2 diferentes AS lo llamamos exterior BGP (eBGP) figura 2.4.

a. Entre router en AS diferentes
b. Usualmente con conexión directa
c. Con next-hop apuntando a si mismo

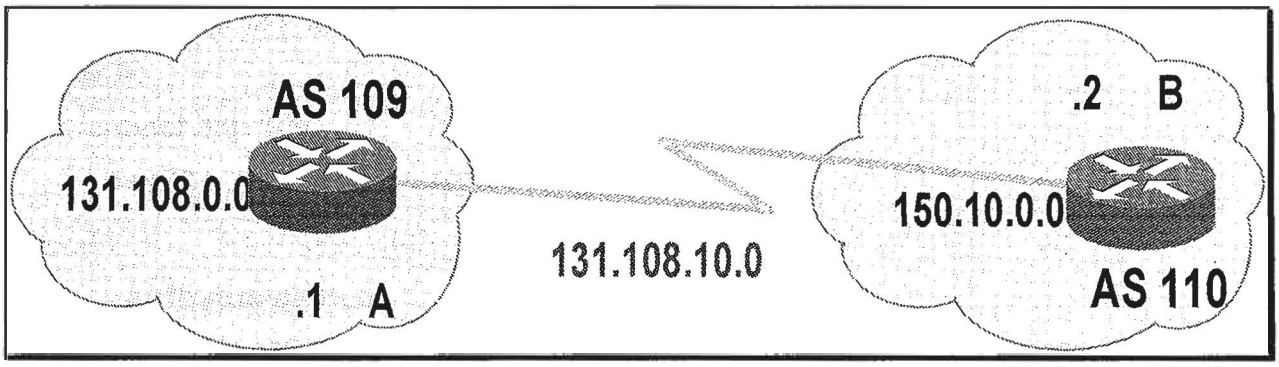

Figura 2.4. BGP Externo.

Router B

router bgp 110

neighbor 131.108.10.1 remote-as 109

Router A

router bgp 109

neighbor 131.108.10.2 remote-as 110

Cuando BGP esta funcionado en elmismo AS lo llamamos iBGP, figura 2.5.

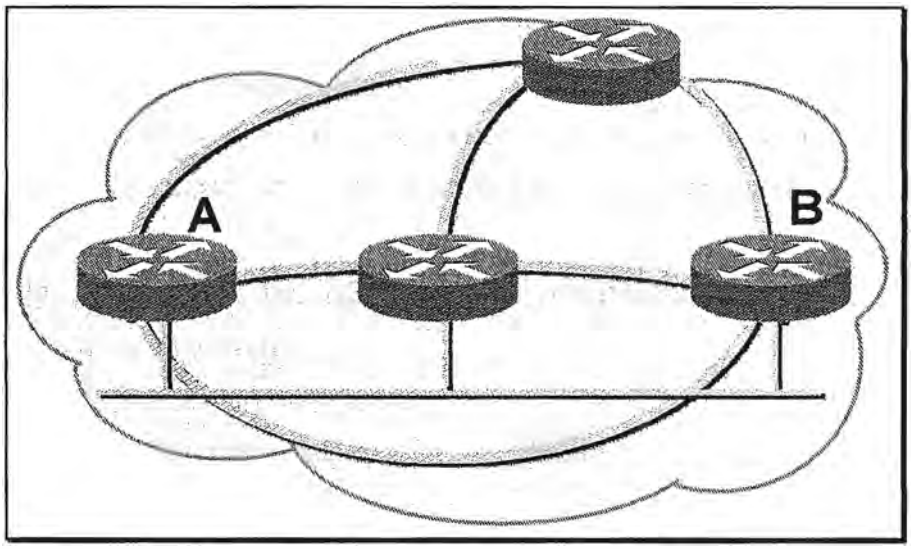

Figura 2.5. BGP Interno.

a. Vecinos en el mismo AS
b. No se modifica el Next-hop
c. No necesariamente con conexión directa
d. No anuncia otras rutas aprendidas por iBGP

Router B:

router bgp 109

neighbor 131.108.30.2 remote-as 109

Router A:

router bgp 109

neighbor 131.108.20.1 remote-as 109

2.6.4. Atributos de BGP

La clave de BGP es su capacidad de desviar el tráfico basándose en criterios determinados por los arquitectos de la red. BGP tiene que ver con la capacidad de manipular el flujo de tráfico a través de la red.

Estas características pueden ser utilizadas para distinguir los caminos (paths) al utilizar PBR. Así que la PBR utiliza los atributos de BGP para tomar decisiones sofisticadas en la selección del path.

BGP direcciona el flujo de tráfico utilizando atributos.

El uso de atributos se refiere al uso de variables en la selección del mejor camino para el protocolo deruta por defecto en el AS y una ruta estática es el AS del ISP o de la organización.

BGP utiliza atributos para seleccionar el mejor camino. Básicamente los atributos son la métrica de BGP.

Las variables describen características o atributos del camino al destino.

Mucha información transportada en los mensajes de actualización es más importante que otra.

Ya que la información de BGP en las actualizaciones varía en la red, la categorización es muy importante.

Los atributos se dividen en dos partes:

a. Well-known: Atributos que su utilización es obligatoria
b. Optional: Atributos opcionales.

Además cada una de las dos divisiones se dividen a su vez en dos más, permitiendo así una mayor granularidad.

2.7. Redes MPLS-VPN

Conmutación de MúltiplesProtocolos mediante Etiquetas(MPLS: Multi Protocol Label Switching), El crecimiento imparable de lasRedes, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a lasprácticas habituales desarrolladas a mitad de los años 90. Nuevas tecnologías detransmisión sobre fibra óptica, tales como Multiplexación por división en

longitudes de onda densas(DWDM), proporcionan una eficaz alternativa al Modo de Transferencia Asíncrona (ATM) para multiplexar múltiplesservicios sobre circuitos individuales. Además, los tradicionales conmutadores Modo de Transferencia Asíncrona (ATM)están siendo desplazados por una nueva generación de encaminadores (routers) con funcionesespecializadas en el transporte de paquetes en el núcleo de las redes. Esta situación secomplementa con una nueva arquitectura de red de reciente aparición, conocida comoConmutación de Múltiples Protocolos mediante Etiquetas(MPLS). MPLS se considera fundamental en laconstrucción de los nuevos cimientos para la Red del siglo XXI.

2.7.1. Características de MPLS

a. Mecanismo para manejar el flujo de tráfico de tamaños variados (Flow Management)
b. Es independiente de protocolos de capa 2 y 3
c. Mapea direcciones IP a rótulos de largo fijo
d. Interconecta a protocolos de existentes (RSVP, OSPF)
e. Soporta ATM, Frame-Relay y Ethernet

Conmutación de Múltiples Protocolos mediante Etiquetases acomodado entre capa 2 y capa 3, figura 2.6.

2.7.2. Túneles en MPLS

La idea es controlar el camino entero sin explícitamente especificar los router intermedios creando túneles a través de routers intermedios que pueden cubrir múltiples segmentos.

2.7.3. Aplicación en VPNs basadas en MPLS.

Una red privada virtual o VPN (siglas en inglés de virtual private network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.Es una red privada en términos lógicos, montada sobre un medio potencialmente compartido. Un conjunto de sitios a los que les es permitidocomunicarse mutuamente. Es el “ámbito alcanzable” por una tabla de rutas.El encaminador de borde de la Red Central y el encaminador del “cliente”usan el mismo protocolo de red para dialogar.El encaminador de cliente (CE) y el encaminador de la Red Central (PE)arman una adyacencia en los términos del protocolocomún. Los encaminadores de la red central conocen la información dedireccionamiento de los encaminadores de “cliente”. Su base es el modelo de pares, pero PEs reciben y mantienen información de rutas de lasVPNs directamente conectadas. Reduce la

cantidad de información que tiene quealmacenar un PE. Se usa MPLS para encaminar en la Red Central(no senecesita conocer información del cliente).

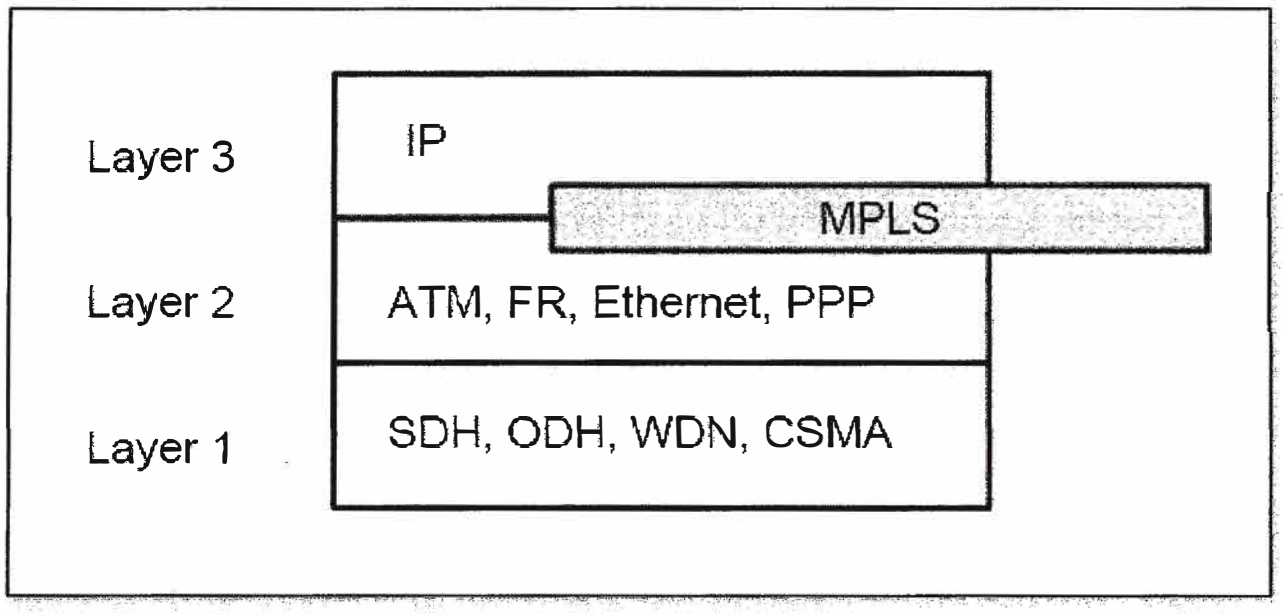

Figura 2.6. MPLS entre Capa 2 y 3.

Provee una solución que permita a Redes IP de gran escala ofrecer servicios de VPNs que escale a un gran número de clientes (100000 a 1000000 VPNs), servicios de Valor agregado, mejor aprovechamiento de la infraestructura existente.

El objetivo de las VPNs es elsoporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz,datos y video sobre infraestructuras de comunicaciones eficaces y rentables. Laseguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee losenlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo dered IP de la Internet. En esta sección se va a describir brevemente las ventajas queMPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras detransmisión compartidas con características implícitas de seguridad y respuestapredeterminada. Tal es el caso de las redes de datos Frame Relay, que permitenestablecer PVCs entre los diversos nodos que conforman la VPN. La seguridad y lasgarantías las proporcionan la separación de tráficos por PVC y el caudal asegurado(CIR) 9. Algo similar se puede hacer con ATM, con diversas clases de garantías. Losinconvenientes de este tipo de solución es que la configuración de las rutas se basa enprocedimientos más bien artesanales, al tener que establecer cada PVC entre nodos,con la complejidad que esto supone al proveedor en la gestión (y los mayores costesasociados). Si se quiere tener conectados a todos con todos, en una topología

lógicatotalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEsdel cliente y restablecer todos los PVCs.

Además, la popularización de las aplicaciones TCP/IP, así como la expansión delas redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para elsoporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño eimplantación y unos menores costes de gestión y provisión de servicio. La forma deutilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construirtúneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dosextremos, de modo que funcionalmente aparezcan conectados. Lo que se hace esutilizar una estructura no conectiva como IP para simular esas conexiones: unaespecie de tuberías privadas por las que no puede entrar nadie que no sea miembro deesa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNssobre túneles; se pretende tan sólo resumir sus características para poder apreciarluego las ventajas que ofrece MPLS frente a esas soluciones.

Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexionesconmutadas de acceso) se pueden establecer de dos maneras:

a. En el nivel 3, mediante el protocolo IPSec10 del IETF.
b. En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantizamediante el cifrado de la información de los datos y de la cabecera de los paquetes IP,que se encapsulan con una nueva cabecera IP para su transporte por la red delproveedor. Es relativamente sencillo de implementar, bien sea en dispositivosespecializados, tales como cortafuegos, como en los propios *routers* de acceso delNSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes dedistintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta lascabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya quela red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles deservicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otrosprotocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (nonecesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la reddel proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades deQoS para priorizar el

tráfico por tipo de aplicación IP. Los clientes VPN puedenmantener su esquema privado de direcciones, estableciendo grupos cerrados deusuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar lainformación por mayor seguridad, pero en este caso limitando las opciones QoS). Adiferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada aun único proveedor.

A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienenunas características comunes que las hacen menos eficientes frente a la soluciónMPLS:

a. Están basadas en conexiones punto a punto (PVCs o túneles).
b. La configuración es manual.
c. La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
d. Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.
e. La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, basados en túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo.

Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IPpara transportar la información del usuario, mientras que en MPLS esta informaciónse transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada elproceso de *routing* IP. Sin embargo, sí se mantiene en todo momento la visibilidad

IPhacia el usuario, que no sabe nada de rutas MPLS sino que ve un internet privado(intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicasQoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hastael destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecerCoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

2.8. Servicios de Softswitch

En un sistema de telefonía IP el término "Softswitch" engloba los procesos y elementos informáticos que controlan las sesiones, el medio (voz, video o mensajes) y los servicios. En términos sencillos, el Softswitch separa los elementos de la red (Hardware) del control de la misma (Software). Recordemos que en la telefonía TDM tradicional el hardware y software no pueden estar completamente separados. Las redes de conmutación de circuitos están diseñadas para comunicaciones telefónicas y se construyen con elementos (HW + SW) dedicados específicamente a determinadas funciones, mientras que en las redes modernas de conmutación de paquetes con el protocolo IP, se puede comunicar voz, datos e imágenes con dispositivos completamente genéricos, capaces de comunicar los diferentes medios. Estos dispositivos se controlan por el software que conforma el Softswitch.

El Softswitch está compuesto por uno o varios ordenadores que controlan el tráfico de VoIP e incluso las pasarelas entre el STDP y la VoIP en cuyo caso enlazan ambos tipos de red y gestionan el tráfico, que en el caso más general puede estar formado por una combinación de voz, fax, datos y video. Los Softswitches también se ocupan de que la señal se procese, en función del tipo de medio que sea, se negocie que tipo de codec se utilizará en cada sesión, o incluso se transcodifique de un codec a otro. Los softswitches están en el lado IP de las redes y se basan en el Protocolo SIP, Session Initiation Protocol, o en el Protocolo H.323. Las Redes de Nueva Generación, (NGN) emplean Softswitches basados en IMS.

No obstante lo anterior, la razón del softswitch no es solamente para separar el hardware del software, sino que pretende que haya un entorno abierto de software que facilite la creación de servicios. Se da por supuesto que las Redes Inteligentes del futuro no seguirán los modelos tradicionales de control de llamadas, que por proceder de la telefonía tradicional están limitados, y en su lugar empleará modelos basados en sesiones, capaces de comunicar datos, voz y servicios multimedia.

También es preciso señalar que un softswitch se puede entender como que es una fórmula centralizada (que cubre zonas o regiones geográficas) propia de una compañía telefónica, y que las empresas más pequeñas e ISPs generalmente no prestan sus servicios de telefonía IP mediante un softswitch, puesto que puede que prefieran emplear arquitecturas más sencillas del tipo peer-to-peer y componentes individualizados, de diferentes fabricantes o procedencias, figura 2.7.

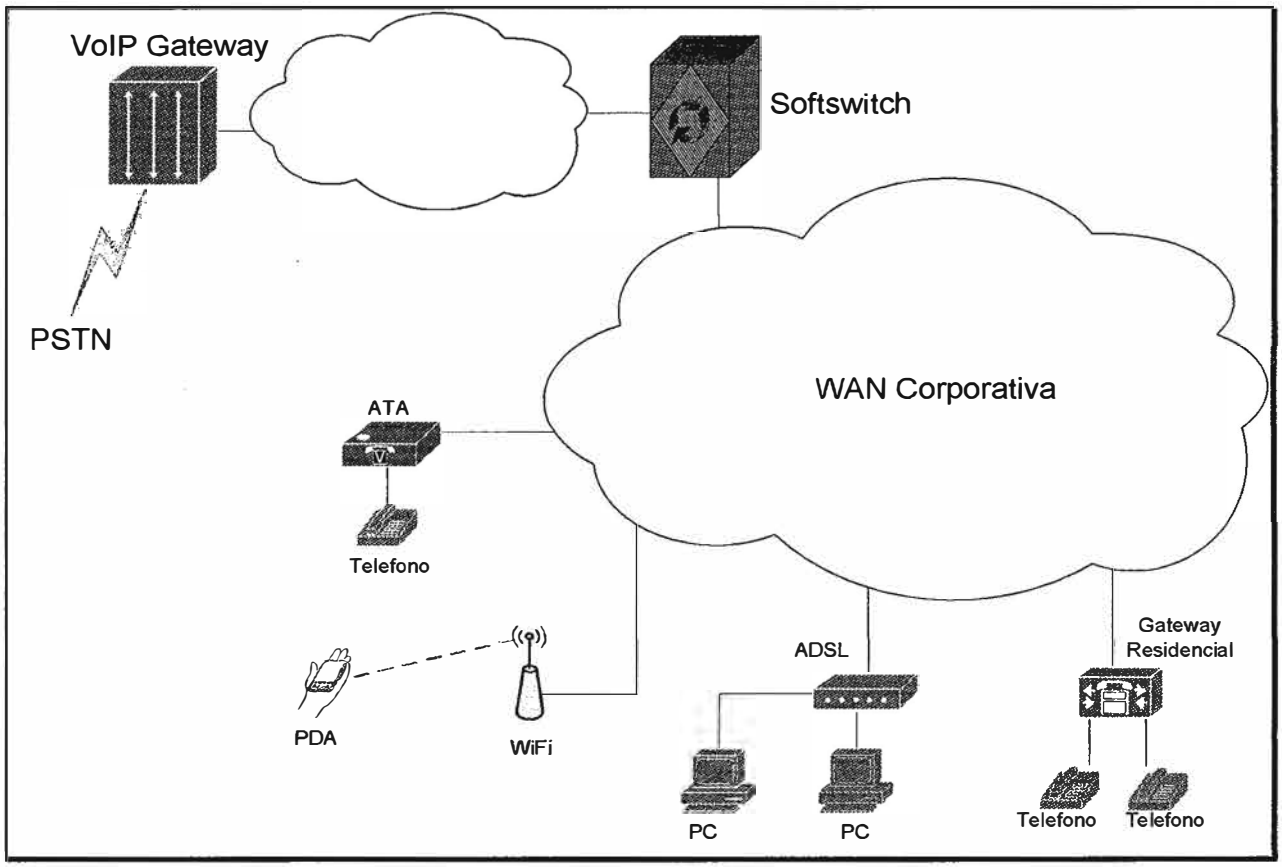

Figura 2.7. Arquitectura de Softswitch.

En redes IP en las que haya control sobre la calidad de servicio (mediante MPLS o IMS) la arquitectura Softswitch puede presentar ventajas. Incluso un operador puede emplear esta arquitectura para interconectar Softswitches entre sí.

Los Softswitches (o elementos especializados con otro nombre) localizan y registran a los usuarios, dialogan, al nivel más bajo, con los dispositivos UA donde se inician y terminan las comunicaciones. Controlan las pasarelas especializadas y los "Media Servers" que ofrecen locuciones, ponen a varios usuarios en conferencia, y consiguen que los medios atraviesen los Firewalls y NATs. También se ocupan de gestionar ENUM e incluso pueden usar dicha técnica para solucionar la portabilidad de número.

Y a un nivel más alto proporcionan servicios diversos, tanto al usuario como, por ejemplo, con servicios de presencia y relevancia de llamadas, como al operador (back office y OSS)

2.9. Calidad de servicio (QoS)

El concepto de calidad de servicio (o Quality of Service, QoS) en telecomunicaciones puede tener, al menos, dos interpretaciones habituales. En primer lugar, se refiere a la capacidad de determinadas redes y servicios para admitir que se fije de antemano las condiciones en que se desarrollarán las comunicaciones (dedicación de recursos, capacidades de transmisión, etc.). En segundo lugar, se habla de calidad de servicio como una serie de cualidades medibles de las redes y servicios de telecomunicaciones, como el tiempo que se tarda en realizar una llamada telefónica (desde que el usuario marca hasta que suena el teléfono en el otro extremo).

La calidad de servicio (QoS) es el rendimiento de extremo a extremo de los servicios electrónicos tal como lo percibe el usuario final. Los parámetros de QoS son: el retardo, la variación del retardo y la pérdida de paquetes. Una red debe garantizar un cierto nivel de calidad de servicio para un nivel de tráfico que sigue un conjunto especificado de parámetros.

La implementación de Políticas de Calidad de Servicio se puede enfocar en varios puntos según los requerimientos de la red, los principales son:

a. Asignar ancho de banda en forma diferenciada
b. Evitar y/o administrar la congestión en la red
c. Manejar prioridades de acuerdo al tipo de tráfico
d. Modelar el tráfico de la red

La implantación de calidad de servicio (QoS) en el backbone es esencial para el éxito de aplicaciones avanzadas, como telemedicina, videoconferencia y VoIP (voz sobre IP o telefonía sobre IP). Estas aplicaciones demandan, además de gran ancho de banda, un servicio diferenciado. En muchos casos es necesario garantizar que la transmisión de los datos sea realizada sin interrupción o pérdida de paquetes.

2.10. Tecnologías de acceso a la red del proveedor de servicios

2.10.1. Equipo local del cliente

Son los terminales o equipo situado en el lado del suscriptor (CPE por sus siglas en ingles de Customer Premises Equipment), para nuestro caso el terminal del suscriptor es el encaminador (router) marca Cisco y las características del equipo deben soportar todos los servicios que se atenderán para el cliente.

2.10.2. Última milla

Es el tramo final o enlace físico entre los equipos de acceso del proveedor de servicios y el usuario o suscriptor final, es decir el cableado o enlace inalámbrico que va desde el punto de presencia de la red del proveedor de servicios hasta la ubicación física del cliente al que se le presta el servicio. Por lo general el costo de la instalación de la última milla es el 90% del total del costo de instalación del servicio.La última milla puede ser vía par de cobre, fibra óptica, laser o inalámbrica.

2.10.3. Fibra óptica como medio físico

Las redes ópticas destraban el cuello de botella del acceso aumentando el anchode banda y la calidad de servicio.

Se pueden clasificar en dos tipos:

a. Por el uso de elementos pasivos y/o activos conocidos como redes ópticas pasivas (PON por sus siglas en inglés Passive Optical Network).

b. Por la cercanía del tramo de fibra al domicilio del cliente.

Una red óptica pasiva (PON) es una única fibra óptica bidireccional y compartidaque utiliza acopladores ópticos para ramificarse formando una económica red deacceso con topología punto – multipunto hasta el usuario final.

Utiliza fibra monomodo y divisores ópticos pasivos para dar servicio a los clientesresidenciales y pequeños abonados de negocios. La red, presenta una divisiónóptica de la señal por medio de un splitter con una entrada y 16 salidas, porejemplo.

En el caso de usuarios residenciales se instala la fibra hasta su domicilio (FTTH,Fiber to the home, fibra hasta el hogar) y, mediante el empleo de una unidaddenominada ONU (Optical Network Unit, unidad de red óptica) se le proporcionael servicio de video a través del STB (Set top Box, equipo para la recepción detelevisión) conectado a la TV, y telefónico o de transmisión de datos, se utiliza latécnica con transmisión DWDM (Dense wavelenght división multiplexing,multiplexación de longitud de onda densa), algunas

empresas y proveedores deservicios montan Gigabit Ethernet sobre fibra oscura arrendada.

Al ser toda la infraestructura de fibra óptica, se proporciona una transmisión muysegura y libre de errores, con una alta capacidad de transferencia si se emplea,por ejemplo, un protocolo como ATM. Al anillo se puede conectar una LAN (LocalÁreaNetwork, red de área local) a través de un cortafuego (firewall), para separarla Intranet de Internet.

2.10.4. Enlace inalámbrico como medio físico

En estas redes los clientes se conectan a la red usando señales de radio enreemplazo del cobre, en parte o en toda la conexión entre el cliente y el equipo de acceso del proveedor de servicios.

Esta técnica de acceso es muy utilizada en regiones donde las redes están aúnen desarrollo, además resulta ideal para un rápido despliegue de red.

La ventaja clara de este tipo de sistemas es la reducción de los costos deinfraestructura, además del pequeño margen de tiempo necesario para sufuncionamiento, puesto que en el momento en que se dispone de la radio base,se llega inmediatamente a miles de usuarios a través de sus antenas receptores.

Los sistemas requieren línea de vista y reutilización de frecuencias del espectro,para nuestro caso utilizamos tecnología WIMAX 3.5G.

Generalmente, tanto los CPEs como las radio bases tienen unidades internas(IDU) y unidades externas (ODU), el equipo terminal en el lado del suscriptor estáformado por una unidad externa o antena exterior ubicada en una parte alta(necesita línea de vista hacia la radio base) y una unidad interior que es la interfazcon el usuario, por medio de la cual recibe los diferentes servicios.

En la estación base es donde se realiza la conversión de la infraestructura de fibra hacia la infraestructura inalámbrica. Los equipos que permiten la conversiónincluyen la interfaz de red para la terminación de fibra, funciones de modulación ydemodulación, equipos de transmisión y recepción de microondas ubicados en torres o mástiles.

2.10.5. Metro Ethernet como tecnología de acceso

La Red Metro Ethernet, es una arquitectura tecnológica destinada a suministrar servicios de conectividad MAN/WAN de nivel 2, a través de UNIs (User Network Interface)Ethernet. Estas redes denominadas "multiservicio", soportan una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye soporte a tráfico en tiempo real(RTP por sus siglas en ingles Real-time Transport Protocol), como puede ser Telefonía IP y Video IP, este tipo de trafico resulta especialmente sensible a retardo, ala fluctuaciónde la señal de reloj (en inglésjitter) y a la baja o poca señal(en inglésgrudge).

La utilización de las líneas de cobre (MAN BUCLE), garantiza el despliegue de un punto de red ethernet, en cualquier punto de la zona urbana.

Las redes Metro Ethernet, están soportadas principalmente por medios de transmisión guiados, como son el cobre (MAN BUCLE) y la fibra óptica, existiendo también soluciones de radio licenciada, los caudales proporcionados son de 10Mbps, 20Mbps, 34Mbps, 100Mbps, 1Gbps y 10Gbps.

La tecnología de agregación de múltiples pares de cobre, (MAN BUCLE), permite la entrega de entre 10 Mbps, 20 Mbps, 34Mbps y 100Mbps, mediante la transmisión simultánea de múltiples líneas de cobre, además esta técnica cuenta con muy alta disponibilidad ya que imposible la rotura de todas las líneas de cobre y en caso de rotura parcial el enlace sigue transmitiendo y reduce el ancho de banda de forma proporcional.

La fibra óptica y el cobre, se complementan de forma ideal en el ámbito metropolitano, ofreciendo cobertura total a cualquier servicio, a desplegar

Los beneficios que Metro Ethernet ofrece son:

a. Presencia y capilaridad prácticamente "universal" en el ámbito metropolitano, en especial gracias a la disponibilidad de las líneas de cobre, con cobertura universal en el ámbito urbano.

b. Muy alta fiabilidad, ya que los enlaces de cobre certificados Metro Ethernet, están constituidos por múltiples pares de en líneas de cobre (MAN BUCLE) y los enlaces de Fibra Óptica, se configuran mediante Spanning tree (activo-pasivo) o LACP (caudal Agregado).

c. Fácil uso: Interconectando con Ethernet se simplifica las operaciones de red, administración, manejo y actualización

d. Economía: los servicios Ethernet reducen el capital de suscripción y operación de tres formas:

- Amplio uso: se emplean interfaces Ethernet que son la más difundidas para las soluciones de Networking
- Bajo costo: Los servicios Ethernet ofrecen un bajo costo en la administración, operación y funcionamiento de la red.
- Ancho de banda: Los servicios Ethernet permiten a los usuarios acceder a conexiones de banda ancha a menor costo.

e. Flexibilidad: Las redes de conectividad mediante Ethernet permiten modificar y manipular de una manera más dinámica, versátil y eficiente, el ancho de banda y la cantidad de usuarios en corto tiempo.

El modelo básico de los servicios Metro Ethernet, está compuesto por una Red conmutada MEN (Metro Ethernet Network), ofrecida por el proveedor de servicios; los usuarios acceden a la red mediante CPEs (Customer Premises Equipment), CPE puede ser un router; Bridge IEEE 802.1Q (switch) que se conectan a través de UNIs (User Network Interface) a velocidades de 10Mbps, 20Mbps, 34Mbps, 100Mbps, 1Gbps y 10Gbps.

Los organismos de estandarización (IEEE, IETF, ITU) y los acuerdos entre fabricantes, están jugando un papel determinante en su evolución. Incluso se ha creado el MEF (Metro Ethernet Forum), organismo dedicado únicamente a definir Ethernet como servicio metropolitano.

CAPITULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL SISTEMA

3.1. Procedimiento de la Investigación

Se realizara un análisis de la topología del cliente, determinando inconvenientes en la red actual, limitaciones en cuanto a los recursos y las necesidades presentes.

3.1.1. Análisis del Problema

Teniendo en cuenta las definiciones teóricas y después de someterlas a un análisis contextualizado, considero conveniente:

La construcción de una red de área local especificada en el estándar de la IEEE número 802.3, llamada comúnmente Ethernet la misma no es una tecnología sino una familia de tecnologías LAN que se pueden entender mejor utilizando el modelo de referencia OSI. Todas las LAN deben afrontar el tema básico de cómo denominar a las estaciones individuales (nodos) y Ethernet no es la excepción. Las especificaciones de Ethernet admiten diferentes medios, anchos de banda y demás variaciones de la Capa 1 y 2. (Más precisamente la especificación 802.3u) 100Base-TX, que se refiere a una transmisión sobre UTP "Categoría 5e" a una velocidad de 100 Mhz con topología en estrella.

La ubicación en un local de ocho (08) metros de frente por doce (12) de fondo con una instalación eléctrica independiente para las computadoras con sus correspondientes descarga a tierra, considero conveniente contar con los artefactos eléctricos indispensables colocados en líneas de alimentación separadas del equipamiento en virtud de ser éstos posibles generadores de campos magnéticos que producirían un grave deterioro a la red.

La disposición de las máquinas responderá a un esquema de "puesto individual de trabajo" o cubículo destinado al efecto, ubicadas en forma longitudinal al salón una al lado de otra guardando una cierta distancia, divididas convenientemente para guardar la privacidad del usuario.

La conexión al modem (DTE) de la empresa que brindará el servicio, lo haremos a través de un cable Ethernet a un mismo ubicado en el local por el proveedor, a uno de los

puertos del switch (DCE) donde comienza nuestra conexión, esta conexión es el principal "cuello de botella" porque estará limitando físicamente el ancho de banda posible de utilizar.

La conexión de toda la red Lan se realizará mediante cableado horizontal. El tendido comienza en las cajas de servicio de cada estación y finaliza en el Switch que se encuentra dentro del rack, el cableado es sobre UTP Categoría 5e norma EIA/TIA 568B, es el que mejor se corresponde con el local y el tipo de instalación a realizar, lo que para evitar daños físicos a los conductores, se colocaran dentro de unos conductos o canaletas que serán, de material conductor debidamente aterrizado evitando así la posibilidad de interferencias electromagnéticas, este tendido va ubicado suspendidos en la parte superior del salón para estar lo más lejos posible del tendido eléctrico que se encuentra empotrado en la pared, favoreciendo el ordenamiento del local.

Las máquinas se conectarán con cualquier otra a través del Switch, las conexiones se realizarán un patch cord (cable directo) con conectores RJ 45 End-Plug (EIA/TIA especifica el uso de un conector RJ-45 para cables UTP. Las letras RJ significan "registered jack" (jack registrado), y el número 45 se refiere a una secuencia específica de cableado). Desde la tarjeta de interfaz de red (NIC)

Para instalar los cables en los conectores correspondientes debemos seguir el estándar establecido para lograr el correcto funcionamiento de nuestra red; el cable UTP Cat. 5e posee 4 pares bien trenzados entre sí:

- Blanco/Azul-------Azul Contactos 5 y 4
- Blanco/ Naranja---Naranja Contactos 3 y 6
- Blanco/ Verde-----Verde Contactos 1 y 2
- Blanco/ Marrón----Marrón Contactos 7 y 8

3.1.2. Esquema del tendido de cables y ubicación de los equipos

Para la comunicación de todas las estaciones y la conexión a Internet el protocolo TCP/IP el cual es un protocolo utilizado por todos los ordenadores conectados a Internet, hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con hardware y software incompatibles en muchos casos, además de todos los medios y formas posibles de conexión; aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativoy con cualquier tipo de hardware.

3.1.3. Determinación de los requerimientos

Para tener una base de los requerimientos del sistema, se recolectó información a través de bibliografías y trabajos anteriormente realizados e Internet, entre otros.

Básicamente la red permite el acceso de cualquier usuario al acceso a la red y la Internet, es importante señalar que se realizó un estudio de factibilidad técnica, económica y operacional en el cual se verificó la disposición y requerimientos de las herramientas a utilizar tanto de hardware como de software.

3.2. Estudio de la factibilidad

El estudio de la factibilidad, se utilizará para recopilar datos, los cuales serán analizados y permitirán tomar una decisión, sobre si deben continuar con el desarrollo del proyecto.

3.2.1. Factibilidad técnica

La presente investigación contempla la posibilidad de realizar el proyecto, para esto se realizó un análisis de la propuesta a desarrollar conociendo las características y especificaciones técnicas de la tecnología disponible para el diseño propuesto.

El Hardware requerido para desarrollar la red es el siguiente:

Tabla Nº 3.1 Lista de dispositivos necesarios en el cliente.

Nº	DESCRIPCIÓN GENERAL	CANTIDAD
1	Computador PersonalPentium 4 de 2.8 Ghz	21
2	Switch 3Com SuperStack 3 Switch 4226T de 26 puertos, proporciona 24 puertos 10/100 con auto detección y dos puertos 10/100/1000 fijos.	1
3	Rack Panel 4 puestos	1
4	Pach Panel de 48 puertos categoría 5e marca hubble	1
5	Bobina de cable utp cat 5e 305 mts	2
6	Conectores RJ-45	300
7	Jack RJ-45	30

8	Canaletas porta cables	100 Mts
9	Cajetin Externo RJ45 CAT.5e	20

3.2.2. Factibilidad Económica

Permitirá conocer la disponibilidad financiera para la elaboración de este proyecto.

3.2.3. Factibilidad Operativa

Permitirá conocer y determinar cuáles serán las aplicaciones, servicios y recursos a compartir, por parte usuarios que acensarán a la Red WAN.

3.2.4. Factibilidad Psicosocial

Permitirá conocer la receptividad (Resistencia al Cambio) del personal de la organización en relación al proyecto. Asimismo, se debe establecer posteriormente a la mplementación de la Red, un adiestramiento adecuado dirigido a todos los usuarios que utilizarán esta tecnología.

3.2.5. Factibilidad del enlace inalámbrico (Site survey)

Se realiza el análisis de la cobertura con los enlaces Wimax (acrónimo de Worldwide interoperability for Microwave Acces), para un enlace fijo-inalámbrico ya que se instalara una antena en un lugar estratégico del local del cliente por lo general con un mástil para lograr un optima señal, esta tecnología tiene como características de establecer el enlace hasta sin línea de vista o con línea de vista parcial, con lo que se puede asegurar casia al 100% todos los enlaces con óptima calidad.

3.2.6. Definir características de los equipos de red adecuados.

Definir primero los servicios que utilizara el cliente sobre la red del proveedor, el ancho de banda utilizado por cada servicio, el nivel de calidad de servicio, las aplicaciones críticas y no críticas que utilizará el enlace como aplicativos en tiempo real como los servicios de Voz, el número de usuario que utilizaran los servicios activos y pasivos, vale decir cuántos usuarios estarán usando el servicio en tiempo real (online), también se debe tener en cuenta el nivel de escalabilidad es decir prever el crecimiento de la red del cliente si afectar o ejecutar demasiados cambios, según esto se revisan las características de los equipos disponibles:

Tabla Nº 3.2 Relación de equipos cisco y capacidades.

Equipo	IOS (mínimo)	BW Soportado	Flash	DRAM
Cisco 2611	12.3.21	590 Kbps	16MB	64 MB
Cisco 2611 XM	12.3.21	1.15 Mbps	32 MB	64 MB
Cisco 3640	12.3.21	1.3 Mbps	32 MB	96 MB
Cisco 1841	12.4.8c	4.0 Mbps	32 MB	128 MB
Cisco 2801	12.4.8c	5.0 Mbps	64 MB	128 MB
Cisco 2811	12.4.8c	4.5 Mbps	64 MB	256 MB
Cisco 2821	12.4.8c	12.0 Mbps	64 MB	256 MB

3.2.7. Diseño de planta interna y externa

Planta interna,se denomina así, al conjunto de equipos e instalaciones que se ubican dentro de los edificios, el elemento característico de la planta interna es la oficina central que tiene las siguientes partes:

Sala de equipo de telecomunicaciones.- Contiene los equipos que permiten el establecimiento de comunicación entre los equipos de los usurarios, de acuerdo a su tecnología estos equipos pueden ser:

Convertidor de medios

Cableado y reflejo

Switch

Router

Sala de energía o cuadro de fuerza.- Contienen los equipos que proveen de la energía eléctrica suficiente para el funcionamiento de los equipos de telecomunicaciones, de transmisiones y alimentan toda los equipos de datos. La carga se efectúa con corriente de 220 voltios y alimentan la planta con 48 voltios de C.C.

Además de la oficina central propiamente dicha existe la Sala de MDF (main distributing frame) o Distribuidor Principal.

3.3. Definiendo Infraestructura de la Red

Infraestructura de red se refiere a la agrupación de equipos físicos y componentes lógicos que se necesitan para proporcionar una serie de características para la red, como la conectividad, las capacidades de enrutamiento y conmutación, seguridad de red, y control de acceso. La infraestructura física de la red se refiere al diseño físico de la red junto con los componentes de hardware. La infraestructura lógica de la red se compone de todos los componentes de software necesarios para permitir la conectividad entre los dispositivos, y para garantizar la seguridad de la red. La infraestructura lógica de la red se compone de productos de software y protocolos de redes y servicios.

3.3.1. Interconexión de Sistemas Autónomos

Conjunto conexiones de redes IP y encaminadores bajo el control de una o varias organizaciones y con política de encaminamiento común, un sistema autónomo es un conjunto de encaminadores administrado y gestionado por una única entidad desde el punto de vista de enrutamiento, utiliza un protocolo de pasarela interior (IGP, Internal Gateway Protocol). Generalmente OSPF o RIP, se comunica con otros AS mediante un protocolo de pasarela de frontera (BGP, Border Gateway Protocol).

3.3.2. Direccionamiento IP en el enlace local

En el cliente se configurarán Redes IP Privadas para sus conexiones entre equipos terminales de las sedes remotas y principal, se configuraran IPs con NAT estático o dinámico según sea el caso, considerando IP con NAT estático para los servidores (Correo, Web, etc.) y NAT dinámico para los usuarios regulares.

3.3.3. Consideraciones de respaldo

En caso se de una avería grave se deben mantener los servicios activos, por esto se deben considerar enlaces y acciones de contingencia tanto a nivel físico y lógico.

Para definir los enlaces de respaldo se deben tener en cuenta el tipo de tráfico para cada enlace, como calidad y/o fidelidad y ancho de banda, también una alta disponibilidad en la red del proveedor de servicios.

Siendo así se utilizara protocolos de enrutamiento dinámico en este caso BGP, BGP permite compartir rutas dinámicamente ante cualquier cambio de la Red con lo cual aseguramos la permanencia de las redes previamente establecidas, por otro lado con este protocolo de ruteo dinámico tiene la ventaja que puede aprender las redes que el cliente pueda modificar en su red LAN.

También se implementa el respaldo en todas las sedes con equipos de telecomunicaciones, es decir se implementara el respaldo o contingencia en la sede principal y las sedes remotas o sucursales, figura 3.1.

3.3.4. Consideraciones de enrutamiento

Definir o configurar los CPEs remotos con una ruta predeterminada o preferencias.

Las configuraciones de enrutamiento deben en lo posible evitar bucles terminando en destinos inalcanzables.

Evitar configurar en la medida de lo posible en los CPEs rutas estáticas, esto para asegurar un gran grado de escalamiento de la Red.

Garantizar la calidad del servicio permitiendo diferenciar y priorizar el tráfico que se genere, para que las distintas aplicaciones (voz, datos y video) no se afecten entre sí.

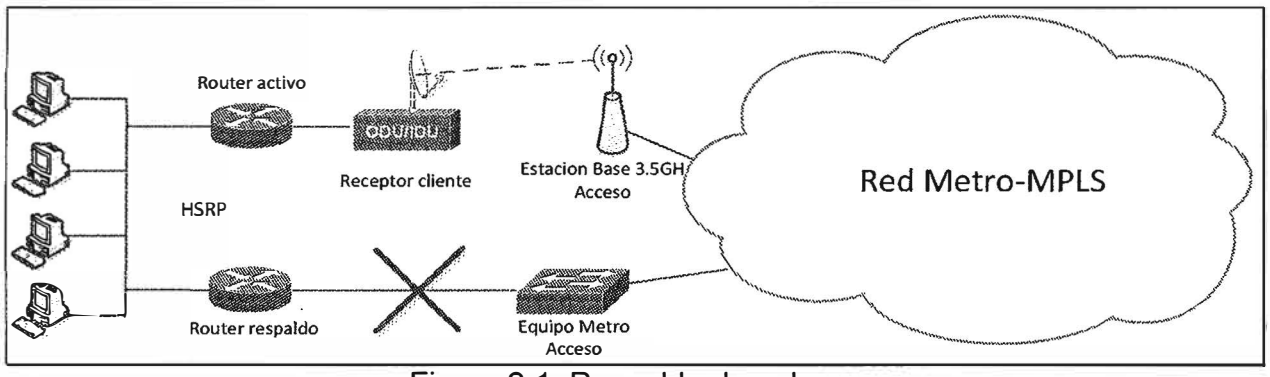

Figura 3.1. Respaldo de enlace.

3.3.5. Infraestructura compartida

Como se explicó anteriormente, la red del cliente esta soportada sobre la red de un proveedor de servicios, el cual presenta funcionalidad de red y de seguridad equivalentes a las que se obtienen con una red privada, el objetivo de esto es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet.

3.3.6. Seguridad sobre la Red MPLS-VPN

Aunque el cliente seguramente ya cuenta con algunas soluciones de seguridad, la estructura completa tiene que formar parte de un proceso continuo que requiere que toda la tecnología esté perfectamente integrada.

Para las empresas que operan en el ámbito internacional, la seguridad no puede abordarse únicamente cuando ocurre un incidente o como una cuestión de responsabilidad, sino que tiene que ser parte integral de todas las decisiones que toma la empresa.

Tradicionalmente, la información electrónica se protegía con tecnologías de seguridad de TI diseñadas para combatir amenazas concretas. El cometido principal de una estrategia de seguridad solía ser evitar intrusiones en las instalaciones corporativas y

en su perímetro operativo. Pero hoy en día, los orígenes de los ataques electrónicos, o vectores de amenazas, son mucho más variados y sutiles. Por este motivo, las organizaciones también tienen que plantearse la seguridad de una forma más sutil y variada para proteger los recursos críticos.

No debe asumirse que el acceso sin autorización solamente se produce desde fuera de la empresa, ya que muchas veces el origen está en recursos internos, como pueden ser los socios y la cadena de suministro. El Informe sobre investigaciones de brechas en la seguridad de los datos de 2009hace hincapié en los cambios en el panorama de la seguridad de TI y en los nuevos vectores en juego como se muestra a continuación:

¿Quiénes son los responsables de las brechas en la seguridad de los datos?

- Fuentes externas: 74% (+1% en comparación con 2008)
- Grupos diversos: 39% (+9%)
- Socios: 32% (-7%)
- Empleados: 20% (+2%)

El informe, basado en 90 brechas confirmadas que los forenses de Verizon Business investigaron en el año 2008, destaca la importancia de examinar todos los aspectos del negocio, tanto internos como externos y demuestra que aunque casi tres cuartos de las brechas procedían del exterior, un quinto de ellas las causaron personas dentro de la empresa, mientras que los socios fueron responsables de casi un tercio. Estos resultados no sólo ilustran la diversidad de las amenazas contra la seguridad, sino que además sugieren la gran complejidad a la que se enfrenta una empresa a la hora de protegerse contra ataques multifacéticos de diversos orígenes.

Debido a su posición como centro de las redes empresariales y los cambios frecuentes en sus relaciones con el mundo exterior, existen varios puntos débiles inherentes a la empresa extendida en lo que a la seguridad se refiere.

Ahora más que nunca, los intrusos atacan los puntos en los que se concentran o agregan datos para obtener la mayor cantidad posible de información de los clientes. Estas personas saben que las empresas se enfrentan con un dilema: por una parte necesitan extender sus límites y poner la información al alcance de quienes la necesitan, mientras que por otra tienen que tener siempre presente la posibilidad de que con ello creen nuevas vulnerabilidades.

Al nivel más básico, la gestión de la seguridad de la información consiste en encontrar un equilibrio entre los costes que puede suponer una brecha en la infraestructura de TI —tanto directos como indirectos— y los esfuerzos necesarios para proteger debidamente dicha infraestructura.

En este sentido es esencial que los recursos más importantes, es decir la información crítica para el negocio, estén protegidos contra amenazas internas y externas. Al proteger la transmisión libre de la propiedad intelectual, es posible ampliar el alcance de la empresa y limitar las interrupciones de las operaciones que puedan obstruir las fuentes de ingresos. Además de esto, los mecanismos de seguridad deben contribuir al cumplimiento de los requisitos externos de conformidad que atañen a la seguridad. Este aspecto ha cobrado una especial importancia en la gestión de riesgos, particularmente en los sectores que exigen el cumplimiento de códigos estrictos de conformidad y gobierno, en los que las ramificaciones de una brecha en la seguridad pueden poner en peligro a la organización entera.

La gestión de la seguridad no implica únicamente la implementación de tecnología, sino que exige la implantación de prácticas que protejan el nombre de la empresa, su reputación y la confianza de los clientes. Estos son los componentes clave de una proposición de valor. La frecuencia de los cambios que se producen en las relaciones o los socios provoca la reevaluación constante de la demarcación entre los recursos privados, los públicos y los compartidos dentro del ámbito de la empresa extendida.

Para proteger debidamente a la empresa extendida hace falta considerarla de manera global y tener en cuenta tanto los recursos internos como las relaciones con el mundo exterior. Es importante concentrarse en los siguientes aspectos:

- Proteger la información.
- Proteger la infraestructura.
- Cumplir con los requisitos de gobierno, riesgo y conformidad, en especial en lo que a normativa se refiere.

Esto también significa abordar la seguridad, no sólo desde el punto de vista empresarial, sino en relación con proveedores, socios y distribuidores.

Es importante adoptar una estrategia que responda a las necesidades de cada empresa y se centre en los procesos. Para ello, es necesario evaluar y priorizar las amenazas contra la información crítica y encontrar un equilibrio entre los riesgos contra la

seguridad de la TI y las prioridades operativas, al tiempo que se controlan los costes y se implementan controles de seguridad adecuados para las necesidades específicas de la empresa.

Lo que se necesita es un marco de trabajo flexible que responda al perfil de riesgo y de conformidad de cada empresa en concreto y que simplifique la seguridad de la información en toda la organización, con un análisis independiente y continuo de los controles implementados.

El principio fundamental es que, en el caso de la seguridad, no existe una única solución para todas las situaciones, sino que los proveedores de tecnología y servicios tienen que ofrecer soluciones diseñadas específicamente para el cliente y suministrarlas de la forma más conveniente para cada empresa, ya sea de forma externalizada, parcialmente externalizada o sin ningún tipo de externalización. La solución tiene que responder a los requisitos y prácticas de la empresa, además de servir de complemento a la red.

3.4. Diez razones para migrar a MPLS VPN

En los últimos tiempos, no sólo se viene hablando de la famosa convergencia de Voz, Video y Datos sobre una misma plataforma, sino también de la necesidad de la migraciónde servicios "Legacy" (heredados) como ATM o Frame Relay a una nueva generación de "IPbased VPNs" (Redes Privadas Virtuales basadas en protocolo IP) como los son las "MPLS VPNs" (Redes Privadas Virtuales basadas en Multiprotocol Label Switching).

Sin embargo, resistencia sigue siendo la primera palabra que se asocia cuando se habla de "cambios", mucho más aún, cuando se trata de migraciones de servicios de comunicaciones, críticos para una empresa.A continuación, encontraremos 10 razones claves para hacer frente a la mencionada "resistencia" a los cambios cuando una empresa, corporación u organismo este pensando en migrar su infraestructura Legacy actual a una IP-Based MPLS VPN

a. Flexibilidad.

Cada empresa, corporación u organismo tiene desarrollada su propia estructura interna, tanto en infraestructura como en recursos humanos, generadas en base a sus necesidades y recursos disponibles. En base a ésta estructura, muchas veces única, se montan los servicios de comunicaciones para acomodar de la mejor manera posible y al

menor costo, el transporte de la información interna, así como también externa, con sus clientes y proveedores.

La topología de una MPLS VPN puede acomodarse acorde a cada necesidad, dada su naturaleza que brinda conexiones "Any-to-Any" (cualquiera con cualquiera) entre los distintos puntos que comprenden la VPN, contando así con el mejor camino o ruta entre cada punto. A su vez se puede obtener mayor flexibilidad realizando configuraciones híbridas con Hub-and-Spoke (estrella), por ejemplo en las conexiones con clientes.

b. Escalabilidad.

Con un nuevo conceptode aprovisionamiento, llamado "Point-to-Cloud" (punto a la nube), se implementan los nuevos puntos de la VPN. Este concepto proviene del hecho de que cada vez que sea necesario "subir" un nuevo punto a la VPN, sólo habrá que configurar el equipamiento del Service Provider que conecte este nuevo punto. De esta forma, evitamos tareas complejas y riesgosas, como las que se producen cuando se activa un nuevo punto en una red basada en circuitos virtuales de Frame Relay o ATM, en donde es necesario re-configurar TODOS los puntos involucrados.

c. Accesibilidad.

La arquitectura de MPLS VPN permite utilizar prácticamente todos las tecnologías de acceso para interconectar las oficinas del cliente con su "Service Provider" (Proveedor de Servicios).Por dicho motivo, la versatilidad que nos permite utilizar xDSL o un enlace Wireless Etherneten las oficinas más pequeñas y hasta incluso en usuarios móviles, mientras que en el headquarter utilizamos leased lines (TDM) en altas capacidades como E3/T3, nos permite dimensionar cada punto de la VPN acorde a sus necesidades sin limitar o restringir la de otros puntos.

d. Eficiencia.

En una infraestructura 100% IP, es decir, aquellas empresasen donde todo el equipamiento involucrado y las aplicaciones utilizadas son IP-based, el uso de servicios de transporte ATM o Frame Relay someten al cliente a incurrir en un costo adicional por el overhead que los protocolos de transporte introducen. Mediante IFX MPLS VPN - un servicio IP-Based VPN - este costo extra desaparece.

e. Calidad de servicio (QoS) y Clases de servicio (CoS).

Las necesidades de comunicación entre dos lugares remotos, hoy en día van mucho más allá de la simple transferencia de datos vía email, web u otras aplicaciones. Siendo

incluso insuficiente muchas veces, la interesante combinación de voz y datos bajo una misma plataforma. Es por ésto, que la ya mencionada Convergencia de datos con aplicaciones real-time y/o interactivas, voz y tambien video de alta calidad, necesitan de una eficiente plataforma de transporte.

Mediante la utilizacion de técnicas y herramientas de Calidad de Servicio (QoS), se ofrecen distintas Clases de Servicio (CoS) dentro de una MPLS VPN para cumplimentar los requerimientos de cada servicio o aplicación.

f. Administración.

Las MPLS VPN son denominadas Network-Based, ésta característica proviene del hecho en que el servicio es implementado sobre la infraestructura del Service Provider; implicando, entre otras cosas, que la administración de enrutamiento es llevada a cabo por el Service Provider; quien por su naturaleza, es especialista en dicha tarea desligando así al cliente de llevarla a cabo.

g. Monitoreo y SLAs.

Las MPLS VPN son monitoreadas, controladas y con un constante seguimiento en forma permanente, las 24 horas los 7 días de la semana, por parte del Service Provider. Además, se extienden "Service Level Agreements" (acuerdos de nivel de servicio) para garantizar y asegurar la estabilidad y performance que el cliente necesite.

h. Fácil Migración.

La simplicidad de la tecnología determina que las tareas de aprovisionamiento, administración y mantenimiento sean actividades sencillas para el Service Provider; lo cual se traslada directamente al cliente, obteniendo una migración del servicio actual sin complicaciones.

i. Seguridad.

Análisis y estudios realizados por los distintos fabricantes y entidades especializadas en el área, determinaron que los niveles deseguridad entregados por una MPLS VPN son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM.

Sin embargo, en escenarios donde estos niveles no son suficientes, como por ejemplo en las necesidades de entidades financieras, una MPLS VPN puede también ser combinada con la encriptación y autenticación que IPSec brinda, elevando aún más la seguridad de la VPN.

j. Bajo Costo.

Son varios los motivos que permiten afirmar que un servicio MPLS VPN ofrece "más por menos", entre ellos podemos destacar:

Independencia de equipos de cliente (CPE): al ser un servicio Network-based, la implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente.

Convergencia: por ser una VPN CoS-Aware (Soporte de Clases de Servicio) se puede integrar distintos servicios y aplicaciones sobre una misma plataforma. De este modo, empresas que al día de hoy mantienen distintos y costosos servicios para soportar sus necesidades de voz, datos y video; pueden unificar estos requerimientos concluyendo en un ahorro significativo y manteniendo relación con un único proveedor de servicios.

3.5. Configuración, habilitación de servicios y puesta en operación

3.5.1. Diseño y asignación de IPs WAN y LAN.

Consideraciones, para toda la red se especifica:

a. La ubicación de cada aplicación o servicio
b. El área de uso de dicha aplicación o servicio
c. Normalmente se detalla a nivel de campus, no a nivel de computadoras
d. Dentro de un campus, puede detallarse a nivel de LANs
e. La idea es construir, de abajo hacia arriba, las especificaciones de desempeño de la red.

Un flujo simple tiene las siguientes especificaciones:

a. Origen y destino
b. Capacidad (bits/seg)
c. Retardo (seg)
d. Confiabilidad (ej. % pérdida)
e. Un flujo puede ser unitario, de dos partes
f. (ejm. "best-effort" + "reservado") o multipartes

Diseño:

a. Elegir parámetros de desempeño con base en las aplicaciones (ancho de banda, porcentaje de pérdida de paquetes, latencia, disponibilidad).

b. Identificar restricciones de diseño (presupuesto, tiempo de implantación, restricciones físicas, restricciones de seguridad).

c. Establecer objetivos viables para los parámetros de desempeño, combinando 1 y 2

d. Elaborar el diseño de alto nivel (niveles jerárquicos, elección de conectividad WAN, routing vs switching, etc.)

e. Estructura jerárquica de la red WAN

f. Estructura de cada una de las redes LAN

g. Grafico enfatizando los servicios

h. Grafico enfatizando los routers, switches, etc.

i. Descripción de asignaciones de números IP

j. Descripción de los mecanismos de enrutamiento

k. Tablas estáticas en cada router (si existen)

3.5.2. Plan de numeración para las redes LAN-WAN:

Tabla Nº 3.3 Distribución de direcciones IPs.

Sedes	Redes LAN (192.168.0.0/20)		Redes WAN (10.10.10.0/26)	
Sede Principal	Datos críticos:	192.168.0.0/24	Datos activa:	10.10.10.0/30
LAN: 192.168.0.0/22	Datos no críticos:		Datos respaldo:	10.10.10.4/30
WAN: 10.10.10.0/29		192.168.1.0/24	Voz activa:	10.10.10.8/30
INTERNET	Voz:	192.167.2.0/24	Voz respaldo:	10.10.10.12/30
WAN:190.81.41.0/27	Internet:		Internet activo:	190.81.41.2/28
LAN:190.223.37.0/26		190.223.37.0/26	Internet respaldo:	190.223.37.50/28
Sede Sucursal 1	Datos críticos:	192.168.4.0/24	Datos activa:	10.10.10.16/30
LAN: 192.168.4.0/22	Datos no críticos:		Datos respaldo:	10.10.10.20/30
WAN: 10.10.10.8/29		192.168.5.0/24	Voz activa:	10.10.10.24/30
	Voz:	192.167.6.0/24	Voz respaldo:	10.10.10.28/30
Sede Sucursal 2	Datos críticos:	192.168.8.0/24	Datos activa:	10.10.10.32/30
LAN:192.168.12.0/22	Datos no críticos:		Datos respaldo:	10.10.10.36/30
WAN:10.10.10.12/29		192.168.9.0/24	Voz activa:	10.10.10.40/30
	Voz:	192.167.10.0/24	Voz respaldo:	10.10.10.44/30

Se realiza una distribución de las IPs para todos los servicios de la siguiente forma: IPs Red LAN Sede principal: 192.168.0.0, con mascara de red: 255.255.252.0

IPs Red LAN Sucursal Sede 1: 192.168.4.0, con mascara de red: 255.255.252.0
IPs Red LAN Sucursal Sede 1: 192.168.8.0, con mascara de red: 255.255.252.0

Plan e numeración para las redes WAN:
IP Red WAN Sede Principal: 10.10.10.0, con mascara de red: 255.255.255.252
IP Red WAN Sede Principal Contingencia: 10.10.10.4, con mascara de red: 255.255.255.252
IP Red WAN Sucursal Sede 1: 10.10.10.8, con mascara de red: 255.255.255.252
IP Red WAN Sucursal Sede 1 Contingencia: 10.10.10.8, con mascara de red: 255.255.255.252
IP Red WAN Sucursal Sede 2: 10.10.10.12, con mascara de red: 255.255.255.252
IP Red WAN Sucursal Sede 2 Contingencia: 10.10.10.16, con mascara de red: 255.255.255.252

Como se mencionó anteriormente se tendrán 2 encaminadores en cada sede (Sede principal y Sedes sucrusales).

Sede principal:
Router Primario: rPrincipal
Router Contingencia: rPrincipalBk
Sede Sucursal 1:
Router Sucursal 1: rSucursal1
Router Sucursal 1 Contingencia: rSucursal1Bk
Sede Sucursal 2:
Router Sucursal 2: rSucursal2
Router Sucursal 2 Contingencia: rSucursal2Bk

3.5.3. Configuraciones:

Para el diseño de esta red se configurar sobre equipos Router Cisco 2821 con interfaces GigaEthernet y FastEthernet a través de una red METRO e Inalámbrico, el acceso hacia el equipo METRO será para el encaminador de la sede Principal activa o la que en estado normal presenta todo el tráfico de datos y los enlaces hacia las otras sedes remotas será a través de la red METRO del proveedor de servicios y el acceso por enlace Inalámbrico será para el encaminador de la sede principal de contingencia y la que en estado normal no presenta tráfico alguno solo caso de avería presentara tráfico de datos.

Tabla 3.4 NºConfiguración de la clasificación de tráfico – LAN

class-map match-any P5	Crea la clase para un tráfico específico
match ip dscp cs5	Clasifica el tráfico definido como CS5 (DSCP 40) dentro de la LAN del Cliente (solo es necesario si el cliente realiza la marcación de su tráfico de voz o video dentro de red LAN con IP DSCP 40 ó IP precedence 5)
match access-group name qos5	Clasifica el tráfico definido dentro de la ACL de Voz-Video
class-map match-any P2	Crea la clase para un tráfico específico
match ip dscp cs2	Clasifica el tráfico definido como CS2 (DSCP 16) dentro de la LAN del cliente (solo es necesario si el cliente realiza la marcación de trafico de sus datos críticos dentro de red LAN con DSCP 16 ó precedence 2)
match access-group name qos2	Clasifica el tráfico definido dentro de la ACL de Datos-Críticos

Tabla Nº 3.5 Configuración de políticas de tráfico LAN

policy-map SetDscpLan	Priorización del tráfico de acuerdo a la clase
class P5	Clase de servicio LAN-P5
set ip dscp cs5	Se marca todos los paquetes con DSCP CS5
class P2	Clase de servicio LAN-P2
set ip dscp cs2	Se marca todos los paquetes con DSCP CS2
class class-default	Clase de servicio LAN-P1
set ip dscp cs1	Se marcan todos los paquetes que no han caído en otro clase con DSCP CS1

Tabla Nº 3.6 Configuración de Clases de Servicio para la administración de congestión –WAN

class-map match-any qos5	Crea la clase para un tráfico específico
match ip dscp cs5	Clasifica el tráfico definido como CS5
match ip dscp cs6	Clasifica el tráfico definido como CS6
class-map match-any qos2	Crea la clase para un tráfico datos específico
match ip dscp cs2	Clasifica el tráfico definido como CS2
class-map match-any qos1	Crea la clase para un tráfico datos específico
match ip dscp cs1	Clasifica el tráfico definido como CS1
El tráfico que no se encuentre dentro de alguna clase definida, serán considerados dentro de	

la clase default

Tabla Nº 3.7 Configuración de Políticas de tráfico para cada sede – WAN

policy-map [DATOS/VOZ]	Priorización del tráfico de acuerdo a la clase
class qos5	Tráfico de CoS 3 que fue definido por el ACL
priority 512	Asigna prioridad de acuerdo al parámetros de ancho de ancho de banda por canal de tráfico del tipo VoIP, ToIP, Videoconferencia o cualquier otro tipo de tráfico sensible al retardo.
police 512000 conform-action transmit exceed-action drop	
Limita el ancho de banda asignado como tráfico con prioridad cs5 al valor de bw3, descartando el exceso.	
class qos2	Referencia al tráfico de tipo P2, y le asigna un ancho de banda
bandwidth 1536	Asigna el ancho de banda para el tráfico con prioridad 2
police 1536000 288000 576000 conform-action transmit exceed-action set-dscp-transmit cs1	
Limita el ancho de banda asignado como tráfico con prioridad 2 (cs2), el exceso de tráfico será remarcado como prioridad 1 (cs1).	
class qos1	Referencia al tráfico de tipo P1, y le asigna un ancho de banda.
bandwidth 2048	Asigna el ancho de banda para el tráfico con prioridad 1
class class-default	Asigna el ancho de banda para el trafico por defecto
fair-queue	Cola con pesos equitativos

Tabla Nº 3.8 Configuración de perfil para limitación del BW de salida en cada sede.

policy-map Shape_[DATOS/VOZ]	
Define el límite del ancho de banda cuando la interface de acceso es ethernet	
class class-default	Define todo el tráfico de salida por la interface WAN como una sola clase
shape average [4096000/512000]	
Promedia el uso de ancho de banda como máximo la suma de los diversos tipos de tráfico.	
service-policy [DATOS/VOZ]	Llama la política definida de acuerdo al servicio.

La configuración en la interface WAN se aplicará en modo troncal para pasar diferentes VLANs para poder habilitar los diferentes servicios (Voz, datos e Internet).

Configuración del encaminador de la sede principal equipo activo:

```
interface GigabitEthernet0/0
 description Interface WAN Sede Principal activa Troncal
no ip redirects
 speed 100
 full-duplex

interface GigabitEthernet0/0.400
 description Interface WAN Sede Principal activa – VOZ
 encapsulation dot1q 400
 ip vrf forwarding 200
 ip address 10.10.10.9 255.255.255.252
 no ip redirects
service-police output Shape_VOZ

interface GigabitEthernet0/0.500
 description Interface WAN Sede Principal activa – INTERNET
encapsulation dot1q 500
 ip address 190.81.41.2 255.255.255.240
 no ip redirects

interface GigabitEthernet0/0.1200
description Interface WAN Sede Principal activa – DATOS
encapsulation dot1q 1200
 ip vrf forwarding 100
 ip address 10.10.10.1 255.255.255.252
 no ip redirects
 service-police output Shape_DATOS
```

La configuración en la interface LAN se aplicará en modo acceso con un puerto para cada servicio conectado a los Host o Gateway de los diferentes servicios (Voz, datos e Internet).

```
interface GigabitEthernet0/1
 description Interface LAN DATOS
 ip vrf forwarding 100
```

```
 ip address 192.168.0.2 255.255.254.0
 standby 10 ip 192.168.0.1
 standby 10 timers 10 31
 standby 10 priority 200
 standby 10 preempt
 standby 10 track GigabitEthernet0/0 100
 service-policy input SetDscpLan

interface FastEthernet0/0/0
 description Interface LAN VOZ
 ip vrf forwarding 101
 ip address 192.168.2.2 255.255.255.0
 standby 20 ip 192.168.2.1
 standby 20 timers 10 31
 standby 20 priority 200
 standby 20 preempt
 standby 20 track GigabitEthernet0/0 100
 service-policy input SetDscpLan

interface FastEthernet0/0/1
 description Interface LAN INTERNET
 ip address 190.223.37.2 255.255.255.0
 standby 50 ip 190.223.37.1
 standby 50 timers 10 31
 standby 50 priority 200
 standby 50 preempt
 standby 50 track GigabitEthernet0/0 100
service-policy input SetDscpLan
```

3.5.4. Protocolos de encaminamiento en CPE

Configuraremos BGP hacia los equipo de acceso:

```
router bgp 64516
bgp log-neighbor-changes
timers bgp 10 30
neighbor WAN_INTERNET peer-group
neighbor WAN_INTERNET remote-as 12252
neighbor WAN_INTERNET password e#&235ty
```

neighbor WAN_INTERNET timers 10 30
neighbor WAN_INTERNET send-community both
neighbor WAN_INTERNET soft-reconfiguration inbound
neighbor WAN_INTERNET prefix-list Permitir_Default in
neighbor WAN_INTERNET route-map TELMEX out
neighbor LAN_INTERNET peer-group
neighbor LAN_INTERNET remote-as 64517
neighbor LAN_INTERNET password e#&235ty
neighbor LAN_INTERNET timers 10 30
neighbor LAN_INTERNET send-community both
neighbor LAN_INTERNET next-hop-self
neighbor LAN_INTERNET soft-reconfiguration inbound
neighbor 190.81.41.1 peer-group WAN_INTERNET
neighbor 190.81.41.1 description Enlace Principal – Internet
neighbor 190.81.41.1 activate
neighbor 190.223.37.3 peer-group LAN_INTERNET
neighbor 190.223.37.3 description Enlace con CPE Backup – Internet
neighbor 190.223.37.3 activate
network 190.223.37.0 mask 255.255.255.128

address-family ipv4 vrf 100
 neighbor WAN_DATOS peer-group
 neighbor WAN_DATOS remote-as 12252
 neighbor WAN_DATOS password e#&235ty
 neighbor WAN_DATOS timers 10 30
 neighbor LAN_DATOS peer-group
 neighbor LAN_DATOS remote-as 64516
neighbor LAN_DATOS password e#&235ty
 neighbor LAN_DATOS timers 10 30
 neighbor WAN_DATOS send-community both
 neighbor WAN_DATOS soft-reconfiguration inbound
 neighbor WAN_DATOS route-map TELMEX_DATOS in
 neighbor WAN_DATOS route-map COMU_DATOS out
 neighbor LAN_DATOS send-community both
 neighbor LAN_DATOS next-hop-self
 neighbor LAN_DATOS soft-reconfiguration inbound
 neighbor 10.10.10.10 peer-group WAN_DATOS

```
 neighbor 10.10.10.10 description Enlace WAN DATOS
 neighbor 192.168.0.3 peer-group LAN_DATOS
 neighbor 192.168.0.3 description Enlace LAN DATOS Respaldo
 neighbor 10.10.10.10 activate
 neighbor 192.168.0.3 activate
 network 192.168.0.0 mask 255.255.254.0

address-family ipv4 vrf 200
 neighbor WAN_VOZ peer-group
 neighbor WAN_VOZ remote-as 12252
 neighbor WAN_VOZ password e#&235ty
 neighbor WAN_VOZ timers 10 30
 neighbor LAN_VOZ peer-group
 neighbor LAN_VOZ remote-as 64516
 neighbor LAN_VOZ password e#&235ty
 neighbor LAN_VOZ timers 10 30
 neighbor WAN_VOZ send-community both
 neighbor WAN_VOZ soft-reconfiguration inbound
 neighbor WAN_VOZ route-map TELMEX_VOZ in
 neighbor WAN_VOZ route-map COMU_VOZ out
 neighbor LAN_VOZ send-community both
 neighbor LAN_VOZ next-hop-self
 neighbor LAN_VOZ soft-reconfiguration inbound
 neighbor 10.10.10.10 peer-group WAN_VOZ
 neighbor 10.10.10.10 description Enlace WAN VOZ
 neighbor 192.168.2.3 peer-group LAN_VOZ
 neighbor 192.168.2.3 description Enlace LAN VOZ Respaldo
 neighbor 10.10.10.10 activate
 neighbor 192.168.2.3 activate
 network 192.168.2.0 mask 255.255.255.0

ip bgp-community new-format

ip access-list extended qos5
 permit ip 192.168.0.0 0.0.0.255 any
 permit ip 192.168.2.0 0.0.0.255 any
```

```
ip access-list extended qos2
 permit ip 192.168.1.0 0.0.0.255 any

ip prefix-list RED_ALL seq 5 permit 0.0.0.0/0 le 32
ip prefix-list RED_LAN seq 5 permit 192.168.0.0/22

route-map COMU_LAN permit 10
 description Setea Comunidad 200
 match ip address prefix-list RED_LAN
 set community 12252:200

route-map DE_TELMEX deny 10
description denegacion de Redes Lans y Redes Lan internas por la WAN
match ip address prefix-list RED_LAN

route-map DE_TELMEX permit 20
 description Permitir las demas Redes de Sedes Remotas
match ip address prefix-list RED_All
```

Configuración del encaminador de la sede principal equipo de respaldo:

```
interface GigabitEthernet0/0
 description Interface WAN Sede Principal respaldo Troncal
no ip redirects
 speed 100
 full-duplex

interface GigabitEthernet0/0.440
 description Interface WAN Sede Principal respaldo – VOZ
encapsulation dot1q 440
 ip vrf forwarding 200
 ip address 10.10.10.13 255.255.255.252
 no ip redirects
service-police output Shape_VOZ

interface GigabitEthernet0/0.550
 description Interface WAN Sede Principal respaldo – INTERNET
encapsulation dot1q 550
```

```
 ip address 190.223.37.50 255.255.255.240
 no ip redirects

interface GigabitEthernet0/0.1220
description Interface WAN Sede Principal respaldo – DATOS
encapsulation dot1q 1220
 ip vrf forwarding 100
 ip address 10.10.10.5 255.255.255.252
 no ip redirects
 service-police output Shape_DATOS

interface GigabitEthernet0/1
 description Interface LAN DATOS
 ip vrf forwarding 100
 ip address 192.168.0.3 255.255.255.0
 standby 10 ip 192.168.0.1
 standby 10 timers 10 31
 standby 10 priority 150
 standby 10 preempt
 standby 10 track GigabitEthernet0/0 100
 service-policy input SetDscpLan

interface FastEthernet0/0/0
 description Interface LAN VOZ
 ip vrf forwarding 101
 ip address 192.168.2.3 255.255.255.0
 standby 20 ip 192.168.2.1
 standby 20 timers 10 31
 standby 20 priority 150
 standby 20 preempt
 standby 20 track GigabitEthernet0/0 100
 service-policy input SetDscpLan

interface FastEthernet0/0/1
 description Interface LAN INTERNET
 ip address 190.223.37.3 255.255.255.0
 standby 50 ip 190.223.37.1
```

```
 standby 50 timers 10 31
 standby 50 priority 150
 standby 50 preempt
 standby 50 track GigabitEthernet0/0 100
service-policy input SetDscpLan
```

Configuraremos BGP hacia los equipo de acceso:

```
router bgp 64516
bgp log-neighbor-changes
timers bgp 10 30
neighbor WAN_INTERNET peer-group
neighbor WAN_INTERNET remote-as 12252
neighbor WAN_INTERNET password e#&235ty
neighbor WAN_INTERNET timers 10 30
neighbor WAN_INTERNET send-community both
neighbor WAN_INTERNET soft-reconfiguration inbound
neighbor WAN_INTERNET prefix-list Permitir_Default in
neighbor WAN_INTERNET route-map TELMEX out
neighbor LAN_INTERNET peer-group
neighbor LAN_INTERNET remote-as 64517
neighbor LAN_INTERNET password e#&235ty
neighbor LAN_INTERNET timers 10 30
neighbor LAN_INTERNET send-community both
neighbor LAN_INTERNET next-hop-self
neighbor LAN_INTERNET soft-reconfiguration inbound
neighbor 190.81.41.17 peer-group WAN_INTERNET
neighbor 190.81.41.17 description Enlace WAN Principal respaldo – Internet
neighbor 190.81.41.17 activate
neighbor 190.223.37.2 peer-group LAN_INTERNET
neighbor 190.223.37.2 description Enlace con RouterPrincipal – Internet
neighbor 190.223.37.2 activate
network 190.223.37.0 mask 255.255.255.128

address-family ipv4 vrf 100
 neighbor WAN_DATOS peer-group
 neighbor WAN_DATOS remote-as 12252
 neighbor WAN_DATOS password e#&235ty
```

```
 neighbor WAN_DATOS timers 10 30
 neighbor LAN_DATOS peer-group
 neighbor LAN_DATOS remote-as 64516
 neighbor LAN_DATOS password e#&235ty
 neighbor LAN_DATOS timers 10 30
 neighbor WAN_DATOS send-community both
 neighbor WAN_DATOS soft-reconfiguration inbound
 neighbor WAN_DATOS route-map TELMEX_DATOS in
 neighbor WAN_DATOS route-map COMU_DATOS out
 neighbor LAN_DATOS send-community both
 neighbor LAN_DATOS next-hop-self
 neighbor LAN_DATOS soft-reconfiguration inbound
 neighbor 10.10.10.6 peer-group WAN_DATOS
 neighbor 10.10.10.6description Enlace WAN DATOS respaldo
 neighbor 192.168.0.2 peer-group LAN_DATOS
neighbor 192.168.0.2 description Enlace LAN DATOS Respaldo
 neighbor 10.10.10.6 activate
 neighbor 192.168.0.2 activate
network 192.168.0.0 mask 255.255.254.0

address-family ipv4 vrf 200
 neighbor WAN_VOZ peer-group
 neighbor WAN_VOZ remote-as 12252
 neighbor WAN_VOZ password e#&235ty
 neighbor WAN_VOZ timers 10 30
 neighbor LAN_VOZ peer-group
 neighbor LAN_VOZ remote-as 64516
 neighbor LAN_VOZ password e#&235ty
 neighbor LAN_VOZ timers 10 30
 neighbor WAN_VOZ send-community both
 neighbor WAN_VOZ soft-reconfiguration inbound
 neighbor WAN_VOZ route-map TELMEX_VOZ in
 neighbor WAN_VOZ route-map COMU_VOZ out
 neighbor LAN_VOZ send-community both
 neighbor LAN_VOZ next-hop-self
 neighbor LAN_VOZ soft-reconfiguration inbound
 neighbor 10.10.10.14 peer-group WAN_VOZ
```

```
 neighbor 10.10.10.14 description Enlace WAN VOZ
 neighbor 192.168.2.2 peer-group LAN_VOZ
neighbor 192.168.2.2 description Enlace LAN VOZ Respaldo
 neighbor 10.10.10.14 activate
 neighbor 192.168.0.2 activate
network 192.168.2.0 mask 255.255.255.0

ip bgp-community new-format

ip access-list extended qos5
 permit ip 192.168.0.0 0.0.0.255 any
 permit ip 192.168.2.0 0.0.0.255 any

ip access-list extended qos2
 permit ip 192.168.1.0 0.0.0.255 any

ip prefix-list RED_ALL seq 5 permit 0.0.0.0/0 le 32
ip prefix-list RED_LAN seq 5 permit 192.168.0.0/22

route-map COMU_LAN permit 10
 description Setea Comunidad 201
 match ip address prefix-list RED_LAN
 set community 12252:201

route-map DE_TELMEX deny 10
description denegacion de Redes Lans y Redes Lan internas por la WAN
match ip address prefix-list RED_LAN

route-map DE_TELMEX permit 20
 description Permitir las demas Redes de Sedes Remotas
match ip address prefix-list RED_All
```

Configuración de Telefonía IP:

Configuración sobre Dispositivo de Acceso Integrado (Integrated Access Devices, IAD), en este caso se utiliza un equipo o dispositivo que proporciona conversión y transporte entre la red IP y la red PSTN en este caso Media Gateway o Pasarela de medios.

La configuración en los equipos Gaoke requiere de másparámetros dado los servicios (routing, POS, etc.) que se van a habilitar. Muchos de ellos estánpuestos a valores por defecto (en la flash del equipo) sin embargo de todos modos amerita surepaso de unprocedimiento para descartar algún problema o entendimiento de operación del equipo. Los parámetros quenecesita configurar se resumen son los siguientes:

Configuración General:

a) Carga del perfil definido de acuerdo a las necesidades

b) Carga de la configuración de fábrica (configuración default)

Carga del Perfil (Comando:**target**)

Ingresar al modo avanzado, ingresando desde el inicio con el password radon, deberá aparecer elprompt con el símbolo $

IAD(2)$WDUJHW

The target client which config the default value

0-------China

1-------Telmex

2-------Entel

3-------Zhongxinghulian

4-------tuoxun

Please choose the target client which configure the default value[1]: 1<Enter>

Carga de la configuración de fábrica (Comando:**load default**)

Enseguida sobre el modo AVANZADO ejecutar los siguientes comandos:

IAD(2)$load default

Are you sure load default configuration? ’yes’ or ’no’[no]: y

Operate Successfully!

Salvar la configuración y hacer reset de la caja

IAD(8)$save

Are you sure save current configuration? 'yes' or 'no'[no]: y

erased 11 kbytes ... 100% complete.

Operate Successfully!

Datos:

Activación del modo NAT en el IAD-Router (preconfigurado en la flash)

Configuracion de las IPs

Configuracion de rutas estáticas

Configuracion de DHCP y DNS (preconfigurado en la flash)

Configuracion de WiFi (preconfigurado en la flash)

Permite habilitar la lógica independiente para los servicios de telefonía y datos.

IAD(8)# VHW— ———— ———ىDW <enter> (Ejecutar el comando SET NAT)

Interface type of NAT server:

0-------Disable

1-------DATA net port

2-------Public LAN net port

->Choose the interface type of NAT server(0-2)[]:

->Both DATA and Voice use the same net port? 'yes' or 'no'[QR]:

Nota: Si se obvia éste paso no aparecerá el campo para habilitar la VLAN para los datos

Configuración de los IPs (Comando: **set ip**)

IAD(2)#set ip (Ejecutar el commando SET IP)

WAN

->**Data port IP Address[138.0.60.1]: 190.81.73.90 (este es un ejemplo, al ingresar el IP WAN INTERNET)

->**Net Mask[255.255.0.0]: 255.255.255.0 (Ingresar la máscara)

->**voice port IP Address[138.1.60.1]: 10.11.253.131 (este es un ejemplo, ingresar el IP del IAD para Voz)

LAN

->**IP Address[192.168.1.1]:<Enter> (dejar este valor por default)

->**Net Mask[255.255.255.0]: <Enter> (dejar este valor por default)

Public Network ipaddress in LAN

->Enable Public Netwok IPAddress in LAN? 'yes' or 'no'[no]: Y (Poner Y si es que el cliente necesita IPPúblico en la LAN, el IP Público que se brinde al router será el Default Gateway para las PCs públicas). Si elcliente no necesita IP público en la LAN colocar en 1 (no)

->**IP Address[200.31.96.1]: 190.14.241.36 (este es un ejemplo, IP Publica que se asignara al IAD en la LAN).

->**Net Mask[255.255.255.0]: 255.255.255.248 (mascara de la IP Pública)

->**Whether Use the Default Gateway, 'yes' or 'no'[no]: 190.81.73.1 (este es un ejemplo, Default gateway de la WAN).

Configuración de rutas estáticas (Comando:**add static-route**)

Dado que las IPs de Voz del IAD no cuenta con una ruta default gateway, es necesario agregaruna ruta estática apuntando a la red del Softswitch.

IAD(2)# add static-route (Ejecutar el commando ADD STATIC-ROUTE)

Choose your route type?(0-host, 1-net): 1 (Elegir 1, agregar una NET)

Please input dst network: 10.0.0.0 (configurar siempre la red 10.0.0.0)

Please input netmask: 255.0.0.0 (configurar siempre la máscara 255.0.0.0)
Choose your interface type?(0-Data, 1-Voice, 2-Config): 2 (Elegir 2 para agregar el Next hop)
Please input gateway address: 10.11.253.1 (Este es un ejemplo, aqui ingresar el Next hop del IAD que sera elIP de voz del tipo X.X.X.1)
Are you sure to change the configurations? 'yes' or 'no'[no]: y

Configuración del DHCP Server e IPs DNS (Comando:**set dhcp server**)
IAD(8)# set dhcp server
->Enable DHCP server ?'yes' or 'no'[yes]: <Enter>
Start IP.....[192.168.1.33]: <Enter>
End IP.....[192.168.1.254]: <Enter>
Pri DNS server.....[200.62.191.12]:<Enter>
Second DNS server....[200.24.191.12————————————————————]:<Enter>
Pri WINS server.....[192.168.1.1]: <Enter>
Second WINS server...[192.168.1.1]:<Enter>
Default GW.....[192.168.1.1]: <Enter>
Subnet Mask.....[255.255.255.0]: <Enter>
Must reset to take effect
Decide to change the configure? 'yes' or 'no'[no]:y <Enter> (Para aceptar los cambios)

Configuración de las VLANs (VLAN 20, VLAN 50) (Comando:**set vlan**)
IAD(2)# set vlan (ejecutar el commando set vlan)
Enable voice VLAN 'yes' or 'no'[no]: y (confirmer yes)
Voice VLAN priority (0~7)[0]: <Enter>
Voice VLAN tag (1~4090)[20]: <Enter>
Enable data VLAN 'yes' or 'no'[no]:y
Data VLAN priority (0~7)[0]:<Enter>
Data VLAN tag (1~4090)[50]:<Enter>
Port 1 Configuration:
Mode (0-route, 1-bridge)[0]:<Enter> (0 indica que el Port 1 será para datos, no Voz)
Port 2 Configuration:
Mode (0-route, 1-bridge)[0]:<Enter> (0 indica que el Port 2 será para datos, no Voz)
Port 3 Configuration:
Mode (0-route, 1-bridge)[0]:<Enter> (0 indica que el Port 3 será para datos, no Voz)
Port 4 Configuration:
Mode (0-route, 1-bridge)[0]:<Enter> (0 indica que el Port 4 será para datos, no Voz)

Are you sure? 'yes' or 'no'[no]:y

Configuración del servicio Wi-Fi (Comando: set wifi)

IAD(2)# set wifi

->Enable WiFi Wireless LAN (WLAN)? 'yes' or 'no' [yes]:<Enter>

->Input WiFi SSID Name(1-32Characters)[CLIENT]: NombreCliente (Elegir nombre)

->Enable WiFi SSID Hide? 'yes' or 'no' [no]: <Enter>

->Input WiFi Channel (1~11)[5]: <Enter> (Ver otros canales alternativos)

Wireless Mode:

1----B

2----G

->Input Wireless Mode(1 - 2)[2]: <Enter> (con esto se elige 802.11G)

Authentication Mode:

0----Open System

1----Shared Key

2----WPA-PSK

3----WPA2-PSK

->Input Authenfication Mode(0 - 3)[0]: <Enter>

Encrytpion Type:

0----NONE

1----WEP

->Input Encrytpion Type(0 - 1)[0]:1 (Elegir el modo de encriptación WEP)

Key Setting:

->Input WiFi Default Key Number(0 - 3)[0]: <Enter>

->Input WiFi Key(0~3)[0]: <Enter> (para ingresar el primer Key)

Key Type:

0----Hex(10/26 Char)

1----ASCII(5/13 Char)

->Input Key Type(0 - 1)[0]: <Enter> (elegir 0 hexadecimal)

->Input key(10/26 Character Hex)[1A2B3C4D5E]: XXXXXXXX(el que se elija con el cliente)

Continuing set key?'yes' or 'no' [no]:Q———————————————— (Elegir 1 para dejar de ingresar mas Keys)

->Input WiFi Beacon Interval(20 - 100ms)[100]:<Enter>

->Input WiFi DTIM Interval(1 - 255)[10]:<Enter>

->Input WiFi Fragment Threshold(256 - 2346)[2346]:<Enter>

->Input WiFi RTS Threshold(256 - 2346)[2346]:<Enter>

WiFi Set Successfully.

Are you sure reset the WIFI module? 'yes' or 'no'[no]: y (Elegir Y para grabar y hacer reset del WiFi)Atheros Wireless Device is Resetting ...

Configuración de la Voz

Telefonía:

Configuracion de los parámetros MGCP (Softswitch) (preconfigurado en la flash)

Configuracion del QoS (DSCP 40) (preconfigurado en la flash)

Configuracion de la preferencia de los codecs (preconfigurado en la flash)

Configuraciónde los parámetros MGCP (Comando:**set mgcp**)

IAD(2)# set mgcp (ejecutar el comando set mgcp)

->**Gateway Name[138.0.60.1]: CLIGA08mg000001 (es un nombre creado en el Softswitch que debe coincidir, el nombre es único para IAD se le asocia a su IP)

->**Gateway Port(Default port is 2427, and not within RTP port range) [2427]: <Enter>

->**RTP Port From (Default:3000, must more than 1024 and be even)[3000]: <Enter>

->**Calling Agent Address:[10.136.2.76]: <Enter> (el IP del Softswitch es: 10.136.2.76 ó 10.136.2.96 para ello deberá corroborar dicha información con el área de Conmutación el IP al que deberían apuntar, los dos son válidos)

->**Calling Agent Port(Default port is 2727)[2727]: <Enter>

->**Use Backup calling agent?'yes' or 'no'[yes]: <Enter>

->**Backup Calling Agent Address [10.136.2.96]: <Enter>

->** Backup Calling Agent Port(Default port is 2727)[2727]: <Enter>

->**Mode of Port Register(0-Single Match, 1-All Match)[1]: <Enter>

->**Transaction handle mode(0-step, 1-loop)[1]: <Enter>

->Mode of Number Transmit(0-single digital, 1-String)[1]: <Enter>

->**Type of Softswitch(0-HUAWEI, 1-NORTEL, 2-ZTE, 3-other)[1]: <Enter>

->Enable Inverpolar signal for accounting?'yes' or 'no'[yes]: <Enter>

->**Enable active heartbeat?'yes' or 'no'[no]: <Enter>

->**Enable passive heartbeat?'yes' or 'no'[no]: <Enter>

->Sending Event with package name?'yes' or 'no'[yes]: <Enter>

->Appoint the IP address in SDP?'yes' or 'no'[no]: <Enter>

Tacking effect must restart the system after configurations be saved!

Are you sure?'yer' or 'no'[no]: y <Enter>

Punto de Venta (POS IP)

Configuración de la VLAN POS MC y POS Visanet (preconfigurado en la flash)

Misceláneos
Configuración del pasword del modo de usuario y del modo privilegiado
Configuración del nombre (hostname) del equipo
Configuración de la velocidad y el tipo de transmisión de las puertas Ethernet (preconfigurado en la flash)

3.5.5. Configuración en los equipos de acceso:

Equipo de cara al cliente METRO (U-PE)

```
class-map match-any qos5
 match ip dscp cs5

class-map match-any qos1
 match ip dscp cs1

class-map match-any qos2
 match ip dscp cs2

policy-map Policer_IN_2048
 Class class-default
  set dscp default
   police 2048000 bps 384000 byte conform-action transmit exceed-action drop

policy-map Policer_OUT_2048
 Class class-default
  police 2048000 bps 384000 byte conform-action transmit exceed-action drop

policy-map Policer_IN_512_512_0_0
class qos5
 police 512000 bps 96000 byte conform-action transmit exceed-action drop
class class-default
 set dscp cs1
  police 128000 bps 24000 byte conform-action transmit exceed-action drop

policy-map Policer_OUT_512_512_0_0
```

```
class qos5
 police 512000 bps 96000 byte conform-action transmit exceed-action drop
class class-default
  police 128000 bps 24000 byte conform-action transmit exceed-action drop

policy-map Policer_IN_4096_512_1536_2048
class qos5
 police 512000 bps 96000 byte conform-action transmit exceed-action drop
class qos2
 police 1536000 bps 288000 byte conform-action transmit exceed-action drop
class qos1
 police 4096000 bps 768000 byte conform-action transmit exceed-action drop
class class-default
 set dscp cs1
  police 128000 bps 24000 byte conform-action transmit exceed-action drop

policy-map Policer_OUT_4096_512_1536_2048
class qos5
 police 512000 bps 96000 byte conform-action transmit exceed-action drop
class qos2
 police 1536000 bps 288000 byte conform-action transmit exceed-action policed-dscp-
transmit
class qos1
 police 4096000 bps 768000 byte conform-action transmit exceed-action drop
class class-default
  police 128000 bps 24000 byte conform-action transmit exceed-action drop

vlan 400
 name VLAN_VOZ
vlan 500
 name VLAN_INTERNET
vlan 1200
 name VLAN_DATOS

interface GigabitEthernet3/16
 description description Conexion WAN con CPE-Cliente
 switchport trunk encapsulation dot1q
```

```
switchport trunk allowed vlan 400,500,1200
 switchport mode trunk
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 10
 switchport port-security violation restrict
 logging event link-status
 load-interval 30
 speed 100
 duplex full
 qos trust dscp
 tx-queue 3
   priority high
 vlan-range 400
  service-policy input Policer_IN_512_512_0_0
  service-policy output Policer_OUT_512_512_0_0
 vlan-range 500
  service-policy input Policer_IN_2048
  service-policy output Policer_OUT_2048
 vlan-range 1200
  service-policy input Policer_IN_4096_512_1536_2048
  service-policy output Policer_OUT_4096_512_1536_2048
 spanning-tree portfast trunk
 spanning-tree bpduguard enable
spanning-tree guard root
```

Equipo de cara al proveedor o red de transporte (N-PE)

```
class-map match-any qos5
  match ip dscp 40
  match ip dscp 48
  match ip dscp 46
  match  precedence 5

class-map match-any qos1
  match ip dscp 8
  match ip dscp 18
  match ip dscp 20
```

```
  match ip dscp 22
class-map match-any qos2
  match ip dscp 16
  match ip dscp 26
  match ip dscp 28
  match ip dscp 30
  match  precedence 2

policy-map Shape4096
 class class-default
  Shape average 4096000

policy-map WAN_4096_512_1536_2048
 class qos5
   priority
  police 512000 96000 192000 conform-action transmit exceed-action drop
 class qos2
  bandwidth 1536
  random-detect
  random-detect precedence 2 2000 packets 8000 packets 1
 class qos1
  bandwidth 2048
  random-detect
  random-detect precedence 1 2000 packets 8000 packets 1
 class class-default
  random-detect

policy-map Shape4096_512_1536_2048
 class class-default
   shape average 4096000
  service-policy WAN_4096_512_1536_2048

policy-map Shape512
 class class-default
  Shape average 512000

policy-map WAN_512_512_0_0
```

```
 class qos5
   priority
  police 512000 96000 192000 conform-action transmit exceed-action drop
 class class-default
  random-detect

policy-map Shape512_512_0_0
 class class-default
   shape average 512000
  service-policy WAN_512_512_0_0

ip vrf 01006
description Servicio de VoIP con plataforma Softswitch
rd 12252:1006
 route-target export 12252:1000001006
 route-target import 12252:1000001006

ip vrf 01200
 description VPN Enlace de Datos
rd 12252:1200
 route-target export 12252:1000001200
 route-target import 12252:1000001200

router bgp 12252
neighbor WAN_INTERNET peer-group
neighbor WAN_INTERNET remote-as 64516
neighbor WAN_INTERNET password e#&235ty
neighbor WAN_INTERNET timers 10 30
neighbor WAN_INTERNET soft-reconfiguration inbound
neighbor WAN_INTERNET remove-private-AS
neighbor WAN_INTERNET route-map dualhome in
neighbor WAN_INTERNET prefix-list REDES_CLIENTE in
neighbor 190.81.41.2 peer-group WAN_INTERNET
neighbor 190.81.41.2 description Enlace Internet Principal activo
neighbor 190.81.41.2 activate
neighbor 190.223.37.50 peer-group WAN_INTERNET
neighbor 190.223.37.50 description  Enlace Internet Principal respaldo
```

```
neighbor 190.223.37.50 activate
address-family ipv4 vrf 01200
 redistribute connected
 neighbor WAN_DATOS peer-group
 neighbor WAN_DATOS remote-as 64516
 neighbor WAN_DATOS password e#&235ty
 neighbor WAN_DATOS timers 10 30
 neighbor WAN_DATOS activate
 neighbor WAN_DATOS send-community both
 neighbor WAN_DATOS as-override
 neighbor WAN_DATOS soft-reconfiguration inbound
 neighbor WAN_DATOS route-map dualhome in
 neighbor 10.10.10.1 peer-group WAN_DATOS
 neighbor 10.10.10.1 description Enlace de Datos Principal activo
 neighbor 10.10.46.5 peer-group WAN_DATOS
 neighbor 10.10.46.5 description Enlace de Datos Principal respaldo
 no synchronization
 exit-address-family

address-family ipv4 vrf 01006
 redistribute connected
 neighbor WAN_VOZ peer-group
 neighbor WAN_VOZ remote-as 64516
 neighbor WAN_VOZ password e#&235ty
 neighbor WAN_VOZ timers 10 30
 neighbor WAN_VOZ activate
 neighbor WAN_VOZ send-community both
 neighbor WAN_VOZ as-override
 neighbor WAN_VOZ soft-reconfiguration inbound
 neighbor WAN_VOZ route-map dualhome in
 neighbor 10.10.10.9 peer-group WAN_DATOS
 neighbor 10.10.10.9 description Enlace de VOZ Principal activo
 neighbor 10.10.46.13 peer-group WAN_DATOS
 neighbor 10.10.46.13 description Enlace VOZ Principal respaldo
 no synchronization
```

```
 exit-address-family
interface GigabitEthernet3/1/6.101200
description Enlace de Datos Principal activo
encapsulation dot1Q 1200
 ip vrf forwarding 01200
 ip address 10.10.10.2 255.255.255.252
 no ip directed-broadcast
 no cdp enable
 service-policy input Shape4096
 service-policy output Shape4096_512_1536_2048

interface GigabitEthernet3/1/6.101220
description Enlace de Datos Principal respaldo
encapsulation dot1Q 1220
 ip vrf forwarding 01200
 ip address 10.10.10.6 255.255.255.252
 no ip directed-broadcast
 no cdp enable
 service-policy input Shape4096
 service-policy output Shape4096_512_1536_2048

interface GigabitEthernet3/1/6.100400
description Enlace de VOZ Principal activo
encapsulation dot1Q 400
 ip vrf forwarding 01006
 ip address 10.10.10.10 255.255.255.252
 no ip directed-broadcast
 no cdp enable
 service-policy input Shape512
 service-policy output Shape512_512_0_0

interface GigabitEthernet3/1/6.100440
description Enlace de VOZ Principal respaldo
encapsulation dot1Q 440
 ip vrf forwarding 01006
 ip address 10.10.10.14 255.255.255.252
 no ip directed-broadcast
```

```
 no cdp enable
 service-policy input Shape512
 service-policy output Shape512_512_0_0

ip prefix-list REDES_CLIENTE seq 5 permit 190.223.37.0/26

ip community-list 1 permit 12252:200
ip community-list 1 permit 0:200
ip community-list 2 permit 12252:201
ip community-list 2 permit 0:201

route-map dualhome permit 10
 match community 1
 set local-preference 100

route-map dualhome permit 20
 match community 2
 set local-preference 98
```

CAPITULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1. Análisis sobre los elementos considerados en la red

El servicio de Red Privada Virtual sobre la red MPLS está orientado a ofrecer la integración de los servicios a través de un proveedor con lo cual tenemos:

Convergencia: Consolidar la comunicación de voz, datos e Internet en un solo enlace, reflejándose una reducción de costos.

Integración: Con el protocolo IP se permite el uso de equipo, dando un reúso a estos equipos.

Seguridad: Se los enlace VPN con autenticación y algoritmos complejos, asegurando la privacidad y seguridad.

Escalabilidad: La red implementada soporta diferentes cambios sobre servicios y redes siendo el cambio o modificaciones de fácil implementación en cuanto coste y horas hombre.

Calidad de servicios: La Red Privada Virtual sobre la red MPLS garantiza la priorización de trafico de acuerdo a las aplicaciones que requieran servicio en tiempo real o si son datos críticos.

Alta disponibilidad: La red implementada tiene una disponibilidad de 99.99%, la cual está asegurada no solo por la solución implementada en el cliente sino también por la red del proveedor.

4.2. Análisis de los servicio implementados sobre la red del cliente

Se han implementado servicio de Voz, servicio de Datos e Internet todo soportado sobre un equipo encaminador como equipo principal y otro como respaldo, se han separado los servicios sobre estos equipos con VPN locales aplicadas sobre el mismo encaminador, esto para asegurar la correcta separación de procesamiento, tráfico y calidad sobre los servicios.

La interconexión entre los equipo de diferentes sedes o locales de cliente es a través de la red del proveedor de servicios, quien asegura en tráfico a nivel capa 3 (IP), capa 2

(Enlace de datos) y física como también la priorización de los tipos de trafica de acuerdo a la calidad requerida por el cliente.

La Red Metro Ethernet del proveedor de servicio soporta puertos con capacidades de Giga bps, con lo cual asegura una escalabilidad para los futuras modificaciones o crecimiento de las redes de los clientes.

Los enlaces de respaldo esta soportado sobre un enlace inalámbrico lo cual asegura en caso de una averia grave mantener activos los servicio del cliente, en comportamiento normal de servicio los enlaces principales tiene como medio físico fibra óptica asegurando confiabilidad.

CONCLUSIONES Y RECOMENDACIONES

1. Los enlaces de contingencia juegan un papel muy importante en las telecomunicaciones, independientes del medio o tecnología que se use, las cuales pueden implementarse de acuerdo a las necesidades de cada usuario, un enlaceinalámbrico o un enlace similar, además de tener contingencia no solo en los servicio sino en los equipos en cada punto del enlace. Esto se debe elegir luego de un estudio en el cual se verificara el costo beneficio por cada punto.
2. Se deben tener muy claros los criterios de enrutamiento para la conmutación del enlace principal al de contingencia, ya que de no estar bien definidos podría derivar en un mal funcionamiento del enlace de contingencia, como consecuencia la activación del enlace alterno sin haberse afectado el enlace principal.
3. En el caso de un enlace de contingencia inalámbrico se debe tener en cuenta la línea de vista para el enlace entre el equipo acceso y el equipo del cliente, ya que este enlaces es muy susceptible debido a las interferencias del medio en este caso el aire, esto podría afectarla disponibilidad de los servicios. Para evitar este tipo de problemas se aseguran los enlaces con torres donde están instaladas las antenas que brindan el enlace inalámbrico.
4. Como se ha desarrollado en este informe se pueden tener enlace inalámbricos para servicios corporativos como son datos críticos y voz manteniendo la calidad en cuanto al enlace y disponibilidad logrando con esto ahorrar costos y tiempo de instalación.
5. En un posible crecimiento de la red se requerirán cambios en el acceso a la red del proveedor, para estos cambio de deben definir nuevamente la factibilidad de usar el enlace de respaldo con fibra óptica, esto para brindar mayor disponibilidad al enlace y menor degradación, esto se debe analizar revisando los recursos del cliente y la factibilidad técnica y económica.

ANEXO A

GLOSARIO DE TERMINOS

10 BASE-T: Esta es una especificación técnica que se utiliza en redes Ethernet. 10 BASE-T forma parte de la especificación del organismo de estándares IEEE para Ethernet (10Mbps) sobre las Categorías 3, 4 o 5 de cable de par trenzado (dos pares de cables - un par para transmitir datos y el segundo para recibirlos). 10 BASE-T tiene un límite de distancia por segmento de 100m (328 pies) aproximadamente.

100 BASE-TX: Esta es una especificación técnica utilizada en las redes Fast Ethernet. 100 BASE-TX forma parte de la especificación del conjunto de estándares IEEE para cable (2 pares de cables - un par para transmitir datos y el segundo para recibirlos) de la Categoría 5 UTP (par trenzado no blindado) o STP (par trenzado blindado) de 100Mbps (Fast Ethernet).

802.1Q: Es también conocido como IEEE 802.1Q VLAN o etiquetado. Se define una red de área local virtual. Es un protocolo que permite a las redes LAN virtuales para comunicarse entre sí utilizando un router 3-capas. Fue desarrollado como parte del estándar IEEE 802.

ADSL: Línea Subscriptora Digital Asimétrica. Línea de teléfono que transfiere datos a alta velocidad. La parte "asimétrica" quiere decir velocidades diferentes de transmisión, desde el cliente a la compañía telefónica, de hasta 640 Kbps, y desde la compañía telefónica al cliente de 1.544 a 6.1 Mbps.

AS: AutonomousSystem, Colección de redes bajo una administración común que comparten una estrategia de enrutamiento común. Los sistemas autónomos se subdividen en áreas. Un sistema autónomo puede ser asignado un número de 16 bits exclusivo por la IANA. A veces se abrevia AS.

ASIC: Application-SpecificIntegratedCircuit o Circuito integrado para una aplicación específica.

ATM: Acrónimo en inglés de Asynchronous Transfer Mode. Modo de Transferencia Asincrónica. Es una tecnología de redes de alta velocidad que transmite múltiples tipos de información (voz, vídeo, datos) mediante la creación de "paquetes de datos.

Back office: Es la parte de las empresas donde tienen lugar las tareas destinadas a gestionar la propia empresa y con las cuales el cliente no necesita contacto directo. Por ejemplo: el departamento de informática y comunicaciones que hace que funcionen los ordenadores, redes y teléfonos, el departamento de recursos humanos, el de contabilidad, etc.

Backbone: La parte de la red que transporta el tráfico más denso: conectaLANs, ya sea dentro de un edificio o a través de una ciudad o región.

Besteffort: En telecomunicaciones se habla de “besteffort”, que se podría traducir (aunque habitualmente no se hace) como “el mejor esfuerzo”, para definir la forma de prestar aquellos servicios para los que no existe una garantía de calidad de servicio (QoS). Esto implica que no existe una preasignación de recursos, ni plazos conocidos, ni garantía de recepción correcta de la información.

BGP: Border Gateway Protocol, protocolo de frontera que proporciona las reglas de comunicación en enlaces WAN.

Bridge: En redes de computadoras, un "bridge" (puente), conecta dos o más redes de área local (LAN) y WLAN entre si. Puede ser un dispositivo, o una computadora lo que haga el puente.

CBS: CommittedBurstSize, es el tamaño de la información utilizado para obtener el CIR respectivo.

CDP: (Cisco DiscoveryProtocol, 'protocolo de descubrimiento de Cisco', es un protocolo de red propietario de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos.

CE: CustomerEdge. Es un router que se ubica en el extremo de la red del cliente que permite el acceso al núcleo MPLS.

CIR: (CommittedInformationRate): es la cantidad promedio de información que se ha transmitido, teniendo en cuenta los retardos, pérdidas, etc.

Codec: Abreviatura de codificador-decodificador. Describe una especificación desarrollada en software, hardware o una combinación de ambos, capaz de transformar un archivo con un flujo de datos (stream) o una señal. Los códecs pueden codificar el flujo o la señal (a menudo para la transmisión, el almacenaje o el cifrado) y recuperarlo o descifrarlo del mismo modo para la reproducción o la manipulación en un formato más apropiado para estas operaciones. Los códecs son usados a menudo en videoconferencias y emisiones de medios de comunicación.

CoS: Class of Service, Es un algoritmo que compara los campos en los paquetes o las etiquetas CoS para clasificarlos y asignarlos a una cola, dependiendo de su prioridad.

CPE: Customer Premies Equipment. Equipo ubicado en la propiedad del usuario.

DCE: Data Circuit-terminatingEquipment (Equipo de Terminación del Circuito de Datos). El equipo que constituye un punto de acceso a la red, o un nodo de red, o el equipo en el cual un circuito de red finaliza; en el caso de una conexión RS-232, el modem es usualmente reconocido como el DCE, mientras que el terminal del usuario es reconocido como al DTE, o equipo terminal de datos.

Dial Up: Conexión de red la cual se puede crear y desechar según se requiera que se establece usando un emulador de terminal y un módem y realiza una conexión de datos a través de una línea telefónica. Los enlaces de marcado por línea telefónica son la forma más sencilla de conexiones con acceso conmutado. Los protocolos utilizados generalmente en este tipo de conexiones son SLIP y PPP.

DSL: Línea Subscriptora Digital. Tecnología para facilitar información de ancho de banda alta a usuarios residenciales y pequeños negocios, a través de líneas telefónicas normales de cobre.

DTE: Data Terminal Equipment (Equipo Terminal de Datos. Generalmente).Dispositivos de usuario, tales como terminales y computadores, que se conecta al Equipo de Terminación del Circuito de Datos (DCE); éstos generan o reciben los datos transportados por la red.

DWDM: Dense wavelengthDivisionMultiplexing, que significa Multiplexación por división en longitudes de onda densas. DWDM es una técnica de transmisión de señales a través de fibra óptica usando la banda C (1550 nm).

eBGP: BGP externo, conexiones BGP entre routers fronterizos (distintos SA).

EBS: ExcessBurstSize, es el tamaño de información que se necesita para obtener el EIR determinado.

EGP: Exterior Gateway Protocol, Protocolo de salida exterior. Protocolo que emite direcciones TCP/IP a la salida en otra red.

EIA: Asociación de Industrias Electrónicas. Es una organización de comercio industrial que, junto con TIA (Asociación de la Industria de la Telecomunicación), define las normas de los productos eléctricos. EIA y TIA especifican las normas de transmisión de datos tales como EIA/TIA-232.

EIR: ExcessInformationRate, especifica la cantidad de información mayor o igual que el CIR, hasta el cual las tramas son transmitidas sin pérdidas.

End-plug: Extremo del cable de red.

ENUM: TelefoneNumberMapping (ENUM o Enum) se diseñó para resolver la cuestión de como se pueden encontrar servicios de internet mediante un número telefónico, es decir cómo se pueden usar los los teléfonos, que solamente tienen 12 teclas, para acceder a servicios de Internet. La parte más básica de ENUM es por tanto la convergencia de las redes del STDP y la IP; ENUM hace que pueda haber una correspondencia entre un número telefónico y un identificador de Internet. En síntesis, Enum es un conjunto de protocolos para convertir números E.164 en URIs, y viceversa, de modo que el sistema de numeración E.164 tenga una función de correspondencia con las direcciones URI en Internet.

Ethernet: Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus; tiene ancho de banda de 10 Mbps, por lo tanto tiene una elevada velocidad de transmisión y se ha convertido en un estándar de red.

EtherType: Es un campo en Ethernet estándar del establecimiento de una red (Ethernet II que enmarca, específicamente). Se utiliza para indicar cuál protocolo se está transportando en Ethernet marco.

FEC: (ForwardingEquivalenceClass): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

Firewall: Combinación de hardware y software la cual separa una red de área local (LAN) en dos o mas partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

Frame-Relay: Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet. Se puede recrear un framerelay usando tunneling.

FTTH: La tecnología de telecomunicaciones FTTH (del inglés FiberToThe Home), también conocida como fibra hasta el hogar, se basa en la utilización de cables de fibra óptica y sistemas de distribución ópticos adaptados a esta tecnología para la distribución de servicios avanzados, como el Triple Play: telefonía, Internet de banda ancha y televisión, a los hogares y negocios de los abonados.

Gateway: Un gateway es un punto de red que actua como entrada a otra red. En el internet, un nodo o "parada" puede ser un "nodo gateway" o un "nodo host". Tanto las computadoras de los usuarios como las computadoras que sirven páginas a usuarios son "nodos host". Las computadoras que controlan el tráfico de data dentro una red local o a nivel de proveedores de internet (ISP) son "nodos gateway". Usualmente los gateways son asociados con el router y switch.

Gigabit Ethernet: También conocida como GigaE, es una ampliación del estándar Ethernet (concretamente la versión 802.3ab y 802.3z del IEEE) que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet (También llamado 100-Base/T).

Hub: El punto central de conexión para un grupo de nodos; útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

HW: Hardware. Maquinaria, componentes físicos de una computadora o de una red (a diferencia de los programas o elementos lógicos que los hacen funcionar).

iBGP: BGP interneo, conexiones BGP dentro de un SA.

ID: Identificación

IDU: InDoorUnit, Unidad interna, es transceiver y demas componentes pasivos y activos.

IEEE: Siglas en ingles para Institute of Electrical and ElectronicsEngineers, organización profesional internacional sin fines de lucro, para el avance de la tecnología relacionada a la electricidad. Tiene la mayor cantidad de miembros que cualquier otra organización profesional técnica en el mundo, con más de 365,000 miembros en cerca de 150 países. IEEE es una de las organizaciones líderes en el mundo creando estándares.

IETF: Internet EngineeringTaskForce (en español Fuerza de Trabajo en Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE. UU. en 1986. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como http: //es.wikipedia.org/wiki/Request_For_Comments.

IGP: (Interior Protocol Gateway) Hace referencia a los protocolos usados dentro de un sistema autónomo. Los protocolos IGP más utilizados son RIP y OSPF.

IMS: Subsistema Multimedia IP (o IP Multimedia Subsystem) forma parte del núcleo de la arquitectura de las redes de siguiente generación. Estas redes son capaces de proporcionar servicios multimedia fijos y móviles. En lo relativo a telefonía, para

establecer la comunicación de voz emplean una variante de voz sobre IP (VoIP) basada a su vez en una variante de SessionInitiationProtocol que fue normalizada por el 3GPP. Estas redes NGN pueden establecer llamadas con la Red Telefónica Conmutada actual, tanto si es de conmutación de circutos como de conmutación de paquetes.

Internet: Una red mundial, de redes de computadoras. Es una interconexión de redes grandes y chicas alrededor del mundo. El Internet empezó en 1962 como una red para los militares llamada ARPANet, para que en sus comunicaciones no existan puntos de falla. Con el tiempo fue creciendo hasta convertirse en lo que es hoy en día, una herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP. Sobre esta red se pueden utilizar multiples servicios como por ejemplo emails, WWW, etc. que usen TCP/IP.

Intranet: Red privada dentro de una compañía u organización que utiliza el navegador favorito de cada usuario, en su computadora, para ver menus con opciones desde cumpleaños del personal, calendario de citas, mensajería instantánea privada, repositorio de archivos y las normativas de la empresa entre otras. Es como si fuera un sitio web dentro de la empresa. Al usar un navegador de internet como Internet Explorer, Firefox, Chrome y Safari, el intranet se convierte en multiplataforma. No importa la marca o sistema operativo de las computadoras dentro de la red, todos se pueden comunicar.

IP-Based: Basado en protocolo IP.

IPsec: Abreviatura de Internet Protocolsecurity es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

ISP: Internet ServiceProvider. Proveedor de Servicio Internet. Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.

Jitter: Término inglés para fluctuación, a la variabilidad temporal durante el envío de señales digitales, una ligera desviación de la exactitud de la señal de reloj (en inglés Clock). El jitter suele considerarse como una señal de ruido no deseada. En general se denomina jitter a un cambio indeseado y abrupto de la propiedad de una señal. Esto puede afectar tanto a la amplitud como a la frecuencia y la situación de fase. El jitter es la primera consecuencia de un retraso de la señal. La representación espectral de las variaciones temporales se denomina ruido de fase.

LACP: Dentro de la especificación IEEE Link Aggregation Control Protocolo proporciona un método para controlar la agrupación de varios puertos físicos para formar un solo canal lógico. LACP permite a un dispositivo de red para negociar un agrupamiento automático de los enlaces mediante el envío de paquetes pares a LACP.

LAN: Local Area Network. Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones. Por ejemplo, computadoras conectadas en una oficina, en un edificio o en varios. Se pueden optimizarse los protocolos de señal de la red hasta alcanzar velocidades de transmisión de 100 Mbps .

LDP: (LabelDistributionProtocol): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.

Leased-line: Línea alquilada, Línea dedicada.

LER: (LabelEdgeRouter): elemento que inicia o termina el túnel (pone y quita cabeceras).

LLC: Control de enlace lógico LLC ("Logical Link Control") define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores. xx Es la más alta de las dos subcapas de enlace de datos definidas por el IEEE y la responsable del control de enlace lógico. La subcapa LLC maneja el control de errores, control del flujo, entramado y direccionamiento de la subcapa MAC.

LSP: (LabelSwitchedPath): nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos.

LSR: (LabelSwitchingRouter): elemento que conmuta etiquetas.

Mac address: Siglas del inglés Media Access Control. Es una dirección que usualmente esta compuesta por números y letras asignado a los equipos que forman parte de una red, que es único e identifica su lugar dentro de la red. El comite de IEEE asigna bloques de direcciones a los fabricantes de tarjetas de red. De esta forma se asegura que no existan dos tarjetas de red con el mismo Mac address.

MAN BUCLE: Se basan en tecnologías Bonding, de forma que los enlaces están formados por múltiples pares de cobre con el fin de ofrecer el ancho de banda necesario, ofrecen velocidades de 10Mbps, 20Mbps, 45Mbps, 75Mbps, sobre pares de cobre y 100Mbps, 1Gbps y 10Gbps mediante Fibra Óptica.

MDF: MainDistributionFrame (MainFrame o en ocasiones denominado Site) es una estructura de distribución de señales para conectar equipo de redes y telecomunicaciones a los cables y equipos que corresponden al proveedor de servicios de telefonía, Internet, entre otros.

Media Servers: Servidor de medios de comunicación se refiere tanto a un aparato o equipo dedicado a una aplicación de software especializados, que van desde una máquina de clase empresarial proporciona vídeo por pago, para, más comúnmente, un pequeño ordenador personal o NAS (Network Attached Storage) para el hogar, dedicado a el almacenamiento de diversos medios digitales (es decir, videos digitales / películas, audio y música, y archivos de imagen).

MEF: Metro Ethernet Forum es un consorcio sin fines de lucro de la industria internacional, dedicada a todo el mundo la adopción de redes Carrier Ethernet Redes y servicios.

Monomodo, fibra: Mono-Modo (Single-Mode = SM), es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación, su transmisión es en línea recta. Su distancia va desde 2.3 km a 100 km máximo y usa centro con cañón

láser de alta intensidad. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias y transmitir elevadas tasas de bit.

MPLS: (MultiprotocolLabelSwitching) Es un mecanismo de transporte de datos estándar creado por la IETF. Opera entre la capa de enlace de datos y la capa de red del modelo OSI.

Multiplexar: Es la combinación de dos o más los cuales pueden ser canales de información en un solo medio de transmisión usando un dispositivo llamado multiplexor. El proceso inverso se conoce como demultiplexación.

NAS: Network Attached Storage, es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (Servidor) con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

NAT: Programa creado a finales de los años noventa por el estudiante ShawnFanning el cual permitia a los usuarios de Internet la búsqueda y descarga de piezas musicales en formato mp3. Tuvo gran presión por parte de artistas y casas disqueras, entre otros, que acusaban a Napster de promover la piratería e infringir en la propiedad intelectual. Napster tuvo que cambiar su formato, y actualmente vende música descargable desde el sitio, www.napster.com. Esta en el glosario porque consideramos que Napster jugó un papel importante en la "masificación" del mp3, lo cual ha creado hoy en día un mercado posible para productos como el ipod.

Netwoking: Término utilizado para referirse a las redes de telecomunicaciones en general.

Network: Red o sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

Next-hop: Se refiere al siguiente salto, el router que sigue en el LSP.

NGN: Red de Siguiente Generación o Red Próxima Generación (NextGenerationNetworking o NGN en inglés) es un amplio término que se refiere a la evolución de la actual infraestructura de redes de telecomunicación y acceso telefónico con el objetivo de lograr la congruencia de los nuevos servicios multimedia (voz, datos, video...) en los próximos 5-10 años.

NIC: Network Interface Card, o Tarjeta de interfaz de red (también conocida como adaptadora o tarjeta adaptadora). Es una placa de circuito instalada en un componente de equipo de informática, como un PC, por ejemplo, que le permite conectar su PC a una red.

NSP: Network ServiceProvider, proveedores de servicio IP/Internet, en lugar de las habituales ISP (Internet ServiceProvider), para hacer énfasis en la provisión del servicio de acceso a backbones IP, más que en el servicio de conexión a Internet de usuarios finales.

ODU: OutDoorUnit, Unidad externa, Generalmente la ODU es la antena y que contiene el transceptor (transceiver); es decir el conjunto con todo y antena.

ONU: Optical Network Unit, unidad de red óptica.

OSI: Modelo teórico propuesto por IEEE que describe cómo deberían conectarse distintos modelos de computadoras a diferentes tipos de red para poder comunicarse entre sí.

OSPF: Open shortestpathfirst, protocolo de frontera que proporciona las reglas de comunicación en enlaces WAN.

OSS: Oficina de Servicios Estratégicos, más conocida por su nombre original en inglés, Office of StrategicServices, fue el servicio de inteligencia de los Estados Unidos de América durante la Segunda Guerra Mundial. Está considerada la predecesora de la Agencia Central de Inteligencia o CIA.

Overhead: Costos operativos, sobrecarga.

Patchcord: Son cables de conexión de red que se usa en una red para conectar un dispositivo electrónico con otro. Su punta termina en un RJ-45 macho.

PBR: Policy-BasedRoutingó Ruteo Basado en Políticas. Que es lo contrario del ruteo ordinario.

PE: ProviderEdge. Son los routers que se colocan en los extremos del núcleo MPLS. Los routers PE clasifican paquetes de ingreso desde los routers CE, según los valores de prioridad IP asociados.

Peer-to-peer: P2P, una red informática que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red.

PON: Red óptica pasiva (del inglés PassiveOptical Network) permite eliminar todos los componentes activos existentes entre el servidor y el cliente introduciendo en su lugar componentes ópticos pasivos (divisores ópticos pasivos) para guiar el tráfico por la red, cuyo elemento principal es el dispositivo divisor óptico (conocido como splitter). La utilización de estos sistemas pasivos reduce considerablemente los costes y son utilizados en las redes FTTH.

PPP: Protocolo Punto a Punto. Es un protocolo que puede ser usado para enviar data por lineas seriales. PPP tiene revisión de error, control de enlace, autenticación, y puede ser usado para transportar IP, IPX y otros protocolos. PPP esta reemplazando a SLIP.

Protocolo: Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

PSTN: Public Switching Telecommunications Network. (Red Telefónica Pública Conmutada).

PVC: Permanent Virtual Circuits, Conexión que reemplaza las líneas privadas por un sólo enlace a la red.

QoS: Calidad de Servicio (Quality of Service, en inglés) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

Registered Jack: Registeredjack (RJ) es un estándar para interfaz física, tanto para la construcción de conectores como para el diseño del cableado, para la conexión de equipos de telecomunicaciones o de datos. Los estándares de diseño para estos conectores y sus cableados se denominan RJ11, RJ14, RJ21, RJ48, etc., y son bastante usados a nivel internacional.

RFC: RequestForComment. Petición de comentarios. Serie de documentos iniciada en 1967 que describe el conjunto de protocolos de Internet. Los RFC son elaborados por la comunidad Internet.

RIB: Base de información de Ruteo

RIP: RoutingInformationProtocol, protocolo de frontera que proporciona las reglas de comunicación en enlaces WAN.

RJ-45: Es un conector estándar que se utiliza para conectar las redes Ethernet. "RJ" son las siglas de las palabras "registeredjack" o clavija registrada.

Router: Un dispositivo que determina el siguiente punto de la red hacia donde se dirige un paquete de data en el camino hacia su destino. El routeresta conectado por lo menos a dos redes, y determina hacia que lado enviar el paquete de data dependiendo en el entendimiento del router sobre las redes que esta conectado. Los routers crean o mantienen una "tabla" de rutas disponibles, y usa esta informacion para darle la mejor ruta a un paquete, en un determinado momento.

RTP: Real Time Protocol, Protocolo de Tiempo Real. Protocolo utilizado para la transmisión de información en tiempo real, en aplicaciones en que una fuente genera un flujo de datos a velocidad constante, y uno o más dispositivos de destino entregan esos datos a una aplicación, a la misma velocidad constante, como en el caso de videoconferencia y video distribución en vivo.

SDH: Jerarquía Digital Síncrona (Synchronous Digital Hierarchy) , se puede considerar como la revolución de los sistemas de transmisión, como consecuencia de la utilización de la fibra óptica como medio de transmisión.

SIP: SessionInitiationProtocol (SIP o Protocolo de Inicio de Sesiones) es un protocolo desarrollado por el grupo de trabajo MMUSIC del IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

SLA: acuerdo de nivel de servicio o ServiceLevelAgreement, también conocido por las siglas ANS o SLA, es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

SLIP: Serial Line Internet Protocol. Protocolo de Internet para líneas en serie. Utilizado para gestionar el protocolo IP en líneas seriales tales como circuitos telefónicos o cables RS-232, interconectando dos sistemas SLIP está definido en RFC 1055, pero no es un estándar oficial de Internet y está siendo reemplazado por el protocolo PPP.

Softswitch: Principal dispositivo en la capa de control dentro de una arquitectura NGN (NextGeneration Network), encargado de proporcionar el control de llamada (señalización y gestión de servicios), procesamiento de llamadas, y otros servicios, sobre una red de conmutación de paquetes (IP).

Splitter: Es un dispositivo que divide la señal de teléfono en varias señales, cada una de ellas en una frecuencia distinta. Este dispositivo se utiliza frecuentemente en la instalación de líneas ADSL, donde es necesario que la señal de datos y de voz convivan en la misma línea telefónica; esto se consigue dividiendo las señales de entrada de baja frecuencia para la transmisión voz y de las de alta frecuencia para datos, permitiendo un uso simultaneo de ambos servicios.

Stack: Una pila (stack en inglés) es una lista ordinal o estructura de datos en la que el modo de acceso a sus elementos es de tipo LIFO (del inglés Last In FirstOut, último en entrar, primero en salir) que permite almacenar y recuperar datos. Se aplica en multitud de ocasiones en informática debido a su simplicidad y ordenación implícita en la propia estructura.

STB: Set top Box, equipo para la recepción de televisión.

STP: SpanningTreeProtocol, es un protocolo de red de nivel 2 de la capa OSI, (nivel de enlace de datos). Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE 802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.

SW: Software, se refiere a programas en general, aplicaciones, juegos, sistemas operativos, utilitarios, antivirus, etc. Lo que se pueda ejecutar en la computadora.

Switch: En una red, un switch es un equipo que por medio de la dirección física del equipo (Mac address) en los paquetes de data determina a que puerto reenviar la data. Usualmente se asocia con el " Gateway".

TCP: Transmission Control Protocol. Protocolo de nivel de transporte de la familia TCP/IP.

TCP/IP: Familia de protocolos definida para la operación en entornos interred.

TDM: Multiplexación por división de tiempo es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de trasmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de trasmisión.

TI: Tecnologías de la información y la comunicación (TIC, TICs o bien NTIC para Nuevas Tecnologías de la Información y de la Comunicación o IT para «InformationTechnology») agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, Internet y telecomunicaciones.

TIA: Asociación de la Industria de la Telecomunicación. Es una organización de estándares de telecomunicación fundada en América en 1988. La TIA se formó por un grupo derivado de la EIA (Asociación de las Industrias Electrónicas) con el fin de definir unos estándares de telecomunicaciones globales, como por ejemplo el EIA/TIA-232.

Token ring: Es el término utilizado para referirse a la norma IEEE 802.5 para implementar una red LAN con topología lógica de anillo. Tecnología creada originalmente por IBM (algunos la llaman "IBM Token Ring").

Transcodificar: Se denomina transcodificar (transcoding) a la conversión directa (de digital a digital) de un códec a otro, en general con pérdida de calidad.

Trunking: Función para conectar dos switchs, routers o servidores del mismo modelo o también de modelos diferentes definiendo varias vias de comunicación, mediante 2 cables en paralelo en modo Full-Duplex.

TTL: (Time to Live) Indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen. Este valor va disminuyendo cada vez que un router recibe y reenvía el paquete. Cuando este valor llega a cero, el paquete deja de ser reenviado.

Tunneling: Tecnología que permite que una red mande su data por medio de las conexiones de otra red. Funciona encapsulando un protocolo de red dentro de los paquetes de la segunda red. Es el acto de encapsular un protocolo de comunicación dentro de otro a través de dispositivos y Routers.

UA: Universal Adapter, Adaptador universal.

UNI: User Network Interface, En las redes Asynchronous Transfer Mode (ATM) (Modo de Transferencia Asíncrona), hay dos tipos de interfaces que describen cómo se comunican estos elementos: interfaces de usuario a red (UNI, User-to-Network Interfaces) e interfaces de red a red (NNI, Network-to-Network Interfaces).

UTP: Par trenzado no blindado. Cable que consiste en un par o más de cables (que se utilizan en una gran variedad de aplicaciones de red) que están enfundados en plástico. UTP es popular porque es muy maleable y no ocupa tanto espacio como los STP y otros cables.

VLAN: Red de área local virtuales. Se trata de un grupo de dispositivos que están conectados en red lógica. Los dispositivos están conectados en red en diferentes

BIBLIOGRFIA

1. Luc De Ghein, "MPLS Fundamentals", Cisco Press, 2007.
2. Corporate Headquarters, "Layer 3 MPLS VPN Enterprise Consumer Guide", Cisco System, Inc., 2006.
3. Giuseppe A. Rattá, "Conceptos Avanzados de Redes", Universidad Complutense de Madrid, 2003.
4. Francisco Córdova, "Tecnologías de Acceso", Conatel, 2006.
5. Ivan Pepelnjak, Cisco Press: Arquitecturas Mpls Y Vpn - Cp, 2002.
6. Antonio Gallego de Torres, Routers Cisco, 2010.
7. Cisco Systems. "Justification for converged networks, An economic approach", Cisco Press. United States. 2001
8. Faynberg, Igor. Gabuzda, Lawrence. Lu, Hui-Lan. "Converged Networks and Services: Internetworking IP and the PSTN". John Wiley & Sons. Julio 2000
9. Franz, David. "Evolution of networking. The principles for converged networks." IEEENetwork Magazine, pp 45-56. Agosto, 2000.
10. http://blogs.clarin.com/planetadigital/category/general/
11. http://eduangi.com/2007/03/09/resumen-de-bgp/
12. http://www.cert.uy/historico/pdf/Presentaci%C3%B3n%2002%20-%20MPLS-VPN.pdf
13. http://www.cisco.com/en/US/tech/tk436/tk428/tsd_technology_support_protocol_home.html
14. http://www.cisco.com/en/US/prod/collateral/routers/ps5763/CRS-1x100GE_DS.pdf