ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO Y DISEÑO DE UNA RED DE DATOS PARA UNA EMPRESA QUE PERMITA CALIDAD DE SERVICIO POR MEDIO DE LA TECNOLOGÍA METROETHERNET INTEGRADA A UNA RED MPLS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

FRANKLIN OSWALDO SIMBAÑA COLLAGUAZO
franklinosw@hotmail.com

DIRECTOR: ING. PABLO WILLIAM HIDALGO LASCANO
phidalgo@ieee.org

Quito, Junio 2015

DECLARACIÓN

Yo, Franklin Oswaldo Simbaña Collaguazo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Franklin Oswaldo Simbaña Collaguazo

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Franklin Oswaldo Simbaña Collaguazo, bajo mi supervisión.

Ing. Pablo Hidalgo
DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Considerando que la gratitud constituye uno de los más grandes valores humanos, me permito expresar mi agradecimiento a la Escuela Politécnica Nacional, en la persona de sus muy dignas autoridades.

De igual manera, manifiesto gratitud perenne hacia todos y cada uno de los destacados docentes que han participado en mi formación profesional en el excelso campo de la Ingeniería Electrónica y Redes de información; de manera especial agradezco al Ing. Pablo Hidalgo, quien con dilecta calidad de ser humano, vastísima capacidad académica y profundo conocimiento, supiera dirigir brillantemente el desarrollo de este Proyecto de Titulación.

A todos quienes me brindaron su contingente para crecer como persona y para formarme profesionalmente, expreso mi gratitud infinita.

Franklin Simbaña

DEDICATORIA

A Dios por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su inmenso amor.

Y a todos quienes creyeron en mí.

Franklin Simbaña

CONTENIDO

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

RESUMEN

Se define la situación actual de los servicios y tipos de datos para una empresa, y se analizan las soluciones de conectividad de múltiples oficinas en una área metropolitana.

Con esta información se diseña una red de datos e Internet acorde al estudio de las necesidades del cliente, mediante la utilización de la tecnología Metroethernet. Se compara técnica y financieramente la solución implementada en la empresa y la alternativa Metroethernet.

En el capítulo 1, se describe la tecnología Metroethernet, los tipos de servicio que provee y se especifican los atributos de servicio, parámetros de desempeño destacando la característica de manejo de calidad de servicio a nivel de *switches*. Se describe además, la calidad de servicio para priorizar el tráfico y se indican los métodos de acceso que se usan con una red de *backbone* y que convergen a una alternativa Metroethernet.

En el capítulo 2, se toma como referencia la solución actual de comunicaciones implementada por una red *legacy* y se consideran los puntos de vista de los requerimientos del cliente en cuanto al porcentaje de tráfico por enlace en la red, tiempos de respuesta, características de los enlaces, entre otros. Con esta información se procede al estudio y análisis de requerimientos con una proyección de crecimiento.

En el capítulo 3, con la información obtenida en el capítulo anterior, se procede a caracterizar la red, diseñar el tipo de interconexión más factible entre las diferentes agencias, tomando en cuenta factores de confiabilidad, tiempo de respuesta y factores técnicos. El análisis financiero contempla la rentabilidad desde el punto de vista del proveedor de servicio en el presente proyecto.

En el capítulo 4, se realiza un modelamiento de una red Metroethernet con equipos ME3400 para poner a prueba los protocolos de protección y realizar una comparación entre ellos.

En el capítulo 5, se establecen las conclusiones y recomendaciones del proyecto.

Los anexos contienen información técnica de los equipos de acceso de última milla, equipos de *internetworking*, de videoconferencia y Audiocodes, que se utilizaron en la solución del diseño de la red de la Entidad Financiera.

Además se incluye la configuración de los segmentos REP del modelamiento del capítulo 4.

PRESENTACIÓN

El presente proyecto tiene como finalidad demostrar las bondades de una red Metroethernet en cuanto a servicios de conectividad de mayor capacidad y velocidad, garantizando un mayor tráfico de información y desempeño con una tecnología diferente a las ya implementadas.

Se propone mediante el análisis y migración tecnológica de una empresa, medidas para robustecer la confiabilidad mediante una red de servicios de alta capacidad y disponibilidad.

Es de mucha importancia la realización del presente Proyecto de Titulación, pues trata de ser un referente para otros proyectos futuros a implementarse con las premisas de una red Metroethernet.

Una tecnología que cuente con el equipamiento que pueda ser actualizado y permita una mayor escalabilidad con un soporte técnico apropiado a las exigencias del mercado, contribuye a proveer soluciones de manera rápida y oportuna.

Por estas razones, el presente proyecto presenta el diseño de una red dentro de un área metropolitana enfatizando en la implementación de calidad de servicio, acompañado con un análisis financiero, comparado con soluciones tradicionales disponibles en el mercado.

Este proyecto está dirigido a diseñadores y administradores de red, proveedores de servicio y estudiantes que requieran profundizar sus conocimientos en los beneficios de la tecnología Metroethernet.

CAPÍTULO 1
TECNOLOGÍA METROETHERNET

1.1 INTRODUCCIÓN A LA TECNOLOGÍA METROETHERNET

Una MAN (*Metropolitan Area Network*) se define como una red de área metropolitana de alta velocidad que soporta diferentes protocolos de capa 2, proporcionando la integración de varios servicios mediante un sistema de transmisión entre los usuarios y el proveedor de servicios.

El protocolo Ethernet se usa como elemento principal, dentro de la tecnología Metroethernet para proporcionar la conectividad de aplicaciones de banda ancha que el cliente requiera.

1.1.1 ESTÁNDAR ETHERNET

Ethernet opera en las capas 1 y 2 englobando los siguientes componentes: características de capa física, protocolos de control de acceso a la red y el formato de trama.

Ethernet originalmente fue desarrollado para que varias computadoras se conecten al mismo medio físico. Para el control de acceso al medio se usa escucha de portadora con detección de colisiones CSMA/CD (*Carrier Sense Multiple Access with Collision Detection)* como protocolo MAC (*Media Access Control*).

El protocolo CSMA/CD permite a los dispositivos de la red enviar o recibir datos pero no simultáneamente; este modo de transmisión se conoce *como half-duplex.*

Cuando una colisión ocurre, ambos dispositivos dejan de transmitir y envían una señal *JAM* que indica a todos los otros dispositivos que se ha producido una colisión, y que no deberían transmitir datos por el medio. Ambos dispositivos esperan un tiempo aleatorio e intentan transmitir si el medio está libre.

Cuando un dispositivo necesita enviar datos, la NIC (*Network Interface Card*) los encapsula en una trama Ethernet

Con equipos de conmutación (*switches*) en una red y la conexión con cables de par trenzado, cada par de transmisión es un circuito independiente. Debido a que ambos lados de la conexión recibirán datos desde un solo dispositivo de red, los paquetes no se corrompen por múltiples estaciones que transmiten simultáneamente. De esta manera el *switch* permite una transmisión *full-duplex* y cada puerto es dedicado a un solo dispositivo; el ancho de banda no es compartido, tal como se indica en la figura 1.1.

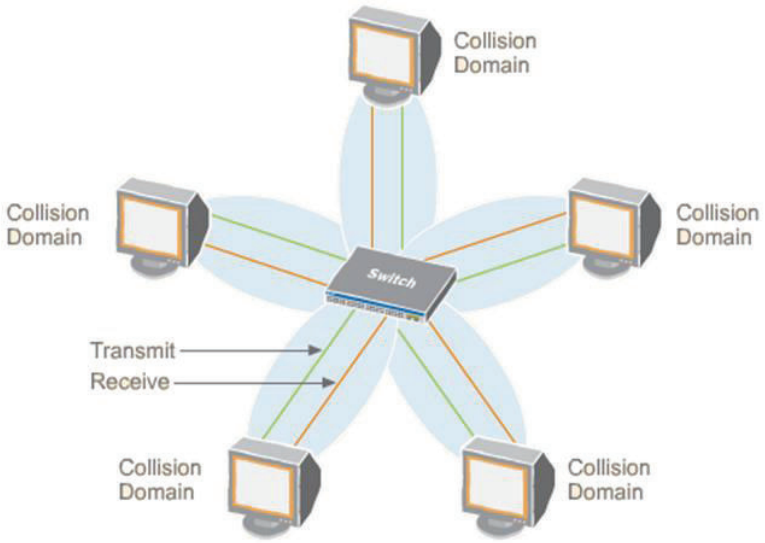


Figura 1.1 Dominios de colisión [1]

Ethernet por su simplicidad, costo y rendimiento frente a otras tecnologías ha sido el estándar dominante en la red global.

Se han definido varias implementaciones Ethernet con sus respectivas características que se detallan en la tabla 1.1.

ESTANDAR	NOMBRE	TIPO DE RED
10BASE2	Ethernet delgada (thin Ethernet)	Red tipo bus de 10 Mbps que utiliza cable coaxial RG-58 (50 Ohms), en segmentos de hasta 185 m.
10BASE5	Ethernet gruesa (thick coaxial)	Red tipo bus de 10 Mbps que utiliza cable coaxial RG-8, en segmentos de hasta 500 m.
FOIRL (Fiber Optic Inter-Repeater Link)	Enlace entre repetidores	Red punto a punto de 10 Mbps que utiliza cable de fibra óptica multimodo para conectar dos repetidores, hasta 1000 m de distancia.
10Broad 36	Ethernet de banda ancha	Red de banda ancha de 10 Mbps (actualmente reemplazado por sistema de fibra óptica), en segmentos de hasta 3600 m entre estaciones.
10BASE-T	Ethernet de pares trenzados	Red en estrella de 10 Mbps que utiliza dos pares de cableado UTP categoría 3 o superior. Distancia hasta los 100 m.
10Base-F: Término genérico para 3 tipos de red de 10 Mbps: 10Base-FB, 10Base-FP y 10Base-FL.		
10Base-FB	Red soporte Ethernet de fibra	Red de fibra óptica de 10 Mbps que utiliza concentradores activos de fibra para extender una red de backbone.
10Base-FP	Ethernet de fibra pasiva	Red de fibra óptica de 10 Mbps que utiliza concentradores de fibra pasivos para conectar estaciones de trabajo.
10Base-FL	Enlace de fibra Ethernet	Red de fibra óptica punto a punto de 10 Mbps; actualización del estándar FOIRL.
100Base-T: Término genérico para todas las opciones Fast Ethernet incluyendo cables UTP y de fibra óptica.		
100Base-X : Identifica a 100Base-TX y 100Base-FX. Los dos utilizan el mismo sistema de codificación 4B5B.		
100BASE-TX	Fast Ethernet	Red de 100 Mbps que utiliza dos pares de cobre de un cable UTP categoría 5 o superior. Distancia hasta los 100 m.
100BASE-FX	Fast Ethernet	Red de 100 Mbps que emplea cable de fibra óptica multimodo, se usa dos líneas de fibra óptica multimodo (MMF), una para recepción y la otra para transmisión. Soporta una distancia de 400 m para las conexiones half-duplex o 2000 m para full-duplex.
100BASE-T4	Fast Ethernet	Red de 100 Mbps que emplea los 4 pares de un cable UTP cat. 3 o superior. Usa la codificación 8B6T, hasta 100 m de distancia.
100Base-T2	Fast Ethernet	Red de 100 Mbps emplea los 2 pares de un cable UTP categoría 3 o superior. Usa la codificación PAM-5 (Pulse-amplitude modulation)
1000BASE-X (802.3z): Término genérico para los estándares Giga Ethernet que se basan en codificación 8B10B, incluyendo 1000 Base-SX, 1000 Base-LX y 1000 Base-CX.		

1000BASE-SX	Gigabit Ethernet	Red de 1000 Mbps que emplea cable de fibra óptica multimodo de pequeña longitud de onda (850 nm). Hasta 550 m.
1000BASE-LX	Gigabit Ethernet	Red de 1000 Mbps que emplea cables de fibra óptica monomodo o multimodo de gran longitud de onda (1350 nm). Distancia de hasta 10 Km en fibra monomodo y 3 Km en multimodo.
1000BASE-LH	Gigabit Ethernet	Red de 1000 Mbps de "larga distancia" que utiliza cable de fibra óptica monomodo. Fibra monomodo hasta 100 Km.
1000BASE-CX	Gigabit Ethernet	Red de 1000 Mbps que emplea 2 pares del cable de cobre STP como los del estándar de canal de fibra. Hasta 25 m de distancia.
1000BASE-ZX	Gigabit Ethernet	Red de 1000 Mbps que emplea cable de fibra óptica monomodo, hasta 100 Km de distancia.
1000BASE-EX	Gigabit Ethernet	Red de 1000 Mbps que emplea cable de fibra óptica monomodo, hasta 40 Km de distancia
1000BASE-T	Gigabit Ethernet	Red de 1000 Mbps que emplea cuatro de los pares de cobre de un cable UTP categoría 5, distancia máxima 100 m.

Tabla 1.1 Tecnologías Ethernet [2]

1.1.1.1 Trama Ethernet

La trama Ethernet que se ilustra en la figura 1.2 tiene los siguientes campos:

Figura 1.2 Trama Ethernet [3]

Dirección destino (6 bytes), es la dirección MAC del dispositivo que recibirá la trama.

Dirección de origen (6 bytes), es la dirección MAC del dispositivo que está enviando la trama.

El campo de Tipo (2 bytes), identifica el protocolo de capa 3 que está siendo transportado en la trama Ethernet. Tipos de protocolo incluyen por ejemplo: IP, AppleTalk (IPX).

El campo Datos (46 – 1500 bytes), contiene los datos originales creados por una aplicación.

El campo de Checksum (4 bytes), incluye una comprobación de redundancia cíclica (CRC) que es un método para detectar errores en los datos que han sido transmitidos en un enlace de comunicación.

1.1.1.2 IEEE 802.3

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) creó un comité para estandarizar las tecnologías de red; se designó al comité como 802 que corresponde al año y mes que fue formado. Uno de los estándares creados por este comité es el 802.3 que es el equivalente al estándar Ethernet.

1.1.1.2.1 Trama IEEE 802.3

Entre la tecnología Ethernet y el estándar IEEE 802.3 una de las diferencias está en los formatos de sus tramas, como se indica en la figura 1.3, en la que se observa que el campo Tipo de Ethernet es redefinido con el campo Longitud de trama en IEEE 802.3 manteniendo su tamaño en 2 bytes.

El Preámbulo, permite la sincronización de la trama, en el protocolo Ethernet tiene una longitud de 8 bytes pero en IEEE 802.3 la longitud es de 7 bytes y el octavo byte es el delimitador de inicio de trama.

Ambos tipos de tramas están definidos y soportados dentro del estándar IEEE 802.3 y pueden coexistir en la misma red.

1.1.2 LAN VIRTUAL (VLAN)

En la figura 1.4, se ilustra una LAN virtual (VLAN) que define una conexión lógica de varios *hosts* sin tener en cuenta su localización física, como si estuvieran en un mismo dominio de *broadcast* y que está conformada por un conjunto de dispositivos de red interconectados (*bridges, switches* o estaciones de trabajo).

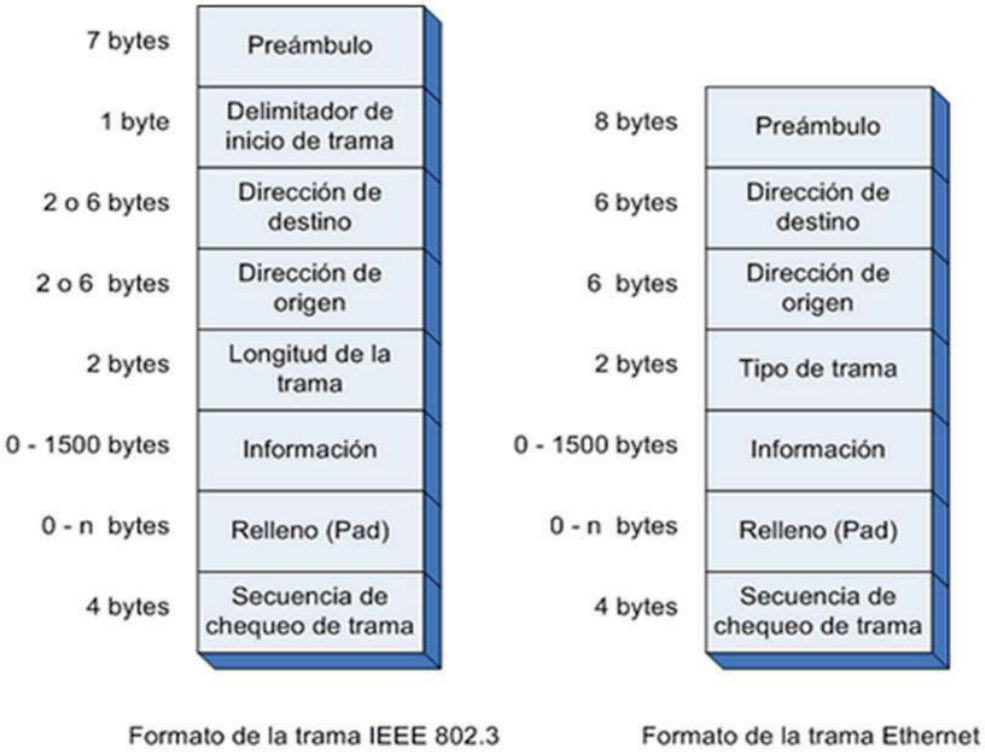


Figura 1.3 Diferencia entre la trama Ethernet y la trama IEEE 802.3 [4]

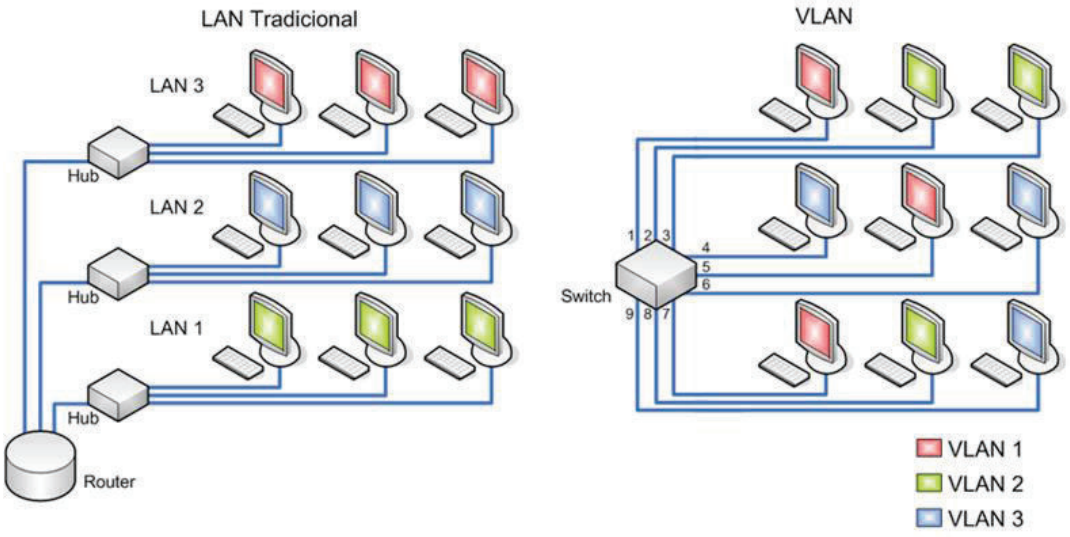


Figura 1.4 LAN Virtual VLAN [5]

El tamaño de trama varía desde 64 a 1518 Bytes, excepto cuando se usa el identificador de VLAN (*tag*), normado por el protocolo IEEE 802.1Q que es un mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (*Trunking*).

Otro método para indicar la información de la VLAN en una trama Ethernet mediante una encapsulación externa es ISL (*Inter-switch Link*).

ISL trabaja a nivel 2, encapsulando con un nuevo *header*; es propietario de Cisco y sirve únicamente para *FastEthernet* y *GigabitEthernet*.

El protocolo 802.1Q añade 4 bytes al encabezado Ethernet original como se observa en la figura 1.5, forzando a un recálculo en el campo FCS *(Frame Check Sequence)*. El valor del campo *EtherType* se cambia a 0x8100 para señalar el cambio en el formato de la trama.

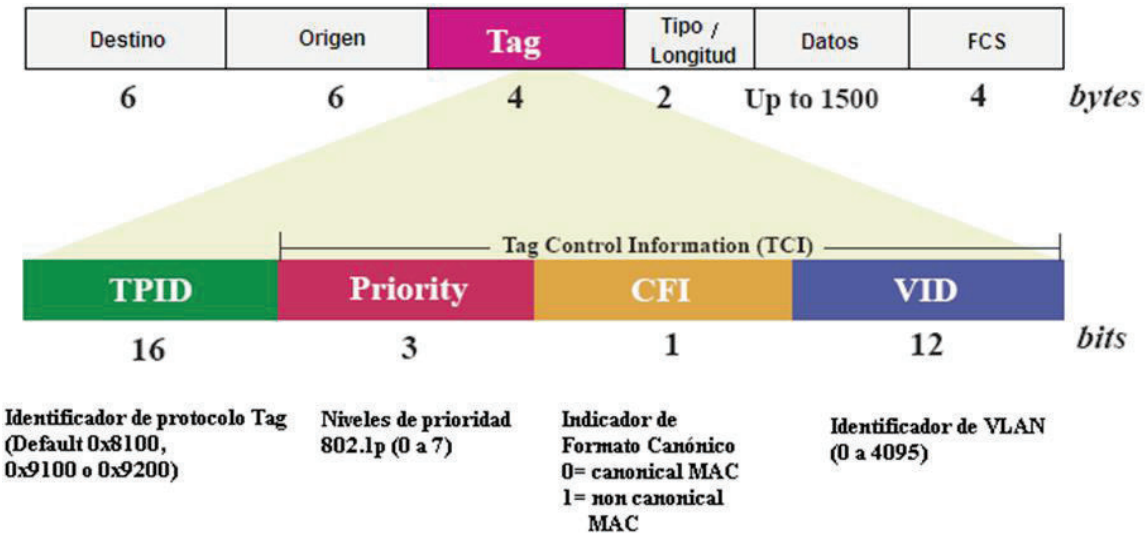


Figura 1.5 Trama Ethernet com 802.1Q [6]

Identificador de Protocolo de Etiqueta (TPID): Campo de 16 bits con un valor de 0x8100 a fin de distinguir las tramas etiquetadas de las sin etiquetar.

Prioridad de Usuario: Define la prioridad de usuario, dando ocho niveles de prioridad. IEEE 802.1P define la operación para estos 3 bits de prioridad de usuario.

Indicador de Formato Canónico (CFI): Siempre es puesto a cero para *switches* Ethernet. CFI se usa por motivos de compatibilidad entre redes de tipo Ethernet y redes de tipo *Token Ring*. Si una trama es recibida en un puerto Ethernet y tiene el CFI en 1, entonces esa trama no debería pasar a un puerto no etiquetado (*untagged*).

VLAN ID es la identificación de la VLAN, tiene 12 bits y permite la identificación de 4096 VLANs. De 4096 VLAN ID posibles, VID= 0 se usa para identificar tramas con prioridad y el VID=4095 es reservado, por lo que las configuraciones VLAN posibles máximas son 4094.

1.1.2.1 Tipos de VLANs

Se han definido los siguientes tipos de VLANs:

1.1.2.1.1 VLAN de puerto central

Es aquella en la que todos los nodos de una VLAN se conectan al mismo puerto del *switch*.

1.1.2.1.2 VLAN Estáticas

Los puertos del *switch* están ya preasignados a las estaciones de trabajo y se lo realiza de manera manual. Para asignarlos se puede realizar de la siguiente forma:

- Por puerto: Se configura los puertos del *switch* indicando qué puertos pertenecen a cada VLAN.
- Por dirección MAC: Los miembros de la VLAN se especifican en una tabla por su dirección MAC.
- Por protocolo: Se asigna a un protocolo una VLAN. El *switch* dependiendo del protocolo asociado a la trama lo derivará a la VLAN respectiva.

- Por direcciones IP: Está basado en el encabezado de la capa 3 del modelo OSI. No actúa como *router* sino para hacer un mapeo de qué direcciones IP están autorizadas a entrar en una VLAN.
- Por nombre de usuario: Se basan en la autenticación del usuario, no por las direcciones MAC de los dispositivos.

1.1.2.1.3 VLAN Dinámicas

Son puertos del *switch* que automáticamente determinan a qué VLAN pertenece cada puesto de trabajo. El funcionamiento de estas VLANs se basa en las direcciones MAC, direcciones lógicas o protocolos utilizados.

Cuando un puesto de trabajo pide autorización para conectarse a la VLAN, el *switch* verifica la dirección MAC ingresada previamente por el administrador en la base de datos de las mismas en un servidor VMPS (*VLAN Management Policy Server*) y automáticamente se configura el puerto al cual corresponde. Con este proceso se tiene una mejor administración que con las VLAN estáticas.

En una red de *switches* existen dos tipos de *puertos, de acceso y trunking*.

- Por medio de puertos de acceso *(Access ports*), donde el tráfico solo pertenece a una VLAN. En este proceso los *switches* eliminan toda la información VLAN antes de realizar un reenvío de la trama, por lo tanto los dispositivos conectados no conocen la topología de la red. Además se puede añadir una segunda VLAN, permitiendo también tráfico de voz para poder conectar un teléfono (*voice access ports*).
- Mientras que en los puertos *trunk* se tienen *links* que transportan el tráfico de varias VLANs.

Cada *switch* identifica la VLAN del *frame tag*, para saber dónde encaminarlo. Si hay un *access port* de esa VLAN, eliminará el tag y lo destinará allí. En caso de que tenga un *trunk* a otro *switch*, el *frame* lo propagará de nuevo a otro *switch*. Los puertos *trunk* soportan tráfico con o sin *tag*.

1.1.2.2 Ventajas de una VLAN

Las ventajas de una VLAN son:

- Mayor seguridad mediante el aislamiento del tráfico dentro de las estaciones de trabajo que son miembros de la VLAN.
- Al limitar el dominio de *broadcast* a la VLAN se conservan recursos de ancho de banda.
- Mayor facilidad de administración para las migraciones de estaciones de trabajo y los cambios de topología de la red, teniendo independencia geográfica.

1.1.3 RED METROETHERNET

1.1.3.1 Introducción

El marco teórico hace referencia al artículo *Metro Ethernet Services –A Technical Overview* dado por la Metro Ethernet Forum (MEF) [7]

Una red Metro Ethernet es una red destinada a proveer servicios de conectividad MAN/WAN de nivel 2 a través de interfaces de red Ethernet**.**

1.1.3.2 Elementos de una red Metroethernet

Se definen los siguientes elementos en los servicios de una red Metroethernet:

1.1.3.2.1 Interfaz usuario-red (UNI - User to Network Interface)

Cumple el estándar IEEE 802.3, maneja velocidades de hasta 10 Gbps y soporta clases de servicio (*QoS*).

1.1.3.2.2 Equipo Terminal (CE - Customer Equipment)

Se conecta a través de *UNIs*, puede ser un *router* o *switch* con características IEEE802.1 Q.

1.1.3.2.3 Red Metro Ethernet (MEN - Metro Ethernet Network)

Puede usar distintas tecnologías de transporte por ejemplo *SONET/SDH, WDM, PON, RPR, MPLS*[1] entre otras.

1.1.3.2.4 Conexión Virtual Ethernet (EVC - Ethernet Virtual Connection)

Es una asociación entre dos o más *UNIs*, creada por el proveedor de servicio para un cliente. La trama en un EVC puede ser enviada a uno o más UNIs del EVC.

1.1.3.3 Servicios Ethernet

1.1.3.3.1 Servicio Ethernet Line (E-LINE)

En la figura 1.6, se puede observar un servicio *E-LINE*, el cual provee una conexión virtual Ethernet de tipo punto a punto. Este esquema se puede encontrar en servicios como *ADI, LAN to LAN* y *Private IP*

1.1.3.3.2 Servicio Ethernet Private Line (EPL)

Se denomina servicio *EPL* a un servicio EVC punto a punto con un ancho de banda dedicado, donde el cliente siempre dispondrá del CIR (*Commited Information Rate*); se implementa normalmente en canales SDH (*Synchronous Digital Hierarchy*) o en redes MPLS. Es como una línea en TDM (*Time Division Multiplexing*), pero con una interfaz Ethernet.

1.1.3.3.3 Servicio Ethernet Virtual Private Line (EVPL)

Si se trata de un servicio EVC punto a punto con un ancho de banda compartido se denomina un servicio *EVPL*, en este caso hay un CIR, un EIR *(Excess Information Rate)* y una métrica para el soporte de SLA´s (*Service - Level Agreement*). Se suele implementar con redes de conmutación de paquetes usando *switches* o *routers*.

1.1.3.3.4 Servicio Ethernet LAN (E-LAN)

En la figura 1.7, se tiene un servicio *E-LAN* el cual provee una conexión virtual Ethernet de tipo multipunto a multipunto. Se pueden tener servicios *LAN to LAN* y *Private IP* en modo E-LAN.

[1] El significado de las siglas se encuentran referidas en los Acrónimos

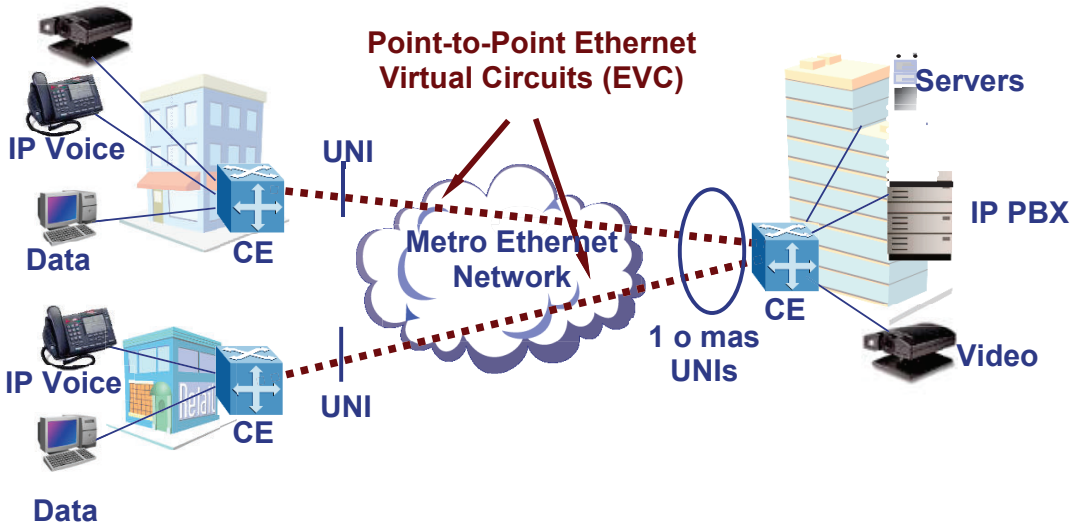


Figura 1.6 Servicio E-LINE [8]

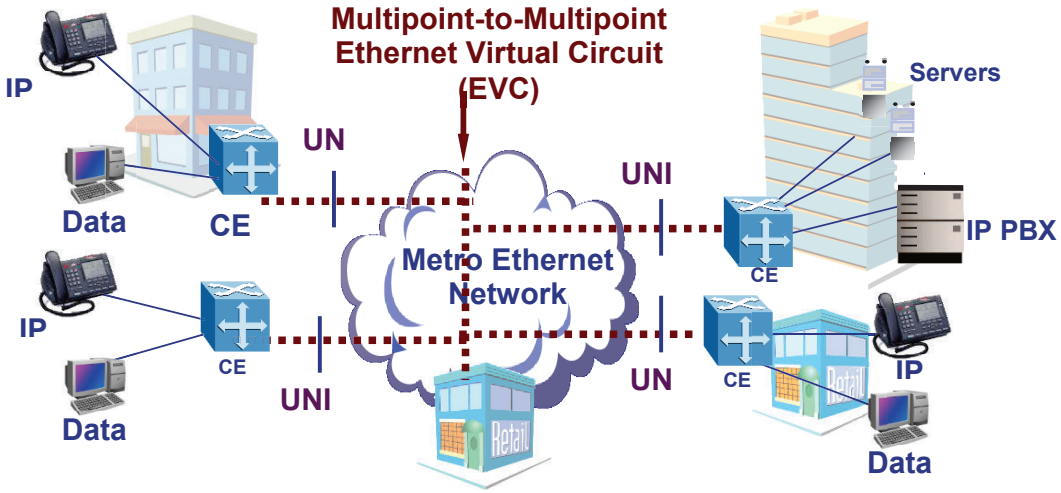


Figura 1.7 Servicio E-LAN [8]

1.1.3.3.5 Ethernet Private LAN (EPLAN)

El servicio *EPLAN* suministra una conectividad multipunto entre dos o más UNI´s, con un ancho de banda dedicado.

1.1.3.3.6 Ethernet Virtual Private LAN (EVPLAN)

Si la EPLAN opera con un ancho de banda compartido se denomina *EVPLAN.*

1.1.3.4 Atributos de servicio

Los atributos del servicio pueden ser definidos bajo las siguientes características:

1.1.3.4.1 Interfaz Física Ethernet

En los atributos de la interfaz física Ethernet se consideran los siguientes parámetros:

- Medio Físico: Está definido por el estándar IEEE 802.3 por ejemplo 10BASE-T, 100BASE-T, 1000 BASE-X, etc.

- Velocidad: Definido por las velocidades Ethernet: 10 Mbps, 100 Mbps, 1 Gbps o 10 Gbps.

- Negociación: Indica el modo de negociación para *full duplex* o *half duplex* o *auto speed* entre los puertos Ethernet.

- La capa MAC especificada en el estándar 802.3.

1.1.3.4.2 Parámetros de Tráfico

La *MEF* ha definido perfiles de ancho de banda que pueden ser aplicados en la UNI o en un EVC. Los atributos de servicio de perfil de ancho de banda son los siguientes: [9]

- Perfil de ingreso y egreso de ancho de banda por UNI.
- Perfil de ingreso y egreso de ancho de banda por EVC.
- Perfil de ingreso y egreso de ancho de banda por identificador de CoS.
- Perfil de ingreso de ancho de banda por destino UNI por EVC.
- Perfil de egreso de ancho de banda por destino UNI por EVC.

1.1.3.4.3 Perfiles de Ancho de Banda

La limitación en el ancho de banda, se lo realiza en función de la velocidad de subida y la de bajada en modo simétrico o asimétrico.

1.1.3.4.4 Parámetros de Desempeño

Entre los parámetros de desempeño se tienen la disponibilidad, el retardo de tramas, el *jitter* y la pérdida de paquetes.

1.1.3.4.5 Entrega de Tramas

La entrega de tramas se lo realiza de manera *unicast*, *multicast* o *broadcast*, dependiendo del destino.

1.2 MULTIPLEXACIÓN ESTADÍSTICA DE SERVICIOS [10],[11]

Básicamente un multiplexor es un *switch* que permite compartir un único canal de salida entre múltiples canales de entrada (multiplexado) y hace que una entrada sea distribuida por múltiples salidas (demultiplexado).

En la multiplexación por división de tiempo (TDM) la velocidad de transmisión del medio es por lo menos igual a la suma de las velocidades de las señales de datos a transmitir.

Las señales de cada fuente se almacenan temporalmente en *buffers* de entrada y éstos son muestreados secuencialmente para formar un tren de señales digitales.

Los sistemas TDM emplean una de las siguientes técnicas:

Técnica de intercalado de bit: Donde cada *time slot* tiene un bit que resulta de intercalar los bits de cada uno de los canales de entrada en forma secuencial; adicionalmente se tiene un canal para la señal de reloj que usa el receptor para la sincronización.

Técnica de intercalado de caracteres: cuando se envían de forma secuencial octetos alternadamente.

“Si los canales de entrada son todos síncronos, el ancho de banda total será la suma de todos los canales excepto el ancho de banda del canal de sincronización.

Sin embargo si los canales son asíncronos, el ancho de banda agregado puede ser mayor si el tamaño del octeto agregado es menor que el tamaño del carácter asíncrono (bits de arranque + datos + bit de *stop*). La razón es porque los bits de arranque y de *stop* de cada octeto son sustituidos antes de la transmisión, por lo que el receptor los debe restituir." [10]

En la multiplexación estadística (*STDM Statistical Time Division Multiplexing*) se asignan dinámicamente los *time slots* a las fuentes de entrada en función de la demanda, de esta manera no se envían *time slots* vacíos a diferencia de TDM donde, si un canal no tiene información se desperdicia su ancho de banda. Esta diferencia se ilustra en la figura 1.8.

La multiplexación estadística es ideal para redes donde las fuentes generan tráfico discontinuo y aplicaciones sensibles al retardo.

Los multiplexores estadísticos son equipos más complejos que los TDM puesto que tiene múltiples configuraciones de gestión, políticas de prioridad a las entradas, compresión de datos entre otras.

1.2.1 INTERACCIÓN METROETHERNET Y MPLS

La multiplexación estadística ha dado las premisas para el desarrollo de aplicaciones en tiempo real. Las redes Metroethernet como redes de acceso se integran a una nube de transporte MPLS, en el *backbone* principalmente, para tener una mayor administración del tráfico como se ilustra en la figura 1.9.

Las implementaciones basadas en MPLS son costosas pero altamente fiables y escalables.

1.3 APLICACIONES METROETHERNET

La red Metroethernet soporta varios tipos de aplicaciones, como puede ser Telefonía IP y Video IP. Estas aplicaciones generan un tipo de tráfico que es especialmente sensible al retardo.

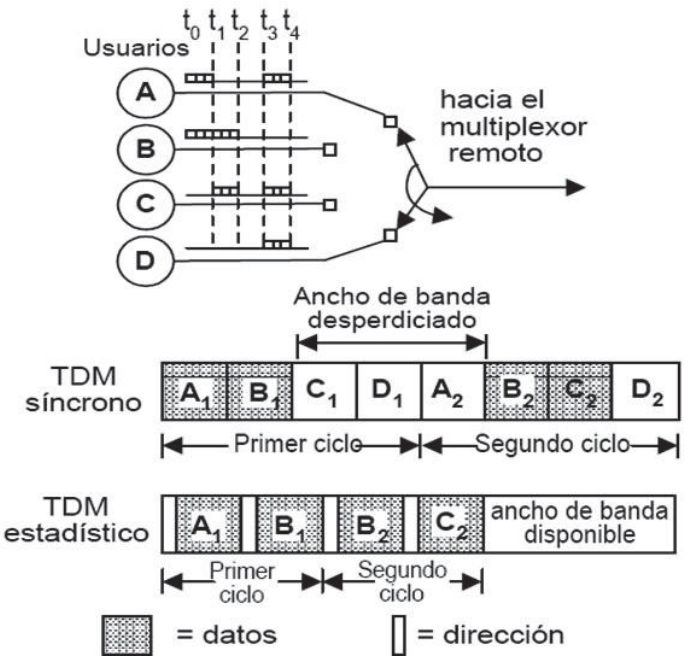


Figura 1.8 TDM síncrono contrastado con el TDM estadístico [11]

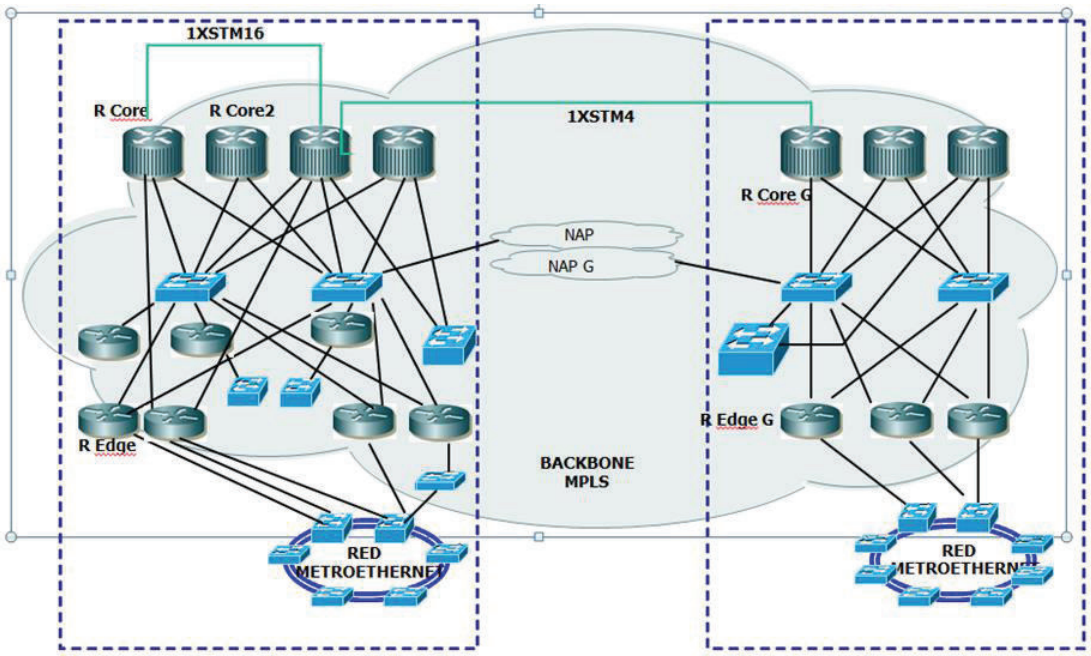


Figura 1.9 Redes Metroethernet y MPLS

1.3.1 CONEXIONES ADI

El sistema Metroethernet se puede usar para establecer conexiones dedicadas (ADI) con el proveedor de servicio de Internet (ISP), para dar soluciones

adaptables a las necesidades del usuario por medio de conexiones virtuales Ethernet, generalmente por medio de circuitos *Ethernet Line*.

1.3.2 INTRANET / EXTRANET

La interconexión punto a punto con enlaces dedicados y robustos se puede establecer entre la Intranet o Extranet empresarial a sitios remotos por medio de una red Metroethernet, haciendo factible el trabajo y gestión remota del cliente.

1.3.3 EXTENSIÓN LAN

En la operación de una empresa, se requiere la gestión y administración en conjunto de todas las sedes como si se tratara de una sola red LAN (Extensión LAN); para ello se pueden configurar circuitos Ethernet Line o Ethernet LAN**.**

1.3.4 SERVICIO DE RED PRIVADA IP

Establecer servicios *Private IP* también es posible dentro de una estructura Metroethernet, además de la interacción con tecnologías propias implementadas en el cliente, dando de esta manera soluciones seguras y personalizadas.

1.4 VENTAJAS DEL USO DE LA RED METROETHERNET

Se describen a continuación algunas de las ventajas que presenta una red Metroethernet con respecto a otras soluciones WAN.

1.4.1 COSTOS COMPETITIVOS

Los avances en electrónica de conmutación y una producción masiva han conllevado a costos considerablemente menores de los equipos en una infraestructura Ethernet con respecto a tecnologías *Frame Relay o ATM,* posibilitando ampliar los servicios en redes metropolitanas.

1.4.2 FLEXIBILIDAD DE CONVERGENCIA

La flexibilidad de un sistema en converger a las necesidades del cliente han sido los inconvenientes que han presentado los sistemas *Legacy y ATM*. Mientras que los servicios de acceso Ethernet ofrecen un amplio rango de velocidades de conexión.

1.4.3 SIMPLIFICACIÓN DE LOS DISEÑOS DE RED

Ethernet es una tecnología basada en tramas asincrónicas que tiene ventajas particulares de flexibilidad sobre tecnologías basadas en celdas o competidores síncronos. Al disponer de funciones que delimitan a una tasa adecuada para manejar los recursos disponibles y con suficiente capacidad en las troncales, Ethernet puede proveer rápidamente ancho de banda bajo demanda.

1.4.4 FACILIDAD DE INTERCONEXIÓN

Con Ethernet se simplifica considerablemente tanto el diseño de red como los costos indirectos de administración, posibilitando la migración de bajas a altas velocidades. Consecuentemente, es relativamente simple integrar e interconectar sistemas de tecnología de la información del cliente final a los servicios Metroethernet.

1.5 LIMITACIONES Y POSIBLES SOLUCIONES EN LA RED METROETHERNET

1.5.1 GARANTIZAR EL RENDIMIENTO PUNTO A PUNTO

Cualquier elemento intermedio afecta a la percepción del cliente, por lo cual Ethernet necesita mecanismos para:

- Administrar la conexión de nuevos requerimientos de servicio sin afectar el rendimiento de servicios establecidos.

- Planificar y monitorear para mantener accesos con anchos de banda que garanticen las demandas en momentos de congestión.
- Garantizar el establecimiento de rutas óptimas para evitar pérdidas, y retrasos.
- Ser capaz de establecer prioridades.

Debido a ello un modo de proporcionar un funcionamiento de servicio aceptable es por medio del sobre aprovisionamiento de un servicio *best-effort.* Sin embargo no es una solución viable económicamente a largo plazo.

MPLS tiene el potencial para ser una solución a largo plazo por las siguientes razones:

- Proporciona la capacidad de Ingeniería de Tráfico.
- Proporciona anchos de banda garantizados.
- Tiene inherente la capacidad de etiquetar paquetes estableciendo prioridades.
- Se aplica perfectamente en la tecnología Ethernet.

1.5.2 ESTABLECIMIENTO DE MECANISMOS DE PROTECCIÓN

Ethernet proporciona una lenta recuperación de errores, pues se maneja mediante algoritmos que pueden tomar varios segundos para converger dependiendo del tamaño de la red, lo cual resulta en un tiempo demasiado largo para aplicaciones críticas de voz y video. Además Ethernet no permite incorporar señales como LOS (*loss of signal),* las mismas que permiten la ubicación de fallas ante un mal funcionamiento.

Los distintos grados de protección se justifican en función del servicio del cliente y en los términos del SLA, por lo cual algunas opciones de tecnología están siendo implementadas con los siguientes estándares:

- *IEEE 802.1s (Multiple Spanning Trees)* es una propuesta que permite más de un *loop-free path* en un ambiente VLAN, dando el beneficio de protección de un *path* redundante.

- *IEEE 802.1w (Rapid Reconfiguration Spanning Tree)* pone en práctica un algoritmo de convergencia más rápida, tomando aproximadamente un segundo para converger. Sin embargo, esto todavía no se acerca a los 50 ms de SONET (*Synchronous Optical Network*).

- *IEEE 802.3ad (Link Aggregation)* es un método para combinar varios *links* físicos en un solo *link* lógico para tener un mayor ancho de banda.

- The IEEE 802.17 (*Resilient Packet Ring*) este grupo de trabajo respalda un protocolo de protección tipo anillo que proporciona restablecimientos en 50 ms.

- *MPLS* ofrece soluciones flexibles y escalables a través de funciones tales como *backup LSP (Label Switched Path)*, reenrutamientos rápidos y niveles de prioridad. Esta flexibilidad permite al proveedor vender diferentes niveles de protección a diferentes precios.

1.5.3 SERVICIOS DE OPERACIÓN, ADMINISTRACIÓN Y MANTENIMIENTO (*OAM*)

Ethernet no tiene en el *overhead* capacidad para monitorear como lo hace el byte de paridad conocido como BIP-8 (*bit interleaved parity),* los cuales monitorean y detectan errores sobre diferentes partes de la trama SONET. Tal capacidad es en particular útil en puntos de demarcación de servicio, donde esto se utiliza para pruebas de accesibilidad.

En la actualidad, este aspecto se está abordando en los diferentes organismos de normalización incluyendo IEEE, el MEF y el UIT-T Q3/13.

IEEE 802.3ah EFM (*Ethernet in the First Mile*) aborda temas necesarios para el despliegue masivo de servicios de Ethernet, tales como operación, administración y gestión (OA & M) y la compatibilidad con tecnologías existentes.

1.5.4 LA ESCALABILIDAD Y LA UTILIZACIÓN DE LOS RECURSOS DE LA RED

Una de las ventajas que tiene Ethernet es la habilidad para realizar particiones lógicas en grupos de usuarios sobre la misma red física, usando el concepto de VLAN. El escalamiento VLAN en la Metro, se realiza con las siguientes alternativas:

1.5.4.1 Limitación de etiquetas (*tag* VLAN)

El estándar IEEE 801.Q define un espacio de direcciones de solo 4.096 etiquetas disponibles. Esto es insuficiente para un servicio de un gran proveedor.

Por esta razón ciertos fabricantes de equipos de red actualmente suministran al equipo, el aumento de espacio de etiqueta disponible VLAN por varios esquemas propietarios (*tag-stacking*), aunque se introduce consideraciones en la complejidad e interoperabilidad.

1.5.4.2 El protocolo STP (*Spanning Tree Protocol)*

El protocolo *Spanning Tree* permite garantizar que la topología esté libre de bucles. Esto implica una distribución de la carga desigual y potenciales “cuellos de botella”. Por eso *MSTP* (*Multiple Spanning Trees Protocol)* está bajo la consideración del grupo de trabajo IEEE 802.1s como tentativa de corregir esta deficiencia.

Dadas las limitaciones en la implementación de S*panning Tree*, varias técnicas MPLS se proyectan dentro del IETF como las soluciones escalables a largo plazo que maximizan la utilización de los recursos de red.

1.5.4.3 El protocolo EAPS (*Ethernet Automatic Protection Switching*)

Otro protocolo de protección es el de conmutación de protección automática Ethernet (EAPS), que se utiliza para crear una topología con tolerancia a fallos mediante la configuración de una ruta primaria y secundaria para cada VLAN. Un

anillo se forma mediante la configuración de un dominio. Cada dominio tiene un único nodo maestro y muchos nodos de tránsito.

Cada nodo tiene un puerto primario y un puerto secundario, ambos conocidos por ser capaces de enviar tráfico de control para el nodo maestro. En el funcionamiento normal solo el puerto primario en el nodo maestro se utiliza para evitar *loops*, el puerto secundario está bloqueado para todo tráfico. Cuando hay una caída del enlace, los dispositivos que detectan la falla envían un mensaje de control al nodo maestro, para desbloquear el puerto secundario e indicar que los nodos de tránsito limpien sus bases de datos. [12]

1.5.4.4 El protocolo REP *(Resilient Ethernet Protocol)*

El protocolo REP es un protocolo propietario de *Cisco* que ofrece una alternativa a STP para controlar los *loops* en la red.

REP habla de segmentos, no habla de anillos, el segmento REP va a uno o dos *switches* que controlen el segmento por medio de los puertos extremos llamados puertos de borde o *Edge Ports*; cada segmento REP se identifica con un ID.

Los segmentos REP no van a tener conectividad entre los puertos de borde de un segmento, y para no tener continuidad algún puerto intermedio del segmento se lo debe bloquear. En este caso en el segmento existirá un puerto en estado *blocking* denominado Puerto Alterno (*Alternate Port*), como se indican en las figuras 1.10 y 1.11.

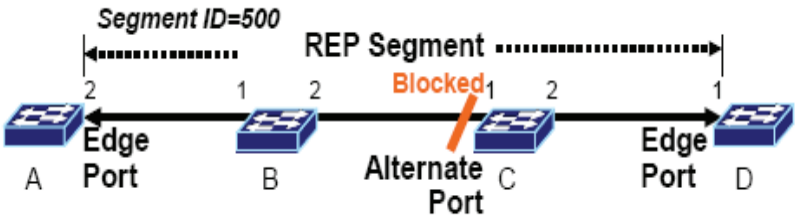


Figura 1.10 Segmento REP [13]

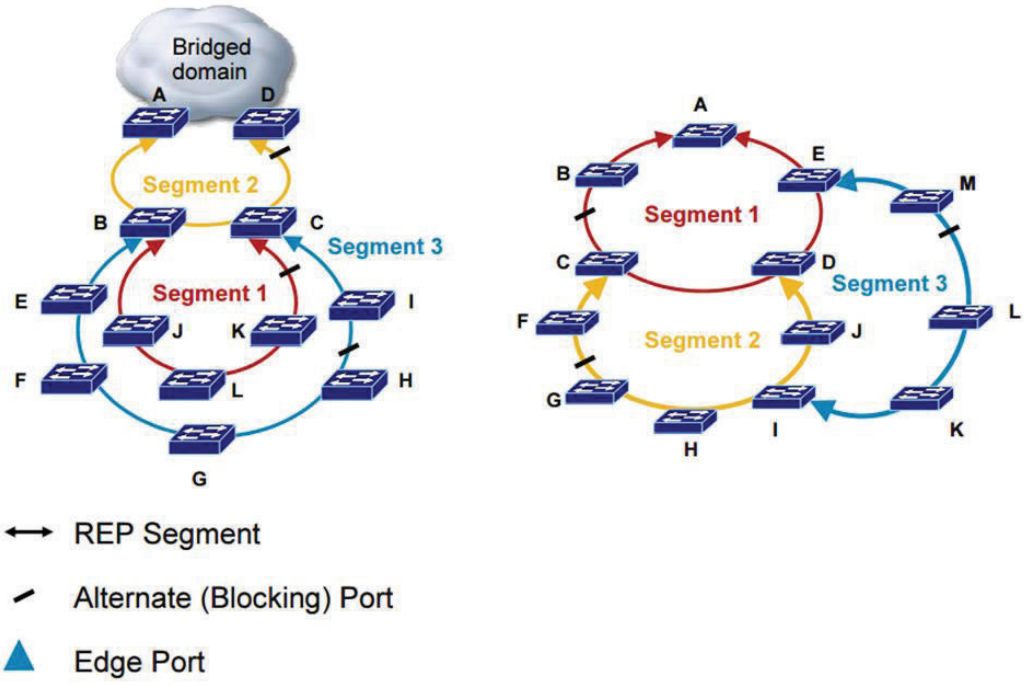


Figura 1.11 Topología REP [13]

La figura 1.12 indica los parámetros de configuración del "anillo" REP.

Donde el puerto Edge Primario se define con el comando ***rep segment 1 edge primary***; y el final del segmento REP con el comando ***rep segment 1 edge.***

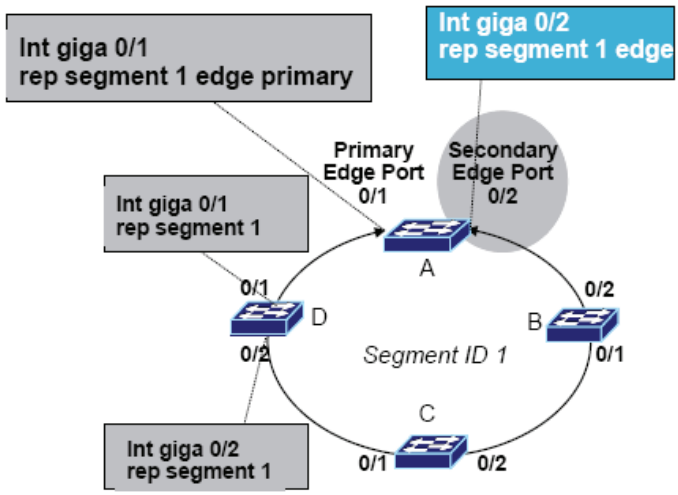


Figura 1.12 Configuración de los puertos de borde

REP puede coexistir con STP o con *switches* que no soportan REP; por medio de configuraciones en los puertos de los equipos de borde se puede detectar cualquier cambio de topología, como se indica en la figura 1.13.

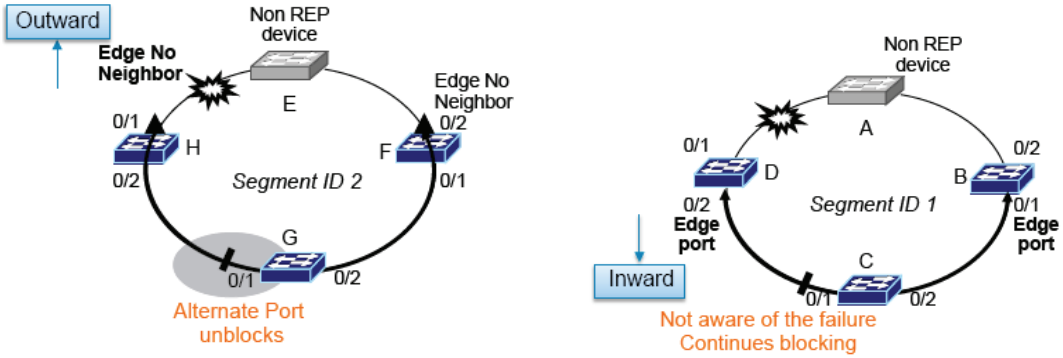


Figura 1.13 Opciones de configuración de los puertos *Edge*

A diferencia de STP que analiza todos los BPDUs (*Bridge Protocol Data Units*) de la red preocupándose de toda la topología de la red, con REP cada segmento se encarga de garantizar que no exista continuidad, de esta manera se tiene una topología en bus o en estrella. En el establecimiento de vecindades entre *switches* se pueden dar cuenta entre ellos si existe una caída en el intercambio de señales de control, esto indica un cambio de topología y los puertos de borde ordenan al puerto que estaba en estado a*lternate* que deje de bloquear el tráfico pasando a estado *Open.*

En la figura 1.14 se indica el diagrama para establecer el puerto alterno. El puerto alterno dentro del segmento REP se puede especificar usando uno de los tres métodos siguientes:

1. Conociendo el número del puerto del switch vecino que será alterno y configurándo en el *switch port* de borde primario. Para establecer el número de puerto se puede seguir una secuencia horario o antihoraria.

switch A (conf)# int giga 0/1
rep block port 4 vlan all

2. Configurando en el *switch* que será alterno, el comando "*preferred*", y luego configurando el puerto *preferred* en el *switch* de borde primario.

switch C (conf)# interface giga0/2
rep segment 1 preferred
switch A (conf)# int giga0/1
rep block port preferred vlan all

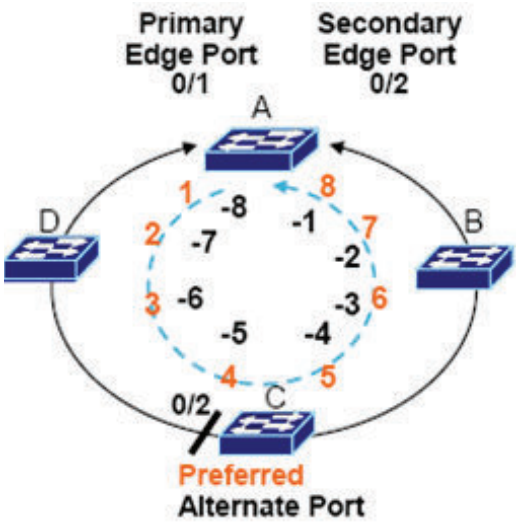


Figura 1.14 Establecimiento del puerto alterno

Las notificaciones de cambio de topología no requieren recursos de CPU, sino que están manejados por *hadware* directamente usando direcciones *multicast*; de esta manera se tiene más robustez en el equipo.

REP tiene un tiempo de conmutación entre 50 y 80 ms; en el caso de “flapeos”, el puerto en el que se produjo el flapeo se queda bloqueado y no vuelve a ser puerto alterno a menos que se especifique un tiempo de *preemtion* para que vuelva a sus condiciones originales; se ha especificado que el tiempo de *preemtion* sea 45 segundos luego de que el puerto esté estable.

Se puede hacer balanceo de carga especificando las VLANs que se bloquearán en los diferentes puertos de los *switches*, procedimiento que se lo puede hacer en MSTP (*Multiple Spanning Tree Protocol*) o en VLAN *Spanning Tree*.

Es un protocolo con alta escalabilidad, pero no protege ante fallas de múltiples anillos.

1.6 DEFINICIÓN DE CLASES DE SERVICIO (COS)

Con las clases de servicio, se selecciona la prioridad que recibe cada aplicación. En una red Metro Ethernet los parámetros de clase de servicio (*CoS*) pueden ser definidos en varios identificadores de *CoS*, como por ejemplo:

1.6.1 PUERTO FÍSICO

La calidad de servicio se aplica al puerto físico de la conexión UNI. Todo el tráfico que entra y sale del puerto recibe la misma calidad de servicio QoS. Si el usuario requiere varias clases de servicio, se separa cada una por puertos físicos.

1.6.2 DIRECCIONES MAC DE ORIGEN Y DESTINO

Este modelo es muy flexible, pero es difícil de administrar. Si el equipo terminal CPE es de capa 2 y es parte del servicio *LAN to LAN*, se deberían monitorear muchas direcciones MAC.

Por otra parte, si los *CPEs* son *routers*, la dirección MAC es monitoreada por las interfaces de los mismos *routers*.

1.6.3 IDENTIFICACIÓN DE VLAN

Permite adjudicar clases de servicio (*CoS*) si el usuario tiene diferentes servicios por un puerto físico donde cada servicio es definido por una identificación VLAN.

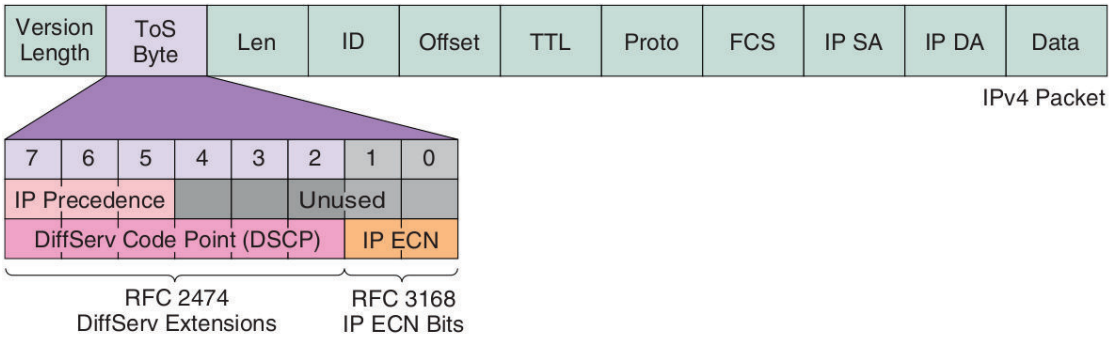
1.6.4 VALOR 802.1P

Permite al proveedor de servicio adjudicar al tráfico del cliente hasta ocho diferentes niveles de prioridades. Este es un método que puede ser usado para distinguir entre tráfico de voz sobre IP *(VoIP)* y tráfico regular o entre el tráfico prioritario y *best effort*.

1.6.5 DIFFSERV/IP TOS

El campo *IP ToS* es un espacio de 3 bits dentro del paquete IP que se usa para proporcionar ocho clases diferentes de servicio conocidas como *IP precedence*. Este campo es similar al campo 802.1p usado para prioridades básicas; sin embargo, se encuentra localizado dentro del *header* IP.

Diffserv ha definido un esquema de *CoS* más sofisticado que el simple esquema de prioridad definido por *ToS*. En la figura. 1.15 se tiene el aspecto del octeto TOS. *Diffserv* tiene en cuenta 64 valores de *CoS* diferentes, llamados puntos de código de *Diffserv* (DSCPs).



Campo DiffServ

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN

- Bits de DSCP-six (DS5-DS0)
- Bits de ECN-two

Figura 1.15 Octeto TOS (DSCP e IP ECN) [14]

Los dos últimos bits (IP ECN *ExplicitCongestion Notification*) se usan para indicar a los remitentes TCP si se experimentó o no congestión durante el tránsito. De esta manera, los remitentes TCP pueden ajustar sus ventanas y no envíar más tráfico hasta que la red pueda dar servicio.

Antes, el descarte de paquetes indicaba que se estaba produciendo congestión. Pero con el uso de IP ECN se tiene la notificación de congestión sin descartar paquetes.
El primer bit IP ECN se usa para indicar si el dispositivo es compatible con IP ECN y el segundo bit se usa para indicar si se experimentó congestión (0 = "sin congestión"; 1 = "congestión "). [15]

Diffserv incluye comportamientos diferentes (*PHBs per hop behaviors*). El PHB es configurado por un mecanismo administrador de red, mediante la tabla de comportamiento de QoS dentro del *router*.

1.6.5.1 Retransmisión PHB

Los diferentes tipos de comportamientos (PHB) son los siguientes:

1.6.5.1.1 Default behavior

El valor DSCP es cero (000 000) y el servicio por defecto donde las pérdidas y congestión son descontroladas; se usa para servicios de mejor esfuerzo.

1.6.5.1.2 Class selector behavior

Los valores DSCP desde el 001000 al 111000 sirven para especificar siete comportamientos diferentes, cada uno de los cuales tiene una mayor probabilidad de un envío a tiempo que su predecesor.

1.6.5.1.3 Reenvío asegurado (Assured Forwarding (AF))

Ofrece diversos niveles de aseguramiento para los paquetes IP recibidos en un dominio del cliente. Hay cuatro clases de AF, AF1x hasta AF4x; dentro de cada clase existen tres probabilidades de prioridad. Dependiendo de la política de la red,

se puede seleccionar un PHB basado en el rendimiento, retardo, *jitter*, o la prioridad de los servicios.

Los bits DS5, DS4 y DS3 definen la clase mientras que los bits DS2 y DS1 indican la probabilidad de caída, mientras que DS0 es siempre cero.

La tabla 1.2 ilustra la codificación DSCP para la clase AF.

	Clase 1	Clase 2	Clase 3	Clase 4
Bajo	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Medio	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Alto	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Tabla 1.2 Codificación AF [16]

1.6.5.1.4 Reenvío Acelerado (Expedited Forwarding (EF))

El RFC 2598 define el EF. El valor recomendado es 101110. EF permite la creación de servicios en tiempo real con una tasa de *throughput* configurable.

El Seleccionador de Clase (CS) sirve para alguna compatibilidad con versiones anteriores con el *IP ToS.*

Cisco da una referencia para la operación en sus equipos definiendo 11 clases de tráfico. El resumen de las clases y sus recomendaciones de marcado se indican en la tabla 1.3.

Aplicación	Clasificación en Capa 3			Capa 2
				CoS/MPLS EXP
	IPP	PHB	DSCP	
Enrutamiento IP	6	CS6	48	6
Voz	5	EF	46	5
Video Interactivo	4	AF41	34	4
Streaming-Video	4	CS4	32	4
Datos definidos como críticos	3	—	25	3
Señalización de llamada	3	AF31/CS3	26/24	3
Datos transaccionales	2	AF21	18	2
Gestión de Red	2	CS2	16	2
Datos	1	AF11	10	1
Sin prioridad	1	CS1	8	1
Mejor Esfuerzo	0	0	0	0

Tabla 1.3 Clases de tráfico [17]

1.7 CALIDAD DE SERVICIO EN REDES METROETHERNET

1.7.1 INTRODUCCIÓN

Para mejorar y adaptar el rendimiento de una red, los administradores deben variar parámetros en el enlace para evitar los retardos en el servicio, manejar variables en la asignación de ancho de banda, evitar pérdidas de paquetes usando técnicas de calidad de servicio (QoS).

Antes de la convergencia de los servicios, el enfoque principal era a la conectividad. En razón que cada aplicación tenía exigencias y características de tráficos diferentes, los diseñadores de red desplegaron redes no integradas, las cuales fueron diseñadas para llevar un tipo específico de tráfico.

Con la convergencia de los servicios todo el tráfico cruza la misma red. Distintos tipos de tráfico exigen la asignación de prioridades.

Por ejemplo, paquetes que llevan tráfico de voz, no toleran retardos. Por otra parte, los paquetes que llevan datos de transferencia de ficheros son típicamente grandes y pueden soportar retardos y retransmisiones.

Los inconvenientes de calidad en redes convergentes se describen en cuatro puntos:

a. Carencia de ancho de banda

La falta de capacidad causa problemas en aplicativos multimedia o transmisión de grandes cantidad de información.

Se solventaría la carencia de ancho de banda, aumentando la capacidad de enlace. Pero esta solución es cara y lleva tiempo en su implementación.

Otra opción es clasificar el tráfico en diferentes clases de calidad de servicio y priorizar el tráfico según su importancia.

Optimizando el enlace al comprimir el *payload* de la trama virtualmente se aumenta el ancho de banda. Los paquetes comprimidos son más pequeños y toman menos tiempo para transmitir. Por otro lado la compresión puede aumentar el retardo debido al proceso de los algoritmos de compresión. *Stacker* y *Predictor* son dos algoritmos de compresión que están disponibles en Cisco.

Otro mecanismo eficiente es la compresión de la cabecera. Este mecanismo es eficiente en redes donde la mayor parte de paquetes llevan pequeñas cantidades de datos.

b. Lentitud extremo a extremo (fijo y variable)

El tiempo que necesita el paquete en alcanzar el destino se considera como el tiempo extremo a extremo.

Procesos que conllevan tiempos de retardo fijos son por ejemplo, la serialización que consiste en colocar los bits en el canal y la propagación que es el tiempo que le toma al paquete transitar por el medio físico.

Por otro lado un tipo de retardo variable es por ejemplo el retardo de procesamiento en equipos de *internetworking* en labores como encapsulamiento, *switching*, cambio de cabecera de paquetes, entre otros.

c. Variación del retardo (*jitter*)

Es un cambio indeseado y abrupto de la propiedad de una señal que puede afectar la amplitud, frecuencia y la fase, durante el envío de señales digitales a causa de la desviación de la exactitud de la señal de reloj. El *jitter* se considera como una señal de ruido no deseada. [18]

d. Pérdida de paquetes

Generalmente se causa por congestión de tráfico en la WAN. El aumento de la capacidad del ancho de banda puede prevenir la congestión, pero se debería garantizar el suficiente ancho de banda e incrementar el espacio en el *buffer* para aplicaciones sensibles a retardos.

Hay algunos otros mecanismos que también se pueden utilizar para prevenir la congestión, como por ejemplo:

- Modelamiento de tráfico (*Traffic shaping*): Se retrasan unos o todos los paquetes en una corriente de tráfico a fin de tener conformidad con un perfil de tráfico.

Un *shaper* por lo general tiene una memoria intermedia de tamaño finito, y los paquetes pueden ser desechados si no hay espacio suficiente para sostener los paquetes retrasados. De esta manera se intenta controlar el tráfico para lograr optimizar o garantizar el rendimiento, baja latencia y ancho de banda. [19].

- Políticas de tráfico (*Traffic policing*): Se puede limitar los paquetes menos importantes para proporcionar el mejor servicio a paquetes sensibles al retardo, en función de la política administrativa y las características del exceso de tráfico.

Los administradores de red habilitan aspectos de QoS para controlar y predecir servicios de una variedad de aplicaciones de red y tipos de tráfico, permitiendo así a los administradores de la red tomar ventaja de las nuevas aplicaciones.

La calidad de servicio ofrece servicios inteligentes de red que, cuando son correctamente aplicados, ayudan a proporcionar un rendimiento consistente y predecible.

Hay tres pasos básicos implicados en la realización de la calidad de servicio en una red:

1. Identificar el tráfico y sus exigencias. Estudiar el tipo de tráfico que pasa por la red para determinar los requerimientos de *QoS* de los diferentes tipos de tráfico.

2. Agrupar el tráfico en clases con similares requerimientos de calidad de servicio (*QoS*). Por ejemplo se podrían establecer cinco clases de tráfico:

    - Voz: Clase en donde se prioriza el tráfico de la voz sobre IP (*VoIP*).
    - Crítica: Clase para aplicaciones críticas de la organización.
    - Transaccional: Clase para base de datos, aplicaciones transaccionales, tráfico interactivo.
    - El mejor esfuerzo (*Best effort*): Clase para tráfico de Internet.
    - No prioritario (*less-than-best-effort*): Ares, Emule, y otras aplicaciones.

3. Definir las políticas de *QoS* para cada clase de tráfico.

Se configura el mínimo ancho de banda garantizado, el límite máximo de ancho de banda, se asigna prioridad para cada clase y se maneja la congestión de tráfico con técnicas de *QoS*.

1.7.2 MODELOS DE CALIDAD DE SERVICIO

Los siguientes modelos se usan para implementar la calidad de servicio en una red.

1.7.2.1 Modelo de mejor esfuerzo (*Best-Effort*)

Con este modelo la calidad de servicio no es aplicada a los paquetes. La red hace todo lo posible para intentar entregar el paquete a su destino, donde no hay garantía de que esto ocurra.

Entre los beneficios de este modelo, se tiene una gran escalabilidad y el no requerir mecanismos de calidad de servicio especiales.

Este modelo no es el apropiado para aplicaciones sensibles al retardo o variaciones de ancho de banda.

1.7.2.2 Servicios Integrados (*IntServ Integrated Services*)

Provee a las aplicaciones un nivel garantizado de servicio, negociando parámetros de red, extremo a extremo.

IntServ fue introducido para garantizar un comportamiento previsible de la red para las aplicaciones, por ser un modelo que puede acomodar exigencias de calidad de servicio múltiples.

La aplicación solicita el nivel de servicio con el fin de operar apropiadamente, el cual se basa en la calidad de servicio *QoS* para que se reserven los recursos de red necesarios antes de que la aplicación comience a operar.

Estas reservaciones se mantienen hasta que la aplicación termina o hasta que el ancho de banda requerido por ésta sobrepase el límite reservado para dicha aplicación.

El modelo *IntServ* se basa en el Protocolo de Reservación de Recursos (*RSVP*) para señalizar y reservar la calidad de servicio deseada para cada flujo en la red.

Mecanismos de encolamiento pueden ser usados con *RSVP* para proporcionar estos niveles de servicio, como por ejemplo una tasa garantizada donde las aplicaciones reservan el ancho de banda según sus exigencias.

El nivel de servicio de carga controlada permite que las aplicaciones tengan un bajo retardo y un rendimiento alto, incluso durante tiempos de congestión.

RSVP realiza peticiones de calidad de servicio por flujo individual. La red puede proporcionar garantías a estos flujos individuales. El problema con esto es que *IntServ* no es escalable a redes grandes debido al gran número de flujos RSVP concurrentes, puesto que la información de reserva de estados, necesita ser mantenida por cada *router* a lo largo del camino.

RSVP informa a los dispositivos de red los parámetros de flujo (direcciones IP y números de puerto). Algunas aplicaciones usan números de puerto dinámicos, que pueden ser difíciles de reconocer por los dispositivos de red.

El reconocimiento de aplicación (*NBAR Network-based application recognition*) es un mecanismo que ha sido introducido para complementar *RSVP* para aplicaciones que usan números de puerto dinámicos, pero no usan *RSVP*.

IntServ soporta el control de admisión que permite que una red rechace nuevas sesiones *RSVP* si una de las interfaces en el camino ha alcanzado todo el ancho de banda reservada.

Los inconvenientes con *IntServ* es la señalización continua debido al estado de operación *RSVP*.

1.7.2.3 Servicios Diferenciados DiffServ (*DiffServ Differentiated Services*)

Proporciona la mayor escalabilidad y flexibilidad en la implementación de calidad de servicio en una red, debido a que es un modelo que incluye un conjunto de herramientas de clasificación y mecanismos de encolamiento para proveer a ciertas aplicaciones o protocolos, determinadas prioridades sobre el resto del tráfico en la red.

Los dispositivos de red reconocen las clases de tráfico y proporcionan diferentes niveles de calidad de servicio a diferentes clases de tráfico.

DiffServ cuenta con *routers* de borde para realizar la clasificación de los distintos tipos de paquetes que circulan por la red. El tráfico de red puede ser clasificado por dirección de red, protocolo, puertos, interfaz de ingreso o cualquier tipo de clasificación que pueda ser alcanzada mediante el uso de listas de acceso en su variante para la implementación de *QoS*.

Con DiffServ los *routers* operan más rápido, ya que se limita la complejidad de la clasificación y el encolado; se minimiza el tráfico de señalización y el almacenamiento.

En *DiffServ*, se definen clases de servicio basadas en exigencias comerciales, cada flujo particular de datos es agrupado en un tipo de clase, la cual puede ser asignada a diferentes niveles de servicio.

Los *routers* internos solo están interesados en el comportamiento por salto (*PHB Per Hop Behavior*), marcado en la cabecera del paquete. Esta arquitectura permite a *DiffServ* rendir en ambientes de bajo ancho de banda, y proveer una mayor potencialidad que una arquitectura *IntServ***.**

Una vez que existe la capacidad de marcar los paquetes utilizando DSCP *(Differentiated Services Code Point*), es necesario proveer del tratamiento apropiado para cada una de estas clases. La colección de paquetes con el mismo

valor DSCP circulando hacia una dirección determinada, se denomina *BA (Behavior Aggregate)*. Es así como múltiples aplicaciones pueden pertenecer al mismo BA. [20]

DiffServ tiene el inconveniente de requerir complejos mecanismos para trabajar en conjunto en toda la red.

1.7.3 MECANISMOS DE CALIDAD DE SERVICIO

Los mecanismos de calidad de servicio *QoS IP* se utilizan para implementar una política coordinada de calidad de servicio en los dispositivos de red.

A continuación se describen diferentes tipos de mecanismos que se utilizan para implementar QoS en una red IP.

1.7.3.1 Clasificación

Es la identificación y separación de tráfico en diferentes clases. En una red en la que se encuentra habilitado QoS, todo el tráfico se clasifica en la interfaz de entrada de todos los dispositivos compatibles con QoS.

La clasificación de paquetes se puede realizar bajo algunos factores como por ejemplo DSCP, IP *Precedence*, Dirección de origen, Dirección de destino, entre otros.

1.7.3.2 Marcación

Se usa para marcar cada paquete como un miembro de una clase de red, de modo que la clase de paquete pueda ser rápidamente reconocida en todas las partes del resto de la red.

El marcado se lleva a cabo lo más cerca del borde de la red como sea posible.

Los mecanismos de calidad de servicio configuran los bits en los campos *DSCP o IP Precedence* de cada paquete IP de acuerdo a la clase a la que el paquete corresponda.

Otros mecanismos de calidad de servicio usan estos bits para determinar el tratamiento cuando el paquete llegue. Si los paquetes son marcados como paquetes de voz prioritarios, los paquetes por lo general no serán descartados por los mecanismos de protección de congestión y serán prioritarios en los mecanismos de administración de encolamiento.

Por otra parte, si los paquetes son marcados como paquetes de transferencia de archivos, éstos tendrán prioridad baja.

1.7.3.3 Manejo de Congestión *(Congestion Management)*

Los mecanismos de manejo de congestión utilizan la marca de cada paquete para determinar en qué cola colocar los paquetes.

El manejo de congestión se realiza en todas las interfaces de salida habilitadas con calidad de servicio QoS mediante el uso de mecanismos de colas. Cada algoritmo de cola ha sido diseñado para resolver un problema de tráfico de red específico y tiene un efecto particular sobre el desempeño de la red.

Entre los métodos para el manejo de la congestión se tienen los siguientes:

1.7.3.3.1 FIFO (First In First Out)

Es el método más simple de encolamiento, se basa en que el primer paquete que entra a la interfaz, es el primero en salir. Es adecuado para interfaces de alta velocidad, no para bajas. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes. [21]

1.7.3.3.2 Prioridad de Encolamiento (PQ - Priority Queuing)

Consiste en un conjunto de colas, clasificadas desde alta a baja prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego siguen las de menor prioridad. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad.

1.7.3.3.3 Encolamiento Personalizado (CQ - Custom Queueing)

Permite al administrador priorizar el tráfico sin los efectos de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada una de ellas es atendida con el esquema *Round Robin*. CQ ofrece un mecanismo más detallado de encolamiento, pero no asegura una prioridad absoluta como PQ.

Se utiliza CQ para proveer a tráficos particulares un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles.

1.7.3.3.4 Weighted Fair Queuing (WFQ)

Es un método automatizado que provee una asignación de ancho de banda para todo el tráfico de la red, utilizado habitualmente para enlaces de velocidades menores a 2048 Kbps.

WFQ ordena el tráfico en flujos, utilizando una combinación de parámetros. Una vez distinguidos estos flujos, el *router* determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegura que los flujos de alto volumen sean ubicados al final de la cola, y los de volúmenes bajos, sensibles al retardo, sean ubicados al principio de la cola.

WFQ es apropiado en situaciones donde se desea proveer un tiempo de respuesta consistente ante usuarios que generen altas y bajas cargas en la red, ya que WFQ se adapta a las condiciones cambiantes del tráfico.

Sin embargo, la carga que significa para el procesador en los equipos de enrutamiento, hace de esta metodología poco escalable.

1.7.3.3.5 Class-Based Weighted Fair Queuing (CBWFQ)

WFQ tiene algunas limitaciones de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta, pudiendo colapsar debido a la cantidad numerosa de flujos que analiza.

CBWFQ fue desarrollada para evitar estas limitaciones, tomando el algoritmo de WFQ y expandiéndolo, permitiendo la creación de clases definidas por el usuario, que permite un mayor control sobre las colas de tráfico y asignación del ancho de banda. Las clases que son posibles implementar con CBWFQ pueden ser determinadas según protocolo ACL *(Access control list)*, valor DSCP, o interfaz de ingreso. Cada clase posee una cola separada, y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola.

Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados.

Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se pueden configurar específicamente el ancho de banda y límite de paquetes máximos para cada clase. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase.

1.7.3.3.6 Encolamiento de Baja Latencia (LLQ - Low Latency Queuing)

Es una mezcla entre PQ y CBWFQ. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. Si existe tráfico

en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas.

Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas.

La cola de prioridad que posee LLQ provee de un máximo retardo garantizado para los paquetes entrantes en esta cola, el cual es calculado como el tamaño del MTU dividido para la velocidad de enlace.

1.7.3.4 Evasión de Congestión (*Congestion Avoidance*)

Se analiza la manera en que los protocolos operan, con el fin de no llegar a la congestión de la red.

1.7.3.4.1 RED (Random Early Detection) y WRED (Weighted Random Early Detection)

Las técnicas de RED y WRED evitan el efecto conocido como sincronización global. Cuando múltiples conexiones TCP operan sobre un enlace común, todas ellas incrementarán el tamaño de su ventana deslizante a medida que el tráfico llega sin problemas. Este aumento gradual consume el ancho de banda del enlace hasta congestionarlo.

En este punto las conexiones TCP experimentan errores de transmisión, lo que hace que disminuyan su tamaño de ventana simultáneamente. Esto conlleva a una sincronización global, donde todos los flujos comienzan a incrementar su tasa de transmisión nuevamente para llegar a otro estado de congestión. Este ciclo es repetitivo, creando picos en la utilización del ancho de banda del enlace.

Los métodos de evasión de congestión tratan con este tipo de situación, descartando paquetes de forma aleatoria. RED exige a que el flujo reduzca el tamaño de la ventana de transmisión, disminuyendo la cantidad de información

enviada. A medida que se alcanza el estado de congestión en la red, más paquetes entrantes son descartados con el fin de no llegar al punto de congestión en el enlace.

Una limitación de estas técnicas de evasión de congestión es que solo sirve para tráfico basado en TCP, ya que otros protocolos no utilizan el concepto de ventana deslizante.

1.7.3.5 Políticas y Modelamiento (*Policing and Shaping*)

Son métodos para limitar el tráfico saliente en una interfaz determinada, con el fin de administrar eficientemente los recursos de la red. Ante esta necesidad existen dos metodologías de limitación de ancho de banda: *Policing* y Modelamiento de Tráfico (TS *Traffic Shaping*).

Mediante *Policing* se especifica la limitación de tasa máxima de transmisión para una clase de tráfico. Si este umbral es excedido, una de las acciones inmediatas será transmitir, descartar, o remarcar. No es posible almacenar los paquetes para posteriormente enviarlos, como es el caso de *Traffic Shaping*.

Las técnicas *Traffic Shaping* en lugar de descartar el tráfico que excede cierta tasa determinada, atrasan parte del tráfico sobrante a través de colas, con el fin de modelarlo a una tasa que la interfaz remota pueda manejar. El resto del tráfico excedente es inevitablemente descartado.

Traffic Shaping es una buena herramienta en situaciones en las cuales el tráfico saliente debe respetar una cierta tasa máxima de transmisión. Este proceso es realizado independientemente de la velocidad real del circuito.

1.7.3.6 Eficiencia de Enlace

Se realiza por medio de la compresión y fragmentación de enlace. La compresión de cabecera puede reducir drásticamente el *overhead* asociado con el transporte de la voz.

1.7.3.6.1 Real-Time Transport Protocol (RTP)

El protocolo de Transporte en tiempo real (*Real-Time Transport Protocol RTP*) es un protocolo *host* a *host* que se utiliza para transportar el tráfico convergente (incluyendo audio y video paquetizado) sobre una red IP.

1.7.3.6.2 Compressed Real-Time Transport Protocol (CRTP)

La compresión normalmente se utiliza en los enlaces WAN para mejorar la eficiencia del ancho de banda, por ejemplo el protocolo de compresión de transporte en tiempo real (*CRTP*).

1.7.3.6.3 Link Fragmentation and Interleaving (LFI)

Otra tecnología es la fragmentación del enlace y el intercalado (*LFI Link Fragmentation and Interleaving*), que puede reducir el "*jitter*" de transmisión de voz mediante la reducción de retardo de los paquetes [22].

1.8 ALTERNATIVAS DE MÉTODOS DE ACCESO EN LA ÚLTIMA MILLA

El acceso de última milla puede ser por medio guiado o por medio no guiado.

1.8.1 ACCESO POR LÍNEAS DE COBRE

Usualmente el TDR (reflectómetro de dominio del tiempo) es el instrumento electrónico usado para localizar los defectos en cables metálicos, detectar aumentos de los niveles de la resistencia en empalmes y conectores. Si existen discontinuidades de impedancia en el recurso, cada discontinuidad creará un eco que se reflejará hacia el TDR. [23]

En el diagrama de la figura 1.16 se presenta un acceso de cobre con módems de línea enlazados en el extremo final al DSLAM, el cual se interconecta a través del switch hacia la red Metroethernet. Entre las marcas de módems se tienen: Zhone, Ericsson y D-Link

En la figura 1.17, se tiene una solución *LAN to LAN* con interconexión directa a la red Metroethernet, la configuración de las VLANs y *QoS* se establece en los equipos de *internetworking* de borde.

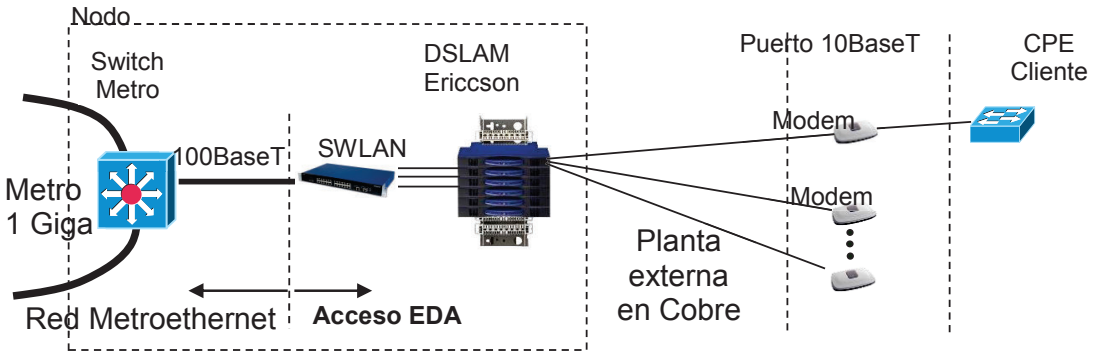


Figura 1.16 Acceso de cobre EDA

Figura 1.17 Acceso de cobre LAN to LAN

1.8.2 ACCESO POR LÍNEAS DE FIBRA ÓPTICA

Desde el *switch* Metroethernet se utiliza conversores de fibra óptica punto a punto para llegar a la sede del cliente, tal como se ilustra en la figura 1.18. En el cliente

se conecta al equipo activo en el puerto *FastEthernet* del *router*. Este esquema no provee un servicio de respaldo en eventos de corte del recurso.

En la figura 1.19, se puede observar una solución de accesos de última milla con fibra óptica para proveer un servicio LAN to LAN por medio de fibra óptica a través de la nube Metroethernet.

Una solución para accesos a usuarios que demandan alta disponibilidad como una Matriz de una organización, se puede implementar mediante una fibra en subanillo, donde los segmentos tienen recorridos diferentes, como se ilustra en la figura 1.20.

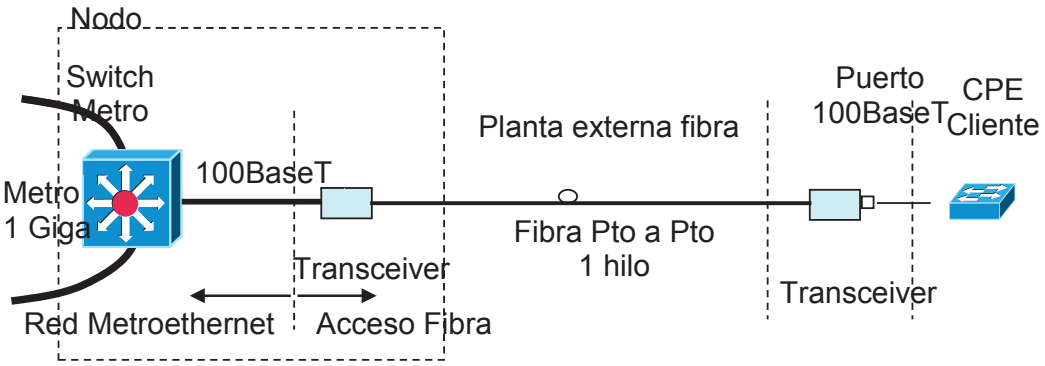


Figura 1.18 Acceso por fibra óptica punto a punto

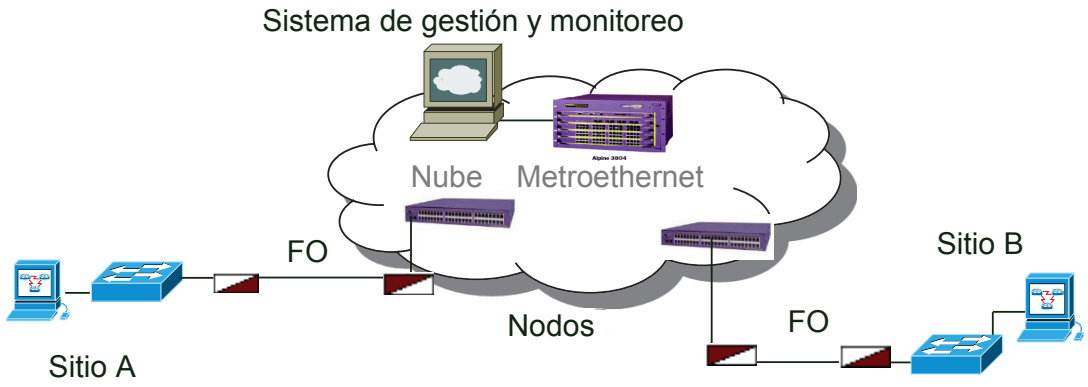


Figura 1.19 Acceso por medio de fibra óptica LAN to LAN

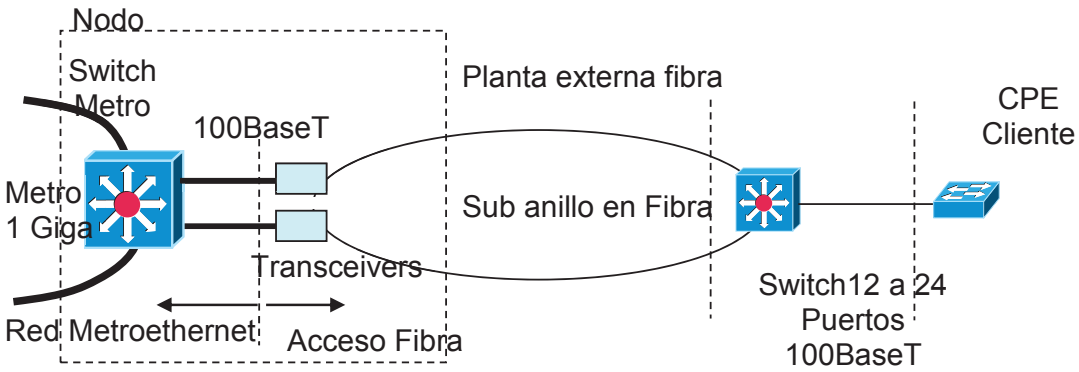


Figura 1.20 Acceso de fibra óptica en Subanillo

1.8.3 ACCESO POR ENLACES DE RADIO PUNTO A PUNTO

De igual manera se puede proveer accesos de radio Punto a Punto por medio de conversores E1 a Ethernet, los cuales se conectan directamente a la nube Metroethernet, como se indica en la figura 1.21.

Generalmente esta solución se implementa como *backup* de usuarios que requieren alta disponibilidad con radios que trabajan en banda licenciada. Entre las marcas de equipos se tienen: SAF y Ceragon.

1.8.4 ACCESO POR ENLACES DE RADIO PUNTO A MULTIPUNTO

En lugares donde la factibilidad de cobre o fibra se restringe, se puede implementar un acceso por medio de radios multipunto IP, como se indica en la figura 1.22.

Es importante la administración y gestión de las remotas para verificar el nivel de señal, posibles interferencias, monitoreo de tráfico y pruebas de errores en los equipos. Un ejemplo de acceso *wireless* Wimax se puede realizar con equipo de la marca Airspan.

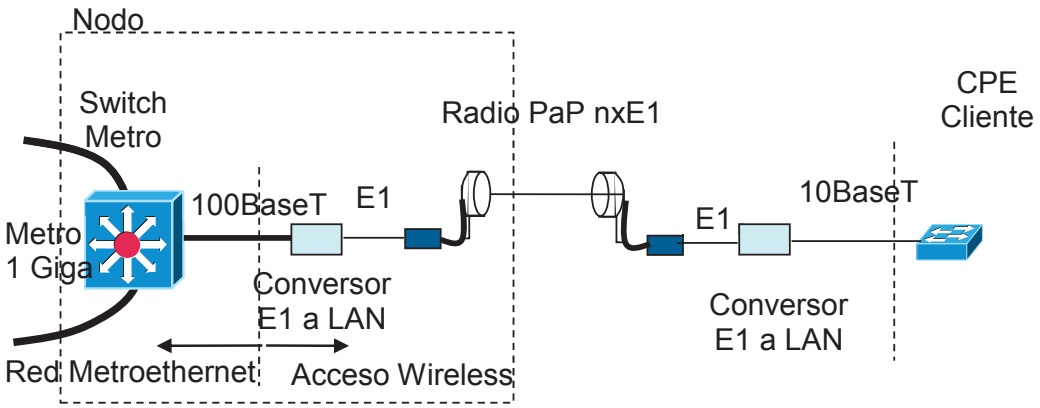


Figura 1.21 Acceso de radio microondas Punto a Punto

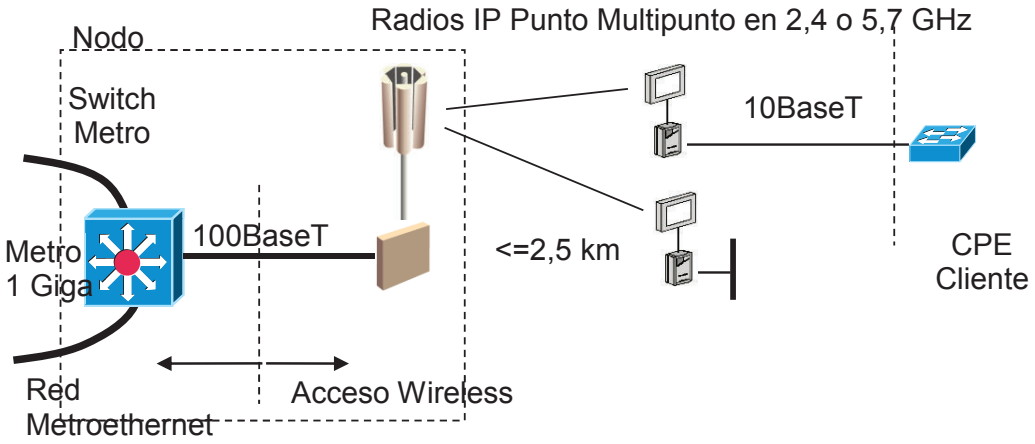


Figura 1.22 Acceso de radio Multipunto

1.9 PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento permiten que un *router* comparta información con otros *routers*, acerca de las redes que conoce así como de su proximidad a otros *routers*.

1.9.1 DISTANCIA ADMINISTRATIVA

La información que un *router* obtiene de otro mediante el protocolo de enrutamiento, se usa para crear y mantener las tablas de enrutamiento.

La confiabilidad de las rutas establecidas por un protocolo de enrutamiento, está caracterizada por la distancia administrativa.

En la tabla 1.4, se detalla el valor de la distancia administrativa que se utiliza como un método de selección de los protocolos de enrutamiento IP.

El protocolo de enrutamiento es el responsable de seleccionar la mejor ruta a cualquier red de destino. Las distancias administrativas han sido asignadas con una preferencia para las entradas manuales sobre las entradas conocidas dinámicamente.

PROTOCOLO	DISTANCIA ADMINISTRATIVA
Red directamente conectada	**0**
Ruta estática	**1**
EIGRP (*Enhanced Interior Gateway Routing Protocol*)	**5**
Ruta BGP externa (*External Border Gateway Protocol*)	**20**
Ruta EIGRP interna	**90**
IGRP	**100**
OSPF	**110**
IS-IS (Intermediate System-to-Intermediate System)	**115**
RIP v1, v2 (Routing Information Protocol)	**120**
EGP (Exterior Gateway Protocol)	**140**
ODR (On Demand Routing)	**160**
Ruta EIGRP externa	**170**
Ruta BGP interna	**200**
Ruta desconocida	**255**

Tabla 1.4 Tabla de Distancias Administrativas [24]

1.9.2 CLASIFICACIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento se clasifican en:

- Enrutamiento Estático: Se usa en redes pequeñas, cuando no hay rutas redundantes, es decir hay un solo punto de unión hacia el resto de la red. Las rutas estáticas son gestionadas y modificadas manualmente por el administrador de red cuando un cambio en la topología de la red requiera una actualización.
- Enrutamiento Dinámico: Una ruta es construida por información intercambiada por los protocolos de enrutamiento y se adapta automáticamente a los cambios de topología.

Los protocolos de enrutamiento dinámico de acuerdo a su función se clasifican en: protocolos de gateway interior (IGP) y protocolos de gateway exterior (EGP). Y los protocolos de gateway interior se clasifican en: protocolos Vector – Distancia y Estado de Enlace, como se indica en la figura 1.23.

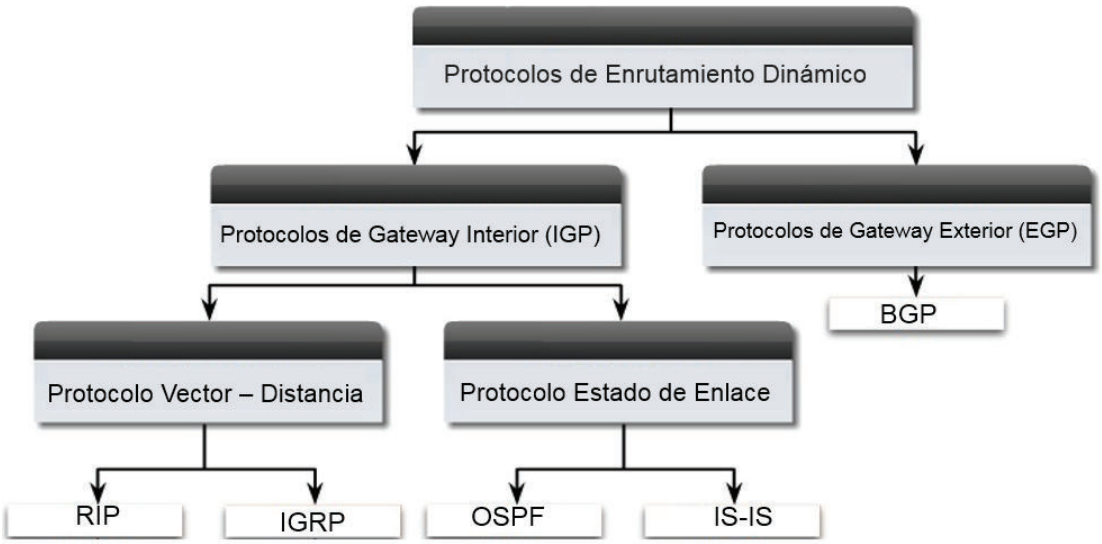


Figura 1.23 Protocolos de enrutamiento dinámico [25]

1.9.2.1 Protocolo de *Gateway* Interior (IGP)

Los protocolos de *gateway* interior se usan para resolver el encaminamiento dentro del propio sistema autónomo. Ejemplos de protocolos IGP son: RIP, IGRP, OSPF, EIGRP, IS-IS.

Los protocolos de *gateway* interior se pueden dividir en dos categorías:

- Protocolo de enrutamiento vector-distancia
- Protocolo de enrutamiento enlace-estado

1.9.2.1.1 Protocolo Vector – Distancia

Los protocolos de enrutamiento por vector – distancia se basan en el número de saltos o cantidad de *routers* que tiene que pasar el paquete para llegar a la red de destino.

Cuando se detecta un cambio de topología de la red, y de manera periódica, se envían copias de las tablas de enrutamiento de un *router* a sus *routers* vecinos. Por esta razón la convergencia es lenta, pero los algoritmos de vector-distancia tienen menos complejidad computacional. Ejemplos: RIP, IGRP.

- **RIP (*Routing Information Protocol*)**

El Protocolo de Información de Enrutamiento, es el método más común para transferir información de enrutamiento entre *routers* ubicados en la misma red, su métrica es el número de saltos, por lo tanto no siempre selecciona la ruta más rápida. El número máximo de saltos es de 15, caso contrario se declara inalcanzable la red destino.

RIP tiene una distancia administrativa de 120 y las rutas tienen un tiempo de vida de 180 segundos. Si pasado este tiempo, no se han recibido mensajes que confirmen que esa ruta está activa, se pone inactiva asignándole una métrica de

16. Las tablas de enrutamiento se actualizan cada 30 segundos, lo que genera gran cantidad de tráfico en la red.

Existen tres versiones diferentes de RIP, las cuales son:

RIPv1: Su especificación está recogida en el RFC 1058, se define como un protocolo basado en las clases de las direcciones IP. Por lo tanto, RIPv1 no soporta máscaras de tamaño variable (VLSM) ni direccionamiento sin clase (CIDR), lo que resulta poco eficiente.

Además, RIPv1 tampoco incluye ningún mecanismo de autentificación de los mensajes, haciéndolo vulnerable a ataques.

Utiliza el puerto UDP 520 para enviar sus mensajes en propagación *Broadcast*.

RIPv2: Su especificación está en el RFC 1723 y RFC 2453. Soporta subredes, CIDR y VLSM.

Para tener compatibilidad con RIPv1, se mantiene la limitación de 15 saltos. Soporta autenticación, utilizando uno de los siguientes mecanismos: no autentificación, autenticación mediante contraseña, autentificación mediante contraseña codificada mediante MD5.

RIPng (RIP *next generation*): RIP para redes basadas en IPv6. Su especificación está recogida en el RFC 2080.

Los tipos de mensajes RIP pueden ser de dos tipos:

Mensajes de petición: Enviados por algún *router* recientemente iniciado que solicita información de los *routers* vecinos.

Mensajes de respuesta: Son mensajes con la actualización de las tablas de enrutamiento y pueden ser tres tipos:

- Mensajes ordinarios: Se envían cada 30 segundos, para indicar que el enlace y la ruta siguen activos.
- Mensajes enviados como respuesta a mensajes de petición.
- Mensajes enviados cuando cambia algún costo. Se envía toda la tabla de enrutamiento.

- **Protocolo de enrutamiento de *gateway* interior IGRP (*Interior Gateway Routing Protocol*)**

Es un protocolo propietario de Cisco basado en la tecnología vector-distancia, aunque también tiene en cuenta el estado del enlace. Utiliza una métrica compuesta para determinar la mejor ruta basándose en el ancho de banda, el retardo, la confiabilidad y la carga del enlace. Por defecto, se envía un *broadcast* de las actualizaciones de enrutamiento cada 90 segundos.

El concepto es que cada *router* no necesita saber todas las relaciones de ruta/enlace para la red entera. Cada *router* publica destinos con una distancia correspondiente. Cada *router* que recibe la información, ajusta la distancia y la propaga a los *routers* vecinos. La información de la distancia en IGRP se manifiesta de acuerdo a la métrica. Esto permite configurar adecuadamente el equipo para alcanzar las trayectorias óptimas.

1.9.2.1.2 Protocolo Estado de Enlace

Los protocolos de estado de enlace generan una inundación de información de ruta, lo que da a cada router una visión completa de la topología de la red [26]. Por ejemplo: OSPF, EIGRP, IS-IS.

El proceso de enrutamiento de estado de enlace es el siguiente:

- Cada *router* conoce sus propias redes conectadas directamente.
- Los *routers* de estado de enlace intercambian un paquete de saludo para conocer a los *routers* de estado de enlace conectados directamente.

- Cada *router* crea su propio paquete de estado de enlace LSP (*Link State Packet*) que incluye información sobre los vecinos, como la ID, el tipo de enlace y el ancho de banda.
- Una vez que se crea el LSP, el *router* lo envía a todos sus vecinos, que almacenan la información y, luego, la reenvían hasta que todos los *routers* tengan la misma información.
- Cuando todos los *routers* han recibido los LSP, los *routers* crean un mapa topológico de la red que se utiliza para determinar las mejores rutas para un destino.

- **Protocolo OSPF *(Open Short Path First)***

Emplea una tecnología de estado de enlace, correspondiendo a un protocolo de enrutamiento interior. Soporta grandes redes, proporcionando rapidez en la convergencia y actualización de rutas. La división en áreas reduce el impacto del protocolo en el CPU y la memoria de los equipos de *internetworking*.

Cada *router* difunde al resto de *routers* de la red las identidades y los costes conocidos mediante un anuncio del estado de enlace (paquete *LSA Link State Advertisement*). Aplicando el Algoritmo de *Dijkstra* se calculan las rutas de coste mínimo para sus tablas de enrutamiento.

Existen consideraciones con respecto a los LSAs, los cuales se envían únicamente cuando se detectan cambios en la topología de la red, los LSAs tienen un tiempo de vida y son eliminados cuando expiran.

Además tienen un número de secuencia que permite comprobar si la información que contiene es o no la más reciente de que se dispone.

La asignación de costes predeterminados OSPF se basa en el ancho de banda del enlace. El coste de ruta de los *routers* se calcula con la fórmula 10^8 / ancho de banda en bps.

La desventaja que presenta OSPF es el consumo elevado de memoria ya que cada *router* almacena la topología de toda la red.

- **EIGRP (*Enhanced Interior Gateway Routing Protocol*)[27]**

Protocolo propietario de *Cisco Systems*, sus funciones tales como las actualizaciones parciales y la detección de vecinos son similares a OSPF.

Los *routers* EIGRP mantienen la información de ruta y topología en memoria RAM, para reaccionar rápidamente ante los cambios.

EIGRP mantiene las siguientes tres tablas:

- La tabla de vecinos que enumera a los *routers* adyacentes.

- La tabla de topología que se compone de todas las tablas de encaminamiento EIGRP recibidas de los vecinos. EIGRP con la tabla de vecinos y la tabla de topología, calcula las rutas de menor costo hacia cada destino; esta información se introduce a la tabla de topología. Existe una tabla de topología por cada protocolo configurado de red, mientras que la tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

- La tabla de encaminamiento EIGRP contiene las mejores rutas hacia un determinado destino, información que se obtiene de la tabla de topología.

Por cada protocolo de red se mantiene una tabla de vecinos, una tabla de topología y una tabla de encaminamiento.

- **IS-IS *(Intermediate System to Intermediate System)* [28]**

IS-IS es un protocolo de enrutamiento interior que permite trabajar *con Type of Service (ToS).*

Permite a sistemas intermedios dentro de un mismo dominio cambiar su configuración e información de ruteo para facilitar la información de encaminamiento.

En IS-IS se definen tres tipos de *routers*:

Router de Nivel 1 (*router Intra-area*): Su conocimiento de la red está limitado al área y emplea una ruta por defecto al router de Nivel 2 más cercano para enrutar tráfico externo al área donde se encuentra.

Router de Nivel 2 (*router Inter-área*): Son necesarios para el enrutamiento entre áreas distintas tal como los *routers* de *backbone*. Los *routers* de Nivel 2 se comunican por medio de paquetes *hello* que solo son comprendidos entre ellos.

Router de Nivel 1-2: Son *routers* tanto *Intra* como Inter-área, pueden tener vecinos en diferentes áreas porque envían paquetes *hello* tanto de Nivel 1 como de Nivel 2 y por lo tanto pueden comunicarse con ambos tipos de *routers*. Almacenan una base de datos de estado-enlace de Nivel 1 y otra para el Nivel 2 con la información necesaria para el enrutamiento Inter-área.

El proceso de ruteo se define en varias fases:

1) Proceso de decisión, que permite el cálculo de las rutas a cada destino del dominio. Se ejecuta por separado para encaminamiento de nivel 1 y nivel 2, y por separado dentro de cada nivel para cada una de las métricas soportadas por el sistema intermedio.

2) Proceso de actualización, donde se genera, recibe y propaga el estado de enlaces de los PDUs. Cada PDU de estado de enlace contiene información sobre la identidad y los valores de la métrica de encaminamiento de las adyacencias del IS que originó el PDU estado de enlace.

3) Proceso de reenvío, en el que se suministra y gestiona los *buffers* necesarios para soportar transmisión NPDU (*Network Protocol Data Unit*) a todos los destinos y el proceso de recepción.

1.9.2.2 Protocolos de G*ateway* Exterior (EGP)

Son protocolos que se usan para conectar sistemas autónomos (AS) entre sí como por ejemplo el protocolo BGP.

1.9.2.2.1 Protocolo BGP (External Border Gateway Protocol) [29]

La versión 1 tiene su especificación en el RFC 1105, la versión 2 en el RFC 1163, la versión 3 en el RFC 1267, y la versión 4 en las especificaciones RFC 1771 y RFC 4271, que proporciona soporte para CIDR (*Classless Interdomain Routing*). BGP es un protocolo que funciona sobre TCP por el puerto 179.

BGP permite el enrutamiento de los paquetes IP que se intercambian entre los distintos AS, para lo cual es necesario el intercambio de prefijos de rutas entre los diferentes AS de forma dinámica, que se lleva a cabo mediante el establecimiento de sesiones BGP inter-AS sobre conexiones TCP.

BGP utiliza un algoritmo similar al tipo vector de distancia, llamado *path-vector*, para seleccionar aquellas rutas que impliquen el mínimo número de AS a atravesar. Las tablas de enrutamiento de BGP almacenan los prefijos para alcanzar las redes. Las rutas están formadas por una secuencia de números de sistemas autónomos que se deben seguir para alcanzar el prefijo indicado.

El último número de AS de la ruta corresponde al AS donde se encuentra el destino, el motivo para almacenar la ruta completa es la detección y eliminación de *loops*, evitando que los paquetes se envíen de forma indefinida pasando varias veces por un mismo AS.

- **Sesiones BGP**

En una sesión BGP participan solo dos *routers* denominados *peers*. En la sesión BGP se lleva a cabo el proceso denominado *peering*, que consiste en que un AS informa a otro sobre las redes que puede alcanzar a partir de éste.

En las sesiones inter-AS los *routers* de borde de un mismo AS deben intercambiar información BGP para conocer las mismas rutas externas e internas. Para ello se utiliza el protocolo I-BGP, que utiliza el mismo tipo de mensajes que E-BGP.

E-BGP es el protocolo utilizado en las sesiones BGP entre dos *gateways* de dos AS distintos. En E-BGP, los prefijos que aprende un *router* de un vecino pueden ser anunciados a otro vecino mediante I-BGP y viceversa, pero un prefijo aprendido de un vecino mediante I-BGP no puede reanunciarse a otro vecino por I-BGP, esta regla sirve para evitar *loops* dentro de un AS.

Como no se pueden reanunciar prefijos entre *routers* I-BGP, es necesario que exista conectividad entre todos los *routers* vecinos que se comuniquen mediante I-BGP dentro de un mismo AS, por lo que se utiliza un mallado virtual ya que se implementa de una forma independiente de la conectividad física.

En el caso de E-BGP, la forma de prevenir bucles es mediante el atributo ASPATH. Este atributo se incluye en cada ruta anunciada y solo se modifica en los anuncios E-BGP. En la figura 1.24, se indica un esquema de sesiones BGP.

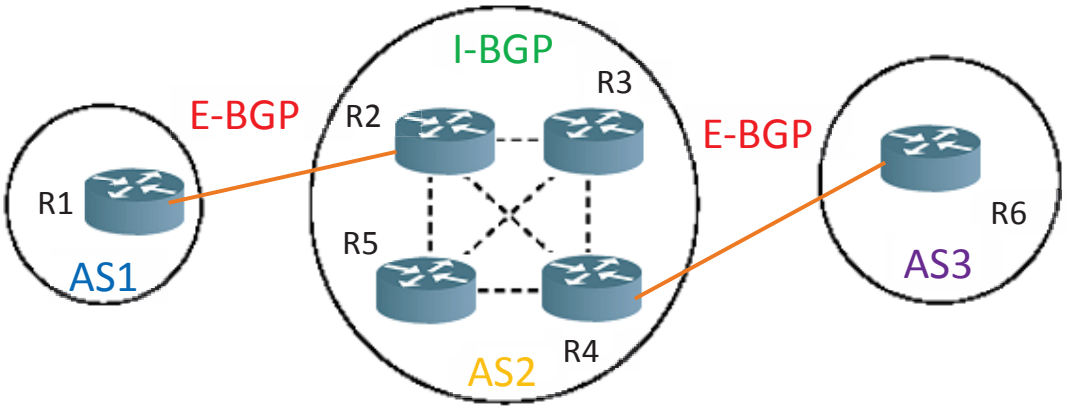


Figura 1.24 Sesiones BGP

- **Funcionamiento del proceso BGP**

Cuando un *router* anuncia un prefijo a uno de sus *router*s vecinos BGP, esa información es considerada válida hasta que el primer *router* anuncia que la información ya no es válida o hasta que la sesión BGP se pierde.

En un principio existirá un alto flujo de mensajes cuando se establece la sesión BGP, pero transcurrido un tiempo de estabilización los *router*s solo necesitarán informar de los cambios que han ocurrido. BGP no requiere que la información de routing se refresque periódicamente.

Para almacenar información de enrutamiento, el protocolo BGP necesita un conjunto de tablas de datos denominadas RIBs (*Routing Information Bases*), que son las siguientes:

- *Adj-RIB-in*: Hay tantas tablas de este tipo como pares BGP. En esta tabla se almacenan prefijos aprendidos de un *router* vecino particular.
- *Loc-RIB*: Hay solo una por cada AS. Almacena las mejores rutas seleccionadas que conoce el proceso BGP bien porque las ha obtenido de la tabla de enrutamiento o porque se han aprendido por BGP (I-BGP o E-BGP).
- *Adj-RIB-out*: Se tiene una tabla de este tipo por cada par BGP. Almacena prefijos para ser anunciados a otros *router*s vecinos.

La figura 1.25 indica los estados y mensajes del proceso BGP.

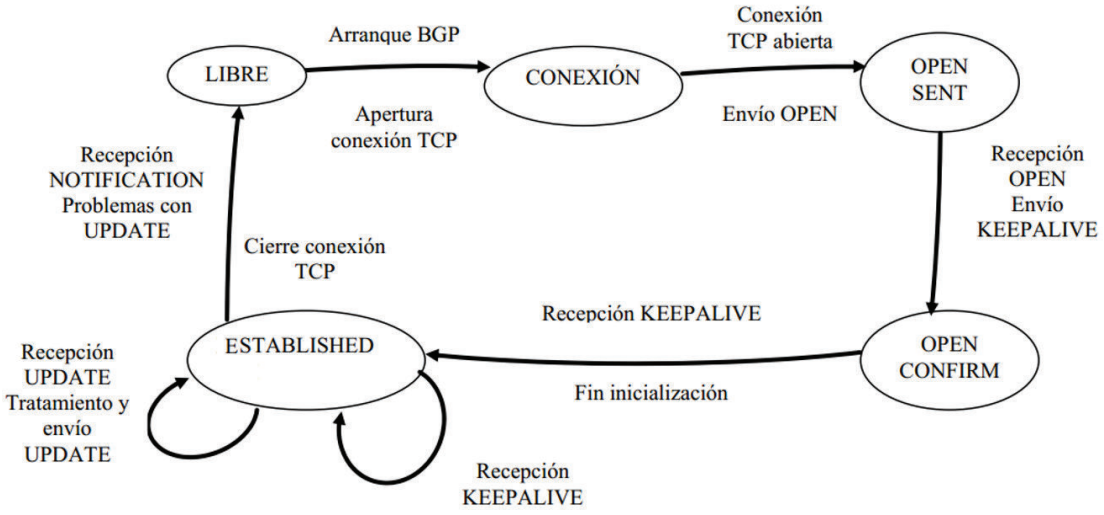


Figura 1.25 Estados y mensajes BGP

Los posibles estados son:

- Estado libre.
- En conexión: Uno de los extremos intenta una conexión TCP.
- Activo: Cuando uno de los extremos no puede establecer conexión y lo reintenta periódicamente.
- *Open Sent*: Cuando un extremo envía un mensaje de identificación.
- *Open Confirm*: Se recibe respuesta al mensaje de identificación.
- *Established*: Se aceptan las identificaciones y la sesión BGP está activa.

Los tipos de mensaje son los siguientes:

- *Open*: Este mensaje se envía tras el establecimiento de la conexión TCP, sirve para informar a los *router*s vecinos varios parámetros como la versión del protocolo BGP, el número de AS y el número identificador del proceso BGP. Una vez que se envía este mensaje, el proceso BGP se queda en espera de recibir un mensaje Keepalive.
- *Keepalive*: Este mensaje sirve como confirmación a un mensaje OPEN.
- *Notification*: Este mensaje sirve para cerrar la sesión BGP, cerrando la conexión TCP. El cierre de la sesión BGP anula las rutas aprendidas en la sesión.
- *Update*: Este mensaje se envía solo cuando existe algún cambio de enrutamiento y su recepción produce la activación del proceso BGP que se encargará de modificar las tablas RIB y de emitir a su vez un mensaje de *Update* hacia los *routers* vecinos.

El mensaje *Update* contiene información adicional asociada al prefijo de la ruta, estos atributos son los siguientes:

- *ORIGIN*: Indica la forma por la que se ha aprendido la ruta.
- *AS_PATH*: Este atributo contiene una lista con los números de los AS a seguir para llegar al destino, además sirve para la detección de *loops*.
- *NEXT-HOP*: Cuando un *router* BGP anuncia un prefijo a otro *router* BGP indica en este atributo la dirección del siguiente *router* para llegar al destino. Este atributo es útil en el caso de que el siguiente *router* no utilice BGP.

- *LOCAL_PREF*: Sirve para ponderar la prioridad de las rutas que se anuncian internamente en el AS mediante I-BGP. Este atributo se tiene en cuenta antes que el atributo *AS_PATH* al momento de seleccionar la mejor ruta hacia un destino.
- *WEIGHT*: Es propietario de *Cisco* y se utiliza como primer criterio de selección para obtener la mejor ruta cuando se tienen varias rutas hacia el mismo destino.
- *COMMUNITY*: Una comunidad es un grupo de prefijos que comparten propiedades comunes, este atributo permite agrupar los destinos en comunidades de destino. Cada destino puede ser miembro de varias comunidades. Para establecer la comunidad a la que pertenece un destino se puede utilizar la directiva *set community* en un *route-map.*

1.10 CARACTERÍSTICAS GENERALES DE MPLS[30]

MPLS es un mecanismo de envío de paquetes basado en etiquetas. Fue diseñado para soportar el envío de varios protocolos (multi-protocolo), así como para trabajar con cualquier encapsulación capa 2.

MPLS sobre ATM usa la cabecera ATM como etiqueta (*cell-mode MPLS),* aplicable solo para conmutadores ATM.

MPLS puede usar Frame Relay, ATM o el protocolo Punto a Punto (PPP) como capa de enlace; es escalable, capaz de funcionar en muchos ambientes incluso SDH y redes ópticas.

MPLS tiene mayor robustez sobre Frame Relay porque requiere menos ancho de banda y puede manejar un mayor *throughput*.

MPLS soporta tanto los Servicios Diferenciados (*DiffServ*) como los Servicios Integrados (*IntServ*) con el Protocolo de Reserva de Recurso (RSVP). Puede separar flujos de tráfico de acuerdo con las exigencias específicas de las clases de servicio (CoS).

Además, por medio del control de Ingeniería de Tráfico, MPLS soporta redes privadas virtuales (VPNs). Aunque MPLS VPNs no se encuentren encriptadas, proporcionan seguridad por medio de la especificación de rutas de flujo de tráfico y el ocultamiento de la dirección IP de destino de dispositivos intermedios.

La arquitectura MPLS tiene dos componentes principales: Plano de Control y el Plano de Datos.

1.10.1 PLANO DE CONTROL (*CONTROL PLANE*)

Realiza el intercambio de información de enrutamiento de capa 3 y etiquetas; contiene mecanismos avanzados para el intercambio de información de enrutamiento tal como: OSPF, EIGRP, IS-IS y BGP.

El plano de control utiliza dos fuentes de información: RIB y LIB.

1.10.1.1 Base de Información de Enrutamiento (RIB *Routing Information Base*)

Esta tabla proporciona información sobre la red destino y los prefijos de subred que se utilizan para la asociación de etiquetas, en esta tabla se encuentran todas las rutas aprendidas por cada uno de los nodos de la red MPLS.

1.10.1.2 Base de Información de Etiquetas (LIB *Label Information Base*)

En esta tabla se encuentran todas las etiquetas asignadas por el nodo MPLS local (etiquetas locales) y las asignaciones de dichas etiquetas a las etiquetas recibidas de los vecinos.

1.10.2 PLANO DE DATOS (*DATA PLANE*)

Define un mecanismo para conmutar los paquetes MPLS entrantes, basándose en las tablas de enrutamiento ofrecidas por el plano de control. Utiliza dos fuentes de información: FIB y LFIB.

1.10.2.1 Base de Información de Envío (FIB *Forwarding Information Base*)

Es una tabla que se utiliza para definir a qué interfaz se debe reenviar el paquete.

1.10.2.2 Base de Información de Reenvío de Etiquetas (LFIB *Label Forwarding Information Base*)

Esta tabla es utilizada para la conmutación de etiquetas. La LFIB usa un subconjunto de etiquetas contenidas en la LIB para el envío del paquete y almacena solo las etiquetas que en ese momento el plano de datos está usando, contiene la información de etiquetas e interfaces entrantes y salientes, y la dirección del próximo salto.

1.10.3 LDP (*LABEL DISTRIBUTION PROTOCOL*)

Es el protocolo utilizado para distribución de etiquetas MPLS. Define una serie de procedimientos y mensajes por los cuales un LSR (*Label Switch Router*) informa a otro de la asociación Etiqueta/FEC, y que será utilizado para el establecimiento de un LSP (*Label Switch Path*).

Dos LSRs que utilizan una sesión LDP para intercambiar la información de mapeo de etiquetas (*label mappings*), tienen una sesión LDP entre ellos (*LDP peers*). En una sola sesión, cada par es capaz de aprender sobre otros *label mappings*.

LDP permite a un LSR distribuir etiquetas a sus LDP *peers* usando el puerto TCP 646.

Existen varios mensajes LDP:

- Descubrimiento (*Discovery*): utilizados para anunciar y mantener la presencia de un LSR en la red. Usa mensajes *Hello* para aprender sobre otros LSRs con los cuales tiene una conexión LDP directa.
- Sesión (*Session*): Para que dos LDP *peers* intercambien información, ellos tienen que primero establecer una sesión LDP. Los mensajes sesión son

utilizados para establecer, mantener y terminar sesiones LDP entre LDP *peers*.

- Anuncio (*Advertisement*): Para crear, cambiar y borrar las asociaciones Etiqueta/FEC.
- Notificación (*Notification*): Provee información de asesoría e información de indicación de errores.

El mecanismo LDP establece las siguientes etapas:

- Descubrimiento LDP: permite a un LSR descubrir LDP *peers* potenciales.
- Establecimiento de la Sesión LDP: El intercambio de mensajes *Hello* entre dos LSRs activa el establecimiento de la sesión LDP. Se establece dos pasos:
    - Establecimiento de la conexión TCP: llevado a cabo por el LSR activo, el cual tiene el identificador LSR más alto.
    - Inicialización de la Sesión: se negocian los parámetros de la sesión intercambiando mensajes de Inicialización. Si el LSR que recibe el mensaje, contesta con un mensaje *KeepAlive* los parámetros son aceptados, caso contrario se envía un mensaje de notificación de error, rechazando la sesión.
- Distribución de Etiquetas

El intercambio de mensajes LDP se indica en la figura 1.26.

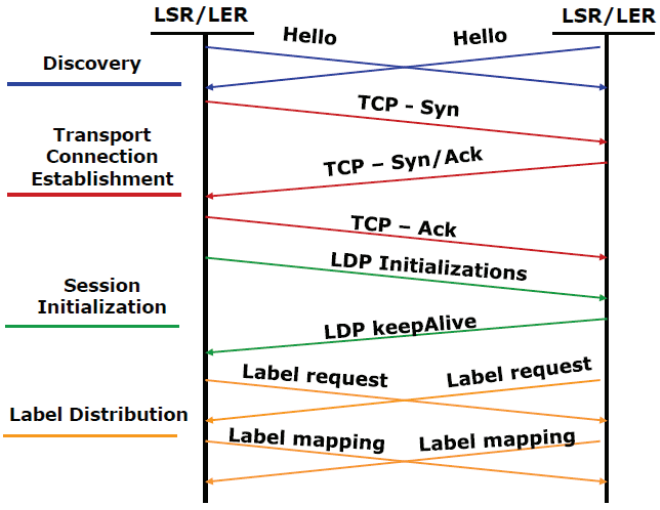


Figura 1.26 Intercambio de mensajes de LDP

1.10.4 LSP (*LABEL SWITCHING PATH*)

La ruta más corta por etiquetas se denomina camino conmutado de etiquetas (LSP).

1.10.5 CABECERA MPLS

En la figura 1.27 se presenta la cabecera MPLS en la que se observa una estructura de 32 bits que comprende los siguientes 4 campos: [31]

bits:	20	3	1	8
	Valor de la etiqueta	**EXP**	**S**	**TTL**

CAMPO	BITS	DESCRIPCIÓN
Etiqueta	20	Campo asignado para el rango de etiquetas (Los valores de 0 a 15 son reservados)
EXP	3	Campo experimental de 3 bits. Usado para realizar CoS (*Class of Service*)
S	1	MPLS permite que sean insertadas múltiples etiquetas. Este bit indica si es la última etiqueta en el paquete. Si el bit está en 1 indica que es la última etiqueta.
TTL	8	Propósito similar al de TTL en IP *Header*, usado para prevenir lazos infinitos de los paquetes.

Figura 1.27 Cabecera MPLS

1.10.6 FEC (*FORWARDING EQUIVALENCE CLASS)*

Generalmente una etiqueta está asignada a un FEC (*Forwarding Equivalence Class*). Una Clase Equivalente de Envío (FEC) es un conjunto de paquetes que han sido re-enviados en la misma manera. Entonces los paquetes con el mismo FEC son típicamente re-enviados sobre el mismo camino con el mismo tratamiento.

Las FECs pueden ser identificadas por direcciones de red, números de puerto, y tipos de protocolo. También se pueden identificar por tipo de paquete, tipo de la clase de servicio, o cabeceras de calidad de servicio *DiffServ*.

La FEC incluye:

- Un conjunto de paquetes *unicast* cuyas direcciones de red destino coinciden con un determinado prefijo de direcciones IP.
- Un conjunto de paquetes *multicast* con la misma dirección de origen y destino.
- Un conjunto de paquetes *unicast* cuyas direcciones de destino coinciden con un determinado prefijo de direcciones IP y cuyos bits de tipo de servicio (ToS) son los mismos.

1.10.7 LSR DE BORDE (*EDGE LABEL SWITCH ROUTER)*

En el ingreso de la nube MPLS el *router* LSR de borde (*Edge Label Switch Router*) o LER (*Label Edge Router*) determinará la Clase Equivalente de Envío (FEC), procesa, analiza, clasifica, filtra el paquete ingresado y le asigna e inserta la cabecera MPLS entre la cabecera de capa 2 de la trama y la cabecera de capa 3 del paquete.

1.10.8 MODO DE OPERACIÓN

Las siguientes acciones son posibles en los LER:

- Un paquete IP recibido es re-enviado basado en su dirección IP destino y es enviado como paquete IP.
- Un paquete IP recibido es re-enviado basado en su dirección IP destino y es enviado como paquete etiquetado.
- Un paquete etiquetado recibido es re-enviado basado en la etiqueta, la etiqueta es cambiada y el paquete etiquetado es enviado.
- Un paquete etiquetado recibido es re-enviado basado en la etiqueta, la etiqueta es retirada y el paquete IP es enviado.

Cuando la red no está configurada apropiadamente se puede presentar que el paquete etiquetado es eliminado si la etiqueta no se encuentra en la tabla LFIB,

incluso si el destino IP existe en la tabla de enrutamiento IP (*FIB Forwarding Information Base*).

Mientras que el paquete IP es eliminado si el destino no es encontrado en la FIB, incluso si existe un LSP MPLS hacia el destino.

El *router* LER inserta una etiqueta MPLS en cada trama o celda; típicamente inserta la etiqueta MPLS en un encabezado de capa 2. Si no hay suficiente espacio para la etiqueta en la cabecera, se coloca la etiqueta en el campo de datos de la celda o trama y se añade un pequeño campo de referencia en la cabecera, que el *router* puede usar para encontrar la etiqueta.

Para las celdas ATM, la etiqueta MPLS se coloca en el campo de Identificador de camino virtual o en el campo de identificador de canal virtual (VPI / VCI). En Frame Relay la etiqueta se inserta en el campo DLCI, como se ilustra en la figura 1.28.

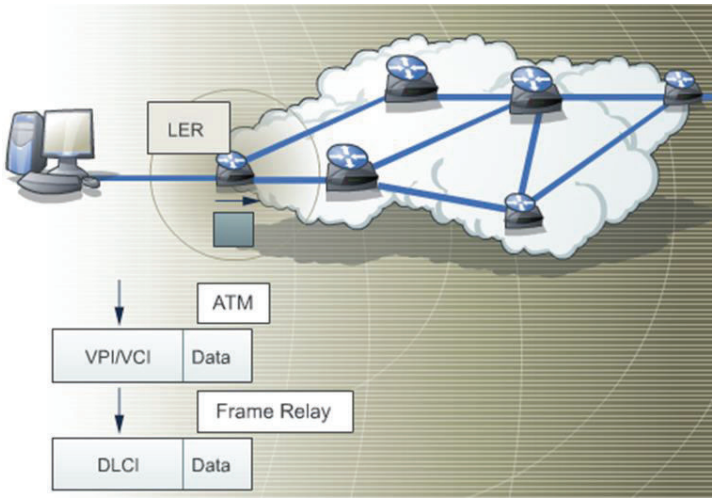


Figura 1.28 Etiquetas en ATM y Frame Relay [32]

Cuando un paquete etiquetado es recibido por un *router* conmutador de etiquetas LSR (*Label Switching Router*) en la nube MPLS se examina la etiqueta y basado en el contenido de la etiqueta el *router* efectuará una operación *SWAP,* donde la etiqueta se cambia por otra, en base al contenido de la LFIB y el paquete se envía en el camino asociado a esta nueva etiqueta. Se puede realizar una operación

PUSH cuando una nueva etiqueta se coloca encima de otra, de manera que la nueva etiqueta encapsula a la anterior.

Igualmente se puede realizar una operación POP en la que se remueve la etiqueta a la salida de la nube o un salto antes (*PHP Penultimate Hop Popping*); este procedimiento de retirar la etiqueta en el penúltimo salto es útil para disminuir el procesamiento del último *router* de borde LER.

Por lo general solo se asigna una etiqueta al paquete, pero puede existir más de una etiqueta (Pila de Etiquetas) como se indica en la figura 1.29.

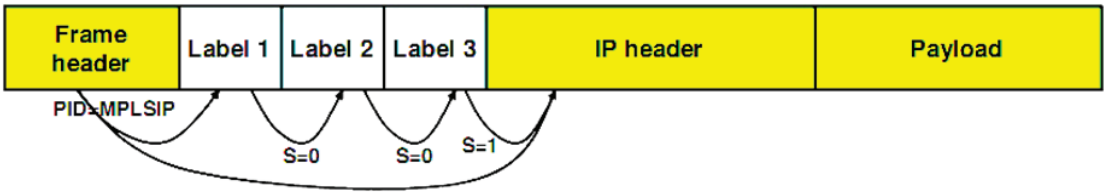


Figura 1.29 *Stack* de Etiquetas [33]

El protocolo identificador PID (*Protocol Identifier*) ubicado en la cabecera de capa 2 especifica que el *payload* comienza con una etiqueta o etiquetas y a continuación viene la cabecera IP.

El bit *botton of stack* (s) indica si el siguiente campo es otra etiqueta o la cabecera IP. El *router* final usa solo la etiqueta *top*.

En los siguientes casos se permitiría utilizar más de una etiqueta:

- MPLS VPNs: La etiqueta *top* indica al *router* siguiente que la segunda etiqueta identifica una VPN.
- MPLS TE: Se puede usar dos o más etiquetas, donde la etiqueta *top* indica el punto final de un túnel de *traffic engineering* y la segunda etiqueta indica el destino.
- MPLS VPNs combinado con MPLS TE usa tres o más etiquetas.

Las aplicaciones se diferencian por las funciones que realizan en el panel de control, pero usan un mismo panel de datos para la conmutación de etiquetas y reenvío.

1.10.9 APLICACIONES MPLS

1.10.9.1 *Unicast* IP *Routing*

Esta configuración requiere un protocolo de enrutamiento IP que brinde la información sobre cómo alcanzar las redes, y un protocolo de distribución de etiquetas que enlace las etiquetas y las redes a través del protocolo de enrutamiento. La FEC es igual a una red de destino almacenada en la tabla de enrutamiento IP.

La calidad de servicio se añade a *IP Unicast Routing* con la finalidad de proveer servicios diferenciados.

1.10.9.2 *Multicast* IP *Routing*

El protocolo PIM v2 (*Protocol Independent Multicast*) se usa para propagar la información de enrutamiento y las etiquetas. La FEC es igual a la dirección *multicast* de destino.

1.10.9.3 MPLS TE

Cada LSR debe ver toda la topología de la red, y necesita información adicional como recursos disponibles y restricciones. RSVP o CR-LDP se usan para establecer túneles TE y para propagar las etiquetas.

1.11 CARACTERÍSTICAS E IMPLEMENTACIÓN DE QoS SOBRE VPNs CAPA 3

1.11.1 CONCEPTO DE REDES PRIVADAS VIRTUALES

Las redes virtuales están clasificadas en tres grupos: redes privadas virtuales (VPN), redes privadas por *dialup* y las redes LAN virtuales.

Esta clasificación se indica en la figura 1.30.

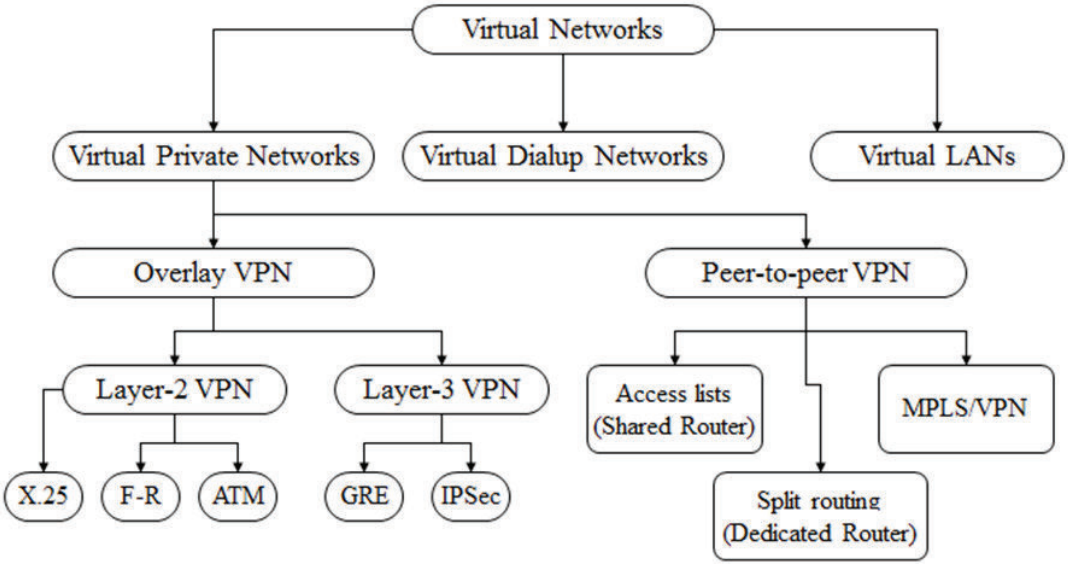


Figura 1.30 Clasificación de redes virtuales [34]

Las VPNs reemplazan a los enlaces dedicados punto a punto al compartir una infraestructura de red común, reduciendo considerablemente los precios tanto para el proveedor como para el usuario.

Los servicios de VPNs pueden ser ofrecidos en base a dos modelos principales: *Overlay* VPNs y *Peer to Peer* VPNs.

1.11.1.1 Modelo *Overlay VPNs*

Este modelo se tiene cuando el proveedor de servicios ofrece enlaces privados punto a punto virtuales entre los distintos sitios del cliente sin intervenir en el ruteo. Se puede implementar usando tecnologías de capa 1 (ISDN, E1 < T1< DS0), de capa 2 como X.25, FR o ATM por medio de PVCs y de capa 3 por medio de túneles (Ipsec, GRE).

Los PVCs deben ser realizados manualmente y requieren una topología *full mesh* de circuito virtuales. Se permite la duplicidad de direcciones.

Los CPEs extremos arman una adyacencia con un protocolo de ruteo y se ven entre ellos directamente, como se muestra en la figura 1.31.

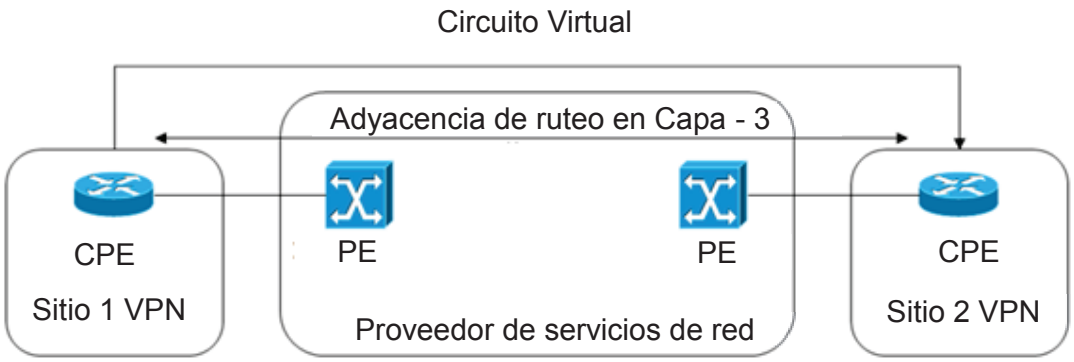


Figura 1.31 *Overlay VPNs*

1.11.1.2 Modelo *Peer to Peer VPNs*

Cuando el proveedor de servicios interviene en el enrutamiento, se garantiza un fácil ruteo entre los sitios del cliente.

El proveedor de servicio necesita una información detallada sobre el enrutamiento IP, y no se permiten duplicidad de direcciones.

El CPE llega por medio de ruteo hacia el equipo de borde PE, donde se comparten recursos. El PE es el encargado de redistribuir hacia el extremo remoto por medio de la nube. La nube es la encargada de realizar el mallado, como se ilustra en la figura 1.32.

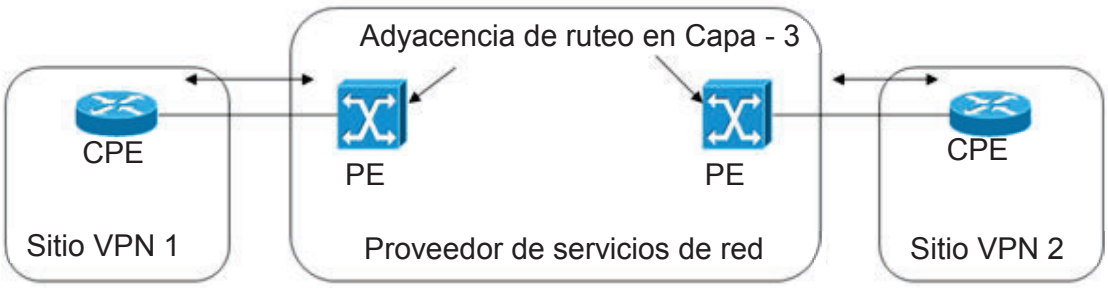


Figura 1.32 *Peer to Peer VPNs*

1.11.2 TOPOLOGÍAS VPN

Las topologías VPN generalmente se dividen en:

1.11.2.1 *Hub and spoke*

Muchos sitios *spoke* están conectados al sitio central del cliente (*hub*) sin que estén entre ellos conectados

1.11.2.2 *Full mesh*

Permite tener un circuito virtual dedicado entre dos sitios cualesquiera del cliente.

1.11.2.3 *Partial mesh*

Reduce el número de circuitos virtuales entre los sitios más relevantes del cliente.

1.11.3 MODELO MPLS VPN

MPLS VPN combina las mejores características de *Overlay* VPN (la seguridad y el aislamiento entre los clientes) y *Peer to Peer* VPN (simplificar el enrutamiento del cliente) de la siguiente manera: [35]

Los *routers* de borde participan en el enrutamiento del cliente, garantizando un óptimo enrutamiento entre los sitios del cliente; además permiten rutas separadas para cada cliente, con lo que se consigue aislar completamente los clientes. De esta manera los clientes pueden tener duplicidad de direcciones.

MPLS VPN divide a la red en una red controlada por el cliente y una red controlada por el proveedor de servicios.

Sitios cercanos al cliente se unen con los *routers* de borde (PE) por medio de un *router* de cliente (CE); los *routers* P se denomina a los *routers* de *core* del proveedor.

Para propagar la información se puede intercambiar la información de enrutamiento de los clientes entre los *routers* de borde del proveedor, corriendo un protocolo IGP por cada cliente que atraviese la red del proveedor. Esta forma de propagación no es adecuada y se la ilustra en la figura 1.33 que a pesar de ser una solución simple no es escalable.

Además los *routers* de *core*, llevan tráfico de cada cliente y los *routers* de *borde* tienen que procesar un gran número de protocolos de enrutamiento.

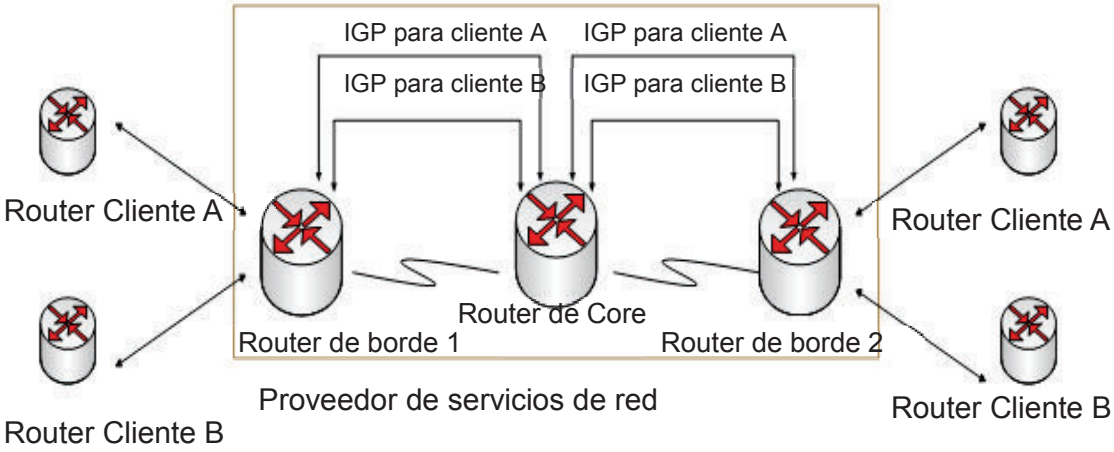


Figura 1.33 Solución con IGP

Otra opción es propagar la información usando un protocolo de enrutamiento, tal como se indica en la figura 1.34. El protocolo de enrutamiento llevaría todas las rutas de los clientes a través del *backbone* del proveedor. Sin embargo todavía los *routers* de *core* están involucrados en el enrutamiento del cliente.

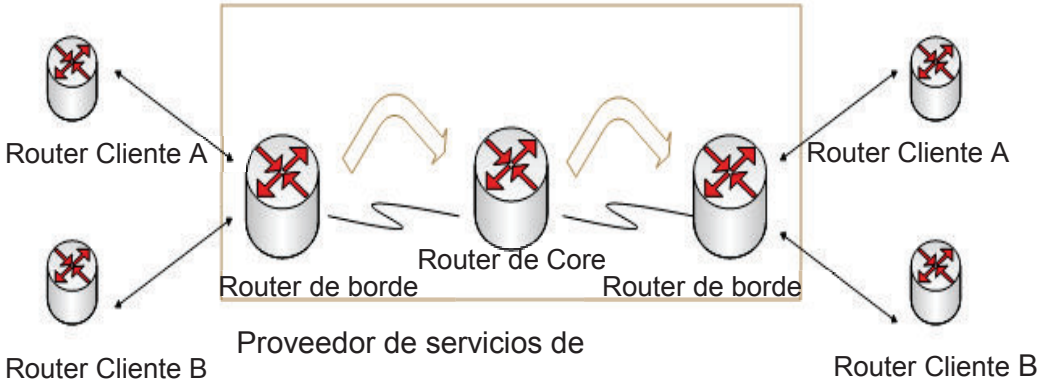


Figura 1.34 Solución con protocolos de enrutamiento.

La solución más conveniente es ejecutar un solo protocolo que lleve todas las rutas del cliente entre los *routers* de borde del proveedor y usar etiquetas MPLS para intercambiar paquetes entre los *routers* de borde, opción ilustrada en la figura 1.35. De esta manera no se involucra a los *routers* de *core* en transportar las rutas del cliente sino solo los *routers* de borde, además se ofrece escalabilidad ya que el número de protocolos de enrutamiento no se incrementa con el incremento del número de clientes.

BGP es el protocolo dedicado al transporte de rutas del cliente entre los *routers* de borde del proveedor. Para evitar la duplicidad de direcciones de subred de los clientes se debe expandir los prefijos IP del cliente, consiguiendo tener un único prefijo que haga única a las direcciones IP de los clientes.

El Distintivo de Ruta RD (*Route Distinguishers*) es un prefijo de 64 bits, que permite convertir una dirección del cliente de 32 bits en una única dirección del cliente de 96 bits llamada dirección VPNv4, que puede ser transportada entre los *routers* de borde del proveedor.

Un RD es de 64 bits de longitud que comprende los siguientes campos: Tipo, Administrador, y Número Asignado. La interpretación del campo Valor depende del valor del campo Tipo. En la actualidad, se han definido tres valores del campo de tipo que son: 0, 1, y 2.

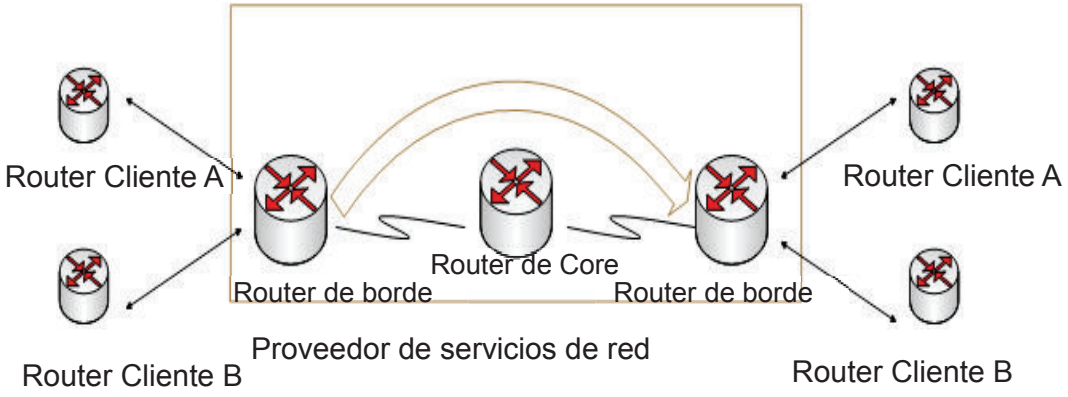


Figura 1.35 Solución con un único protocolo de enrutamiento

- Tipo 0: El subcampo administrador contiene el número de sistema autónomo (ASN). Si este ASN es del espacio público ASN, debe ser asignado por la autoridad competente (se rechaza el uso de valores ASN del espacio de ASN privados). Mientras que el subcampo número asignado contiene un número de un espacio de numeración que es administrado por la empresa a la cual el ASN ha sido asignado por una autoridad competente.

- Tipo 1: El subcampo administrador contiene una dirección IP. Si esta dirección IP es del espacio de direcciones IP públicas, que debe ser asignado por una autoridad competente (se rechaza el uso de direcciones del espacio de direcciones IP privadas).

  El subcampo número asignado contiene un número de un espacio de numeración que es administrado por la empresa a la que se ha asignado la dirección IP.

- Tipo 2: El subcampo administrador contiene un número de sistema autónomo de 4 bytes [BGP- AS4] .Si este ASN es del espacio público ASN, que debe haber sido asignado por la autoridad competente (se rechaza el uso de valores ASN del espacio ASN privado).

  El subcampo número asignado contiene un número de un espacio de numeración que es administrado por la empresa a la que el ASN ha sido asignado por una autoridad competente.

En la tabla 1.5 se especifican los tipos de *Route Distinguisher* (RD)

Campo Tipo (2 bytes)	Campo Valor (6 bytes)	
	Subcampo Administrador	Subcampo Número Asignado
Tipo: 0	2 bytes ASN	4 bytes
Tipo: 1	4 bytes IP	2 bytes
Tipo :2	4 bytes ASN	2 bytes

Tabla 1.5 Tipos de RD [36]

El BGP que soporta otras familias de direcciones adicionales a las direcciones IPv4 es llamado Multiprotocolo BGP (MP-BGP). Las sesiones MP-BGP tienen que ser ejecutadas entre las interfaces de *loopback*.

Generalmente MPLS VPN se usa dentro de un mismo sistema autónomo por lo que la sesión BGP ente los *routers* de borde es una sesión IBGP.

El transporte de rutas a través de MPLS VPN realiza el siguiente proceso:

1. El *router* del cliente envía una actualización de enrutamiento IPv4 al *router* de borde del proveedor.
2. El *router* de borde coloca un RD de 64 bits a la actualización de enrutamiento IPv4 obteniendo un prefijo único VPNv4
3. El prefijo VPNv4 se propaga a través de la sesión MP-IBGP a los otros *routers* de borde.
4. El *router* de borde que recibe la VPNv4 retira el RD obteniéndose nuevamente el prefijo IPv4.
5. Este prefijo es enviado al otro *router* del cliente dentro de la actualización del enrutamiento IPv4.

Este procedimiento se indica en la figura 1.36.

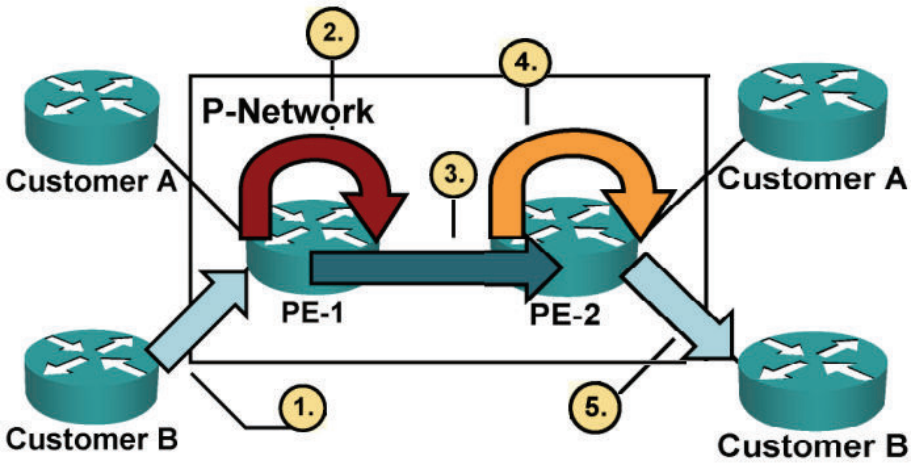


Figura 1.36 Transporte MPLS VPN [37]

Algunos clientes necesitan participar en más de una VPN. El RD no se puede utilizar como identificativo en más de una VPN. El RT (*Route Target*) permite especificar qué comunidad se añadirá a la dirección IPV4 por medio de la opción *export* y también especifica las comunidades que ingresan a la tabla VRF por medio de la opción *import*. RT se crea dentro de MPLS VPN para soportar complejas topologías VPN.

La tabla de enrutamiento virtual (VRF *Virtual Routing and Forwarding Table*) se usa para enrutamiento y envío de información de un grupo de lugares con idénticos requerimientos de conectividad. Está asociada con el RD y con el RT. El RD sirve para distinguir a una tabla VRF; si no se configura el RD la tabla VRF no funciona.

Las interfaces VPN pueden ser interfaces físicas, subinterfaces e interfaces lógicas que son asignadas a las VRFs.

Pueden existir muchas interfaces por VRF, pero cada interfaz es asignada a solo una VRF.

1.11.3.1 Establecimiento de la sesión MP- IBGP

Las sesiones MP-BGP tienen que ser ejecutados entre las interfaces de *loopback* y se sigue el siguiente proceso:

1.11.3.1.1 Definición del neighbor

Es la dirección IP de la interfaz de *loopback* en el *router* de borde del otro extremo. El sistema autónomo es el mismo debido a que se tiene una misma sesión IBGP.

Ejemplo: Router(config)# router bgp 27757
Router(config-router)#neighbor 10.15.200.39 remote as 27757

1.11.3.1.2 Definición de la IBGP

Es necesario realizar las actualizaciones BGP desde la interfaz identificada como el origen de toda actualización. La *loopbak* 100 es la interfaz estándar de MPLS.

Ejemplo: Router(config-router)#neighbor 10.15.200.39 update-source loopback 100

1.11.3.1.3 Activación de la sesión VPNv4

Permite ingresar parámetros específicos VPNv4. Por defecto siempre está activa.

Ejemplo: Router(config-router)#address-family vpnv4
Router(config-router-af)#neighbor 10.15.200.39 activate

1.11.3.1.4 Definición del próximo salto

Es necesario debido a que en la tabla de enrutamiento del BGP, es importante que se defina como próximo salto al *neighbor* MPLS donde se originó la ruta.

Ejemplo: Router(config-router-af)#neighbor 10.15.200.39 next-hop-self

1.11.3.1.5 Habilitación de comunidades

Es necesario para habilitar el transporte de comunidades estándar y extendidas a través de la sesión IBGP.

Ejemplo: Router(config-router-af)#neighbor 10.15.200.39 send-community both

1.11.3.1.6 Configuración de la VRF

Las tablas VRFs se configuran únicamente en los *routers* de borde y se asigna un único RD para la tabla VRF. Las VRF tienen significado local.

Ejemplo: Router(config)# ip vrf name

1.11.3.1.7 Definición de un RD

Con el RD se distingue una tabla VRF. Por ejemplo:

Router(config-vrf)#rd route-distinguisher

1.11.3.1.8 Definición de un RT

Se define por medio de siguiente comando:

Router(config-vrf)#route-target [both|export|import] RT

1.11.3.2 Diseño de QoS MPLS VPN

El diseño de QoS MPLS VPN puede verse desde dos perspectivas distintas:

- Desde el cliente empresarial subscrito a un servicio MPLS VPN.
- Desde el proveedor de servicio provisionando QoS a nivel de equipos de *edge* y *core* dentro del servicio MPLS VPN.

Para alcanzar los niveles de servicio de extremo a extremo, ambos diseños de QoS deben ser consistentes y complementarios.

MPLS es una combinación de enrutamiento y tecnologías de conmutación que pueden proporcionar las VPN escalables con la calidad de servicio de extremo a extremo.

MPLS VPN provee servicios virtuales WAN de capa 3 totalmente mallados interconectando a todos los *routers* CE. En cambio, la mayoría de diseños WAN de capa 2 giran en torno a un modelo de *hub-spoke*, donde el QoS principalmente se administra en el *router hub* por la empresa.

Políticas de encolamiento son obligatorias en los *routers* CE y PE por las implicaciones de una red MPLS VPN completamente mallada para hacer cumplir los SLA.

Mientras que las políticas de calidad de servicio en los *routers* P de *core* son opcionales, dependiendo del aprovisionamiento por parte del proveedor de servicio en su red de *backbone* MPLS. O por el contrario otros proveedores pueden implementar políticas *DiffServ* o incluso podrían desplegar la ingeniería de tráfico MPLS (MPLS TE) para manejar escenarios de congestión dentro de sus redes troncales.

En la figura 1.37 se indica los puntos en la red donde se puede aprovisionar las políticas de calidad de servicio dentro de una arquitectura MPLS VPN.

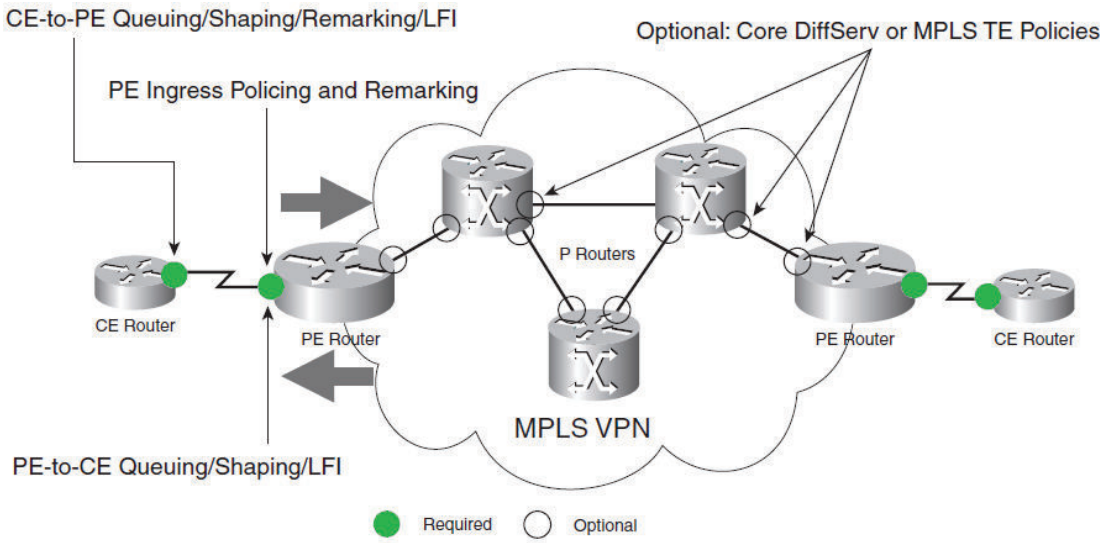


Figura 1.37 QoS requerido en una arquitectura MPLS VPN.

1.11.3.2.1 Consideración de diseño de QoS a nivel de CE

Estas consideraciones se deben tomar en cuenta para el diseño de MPLS VPN QoS CE:

- Diseño de la calidad de servicio en el acceso a nivel de capa 2. La mayoría de los proveedores soporta *Frame Relay* y ATM como medios de acceso, esto hace que la migración de WANs capa 2 a MPLS VPNS capa 3 sea sencillo de administrar. Además algunos proveedores soportan Ethernet como un medio de acceso y garantizan usualmente un CIR.

- Acuerdos de SLA con el proveedor de servicios. Se contemplan los requisitos de extremo a extremo de SLA de voz y vídeo interactivo que son los siguientes:
  - No más de 150 ms de latencia de un solo sentido. (por norma ITU G.114).
  - No más de 30 ms de *jitter.*
  - No más del 1 por ciento en pérdida de paquetes.

- Modelos de mapeo entre empresa y proveedor de servicio: Las siguientes indicaciones se deben recordar al momento de decidir la mejor forma de integrar las clases empresariales en los modelos de calidad de servicio del proveedor de servicios.

- La voz y vídeo no deben asignarse ambos en una cola de baja latencia (LLQ), porque los paquetes normalmente no están fragmentados y pueden causar retrasos excesivos para los paquetes de VoIP en los enlaces de baja velocidad.
- VoIP requiere el aprovisionamiento no solo del tráfico de voz por RTP, sino también del tráfico de señalización de llamada, que es muy ligero y requiere solo una cantidad moderada de ancho de banda garantizado.
- Por lo general no se debe mezclar el tráfico basado en TCP con tráfico basado en UDP (especialmente *Streaming* de Video) dentro de una sola clase debido a los diferentes comportamientos de estos protocolos durante períodos de congestión, donde los flujos TCP reducen sus tasas de transmisión, lo que renuncia a su ancho de banda para los flujos UDP que son descartados. No siempre es posible separar los flujos TCP y UDP pero es beneficiosos en lo posible hacerlo.
- La mayoría de los proveedores de servicios usan atributos de marcado de capa 3 (IPP o DSCP). Por lo tanto, las empresas deben marcar o remarcar su tráfico con un criterio consistente a su proveedor de servicio. Y si el cliente requiere un remarcado se recomienda realizarlo a la salida del *router* CE.

Se tienen modelos de 3, 4 y 5 clases, donde las aplicaciones de una empresa tienen su correspondencia con las clases definidas por parte del proveedor de servicios en el PE. A continuación se indica un modelo de 5 clases.

1.11.3.2.2 Modelo y remarcado de 5 clases de servicio

En este modelo, el proveedor de servicios ofrece cinco clases de servicio: tiempo real (prioridad estricta), los datos críticos (ancho de banda garantizado), Video, datos masivos y mejor esfuerzo, como se indica en la figura 1.38.

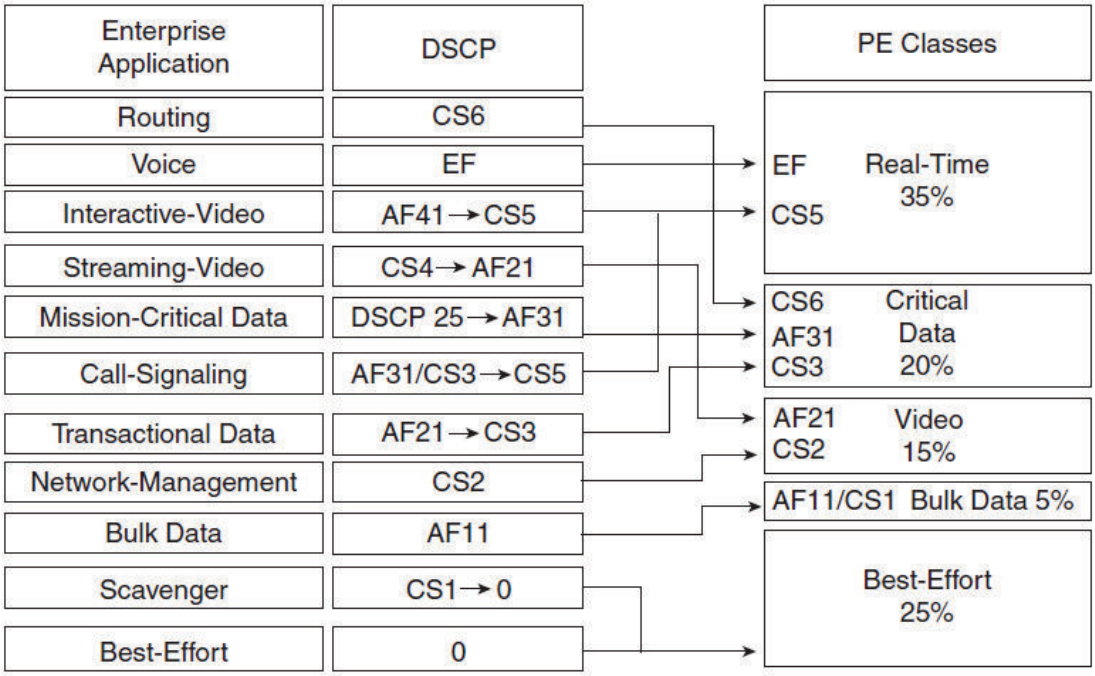


Figura 1.38 Modelo de 5 clases y diagrama de remarcado

El criterio de admisión para la clase en tiempo real es o DSCP EF o CS5.

El criterio de admisión para los datos críticos es DSCP CS6, AF31, o CS3.

El criterio de admisión para la clase video es o DSCP AF21 o CS2. Esta clase se puede utilizar para *streaming* de video y para la administración del tráfico de la red.

El criterio de admisión para los datos masivos es o DSCP AF11 o CS1.

Ejemplo de configuración en el *router* CE para el modelo de 5 clases. [38]

```
class-map match-all ROUTING
match ip dscp cs6
class-map match-all VOICE
match ip dscp ef
class-map match-all INTERACTIVE-VIDEO
match ip dscp af41
class-map match-all STREAMING-VIDEO
match ip dscp cs4
class-map match-all MISSION-CRITICAL-DATA
match ip dscp 25
class-map match-any CALL-SIGNALING
match ip dscp af31
match ip dscp cs3
class-map match-all TRANSACTIONAL-DATA
match ip dscp af21
class-map match-all NETWORK-MANAGEMENT
```

```
match ip dscp cs2
class-map match-all BULK-DATA
match ip dscp af11
class-map match-all SCAVENGER
match ip dscp cs1
!
!
policy-map CE-FIVE-CLASS -MODEL
class ROUTING
bandwidth percent 3 ! Ruteo es asignado por defecto a la clase crítica.
class VOICE
priority percent 18 ! Voz es admitido en la clase en tiempo real
class INTERACTIVE-VIDEO
priority percent 15
set ip dscp cs5 ! Video interactivo se asigna al tiempo real
class STREAMING-VIDEO
bandwidth percent 13
set ip dscp af21 ! Transmisión de vídeo se asigna a la clase video
class CALL-SIGNALING
priority percent 2 !
set ip dscp cs5 !  Señalización de llamada se asigna a la clase en tiempo real
class MISSION-CRITICAL-DATA
bandwidth percent 12
random-detect
set ip dscp af31 ! Los datos críticos se asignan a la clase crítica
class TRANSACTIONAL-DATA
bandwidth percent 5
random-detect
set ip dscp cs3 ! Datos transaccionales se asigna a la clase crítica.
class NETWORK-MANAGEMENT
bandwidth percent 2 ! Gestión de red es admitida en la clase video

class BULK-DATA
bandwidth percent 5 ! Datos Masivos es asignado a la clase de datos masivos.
random-detect
class SCAVENGER
bandwidth percent 1
set ip dscp 0 ! Scavenger es re- marcado a 0
class class-default
bandwidth percent 24
random-detect
```

Ejemplo de configuración en el *router* PE para el modelo de 5 clases.

```
class-map match-any REALTIME
match ip dscp ef
match ip dscp cs5
class-map match-any CRITICAL-DATA
match ip dscp cs6
match ip dscp af31

match ip dscp cs3
class-map match-any VIDEO
```

```
match ip dscp af21
match ip dscp cs2
class-map match-any BULK-DATA
match ip dscp af11
match ip dscp cs1
!
policy-map PE-FIVE-CLASS- -MODEL
class REALTIME
priority percent 35 ! Clase de tiempo real obtiene el 35% LLQ
class CRITICAL-DATA
bandwidth percent 20 ! Critical-Data class obtiene el 20% CBWFQ
random-detect dscp-based ! DSCP-based WRED habilitado en la clase datos críticos.
class VIDEO
bandwidth percent 15 ! La clase video obtiene el 15% CBWFQ
random-detect dscp-based ! DSCP-based WRED habilitada en la clase video
class BULK-DATA
bandwidth percent 5 !  La clase Bulk Data obtiene el 15% CBWFQ
random-detect dscp-based ! DSCP-based WRED habilitada en la clase Bulk Data
class class-default
bandwidth percent 25 ! La clase Best Effort obtiene el 25% CBWFQ
random-detect ! WRED habilitado en la clase Best Effort
```

CAPÍTULO 2
REQUERIMIENTOS DE COMUNICACIONES DE LA EMPRESA

2.1 GENERALIDADES

La entidad financiera provee a la sociedad un portafolio de servicios, donde se demanda una alta disponibilidad de la red. Esto conlleva que periódicamente se actualicen los sistemas, se realicen tareas de respaldo, se efectúen auditorías y mantenimientos programados.

La disposición en el mercado de varias entidades financieras da lugar a que el servicio diferenciado sea una ventaja competitiva, siendo vital que las operaciones transaccionales no sean interrumpidas, para de esta manera ser un aliado estratégico con el cliente.

2.2 SITUACIÓN ACTUAL DE LA EMPRESA

La entidad financiera posee varias agencias ubicadas en la ciudad de Quito y Guayaquil, con diferentes tipos de acceso, manejando internamente políticas de seguridad y control para proteger la información.

Los equipos de comunicación en la sede Matriz y en la agencia principal en Guayaquil se ubican en *racks*; tienen alimentaciones reguladas, con sistema de aire acondicionado, sistema contra incendios y generadores eléctricos como respaldo de energía.

Internamente el cableado se encuentra canalizado e instalado, empleando para el cableado vertical y horizontal cable UTP categoría 5e. Además se cuenta con *patchpanels* y *switches* de marca 3COM en la LAN.

Se intercambian actualizaciones de la base de datos entre las agencias conectadas en Quito y Guayaquil.

Actualmente la empresa tiene implementada una solución principalmente por medio de una red *legacy* con enlaces transparentes (*Clear Channel*) y tecnología *Frame Relay*. Posee un solución en topología en estrella extendida con la matriz ubicada en Quito hacia la cual se comunican varias agencias; y, una sucursal principal Guayaquil a la que convergen otras sedes.

2.2.1 ORGANIGRAMA

La figura 2.1 muestra la estructura orgánica de la entidad financiera que cuenta con varios departamentos administrativos y operativos.

- Departamento de Operaciones: Es el responsable de la seguridad de la información a nivel nacional, asi como de comprobar que los enlaces permanezcan activos, habilitar los enlaces de *backup*, administrar los equipos *Firewall* y dar soporte en hardware y software a los equipos de *internetworking*.

- Departamento de Sistemas: Es el encargado de mantener la operación de aplicativos y servicios de los usuarios de la LAN, otorgar diferentes perfiles de usuario, habilitar permisos de acceso a los usuarios por medio de tarjetas de proximidad y de la seguridad física de las sedes.

- Departamento Financiero: Responsable de los análisis de activos, inversiones, fondos, gastos y utilidades netas de la corporación.

- Departamento Comercial: Alli se encuentran los asesores y ejecutivos encargados de los contratos, tarjetas de crédito, pólizas, seguros y el portafolio de servicios que ofertan al cliente.

- Departamento de Servicios Bancarios: Apoya en la operación de la entidad con el servicio al cliente en cajas, balcón de servicios, recepción de créditos y préstamos.

- Departamento de Red de Agencias: Los supervisores o jefes de las sucursales son los responsables de la operación de cada una de las agencias a cargo. De requerir asistencia técnica lo direcciona a la sede Matriz con el departamento respectivo.

- Departamento Legal: Es el encargado de los procesos jurídicos de adquisición de equipos. Además determina, verifica y supervisa los términos y condiciones de contratos, gestiona los procesos contractuales y notariza los contratos.

- Departamento de Planeación y Desarrollo: Realiza modelos del comportamiento de mercado, determina premisas de inversión, compra de activos, compra o venta de acciones y planifica nuevos servicios hacia otros segmentos del mercado.

2.2.2 TOPOLOGÍA DE LA RED

En la figura 2.2 se muestra la topología de servicios, donde el servicio de *Internet* se ofrece por medio de un enlace dedicado hacia la Matriz ubicada en Quito con relación 1:1 sin compartición, por lo cual las sedes ubicadas en Guayaquil, saldrán por el enlace Quito-Guayaquil.

La entidad cuenta en Quito y en Guayaquil con servidores de correo electrónico y de dominio. Por temas de seguridad se tiene implementado un *firewall* en la sede Matriz Quito.

La figura 2.3 muestra las conexiones lógicas de las diferentes sedes con la descripción del medio de acceso de última milla para la red de la Entidad Financiera.

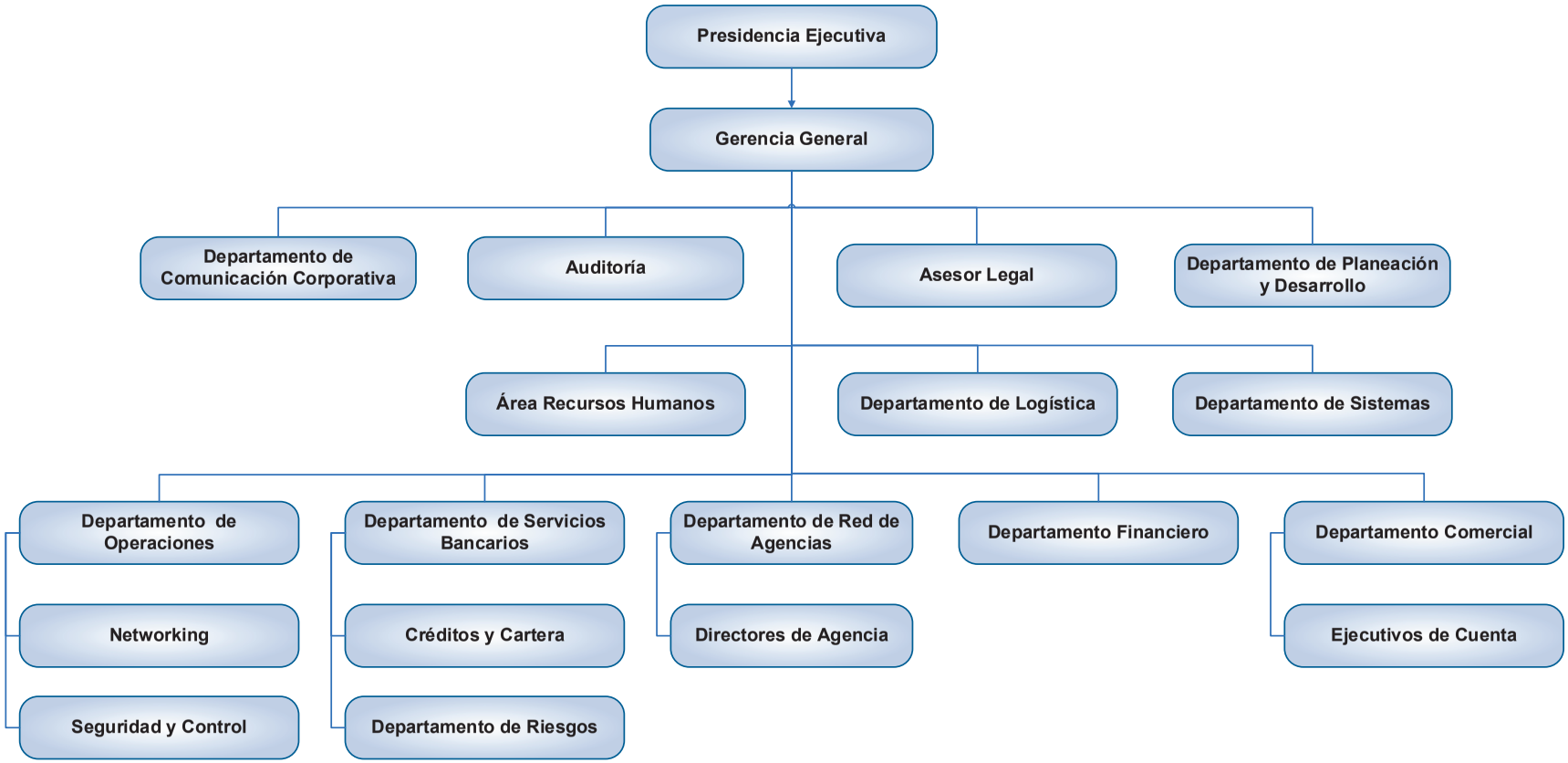


Figura 2.1 Estructura Orgánica Institucional

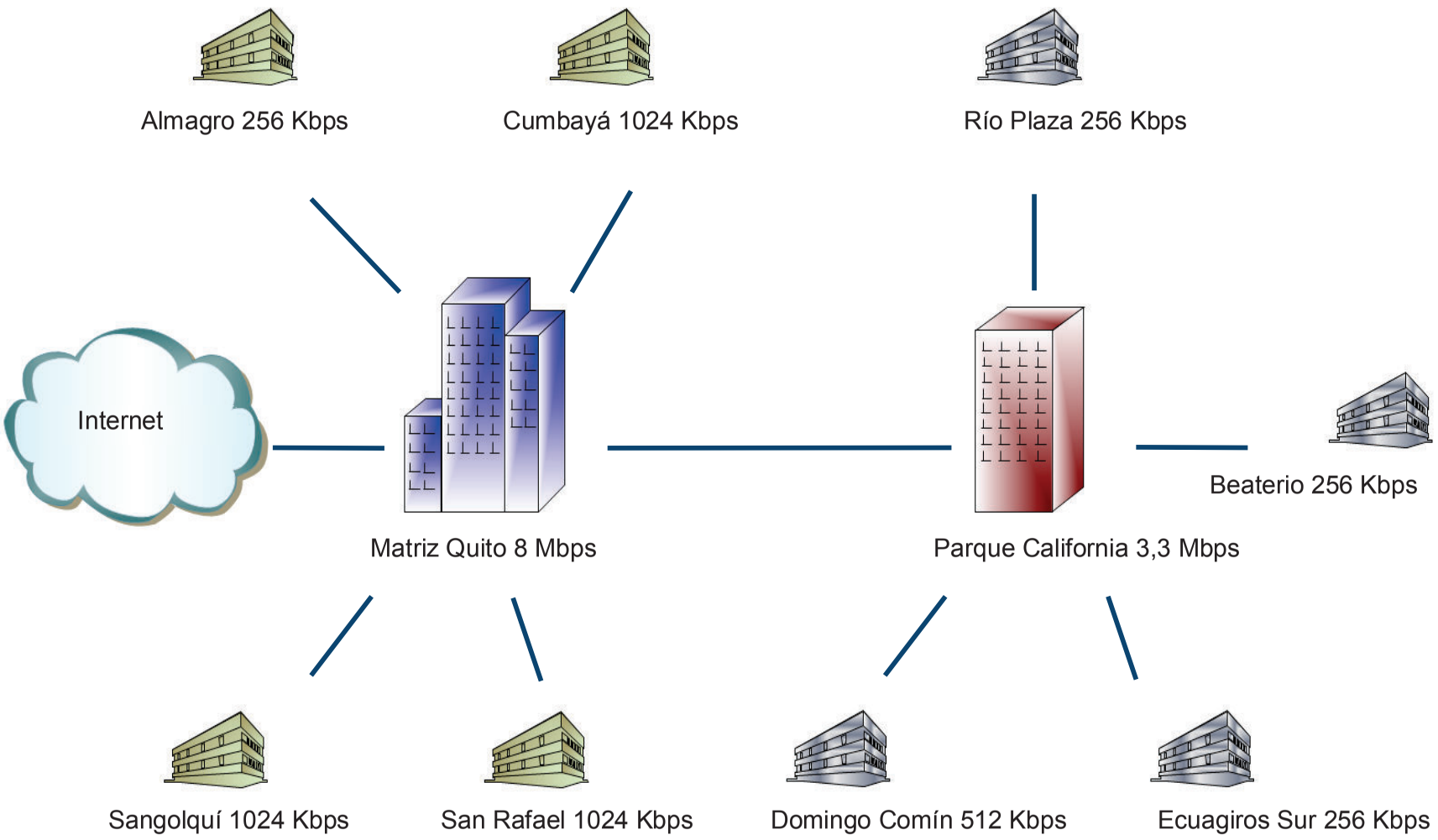


Figura 2.2 Topología de servicios

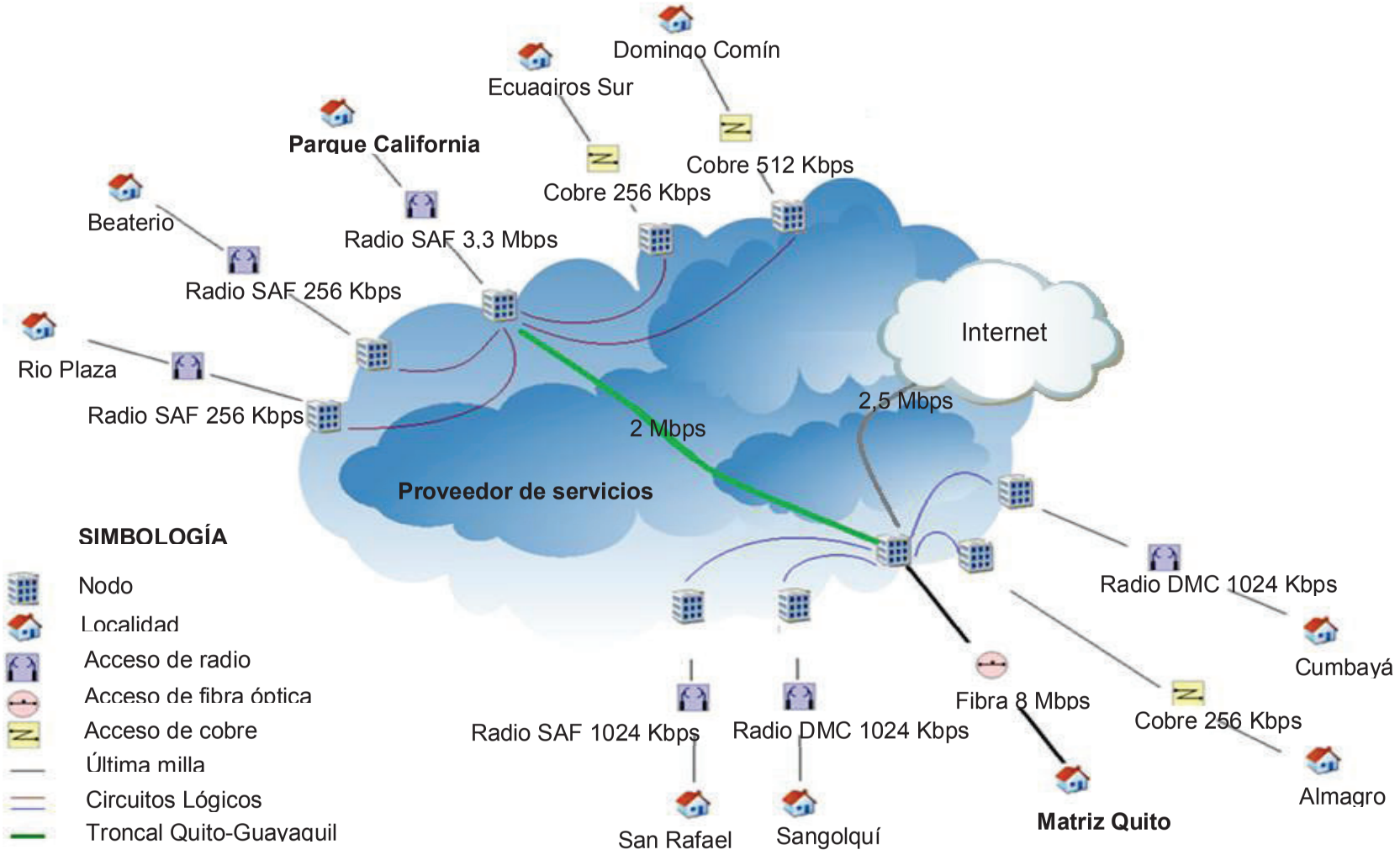


Figura 2.3 Diagrama de Red

2.2.3 CARACTERÍSTICAS DE LOS ENLACES DE LA EMPRESA

2.2.3.1 Sede Matriz Quito

La matriz de la empresa está ubicada en una zona comercial de Quito y es el sitio donde se encuentran los siguientes servidores: Correo electrónico, Web, Base de Datos Oracle, Dominio, Aplicaciones y Antivirus Symantec.

Se cuenta con salida a *Internet* con una capacidad de 2,5 Mbps y las sedes que se comunican directamente con la matriz son las agencias Almagro, Cumbayá, Sangolquí y San Rafael.

Se tiene implementado un canal de comunicación con la sucursal principal de Guayaquil de 2 Mbps, permitiendo cursar las actualizaciones de información de las sucursales conectadas a la agencia principal de Guayaquil.

El enlace implementado desde la Matriz a la nube del proveedor es por medio de una fibra óptica multimodo 50/125 um, con tecnología de transmisión SDH (*synchronous Digital Hierarchy*), la velocidad del enlace es de 8 Mbps.

Con un equipo de multiplexación *Newbridge* se entrega los servicios a equipos *routers Cisco* en interfaces V35, como se indica en la figura 2.4.

La dirección IP de la LAN es 10.0.15.0 /25 en la que se tiene como dirección de *gateway* la IP 10.0.15.123/25, dando lugar a 126 *host* en la red.

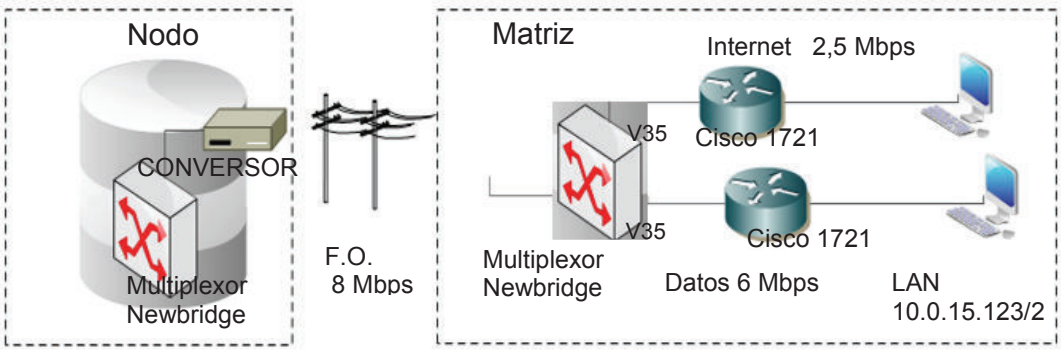


Figura 2.4 Esquema de conectividad Matriz Quito

2.2.3.2 Sucursal principal Guayaquil Parque California

Esta sede posee servidores de correo y de dominio igual que la Matriz, que acogen a los clientes de las agencias Río Plaza, Beaterio, Eguagiros Sur y Domingo Comín.

El acceso de última de milla desde la agencia principal en Guayaquil hasta la nube del proveedor es por medio de una radio microonda de marca SAF que opera en la banda de 23 GHz a una velocidad de 3,3 Mbps.

Las especificaciones del equipo de radio se encuentran en el Anexo A. En la figura 2.5 se ilustra el equipo radio modem.

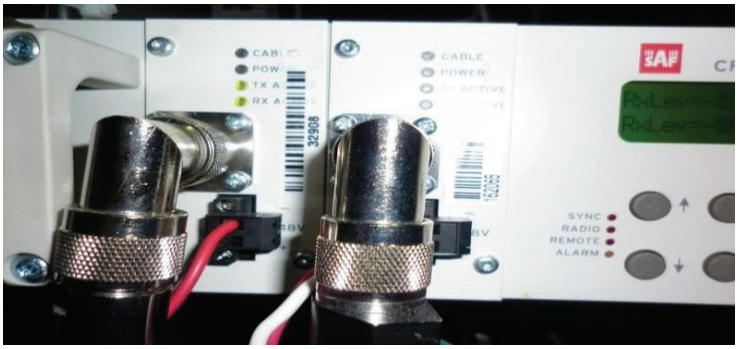


Figura 2.5 Equipo de radio SAF

El esquema de conectividad se presenta en la figura 2.6, la dirección IP de la LAN es 10.0.16.0 /25, en la que se tiene como dirección de *gateway* la IP 10.0.16.123/25, dando lugar a 126 *host* en la red.

El monitoreo de tráfico del canal se realizó en un horario de actualización de datos y se observaron picos de hasta 2 Mbps, lo que indica que el canal está dimensionado para soportar un mayor tráfico para horas pico.

En la figura 2.7 se observa la estadística de tráfico respectiva.

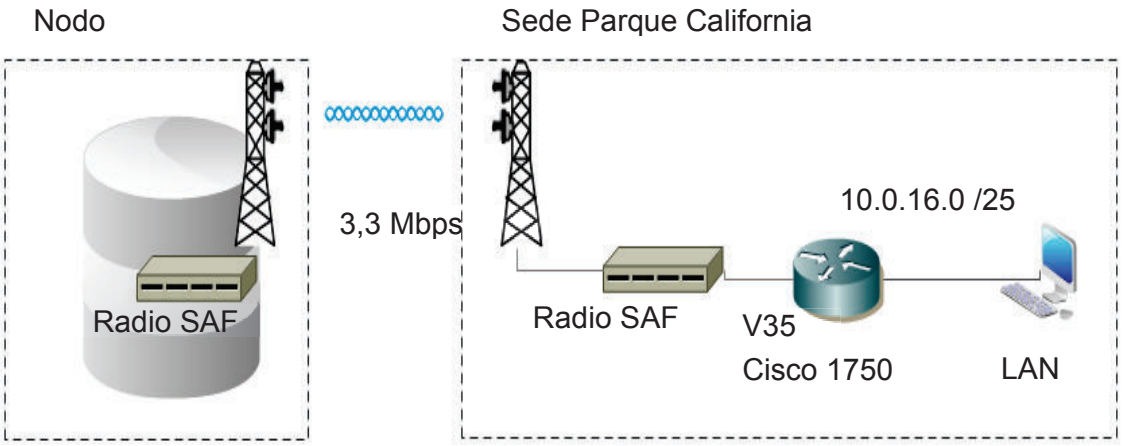


Figura 2.6 Esquema de conectividad Parque California.

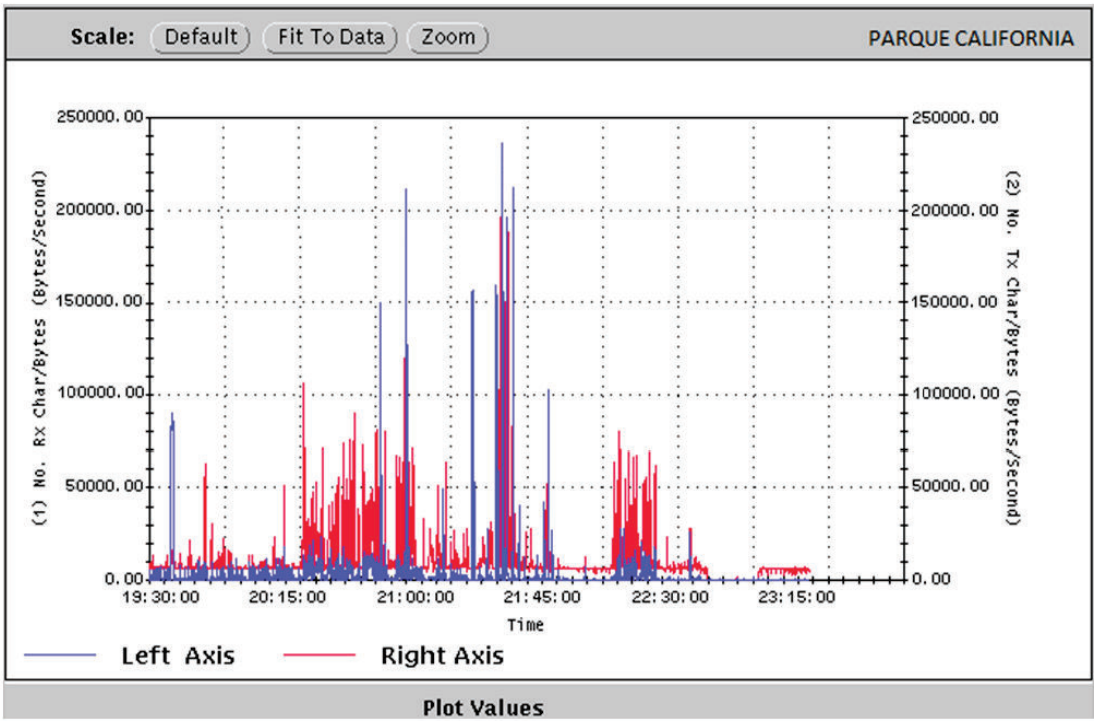


Figura 2.7 Estadística de tráfico sucursal Parque California

2.2.3.3 Troncal Quito- Guayaquil

El circuito troncal Quito-Guayaquil es un canal transparente *Clear Channel* a 2 Mbps. Por una limitación en la gestión del monitoreo y por ser los equipos de *internetworking* administrados por el cliente no fue posible determinar estadísticas de tráfico.

2.2.3.4 Agencia Almagro

Igualmente no se logró obtener estadísticas de tráfico en el canal *Clear Channel* por una limitación en la gestión del monitoreo. El acceso de última milla es por medio de un acceso HDSL con módems *music* 200 punto a punto a una velocidad de 256 Kbps por líneas de cobre hasta la nube del proveedor. En el Anexo B se adjuntan las características del equipo modem *music 200*, y se muestra el equipo en la figura 2.8.

Figura 2.8 Equipo modem Music 200

En la figura 2.9 se presenta el esquema de conectividad. La dirección IP de la LAN es 10.0.17.0 /25, en la que se tiene como dirección de *gateway* la IP 10.0.17.123/25, dando lugar a 126 *host* en la red.

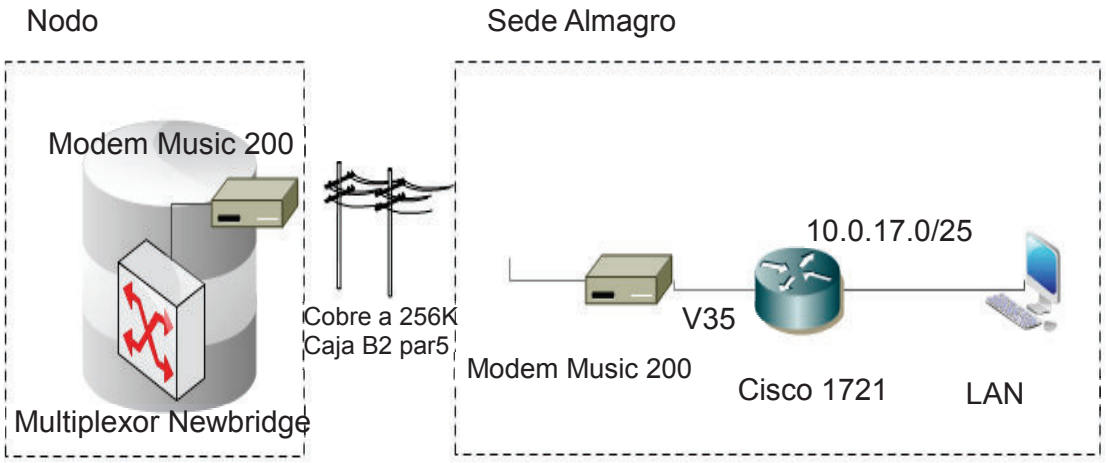


Figura 2.9 Esquema de conectividad sede Almagro

2.2.3.5 Agencia Cumbayá

El tipo de enlace desde esta agencia a la nube del proveedor es por medio de un radio microonda de marca DMC Classic II en la banda de 23 GHz a una velocidad de 1024 Kbps. Se tiene implementado un servicio *Frame Relay* sobre un PVC con velocidades de CIR 1024 Kbps / Bc 1024 Kbps / Be 0 Kbps, con DLCI 52.

En el Anexo C se adjuntan los detalles del equipo de radio. En la figura 2.10 se muestra un equipo de radio DMC.

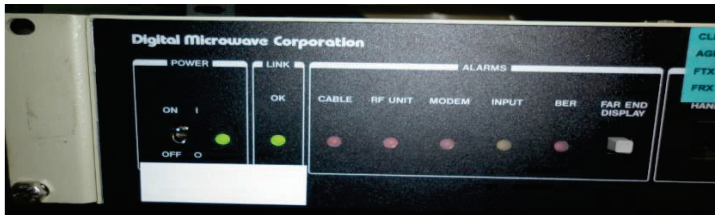


Figura 2.10 Modem de Radio DMC Classic II

El esquema de conectividad se presenta en la figura 2.11. La dirección IP de la LAN es 10.0.18.0 /25 en la que se tiene como dirección de *gateway* la IP 10.0.18.123/25, dando lugar a 126 *host* en la red.

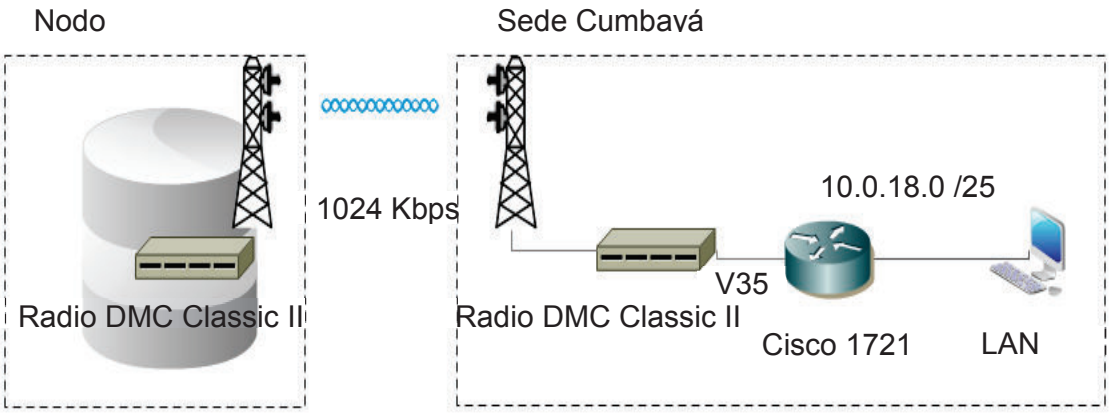


Figura 2.11 Esquema de conectividad sede Cumbayá

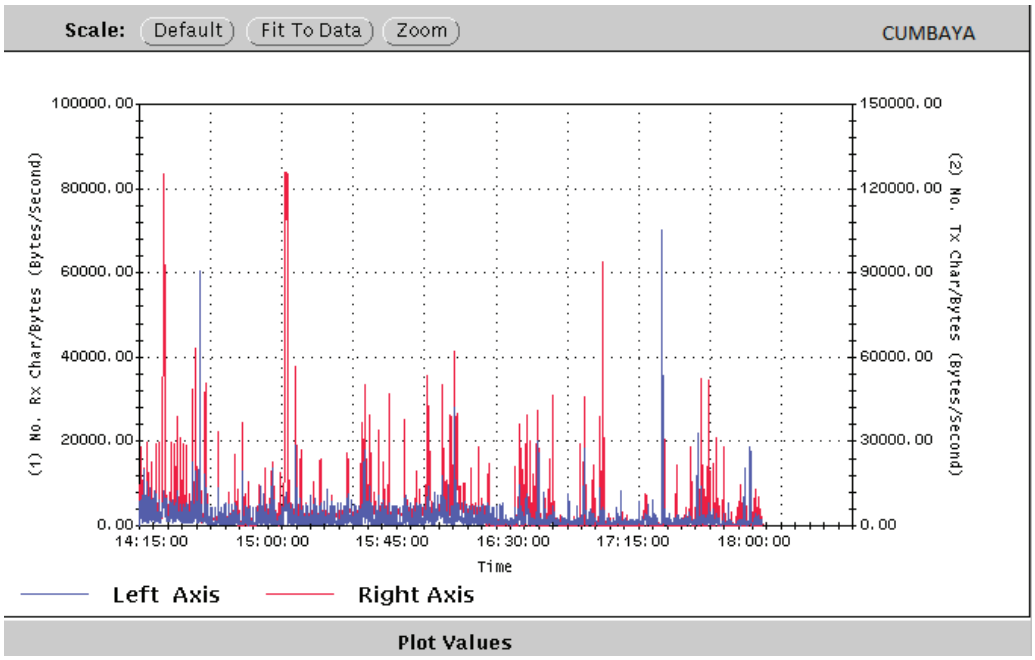


Figura 2.12 Estadística de tráfico sucursal Cumbayá

El monitoreo del tráfico de la agencia se realizó en horas de mayor tráfico, y se observan picos de hasta 1040 Kbps, con lo que se puede llegar a saturar la capacidad contratada y presentar lentitud en los aplicativos. El tráfico obtenido para este enlace se puede observar en la figura 2.12.

2.2.3.6 Agencia Sangolquí

Desde esta agencia a la nube del proveedor se tiene un acceso de radio DMC Classic II operando en la banda de 23 GHz a una velocidad de 1024 Kbps. El servicio se encuentra implementado en un circuito *Frame Relay* sobre un PVC con velocidades de CIR 1024 Kbps / Bc 1024 Kbps / Be 0 Kbps con DLCI 34.

El esquema de conectividad se presenta en la figura 2.13. La dirección IP en la LAN es 10.0.19.0 /25, en la que se tiene como dirección de *gateway* la IP 10.0.19.123/25.

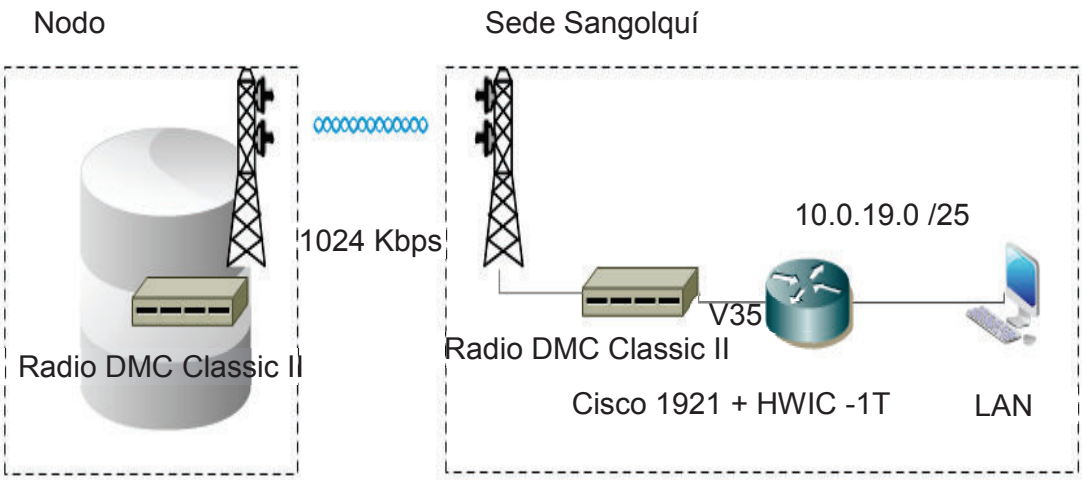


Figura 2.13 Esquema de conectividad sede Sangolquí

La estadística de tráfico obtenido para este enlace se puede observar en la figura 2.14, donde se presentan periodos con un tráfico máximo de 848 Kbps, que no supera la capacidad contratada.

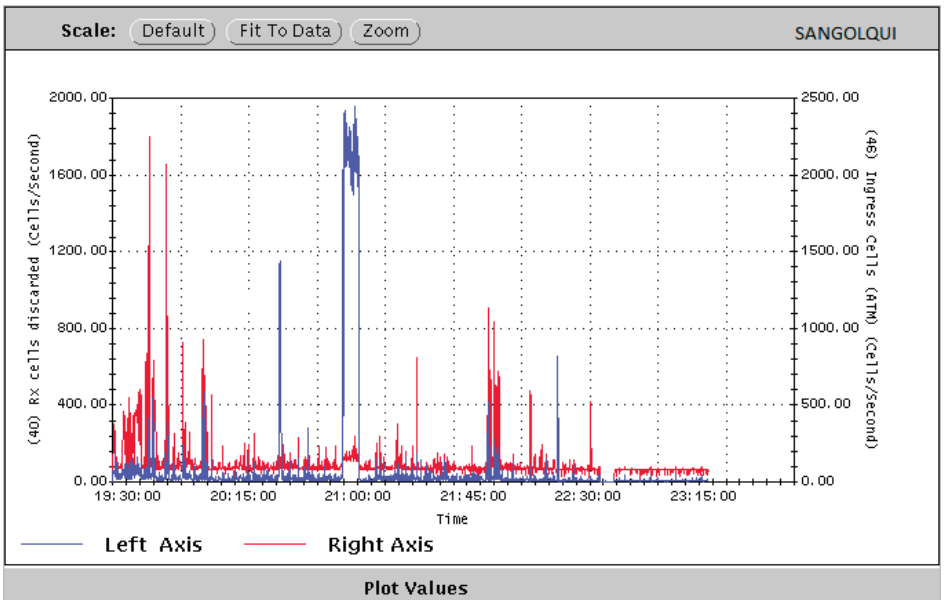


Figura 2.14 Estadística de tráfico sucursal Sangolquí

2.2.3.7 Agencia San Rafael

El acceso de última milla desde la agencia San Rafael a la nube del proveedor es por medio de una radio SAF en la banda de 23 GHz a una velocidad de 1024 Kbps. El circuito implementado es un *Clear Channel,* que por limitaciones en la gestión de monitoreo no fue posible obtener estadísticas de tráfico.

El esquema de conectividad se presenta en la figura 2.15. La dirección IP de la LAN es 10.0.20.0 /25 como dirección de *gateway* la IP 10.0.20.123/25.

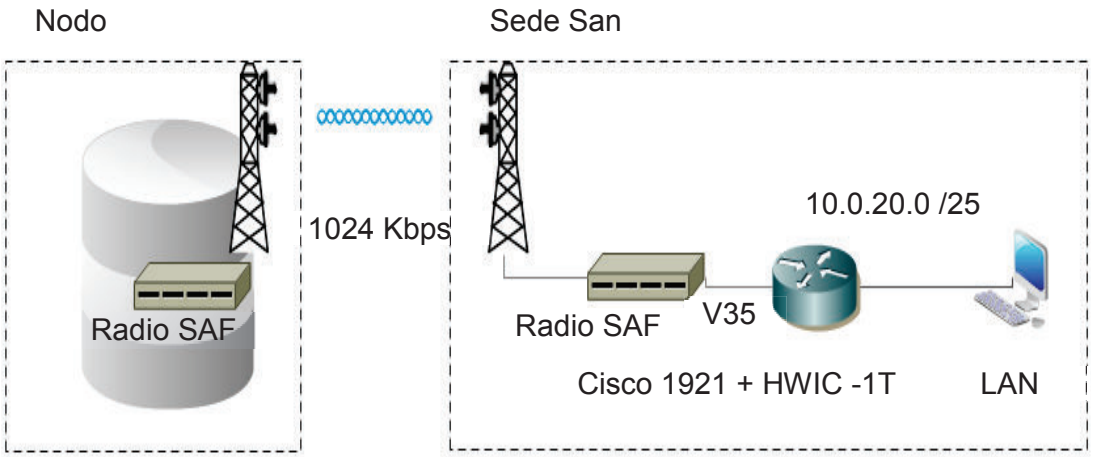


Figura 2.15 Esquema de conectividad sede San Rafael

2.2.3.8 Agencia Río Plaza

Para esta agencia el acceso a la nube del proveedor es por medio de una radio de marca SAF operando en la banda de 23 GHz a una velocidad de 256 Kbps. Implementado sobre un circuito *Frame Relay* con un PVC con velocidades de CIR 256 Kbps / Bc 256 Kbps / Be 0 Kbps, con DLCI 44.

El esquema de conectividad se presenta en la Figura 2.16. La dirección IP de la LAN es 10.0.21.0 /25, en la que se tiene como dirección de *gateway* la IP 10.0.21.123/25.

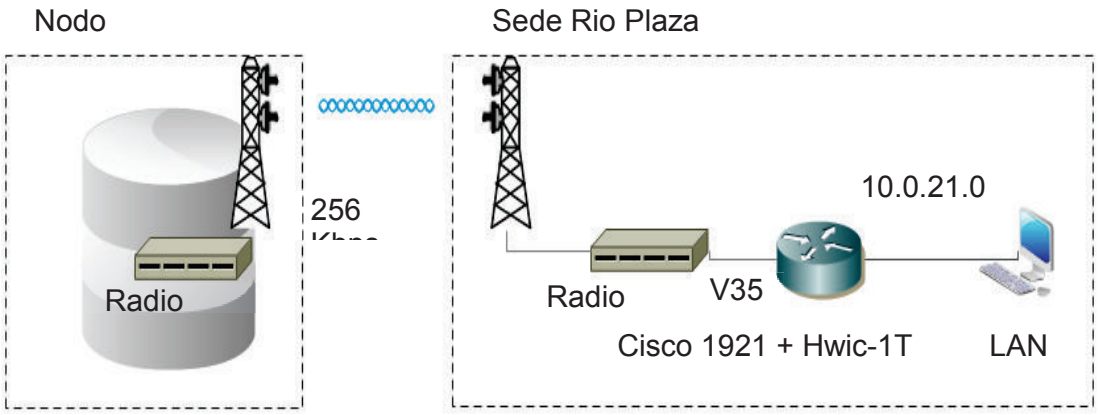


Figura 2.16 Esquema de conectividad sede Río Plaza

El monitoreo de tráfico se realizó al momento de cierre de agencia; en él se observa saturación del enlace, lo que se tomará en cuenta en el diseño de la red. La estadística de tráfico obtenida se ilustra en la figura 2.17.

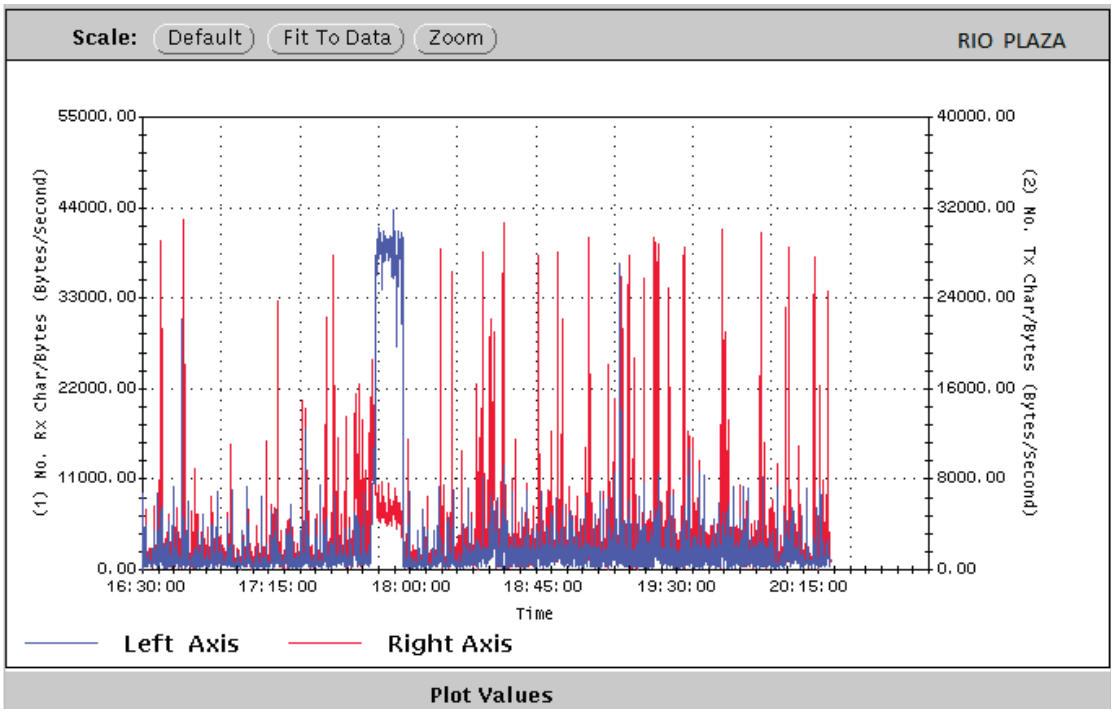


Figura 2.17 Estadística de tráfico sucursal Río Plaza

2.2.3.9 Agencia Beaterio

De igual manera para esta sede se tiene implementado el acceso por medio de una radio SAF en la banda de 23 GHz a una velocidad de 256 Kbps. El circuito *Frame Relay* se encuentra configurado de la siguiente manera: PVC con velocidades de CIR 256 Kbps / Bc 256 Kbps / Be 0 Kbps con DLCI 27.

El esquema de conectividad se presenta en la figura 2.18. La dirección IP de la LAN es 10.0.22.0 /25, en la que se tiene como dirección de *gateway* la IP 10.0.22.123/25.

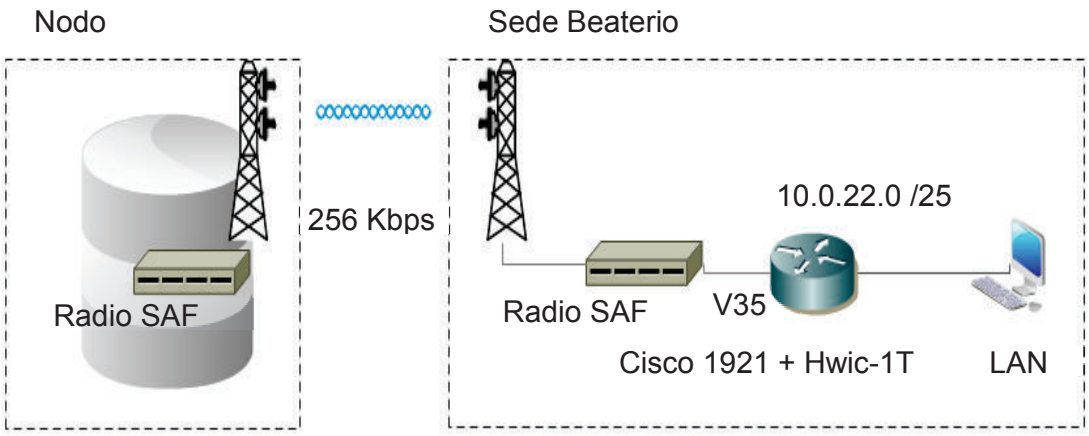


Figura 2.18 Esquema de conectividad sede Beaterio

En el monitoreo del enlace se observó picos de hasta 240 Kbps, que pueden producir saturación del enlace; el dimensionamiento será verificado en la etapa de diseño. En la figura 2.19 se tienen las estadísticas de tráfico del enlace.

2.2.3.10 Agencia Ecuagiros Sur

Para esta agencia el acceso de última milla a la nube del proveedor es por medio de una línea de cobre con un módem music 200 a una velocidad de 256 Kbps. Implementado sobre un circuito PVC *Frame Relay* con velocidades de CIR 256 kbps / Bc 256 kbps / Be 0 kbps con DLCI 31.

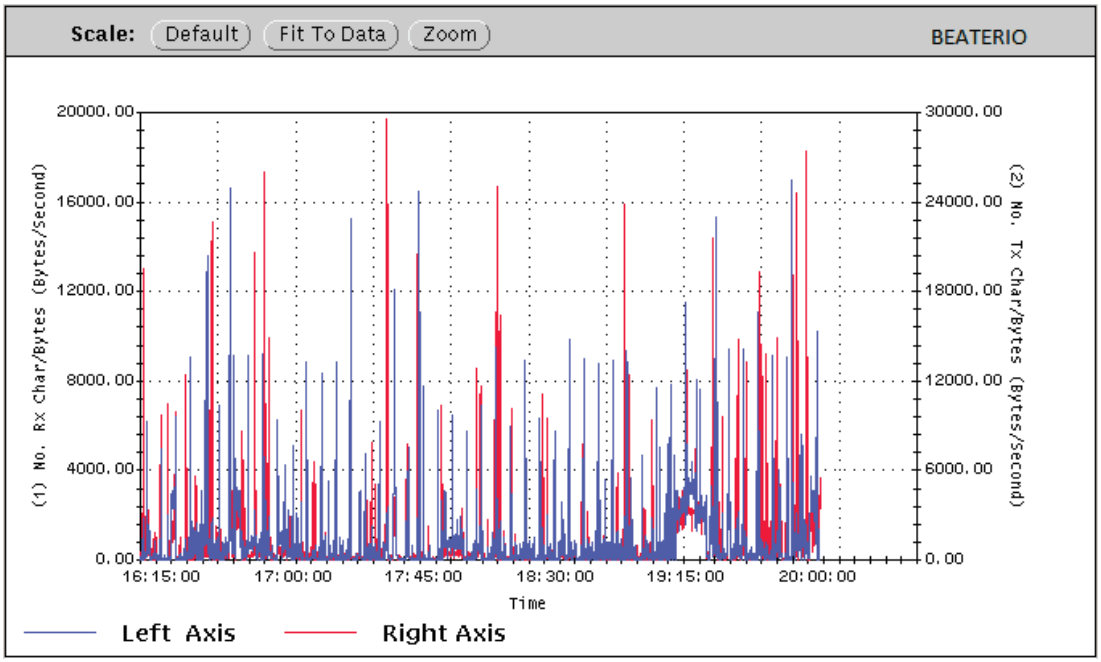


Figura 2.19 Estadística de tráfico sucursal Beaterio

El esquema de conectividad se presenta en la figura 2.20. La dirección IP de la LAN es 10.0.23.0 /25 como dirección de *gateway* la IP 10.0.23.123/25.

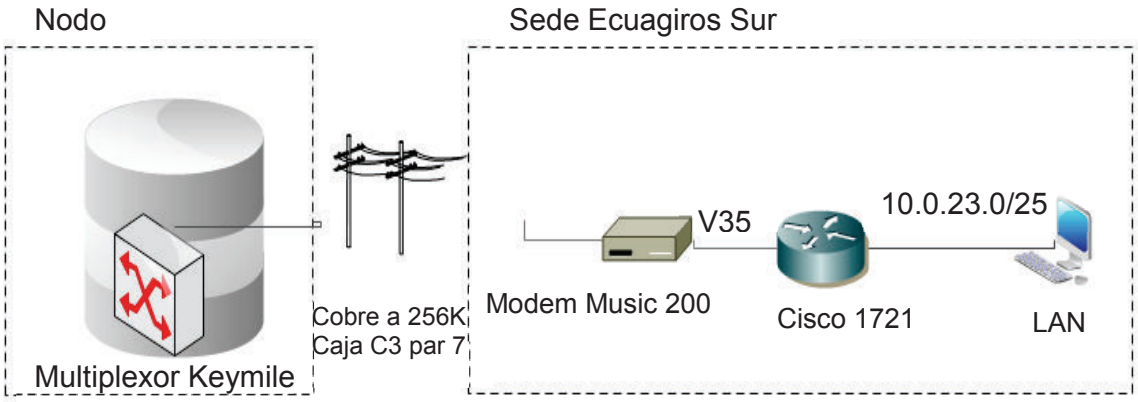


Figura 2.20 Esquema de conectividad Ecuagiros Sur

En el monitoreo se evidenció saturación en el enlace a 256 Kbps, lo que produce lentitud en el servicio, a la hora de cierre de caja. La estadística de tráfico obtenida se ilustra en la figura 2.21.

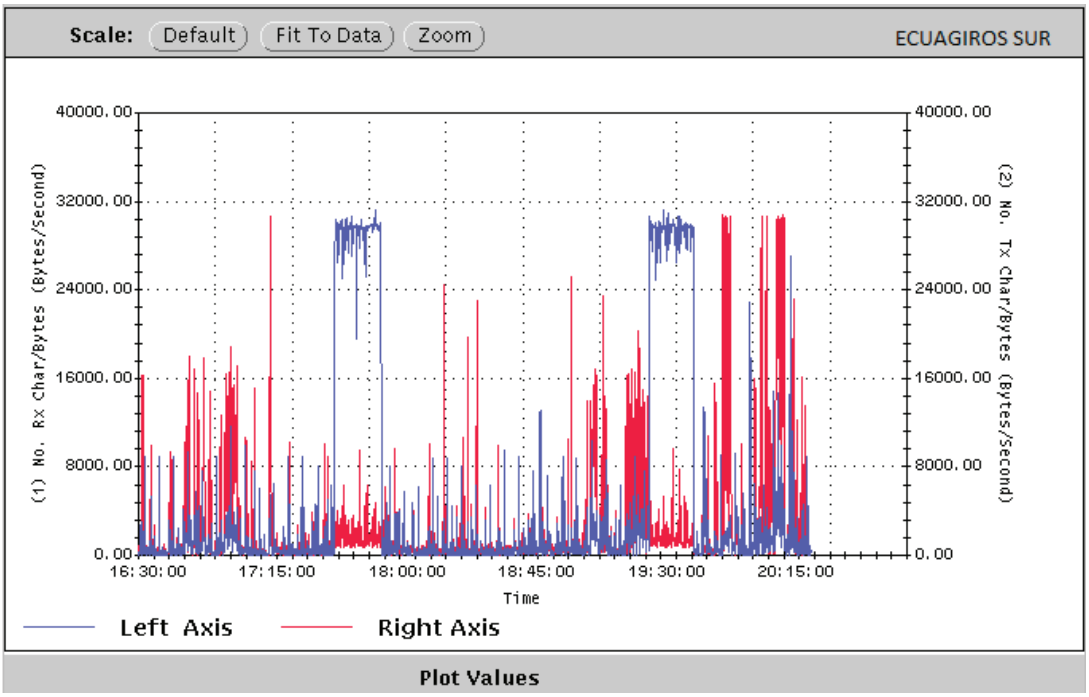


Figura 2.21 Estadística de tráfico sucursal Ecuagiros Sur

2.2.3.11 Agencia Domingo Comín

De igual manera el acceso a la sede Domingo Comín es mediante una línea de cobre con módems *music 200* a una velocidad de 512 kbps. Implementado por medio de un PVC *Frame Relay* con velocidades de CIR 512 Kbps / Bc 512 kbps / Be 0 kbps con DLCI 18.

El esquema de conectividad se presenta en la figura 2.22. La dirección IP en la LAN es 10.0.24.0 /25, en la que se tiene como dirección de *gateway* la IP 10.0.24.123/25.

Del monitoreo realizado se observó picos de tráfico de 320 Kbps, sin que presente problemas en los aplicativos del cliente. La estadística de tráfico se observa en la figura 2.23.

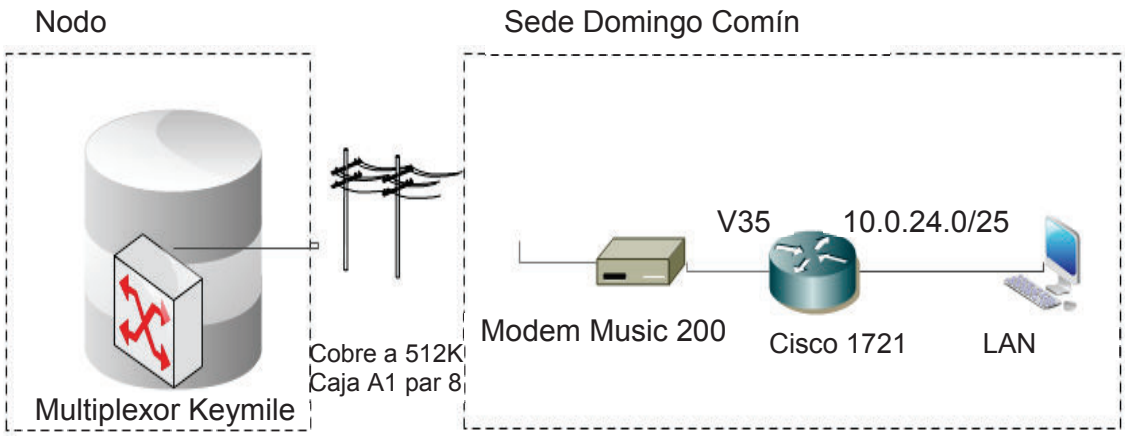


Figura 2.22 Esquema de conectividad sede Domingo Comín

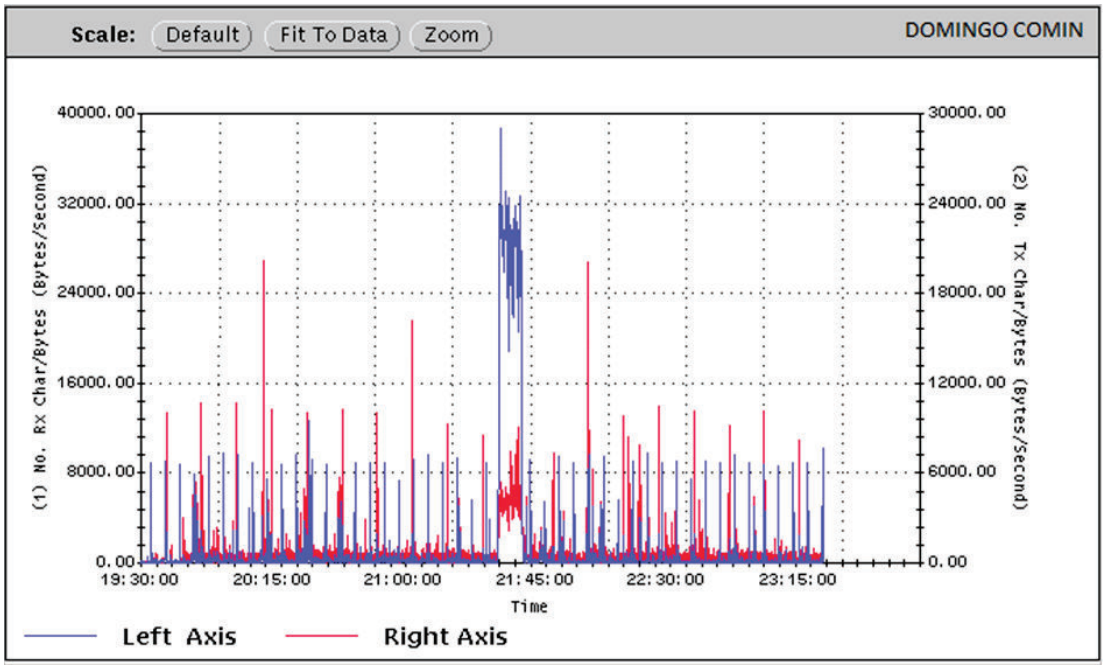


Figura 2.23 Estadística de tráfico sucursal Domingo Comín

2.2.3.12 Canal de Internet

Por medio del programa *haystack* (aplicación que permite obtener estadísticas de tráfico entrante y saliente de la interfaz de un equipo en intervalos de 30 segundos*)* se obtuvieron los reportes de tráfico del canal de Internet, el cual tiene una velocidad

de 2,5 Mbps simétrico. Las estadísticas de tráfico se presentan en las gráficas de las figuras 2.24 y 2.25.

De las gráficas se observa picos de tráfico que llegan a la capacidad contratada, por lo que es necesario el redimensionamiento del canal en el diseño de la red.

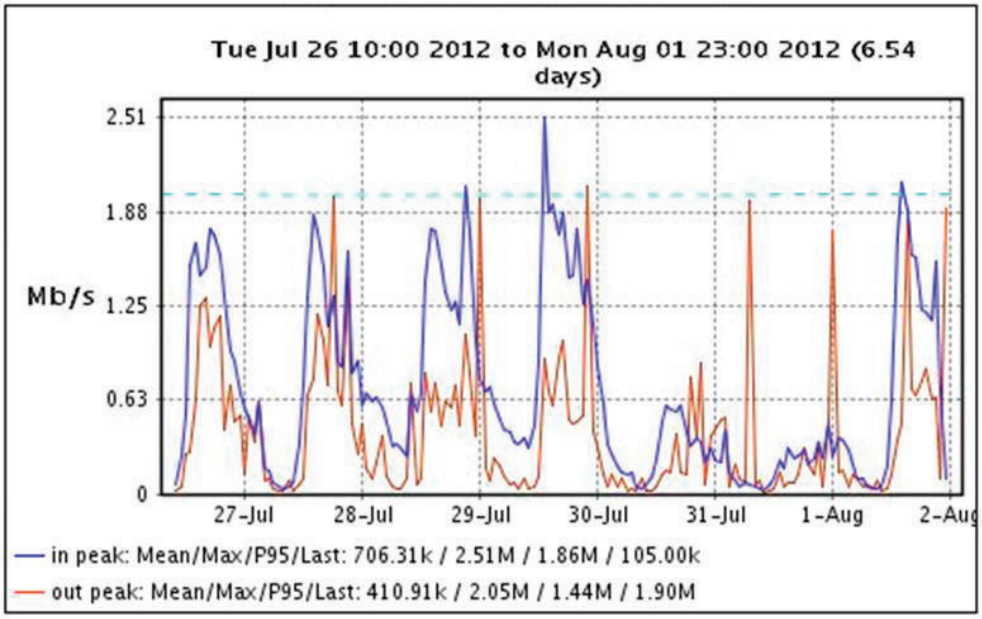


Figura 2.24 Estadística de tráfico Internet semanal

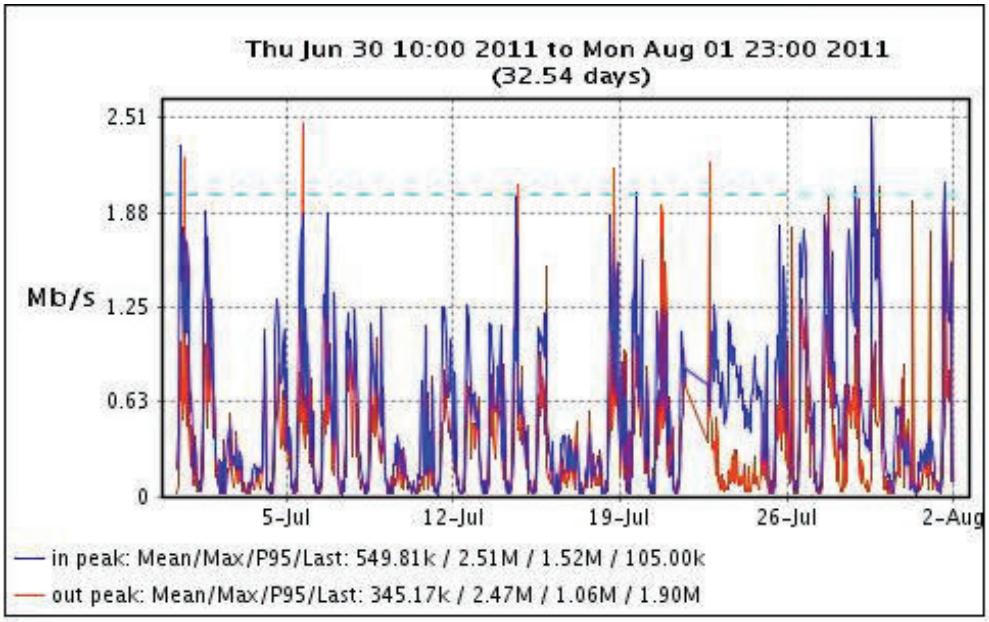


Figura 2.25 Estadística de tráfico Internet mensual

En la tabla 2.1 se presenta un resumen de los enlaces instalados.

Sede	Tasa de transferencia por sede	Tipo de acceso
Matriz Quito	8 Mbps	Fibra óptica (SDH)
Parque California	3,3 Mbps	Microonda (23 GHz)
Ag. Cumbayá	1024 Kbps	Microonda (23 GHz)
Ag. San Rafael	1024 Kbps	Microonda (23 GHz)
Ag. Sangolqui	1024 Kbps	Microonda (23 GHz)
Ag. Almagro	256 Kbps	HDSL (acceso de cobre)
Ag. Rio Plaza	256 Kbps	Microonda (23 GHz)
Ag. Beaterio	256 Kbps	Microonda (23 GHz)
Ag. Ecuagiros Sur	256 Kbps	HDSL (acceso de cobre)
Ag. Domingo Comín	512 Kbps	HDSL (acceso de cobre)
Enlace Quito-Guayaquil	2 Mbps	*Backbone* Proveedor
Acceso a Internet	2,5 Mbps	*Backbone* Proveedor(Simétrico)

Tabla 2.1 Resumen de enlaces instalados

2.3 ANÁLISIS DE REQUERIMIENTOS DE TASA DE TRANSFERENCIA POR AGENCIA

Analizando el origen y características del tráfico generado actualmente, se puede determinar el requerimiento de las tasas de transferencia en una red de datos.

Es importante determinar las aplicaciones que podrían causar congestión en la red bajo ciertas circunstancias.

Existen varios factores a considerar en los requerimientos de los enlaces y rendimiento de la red actual, entre los cuales se pueden indicar los siguientes:

- Número de usuarios de las diferentes aplicaciones implementadas en la empresa.
- Tipo de servicio que puede estar relacionado con bases de datos, correo electrónico, videoconferencias, entre otros.
- Intervalos de tiempo de mayor requerimiento de los servicios y aplicaciones de la red.
- Servicios y transferencia de información al *Internet*.
- Servicios centralizados, con aplicaciones en servidores principales.
- Proyección y oportunidad de crecimiento de la empresa.

El cliente cuenta con un aplicativo en Java sobre una base de datos en Oracle para un sistema de créditos, que se despliega sobre un servidor de aplicaciones Jboss que está sobre Linux.

De acuerdo a datos experimentales por parte del administrador del sistema, se ha establecido que el aplicativo de crédito requiere una tasa promedio de 11,4 Kbps por usuario.

En el servicio de Internet se restringen páginas de redes sociales, salas de chat, páginas de reproducción de videos y videoconferencia, el tráfico es por ráfagas y se ha determinado con el administrador de la red interna que alrededor del 10 % de los usuarios requieren descargar páginas de Internet al mismo tiempo en la hora de mayor tráfico.

Debido a que una conexión aceptable en cuanto a velocidad de transferencia oscila en promedio alrededor de los 62 Kbps, es decir una página promedio de unos 55 Kbytes se abre en 7,1 segundos, se considerará este valor como el límite mínimo de acceso por usuario conectado a Internet a la hora pico.

Dependerá del criterio del administrador para filtrar los aplicativos que se pueden usar en *Internet* de acuerdo al perfil y requerimiento de trabajo del usuario, con la finalidad de no congestionar la red.

En cuanto al aplicativo de correo electrónico se considera que no es simultánea la transmisión y la recepción de los correos, teniendo un tráfico *half-duplex*, por lo que se tomará el mayor de los valores.

Para la transferencia de correo electrónico se estableció que el tamaño promedio de los archivos transferidos en el día por un usuario es de 90 KB, considerando un tiempo de espera aceptado para la llegada del correo de 3 minutos (180 segundos).

De acuerdo al administrador de la red interna se pudo establecer que aproximadamente un 15 % de los usuarios utilizan el correo electrónico simultáneamente, valor aproximado para todas las agencias.

Bajo estos criterios se procede a realizar los cálculos de tráfico por cada agencia.

2.3.1 AGENCIA ALMAGRO

En esta agencia trabajan 20 empleados cada uno con un computador personal (PC).

2.3.1.1 Aplicación sistema de crédito

A esta aplicación tienen conexión permanente 7 usuarios según lo indicado por el administrador del sistema, y requiere cada uno una tasa de transferencia de 11,4 Kbps dando un total de 79,8 Kbps.

$$\boldsymbol{Capacidad\ sistema\ de\ cr\acute{e}dito = usuarios\ simult\acute{a}neos\ x\ tasa\ de\ transferencia}$$

$$\boldsymbol{Capacidad\ sistema\ de\ cr\acute{e}dito = 7\ x\ 11,4\ Kbps = 79,8\ Kbps}$$

2.3.1.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 20 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tienen 3 usuarios que utilizan el correo electrónico, generando un tráfico de 12 Kbps.

Usuarios simultáneos: 3
Tamaño promedio de email: 90 KB
Tiempo de descarga: 180 s

$$\textbf{Capacidad de correo} = \textbf{usuarios simultáneos } x \frac{\textbf{Tamaño promedio de email}}{\textbf{Tiempo de descarga}}$$

$$\textbf{Capacidad de correo} = 3\ x\ \frac{90KB}{180s}\ x\ \frac{8Kb}{1KB} = 12Kbps$$

2.3.1.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 Kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 124 Kbps.

$$\textbf{Capacidad internet} = \textbf{usuarios simultáneos x tasa de transferencia}$$
$$\textbf{Capacidad internet} = 2\ x\ 62Kbps = 124Kbps$$

2.3.2 AGENCIA CUMBAYÁ

En esta agencia existen 50 empleados con un computador personal (PC).

2.3.2.1 Aplicación sistema de crédito

A esta aplicación tienen conexión permanente 40 usuarios, y requiere cada uno una tasa de transferencia de 11,4 Kbps, dando un total de 456 Kbps.

2.3.2.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 50 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tienen 7 usuarios utilizando el correo electrónico, generando un tráfico de 28 Kbps.

2.3.2.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 Kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 310 Kbps para este acceso.

2.3.3 AGENCIA SANGOLQUÍ

En esta agencia existen 50 empleados con un computador personal (PC).

2.3.3.1 Aplicación sistema de crédito

A esta aplicación tienen conexión permanente 38 usuarios, y requiere cada uno una tasa de transferencia de 11,4 Kbps, dando un total de 433,2 Kbps.

2.3.3.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 50 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tienen 7 usuarios utilizando el correo electrónico, generando un tráfico de 28 Kbps.

2.3.3.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 Kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 310 Kbps.

2.3.4 AGENCIA SAN RAFAEL

En esta agencia existen 50 empleados con un computador personal (PC).

2.3.4.1 Aplicación sistema de crédito

A esta aplicación tienen conexión permanente 35 usuarios, y requiere cada uno una tasa de transferencia de 11,4 Kbps, dando un total de 399 Kbps.

2.3.4.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 50 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tienen 7 usuarios utilizando el correo electrónico, lo que genera un tráfico de 28 Kbps.

2.3.4.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico se requerirá de 310 Kbps.

2.3.5 AGENCIA RÍO PLAZA

En esta agencia existen 20 empleados con un computador personal (PC)

2.3.5.1 Aplicación sistema de crédito

A esta aplicación tienen conexión permanente 6 usuarios, y requiere cada uno una tasa de transferencia de 11,4 kbps dando un total de 68,4 Kbps.

2.3.5.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 20 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tiene 3 usuarios utilizando el correo electrónico, lo que genera un tráfico de 12 Kbps.

2.3.5.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico se requerirá de 124 Kbps.

2.3.6 AGENCIA BEATERIO

En esta agencia existen 20 empleados con un computador personal (PC).

2.3.6.1 Aplicación sistema de crédito

A esta aplicación tienen conexión permanente 5 usuarios, y requiere cada uno una tasa de transferencia de 11,4 kbps dando un total de 57 Kbps.

2.3.6.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 20 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tienen 3 usuarios utilizando el correo electrónico, lo que genera un tráfico de 12 Kbps.

2.3.6.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 124 Kbps.

2.3.7 AGENCIA ECUAGIROS SUR

En esta agencia existen 20 empleados con un computador personal (PC).

2.3.7.1 Aplicación sistema de crédito

A esta aplicación tienen conexión permanente 6 usuarios, y requiere cada uno una tasa de transferencia de 11,4 Kbps, dando un total de 68,4 Kbps.

2.3.7.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 20 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tienen 3 usuarios utilizando el correo electrónico, lo que genera un tráfico de 12 Kbps.

2.3.7.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 124 Kbps.

2.3.8 AGENCIA DOMINGO COMÍN

En esta agencia se cuenta con 30 empleados cada uno con un computador personal.

2.3.8.1 Aplicación de crédito

A esta aplicación tienen conexión permanente 13 usuarios, y requiere cada uno una tasa de transferencia de 11,4 Kbps dando un total de 148,2 Kbps.

2.3.8.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 30 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tienen 4 usuarios utilizando el correo electrónico generando un tráfico de 16 Kbps

2.3.8.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 Kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 186 Kbps.

2.3.9 AGENCIA PRINCIPAL PARQUE CALIFORNIA

En esta agencia existen 50 empleados con un computador personal.

2.3.9.1 Aplicación sistema de crédito

A esta aplicación tienen conexión permanente 38 usuarios, y requiere cada uno una tasa de transferencia de 11,4 Kbps dando un total de 433,2 Kbps.

2.3.9.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 50 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tienen 8 usuarios utilizando el correo electrónico generando un tráfico de 32 Kbps.

Sin embargo el administrador de red considera que únicamente el 50% de los emails se dirige hacia la Matriz, por lo que se necesitaría de 10,8 Kbps para este servicio a través del enlace Quito –Guayaquil.

2.3.9.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 310 Kbps.

2.3.10 ENLACE TRONCAL QUITO – GUAYAQUIL

Se considera el total de 140 PCs existentes en las agencias Parque California, Rio Plaza, Beaterio, Ecuagiros Sur y Domingo Comín que necesitarían comunicarse hacia la Matriz.

2.3.10.1 Aplicación sistema de crédito

Considerando que el servidor de aplicación se encuentra en la Matriz y que cuentan con una conexión permanente 68 usuarios, y requiere cada uno una tasa de transferencia de 11,4 Kbps se tiene un total de 775,2 Kbps.

2.3.10.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 140 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tiene 21 usuarios utilizando el correo electrónico generando un tráfico de 84 Kbps.

Sin embargo el administrador de red considera que el únicamente el 50% de los *emails* se dirige hacia la Matriz, por lo que se necesitaría 42 Kbps para este servicio a través del enlace Quito – Guayaquil.

2.3.10.3 Acceso a Internet

Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 868 kbps para este acceso.

2.3.11 SEDE MATRIZ QUITO

2.3.11.1 Aplicación sistema de crédito

Considerando que el servidor de aplicación se encuentra en la Matriz y que cuenta con una conexión permanente 50 usuarios, y requiere cada uno una tasa de transferencia de 11,4 Kbps, se tendrá un total de 570 Kbps.

2.3.11.2 Correo electrónico

Pueden enviar y recibir correo electrónico los 65 empleados. Si se considera que un 15% de ellos está utilizando simultáneamente este servicio, se tiene 10 usuarios utilizando el correo electrónico, lo que generea un tráfico de 40 Kbps.

2.3.11.3 Acceso a Internet

El número de PCs existentes en la Matriz es de 65, con lo que el número total de equipos en la empresa es de 375 PCs. Considerando que el 10% de los usuarios acceden a Internet al mismo tiempo y que los 62 Kbps es la mínima tasa de transferencia aceptada por la empresa para la conexión a Internet por usuario en hora pico, se requerirá de 2,325 Mbps.

En la tabla 2.2 se tiene el resumen de requerimiento de comunicación de la empresa.

Tanto el número totales de usuarios como el número de usuarios del sistema de crédito para el enlace Quito-Guayaquil, es la suma de los usuarios de las sedes ubicadas en la ciudad de Guayaquil.

Es decir:

$$\boldsymbol{Enlace\ Quito\_Guayaquil}_{(\boldsymbol{Usuarios\ totales})} = \boldsymbol{Parque\ California}_{(\boldsymbol{Usuarios\ totales})} + \boldsymbol{Río\ Plaza}_{(\boldsymbol{Usuarios\ totales})} + \boldsymbol{Beaterio}_{(\boldsymbol{Usuarios\ totales})} + \boldsymbol{Ecuagiros\ Sur}_{(\boldsymbol{Usuarios\ totales})} + \boldsymbol{Domingo\ Comín}_{(\boldsymbol{Usuarios\ totales})}$$

$$\boldsymbol{Enlace\ Quito\_Guayaquil}_{(\boldsymbol{Usuarios\ totales})} = \mathbf{50} + \mathbf{20} + \mathbf{20} + \mathbf{20} + \mathbf{30} = \mathbf{140}$$

$$\boldsymbol{Enlace\ Quito\_Guayaquil}_{(\boldsymbol{Usuarios\ sistema\ de\ crédito})} = \mathbf{38} + \mathbf{6} + \mathbf{5} + \mathbf{6} + \mathbf{13} = \mathbf{68}$$

Todos los usuarios de la empresa sin considerar los usuarios que usan el enlace Quito-Guayaquil, corresponde al número de usuarios del Internet Total.
Es decir:

$$Internet\ Total_{(Usuarios\ totales)} = Matriz\ Quito_{(Usuarios\ totales)} + Parque\ California_{(Usuarios\ totales)} + Cumbayá + San\ Rafael + Sangolquí + Almagro + Río\ Plaza + Beaterio + Ecuagiros\ Sur + Domingo\ Comín$$

$$Internet\ Total_{(Usuarios\ totales)} = 65 + 50 + 50 + 50 + 50 + 20 + 20 + 20 + 20 + 30 = 375$$

La tasa total de bit por sede se obtiene de la siguiente manera:

$$Tasa\ total\ de\ bit\ por\ sede = Tasa\ de\ bit\ de\ la\ aplicacion\ del\ sistema\ para\ crédito + tasa\ de\ bit\ del\ correo\ eletrónico + tasa\ de\ bit\ del\ Internet$$

Por ejemplo para la sede Matriz Quito, la tasa total de bit es:

$$Matriz\ Quito_{(Tasa\ total\ bit\ por\ sede)} = 570\ Kbps + 40\ Kbps + 434\ Kbps = 1044\ Kbps$$

La tasa total de bit por acceso para la sede Matriz Quito, es la suma de las tasas totales de bit de las siguientes sedes:

$$Matriz\ Quito_{(Tasa\ total\ bit\ por\ acceso)} = Matriz\ Quito_{(Tasa\ total\ bit\ por\ sede)} + Cumbayá_{(Tasa\ total\ bit\ por\ sede)} + San\ Rafael_{(Tasa\ total\ bit\ por\ sede)} + Sangolquí_{(Tasa\ total\ bit\ por\ sede)} + Almagro_{(Tasa\ total\ bit\ por\ sede)} + Enlace\ Quito\_Guaquil_{(Tasa\ total\ bit\ por\ sede)} + Internet_{(Tasa\ total\ bit\ por\ sede)}$$

$$Matriz\ Quito_{(Tasa\ total\ bit\ por\ acceso)} = 1044\ Kbps + 794\ Kbps + 737\ Kbps + 771,2\ Kbps + 215,8\ Kbps + 1685,2\ Kbps + 2325\ Kbps = 7572,2\ Kbps$$

Mientras que la tasa total de bit por acceso para la sede Parque California se obtiene de la suma de las tasas totales de bit de las siguientes sedes:

$$Parque\ California_{(Tasa\ total\ bit\ por\ acceso)}$$
$$= Parque\ California_{(Tasa\ total\ bit\ por\ sede)}$$
$$+ Río\ Plaza_{(Tasa\ total\ bit\ por\ sede)} + Beaterio_{(Tasa\ total\ bit\ por\ sede)}$$
$$+ Ecuagiros\ Sur_{(Tasa\ total\ bit\ por\ sede)}$$
$$+ Domingo\ Comín_{(Tasa\ total\ bit\ por\ sede)}$$
$$+ Enlace\ Quito\_Guaquil_{(Tasa\ total\ bit\ por\ sede)}$$
$$Parque\ California_{(Tasa\ total\ bit\ por\ acceso)}$$
$$= 775,2\ Kbps + 204,4\ Kbps + 193\ Kbps + 204,4\ Kbps$$
$$+ 350,2\ Kbps + 1685,2\ Kbps = 3412,4\ Kbps$$

Para las agencias la tasa total de bit por acceso es igual a la tasa por bit por sede porque no concentran el tráfico de otras localidades.

2.4 CONSIDERACIONES DE CALIDAD DE SERVICIO

Para la calidad de servicio se diferenciará los diferentes tipos de tráfico que cruzan la red, con la finalidad de tener una red convergente.

El cliente tiene previsto incluir en la red, voz sobre IP (VoIP) entre las sedes principales y las agencias.

Además se implementará un servicio de videoconferencia entre la sede Matriz con la sucursal Mayor Guayaquil.

Hay que considerar que el retardo es crítico en transmisiones de voz y video. Para el apropiado desempeño de los servicios, en el diseño de la red es necesario considerar los parámetros mínimos de ancho de banda para cada servicio

A continuación se hace el análisis para los diferentes tipos de servicio a prestarse.

.

Sede	Usuarios Totales	Aplicación Sistema para Créditos (11,4 Kbps)		Correo electrónico (4 Kbps)		Internet (62 Kbps)		Tasa total de bit por sede (kbps)	Tasa total de bit por acceso (kbps)	Capacidad Contratada
		Número de usuarios	Tasa de bit (Kbps)	Número de usuarios (15% del total)	Tasa de bit (Kbps)	Número de usuarios (10% del total)	Tasa de bit (kbps)			
Matriz Quito	65	50	570	10	40	7	434	1044	7572,2	8 Mbps
Parque California	50	38	433,2	8	32	5	310	775,2	3412,4	3,3 Mbps
Ag. Cumbayá	50	40	456	7	28	5	310	794	794	1024 Kbps
Ag. San Rafael	50	35	399	7	28	5	310	737	737	1024 Kbps
Ag. Sangolquí	50	38	433,2	7	28	5	310	771,2	771,2	1024 Kbps
Ag. Almagro	20	7	79,8	3	12	2	124	215,8	215,8	256 Kbps
Ag. Rio Plaza	20	6	68,4	3	12	2	124	204,4	204,4	256 Kbps
Ag. Beaterio	20	5	57	3	12	2	124	193	193	256 Kbps
Ag. Ecuagiros Sur	20	6	68,4	3	12	2	124	204,4	204,4	256 bbps
Ag. Domingo Comín	30	13	148,2	4	16	3	186	350,2	350,2	512 Kbps
Enlace Quito- Guayaquil (para correo electrónico 50%)	140	68	775,2	21	**42**	14	868	**1685,2**	1685,2	2 Mbps
Internet Total	375					37,5	2325	2325	2325	2,5Mbps

Tabla 2.2 Resumen de requerimientos actuales de comunicación de la empresa

2.4.1 DATOS

Aplicativos del cliente y servicio de correo electrónico son sensibles en el tiempo; se proyecta los anchos de banda con el crecimiento de la entidad financiera y políticas aplicadas a los diferentes grupos de usuarios.

2.4.2 TELEFONÍA

Es importante una correcta planificación de capacidad para obtener una buena calidad de voz. Los cálculos para determinar el ancho de banda para el servicio de Voz sobre IP, se ha tomado como referencia el documento de Cisco Systems. [39]

Para el ancho de banda por llamada se han considerado los encabezados de los siguientes protocolos:

- (18 bytes) encabezado Ethernet, incluidos 4 bytes de verificación por redundancia cíclica (CRC).
- (20 bytes) encabezado para el protocolo IP.
- (8 bytes) encabezado para el protocolo de datagrama de usuario (UDP).
- (12 bytes) encabezado del protocolo de transporte en tiempo real (RTP).

La Unión Internacional de Telecomunicaciones (ITU) ha establecido codificadores estandarizados para la transmisión de voz como se indica en la Tabla 2.3.

Velocidad de bits del códec (kbps): Es el número de bits a transmitir por segundo para realizar una llamada de voz.

$$\boldsymbol{Velocidad\ de\ bits\ del\ codec} = {\boldsymbol{tamaño\ del\ códec}}/{\boldsymbol{intervalo\ del\ códec}}$$

Tamaño del códec (bytes): Es el número de bytes capturados por el Procesador de señales digitales (DSP) en cada intervalo del códec.

Información de códec				Cálculos de ancho de banda			
Velocidad de bits y códec (kbps)	Ejemplo de tamaño del códec (bytes)	Ejemplo de intervalo del códec (ms)	Mean Opinion Score (MOS)	Tamaño de la carga útil de voz (bytes)	Tamaño de la carga útil de voz (ms)	Paquetes por segundo (PPS)	Ancho de banda Ethernet (kbps)
G.711 (64 kbps)	80 bytes	10 ms	4,1	160 bytes	20 ms	50	87,2 kbps
G.729 (8 kbps)	10 bytes	10 ms	3,92	20 bytes	20 ms	50	31,2 kbps
G.723.1 (6.3 kbps)	24 bytes	30 ms	3,9	24 bytes	30 ms	34	21,9 kbps
G.723.1 (5.3 kbps)	20 bytes	30 ms	3,8	20 bytes	30 ms	34	20,8 kbps
G.726 (32 kbps)	20 bytes	5 ms	3,85	80 bytes	20 ms	50	55,2 kbps
G.728 (16 kbps)	10 bytes	5 ms	3,61	60 bytes	30 ms	34	31,5 kbps

Tabla 2.3 Códecs estandarizados de Voz IP [39]

Intervalo del códec (ms): Es el ejemplo de intervalo en el que el códec opera.

MOS: Es un sistema que clasifica la calidad de la voz de las conexiones telefónicas. Los oyentes juzgan con una escala que va del 1 (mala) al 5 (excelente).

Tamaño de la carga útil de voz (bytes): representa el número de bytes que rellenan un paquete y debe ser un múltiplo del tamaño del códec.

Tamaño de la carga útil de voz (ms): También se puede representar en términos de acuerdo al códec.

PPS: Representa el número de paquetes que es necesario transmitir por segundo para enviar la velocidad de bits del códec.

Las siguientes fórmulas se usan para el cálculo de ancho de banda:

$$\boldsymbol{Tamaño\ total\ del\ paquete} = (\textbf{encabezado capa 2 Ethernet}) + (\textbf{encabezado IP/UDP/RTP}) + (\textbf{tamaño de carga útil de voz})$$

$$\boldsymbol{Paquetes\ por\ segundo\ (PPS)} = \boldsymbol{(velocidad\ de\ bits\ del\ códec)} \Big/ \boldsymbol{(tamaño\ de\ la\ carga\ útil\ de\ voz)}$$

$$\boldsymbol{Ancho\ de\ banda\ (AB) = Tamaño\ total\ del\ paquete\ x\ PPS}$$

Considerando un tamaño de carga útil de voz de 20 bytes (160 bits), para el caso de la codificación G.729, se obtiene el ancho de banda de la siguiente manera:

$$\boldsymbol{Tamaño\ total\ del\ paquete} = \boldsymbol{(18\ bytes) + (20\ bytes + 8\ bytes + 12\ bytes) + (20\ bytes)}$$

$$\boldsymbol{= 78\ bytes\ \ = 78\ bytes\ x\ \frac{8\ bits}{1\ byte} = 624\ bits}$$

$$\boldsymbol{Paquetes\ por\ segundo\ (PPS) = (8\ kbps) \Big/ (160\ bits) = 50\ PPS}$$

$$\boldsymbol{Ancho\ de\ banda\ (AB) = 624\ bits\ x\ 50\ pps = 31,2\ Kbps}$$

Tomando en cuenta el valor del MOS de la tabla de códecs, los códec G.729 y G.711 se aprecian con una mejor calidad, pero se ha seleccionado para el diseño, el códec G.729 por ocupar un menor ancho de banda.

2.4.3 VIDEOCONFERENCIA

Las consideraciones para la solución de implementación del sistema de Videoconferncia, se tomó como referencia la documentación de Cisco Systems [40]

El protocolo H.323 es el estándar con la aceptación global de conferencias multimedia en una red IP. Por lo cual se describirá las recomendaciones para implementar la Calidad de Servicio (QoS) para las videoconferencias H.323 sobre una WAN.

Cuando se implementa terminales H.323, deben soportar el codificador-decodificador H.261 y con el soporte opcional para el estándar H.263.

El protocolo H.261 es un códec de video para servicios audiovisuales en múltiplos de 64 kbps. Mientras que el protocolo H.263 es un codec de video para el servicio telefónico sencillo (POTS).

En la tabla 2.4 se presentan los codificadores más utilizados para la transmisión de video que permiten comprimir y descomprimir el video digital.

Tipo de codec	Velocidad de Transmisión
H.261	4 Kbps hasta 2 Mbps
H.263	64 Kbps

Tabla 2.4 Codificadores de Video

Al aprovisionar tráfico de videoconferencia IP, se debe tomar en cuenta las siguientes consideraciones: [41]

- El tráfico debe estar marcado para DSCP AF41; el exceso de tráfico se puede marcar por un controlador de políticas a AF42 o AF43.
- Las pérdidas debe ser no más de 1%.
- Una calidad aceptable debe permitir entre 15 y 30 imágenes por segundo.
- La latencia debe ser no más de 150 ms.
- El *jitter* debe ser no más de 30 ms.

En la tabla 2.5 se muestra el ancho de banda necesario, de acuerdo a la calidad de imagen y una estimación de *overhead*.

Calidad	Ancho de Banda	Consumo real de ancho de banda +25%(overhead)
15 cuadros /seg	128 Kbps	160 Kbps
30 cuadros/seg	192 Kbps	240 Kbps

Tabla 2.5 Ancho de banda para Videoconferencia

El tráfico de voz y video tiene un tratamiento similar, manteniendo un ancho de banda constante. Para la transmisión del tráfico de video se considerará utilizar las recomendaciones del protocolo H.323.

2.4.4 INTERNET

Por las transacciones con varias entidades que se pueden realizar por este medio, el tráfico de Internet se lo realizará con una proyección de crecimiento a 3 años con una compartición de canal de 1:1, y con la factibilidad de tener redundancia de servicio.

CAPÍTULO 3
DISEÑO DE LA RED Y ANÁLISIS FINANCIERO

3.1 GENERALIDADES

Se analizarán los requerimientos de servicio para cada sede; y, para el diseño de la red del cliente se deben considerar recursos a nivel del acceso de última milla, que involucra el segmento de red desde el nodo más cercano del proveedor hasta la ubicación física del cliente; se consideran los recursos a nivel de planta externa y las características de los equipos a configurarse.

Por otra parte, se requiere la configuración a nivel de capa 2 con la asignación y configuración de las VLANs a nivel del cliente, la configuración en los *switches* ubicados en los nodos de acceso y la configuración en la nube Metroethernet.

Para la interconexión entre las diferentes sedes, se requieren recursos a nivel IP, que se configuran en los *routers* de cada sede y en la nube IP/MPLS. Además de las configuración de limitación de AB y calidad de servicio.

A continuación se detalla lineamientos de la metodología de diseño de una red Metroethernet; además se detallarán los equipos a utilizar a nivel de última milla. Posteriormente, se procede a diseñar la solución de la red de la Entidad Financiera, tomando en cuentra proyecciones y nuevos requerimientos

Es importante indicar que en el capítulo 4 se modelará una red Metroethernet.

3.1.1 METODOLOGÍA DE DISEÑO METROETHERNET

Las premisas para la implementación de la red Metroethernet están basadas en el documento de especificaciones técnicas TSD (*Technical Specification Document).* [42]

3.1.1.1 Lineamientos de implementación de la red Metroethernet

Se debe considerar que los *switches* van a operar en capa 2. Éstos van a tener las funcionalidades de monitoreo, configuraciones IP, pero no van a realizar las tareas de ruteo en capa 3, por lo cual la opción de ruteo va a estar deshabilitada en los *switches* Metroethernet.

Dentro del *backbone,* al manejar equipos Cisco, el protocolo de protección de capa 2 va a ser REP.

Hay anillos de agregación de alta capacidad de 10GbE o nx1 Gigas que concentran el tráfico de clientes o de múltiples servicios de clientes que provienen de redes de acceso asociadas a la red Metroethernet, como redes GPON, BPON o redes multipunto.

En las redes Metroethernet para tener una correcta administración se utilizará QinQ casi de extremo a extremo; deberá implementarse el doble *tag* de VLAN desde los puertos más lejanos o extremos dentro de la red hacia el cliente.

Se cuenta con anillos de *Core* con *switches* de *Core* Metro, que manejan los anillos de agregación de alta capacidad y los *switches* de acceso o de *edge* Metro que van a ser los que reciben los accesos de clientes.

Existe también *switches* de cliente que forman parte de un anillo, conectado en capa 2 que manejan la redundancia *dual-homing* conectados contra dos nodos.

3.1.1.2 Tipos de switches y equipos homologados

Los diferentes equipos homologados y tipos de nodos considerados en el TSD son equipos de la marca *Cisco Systems.*

3.1.1.2.1 Switches Principales

Se define a los equipos de las plataformas *Cisco 7606-S* o 7609-S que son concentradores principales donde se centraliza la mayor cantidad de tráfico. Son

equipos que van a tener conexiones hacia la red *IP* o *WHIP (World Hardiest IP Network)* y también las conexiones hacia redes de otros proveedores; para eso se hace mención a las interfaces *ENNIs (Ethernet network to network interfaces)*. Este tipo de nodo en sí mismo, forma segmentos REP que vendrían a transformarse en anillos de alta capacidad dentro de la red Metroethernet.

3.1.1.2.2 Switches secundarios

Pueden estar formados por plataformas *Cisco ME3800X*, *Cisco 7606-S o Cisco 7609-S* que son nodos secundarios pero que también forman parte del anillo de agregación principal o de alta capacidad y pueden recibir conexiones de otras redes Ethernet pero no van a manejar conexiones hacia la red IP.

3.1.1.2.3 Switches de acceso

Están definidos por plataformas Cisco *ME3600x o ME 3400E;* su propósito es el crecimiento de puertos, aumentando la capacidad de puertos que se puede tener dentro de un nodo**.**

En principio podrían recibir las conexiones de otras redes de acceso, como redes GPON o redes multipunto inalámbricas y recibir conexiones punto a punto directo de clientes, por ejemplo enlaces de fibra óptica punto a punto que vengan desde un cliente y se reciban en puertos de estos *switches*.

3.1.1.2.4 Switch menor o en el cliente

Están conformados por la plataforma de *switches Cisco ME3400E;* este tipo de *switch* sí puede formar parte de un anillo de acceso e incluso pueden referirse a un dispositivo de red, de *backbone* o un dispositivo de cliente. En principio se podría tener anillos de clientes con el protocolo REP conformados por múltiples nodos ubicados en los *switches Cisco ME3400* de cada cliente, pero en lo posible ya no se debería tener switches menores ubicados en las sedes del cliente formando anillos, porque si más de dos clientes apagan los *switches*, se dejaría sin servicio a los demás clientes del anillo.

3.1.1.2.5 Switch en el cliente

Este tipo de switch está contemplado para utilizar con *switches Cisco ME3400E*; principalmente es un equipo capa 2 dentro de la localidad del cliente.

Su acceso de última milla puede ser por medio de un acceso simple o con doble, ya sea con *EtherChannel* o con Agregación de Enlace o que forme parte de un anillo con único cliente. Los tipos de *switches* y su estructura general se indican en la figura 3.1.

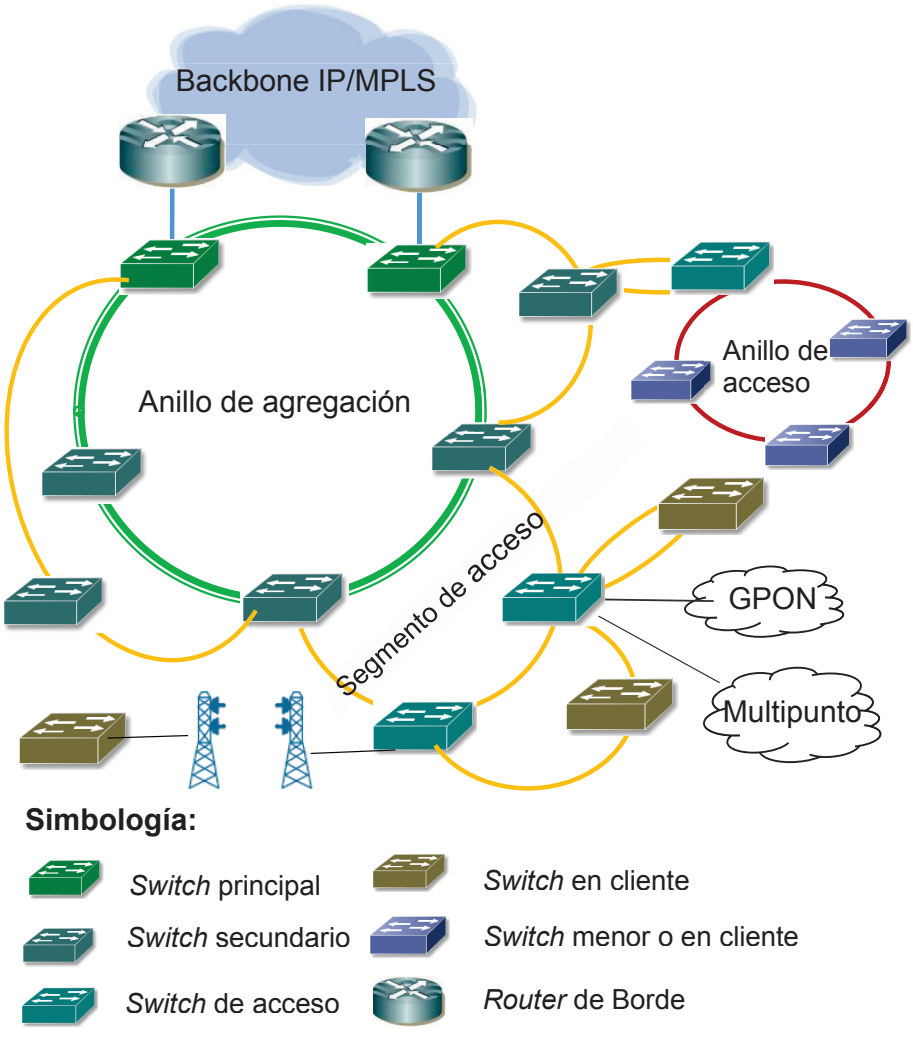


Figura 3.1 Tipos de *switches* de una red Metroethernet

3.1.1.3 Equipos para la implementación inicial

Varias características importantes de las plataformas se deben considerar como por ejemplo la capacidad de aprendizaje de direcciones MAC, el MTU que soportan, la cantidad de *bridge domains* o *VLANs* activas que podría tener cada plataforma dependiendo el caso y el sistema IOS recomendado, tal como se indica en la tabla 3.1.

Plataforma	Aprendizaje Mac address	MTU	Bridge Domains / Active VLANs	IOS
Cisco 7606-S or 7609-S with RSP720-CXL	96000	9216	4000	c7600rsp72043-advipservicesk9-mz.122-33.SRD6.bin
ME3800X	64000	9800	4000	me380x-universalk9-mz.152-2.S.bin
ME3600X	8000	9800	4000	me360x-universalk9-mz.152-2.S.bin
ME3400E	8000	9000 (1998 for FE)	1005	me340x-metroipaccessk9-mz.122-55.SE.bin / me340x-metroipaccessk9-mz.122-55.SE3.bin

Tabla 3.1 Características de equipos Cisco

En los equipos *Cisco 7600, ME 3800X y ME3600X* para forzar el MTU a los valores máximos hay que definir la especificación por interfaz con el comando ***mtu***, mientras que en los equipos *Cisco ME3400E* hay que hacerlo en la configuración de manera global y esto implica un reinicio del equipo para que tome efecto el comando. El comando es ***system mtu*** y luego especificar el MTU; para interfaces Gigabit Ethernet el comando ***system mtu jumbo*** y luego se debe especificar el soporte de *jumbo frames* a 9000 bytes.

Además en los equipos Cisco ME3400E si se necesita soportar las 8000 direcciones MACs, en lugar de las 5000 MACs que es el valor por defecto, se debe especificar en la configuración de manera global el comando ***sdm prefer layer-2;*** pero con ello se modifican algunas características de capa 3 por ejemplo, se resta capacidad en cuanto a manejo de tablas en capa 3, por lo tanto es importante tomar esta consideración al inicio de la implementación del equipo.

Los IOS recomendados deberían considerar algunas características que se van a tener dentro de los equipos. Al no usar los IOS recomendados se pueden tener problemas por ejemplo en el funcionamiento del protocolo REP donde se podría generar trafico *multicast* excesivo o donde se podrían generar *loops* o para el caso de *QinQ*, que no exista en realidad la encapsulación adecuada con *QinQ* en algún momento determinado.

3.1.1.4 Administración de VLAN

Se debe tomar en cuenta las recomendaciones en cuanto al manejo de la administración del espacio de las VLAN ID, particularmente para la implementación QinQ cuando se hace referencia a las *Service VLANs (*S-VLANs*)* las cuales encapsularán a las *Customer VLANs (*C-VLANs*)*, como se indica en la tabla 3.2. En la práctica se está sujeto de acuerdo al crecimiento de la utilización de VLANs con el tiempo.

S-VLAN IDs per domain (range)		Use
1	400	Reserved (Management)
401	1000	Basic L2 customer services (QinQ implementation on net)
1001	1600	Advance L2 customer services (without QinQ implementation on net)*
1601	2000	IP VPN Services
2001	2400	Third Parties L2 NNI – eNNI
2401	2700	Massive Services (Internet)
2701	2900	Massive Services (Telephony)
2901	3093	Future assignments
3094	4096	Reserved

Tabla 3.2 Espacio de Administración ID de VLAN [43]

3.1.2 PREMISAS GENERALES METROETHERNET – IP/MPLS

Las premisas generales están basados en la documentación TSD de implementación de Level3.

Una red Metroethernet es una red de acceso de alta disponibilidad en capa 2, conformada por un anillo principal de agregación y varios segmentos de *switches* en subanillos**.**

Se alcanza la nube IP/MPLS solo desde un *switch* principal del anillo de agregación a través de interfaces GE o 10GE. Estas interfaces utilizarán conexiones virtuales Ethernet para manejar los servicios de Ethernet a través de ellos.

El uso de múltiples *routers* de *Edge* permitirá el balanceo de carga de los servicios entre los equipos. Los servicios de capa 3 requieren un acceso de alta disponibilidad, así como un esquema de protección, por lo que se puede utilizar sesiones BGP entre el CPE del cliente hacia los *routers* de borde.

El anillo principal de agregación debe tener la más alta capacidad de ancho de banda del dominio Metroethernet y debe estar compuesto por estrategias de implementación de puerto con agregación, con el propósito de aumentar la capacidad de ancho de banda de acuerdo al crecimiento de la red.

La topología Metroethernet e IP/MPLS, se interconectan por medio de troncales nacionales e internacionales; de esta manera se provee conectividad a un cliente entre sedes ubicadas en distintos lugares.

El esquema general de interconexión de topologías Metroethernet IP/MPLS se indica en la figura 3-2.

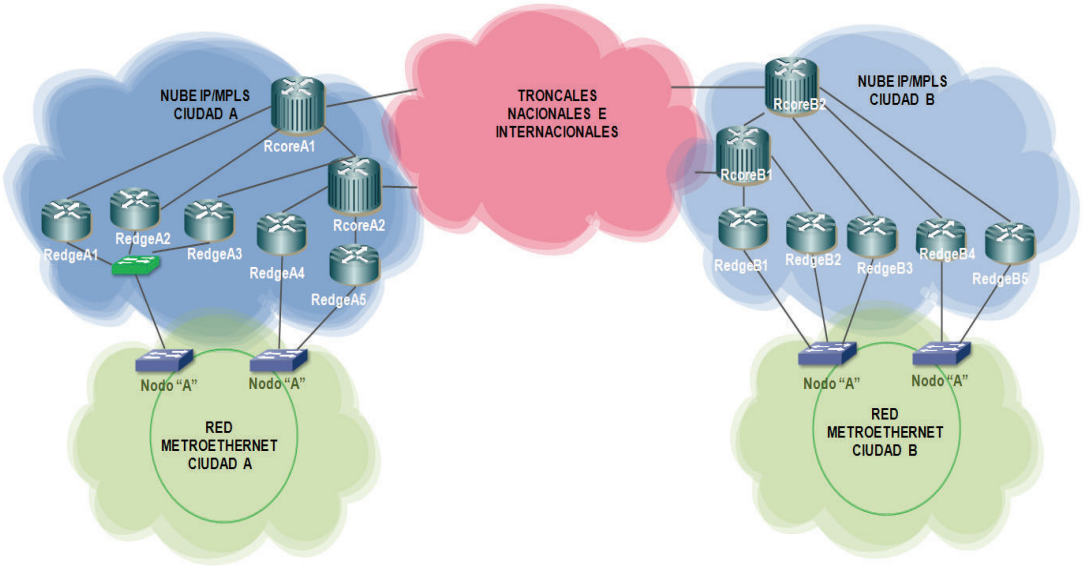


Figura 3.2 Interconexión General Metroethernet IP/MPLS

3.2 ALTERNATIVA DE INTERCONEXIÓN ENTRE OFICINAS REMOTAS

A continuación se realiza una descripción de los tipos de equipos, sus características y los parámetros necesarios para su configuración, de acuerdo al tipo de acceso de última milla.

3.2.1 ACCESOS INALÁMBRICOS

3.2.1.1 Enlace multipunto WIMAX

La IEEE definió un estándar para el despliegue de redes inalámbricas de banda ancha conocido como WIMAX (*Worldwide Interoperability for Microwave Access).*

Esta tecnología se definió bajo la norma IEEE 802.16 para un acceso inalámbrico de alta velocidad y bajo costo, con facilidad de implantación que provee una solución escalable.

Actualmente se dispone de varias versiones como las detalladas en la tabla 3.3.

Estándar	Descripción	Estado
802.16-2001	Fixed Broadby Wireless Access (10–66 GHz)	Reemplazada
802.16.2-2001	Práctica recomendada para coexistencia	Reemplazada
802.16c-2002	Perfiles de sistema para 10–66 GHz	Reemplazada
802.16a-2003	Capa física y definiciones de MAC para la banda de 2–11 GHz	Reemplazada
P802.16b	Frecuencias exentas de licencia (Proyecto retirado)	Retirada
P802.16d	Mantenimiento y perfiles de sistema para 2–11 GHz (Proyecto fusionado con 802.16-2004)	Fusionado
802.16-2004	Interfaz aérea para conexión a un punto de acceso fijo de banda ancha (Paquete acumulativo de 802.16-2001, 802.16a, 802.16c y P802.16d)	Reemplazada
P802.16.2a	Coexistencia con 2–11 GHz y 23.5–43.5 GHz (Proyecto fusionado con 802.16.2-2004)	Fusionado
802.16.2-2004	Prácticas recomendadas para coexistencia (Proyecto fusionado con 802.16.2-2004) (Mantenido y paquete acumulativo de 802.16.2-2001 y P802.16.2a)	En uso
802.16f-2005	Base de información para 802.16-2004	Reemplazada
802.16-2004/Cor 1-2005	Correcciones para operaciones fijas (co-publicado con 802.16e-2005)	Reemplazada
802.16e-2005	Mobile Broadband Wireless Access System	Reemplazada
802.16k-2007	Puenteo en redes 802.16 (una ampliación de IEEE 802.1D)	En uso
802.16g-2007	Procedimientos plano de gestión y servicios	Reemplazada
P802.16i	Gestión de la base de información móvil (Proyecto Fusionado en 802.16-2009)	Fusionado
802.16-2009	Interfaz aérea para acceso a un punto fijo de banda ancha (paquete acumulativo de 802.16-2004, 802.16-2004/Cor 1, 802.16e, 802.16f, 802.16g y P802.16i)	En uso
802.16j-2009	Retransmisión multisalto	En uso
802.16h-2010	Mecanismos mejorados de coexistencia para operación exenta de licencia.	En uso
802.16m-2011	Interfaz aérea avanzada con tasa de transferencia de 100 Mbit/s móvil y 1 Gbit/s sobre punto fijo. También se conoce como Mobile WiMAX. Con el objetivo de cumplir con los requerimientos de ITU-R IMT-Advanced para sistemas 4G. Release 2 o WirelessMAN-Advanced.	En uso
P802.16n	Redes de mayor fiabilidad	En desarrollo
P802.16p	Mejoras para soportar aplicaciones con conexión Máquina a Máquina (Machine-to-Machine)	En desarrollo

Tabla 3.3 Versiones norma IEEE 802.16 [44]

La versión del estándar fijo es WIMAX 802.16-2004, el cual es referenciado en algunas ocasiones como 802.16d. Es esencialmente independiente de la frecuencia, permitiendo operación sin línea de vista *(NLoS non line-of-sight)* en el límite inferior del rango de frecuencia.

Las interfaces de acceso de radio están basadas en la tecnología OFDM [2]*(Orthogonal Frequency Division Multiplexing)* con 256 subportadoras. OFDM permite una buena respuesta al desvanecimiento multicamino *(multipath fading).* Los rangos de ancho de banda del canal van desde 1.5 a 10 MHz, y FDD o TDD como mecanismo de duplexación.

Los detalles técnicos de los equipos Airspan se adjuntan en el Anexo D. Las características generales de los equipos se detallan en la tabla 3.4.

Marca	Airspan
Modelo Base	BSR Micromax SOC
Versión de software	SR7.8
MTU Max	1560 bytes
Sistema de gestión	Netspan software 7.80.002
Modelo de remota	SS ProST y EasyST
Tecnología de acceso	OFDM 256 subportadoras
Banda de Frecuencia	**Ancho de banda de canal**
1,42 – 1,52 GHz in TDD mode	1,5 MHz, 1,75 MHz, 3,5 MHz, 5 MHz
3,3 – 3,5 GHz in TDD mode	1,75 MHz, 2,75 MHz, 3 MHz, 3,5 MHz, 5 MHz
3,4 – 3,5 GHz in FDD mode	1,75 MHz, 3,5 MHz, 5 MHz
3,4 – 3,6 GHz in FDD mode (Lo, Hi)	1,75 MHz, 3,5 MHz
3,4 – 3,6 GHz in TDD mode	1,75 MHz, 3,5 MHz, 5 MHz
3,6 – 3,8 GHz in FDD mode (Lo, Hi)	1,75 MHz, 3,5 MHz
3,6 – 3,8 GHz in TDD mode	1,75 MHz, 3,5 MHz, 5 MHz, 7 MHz
4,9 – 5,0 GHz in TDD mode	2,5 MHz, 5 MHz, 10 MHz
5,15 – 5,35 GHz in TDD mode	2,5 MHz, 5 MHz, 10 MHz
5,47 – 5,725 GHz in TDD mode	2,5 MHz, 5 MHz, 10 MHz
5,725 – 5,875 GHz in TDD mode	2,5 MHz, 5 MHz, 10 MHz
5,85 – 5,95 GHz in TDD mode	2,5 MHz, 5 MHz, 10 MHz

Tabla 3.4 Características de equipos de radio marca Airspan

[2] "OFDM es la combinación de dos o más canales de información en un solo medio de transmisión el cual envía un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM, PSK o QPSK."[45]

El tamaño de la celda WIMAX es independiente de la banda de frecuencia de operación utilizada, pero el radio de cubrimiento típico de los equipos de las estaciones base van de 1 a 2 Km para enlaces NLoS y hasta los 10 a 16 Km para enlaces con línea de vista.

3.2.1.1.1 Elementos del sistema Micromax

El sistema de radio multipunto consta de los siguientes componentes:

Radio Base
Unidad exterior

- Equipo ODU de la estación radio base del equipo MicroMAX (BSR)
- Antena externa TILTEK TA-1404F-4 (opcional), cuya ganancia puede ser de: 15dBi@60°, 13dBi@90°, 12dBi@120°, 10,5dBi@160° como se indica en la figura 3.3.

Unidad Interior:

- Modem SDA-4SDC Tipo II con alimentación de 48 V que incorpora un *switch* LAN.
- BSDU es responsable de la conectividad, sincronización y alimentació de -48 voltios a múltiples BSRs.

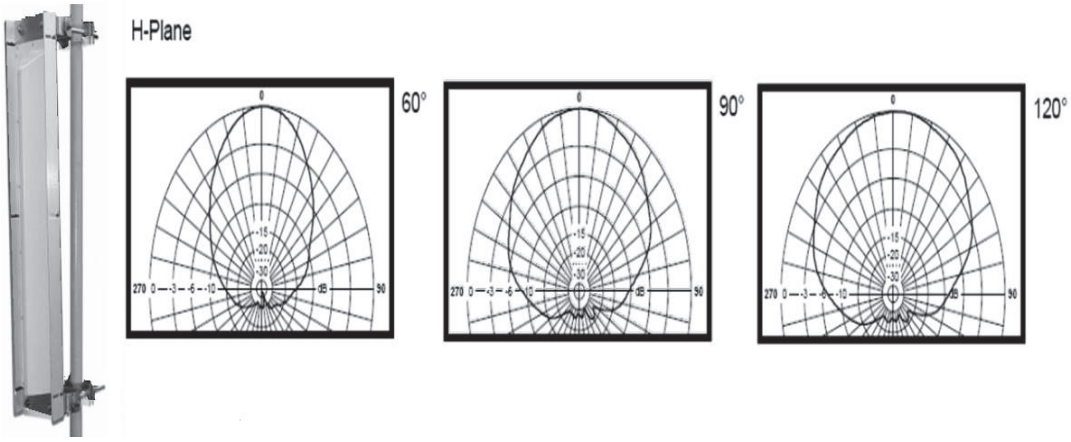


Figura 3.3 Antena Externa Tiltek

Estación Remota
Unidad Exterior

- Equipo remoto MicroMAX (ProST).

Unidad Interior:

- SDA-4S Tipo II: IDU que incorpora un *switch* LAN.

Conectividad IDU / ODU

La BSR requiere un cable blindado SFTP CAT 5e, con una distancia máxima de 100 metros. En la figura 3.4 se indica la forma de conexión de los equipos con los diferentes tipos de conectores.

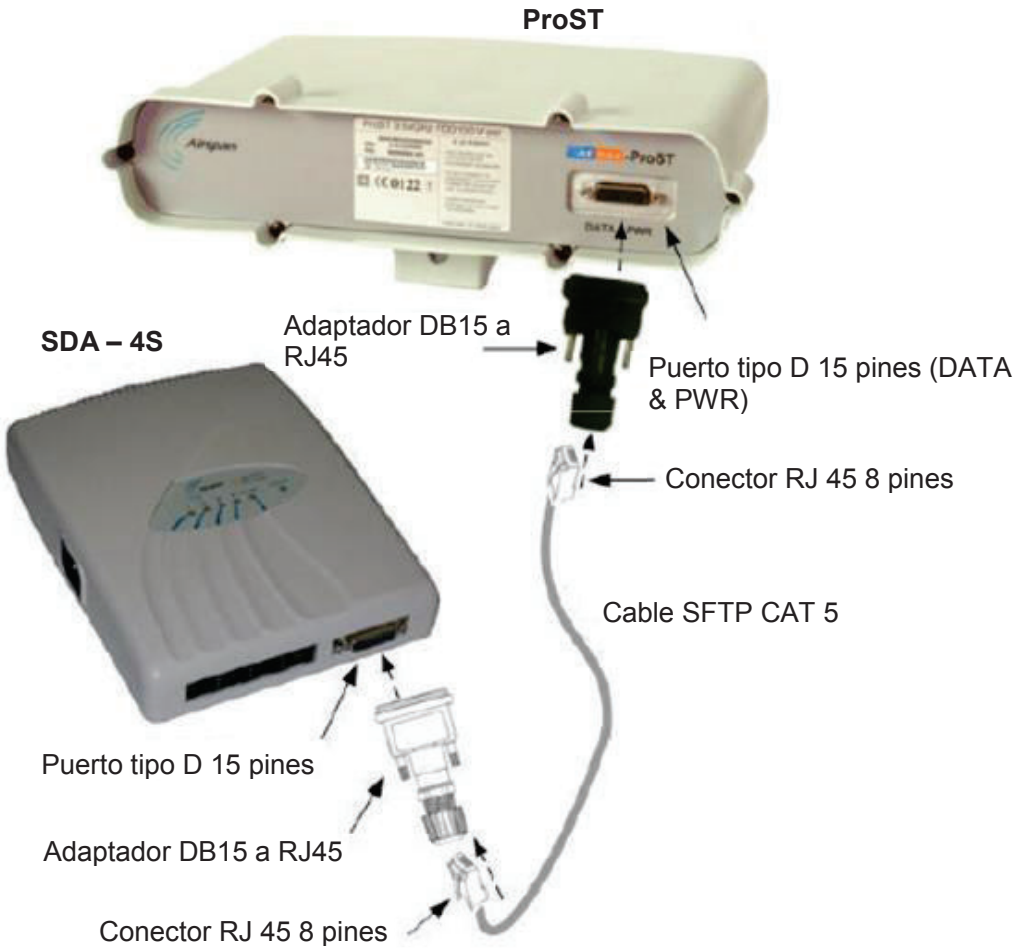


Figura 3.4 Conectividad entre los equipos ODU e IDU

Características del sistema

La codificación y modulación es adaptativa para optimizar el aprovechamiento del canal de comunicaciones ante condiciones cambiantes de propagación e interferencia desde ½ BPSK hasta ¾ 64QAM.

Con los diferentes tipos de modulación se tienen los parámetros en la frecuencia de operación con un AB de 3.5 MHz, que se indican en la tabla 3.5.

MODULATION	FEC	Rx Sensitivity 5 Mhz (dBm)	SNR (dB)	Total system gain (dB)
64 QAM	3/4	-75,4	27	102,4
64 QAM	2/3	-77,2	26,3	103,5
16 QAM	3/4	-80,5	21,9	102,4
16 QAM	1/2	-85,1	17,6	102,7
QPSK	3/4	-86,9	15,9	102,8
QPSK	1/2	-89,8	12,7	102,5
BPSK	1/2	-95,7	5,4	101,1

Tabla 3.5 Parámetros con diferentes tipos de modulación

Software de Gestión

Las configuraciones de operación de los equipos se realizan por medio del sistema de gestión de red *Netspan*.

Las bases BSR y las remotas ProSt pueden ser configuradas por medio de una página HTTP, asi como para la inicialización de los equipos y para realizar *upgrades* individuales de *software*, como se indica en la figura 3.5.

3.2.1.1.2 Wimax MAC y QoS avanzado

Un sofisticado mecanismo de calidad de servicio de bajo nivel fue definido para permitir a los operadores el envío de los servicios y cumplir así con acuerdos de SLA.

Los flujos son asignados a las remotas a través de los servicios de producto. Un servicio de producto puede contener hasta 16 flujos de servicio. Las especificaciones de QoS están definidas en las clases de servicio.

Las reglas de clasificación filtran el tipo de tráfico sobre el cual se va a aplicar un cierto criterio de QoS, indicado en la figura 3.6.

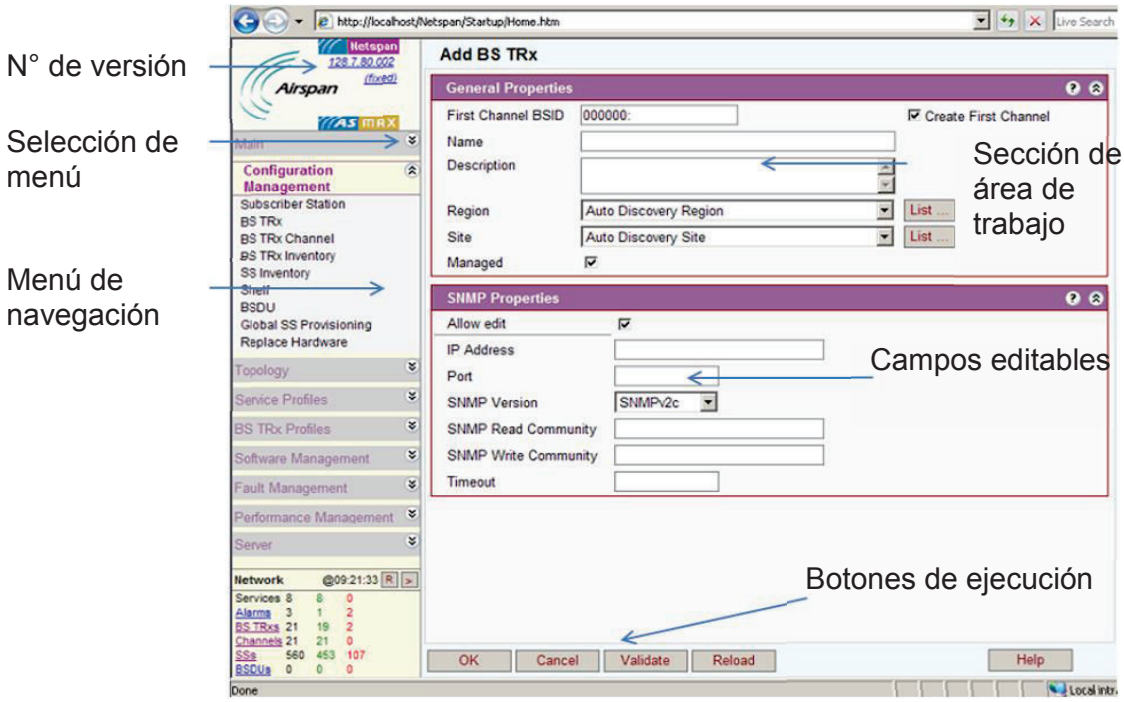


Figura 3.5 Sistema de gestión Airspan

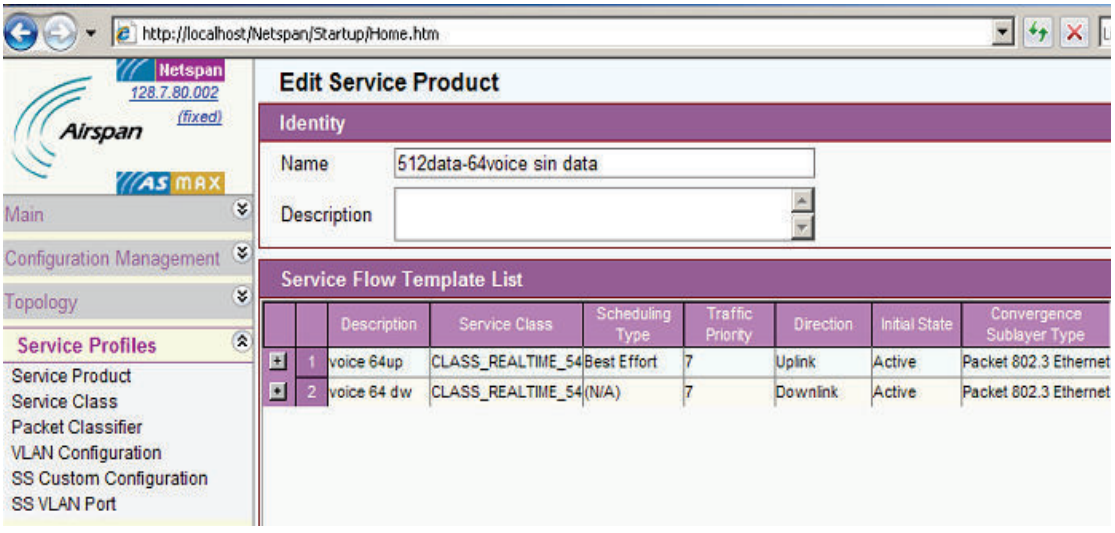


Figura 3.6 Perfiles de servicio equipo Airspan

Una regla de QoS definida en una clase de servicio puede estar asociada con una o más reglas de clasificación.

La calidad de servicio QoS y los mecanismos de manejo de ancho de banda están asociados con el provisionamiento de los flujos.

Todo el tráfico de la remota se clasificará en capa 3 mediante el Byte TOS, usando los bits de precedencia IPP, de acuerdo a la tabla 3.6.

Nombre	PHB	IPP	bits 7,6,5	Observaciones	Prog. Micromax	Prioridad
Tiempo Real	EF	5	101	VoIP	BE	7
Video	AF41	4	100	Video solamente	BE	6
Crítica	AF31	3	011	Aplicación definida por cliente	BE	4
Prioritaria	AF21	2	010	Aplicación definida por cliente	BE	2
Estándar	AF11	1	001	Mínima Calidad MPLS/VPN	BE	2
Best Effort	BE	0	000	Tráfico Internet Exclusivo	BE	0

Tabla 3.6 Clasificación de tráfico

3.2.1.1.3 Asignación de recursos

Los parámetros de configuración necesarios que se deben ingresar en el sistema de gestión para habilitar y provisionar a la estación remota son los siguientes:

- Nombre del cliente.
- MAC-Address de la estación remota.
- VLANs
- Puerto de la VLAN
- Velocidad del canal
- Flujos de tráfico
- Dirección IP
- Máscara de subred
- *Default gateway*
- Modo de asignación de direccionamiento
- Frecuencia de operación
- Ancho de Banda

Se debe considerar que las estaciones remotas que corresponden a la misma radio base deben tener una separación mínima de un metro.

Mientras que en las remotas que corresponden a radio bases diferentes, la separación mínima debe ser de 3 metros. Además la VLAN de gestión viaja como parte del tráfico.

3.2.1.2 Enlace de radio punto a punto

A continuación se describen las características y modo de operación de los equipos de la gama *Ceragon*, información tomada de los manuales técnicos y documentos de especificaciones técnicas (TSD).

Los detalles completos de la gama de equipos Ceragon se detallan en el Anexo E.

3.2.1.2.1 Elementos del sistema

- **EQUIPO MODEM DE RADIO (IDU)**

El equipo de radio modelo *IP10- E-Series* permite tener 2 puertos *gigabitethernet* y cinco puertos *fastethernet*. Básicamente los equipos se utilizarán como un *bridge* punto a punto entre nodo y cliente, tomando en cuenta las recomendaciones del TSD.

El modelo *IP10-G –Series*, cuenta con un *slot* de expansión para insertar módulos con puertos para manejar el tráfico Ethernet y TDM. Hay tarjetas de 16 E1s y de STM1s. Estos modelos se indican en las figuras 3.7 y 3.8.

Figura 3.7 Equipo IDU Ceragon IP10-E

Figura 3.8 Equipo IDU Ceragon IP10-G

Por medio de un *shelf* se pueden hacer nodos con agregación de canales de radio frecuencia, donde se apilan los equipos para tener una mayor capacidad.

La licencia estándar de los equipos es de 10 Mbps, pero se pueden tener licencias de diferente capacidad tanto para Ethernet como para TDM.

Los equipos tienen la opción de soluciones de redundancia en modo *hot standby,* que es una configuración de protección, que usa dos canales de radio, dos *ODUs* y dos *IDUs*, donde un equipo trabaja como principal y otro como *backup*, como se indica en la figura 3.9.

Figura 3.9 Modo de operación redundante

En la figura 3.10 se detalla el tipo y operación de cada puerto del equipo modem.

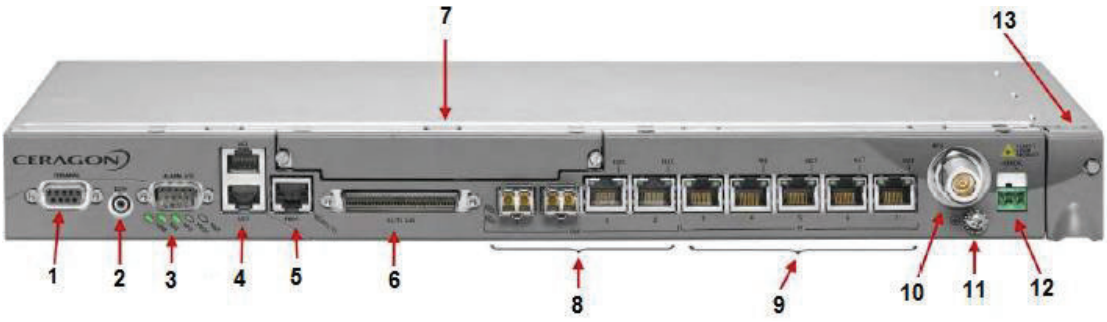


Figura 3.10 Detalles del equipo IDU Ceragon IP10-G

1. Puerto BDB9 para administración del equipo
2. Puerto de comunicación con *headset*
3. Puerto de alarmas externas (DB9)
4. Puertos asincrónicos/sincrónicos para monitoreo (canales de usuario RJ45)
5. Puerto de protección (RJ45)
6. Módulo de 16 E1s (opcional)
7. *Slot* de expansión para módulos de tarjetas de 16E1, STM1 (Las tarjetas se colocan con el equipo apagado)
8. Dos pares de puertos GbE (Puerto óptico SFP o eléctrico RJ45, se habilita uno a la vez).
9. Puertos Fastethernet para datos y gestión (puertos 3-7)
   Los puertos GBE y Fastethernet soportan QoS.
10. Interfaz RF (tipo N), se conecta el cable que viene de la ODU.(Cable no mayor de 300 metros.
11. Conexión a tierra
12. Alimentación del equipo es de -48 VDC.(el umbral de operación es de -40,5 VDC a -57,5 VDC)
13. Compartimiento del ventiladores

En cuanto al estado de los *leds* de equipo, como se indica en la figura 3.11 presentan diferentes colores de acuerdo al tipo de operación.

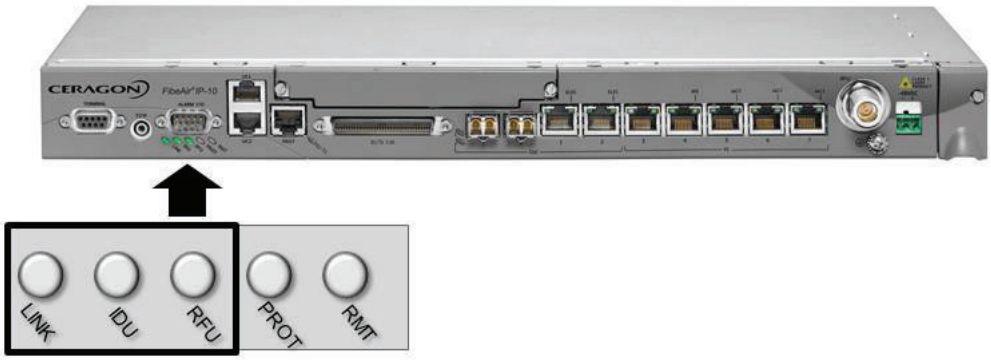


Figura 3.11 Estado de los leds del equipo

LINK

VERDE: Radio operativo, el nivel de recepción es adecuado.

ANARANJADO: Alarma menor de tasa BER en la radio

ROJO: Pérdida de señal, alarma mayor de tasa de BER en la radio.

IDU

VERDE: Función normal de la IDU.

ANARANJADO: Falla en los ventiladores.

ROJO: Alarma mayor en la IDU.

RFU

VERDE: Operación normal de la ODU

ANARANJADO: Pérdida de la comunicación entre la IDU y la ODU.

ROJO: Falla de la ODU.

PROT

APAGADO: Protección deshabilitada o no soportada en el equipo.

VERDE: La radio trabaja en modo principal en el enlace protegido, y no hay alarmas presentes.

AMARILLO: La radio trabaja en modo *standby* en el enlace protegido y no hay alarmas presentes.

ANARANJADO: Protección activada, falla del enlace principal.

ROJO: Errores físicos, falla de cable o del puerto de protección.

RMT

VERDE: Operación normal de la radio remota, sin alarmas.

ANARANJADO: Alarma menor en la radio remota.

ROJO: Alarma mayor en la radio remota.

- **EQUIPO DE RADIO FRECUENCIA ODU**

El equipo va a operar en la banda licenciada de 23 GHz usando la unidad de RF RFU-C *Outdoor*, equipo ilustrado en la figura 3.12.

El consumo de potencia se detalla en la tabla 3.7, el cual varía de acuerdo a la banda de trabajo y al sistema de redundancia que se haya implementado.

Figura 3.12 Unidad RF *Standard Power* 6-42 GHz

RFU Band	1+0 Configuration	1+1 Configuration
6 – 26 GHz	22 W	39 W
28 – 38 GHz	26 W	43 W

Tabla 3.7 Consumo de potencia [46]

El trabajar en la banda de 23 GHz condiciona el tipo de portadora que se asigne, dependiendo de la capacidad que el cliente requiera será la modulación con que va a operar el enlace, es decir en 23 GHz se trabaja con portadoras de 3,5, 14 y 18 MHz y dependiendo del ancho de banda de la portadora se puede tener varias opciones de modulación. Con 18 y 14 MHz se tienen todas las opciones de modulación disponibles. Mientras con 3,5 MHz se tienen 2 tipos de modulación 16 QAM y 64 QAM (a mayor modulación menor potencia).

En la tabla 3.8, se tienen las especificaciones de la Potencia de Transmisión (dBm) para equipos Ceragon FibeAir IP-10.

Modulation	6-8 GHz	11-15 GHz	18-23 GHz	26 GHz	28 GHz	36 GHz	38 GHz
QPSK	26	24	22	21	14	12	18
8 PSK	26	24	22	21	14	12	18
16 QAM	25	23	21	20	14	11	17
32 QAM	24	22	20	19	14	10	16
64 QAM	24	22	20	19	14	10	16
128 QAM	24	22	20	19	14	10	16
256 QAM	22	20	18	17	12	8	14

* All values are guaranteed values.

Tabla 3.8 Especificaciones de Potencia de Transmisión para equipos Ceragon

Para el apuntamiento del enlace, la unidad de radio frecuencia (RFU) cuenta con un conector BNC para medir el AGC por medio de un multímetro, que va a ser proporcional al nivel de recepción que se va a tener en la IDU. El AGC puede variar entre 1,2 a 1,7 VDC (voltios DC) medidos en el conector BNC de la RFU. La relación de valores se indica a continuación:

1,30 VDC = -30 dBm

1,45 VDC = -45 dBm

1,60 VDC = -60 dBm

- **GESTOR DE ADMINISTRACIÓN**

Se administra la radio por medio de un portal Web, el mismo que presenta las alarmas activas e histórica, y con el contador de estadísticas (RMON) se puede tener registros de paquetes errados, descartados, recibidos, entre otros.

A nivel de RF el equipo permite obtener estadísticas a nivel de recepción de la señal, puerto agregado, MRMC (*Multi Rate Multi Coding*), MSE (*Mean Square Error*) que es un parámetro calculado del nivel de recepción con relación al ruido, tal como se indica en la figura 3.13.

En la opción configuración, el submenú parámetros de equipo despliega la información del nombre del sistema, dirección IP asignada, persona de contacto,

tiempo que el sistema ha estado operativo, el voltaje de entrada a la IDU, los niveles de temperatura de la IDU y ODU, entre otros.

Además se tienen las opciones para configurar la hora y fecha e información serial del equipo que es importante al momento de enviar la solicitud de una licencia de actualización para ampliar la capacidad de operación del equipo Para las alarmas externas, se tienen 5 entradas de alarmas y una salida, que pueden ser configuradas con una determinada prioridad.

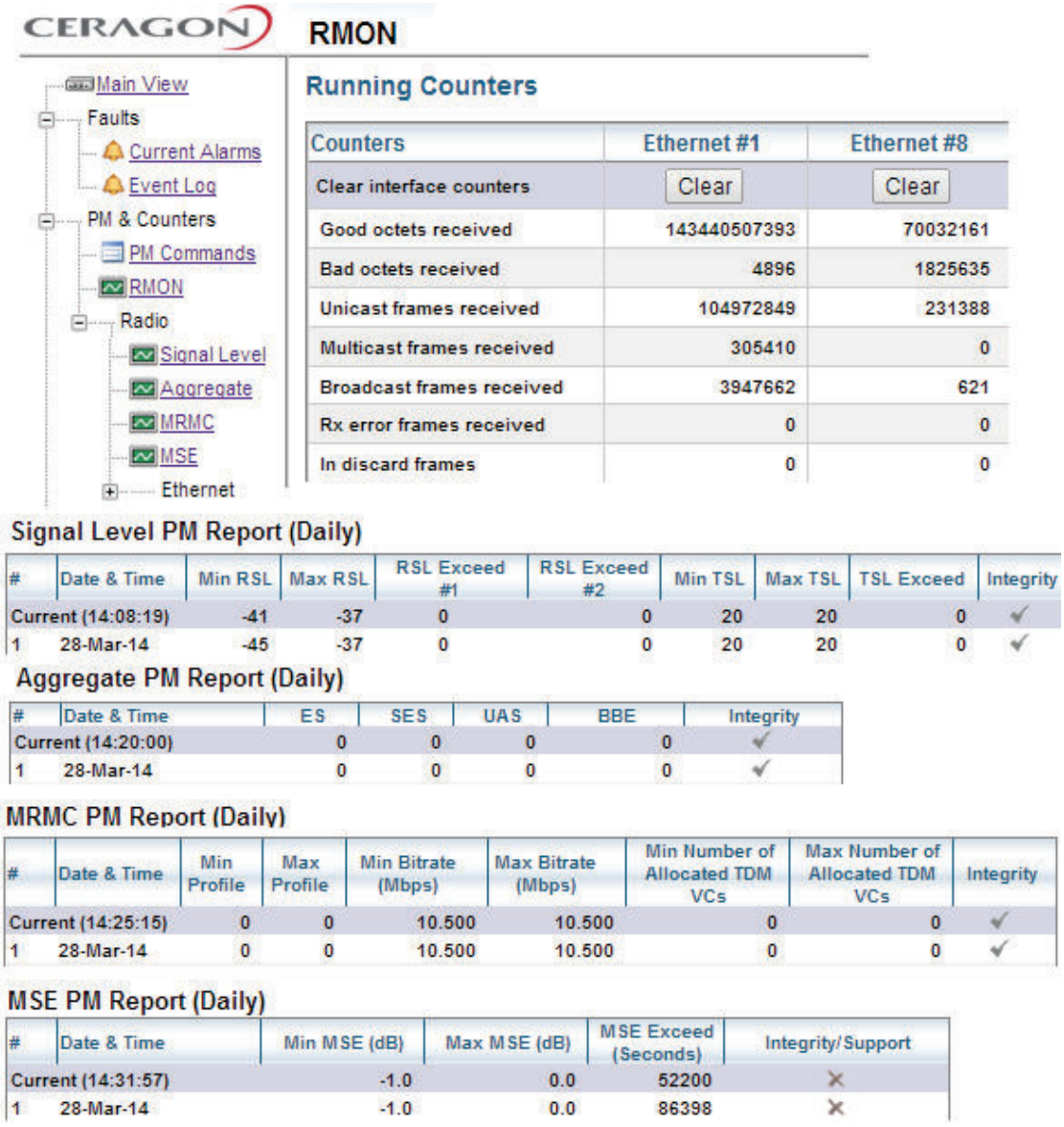


Figura 3.13 Reporte de Estadísticas

En el submenú Administración se configura la dirección IP, máscara y *Gateway*.

Además se pueden habilitar hasta 3 puertos de gestión que corresponden a los puertos 5, 6 y 7. Si se configura la VLAN de gestión con la opción *In Band*, implica que la gestión va a ir en el canal de datos del cliente; pero si está con la opción de *Out Band*, la gestión va a ser transportada independiente del canal de datos del cliente. Se especifica el tipo de negociación del puerto con las opciones 10 o 100 Mbps, en half o full dúplex o en modo auto.

Los equipos cuentan con una licencia demo con una validez de 60 días, con este licenciamiento el equipo habilita todas la características que pueda tener. Además el equipo tiene un contador el cual se lo puede pausar, de acuerdo al uso. Si se define la licencia que se va a usar, se compra y el proveedor la entrega en un sitio web, donde se ingresa el número serial de la IDU y se asocia la licencia que se necesita. El portal genera un código que se ingresa en el campo *Licence code*, de esta manera queda habilitado el equipo con la licencia que se ha comprado. Para la actualización de la licencia se requiere reiniciar el equipo. Todos estos parámetros se indican en la figura 3.14.

En el submenú parámetros de la radio, se configura las frecuencia de operación, la habilitación de la interfaz IF, nivel máximo de potencia, entre otros. Además en la opción MRMC se tiene los diferentes perfiles para configurar la capacidad del equipo, tal como se indica en la figura 3.15.

La IDU Fiber Air IP-10 utiliza modulación adaptativa (ACM) tiene 8 pasos de modulación diferentes desde QPSK hasta 256 QAM. Esta configuración cambia dependiendo de las condiciones del ambiente y del margen de desvanecimiento para mantener una señal de radio estable; este proceso es automático.

La radio cuenta con varios perfiles preconfigurados que le permiten conmutar en el caso de degradación. La radio hace un cálculo del nivel MSE y el módulo define hacer la conmutación de la modulación para que el enlace se mantenga estable y permanezca en las condiciones de disponibilidad.

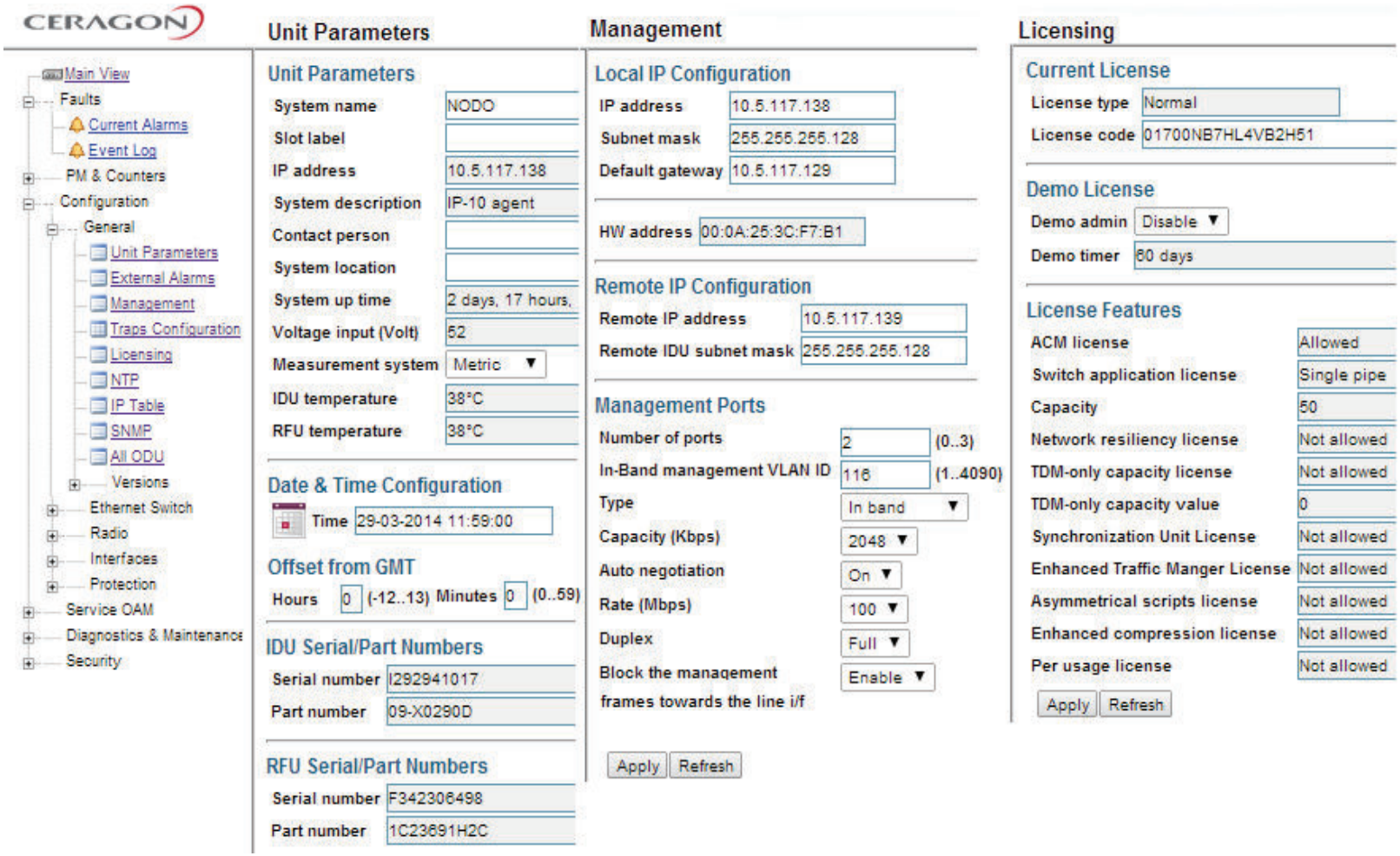


Figura 3.14 Configuración general del equipo Ceragon

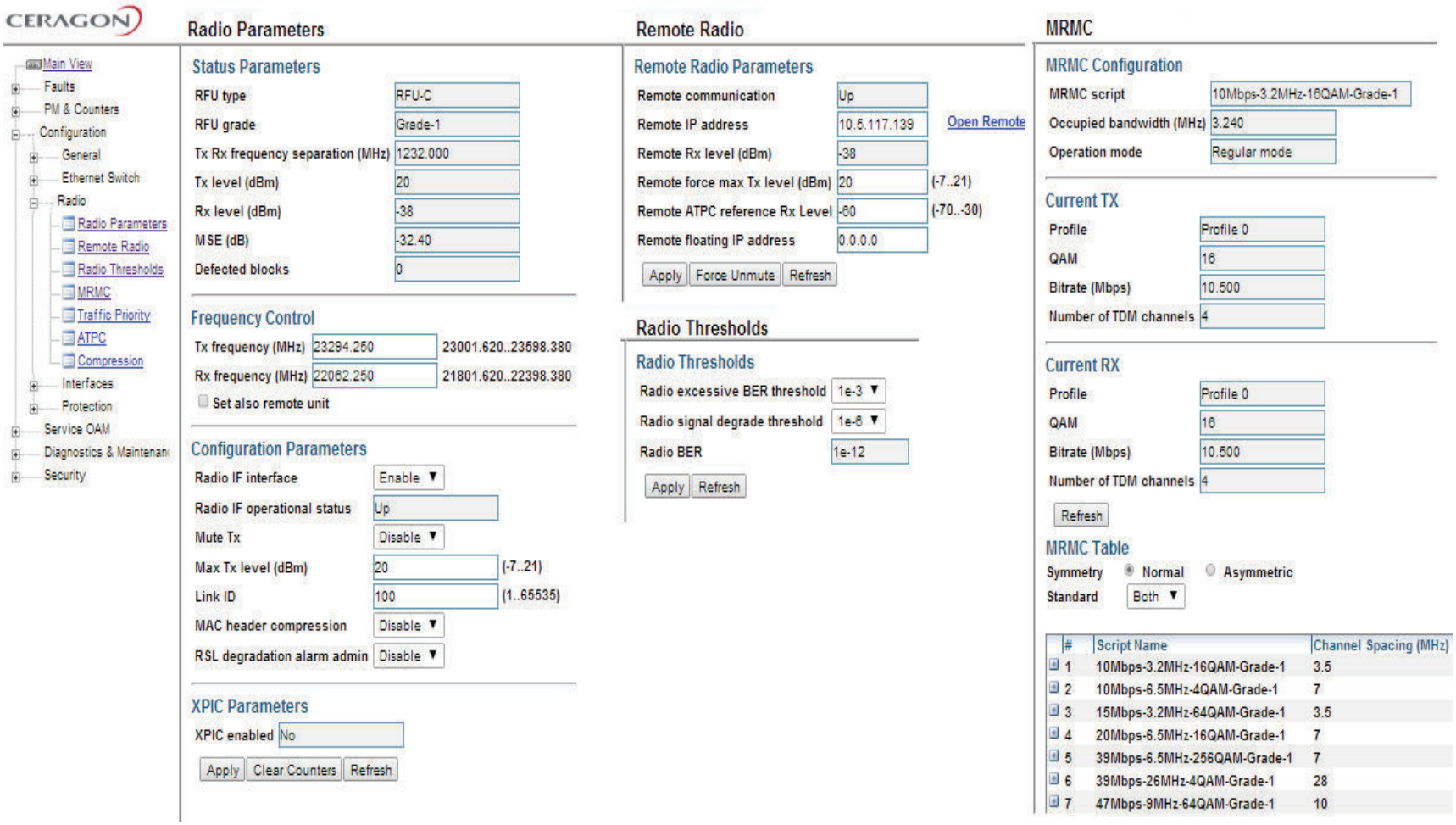


Figura 3.15 Configuración de los parámetros de la radio Ceragon

En condiciones normales se puede configurar la modulación, pero a medida que las condiciones ambientales cambian, el equipo va a hacer el recálculo del MSE y automáticamente va a pasar a la siguiente modulación, nuevamente calcula y verifica que su nivel de recepción sea adecuado para mantener la disponibilidad; se mantiene en ese nivel hasta que las condiciones del medio cambien.

El equipo ajusta su modulación a las condiciones climáticas favorables o desfavorables. A mayor modulación se tiene mayor capacidad en radio frecuencia, por lo cual se debe proveer al cliente una licencia adecuada que permita la capacidad que necesita y que, a pesar de los cambios que existan según la modulación adaptativa, mantenga la capacidad que el cliente requiera.

La capacidad que puede tener la radio depende del ancho de banda de la portadora; para Ecuador se trabaja con portadoras de 3.5 MHz, 14 MHz y 28 MHz.

Para 28 MHz se obtiene un *throughput* promedio entre 45 y 220 Mbps; con una portadora de 14 MHz se va a tener entre 25 y 100 Mbps. Mientras con una portadora de 3,5 MHz se tiene hasta 10 Mbps. Estas capacidades dependen de la licencia y de la modulación.

En el submenú interfaces se configuran los puertos Ethernet, asi como un ancho de banda dedicado para un uso específico (*Wayside channel*) y el sincronismo, tal como se indica en la figura 3.16.

El equipo además permite manejar QoS, hacer limitación de tráfico, colas, identificación de bits y *shaping*. Se manejan 4 colas de prioridad. El equipo no marca los paquetes, solo los lee y los encola según la prioridad que tengan.

A nivel de Ethernet permite verificar la existencia de errores, segundos errados, severamente errados o pérdida de sincronismo. Además se tiene un comprobador de integridad para identificar si el evento es válido o no.

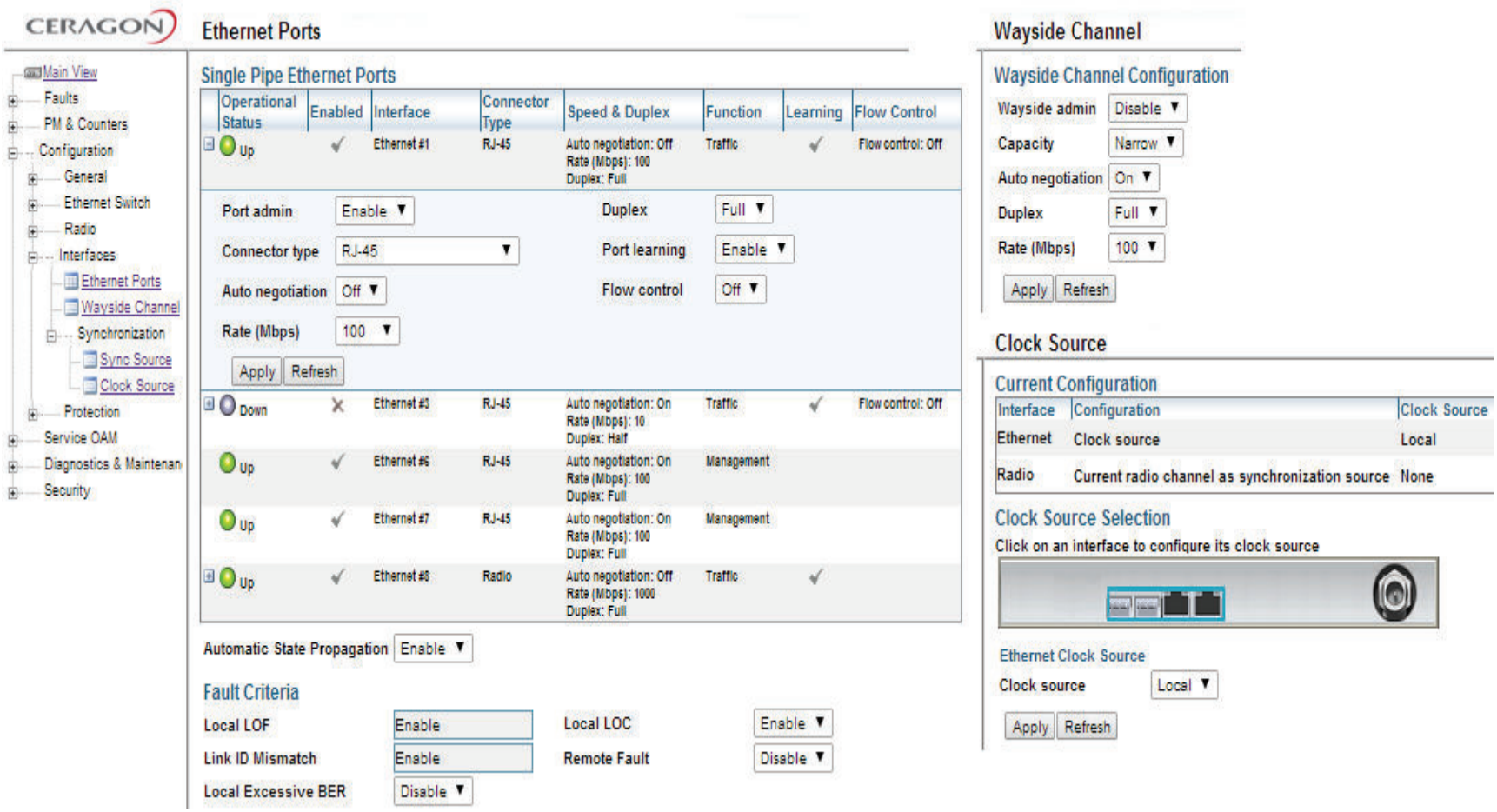


Figura 3.16 Configuración de puertos Ethernet

3.2.1.2.2 Asignación de recursos

Para establecer un enlace de radio, se necesita configurar y verificar los siguientes parámetros:

Frecuencias de TX / RX: Se configura las frecuencias asignadas y autorizadas.
RSL (*Received Signal [dBm*]): Nivel de recepción.
MSE (*Mean Square Error [dB]*): Es un cálculo para aplicar la modulación adaptativa**.**
Max. TSL *(Max. allowed Transmission Signal [dBm]):* Se puede configurar un máximo de nivel de potencia para no afectar a otros enlaces en el mismo nodo.
Monitored TSL *(Actual Transmission level [dBm]):* Nivel actual de transmisión.
IF Interface: Se puede habilitar o deshabilitar el interfaz IF; se usa para actividades de mantenimiento.
Link ID: Identificador del enlace, debe ser el mismo en ambos extremos.
ATPC *(Automatic Transmit Power Control):* Es una característica de la radio que permite mantener la modulación únicamente cambiando el nivel de transmisión del equipo; los ajustes se hacen en base a un umbral de la lectura de recepción. ATPC no funciona en conjunto con ACM.
MRMC *(Multi Rate Multi Coding):* En la IDU se tienen preconfigurados 8 perfiles de modulación para que el ACM pueda trabajar y poder conmutar entre las modulaciones disponibles dependiendo del ancho de banda de la portadora y que el enlace pueda mantenerse con su disponibilidad adecuada.
Adaptive Power – ON / OFF: Debe estar en ON cuando se trabaja con ACM; trabaja en conjunto con MRMC.
Green Mode (RFU-HP): Se usa en sistemas con redundancia; se provee la alimentación mínima hacia la IDU que permanece en *standby*, teniendo un ahorro de energía.
IFC: Parámetro que se recibe en sistemas de redundancia**.**
MAC *Header Compression* (Propietario de Ceragon): Para que el equipo pueda hacer compresión de *header* en las tramas IP, haciendo un ahorro de canal aumentando el *throughput* en un 45 %, siempre y cuando el tamaño de los paquetes sea de 64 bytes.

En una configuración del puerto Gigabitethernet, se deben considerar los siguientes parámetros:

- Habilitar o deshabilitar la administración
- Tipo de conector.
- Habilitar o deshabilitar la negociación del puerto.
- El puerto de aprendizaje, se recomienda deshabilitar en el lado nodo y habilitarlo en el lado del cliente. Esta opción crea el evento en el puerto físico de la IDU.

3.2.2 ACCESOS ALÁMBRICOS

3.2.2.1 Accesos punto a punto de fibra óptica

Los accesos de fibra óptica tienen ventajas sobre los recursos de cobre, en cuanto a que tienen bajas pérdidas de señal, no presenta inducción frente a señales electromagnéticas y de radio frecuencia, entre otras.

Para las transmisiones por fibra óptica se utilizan las longitudes de onda del infrarrojo, valores de 850, 1300 y 1550 nm.

Una fibra monomodo generalmente tiene un núcleo de 8 micrones y una cubierta de 125 micrones de diámetro. La distancia máxima para un enlace de fibra óptica monomodo generalmente es de 20 km. Mientras que una fibra multimodo tiene un núcleo de 50 o 62,5 micrones y una cubierta de 125 micrones de diámetro. La distancia máxima para un enlace de fibra óptica multimodo (62,5/125) es de 3 km.

Entre los tipos de conectores de fibra óptica se tiene:

- FC: se utiliza en la transmisión de datos y en telecomunicaciones.
- FDDI: se utiliza para redes de fibra óptica.
- LC y MT-Array: se utilizan en transmisiones de alta densidad de datos.
- SC y SC-Dúplex: se utilizan para la transmisión de datos.
- ST: se utiliza en redes de edificios y en sistemas de seguridad

En la figura 3.17 se indican los tipos de conectores de fibra óptica. En la tabla 3.9 se detallan las caraterísticas de los conectores más usados. [47]

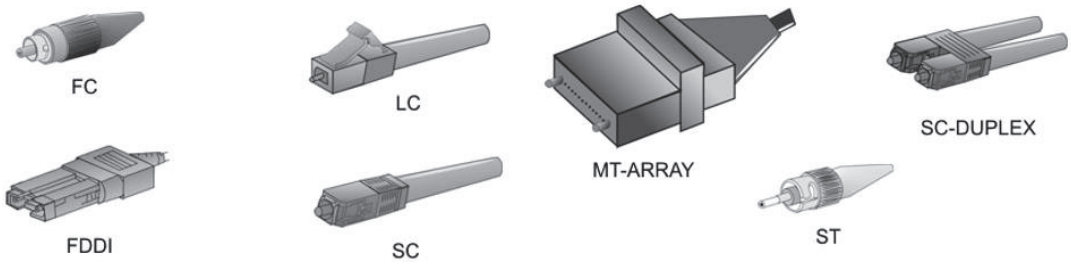


Figura 3.17 Tipos de conectores de fibra óptica

Conectores	Acoplamiento	Tipo de fibra óptica	Pérdida Conectores (dB)
ST	Bayoneta	SM Y MM	0,30 SM - 0,40 MM
SMA	Rosca	MM	0,60 MM
FC	Guía + Rosca	SM Y MM	0,20 SM - 0,15 MM
SC	Push - Pull	SM Y MM	0,20 SM - 0,15 MM

Tabla 3.9 Características de conectores de fibra óptica

Los accesos de última milla se pueden considerar un recurso de fibra óptica punto a punto, con equipos que cumplen con las normas y protocolos IEEE 802.3, IEEE 802.3u, IEEE 802.3x, con tecnología WDM.

Entre la diversidad de equipos conversores de fibra óptica que tienen la función de convertir la señal de un segmento 100 Base-TX a un segmento 100Base-FX y viceversa, dos alternativas de conversores se detallan a continuación:

3.2.2.1.1 Conversores de fibra de la marca CTC

Son equipos que trabajan en pares; el modelo FIB1-10/100W/SC20AF que transmite a 1550 nm se lo instala en el nodo y el modelo FIB1-10/100W/SC20BF que transmite a 1310 nm se lo instala en el cliente. El equipo mencionado se ilustra en la figura 3.18. En el Anexo F se indican las características del equipo.

Figura 3.18 Conversor de F.O. marca CTC

3.2.2.1.2 Conversores de fibra TP-Link

El equipo convertidor de medios de la marca TP-LINK TL-MC112CS que transmite en la longitud de onda de 1550 nm se instala en el nodo, en tanto que para la recepción se requiere el conversor de medio TPL-LINK TL-MC111CS, el cual se instala en el lado del cliente y transmite a 1310 nm. El equipo TP-Link se ilustra en la figura 3.19.

Los detalles técnicos de los equipos se adjuntan en el Anexo G.

Figura 3.19 Conversor de fibra TP-Link

3.3 DISEÑO DE LA RED

Para el diseño de red se ha considerado una proyección a 3 años, pues al cambiar los accesos de última milla por equipos que manejan el protocolo IP, esta infraestructura terminal de equipos de telecomunicaciones se amortiza a 3 años.

Se ha considerado ampliar el rango de *hosts* para la LAN de 126 *hosts* a 254 *hosts* tomando en cuenta que se incorporan servicio de telefonía IP y un sistema de videoconferencia.

Además se ha tomado en consideración el historial del crecimiento de recursos humanos de los últimos años, y se ha proyectado su crecimiento a 3 años:[3]

% Incremento 2010 a 2011 6,37%
% Incremento 2011 a 2012 5,23%
% Incremento 2012 a 2013 4,63%
% Incremento 2013 a 2014 5,41%

Si el incremento del personal en la Entidad Bancaria es en promedio de 5,41% por año, se obtendría una proyección igual a la que se indica en la tabla 3.10.

Sede	Número de usuarios actuales	Año 1	Año 2	Año 3	Porcentaje total de crecimiento
Matriz Quito	65	69	73	77	18,50%
Parque California	50	53	56	59	18,00%
Ag. Cumbayá	50	53	56	59	18,00%
Ag. San Rafael	50	53	56	59	18,00%
Ag. Sangolquí	50	53	56	59	18,00%
Ag. Almagro	20	21	22	23	15,00%
Ag. Rio Plaza	20	21	22	23	15,00%
Ag. Beaterio	20	21	22	23	15,00%
Ag. Ecuagiros Sur	20	21	22	23	15,00%
Ag. Domingo Comín	30	32	34	36	20,00%

Tabla 3.10 Proyección del recurso humano a 3 años

[3] Información suministrada por la Gerente de RRHH de la Entidad Financiera.

Considerando las estadísticas de un aumento de personal en un 18% en 3 años, así como tomando en cuenta que la red actual trabaja en condiciones de saturación, y por la competitividad de los proveedores de servicios en cuanto a precios, se ha considerado que los nuevos recursos se diseñen al doble de su capacidad actual.

Al ser una migración tecnológica de una red *legacy* a una red IP, en los accesos de última milla de radio, los herrajes y polos se mantendrán para la nueva implementación.

En la figura 3.20 se presenta el diseño completo de la red de manera general con las diferentes tecnologías de accesos de última milla, la cuales se interconectan a las redes Metroethernet y éstas, hacia el *backbone IP/MPLS.*

A continuación se analiza cada una de las sedes, detallando el tipo de acceso, las configuraciones de los equipos y las políticas aplicadas.

3.3.1 SEDE MATRIZ QUITO

La sede Matriz tiene un acceso de fibra óptica, por medio de un transporte SDH con equipos de multiplexación marca *Newbridge* y equipo terminales *routers* CE con interfaces V35.

Se diseña la solución por medio de un *switch* Cisco ME 3400 que estará ubicado en el cliente y que se conecta directamente a *switches* secundarios del anillo principal, ubicados en nodos diferentes, ya que al ser el punto más sensible de la red, se requieren protecciones que se obtienen al estar conectado lo más cercano posible al anillo principal de agregación.

El switch ME 3400 tiene módulos ópticos SFP, las características del equipo se indican en la tabla 3.11.

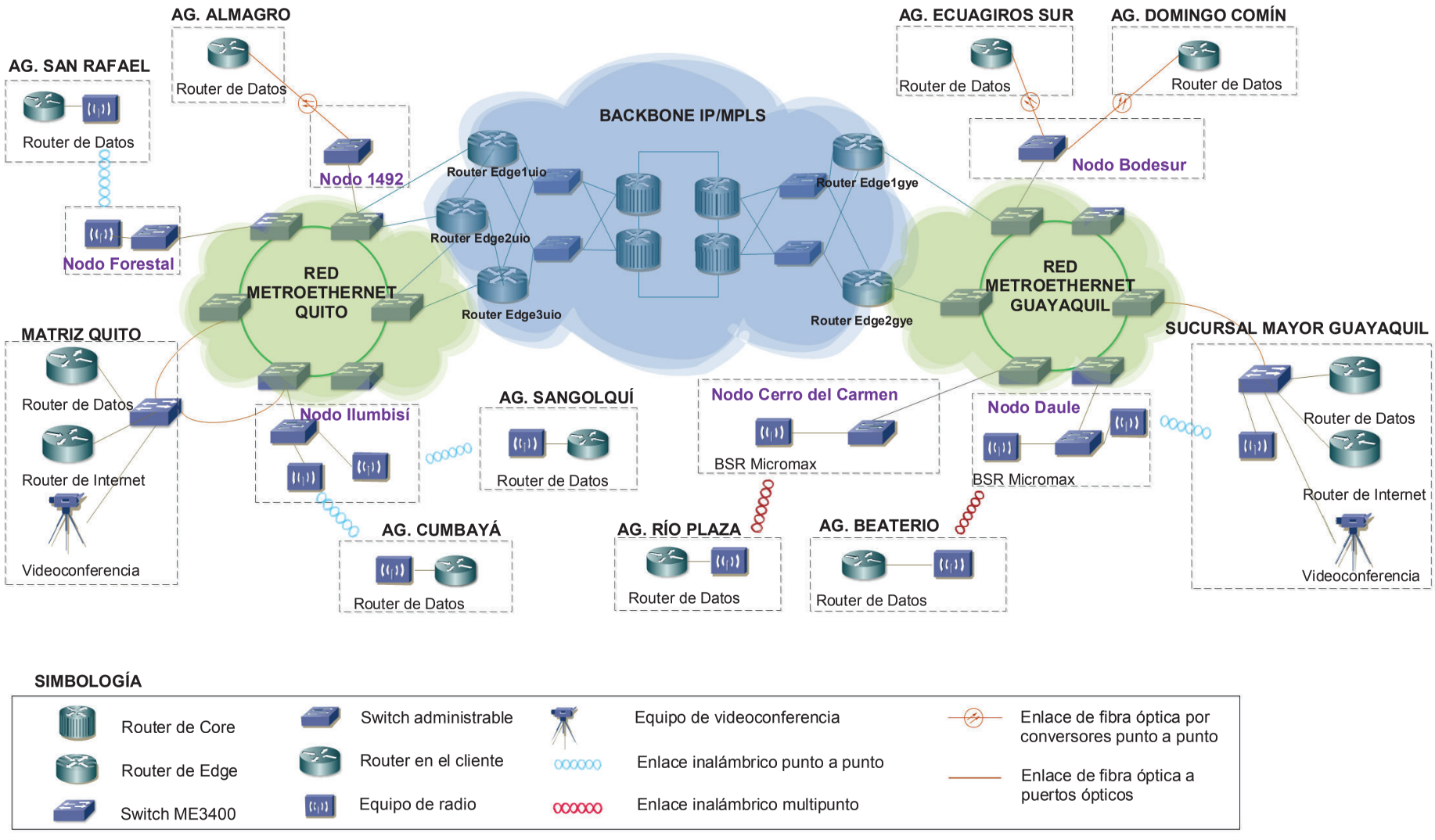


Figura 3.20 Diagrama general del diseño de la red

Switch Cisco ME 3400G-12CS AC	• 12 puertos de doble propósito (10/100/1000 y Small Form-Factor Pluggable [SFP]) • 4 puertos Gigabit Ethernet basado en SFP 100BASE-X • Fuentes de alimentación de CA redundantes duales fijos • 26-Mpps tasa de reenvío • Una unidad de rack (RU) • Gigabit switch de acceso Ethernet construido específicamente para el mercado Metro Ethernet • Opciones para 3 imágenes IOS con características de software (MetroBase, MetroAccess y METROIPACCESS)

Tabla 3.11 Características equipo Cisco ME3400 [48]

La redundancia de los servicios se configura hacia dos *routers* de *edge* diferentes para el caso que exista la caída de uno de los *routers* de borde; por esta razón se configura en los *routers* el protocolo BGP.

El diagrama de servicios de la sede Matriz se ilustra en la figura 3.21.

3.3.1.1 Servicio de Internet sede Matriz

***Router Cisco* 871**

Para el servicio de Internet se ha seleccionado un *router* Cisco 871, que integra 4 puertos conmutados. Se deben configurar las IPs WAN principal, *backup* y LAN; además establecer la sesión BGP, definir los DNS y establecer políticas de limitación de ancho de banda.

Se ha definido la VLAN 2314 con la IP WAN 201.234.192.38/30 para el enlace principal y la VLAN 2322 con la IP WAN 201.234.219.110/30 para el enlace de backup. La IP LAN es la 200.41.1.249/29. La configuración del equipo es la siguiente:

```
hostname BANCO_INTERNET          Nombre del router
```

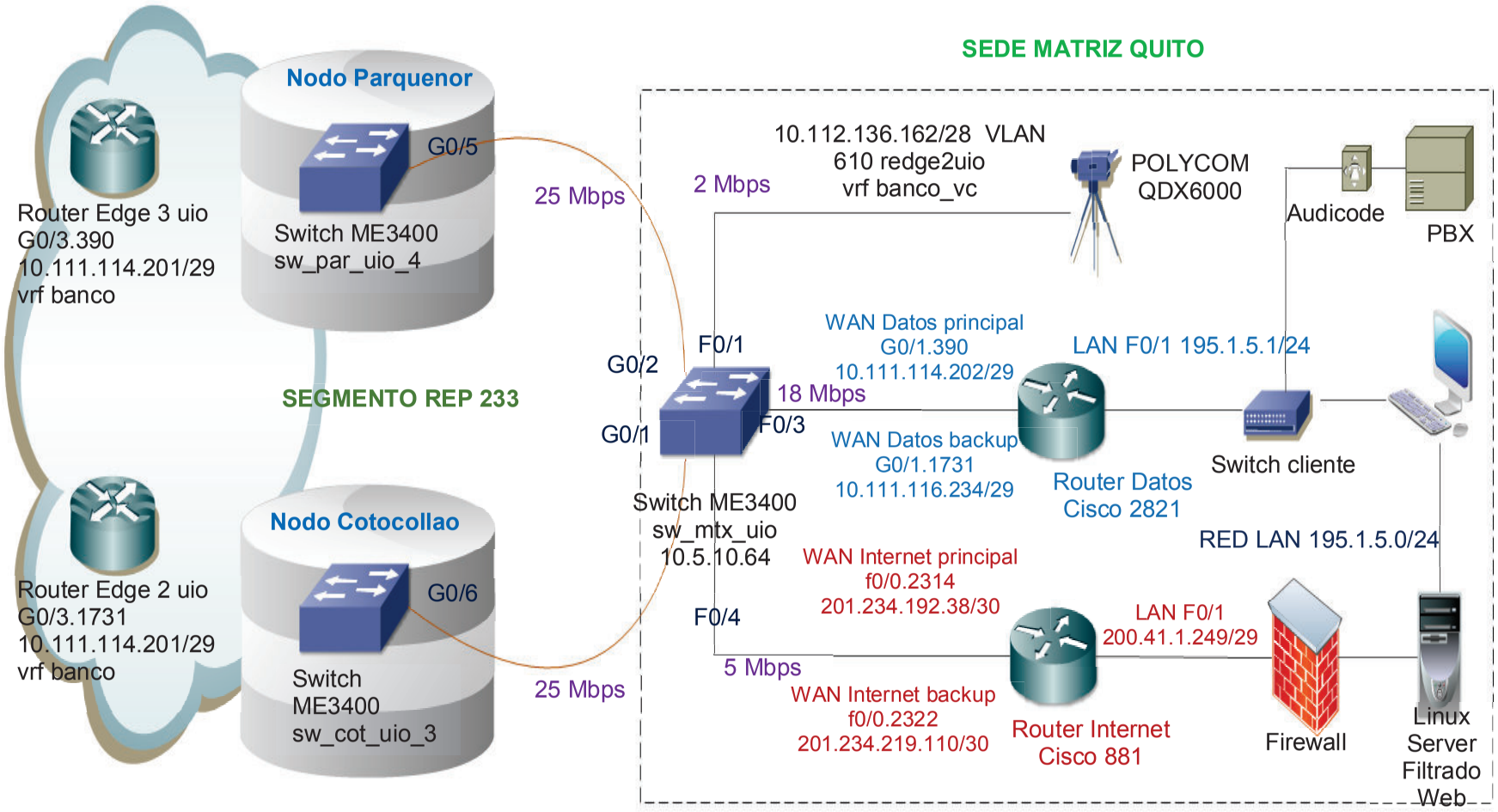


Figura 3.20 Diagrama de servicios de la sede Matriz Quito

Configuración de las interfaces y subinterfaces para la WAN principal, WAN *backup* y LAN.

```
interface FastEthernet0/0.2314
 description PRINCIPAL
 encapsulation dot1Q 2314
 ip address 201.234.192.38 255.255.255.252
 service-policy output QOS                    Se aplica la política QoS.

interface FastEthernet0/0.2322
 description BACKUP
 encapsulation dot1Q 2322
 ip address 201.234.219.110 255.255.255.252
 service-policy output QOS
!
interface FastEthernet0/1
 description LAN
 ip address 200.41.1.249 255.255.255.248
  ip flow ingress
 load-interval 30
 duplex auto
 speed auto
```

Establecimiento de la sesión BGP

```
router bgp 65260
 bgp log-neighbor-changes
 neighbor 201.234.192.37 remote-as 6140          Definición del neighbor
 neighbor 201.234.192.37 description BANCO_INTERNET_PRINC
 neighbor 201.234.219.109 remote-as 6140
 neighbor 201.234.219.109 description BANCO_INTERNET_BKP

 address-family ipv4
 neighbor 201.234.192.37 activate                Activación de la sesión VPNv4
 neighbor 201.234.192.37 send-community
 neighbor 201.234.192.37 soft-reconfiguration inbound
 neighbor 201.234.192.37 prefix-list CUSTOMER:AS6140 out
 neighbor 201.234.192.37 route-map CLI:BANCO_INTERNET_PRINC:6140:IN-1 in
 neighbor 201.234.192.37 route-map CLI:BANCO_INTERNET_PRINC:6140:OUT-1 out
 neighbor 201.234.192.37 maximum-prefix 20 90 restart 5
 neighbor 201.234.219.109 activate
 neighbor 201.234.219.109 send-community         Habilitación de comunidades
 neighbor 201.234.219.109 soft-reconfiguration inbound
 neighbor 201.234.219.109 prefix-list CUSTOMER:AS6140 out
 neighbor 201.234.219.109 route-map CLI:BANCO_INTERNET_PRINC:6140:IN-2 in
 neighbor 201.234.219.109 maximum-prefix 20 90 restart 5
 no auto-summary
 no synchronization
 network 200.41.1.248 mask 255.255.255.248
 exit-address-family
ip bgp-community new-format

ip prefix-list CUSTOMER:AS6140 seq 10 permit 200.41.1.248/29
```

Se definen los DNS del proveedor de servicios.

```
ip name-server 200.31.6.34
ip name-server 200.31.6.38
```

Se define una política para el ancho de banda de 5 Mbps.

```
policy-map QOS
 class class-default
  shape average 5120000
```

Se configura el *route map* con su respectivo peso para establecer la sesión activa.

```
route-map CLI:BANCO_INTERNET_PRINC:6140:IN-2 permit 10
 set weight 100

route-map CLI:BANCO_INTERNET_PRINC:6140:IN-1 permit 10
 set weight 350

route-map CLI:BANCO_INTERNET_PRINC:6140:OUT-1 permit 10
 match ip address prefix-list CUSTOMER:AS6140
 set community 3549:350
```

Cabe señalar que el establecimiento BGP se hace con el *router* PE. A continuación se indica como ejemplo la configuración básica por parte del proveedor en el *router* de borde, para el enlace principal de Internet.

Configuración de la interfaz:

```
interface GigabitEthernet0/3.2314 description BANCO INTERNET PRINCIPAL
interface GigabitEthernet0/3.2314 bandwidth 5120
interface GigabitEthernet0/3.2314 encapsulation dot1Q 2314
interface GigabitEthernet0/3.2314 ip address 201.234.192.37 255.255.255.252
interface GigabitEthernet0/3.2314 ip access-group 2646 in
interface GigabitEthernet0/3.2314 no ip redirects
interface GigabitEthernet0/3.2314 no ip proxy-arp
interface GigabitEthernet0/3.2314 no cdp enable
interface GigabitEthernet0/3.2314 service-policy input 5M
interface GigabitEthernet0/3.2314 service-policy output 5M
```

Establecimiento de política

```
policy-map 5M class class-default
policy-map 5M class class-default police cir 5120000 bc 640000 be 1280000
```

Configuración BGP:

```
router bgp 3549 neighbor 201.234.192.38 remote-as 65260
router bgp 3549 neighbor 201.234.192.38 local-as 6140 no-prepend
router bgp 3549 neighbor 201.234.192.38 description BANCO-INTERNET S.A.-AS65260-1-GE
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 activate
```

```
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 send-community
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 default-originate
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 remove-private-as
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 soft-reconfiguration inbound
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 prefix-list CUSTOMER:AS65260 in
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 prefix-list CUS:DEFAULT-ONLY out
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 route-map transit-customer-map in
router bgp 3549 address-family ipv4 neighbor 201.234.192.38 maximum-prefix 2000 90 restart 5
```

Es importante verificar que las interfaces estén activas y las sesiones BGP operando correctamente; a continuación se indican el estado del *router* CE de Internet.

```
BANCO_INTERNET #sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES NVRAM  up                    up
FastEthernet0/0.2314   201.234.192.38  YES NVRAM  up                    up
FastEthernet0/0.2322   201.234.219.110 YES NVRAM  up                    up
FastEthernet0/1        200.41.1.249    YES NVRAM  up                    up

BANCO_INTERNET #sh ip bgp sum
BGP router identifier 201.234.219.110, local AS number 65260
BGP table version is 5, main routing table version 5
4 network entries using 468 bytes of memory
7 path entries using 364 bytes of memory
3/2 BGP path/bestpath attribute entries using 372 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1228 total bytes of memory
2 received paths for inbound soft reconfiguration
BGP activity 4/0 prefixes, 9/2 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
201.234.192.37  4  6140  103407   94023        5    0    0   00:15:00        1
201.234.219.109 4  6140  103449   94023        5    0    0   00:09:40        1
```

3.3.1.2 Servicio de Datos sede Matriz

Router Cisco 2821

Se ha seleccionado el *router* Cisco 2821 por sus características de procesamiento y rendimiento para la sede Matriz. Se ha definido la VLAN 390 para el enlace principal de datos y la VLAN 1731 para el enlace de *backup.*

En este equipo se deben configurar:

- Las direcciones IPs WAN y LAN
- Establecer la sesión BGP
- Políticas de limitación de ancho de banda
- Políticas de QoS.

Se ha definido la VLAN 390 con la IP WAN 10.111.114.202/29 para el enlace principal y la VLAN 1731 con la IP WAN 10.111.116.234/29 para el enlace de *backup* y la IP LAN 195.1.5.1/24. La configuración del equipo es la siguiente:

```
hostname BANCO_MTX_UIO_DATOS
```

Nombre del *router*

Configuración de las interfaces y subinterfaces para la WAN principal, WAN *backup* y LAN.

```
interface GigabitEthernet0/1.390
 description BANCO_PRINCIPAL
 encapsulation dot1Q 390
 ip address 10.111.114.202 255.255.255.128
 ip access-group 101 out
 no snmp trap link-status
 service-policy output QoS

interface GigabitEthernet0/1.1731
 description BANCO_BKP
 encapsulation dot1Q 1731
 ip address 10.111.116.234 255.255.255.248
 no snmp trap link-status
 no cdp enable
 service-policy output QoS

interface GigabitEthernet0/0
 description LAN BANCO UIO
 ip address 195.1.5.1 255.255.255.0
 ip accounting output-packets
 ip route-cache flow
 load-interval 30
 duplex auto
 speed auto
```

Establecimiento de la sesión BGP.

```
router bgp 64523
 bgp log-neighbor-changes
 neighbor 10.111.114.201 remote-as 6140
 neighbor 10.111.114.201 description CUSTOMER--BANCO-AS6140-1-GE
 neighbor 10.111.116.233 remote-as 6140
 neighbor 10.111.116.233 description CUSTOMER-BANCO-AS6140-2-GE
```

```
 !
 address-family ipv4
 redistribute connected
neighbor 10.111.114.201 activate
 neighbor 10.111.114.201 send-community
 neighbor 10.111.114.201 soft-reconfiguration inbound
 neighbor 10.111.114.201 prefix-list CUSTOMER:AS6140 out
 neighbor 10.111.114.201 route-map CLI:BANCO:6140:IN-1 in
 neighbor 10.111.114.201 route-map CLI:BANCO:6140:OUT-1 out
 neighbor 10.111.114.201 maximum-prefix 300 90 restart 5
 neighbor 10.111.116.233 activate
 neighbor 10.111.116.233 send-community
 neighbor 10.111.116.233 soft-reconfiguration inbound
 neighbor 10.111.116.233 prefix-list CUSTOMER:AS6140 out
 neighbor 10.111.116.233 route-map CLI:BANCO:6140:IN-2 in
 neighbor 10.111.116.233 maximum-prefix 300 90 restart 5
 default-information originate
 no auto-summary
 no synchronization
 network 195.1.5.0
 exit-address-family

ip classless
ip route 0.0.0.0 0.0.0.0 195.1.5.81 name INTERNET
ip bgp-community new-format
```

Se definen los *class-map* para el servicio de Internet y para el servicio de voz.

```
class-map match-all INTERNET
 match access-group name INTERNET
class-map match-all VOZ
 match access-group name VOZ
```

Se define una política anidada *policy–map* QoS con un ancho de banda de 16 Mbps y un ancho de banda de 2 Mbps para el servicio de voz.

```
policy-map BANCO
class VOZ
  priority 2048
  set ip precedence 5
policy-map QoS
 class class-default
  shape average 16384000
  service-policy BANCO
```

Se definen las listas de acceso.

```
ip access-list extended INTERNET
 permit ip host 195.1.5.81 any
 permit tcp any any eq www
 permit tcp any eq www any
```

```
 permit tcp any any eq 443
 permit tcp any eq 443 any
ip access-list extended VOZ
 permit tcp any any eq 4060
 permit tcp any eq 4060 any
 permit tcp any any range 12250 12950
 permit tcp any range 12250 12950 any
 permit tcp any eq 1720 any
 permit tcp any any eq 1720
 permit udp any range 29100 29159 any
 permit udp any any range 29100 29159
!
!
ip prefix-list CUSTOMER:AS6140 seq 5 permit 195.1.5.0/24
ip prefix-list CUSTOMER:AS6140 seq 20 permit 0.0.0.0/0

access-list 101 deny   tcp any any eq 445
access-list 101 deny   tcp any eq 445 any
access-list 101 permit ip any any
no cdp run
```

Configuración del *route-map* estableciendo la sesión BGP con mayor prioridad.

```
route-map CLI:BANCO:6140:OUT-1 permit 10
 match ip address prefix-list CUSTOMER:AS6140
 set community 3549:350

route-map CLI:BANCO:6140:IN-2 permit 10
 set weight 100

route-map CLI:BANCO:6140:IN-1 permit 10
 set weight 350
```

Un ejemplo del establecimiento de la sesión BGP y la creación de la VRF banco realizado en el PE del proveedor para el enlace de respaldo se indica a continuación:

Configuración de la interfaz:

```
interface GigabitEthernet0/3.1731 description BANCO DATOS BACKUP
interface GigabitEthernet0/3.1731 bandwidth 30720
interface GigabitEthernet0/3.1731 encapsulation dot1Q 1731
interface GigabitEthernet0/3.1731 ip vrf forwarding banco
interface GigabitEthernet0/3.1731 ip address 10.111.116.233 255.255.255.248
interface GigabitEthernet0/3.1731 ip access-group 2646 in
interface GigabitEthernet0/3.1731 no ip redirects
interface GigabitEthernet0/3.1731 no ip proxy-arp
interface GigabitEthernet0/3.1731 no cdp enable
interface GigabitEthernet0/3.1731 service-policy input 18M
interface GigabitEthernet0/3.1731 service-policy output banco_uio
```

Establecimiento de la política:

```
policy-map banco_uio class class-default
policy-map banco_uio class class-default shape average 18432000
policy-map banco_uio service-policy banco_uio_nested
```

Configuración *VRF y route-target:*

```
interface GigabitEthernet0/3.1731 ip vrf forwarding banco
ip vrf banco rd 65140:1100878
ip vrf banco route-target export 65140:1100878
ip vrf banco route-target import 65140:1100878
ip vrf banco route-target import 16528:20
ip vrf banco route-target import 65140:10
```

Configuración *BGP:*

```
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 remote-as 64523
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 local-as 6140 no-prepend
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 description BANCO-DAT_BACKUP
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 activate
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 send-community
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 as-override
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 soft-reconfiguration inbound
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 route-map vpn-customer-ecuador in
router bgp 3549 address-family ipv4 vrf banco neighbor 10.111.116.234 maximum-prefix 100 90 restart 5
```

3.3.1.3 Configuración switch ME3400 sede Matriz

Por características específicas de los equipos de videoconferencia que se detallarán más adelante, se ha creado una VLAN directamente en el *switch* Cisco ME3400; ésta es la VLAN 610.

A continuación se indica la configuración del equipo Cisco ME3400, donde se tienen las VLANs hacia el segmento REP.

Se definen las VLANs principales en la cuales se encapsulan las VLAN de cliente; se define la VLAN 233 del segmento REP y la 610 de videoconferencia.

El encapsulamiento de las *customer VLANs* en las *service VLANs* se realiza para un manejo apropiado en cuanto a la administración de la red.

```
rep admin vlan 233      Se define la VLAN 233 de administración para segmento REP
```

```
vlan 5
 name METRO_UIO_BKP

vlan 6
 name METRO_UIO

vlan 233
 name ADMIN_REP_233

vlan 610
 name Video_Conferencia

class-map match-any dot1p-EF
 match cos  4  5
class-map match-any dot1p-AF
 match cos  2  3
class-map match-any dot1p-BE
 match cos  0  1  6  7
class-map match-any QoS-Group-EF
 match qos-group 3
class-map match-any QoS-Group-AF
 match qos-group 2
class-map match-any QoS-Group-BE
 match qos-group 1
```

Se definen las políticas de clase de servicio, en este ejemplo, se tiene contemplado para varios anchos de banda.

```
policy-map CUST-Ingress-30M
 class class-default
    police cir 30000000 bc 384000 be 768000
      conform-action transmit
      exceed-action set-cos-transmit 0
      violate-action drop

policy-map GX-Egress_child
 class QoS-Group-EF
    priority
 class QoS-Group-AF
    bandwidth remaining percent 90
 class QoS-Group-BE
    bandwidth remaining percent 9
 class class-default
    bandwidth remaining percent 1

policy-map GX-Egress-GE
 class class-default
    shape average 1000000000
  service-policy GX-Egress_child

policy-map CUST-Ingress-2M
 class class-default
```

```
    police cir 2048000 bc 384000 be 768000
      conform-action transmit
      exceed-action set-cos-transmit 0
      violate-action drop

policy-map CUST-Ingress-5M
 class class-default
    police cir 5120000 bc 640000 be 1280000
      conform-action transmit
      exceed-action set-cos-transmit 0
      violate-action drop

policy-map GX-Ingress-GE
 class dot1p-EF
    police cir 1000000000
      conform-action set-qos-transmit 3
 class dot1p-AF
    police cir 1000000000
      conform-action set-qos-transmit 2
 class dot1p-BE
    police cir 1000000000
      conform-action set-qos-transmit 1
```

En el puerto fastethernet0/1 se configura la VLAN 610 correspondiente a la conexión hacia el equipo de videoconferencia.

```
interface FastEthernet0/1
 description CUSTOMER:IMPS-CLI:1-CXOIG:BANCO S.A.[VIDEOCONF]
 port-type nni
 switchport access vlan 610
 switchport port-security violation restrict
 load-interval 30
 storm-control broadcast level pps 300 100
 storm-control multicast level pps 300 100
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
 spanning-tree guard root
 service-policy input CUST-Ingress-2M
```

Se configura el puerto fastethernet0/3 al cual se conecta el *router* de datos. Se encapsula la VLAN principal de datos 390 en la VLAN 6 y la VLAN secundaria de datos 1731 en la VLAN 5.

```
interface FastEthernet0/3
 description CUSTOMER:IMPS-CLI:1-CXOIG:BANCO S.A.[DATOS PRIN-BACK]
 port-type nni
 switchport trunk allowed vlan 5,6
 switchport mode trunk
```

```
 switchport vlan mapping 390 dot1q-tunnel 6
 switchport vlan mapping 1731 dot1q-tunnel 5
 switchport vlan mapping default drop
 switchport port-security maximum 3
 switchport port-security
 switchport port-security violation restrict
 load-interval 30
 storm-control broadcast level pps 300 100
 storm-control multicast level pps 300 100
 storm-control action trap
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
 spanning-tree guard root
 service-policy input CUST-Ingress-30M
```

Se configura el puerto fastethernet0/4 hacia el cual se conecta el *router* de Internet. Se encapsula la VLAN principal 2314 en la VLAN 6 y la VLAN secundaria 2322 en la VLAN 5.

```
interface FastEthernet0/4
 description CUSTOMER:IMPS-CLI:1-CXOIG:BANCO S.A.[ADI PRIN-BACK]
 port-type nni
 switchport trunk allowed vlan 5,6
 switchport mode trunk
 switchport vlan mapping 2314 dot1q-tunnel 6
 switchport vlan mapping 2322 dot1q-tunnel 5
 switchport vlan mapping default drop
 switchport port-security maximum 3
 switchport port-security
 switchport port-security violation restrict
 load-interval 30
 storm-control broadcast level pps 300 100
 storm-control multicast level pps 300 100
 storm-control action trap
 no cdp enable
 no cdp tlv server-location
 no cdp tlv app
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
 spanning-tree guard root
 service-policy input CUST-Ingress-5M
```

Se configuran los puertos Gigabit Ethernet que serán parte del segmento REP 233 y se permiten únicamente las 4 VLANs (5, 6, 233,610) para que se propaguen en el anillo.

```
interface GigabitEthernet0/1
 description TRUNK:SW3.COT.UIO.EC:GE:G0/6
 port-type nni
 switchport trunk native vlan 233
 switchport trunk allowed vlan 5,6,233,610
 switchport mode trunk
 bandwidth 1000000
 udld port aggressive
 rep segment 233
 rep preempt delay 45
 storm-control broadcast level pps 300 100
 storm-control multicast level pps 300 100
 storm-control action trap
 service-policy input GX-Ingress-GE
 service-policy output GX-Egress-GE

interface GigabitEthernet0/2
 description TRUNK:SW4.PNR.UIO.EC:GE:G0/6
 port-type nni
 switchport trunk native vlan 233
 switchport trunk allowed vlan 5,6,233,610
 switchport mode trunk
 bandwidth 1000000
 load-interval 30
 udld port aggressive
 rep segment 233 preferred
 rep preempt delay 45
 storm-control broadcast level pps 300 100
 storm-control multicast level pps 300 100
 storm-control action trap
 service-policy input GX-Ingress-GE
 service-policy output GX-Egress-GE
```

Se configura la dirección IP de monitoreo del *switch*.

```
interface Vlan6
 ip address 10.5.10.64 255.255.255.0
```

En el Anexo H se detallan las características técnicas del *router Cisco* 2821, en el Anexo I las características del *router Cisco* 881 y en el Anexo J se indica el s*witch* ME3400.

3.3.2 SUCURSAL PRINCIPAL GUAYAQUIL PARQUE CALIFORNIA

Para la sede de la sucursal mayor Guayaquil, se ha diseñado la solución con un enlace de fibra óptica punto a punto y un enlace secundario inalámbrico punto a

punto, dos diferentes tipos de tecnologías, y a nodos distintos. Además en el enrutamiento se ha considerado conexiones a *routers* de *edge* diferentes.

El acceso inalámbrico es por medio de un radio de marca *Ceragon* modelo *IP10 E;* no se ha considerado la opción de habilitar la opción *hot standby*, porque al usar la banda licenciada de 23 GHz, no tendrá problemas de interferencias, además la solución por acceso de fibra óptica en el enlace principal es fiable, como se indica en la figura 3.22.

Con una solución similar a la sede Matriz Quito, se ha diseñado con un *router Cisco* de la serie 2800 para el servicio de datos y de la serie 800 para el Internet y un *switch* Cisco ME3400 ubicado en la sede del cliente.

El acceso de fibra óptica punto a punto es por medio de conversores de fibra óptica de la marca TP-Link, conectados en el nodo y en la sede del cliente a los *switches* ME3400 respectivos.

3.3.2.1 Servicio de Internet Sucursal Mayor Guayaquil

***Router Cisco* 871**

La configuración es similar a la Matriz Quito, variando las direcciónes IPs WAN y LAN. Para esta sede ha definido VLAN 2314 con la IP WAN 190.216.212.210/30 para el enlace principal y la VLAN 2322 con la IP WAN 190.216.212.214/30 para el enlace de *backup*. La IP LAN es la 201.234.204.73/29. La configuración del equipo es la siguiente:

```
hostname C871_BANCO_INTERNET_GYE                Nombre del equipo

interface FastEthernet4.2314
 encapsulation dot1Q 2314
 ip address 190.216.212.210 255.255.255.252
!
interface FastEthernet4.2322
 encapsulation dot1Q 2322
 ip address 190.216.212.214 255.255.255.252
!
interface Vlan1
 ip address 201.234.204.73 255.255.255.248
!
```

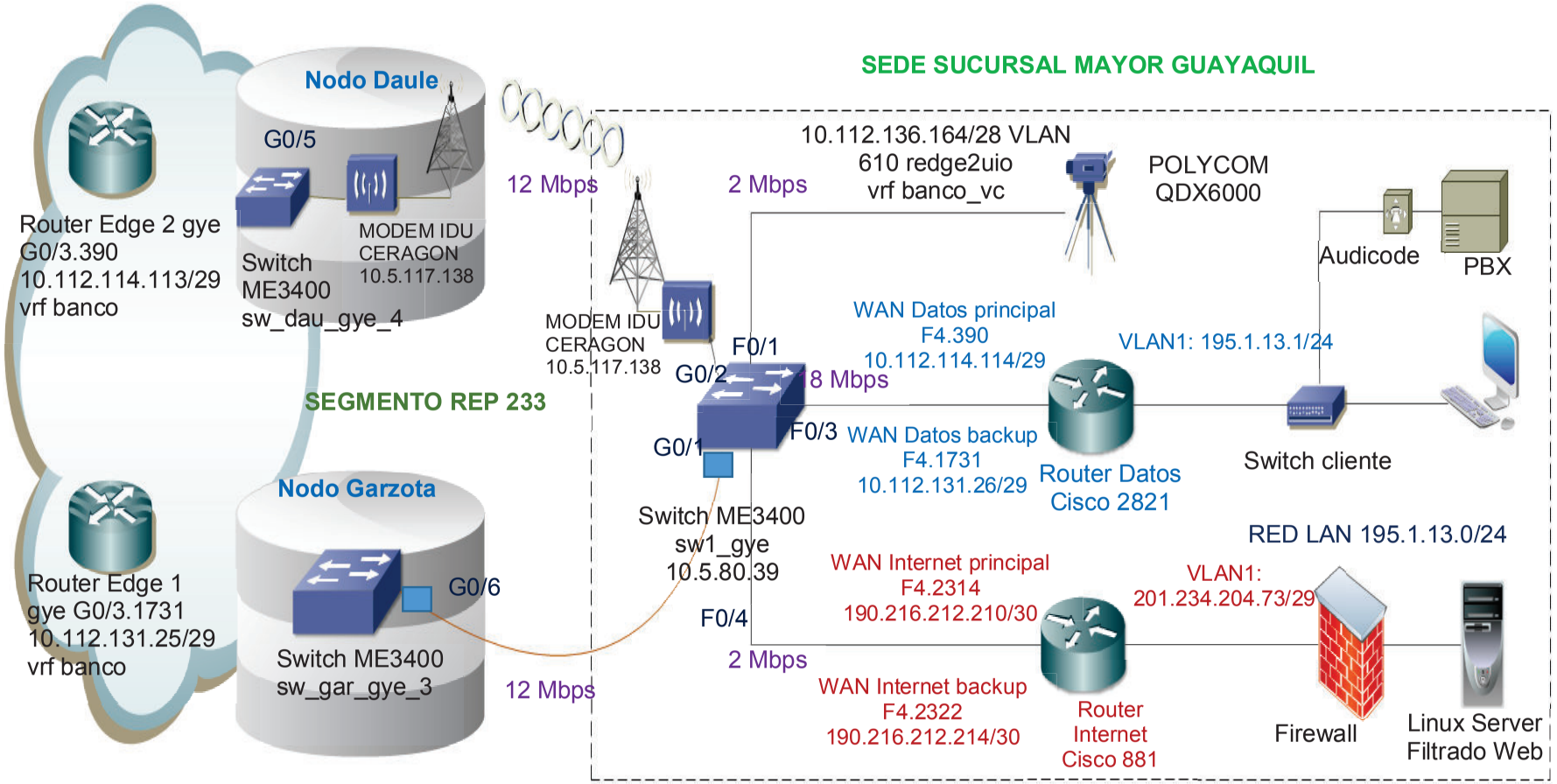


Figura 3.21 Diagrama de servicios sucursal Mayor Guayaquil

```
router bgp 65260
 bgp log-neighbor-changes
 neighbor 190.216.212.209 remote-as 3549

neighbor 190.216.212.209 description Banco_GYE-AS3549-1-GE
 neighbor 190.216.212.213 remote-as 3549
 neighbor 190.216.212.213 description Banco_GYE-AS3549-2-GE
 !
 address-family ipv4
 neighbor 190.216.212.209 activate
 neighbor 190.216.212.209 send-community
 neighbor 190.216.212.209 soft-reconfiguration inbound
 neighbor 190.216.212.209 prefix-list CUSTOMER:AS3549 out
 neighbor 190.216.212.209 route-map CLI:Banco_GYE:3549:IN-1 in
 neighbor 190.216.212.209 route-map CLI:Banco_GYE:3549:OUT-1 out
 neighbor 190.216.212.209 maximum-prefix 200 90 restart 5
 neighbor 190.216.212.213 activate
 neighbor 190.216.212.213 send-community
 neighbor 190.216.212.213 soft-reconfiguration inbound
 neighbor 190.216.212.213 prefix-list CUSTOMER:AS3549 out
 neighbor 190.216.212.213 route-map CLI:Banco_GYE:3549:IN-2 in
 neighbor 190.216.212.213 maximum-prefix 200 90 restart 5
 no auto-summary
 no synchronization
 network 201.234.204.72 mask 255.255.255.248
 exit-address-family
!
ip classless
!
!
ip prefix-list CUSTOMER:AS3549 seq 5 permit 201.234.204.72/29
!
route-map CLI:Banco_GYE:3549:OUT-1 permit 10
 match ip address prefix-list CUSTOMER:AS3549
 set community 232587614
!
route-map CLI:Banco_GYE:3549:IN-1 permit 10
 set weight 350
!
route-map CLI:Banco_GYE:3549:IN-2 permit 10
 set weight 100
```

3.3.2.2 Servicio de Datos Sucursal Mayor Guayaquil

***Router* 2821**

Presenta una configuración similar a la sede Quito, variando el direccionamiento IP, políticas, y limitaciones del canal. Se ha definido la VLAN 390 con la IP WAN 10.112.114.114/29 para el enlace principal y la VLAN 1731 con la IP WAN

10.112.131.26/29 para el enlace de *backup* y la IP LAN 195.1.13.1/24. La configuración del equipo es la siguiente:

```
hostname 021.BANCO_GYE.datos
```

Se defiene los *class-map* que se van a usar con los diferentes tipos de servicios.

```
class-map match-all INTERNET
 match access-group name INTERNET
class-map match-all VOICE
 match access-group name VOICE
```

Se definen las políticas de ancho de banda para aplicar en las interfaces

```
policy-map BANCO
 class VOICE
  set ip precedence 5
  priority 384
class INTERNET
  police cir 2048000
policy-map QoS_IN
 class class-default
  police cir 8192000
policy-map QoS
 class class-default
  shape average 8192000
  service-policy BANCO
```

Se configuran las interfaces WAN principal y *backup*.

```
interface FastEthernet4.390
 description PRINCIPAL EDGE GYE 2
 encapsulation dot1Q 390
 ip address 10.112.114.114 255.255.255.248
 ip access-group 101 out
 service-policy input QoS_IN
 service-policy output QoS

interface FastEthernet4.1731
 description BACKUP EDGE GYE
 encapsulation dot1Q 1731
 ip address 10.112.131.26 255.255.255.248
 ip access-group 101 out
 service-policy input QoS_IN
 service-policy output QoS
```

Se configura la interfaz VLAN 1 para la LAN.

```
interface Vlan1
 ip address 195.1.13.1 255.255.255.0
 ip accounting output-packets
```

```
 ip route-cache flow
```

Se establece la sesión BGP.

```
router bgp 64523
 bgp log-neighbor-changes
 neighbor 10.112.114.113 remote-as 6140
 neighbor 10.112.114.113 description BANCO-AS6140-1-GE
 neighbor 10.112.131.25 remote-as 6140
 neighbor 10.112.131.25 description BANCO-AS6140-2-GE
 !
 address-family ipv4
 neighbor 10.112.114.113 activate
 neighbor 10.112.114.113 send-community
 neighbor 10.112.114.113 soft-reconfiguration inbound
 neighbor 10.112.114.113 prefix-list CUSTOMER:AS6140 out
 neighbor 10.112.114.113 route-map CLI:BANCO:6140:IN-1 in
 neighbor 10.112.114.113 route-map CLI:BANCO:6140:OUT-1 out
 neighbor 10.112.114.113 maximum-prefix 2000 90 restart 5
 neighbor 10.112.131.25 activate
 neighbor 10.112.131.25 send-community
 neighbor 10.112.131.25 soft-reconfiguration inbound
 neighbor 10.112.131.25 prefix-list CUSTOMER:AS6140 out
 neighbor 10.112.131.25 route-map CLI:BANCO:6140:IN-2 in
 neighbor 10.112.131.25 maximum-prefix 2000 90 restart 5
 no auto-summary
 no synchronization
 network 195.1.13.0
 exit-address-family
!
ip bgp-community new-format
!
ip access-list extended INTERNET
 permit ip any host 195.1.5.81
 permit tcp any any eq www
 permit tcp any eq www any
 permit tcp any any eq 443
 permit tcp any eq 443 any
ip access-list extended VOICE
 permit tcp any eq 1719 any
 permit tcp any any eq 1719
 permit tcp any eq 1720 any
 permit tcp any any eq 1720
ip prefix-list CUSTOMER:AS6140 seq 5 permit 195.1.13.0/24
access-list 101 deny   tcp any any eq 445
access-list 101 deny   tcp any eq 445 any
access-list 101 permit ip any any
access-list 112 remark VOICE
access-list 112 permit udp any any range 16384 37276
access-list 112 permit tcp any eq 1720 any
access-list 112 permit tcp any any eq 1720
```

Se definen los *route-map* con el peso para dar prioridad a una de las sesiones BGP como principal.

```
route-map CLI:BANCO:6140:OUT-1 permit 10
 match ip address prefix-list CUSTOMER:AS6140
 set community 3549:350
!
route-map CLI:BANCO:6140:IN-2 permit 10
 set weight 100
!
route-map CLI:BANCO:6140:IN-1 permit 10
 set weight 350
```

3.3.2.3 Equipos de acceso

A nivel de acceso se detalla a continuación la configuración para el *switch* ME3400 ubicado en la sede del cliente y los parámetros para el enlace de radio punto a punto Ceragon.

3.3.2.3.1 Switch ME3400 sede Sucursal Mayor Guayaquil

Se considera la VLAN 330 para el segmento REP, y las VLAN de los clientes se encapsulan en las VLAN 7 y 8 para los servicios principales y *backup* respectivamente.

```
rep admin vlan 330
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
no spanning-tree vlan 1-4094
!
vlan 7
 name METRO_GYE_BKP
!
vlan 8
 name METRO_GYE

vlan  330
 name ADMIN_REP_ 330

vlan 610
 name Video_Conferencia
```

Se definen las políticas de clase de servicio.

```
class-map match-any dot1p-EF
 match cos  4  5
class-map match-any dot1p-AF
 match cos  2  3
class-map match-any dot1p-BE
 match cos  0  1  6  7
class-map match-any QoS-Group-EF
 match qos-group 3
class-map match-any QoS-Group-AF
 match qos-group 2
class-map match-any QoS-Group-BE
 match qos-group 1

policy-map GX-Egress_child
 class QoS-Group-EF
    priority
 class QoS-Group-AF
    bandwidth remaining percent 90
 class QoS-Group-BE
    bandwidth remaining percent 9
 class class-default
    bandwidth remaining percent 1
policy-map GX-Egress-GE
 class class-default
    shape average 1000000000
  service-policy GX-Egress_child
policy-map CUST-Ingress-2M
 class class-default
    police cir 2048000
      conform-action transmit
      exceed-action set-cos-transmit 0
      violate-action drop
policy-map CUST-Ingress-7M
 class class-default
    police cir 7168000
      conform-action transmit
      exceed-action set-cos-transmit 0
      violate-action drop
policy-map CUST-Ingress-8M
 class class-default
    police cir 8192000
      conform-action transmit
      exceed-action set-cos-transmit 0
      violate-action drop
policy-map GX-Ingress-GE
 class dot1p-EF
    police cir 1000000000
      conform-action set-qos-transmit 3
 class dot1p-AF
    police cir 1000000000
      conform-action set-qos-transmit 2
 class dot1p-BE
    police cir 1000000000
      conform-action set-qos-transmit 1
```

Se configura el puerto en el *switch* hacia el *router* de Datos. Se encapsula la VLAN principal 390 en la VLAN 8 y la VLAN secundaria 1731 en la VLAN 7.

```
interface FastEthernet0/1
 descriptionBANCO DATOS PRIN-BACK
 port-type nni
 switchport trunk allowed vlan 7, 8
 switchport mode trunk
 switchport vlan mapping 390 dot1q-tunnel 8
 switchport vlan mapping 1731 dot1q-tunnel 7
 switchport port-security maximum 6
 switchport port-security
 switchport port-security aging time 5
 switchport port-security violation restrict
 bandwidth 4000
 storm-control broadcast level pps 300 100
 storm-control multicast level 10.00
 storm-control action trap
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
 spanning-tree guard root
 service-policy input CUST-Ingress-8M

interface FastEthernet0/2
 description BANCO ADI PRIN-BACK
 port-type nni
 switchport trunk allowed vlan 7,8
 switchport mode trunk
 switchport vlan mapping 2314 dot1q-tunnel 8
 switchport vlan mapping 2322 dot1q-tunnel 7
 switchport port-security maximum 4
 switchport port-security
 switchport port-security aging time 5
 switchport port-security violation restrict
 bandwidth 3000
 storm-control broadcast level pps 300 100
 storm-control multicast level 10.00
 storm-control action trap
 spanning-tree portfast trunk
 spanning-tree bpdufilter enable
 spanning-tree guard root
 service-policy input CUST-Ingress-2M

interface FastEthernet0/4
 description CUSTOMER:IMPS-MPLS:1-CXOIG:BANCO VIDEO.CONF
 port-type nni
 switchport access vlan 610
 bandwidth 4000
 service-policy input CUST-Ingress-2M
```

Se define la VLAN nativa en el segmento REP la VLAN 330, y se especifican las 4 VLAN permitidas (7, 8, 330,610).

```
interface GigabitEthernet0/1
 description TRUNK:SW3.CAZ.GYE.EC:GE0/3
 port-type nni
 switchport trunk native vlan 330
 switchport trunk allowed vlan 7,8,330,610
 switchport mode trunk
 bandwidth 1000000
 rep segment 233
 rep preempt delay 45
 storm-control broadcast level pps 300 100
 storm-control multicast level pps 300 100
 storm-control action trap
 service-policy input GX-Ingress-GE
 service-policy output GX-Egress-GE

interface GigabitEthernet0/2
 description TRUNK:MESB2.DAU.GYE.EC:GE0/3
 port-type nni
 switchport trunk native vlan 330
 switchport trunk allowed vlan 7,8,330,610
 switchport mode trunk
 bandwidth 1000000
 load-interval 30
 rep segment 330 preferred
 rep preempt delay 45
 storm-control broadcast level pps 300 100
 storm-control multicast level pps 300 100
 storm-control action trap
 service-policy input GX-Ingress-GE
 service-policy output GX-Egress-GE
```

Se configura la dirección IP de monitoreo del *switch*.

```
interface Vlan8
 ip address 10.5.80.39 255.255.255.0
!
ip default-gateway 10.5.80.254
```

3.3.2.3.2 Radio Ceragon sede Sucursal Mayor Guayaquil

Para el equipo de radio se asignaron los siguientes parámetros de configuración, para el monitoreo respectivo.

IP Monitoreo Radio Nodo: 10.5.117.136

IP Monitoreo Radio Cliente 10.5.117.137

MASK: 255.255.255.128

GW: 10.5.117.129
sw.dau.gye.ec
Puerto0/ 10 Vlan 116
Frec TX Nodo: 23317.000
Frec TX Cliente: 22085.000
LINK ID: 2302
Polaridad : Vertical
Diámetro de Antena: 0,6 m

3.3.3 AGENCIA ALMAGRO

La sede cuenta con un acceso de cobre por medio de equipos MUSIC 200. Para el diseño se ha considerado una solución por medio de conversores de fibra óptica punto a punto como se indica en la figura 3.23.

Los conversores de marca TP-Link, se enlazan por medio de un hilo de fibra óptica dando conectividad al equipo *router* 881 ubicado en la sede del cliente y el *switch* de acceso ubicado en el nodo 1492.

3.3.3.1 Servicio de Datos sede Almagro

Router 881

Se ha definido la VLAN de datos 390, en el *router* CE se debe configurar una ruta estática hacia el *router* de borde, y por medio de la nube IP/MPLS se provee la conexión con las demás sedes. Las sedes alternas que no cuentan con la criticidad de una sede principal, usualmente se tienen *backups* con otro proveedor de servicios.

Para la sede Almagro la IP WAN es 10.111.114.203/29 y la IP LAN es 195.1.6.1/24. A continuación se indica la configuración del *router*:

hostname ALMAGRO Nombre del equipo

Se configura la IP WAN y la IP LAN en el *router*.

```
interface FastEthernet4.390
 encapsulation dot1Q 390
 ip address 10.111.114.203 255.255.255.128
interface Vlan1
 ip address 195.1.6.1 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.111.114.201
```

3.3.3.2 Equipo de acceso a nivel de nodo

Se configura la VLAN 390 en el *switch* del Nodo 1492

```
interface FastEthernet0/9
 description  Banco_Almagro
 switchport trunk allowed vlan 390
```

3.3.4 AGENCIAS CUMBAYÁ, SANGOLQUÍ Y SAN RAFAEL

Se ha utilizado la infraestructura física de las sedes para instalar los nuevos equipos de radio en las 3 sedes.

El acceso se lo ha diseñado por medio de equipos de radio *Ceragon* modelo *IP10 E.,* en la banda de 23 GHz, con datos a 2 Mbps, con los cuales se da conectividad a los equipos Cisco 881 ubicados en la sede del cliente con el *switch* de acceso ubicado en el nodo, tal como se indica en las figuras 3.24 y 3.25.

3.3.4.1 Servicio de datos sedes Cumbayá, Sangolquí y San Rafael

En el *router* se configura la interfaz WAN encapsulada en la VLAN 390 con su respectiva dirección IP, y en la VLAN 1 se configura la dirección IP LAN respectiva para cada sede. Además se configura la ruta estática hacia el *router* de borde.

Para la sede Cumbayá la IP WAN es 10.111.114.204/29 y la IP LAN es 195.1.7.1/24.
Para la sede Sangolquí la IP WAN es 10.111.114.205/29, en tanto que la IP LAN es 195.1.8.1 /24.

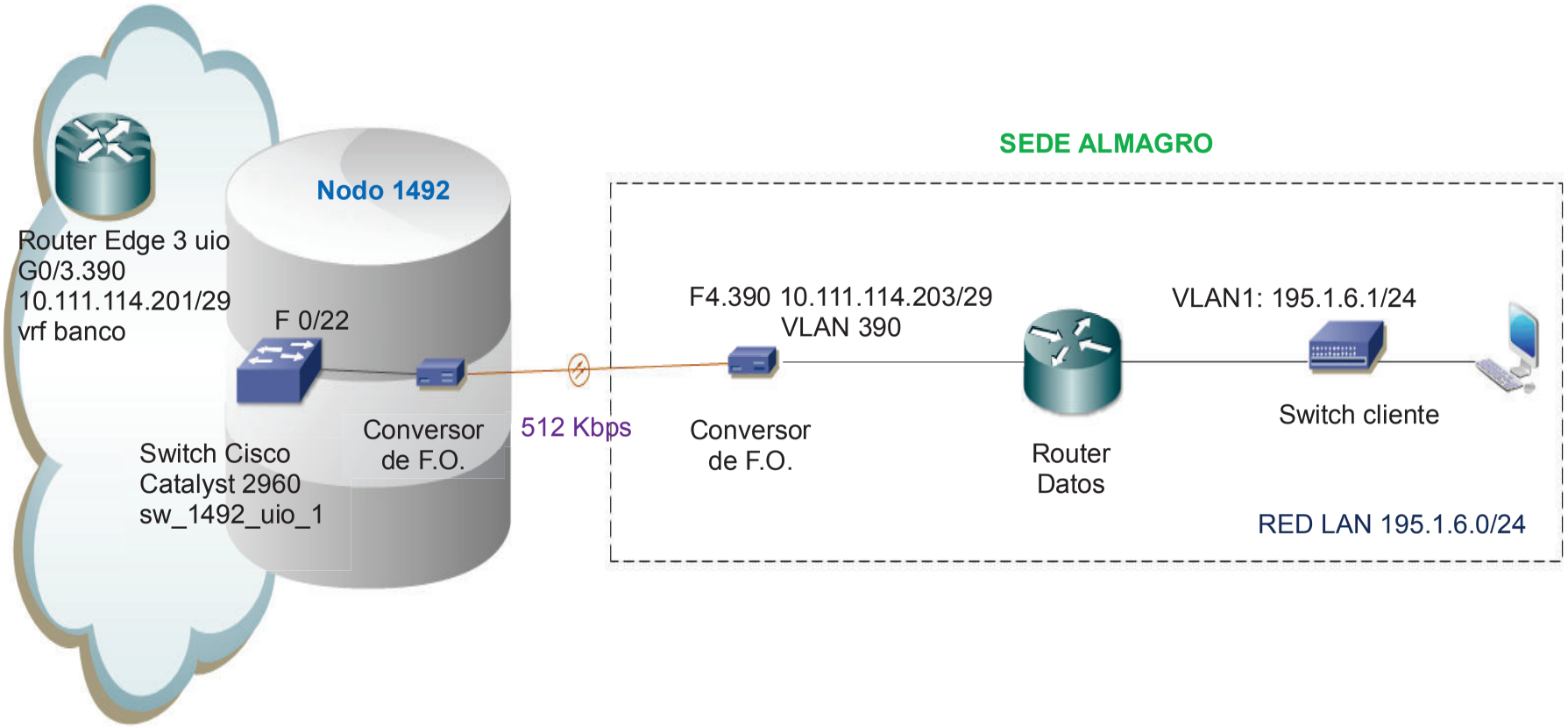


Figura 3.22 Diagrama de servicios para la sede Almagro

Para la sede San Rafael la IP WAN es 10.111.114.206/29, mientras que la IP LAN es 195.1.9.1 /24.

A continuación a manera de ejemplo se indican los comandos de configuración de la sede Cumbayá.

```
CUMBAYA#sh run
hostname CUMBAYA

interface FastEthernet4.390
 encapsulation dot1Q 390
 ip address 10.111.114.204 255.255.255.128     Se configura la IP WAN
interface Vlan1
 ip address 195.1.7.1 255.255.255.0            Se configura la IP LAN.
ip route 0.0.0.0 0.0.0.0 10.111.114.201        Se configura la ruta estática.
```

3.3.4.2 Equipos de acceso

3.3.4.2.1 Equipo de radio Ceragon

Se asignaron los siguientes recursos para los equipos de radio Ceragon para las 3 sedes tal como se indica en la tabla 3.12.

	Cumbayá	Sangolquí	San Rafael
IP Mon.Radio Nodo	10.5.113.136	10.5.113.138	10.5.113.100
IP Mon. Radio Cliente	10.5.113.137	10.5.113.139	10.5.113,101
Máscara	255.255.255.128	255.255.255.128	255.255.255.128
Concentrador	sw_ilum_uio_1	sw_ilum_uio_1	sw_fore_uio2
Puerto concentrador	ethe1/0/3	ethe1/0/4	ethe1/0/1
VLAN	116	116	116
Frec. TX Nodo	23317	23247	23401
Frec. TX Cliente	22085	22015	22169
LINK ID:	1002	1703	1732
Polaridad	Vertical	Vertical	Vertical
Diámetro de Antena	0,6m	0,6m	0,6m

Tabla 3.12 Recursos enlaces de radio Cumbayá, Sangolquí y San Rafael

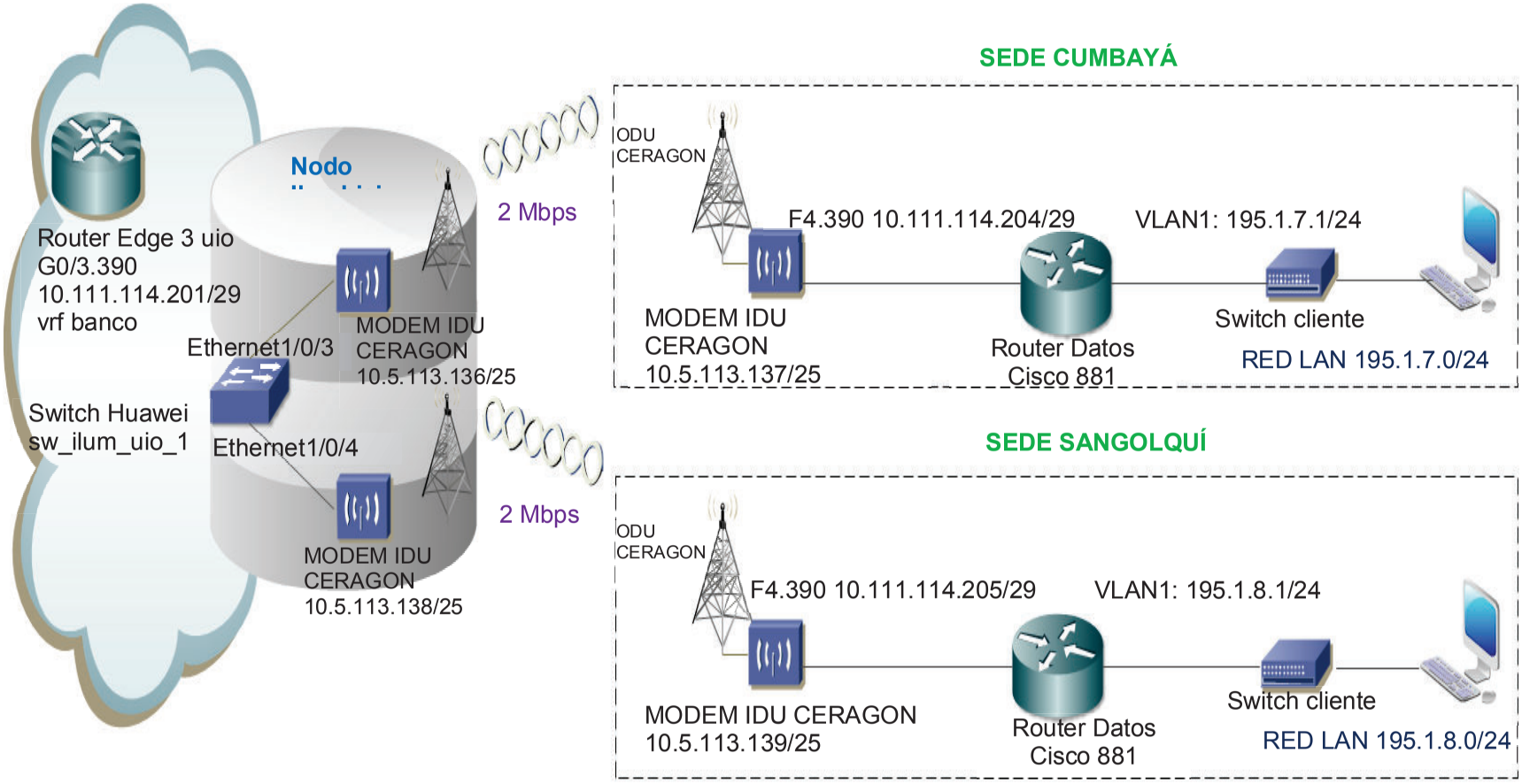


Figura 3.23 Diagrama de servicios de las sedes Cumbayá y Sangolquí

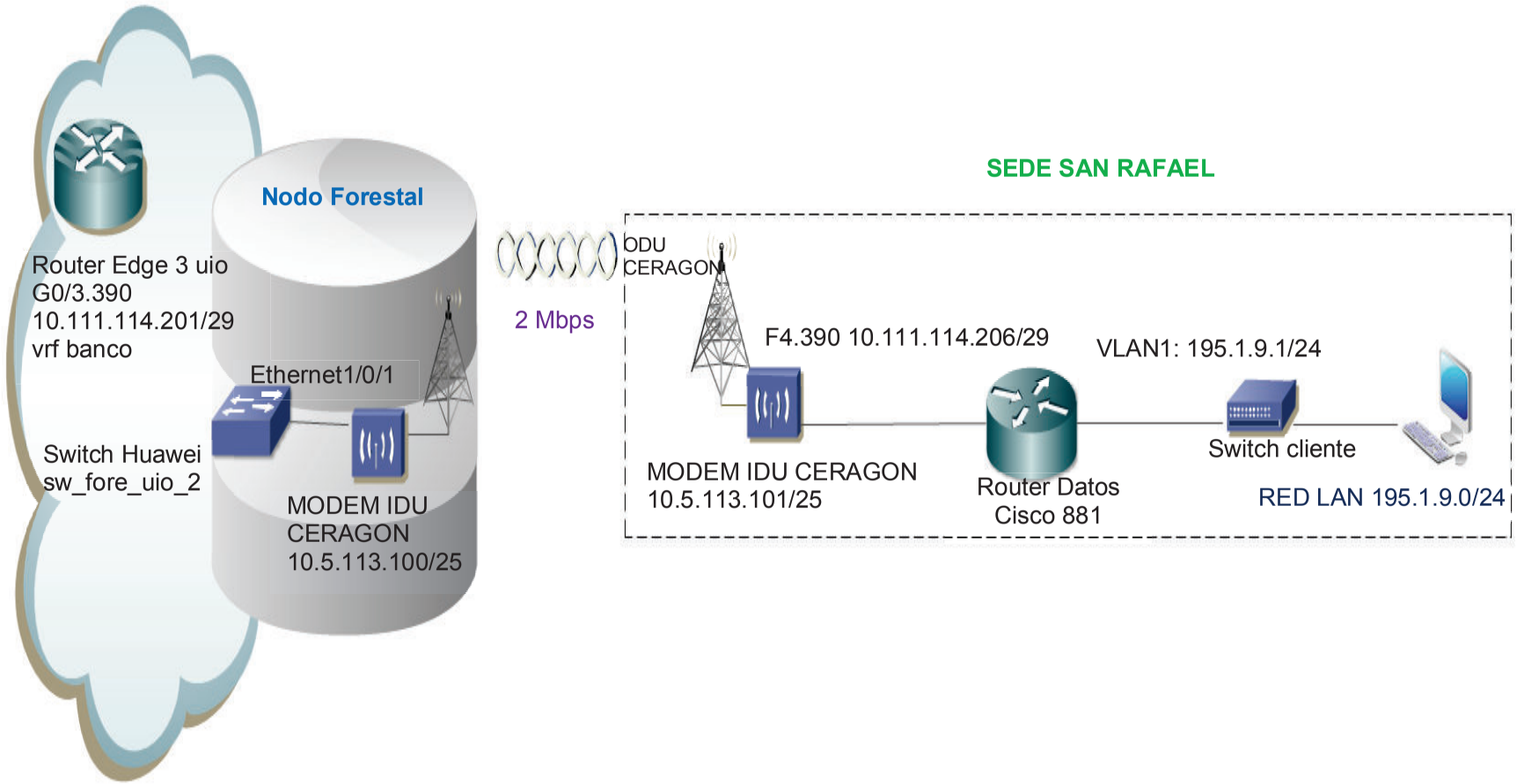


Figura 3.24 Diagrama de servicios de la sede San Rafael

3.3.4.2.2 Configuración del switch en el nodo

En los nodos, el enlace de radio se conecta a un *switch* Huawei, donde en cada puerto correspondiente a cada enlace, se configura la VLAN 390 y se limita el ancho de banda, de la siguiente manera:

```
interface Ethernet1/0/3
 description CUMBAYA
port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 390
 broadcast-suppression PPS 300
 multicast-suppression PPS 300
 mac-address max-mac-count 1
 loopback-detection control enable
 loopback-detection per-vlan enable
 loopback-detection enable
 line-rate inbound 2048
 line-rate outbound 2048
```

3.3.5 AGENCIA RÍO PLAZA Y BEATERIO

Para las dos sedes, por el rango de cobertura, se ha considerado una solución inalámbrica; para la sede Río Plaza hacia la radio base Cerro del Carmen y para la sede Beaterio hacia la radio base Daule.

Por el tráfico moderado de 512 Kbps que van a soportar las radio bases, los recursos de una base multipunto deben solventar los requerimientos adecuadamente. Un diagrama de parámetros de configuración de estas sedes se indica en la figura 3.26.

Se han asignado recursos de radio (SDA y SPR) y un *router* Cisco 871 para cada enlace.

3.3.5.1 Servicio de Datos sede Río Plaza y Beaterio

En el *router* se configura la interfaz WAN que se encapsula en la VLAN 390 con su respectiva dirección IP, y en la VLAN 1 se configura la dirección IP LAN para cada sede; además se configura la ruta estática hacia el *router* de borde.

Se muestra a continuación un ejemplo de configuración del *router* de datos para la sede Río Plaza.

```
RIOPLAZA#sh run
hostname RIOPLAZA
!
interface FastEthernet4.390
 encapsulation dot1Q 390
 ip address 10.112.114.115 255.255.255.128

interface Vlan1
 ip address 195.1.14.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.112.114.113
```

Para la sede Beaterio la IP WAN es 10.112.114.116/29, en tanto que la IP LAN es 195.1.15.1 /24.

3.3.5.2 Equipos de acceso para la sede Río Plaza y Beaterio

3.3.5.2.1 Equipo remoto Micromax

Para la gestión del equipo se configuran los parámetros de direcciones IP, en la tabla de canales se escoge la opción de 3.5 MHz, se configura el identificador de la radio base a la cual va a pertenecer la estación remota, además se configura la potencia máxima de transmisión así como la velocidad y duplexación de los puertos Ethernet, tal como se indica en la figura 3.27.

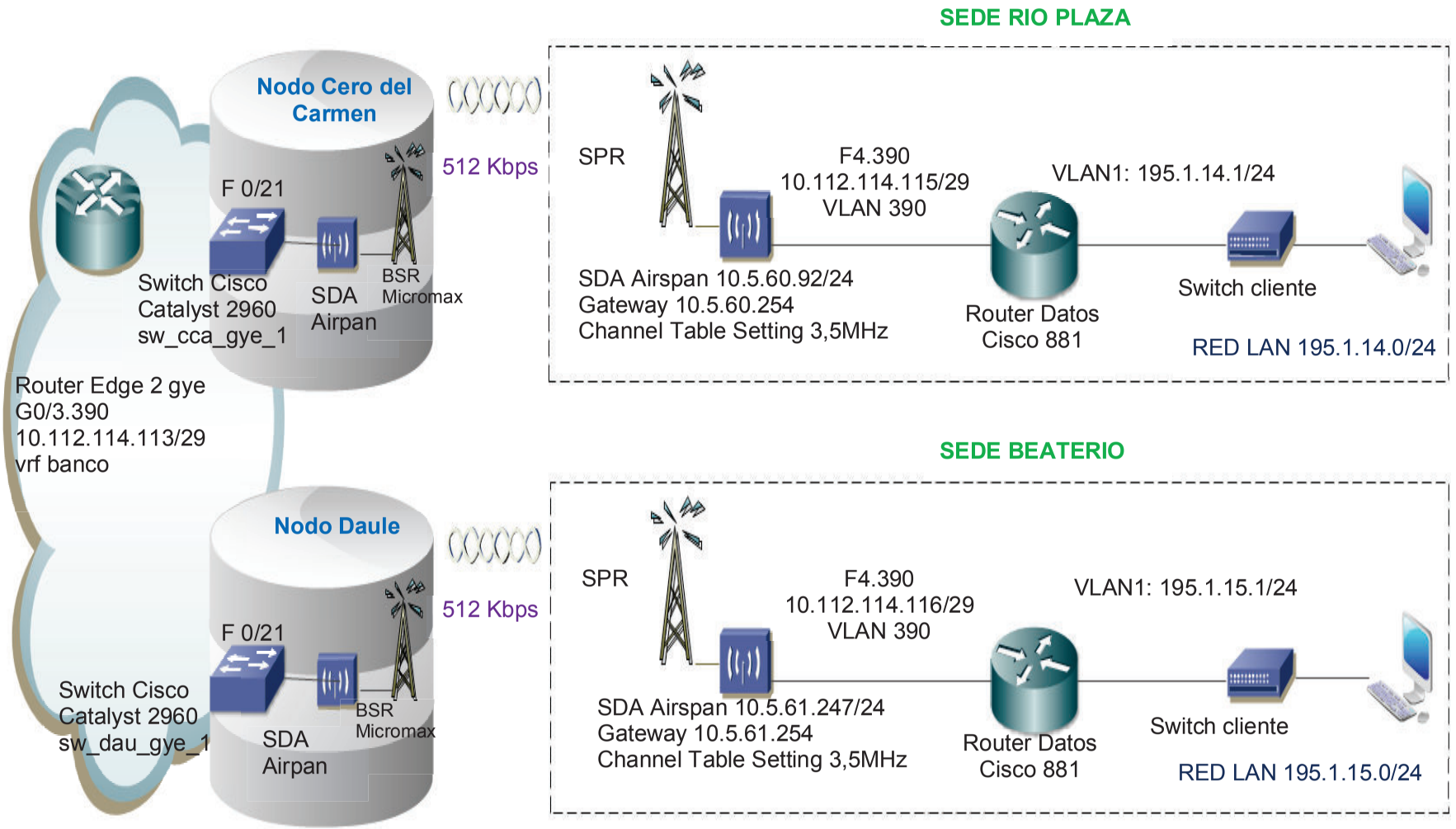


Figura 3.25 Diagrama de servicios de la sede Río Plaza y Beaterio

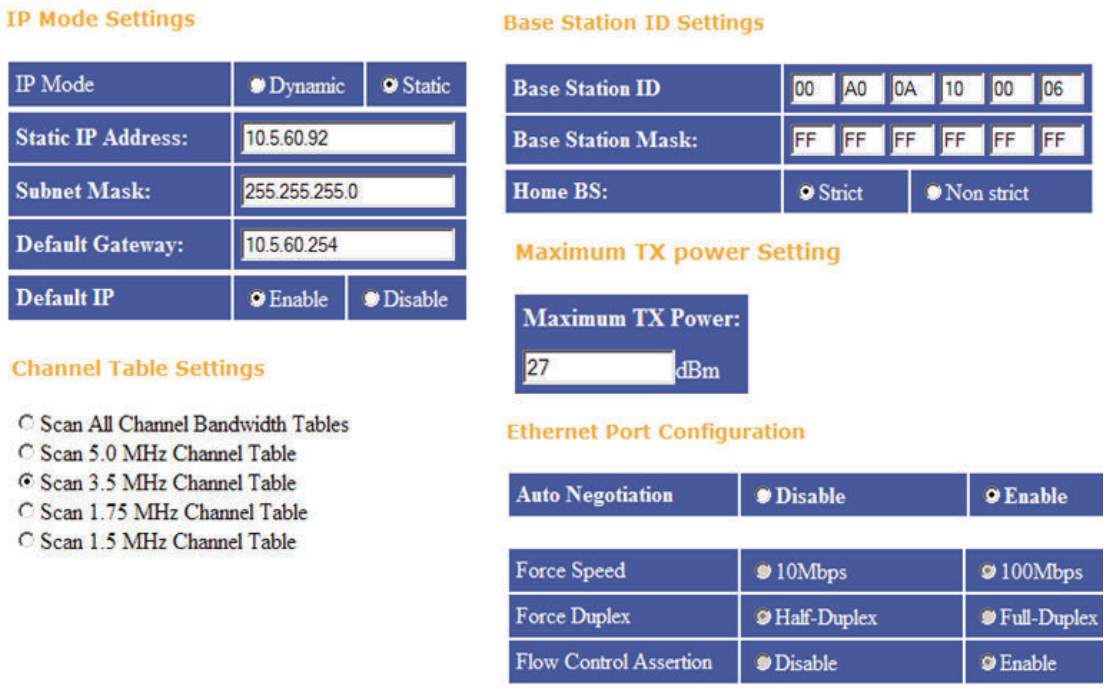


Figura 3.26 Configuración de los parámetros para la sede Río Plaza

Los parámetros de configuración se indican en la tabla 3.13.

	Río Plaza	Beaterio
Micromax	CERRO DEL CARMEN	DAULE NORTE
IP MODE	Static	Static
IP Address:	10.5.60.92	10.5.61.247
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway:	10.5.60.254	10.5.61.254
Channel Table Setting:	3,5 MHz	3,5 MHz
First UL Channel Frec	1429500 khz	1427500 Khz
Last UL Channel Frec	1524000 khz	1522000Khz
Bs id:	00:a0:0a:10:00:06	00:a0:0a:10:00:09
Bd mask	ff:ff:ff:ff:00:00	ff:ff:ff:ff:00:00

Tabla 3.13 Recursos de las estaciones remotas Río Plaza y Beaterio.

3.3.5.2.2 Gestión radio Base a nivel de nodo

Para registrar el equipo remoto SDA en la radio base del nodo, se debe ingresar la dirección *mac-address* de la remota, el producto de servicio, perfil de configuración personalizada, VLAN en el perfil de puerto donde se etiqueta la VLAN de datos,

canal de servicio permitido y los canales registrados como se indica en la figura 3.28.

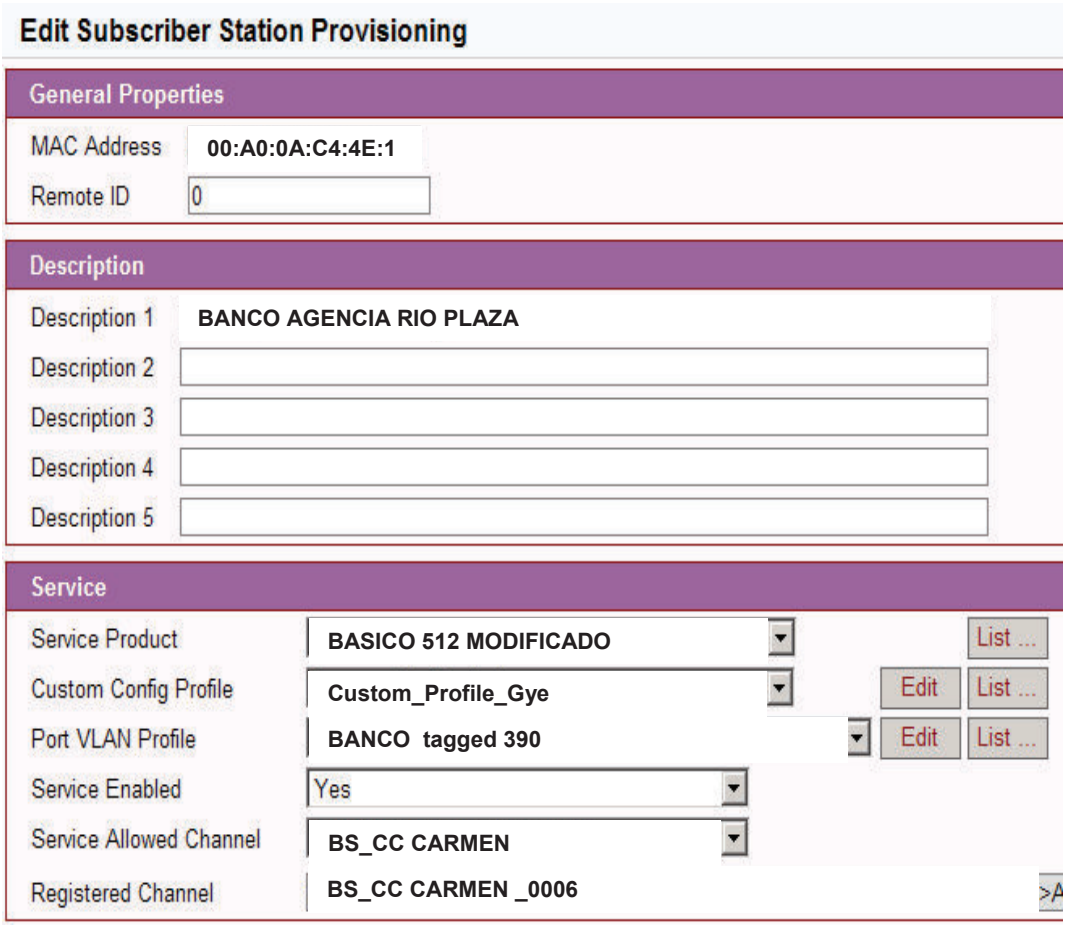


Figura 3.27 Registro de la estación remota en la radio Base de la sede Río Plaza

Para la sede Beaterio se consideran los mismos parámetros de configuración de Río Plaza, únicamente modificando la *mac-address* de la remota que es 00:A0:0A:CA:58:F8, y el canal de servicio permitido que es BS_DAULE.

3.3.5.2.3 Switch en el nodo

Se debe configurar la VLAN 390 en el *switch* que se conecta atrás de la radio base, para propagar la VLAN por la red.

Esta configuración debe estar tanto en el *switch* sw_cca_gye_1 como en el sw_dau_gye_1.

```
interface FastEthernet0/21
 description TRUNK:WIRELESS [WIPLL_MICROMAX_CCARMEN]
```

Se observa VLANs de otros clientes que llegan a la base Micromax Cerro del Carmen, entre ellas está la VLAN 390 configurada para el cliente.

Además se configuran las protecciones respectivas de *Spanning Tree.*

```
switchport trunk allowed vlan 70,108,261,263,270,280,297,306,349,390
switchport mode trunk
 storm-control broadcast level pps 300 100
 storm-control multicast level pps 300 100
 storm-control action trap
 no cdp enable
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
 spanning-tree guard root
```

3.3.6 AGENCIA EGUAGIROS SUR Y DOMINGO COMÍN

Por las ventajas que tiene la fibra óptica sobre el cobre en larga distancia y por ser este último un recurso susceptible a hurtos, se ha procedido a diseñar una solución por medio de fibra óptica punto a punto para la sedes Ecuagiros Sur y Domingo Comín tal como se indica en la figura 3.29.

Los recursos utilizados en el diseño por sede son conversores de fibra óptica marca CTC conectados por medio de un hilo de fibra óptica para dar conectividad al *router Cisco* 881 ubicado en el cliente con el *switch* de acceso ubicado en el nodo.

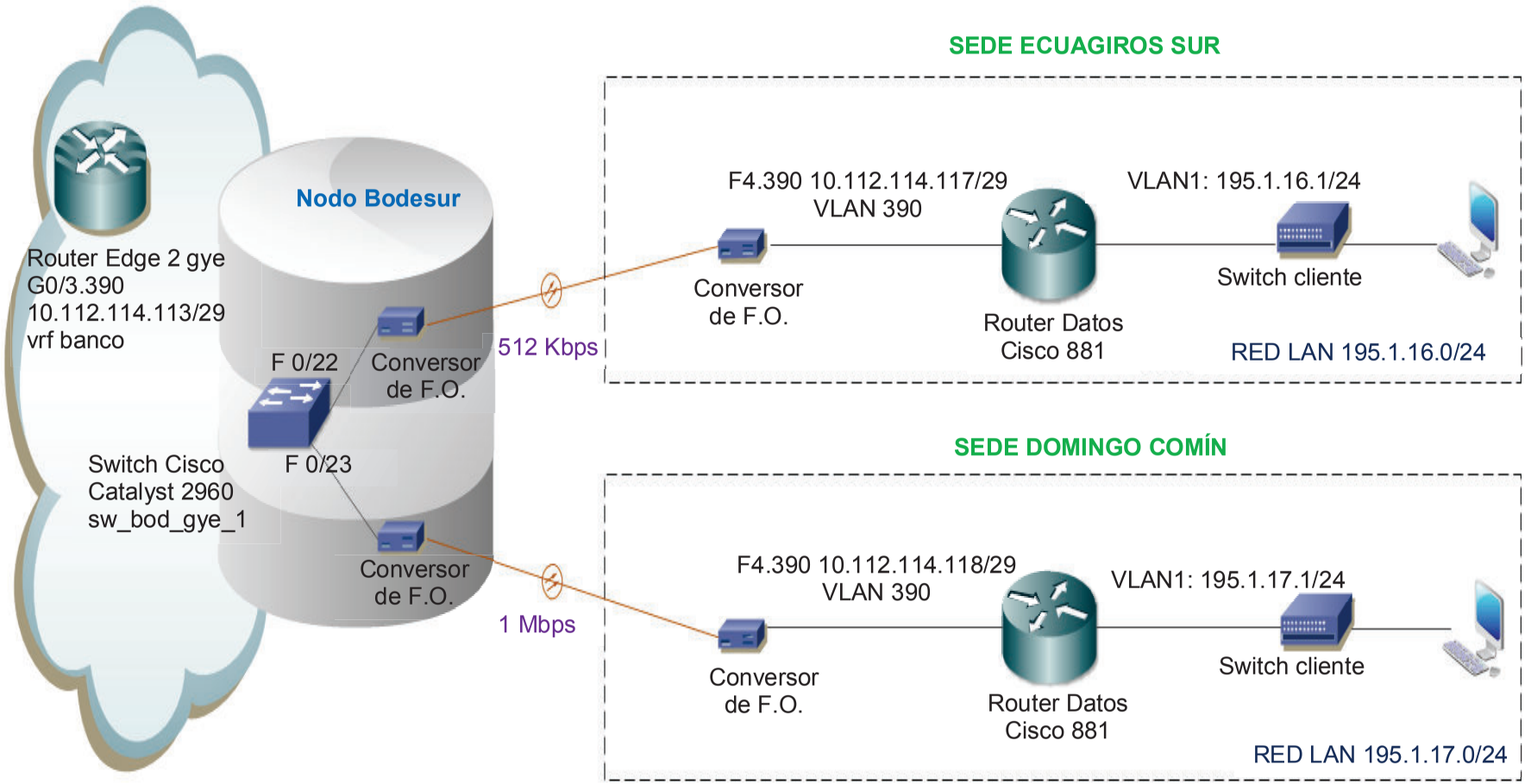


Figura 3.28 Diagrama de servicios de las sedes Ecuagiros Sur y Domingo Comín

3.3.6.1 Servicio de Datos sede Ecuagiros Sur y Domingo Comín

Se mantiene la configuración de las agencias donde solo cursan datos. Para la sede Ecuagiros Sur, la IP WAN es 10.112.114.117 255.255.255.128 y la IP LAN es 195.1.16.1 255.255.255.0.
Mientras que para la sede Domingo Comín la IP WAN es 10.112.114.118 255.255.255.128 y la IP LAN es 195.1.17.1/24.

En ambos *routers* se configura la ruta estática hacia el *router* de borde.

```
ip route 0.0.0.0 0.0.0.0 10.112.114.113
```

3.3.6.2 *Switch* de acceso a nivel de nodo

A nivel de *switch* en el nodo se aplican políticas para limitar la velocidad del canal a 512 Kbps para Ecuagiros Sur y a 1 Mbps para Domingo Comín

```
interface FastEthernet0/22
 description ECUAGIRO SUR.
 switchport trunk allowed vlan 390
 switchport mode trunk
 switchport port-security maximum 1
 switchport port-security
 switchport port-security violation restrict
 bandwidth 512
 speed 100
 duplex full
 storm-control broadcast level pps 300
100
 storm-control multicast level pps 300
100
 storm-control action trap
 service-policy input 512K
 service-policy output 512K

policy-map 512K
 class class-default
   police cir 512000 bc 64000 be 128000
     conform-action transmit
     exceed-action drop
```

```
interface FastEthernet0/23
 descriptionDOMINGOCOMIN
 switchport trunk allowed vlan 390
 switchport mode trunk
 switchport port-security maximum 1
 switchport port-security
 switchport port-security violation restrict
 bandwidth 1024
 speed 100
 duplex full
 storm-control broadcast level pps 300
100
 storm-control multicast level pps 300
100
 storm-control action trap
 service-policy input 1024K
 service-policy output 1024K

policy-map 1024K
 class class-default
   police cir 1024000 bc 128000 be
256000
     conform-action transmit
     exceed-action drop
```

3.3.7 CUADRO RESUMEN DE DIRECCIONAMIENTO IP

Direccionamiento por sede y capacidad configurada por acceso se indica en la tabla 3.14

Sede	Equipo Edge	Edge	WAN	LAN	VLAN	Servicio	Capacidad
Matriz Quito	edgeuio3	10.111.114.201/29	10.111.114.202/29		390	Datos Principal	18 Mbps
	edgeuio2	10.111.116.233/29	10.111.116.234/29	195.1.5.1/24	1731	Datos *Backup*	18 Mbps
	edgeuio1	201.234.192.37/30	201.234.192.38/30		2314	Internet Principal	5 Mbps
	edgeuio4	201.234.219.109/30	201.234.219.110/30	200.41.1.249/29	2322	Internet *Backup*	5 Mbps
				10.112.136.162/28	610	Video	2 Mbps
Parque California	edgegye2	10.112.114.113/29	10.112.114.114/29		390	Datos Principal	8 Mbps
	edgegye1	10.112.131.25 / 29	10.112.131.26 /29	195.1.13.1/24	1731	Datos *Backup*	8 Mbps
	edgegye3	190.216.212.209/30	190.216.212.210/30		2314	Internet Principal	2 Mbps
	edgegye4	190.216.212.213/30	190.216.212.214/30	201.234.204.73/29	2322	Internet *Backup*	2 Mbps
				10.112.136.164	610	Video	2 Mbps
Ag. Almagro	edgeuio3	10.111.114.201/29	10.111.114.203/29	195.1.6.1/24	390	Datos	512 Kbps
Ag. Cumbayá	edgeuio3	10.111.114.201/29	10.111.114.204/29	195.1.7.1/24	390	Datos	2 Mbps
Ag. Sangolquí	edgeuio3	10.111.114.201/29	10.111.114.205/29	195.1.8.1/24	390	Datos	2 Mbps
Ag. San Rafael	edgeuio3	10.111.114.201/29	10.111.114.206/29	195.1.9.1/24	390	Datos	2 Mbps
Ag. Río Plaza	edgegye2	10.112.114.113/29	10.112.114.115/29	195.1.14.1/24	390	Datos	512 Kbps
Ag. Beaterio	edgegye2	10.112.114.113/29	10.112.114.116/29	195.1.15.1/24	390	Datos	512 kbps
Ag. Ecuagiros Sur	edgegye2	10.112.114.113/29	10.112.114.117/29	195.1.16.1/24	390	Datos	512 Kbps
Ag. Domingo Comín	edgegye2	10.112.114.113/29	10.112.114.118/29	195.1.17.1/24	390	Datos	1 Mbps

Tabla 3.14 Cuadro resumen de direccionamiento IP y capacidades

3.4 SERVICIOS DE VIDEOCONFERENCIA Y TELEFONÍA EN LA RED

Se definen las políticas para priorizar el tráfico de audio y video con respecto al tráfico de datos.

3.4.1 SERVICIO DE VIDEOCONFERENCIA

El servicio de videoconferencia es importante para reuniones virtuales entre los ejecutivos de las sedes Quito y Guayaquil, por lo cual se debe considerar las políticas adecuadas en la red para brindar un servicio de calidad.

3.4.1.1 Equipos de Videoconferencia

El equipo de videoconferencia HD es de la marca Polycom® modelo QDX6000. La versión de software es QDX6000 Release - 4.0.1-3040, que cumple con los estándares de video H.264, H.263, H.261, entre otros; para la solución se ha habilitado el estándar H.323.

En la figura 3.30 se indican algunos de los parámetros de configuración del equipo Polycom.

Por comandos se pueden verificar los parámetros activos en el equipo de videoconferencia, tal como se indican a continuación.

```
-> display whoami
2013-04-11 19:05:05 DEBUG avc: pc[0]: uimsg: C: display whoami
Hi, my name is :                QDX6000
Model:                          QDX 6000
Serial Number:                  Q61037BE4EAE1981
Software Version:       Release - 4.0.1-3040
SNTP Time Service:              Off oosync 0.0.0.0
Local Time is:                  Thu, 01 Apr 2014 14:05:05
IP Video Number:        10.112.136.162
Link-Local Address:     fe80::204:f2ff:febe:4eae/64
ISDN Video Number:      593.
H323 Enabled:           True
HTTP Enabled:           True
```

SNMP Enabled: True

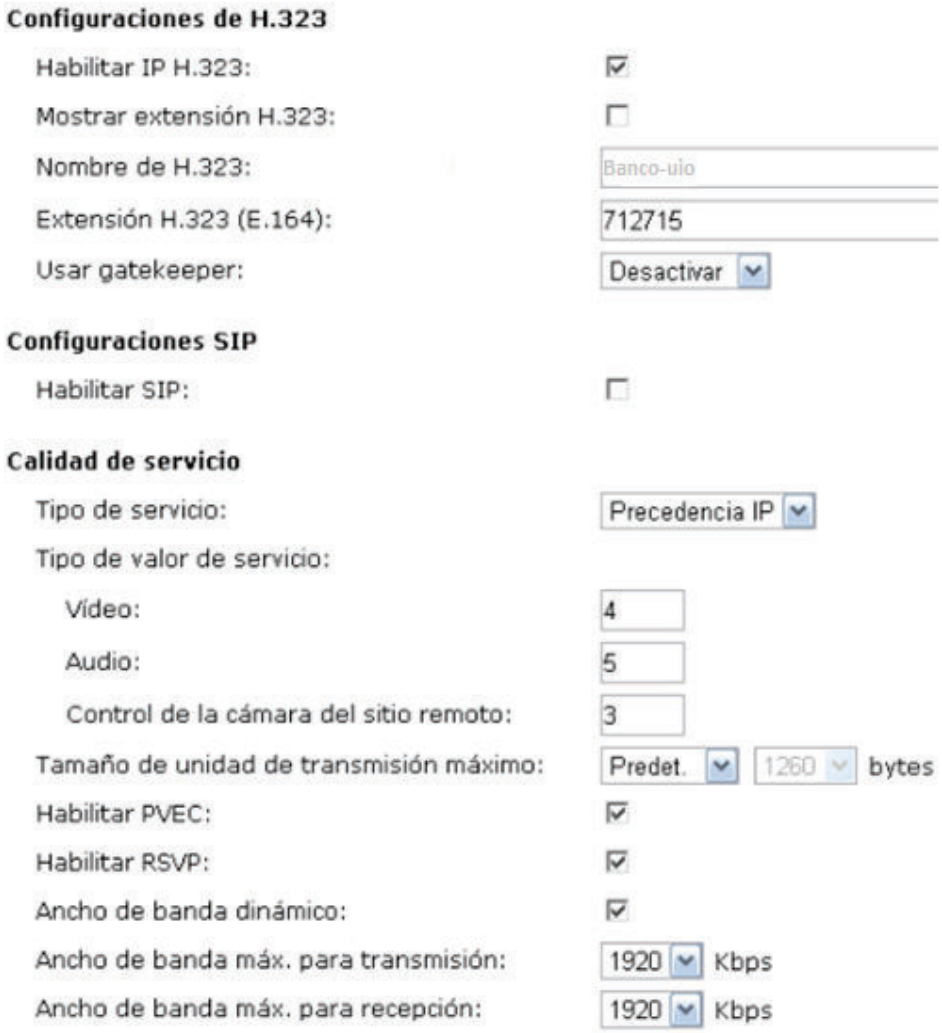


Figura 3.29 Configuración de parámetros del equipo Polycom

-> displayparams
systemname QDX6000
hostname bancouio
ipaddress 10.112.136.162
version "Release - 4.0.1-3040"
serialnum q61037be4eae1981
displaygraphics yes
vgaresolution 60hz1280x720
vgaphase 32
numberofmonitors 2
monitor1 16:9
monitor2 4:3
vgahorizpos 128
vgavertpos 128
cameradirection normal
farcontrolnearcamera yes
primarycamera 1
backlightcompensation no
telecountrycode <empty>

```
teleareacode <empty>
telenumber <empty>
roomphonenumber <empty>
echocancellerred no
echocancellerwhite no
muteautoanswer no
vcraudioout no
redlineinput vcr
whitelineinput vcr
redlinelevel 5
whitelinelevel 5
lineoutputs monitor
lineoutputslevel 5
mpmode auto
sleeptime 3
sleeptext <empty>
rs232 mode control
rs232 baud 9600
rs232port1 mode vortex_mixer
rs232port1 baud 9600
2013-04-11 19:17:29 DEBUG avc: pc[0]:
uimsg: C: displayparams

> ipstat
hostname Banco-uio
winsresolution no
dhcp off
ipaddress 10.112.136.162
defaultgateway 10.112.136.161
subnetmask 255.255.255.240
winsserver 0.0.0.0
lanport auto
webaccessport 80
```

Para observar cómo está configurado el puerto LAN y las opciones que presenta el puerto se pueden ingresar los siguientes comandos:

```
-> lanport get
lanport auto

-> lanport
auto, 10, 10hdx, 10fdx,100, 100hdx, 100fdx, autohdx, autofdx, get,
```

Detalles técnicos y de instalación se adjuntan en el Anexo K.

3.4.1.2 Configuraciones en la red

Los equipos de Videoconferencia son equipos de alta definición, que en pruebas prácticas no funcionan atrás de los *routers*, por inconvenientes en el manejo de las tramas; por esta razón se ha diseñado la solución por medio de una LAN extendida,

en la que los equipos están conectados directamente a los puertos del *switch*, y en el *backbone* estarán bajo la VRF **banco_vc**.

En el *router* de *edge* se tiene la siguiente configuración:

```
address-family ipv4 vrf banco_vc
  no synchronization
  redistribute connected
  redistribute static
 exit-address-family

interface GigabitEthernet0/3.610
 description BANCO VIDEO VIDEOCONFERENCIA]
encapsulation dot1Q 610
 ip vrf forwarding banco_vc
 ip address 10.112.136.161 255.255.255.248
 ip access-group 2646 in
 no ip redirects
 no ip proxy-arp
 no cdp enable
 arp timeout 300
 service-policy input  BANCO_IN
 service-policy output BANCO_OUT
```

Las listas de acceso, son utilizadas para identificar adecuadamente el tráfico que tendrá que estar marcado en el punto de entrada.

```
access-list 2646 deny   udp any any eq 646
access-list 2646 deny   tcp any any eq 646
access-list 2646 deny   46 any any
access-list 2646 permit ip any any
```

Los *class-map*, se crean para colocar el tráfico identificado por las listas de acceso en las clases de QoS apropiados.

```
class-map match-any VOICE
  match ip precedence 5
  match ip dscp ef

class-map match-any VIDEO
  match ip precedence 4
  match ip dscp af41
```

Se configuran las políticas aplicadas para el servicio de video a 2 Mbps.

```
policy-map BANCO_OUT
  class class-default
    shape average 10000000
   service-policy BANCO_OUT_ANIDADO
```

```
policy-map BANCO_OUT_ANIDADO
  class VOICE
    priority 2048
  class VIDEO
    bandwidth 2048

policy-map BANCO_IN
  class class-default
    shape average 10000000
   service-policy BANCO_IN_ANIDADO

policy-map BANCO_IN_ANIDADO
  class VOICE
    priority 2048
  class VIDEO
    bandwidth 2048
```

Se debe considerar que el equipo Polycom de la sede Matriz tiene la IP 10.112.136.162 y el equipo en la sede Guayaquil tiene la IP 10.112.136.164. El *default gateway* es la IP del *router* de borde 10.112.136.161.

3.4.2 SERVICIO DE TELEFONÍA

3.4.2.1 Equipos de telefonía

Para la solución se ha considerado equipos de la marca Audiocodes Series Mediant 1000 y MP 11X que transforman la señal analógica en digital, porque en pruebas de homologación han demostrado robustez y calidad en el servicio de telefonía. Detalles técnicos y de instalación se adjuntan en el Anexo L y Anexo M.

La solución que entregue el proveedor dependerá si el cliente dispone de una PBX analógica o digital.

Para el diseño se ha considerado el códec G.729, ya que ocupa 32 Kbps, para un buen rendimiento en el servicio; con un dimensionamiento de hasta 50 líneas, el ancho de banda reservado para telefonía es de 2 Mbps.

El modelo Mediant 1000 puede entregar a la central telefónica interfaces E1, FXS o FXO y puede manejar un total de hasta 100 lineas. El equipo se indica en la figura 3.31.

Figura 3.30 Equipo Mediant 1000

El modelo MP-118 cuenta con puertos FXS y puertos FXO, dependiendo del modelo puede ser de 4 o 8 puertos para el caso que se conecte a una central telefónica pequeña o terminales telefónicos. El equipo se ilustra en la figura 3.32.

Figura 3.31 Equipo Audio Codes MP-118 VoIP Gateway

Además el equipo consta de opciones de configuración, monitoreo, diagnóstico que facilitan el soporte técnico cuando se presenta una falla en el equipo.

3.4.2.1.1 Configuración

La administración del equipo se realiza por medio de un portal web con la IP por defecto 10.1.10.10. Se configuran los parámetros de red como la dirección IP, máscara y *gateway*. El equipo permite varios *códecs* de telefonía como G.729 G.723, G.711 entre otros, tal como se indica en el ejemplo de la figura 3.33.

Se configuran los números, extensiones y la dirección IP de destino; el protocolo de transporte por defecto es UDP, tal como se indica en la figura 3.34. En la figura 3.35 se asigna a cada puerto la extensión que va a usar localmente.

Se puede configurar la opción de automarcado en cada puerto y el número de destino que se va a llamar, como indica la figura 3.36.

El equipo cuenta con la opción de guardar la configuración en un archivo .ini en el caso de querer instalar un nuevo equipo con el propósito de reemplazarlo; esto facilita los trabajos de soporte técnico. A continuación se muestra la información del archivo .ini:

```
;**************
;** Ini File **
;**************

;Board: Mediant 1000
;Serial Number: 2995852
;Slot Number: 1
;Software Version: 5.40A.029
;DSP Software Version: 624AE3 => 540.15
;Board IP Address: 64.76.192.74
;Board Subnet Mask: 255.255.255.224
;Board Default Gateway: 64.76.192.65
;Ram size: 128M   Flash size: 32M
;Num DSPs: 20  Num DSP channels: 120
;Profile: NONE

;------- Mediant-1000 HW components-------
;
; Slot # : Module type : # of ports
;----------------------------------------
;      1 : FALC56      : 4
;----------------------------------------


[SYSTEM Params]

SyslogServerIP = 64.76.192.3
EnableSyslog = 1
DisableRS232 = 1
VXMLFIleName = ''
VoiceMenuPassword = 'disable'

[BSP Params]
```

En la figura 3.37 se indica el diagrama general de conexión entre las sedes principales con equipos Mediant 1000 y las sucursales con equipos Audiocodes.

Se ha tomado el ejemplo de configuración para la sede Almagro que se indica a continuación:

```
!
class-map match-all VOICE
 match access-group name VOICE
!
policy-map POLITICA
 class VOICE
  priority percent 20              Garantizo el 20% del AB para VOZ.
  set ip precedence 5              Defino a la VOZ con IPP 5
policy-map QOS
 class class-default
  shape average 512000
  service-policy POLITICA
!

interface FastEthernet1
 switchport access vlan 2         Puerto físico para telefonía
 duplex full
 speed 100
!
!
interface Vlan2
 ip address 172.16.140.9 255.255.255.248      LAN telefonía
!
ip access-list extended VOICE
 permit ip 172.16.140.32 0.0.0.7 any          Red de telefonía y wildcard
```

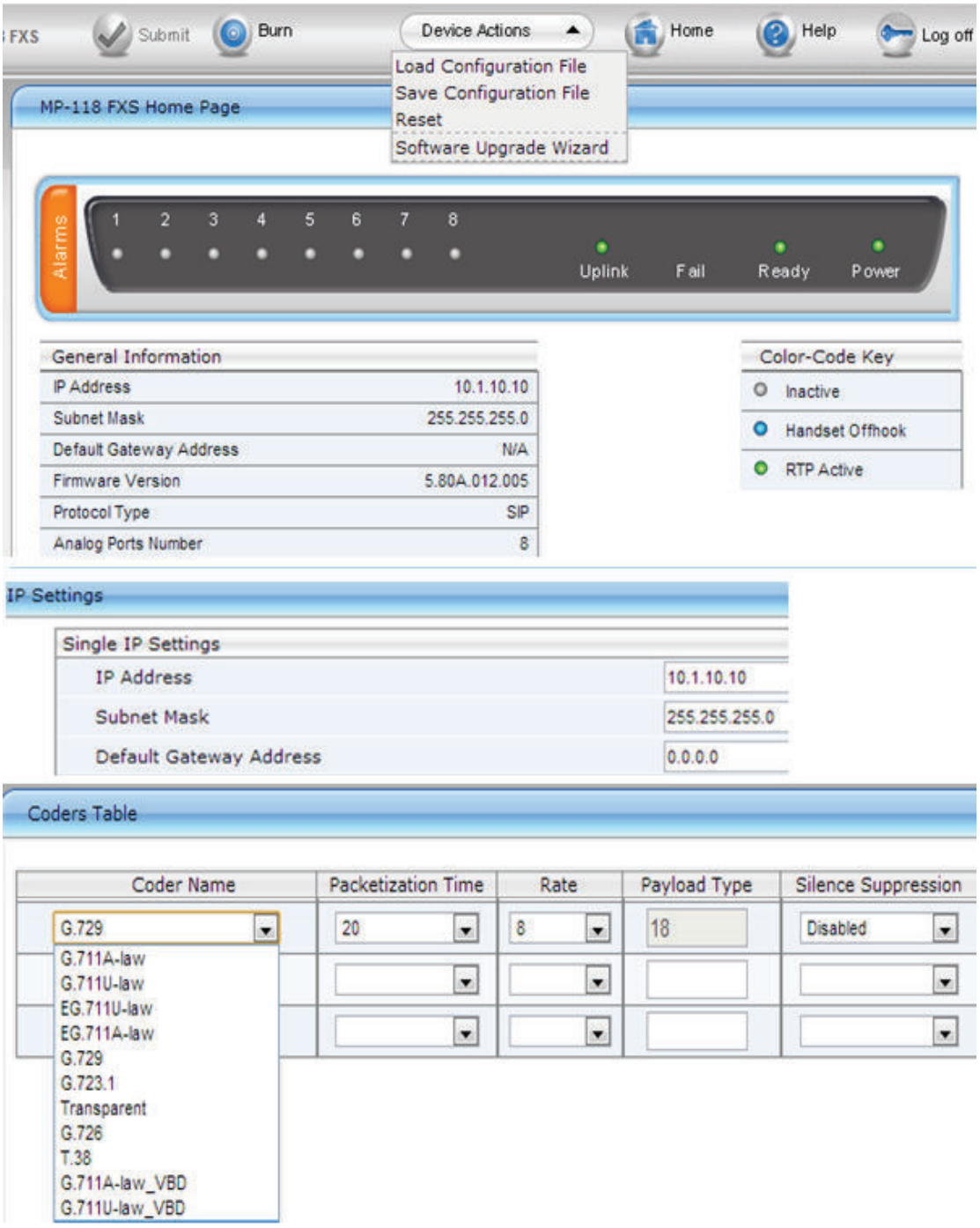


Figura 3.32 Parámetros generales del equipo Audiocodes

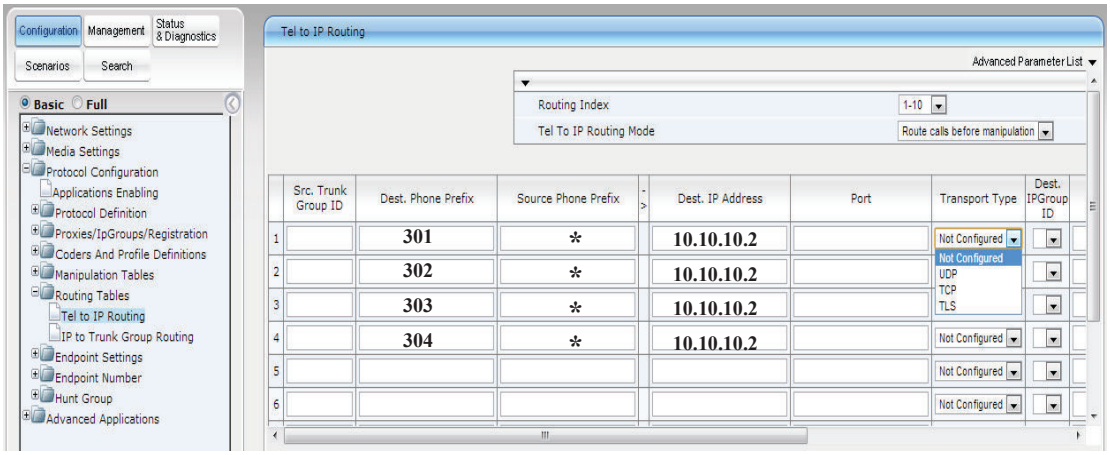


Figura 3.33 Enrutamiento telefonía a IP

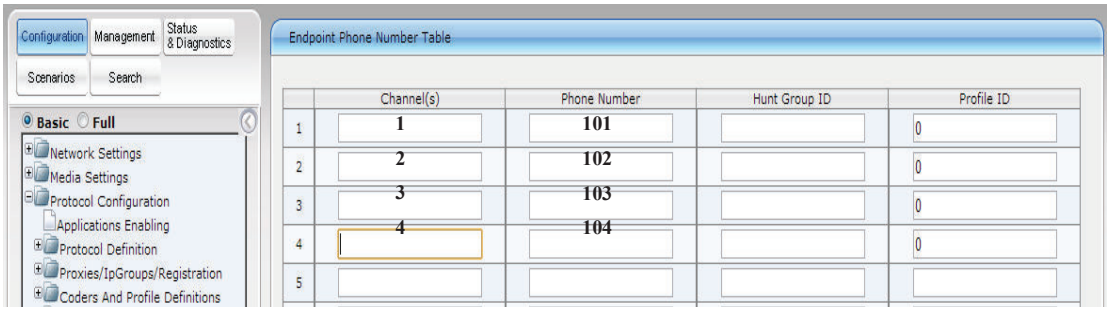


Figura 3.34 Configuración canal- extensión

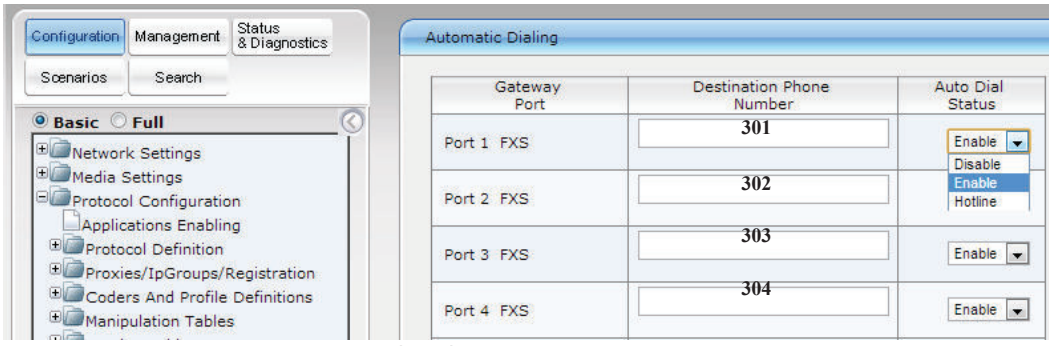


Figura 3.35 Configuración de marcado automático

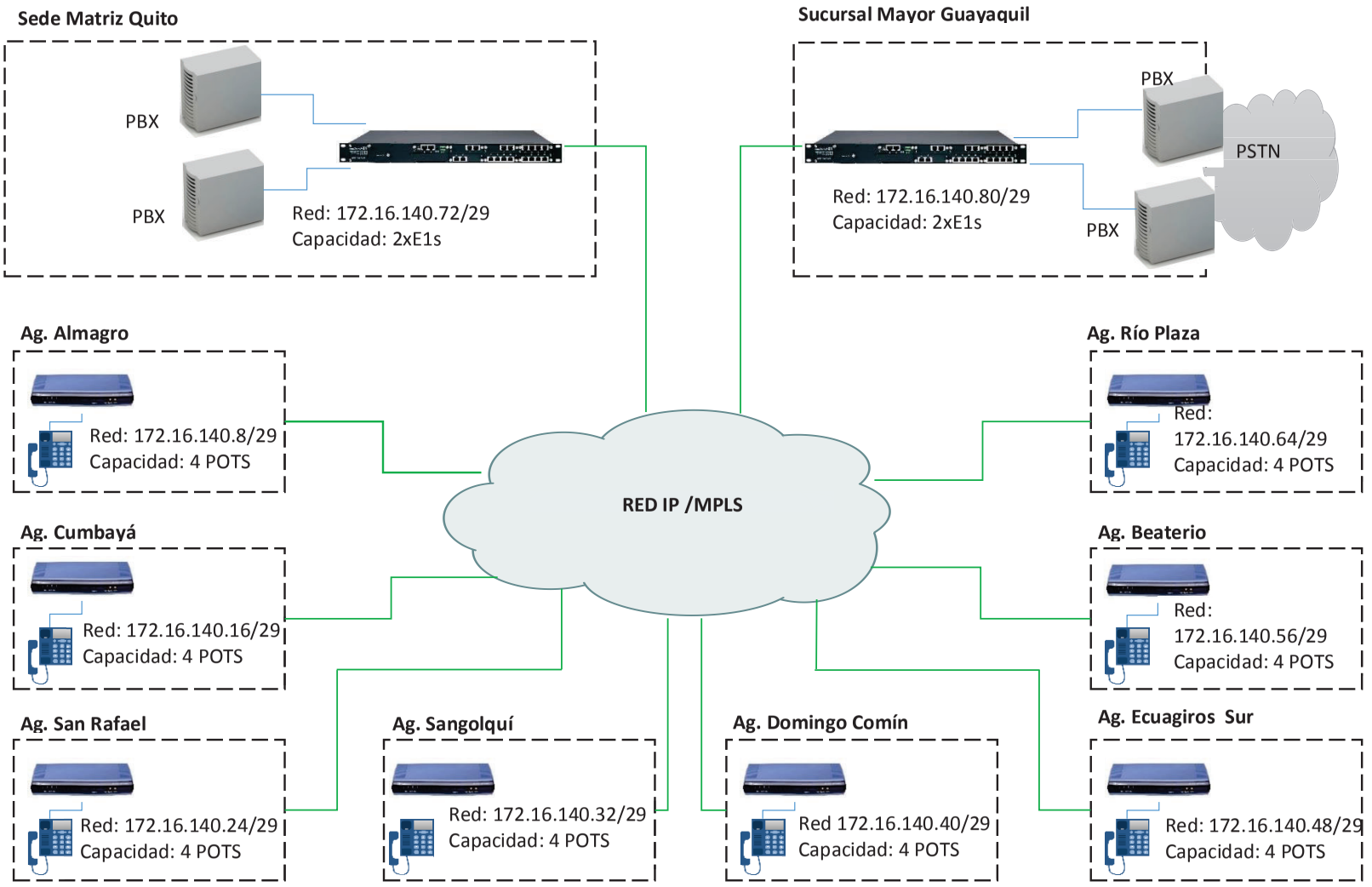


Figura 3.36 Diagrama General de Telefonía

3.5 ANÁLISIS FINANCIERO DEL PROYECTO

Desde el punto de vista del cliente su servicio se ve afectado por el tiempo de indisponibilidad del mismo, independiente del tipo de acceso de última milla. Los sistemas *legacy* al estar siendo remplazados por otras tecnologías, son caros y en ocasiones con elementos de difícil reposición.

Mientras que desde el punto de vista del proveedor de servicio, como estrategia de negocio, se actualizan los accesos y equipos de última milla, manteniendo condiciones de SLA con proyección a crecimiento.

Los equipos y solución de la antigua red *legacy* constituyen un costo hundido[4] para el proveedor, es decir los valores de los equipos durante el anterior proyecto, en su tiempo de vida útil, fueron trasladados a las tarifas de pago del cliente.

En el valor de los ingresos del proyecto se ha considerado el valor por enlace que el cliente pagará al proveedor de servicio mensualmente (*MRC Monthly Recurrent Charge*); adicionalmente se tendrá el valor por instalación del servicio que el cliente pagará al proveedor por única ocasión (*NRC Non Recurrent Charge*). Los valores referenciales se indican en la tabla 3.15, y fueron tomados de la fuente *Level3 Communication.*

Los costos que el proveedor de servicios incurre en cada sede se han detallado en las tablas 3.16 y 3.17.

Se han considerando los equipos de *internetworking* en cada sede como una inversión (Capex), así como los gastos en la compra de elementos para la instalación y servicios de instalación que se incurre una sola ocasión (Opex eventual).

[4] Costo hundido se considera al bien que se ha depreciado en el tiempo y tiene un valor de cero.

Mientras que los gastos que se incurren de manera periódica como valor por puerto, arrendamientos de ductos, pago por permisos de operación de los enlaces de radio en la Superintendencia de Telecomunicaciones[5], mantenimiento de enlaces, así como rubros que se aplican en casos de eventualidades por reparación del servicio, se han considerado como Opex Recurrente.

El modelo *WACC (Weighted Average Cost of Capital)* se define con la siguiente fórmula:

$$r_{wacc} = \%E * [r_F + \beta * m + C] + \%D * I * (1 - T)$$

Donde:

%E y %D: Son el porcentaje en capital (*%Equity)* y en Deuda (*%Debt)* que constituyen la estructura de capital de una empresa.

r_F: Es la tasa libre de riesgo, que por definición corresponde a la tasa de los Bonos del Tesoro de los Estados Unidos. El valor de r_F actual es de 7.8%.

m: *Market Premium*, corresponde a la diferencia entre la rentabilidad de la cartera del mercado de la línea de negocios y la tasa sin riesgo.

β: Índice de la sensibilidad de la rentabilidad de un negocio particular con respecto a la rentabilidad de la cartera del mercado de esa línea de negocios.

C: Tasa de riesgo país, para el caso del Ecuador está estimado en 10%.

I: Interés al que se ha contratado la deuda.

T: Escudos fiscales.

Se considera que el proveedor de servicios invierte en el proyecto, para la infraestructura terrestre de telecomunicaciones en el Ecuador, con una estructura de capital de 70% en activos y 30% en deuda; si se asume que se consiguen préstamos en interés I al 15% y se tiene escudos fiscales T del 35%, la tasa de descuento será:

r_{wacc} = 70%*(0.078 + 1.15* 0.07 + 0.10) + 30%*0.15*(1-0.35)

r_{wacc}=18.095+ 2.925

r_{wacc}=21.02%

[5] Hoy se llama ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones)

Precios del proyecto				
Sedes	**Servicio**	**Capacidad**	**MRC**	**NRC**
Matriz Quito	Datos Principal y *backup* (FO) *dual home*	18 Mbps	$ 1.120	$ 600
	Internet (FO)	5 Mbps	$ 350	$ 300
Parque California	Datos Principal (FO)	8 Mbps	$ 243	$ 300
	Datos *Backup* (radio)	8 Mbps	$ 180	$ 500
	Internet	2 Mbps	$ 150	$ 100
Ag. Almagro	Datos (F.O)	512 Kbps	$ 70	$ 300
Ag. Cumbayá	Datos (radio)	2 Mbps	$ 180	$ 500
Ag. Sangolquí	Datos (radio)	2 Mbps	$ 180	$ 500
Ag. San Rafael	Datos (radio)	2 Mbps	$ 180	$ 500
Ag. Río Plaza	Datos (radio)	512 Kbps	$ 90	$ 500
Ag. Beaterio	Datos (radio)	512 Kbps	$ 90	$ 500
Ag. Ecuagiros Sur	Datos (F.O)	512 Kbps	$ 70	$ 300
Ag. Domingo Comín	Datos (F.O)	1024 Kbps	$ 130	$ 300
Costo Mensual			**$ 3.033**	**$ 5.200**

Tabla 3.15 Ingreso mensual del proyecto por sede

El flujo de caja (F) es un informe financiero que presenta un detalle de los flujos de ingresos y egresos de dinero que un proyecto en un periodo de tiempo determinado; éste se indica en la tabla 3.18.

Valor Actual (P): En los cálculos a partir del flujo de caja se ha obtenido el valor actual (P), que corresponde al valor de un flujo futuro de caja descontado con la tasa adecuada de interés en el mercado, donde n es el número de periodo.

$$P = \frac{F}{\left(1 + \frac{rwacc\%}{12}\right)^{n}}$$

$$P = \frac{7360,53}{\left(1 + \frac{21,02\%}{12}\right)^{1}} = 7233,8176 \qquad P = \frac{2160,53}{\left(1 + \frac{21,02\%}{12}\right)^{2}} = 2086,78$$

El valor del flujo acumulado: Corresponde a la suma del valor actual más el flujo acumulado del periodo anterior.

ITEM	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)	TIPO (CAPEX /OPEX EVENTUAL / OPEX RECURRENTE)	TIPO POR DISTRIBUCION
Sede Matriz Quito					
Router Cisco 2821 (Datos)	1	2300	**2300**	CAPEX	TERMINAL
Router Cisco 881 (Internet)	1	220	**220**	CAPEX	TERMINAL
Equipo de Video Polycom	1	6000	**6000**	CAPEX	TERMINAL
Cisco ME 3400	1	960	**960**	CAPEX	TERMINAL
Audicode Mediant 1000	1	2200	**2200**	CAPEX	TERMINAL
Puerto IP (Video)	2	16	**32**	OPEX RECURRENTE	TERMINAL
Puerto IP(Datos-Internet)	23	8	**184**	OPEX RECURRENTE	TERMINAL
Arrendamiento de ductos	1	20	**20**	OPEX RECURRENTE	TERMINAL
Instalación	1	500	**500**	OPEX EVENTUAL	TERMINAL
Odf	2	17	**34**	OPEX EVENTUAL	TERMINAL
Mantenimiento	1	41,66	**41,66**	OPEX RECURRENTE	TERMINAL
SUBTOTAL			**$ 12.491,66**		
Sede Sucursal Mayor Guayaquil					
Router Cisco 2821 (Datos)	1	2300	**2300**	CAPEX	TERMINAL
Router Cisco 881 (Internet)	1	220	**220**	CAPEX	TERMINAL
Equipo de Video Polycom	1	6000	**6000**	CAPEX	TERMINAL
Cisco ME 3400	1	960	**960**	CAPEX	TERMINAL
Audicode Mediant 1000	1	2200	**2200**	CAPEX	TERMINAL
Equipo radio Ceragon	2	486	**972**	CAPEX	TERMINAL
Puerto IP (Video)	2	16	**32**	OPEX RECURRENTE	TERMINAL
Puerto IP(Datos-Internet)	10	8	**80**	OPEX RECURRENTE	TERMINAL
Supertel	1	50	**50**	OPEX RECURRENTE	TERMINAL
Arrendamiento de ductos	1	10	**10**	OPEX RECURRENTE	TERMINAL
Odf	1	17	**17**	OPEX EVENTUAL	TERMINAL
Instalación	1	500	**500**	OPEX EVENTUAL	TERMINAL
Mantenimiento	1	41,66	**41,66**	OPEX RECURRENTE	TERMINAL
SUBTOTAL			**$ 13.382,66**		

Tabla 3.16 Costos del proyecto sede Matriz y Sucursal Mayor

ITEM	CANTIDAD	PRECIO UNITARIO (USD)	PRECIO TOTAL (USD)	TIPO (CAPEX /OPEX EVENTUAL / OPEX RECURRENTE)	TIPO POR DISTRIBUCION
Sucursal Almagro					
Conversores de Fibra	2	15	30	CAPEX	TERMINAL
Router Cisco 881 (Datos)	1	220	220	CAPEX	TERMINAL
Audiocode MP 118	1	310	310	CAPEX	TERMINAL
Puerto IP(Datos)	1	8	8	OPEX RECURRENTE	TERMINAL
Arrendamiento de ductos	1	10	10	OPEX RECURRENTE	TERMINAL
Instalación	1	130	130	OPEX EVENTUAL	TERMINAL
Odf	1	17	17	OPEX EVENTUAL	TERMINAL
Mantenimiento	1	10,83	10,83	OPEX RECURRENTE	TERMINAL
SUBTOTAL			**$ 735,83**		
Sede Cumbayá, Salgolquí y San Rafael					
Equipo radio Ceragon	6	486	2916	CAPEX	TERMINAL
Router Cisco 881 (Datos)	3	220	660	CAPEX	TERMINAL
Audiocode MP 118	3	310	930	CAPEX	TERMINAL
Puerto IP(Datos)	6	8	48	OPEX RECURRENTE	TERMINAL
Instalación	3	270	810	OPEX EVENTUAL	TERMINAL
Supertel	3	10	30	OPEX RECURRENTE	TERMINAL
Mantenimiento	3	22,5	67,5	OPEX RECURRENTE	TERMINAL
SUBTOTAL			**$ 5.461,50**		
Sede Río Plaza y Beaterio					
Equipo radio Airspam	2	450	900	CAPEX	TERMINAL
Router Cisco 881 (Datos)	2	220	440	CAPEX	TERMINAL
Audiocode MP 118	2	310	620	CAPEX	TERMINAL
Puerto IP(Datos)	1	8	8	OPEX RECURRENTE	TERMINAL
Instalación	2	109	218	OPEX EVENTUAL	TERMINAL
Supertel	2	15	30	OPEX RECURRENTE	TERMINAL
Mantenimiento	2	9,08	18,16	OPEX RECURRENTE	TERMINAL
SUBTOTAL			**$ 2.234,16**		
Sede Ecuagiros Sur y Domingo Comín					
Conversores de Fibra	4	15	60	CAPEX	TERMINAL
Router Cisco 881 (Datos)	2	220	440	CAPEX	TERMINAL
Audiocode MP 118	2	310	620	CAPEX	TERMINAL
Puerto IP(Datos-Internet)	2	8	16	OPEX RECURRENTE	TERMINAL
Instalación	2	130	260	OPEX EVENTUAL	TERMINAL
Odf	2	17	34	OPEX EVENTUAL	TERMINAL
Arrendamiento de ductos	2	5	10	OPEX RECURRENTE	TERMINAL
Mantenimiento	2	10,83	21,66	OPEX RECURRENTE	TERMINAL
SUBTOTAL			**$ 1.461,66**		

Tabla 3.17 Costos del proyecto por agencias

	RTWACC	21,02%												
	MES	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
	INSTALACIÓN		5200											
	PAGO DE SERVICIO		3033	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033
INGRESOS	Subtotal Ingresos	0	8233	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033
	CAPEX	-32478												
	OPEX EVENTUAL	-2520												
	OPEX RECURRENTE		-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5
EGRESOS	Subtotal Egresos	-34998	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5
SUBTOTAL MES		**-34998**	**7463,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**

	MES	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
	INSTALACIÓN												
	PAGO DE SERVICIO	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033
INGRESOS	Subtotal Ingresos	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033	3033
	CAPEX												
	OPEX EVENTUAL												
	OPEX RECURRENTE	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5
EGRESOS	Subtotal Egresos	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5	-769,5
SUBTOTAL MES		**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**	**2263,5**

Tabla 3.18 Flujo de caja subtotal por mes

En el proyecto se han calculado los siguientes parámetros:

Valor actual neto (VAN): "Calcula la ganancia o pérdida monetaria esperada de un proyecto, al descontar todas las entradas o salidas de efectivo futuras al momento presente, utilizando una tasa de descuento requerida." [49]

$$VAN = \sum P - \text{Inversión Inicial}$$

Payback: "Permite determinar el número de años y meses que le toma al proyecto en recuperar la inversión inicial" [50]

En el proyecto se recupera la inversión en un tiempo de 16 meses.

Máxima Exposición: "Es la capacidad financiera que le exige el proyecto al inversor, consistente en el volumen de fondos del que debe disponer el inversor para financiar el proyecto antes de comenzar a recuperar la inversión.

Se determina calculando las sumatorias acumuladas de flujos de fondos de cada período e identificando el monto negativo de mayor magnitud." [51]

Tasa interna de retorno (TIR): "Calcula la tasa de descuento, en la cual, el valor presente de los ingresos de efectivo esperados de un proyecto, es igual al valor presente de los egresos de efectivo esperados." [52]

Los resultados de los cálculos se indican en la tabla 3.19. La figura 3.38 muestra el desarrollo del proyecto a 2 años.

Se puede concluir que con una VAN de $14154 el proyecto es económicamente viable, considerando que la inversión se recupera en 16 meses.

Pero se debe considerar que existe una exposición máxima al inicio del proyecto de $34998.

RTWACC	21,02%												
MES	0	1	2	3	4	5	6	7	8	9	10	11	12
SUBTOTAL MES	-34998	7463,53	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5
SUBTOTAL MES (VALOR PRESENTE)	-34998	7335,04	2186,3	2148,6	2111,6	2075,3	2039,6	2004,5	1969,9	1936	1902,7	1869,9	1837,8
FLUJO ACUMULADO	-34998	-27662,96	-25477	-23328	-21216	-19141	-17102	-15097	-13127	-11191	-9288	-7418	-5581

RTWACC	21,02%											
MES	13	14	15	16	17	18	19	20	21	22	23	24
SUBTOTAL MES	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5	2263,5
SUBTOTAL MES (VALOR PRESENTE)	1806,1	1775	1744,5	1714,4	1684,9	1655,9	1627,4	1599,4	1571,9	1544,8	1518,2	1492,1
FLUJO ACUMULADO	-3775	-2000	-255,1	1459,3	3144,2	4800,2	6427,6	8027	9598,8	11144	12662	14154

VAN	$	14.154
PAYBACK		16
MÁXIMA EXPOSICIÓN	$	(34.998)
TIR		5%

Tabla 3.19 Cálculo de índices financieros.

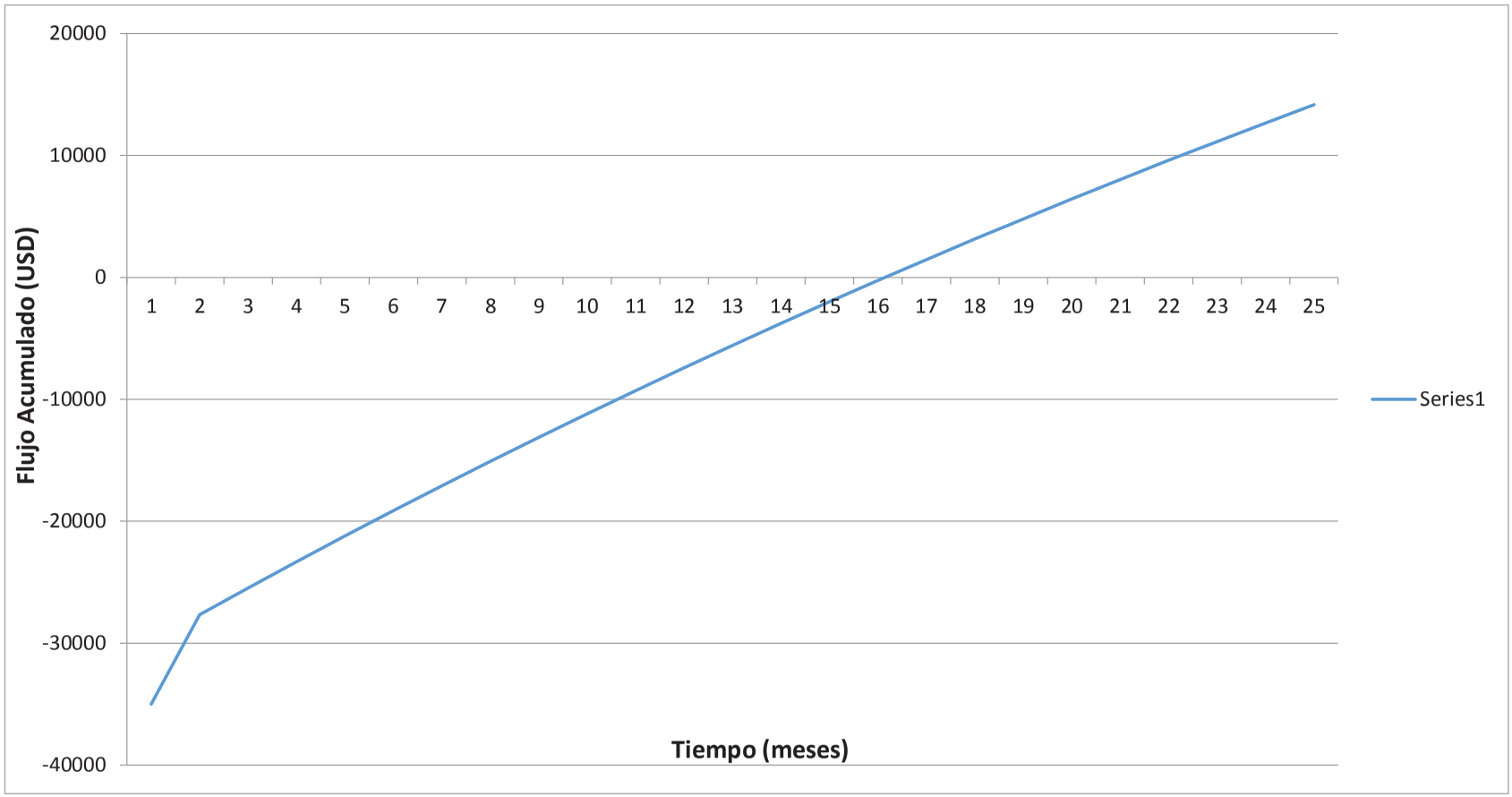


Figura 3.37 Desarrollo del proyecto

CAPÍTULO 4
MODELAMIENTO DE LA RED METROETHERNET

4.1 TOPOLOGÍA Y CONFIGURACIÓN

4.1.1 MODELAMIENTO METROETHERNET

En la práctica los nodos principales de una ciudad, que concentran la mayor cantidad de clientes, deben ser tomados en cuenta para la instalación de un *switch* que formará parte del anillo de agregación. La secuencia de conformación del diagrama Metroethernet es a base de la conexión física entre los puertos de los *switches*, independiente de la ubicación física de los nodos.

Para determinar la factibilidad de servicio para un cliente se debe analizar la disponibilidad de puertos del nodo más cercano.

Bajo estas consideraciones se ha diseñado un modelo ilustrativo de red Metroethernet con diferentes opciones de conexión. El diseño consta de un anillo de agregación principal y varios subanillos donde un protocolo de protección conmutará el tráfico ante un eventual inconveniente.

Los segmentos secundarios que recogen el tráfico procedente de varios clientes por medio de fibra óptica u otro sistema de acceso inalámbrico pueden interconectarse describiendo una topología de anillo a un mismo *switch* principal o a dos *switches* principales diferentes (conocido como *Dual Homing*). Incluso los anillos de acceso pueden estar compuestos por varios nodos "D" colocados en las instalaciones de clientes, la cual es una topología no recomendada. Como excepción a esta regla se puede desarrollar un subanillo entre el anillo principal y las instalaciones de un solo cliente.

Para el presente modelamiento se ha considerado el protocolo de protección REP, con *switches Cisco* ME3400.

Se ha configurado un anillo de agregación principal con el REP 60, y 6 segmentos en subanillo desde el REP 61 al REP 66. Un gráfico general se indica en la figura 4.1.

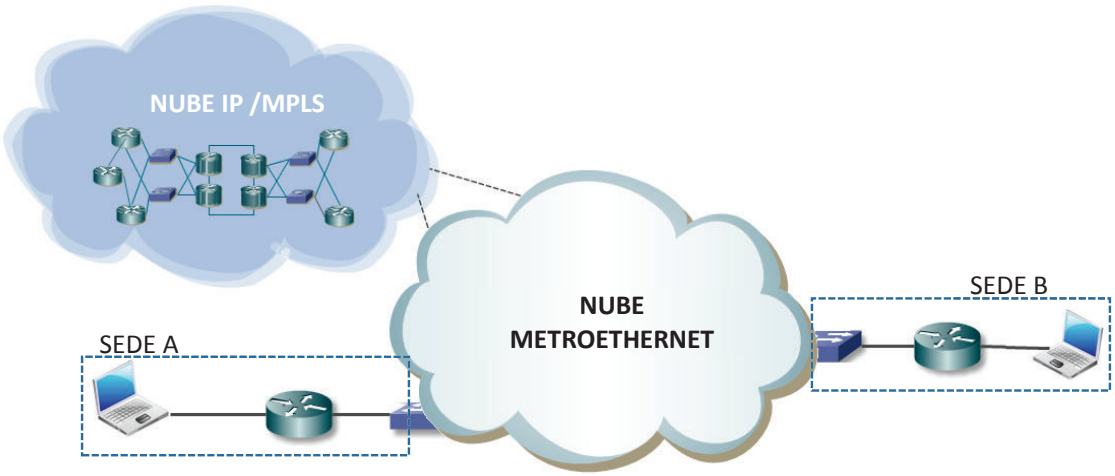


Figura 4.1 Diagrama general Metroethernet- Usuario Final

4.1.1.1 Definición de VLANs

Se ha definido la S-VLAN 49 para la administración de los equipos, mientras que la S-VLAN 8 encapsula los paquetes para enlaces principales y la S-VLAN 7 para enlaces de respaldo.

Los equipos realizarán los reportes de eventos cada 30 segundos, además de las notificaciones de control de tormentas de tráfico *broadcast* y *multicast*.

Además se incluye la configuración de calidad de servicio a aplicarse en cada uno de los puertos Gigabit Ethernet.

Se ha colocado una C-VLAN 1053 que es la VLAN de cliente a encapsularse en la S-VLAN 8. Para luego desencapsularse y entregar a la nube IP/MPLS.

En la figura 4.2 se indica el modelamiento de una red Metroethernet a detalle y en la figura 4.3 se ilustran los equipos utilizados.

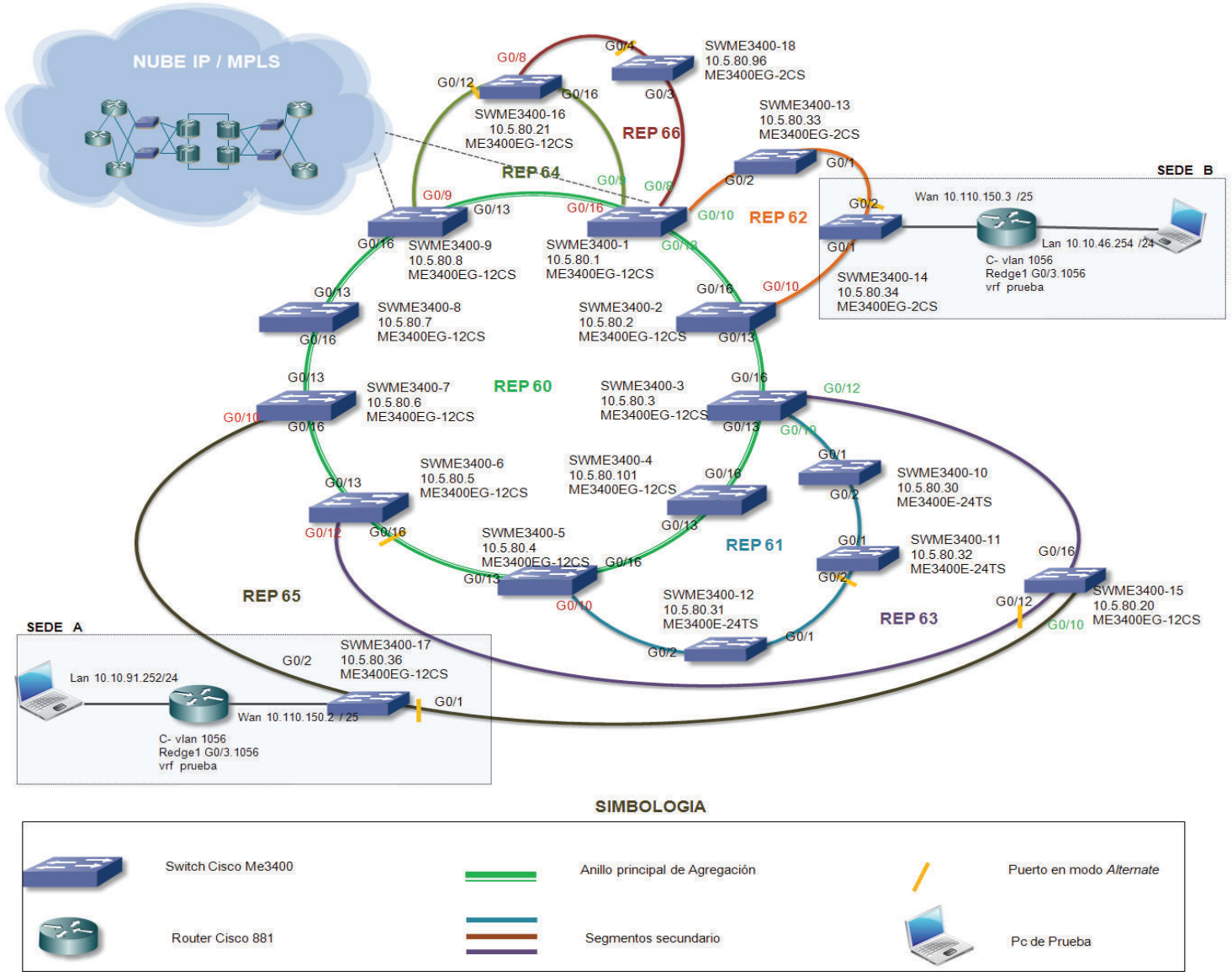


Figura 4.2 Topología del Modelamiento de la red Metroethernet

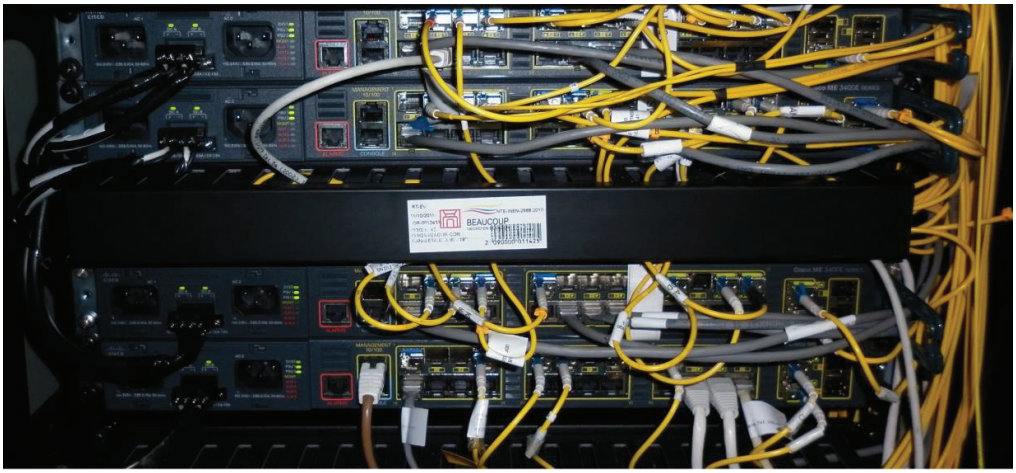


Figura 4.2 Equipos *Cisco* ME 3400

4.1.1.2 Preparación del *Switch* ME·3400

Para preparar el equipo *switch* ME3400 se debe instalar un IOS determinado que permitirá que se habilite correctamente las características de conmutación del protocolo REP. Además se configura el SDM (*Switch Database Management*) para ampliar la capacidad de aprendizaje MAC predeterminado de 5K a 8K y por último se verifica el estado correcto del equipo. Los pasos indicados se detallan a continuación:

Cargar IOS en el equipo

```
Switch#copy tftp: flash:
me340x-metroipaccessk9-mz.122-55.SE.bin
```

Finalizada la carga se realiza la verificación del archivo cargado.

```
Switch#show flash
Directory of flash:/
   7  -rwx         556   Mar 1 1993 00:00:59 +00:00  vlan.dat
   8  -rwx          24   Mar 1 1993 00:05:50 +00:00  private-config.text
   9  -rwx    12619566   Mar 1 1993 00:06:43 +00:00  me340x-metroipaccessk9-
mz.122-55.SE.bin
  10  -rwx        1048   Mar 1 1993 00:05:57 +00:00  multiple-fs
   2  drwx         512   Mar 1 1993 00:11:02 +00:00  me340x-metroaccessk9-mz.122-
50.SE1
  11  -rwx         926   Mar 1 1993 00:05:50 +00:00  config.text

25933824 bytes total (4665344 bytes free)
```

```
Switch#verify /md5 flash:me340x-metroipaccessk9-mz.122-55.SE.bin
Done!
verify /md5 (flash:me340x-metroipaccessk9-mz.122-55.SE.bin) =
116ed60720c5372bdef5b35cda86c50f
```

Se verifica el IOS a ser cargado en el próximo *reload*.

```
Switch#show boot system
flash:me340x-metroaccessk9-mz.122-50.SE1/me340x-metroaccessk9-mz.122-
50.SE1.bin
```

Se cambia el *boot*.

```
Switch(config)#boot system flash:me340x-metroipaccessk9-mz.122-55.SE.bin
```

Se verifica el SDM.

```
Switch#show sdm prefer
The current template is "default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  5K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    9K
  number of directly-connected IPv4 hosts:          5K
  number of indirect IPv4 routes:                   4K
  number of IPv4 policy based routing aces:         0.5K
  number of IPv4/MAC qos aces:                      0.5K
  number of IPv4/MAC security aces:                 1K
```

Se verificar MTUs.

```
Switch#show system mtu

System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
Routing MTU size is 1500 bytes
```

Se cambia SDM y MTUs.

```
Switch(config)#sdm prefer layer-2
Changes to the running SDM preferences have been stored, but cannot take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently active.

Switch(config)#system mtu jumbo 9000
Changes to the system jumbo MTU will not take effect until the next reload is done
```

```
Switch(config)#system mtu 1998
Changes to the system MTU will not take effect until the next reload is done
```

Se guarda configuración y se reinicia.

```
Switch(config)#exit
Switch#wr
Switch#reload
```

Luego de cargar el IOS comprueba que los cambios se han efectuado.

```
Switch#show sdm prefer
 The current template is "layer-2" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:              8K
  number of IPv4 IGMP groups:                   1K
  number of IPv4 multicast routes:              0
  number of IPv4 unicast routes:                0
  number of IPv4 policy based routing aces:     0
  number of IPv4/MAC qos aces:                  0.5K
  number of IPv4/MAC security aces:             1K
```

```
Switch#show system mtu

System MTU size is 1998 bytes
System Jumbo MTU size is 9000 bytes
System Alternate MTU size is 1998 bytes
Routing MTU size is 1500 bytes
```

4.1.1.3 Parámetros de QoS

Se aplican parámetros de Qos en las interfaces de los equipos *Cisco* ME3400, dependiendo si se trata de una interfaz de agregado donde se utilizarán las políticas:

```
service-policy input GX-Ingress-GE
service-policy output GX-Egress-GE
```

Si se trata de una interfaz hacia un *switch* de cliente se aplicarán las siguientes políticas.

```
service-policy input GX-Ingress-FE
service-policy output GX-Egress-FE
```

La diferencia radica en el AB máximo que se asocia al puerto; por seguridad se configura un límite de 100 Mbps en *switches* de clientes.

A continuación se indica un ejemplo de configuración:

Definición de *Class-maps*

```
class-map match-any dot1p-EF
 match cos  4  5  6  7
class-map match-any dot1p-AF
 match cos  2  3
class-map match-any dot1p-BE
 match cos  0  1
class-map match-any QoS-Group-EF
 match qos-group 3
class-map match-any GX-EF
 match cos  4  5  6  7
class-map match-any QoS-Group-AF
 match qos-group 2
class-map match-any QoS-Group-BE
 match qos-group 1
class-map match-any GX-AF
 match cos  2  3
class-map match-any GX-BE
 match cos  0  1
```

Política anidada de salida Fast Ethernet.

```
policy-map GX-Egress-FE_child
 class GX-EF
   police cir 75000000
   priority
 class GX-AF
   bandwidth percent 23
   queue-limit 544
 class GX-BE
   bandwidth percent 1
   queue-limit 544
 class class-default
   bandwidth percent 1
   queue-limit 544
```

Política anidada de salida Gigabit Ethernet.

```
policy-map GX-Egress-GE_child
 class GX-EF
   police cir 750000000
   priority
 class GX-AF
   bandwidth percent 23
   queue-limit 544
 class GX-BE
   bandwidth percent 1
   queue-limit 544
 class class-default
   bandwidth percent 1
   queue-limit 544
```

Política para tráfico de entrada en puertos Gigabit Ethernet limitado a 1000 Mbps.

```
policy-map GX-Egress-GE
 class class-default
   shape average 1024000000
  service-policy GX-Egress-GE_child
```

Política para tráfico de salida en puertos Fast Ethernet limitado a 100 Mbps.

```
policy-map GX-Egress-FE
 class class-default
   shape average 102400000
  service-policy GX-Egress-FE_child
```

Política para tráfico de entrada en puertos Fastethernet limitado a 100 Mbps.

```
policy-map GX-Ingress-FE
 class dot1p-EF
   police cir 102400000
     conform-action set-qos-transmit 3
 class dot1p-AF
   police cir 100000000
     conform-action set-qos-transmit 2
 class dot1p-BE
   police cir 100000000
     conform-action set-qos-transmit 1
```

Política para tráfico de entrada en puertos Gigabit Ethernet limitado a 1000 Mbps.

```
policy-map GX-Ingress-GE
 class dot1p-EF
   police cir 1024000000
     conform-action set-qos-transmit 3
 class dot1p-AF
   police cir 1000000000
     conform-action set-qos-transmit 2
 class dot1p-BE
   police cir 1000000000
     conform-action set-qos-transmit 1
```

4.1.1.4 Configuración de los anillos

Configuración Anillo Principal REP 60

Las S-VLANs que se propagarán y se configuran para el anillo principal son:

La S-VLAN 7 encapsula las C-VLAN de enlaces de respaldo.
La S-VLAN 8 encapsula las C-VLAN de enlaces principales.
La S-VLAN 49 para el monitoreo y gestión de todos los *switches Cisco ME3400.*

La S-VLAN 60 se configura para el segmento REP.

```
vlan 7          name METRO_GYE_BKP
vlan 8          name METRO_GYE
```

```
vlan 49          name MGMT:METRO_GYE
vlan 60          name ADMIN_REP_60
```

Los siguientes parámetros se configuran de manera general en todos los equipos del segmento REP 60.

Configuración del puerto tipo NNI *(Network-Network Interface).*

```
port-type nni
```

Configuración de la VLAN nativa 60.

```
switchport trunk native vlan 60
```

Configuración de las VLANs permitidas.

```
switchport trunk allowed vlan 7-10,49,60
```

Configuración de la interfaz tipo trunk.

```
switchport mode trunk
```

Descripción del AB de la interfaz

```
bandwidth 1000000
```

Se genera la notificación de snmp/syslog cada 30 segundos.

```
load-interval 30
```

El puerto detecta si la transmisión o recepción se afecta para bajar el puerto.

```
udld port aggressive
```

Se configura un tiempo de 45 segundos que el segmento afectado debe estar activo para retornar a la topología original.

```
rep preempt delay 45
```

Se configura para que la notificación del control de tráfico *broadcast* se origine cuando esté al 1% de la capacidad del canal y cuando esté al 10% de tráfico *multicast*.

```
storm-control broadcast level 1.00
storm-control multicast level 10.00
storm-control action trap
```

Se aplica los parámetros de Qos en la interfaz.

```
service-policy input GX-Ingress-GE
service-policy output GX-Egress-GE
```

Switch Cisco **SWME3400-1 10.5.80.1 ME3400EG-12CS**

Se configura el inicio del segmento REP y se define el ID del puerto que va a estar en estado de bloqueo (*Alternate*), bloqueando todas las VLANs.

```
interface GigabitEthernet0/13
description TRUNK:SWME3400-2:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60 edge primary
rep block port id 00108CB64F742300 vlan 1-4094
```

Se configura el final del segment REP

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-9:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60 edge
```

Se asigna la dirección IP de monitoreo del *switch*

```
interface Vlan49
ip address 10.5.80.1 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Switch Cisco **SWME3400-2 10.5.80.2 ME3400EG-12CS**

Se configuran las interfaces de paso, del segmento REP.

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-1:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60

interface GigabitEthernet0/13
description TRUNK:SWME3400-3:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60
```

Se asigna la dirección IP de monitoreo del *switch*

```
interface Vlan49
ip address 10.5.80.2 255.255.255.0
ip default-gateway 10.5.80.254
```

Switch Cisco **SWME3400-3 10.5.80.3 ME3400EG-12CS**

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-2:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60

interface GigabitEthernet0/13
description TRUNK:SWME3400-5:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60

interface Vlan49
ip address 10.5.80.3 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Switch Cisco **SWME3400-4 10.5.80.101 ME3400EG-12CS**

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-3:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60

interface GigabitEthernet0/13
description TRUNK:SWME3400-5:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60

interface Vlan49
ip address 10.5.80.101 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Switch Cisco **SWME3400-5 10.5.80.4 ME3400EG-12CS**

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-3:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60

interface GigabitEthernet0/13
description TRUNK:SWME3400-6:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60

interface Vlan49
ip address 10.5.80.4 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Switch Cisco **SWME3400-6 10.5.80.5 ME3400EG-12CS**

Se configura el puerto preferido, que será el que permanece bloqueado hasta que se presente un evento.

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-5:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60 preferred
```

Se configura el puerto de paso del segmento REP.

```
interface GigabitEthernet0/13
description TRUNK:SWME3400-7:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60

interface Vlan49
ip address 10.5.80.5 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Con el siguiente comando se obtiene el PortID que se configura en la interfaz de inicio del segmento REP.

```
SWME3400-6#sh int g0/16 rep detail
GigabitEthernet0/16   REP enabled
Segment-id: 60 (Preferred)
PortID: 00108CB64F742300
Preferred flag: Yes
Operational Link Status: TWO_WAY
Current Key: 000D8CB64F7406801F5C
Port Role: Alternate
Blocked VLAN: 1-4094
Admin-vlan: 60
Preempt Delay Timer: 45 sec
```

Switch Cisco **SWME3400-7 10.5.80.6 ME3400EG-12CS**

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-6:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60

interface GigabitEthernet0/13
description TRUNK:SWME3400-8:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60

interface Vlan49
ip address 10.5.80.6 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Switch Cisco **SWME3400-8 10.5.80.7 ME3400EG-12CS**

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-7:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60

interface GigabitEthernet0/13
description TRUNK:SWME3400-9:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60

interface Vlan49
ip address 10.5.80.7 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Switch Cisco **SWME3400-9 10.5.80.8 ME3400EG-12CS**

```
interface GigabitEthernet0/13
description TRUNK:SWME3400-1:GE0/16-GE [ANILLO PRINCIPAL]
rep segment 60

interface GigabitEthernet0/16
description TRUNK:SWME3400-8:GE0/13-GE [ANILLO PRINCIPAL]
rep segment 60

interface Vlan49
ip address 10.5.80.8 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Se verifica que el anillo esté configurado correctamente.

El puerto primario (Pri) inicia el segmento REP y el puerto secundario (Sec) es el final del segmento REP; mientras que el puerto preferido (*Alternate*) se encuentra bloqueado en condiciones normales.

```
SWME3400-1#sh rep topology segment 60
REP Segment 60
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-1  Gi0/13     Pri  Open
SWME3400-2   Gi0/16        Open
SWME3400-2   Gi0/13        Open
SWME3400-3   Gi0/16        Open
SWME3400-3   Gi0/13        Open
SWME3400-4   Gi0/16        Open
SWME3400-4   Gi0/13        Open
SWME3400-5   Gi0/16        Open
```

```
SWME3400-5   Gi0/13        Open
SWME3400-6   Gi0/16        Alt
SWME3400-6   Gi0/13        Open
SWME3400-7   Gi0/16        Open
SWME3400-7   Gi0/13        Open
SWME3400-8   Gi0/16        Open
SWME3400-8   Gi0/13        Open
SWME3400-9   Gi0/16        Open
SWME3400-9   Gi0/13        Open
SWME3400-1   Gi0/16     Sec  Open
```

Se verifica en detalle la topología del anillo, donde se identifica el puerto primario, secundario e intermedios.

```
SWME3400-1#sh rep topology detail
REP Segment 60
SWME3400-1, Gi0/13 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f74.0680
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 1 / [-18]

SWME3400-2, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: c062.6b87.7b80
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-17]

SWME3400-2, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: c062.6b87.7b80
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 3 / [-16]

SWME3400-3, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4a80
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 4 / [-15]

SWME3400-3, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4a80
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 5 / [-14]

SWME3400-4, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: a418.75f8.3500
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 6 / [-13]

SWME3400-4, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: a418.75f8.3500
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 7 / [-12]

SWME3400-5, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4d00
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 8 / [-11]

SWME3400-5, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4d00
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 9 / [-10]

SWME3400-6, Gi0/16 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 8cb6.4f74.2300
  Port Number: 010
  Port Priority: 050
  Neighbor Number: 10 / [-9]

SWME3400-6, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f74.2300
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 11 / [-8]

SWME3400-7, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.5780
```

```
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 12 / [-7]

SWME3400-7, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.5780
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 13 / [-6]


SWME3400-8, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: c062.6b86.0580
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 14 / [-5]

SWME3400-8, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: c062.6b86.0580
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 15 / [-4]

SWME3400-9, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.1f80
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 16 / [-3]

SWME3400-9, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.1f80
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: 17 / [-2]

SWME3400-1, Gi0/16 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f74.0680
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 18 / [-1]
```

Configuración segmento REP 61

La S-VLAN 61 se configura para el segmento REP.

```
vlan 7          name BBONE:GYE:BKP
vlan 8          name BBONE:GYE
vlan 49         name MGMT:METRO_GYE
vlan 61         name ADMIN_REP_61
```

Los siguientes parámetros se configuran en las interfaces correspondientes al segmento REP 61.

```
port-type nni
switchport trunk native vlan 61
switchport trunk allowed vlan 7,8,49,61
switchport mode trunk
bandwidth 100000
load-interval 30
udld port aggressive
rep preempt delay 45
storm-control broadcast level 1.00
storm-control multicast level 10.00
storm-control action trap
service-policy input GX-Ingress-GE
service-policy output GX-Egress-GE
```

Switch Cisco **SWME3400-3 10.5.80.3 ME3400EG-12CS**

Se configura el puerto de inicio del segmento REP.

Además se configura la notificación de cambio de topología al anillo principal REP60 (STCN *Segment Topology Change Notification*).

Se configura el ID del puerto preferido a ser bloqueado en el segmento.

```
interface GigabitEthernet0/10
description TRUNK:SWME3400-10:GE0/2
rep segment 61 edge primary
rep stcn segment 60
rep block port id 00021C17D3D6B400 vlan 1-4094
```

Switch Cisco **SWME3400-10 10.5.80.30 ME3400E-24TS**

```
interface GigabitEthernet0/1
description TRUNK:SWME3400-3:GE0/10
rep segment 61

interface GigabitEthernet0/2
description TRUNK:SWME3400-11:G0/1
rep segment 61

interface Vlan49
ip address 10.5.80.30 255.255.255.0
!
ip default-gateway 10.5.80.254
```

Switch Cisco **SWME3400-11 10.5.80.32 ME3400E-24TS**

```
interface GigabitEthernet0/1
description TRUNK:SWME3400-10:GE0/2
rep segment 61

interface GigabitEthernet0/2
description TRUNK:SWME3400-12:GE0/1
rep segment 61 preferred

interface Vlan49
ip address 10.5.80.32 255.255.255.0
!
ip default-gateway 10.5.80.254

SWME3400-11#sh int g0/2 rep detail
GigabitEthernet0/2   REP enabled
Segment-id: 61 (Preferred)
PortID: 00021C17D3D6B400
```

Preferred flag: Yes
Operational Link Status: TWO_WAY
Current Key: 00011C17D3D6B4001366
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 61
Preempt Delay Timer: 45 sec
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none

Switch Cisco **SWME3400-12 10.5.80.31 ME3400E-24TS**

interface GigabitEthernet0/1
description TRUNK:SWME3400-11:GE0/1
rep segment 61
!
interface GigabitEthernet0/2
description TRUNK:SWME3400-5:GE0/10
rep segment 61

interface Vlan49
ip address 10.5.80.31 255.255.255.0
!
ip default-gateway 10.5.80.254

Switch Cisco **SWME3400-5 10.5.80.4 ME3400EG-12CS**

interface GigabitEthernet0/10
description TRUNK:SWME3400-12:GE0/1
rep segment 61 edge
rep stcn segment 60

Se verifica que el segmento REP 61 esté configurado correctamente.

SWME3400-3#sh rep topology segment 61
REP Segment 61
BridgeName PortName Edge Role
---------- ---------- ---- ----
SWME3400-3 Gi0/10 Pri Open
SWME3400-10 Gi0/1 Open
SWME3400-10 Gi0/2 Open
SWME3400-11 Gi0/1 Open
SWME3400-11 Gi0/2 Alt
SWME3400-12 Gi0/1 Open
SWME3400-12 Gi0/2 Open
SWME3400-5 Gi0/10 Sec Open

Los demás segmentos se configuran de manera similar tomando en cuenta el puerto que va a ser *edge primary y edge* (los extemos del segmento REP), además de configurar el respectivo puerto *alternate* y habilitar en cada segemento la S-VLAN correspondiente. El detalle de configuración de los demás segmentos se detalla en el Anexo N.

4.2 PRUEBAS Y RESULTADOS

Para verificar el comportamiento y robustez del protocolo REP y de la red se ha simulado el corte en varios segmentos del modelo y la caída total de un equipo.

4.2.1 CAÍDA DE UN SEGMENTO DEL ANILLO PRINCIPAL

Se realizó la simulación de la caída física de un segmento del anillo principal entre el *switch* SWME3400-2 G0/13 y el SWME3400-3 G0/16; se analizó el protocolo de protección REP que conmuta el tráfico protegiendo la integridad de la comunicación. La simulación se observa en la figura 4.4.

Caída del segmento SWME3400-2 G0/13 y el SWME3400-3 G0/16

Desde el switch SWME3400-1 se observa alarma de falla en el equipo SWME3400-2 puerto G0/13, en tanto que con el comando de detalle de puerto se indica la causa de la falla. (*Failed Port, Reason: Physical link down*).

```
SWME3400-1# sh rep topology segment 60
REP Segment 60
Warning: REP detects a segment failure, topology may be incomplete

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-1 Gi0/13     Sec  Open
SWME3400-2   Gi0/16        Open
SWME3400-2   Gi0/13        Fail
```

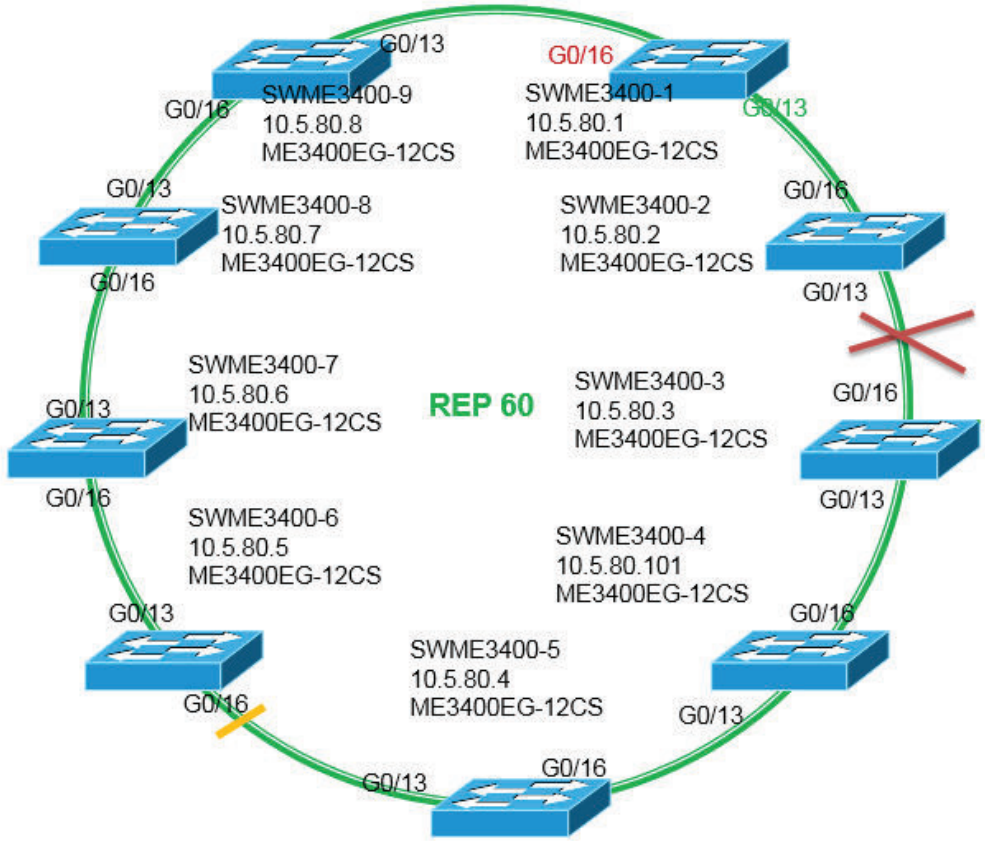


Figura 4.3 Simulación de la caída de un segmento en el anillo principal.

```
SWME3400-1# sh rep topology detail
REP Segment 60
Warning: REP detects a segment failure, topology may be incomplete
SWME3400-1, Gi0/13 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f74.0680
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-2, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: c062.6b87.7b80
  Port Number: 010
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-2, Gi0/13 (Intermediate)
  Failed Port, Reason: Physical link down
  Bridge MAC: c062.6b87.7b80
  Port Number: 00D
  Port Priority: 800
  Neighbor Number: Not available
```

Desde el *switch* SWME3400-6 se observa la falla en el segundo puerto del segmento y el puerto G0/16 configurado en *alternate* en estado *Open.* De esta manera se observa la protección de la integridad del segmento.

```
SWME3400-6#sh rep topology segment 60
REP Segment 60
Warning: REP detects a segment failure, topology may be incomplete

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-3   Gi0/16         Fail
SWME3400-3   Gi0/13         Open
SWME3400-4 Gi0/16          Open
SWME3400-4 Gi0/13          Open
SWME3400-5   Gi0/16         Open
SWME3400-5   Gi0/13         Open
SWME3400-6   Gi0/16         Open
SWME3400-6   Gi0/13         Open
SWME3400-7   Gi0/16         Open
SWME3400-7   Gi0/13         Open
SWME3400-8   Gi0/16         Open
SWME3400-8   Gi0/13         Open
SWME3400-9 Gi0/16          Open
SWME3400-9 Gi0/13          Open
SWME3400-1 Gi0/16     Sec  Open


SWME3400-6#sh rep topology detail
REP Segment 60
Warning: REP detects a segment failure, topology may be incomplete

SWME3400-3, Gi0/16 (Intermediate)
  Failed Port, Reason: Physical link down
  Bridge MAC: 8cb6.4f3a.4a80
  Port Number: 010
  Port Priority: 800
  Neighbor Number: Not available

SWME3400-3, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4a80
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-4, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
```

```
  Bridge MAC: a418.75f8.3500
  Port Number: 010
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-4, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: a418.75f8.3500
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-5, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4d00
  Port Number: 010
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-5, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4d00
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-6, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f74.2300
  Port Number: 010
  Port Priority: 050
  Neighbor Number: Not available

SWME3400-6, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f74.2300
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-7, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.5780
  Port Number: 010
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-7, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
```

```
  Bridge MAC: 8cb6.4f3a.5780
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-8, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: c062.6b86.0580
  Port Number: 010
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-8, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: c062.6b86.0580
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-9, Gi0/16 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.1f80
  Port Number: 010
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-9, Gi0/13 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.1f80
  Port Number: 00D
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-1, Gi0/16 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f74.0680
  Port Number: 010
  Port Priority: 000
  Neighbor Number: Not available
```

Durante las pruebas se realizaron pruebas de ping continuas hacia los *switches*, para comprobar que el protocolo de protección REP conmuta los paquetes en un tiempo menor a 1 segundo, tal como lo define la teoría, ya que no se evidenció corte en el servicio.

Estas pruebas se indican en la figura 4.5.

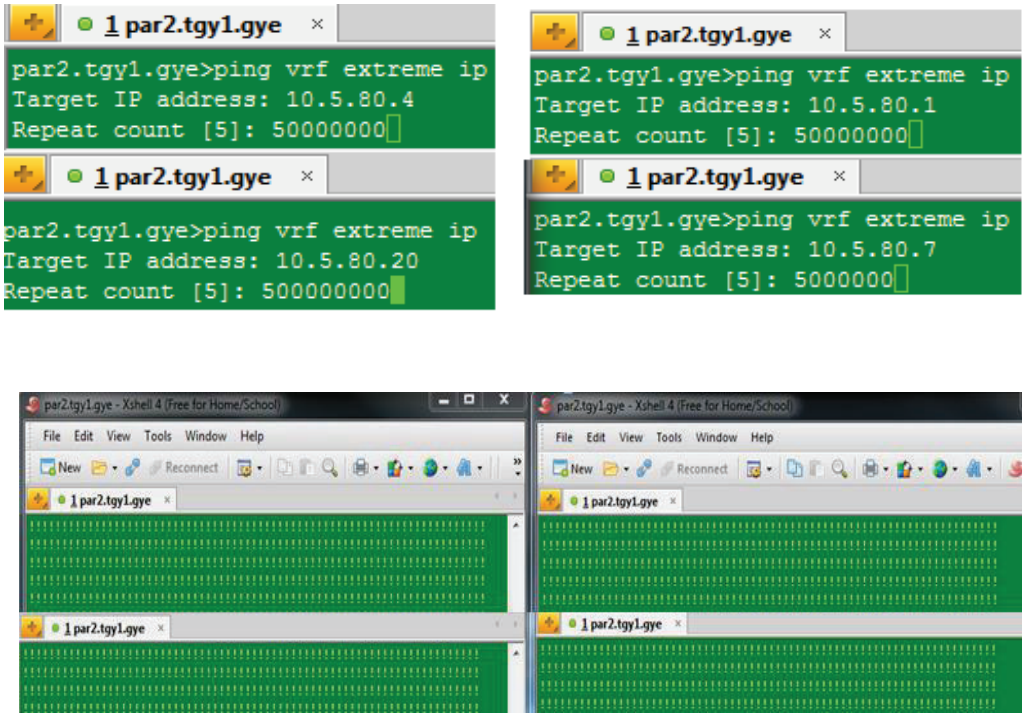


Figura 4.4 Pruebas de respuesta de los *switches* del anillo principal

4.2.2 CAÍDA DE UN *SWITCH*

También se desconectó un *switch*, para simular una falla de hardware y determinar el estado de los segmentos por medio del protocolo REP, tal como se indica en la figura 4.6.

Apagado del equipo SWME3400-15

Con el commando ***sh rep topology archive*** se despliega el estado histórico de un segmento.

```
SWME3400-3#sh rep topology archive
REP Segment 63
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-3   Gi0/12     Pri  Open
SWME3400-15   Gi0/16         Open
SWME3400-15   Gi0/12         Alt
SWME3400-6   Gi0/12     Sec  Open
```

Al apagar el *switch* se simula la falla del equipo y se observa el segmento desde el *switch* ME 3400-3 de la siguiente forma:

```
SWME3400-3#sh rep topology segment 63
REP Segment 63
Warning: REP detects a segment failure, topology may be incomplete

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-3   Gi0/12     Sec  Fail

SWME3400-3#sh rep topology detail
REP Segment 63
Warning: REP detects a segment failure, topology may be incomplete

SWME3400-3, Gi0/12 (Secondary Edge)
  Failed Port, Reason: Physical link down
  Bridge MAC: 8cb6.4f3a.4a80
  Port Number: 00C
  Port Priority: 800
  Neighbor Number: Not available
```

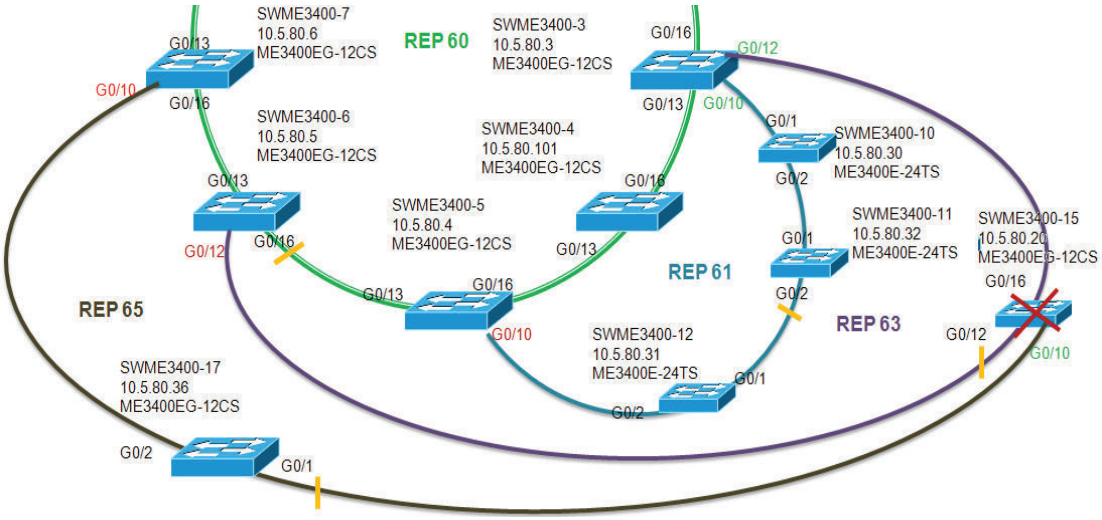


Figura 4.5 Simulación de caída de un *switch* Cisco ME3400

```
SWME3400-6#sh rep topology segment 63
REP Segment 63
Warning: REP detects a segment failure, topology may be incomplete
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-6   Gi0/12     Sec  Fail
```

```
SWME3400-6#sh rep topology detail
REP Segment 63
Warning: REP detects a segment failure, topology may be incomplete

SWME3400-6, Gi0/12 (Secondary Edge)
  Failed Port, Reason: Physical link down
  Bridge MAC: 8cb6.4f74.2300
  Port Number: 00C
  Port Priority: 800
  Neighbor Number: Not available

SWME3400-17#sh rep topology segment 65
REP Segment 65
Warning: REP detects a segment failure, topology may be incomplete

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-17- Gi0/1          Fail
SWME3400-17- Gi0/2          Open
SWME3400-7   Gi0/10     Sec  Open


SWME3400-17#sh rep topology detail
REP Segment 65
Warning: REP detects a segment failure, topology may be incomplete

SWME3400-17, Gi0/1 (Intermediate)
  Failed Port, Reason: Physical link down
  Bridge MAC: 6c9c.edc1.7480
  Port Number: 001
  Port Priority: 850
  Neighbor Number: Not available
SWME3400-17, Gi0/2 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 6c9c.edc1.7480
  Port Number: 002
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-7, Gi0/10 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.5780
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: Not available

SWME3400-7#sh rep topology segment 65
REP Segment 65
Warning: REP detects a segment failure, topology may be incomplete
```

```
BridgeName      PortName   Edge Role
--------------- ---------- ---- ----
SWME3400-7   Gi0/10     Sec  Open
SWME3400-17- Gi0/2          Open
SWME3400-17- Gi0/1          Fail
```

Al levantar el equipo *switch* apagado, se verifica que se restablezcan los segmentos REP.

SWME3400-15#sh ver

```
Cisco IOS Software, ME340x Software (ME340x-METROIPACCESSK9-M),
Version 12.2(55)SE, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Sun 08-Aug-10 00:21 by prod_rel_team
Image text-base: 0x01000000, data-base: 0x02F00000

ROM: Bootstrap program is ME340x boot loader
BOOTLDR: ME340x Boot Loader (ME340x-HBOOT-M) Version 12.2(44r)EY,
RELEASE SOFTWARE (fc1)

SWME3400-15 uptime is 8 minutes
System returned to ROM by power-on
System restarted at 12:27:17 UTC Mon Apr 14 2014
System image file is "flash:me340x-metroipaccessk9-mz.122-55.SE.bin"
```

SWME3400-15#sh rep topology segment 63

```
REP Segment 63
BridgeName      PortName   Edge Role
--------------- ---------- ---- ----
SWME3400-3   Gi0/12     Pri  Open
SWME3400-15   Gi0/16         Open
SWME3400-15   Gi0/12         Alt
SWME3400-6   Gi0/12     Sec  Open
```

En la práctica se sugiere implementar en el cliente soluciones alternativas con otra tecnología u otro proveedor, ya que la caída de un *switch* es un riesgo para los servicios y enlaces que lleguen al equipo.

4.2.3 CAÍDA DE UN SEGMENTO EN EL ANILLO SECUNDARIO

Se realizó la simulación de una falla en un segmento secundario del modelamiento Metroethernet en el segmento entre los *switches* SWME3400-10 y SWME3400-11, tal como se indica en la figura 4.7.

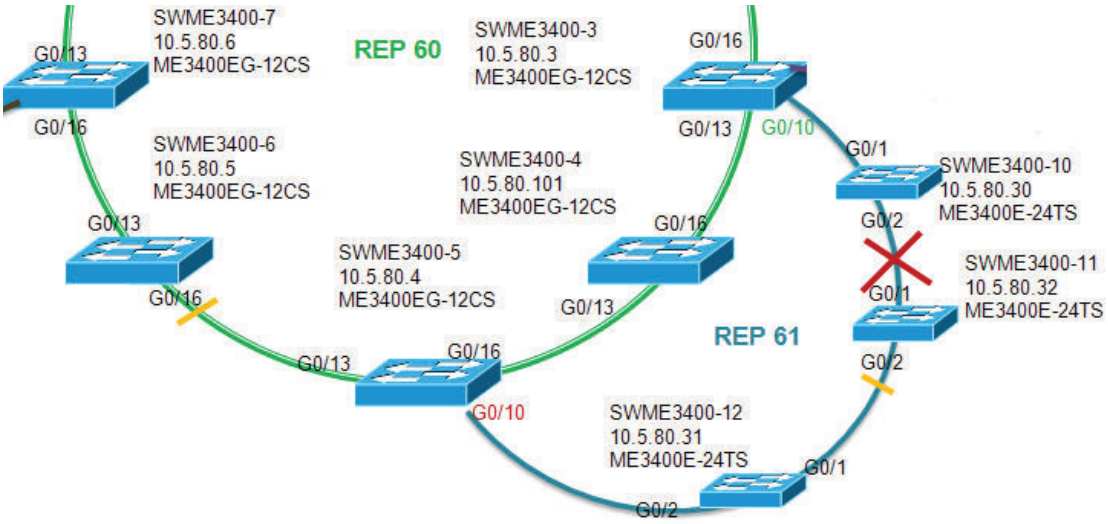


Figura 4.6 Simulación de la caída de un segmento secundario

Se monitorean los cambios de topología y el protocolo REP detecta la falla en el segmento alertando que la topología se encuentra incompleta.

Desde el *switch* ME3400-3 se puede verificar lo siguiente:

```
SWME3400-3#sh rep topology segment 61
REP Segment 61
Warning: REP detects a segment failure, topology may be incomplete

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-3       Gi0/10     Sec  Open
SWME3400-10      Gi0/1           Open
SWME3400-10      Gi0/2           Fail

SWME3400-3#sh rep topology detail
REP Segment 61
Warning: REP detects a segment failure, topology may be incomplete
```

```
SWME3400-3, Gi0/10 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4a80
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-10, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 1c17.d306.7b00
  Port Number: 001
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-10, Gi0/2 (Intermediate)
  Failed Port, (No Ext Neighbor) Reason: No REP neighbor
  Bridge MAC: 1c17.d306.7b00
  Port Number: 002
  Port Priority: 400
  Neighbor Number: Not available
```

Desde el segundo *switch* principal ME3400-5 se observan el puerto G0/1 del *switch* ME3400-11 con falla.

```
SWME3400-5#sh rep topology segm 61
REP Segment 61
Warning: REP detects a segment failure, topology may be incomplete

BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-5   Gi0/10     Sec  Open
SWME3400-12  Gi0/2          Open
SWME3400-12  Gi0/1          Open
SWME3400-11  Gi0/2          Open
SWME3400-11  Gi0/1          Fail

SWME3400-5#sh rep topology detail
REP Segment 61
Warning: REP detects a segment failure, topology may be incomplete

SWME3400-5, Gi0/10 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 8cb6.4f3a.4d00
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-12, Gi0/2 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 1c17.d30b.5f00
  Port Number: 002
```

```
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-12, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 1c17.d30b.5f00
  Port Number: 001
  Port Priority: 000
  Neighbor Number: Not available
SWME3400-11, Gi0/2 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 1c17.d3d6.b400
  Port Number: 002
  Port Priority: 050
  Neighbor Number: Not available
SWME3400-11, Gi0/1 (Intermediate)
  Failed Port, (No Ext Neighbor) Reason: No REP neighbor
  Bridge MAC: 1c17.d3d6.b400
  Port Number: 001
  Port Priority: 400
  Neighbor Number: Not available
```

De las pruebas realizadas se concluye que el protocolo REP conmuta el tráfico de manera eficiente en un tiempo menor a 1 segundo, por lo cual no es comparable a otro tipo de protocolo de protección.

Se debe considerar que los *switches* secundarios deben llegar al anillo agregado principal para no generar subanillos en cascada que podrían provocar afectación de clientes a gran escala.

CAPÍTULO 5
CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La creciente necesidad de la reducción de costos de operación, así como la de soportar una mayor gama de aplicaciones, elevando la seguridad de las redes con garantías de calidad de servicio, ha llevado a buscar soluciones escalables y eficientes en la red.

- MPLS integra varios beneficios como el ahorro de costos en comparación a Frame Relay y ATM; además soporta QoS mediante la priorización de tráfico en tiempo real, indispensable en aplicaciones de voz y video.

- MPLS permite conexiones redundantes múltiples entre nodos, importante para la recuperación ante fallas o desastres, a diferencia de Frame Relay o ATM donde se requieren circuitos virtuales de *backup* permanentes o conmutados.

- Con MPLS se puede reducir el número de saltos entre puntos lo que produce un mejor tiempo de respuesta y mayor rendimiento de las aplicaciones.

- MPLS es una técnica de enrutamiento de tráfico IP basado en etiquetas; puede ser usado para redes privadas virtuales (VPNs) mediante túneles con etiquetas apiladas, además puede proveer ingeniería de tráfico IP. Por estas cualidades MPLS ha tenido un crecimiento en redes de *backbone* constituyéndose en una tecnología robusta.

- La capacidad limitada, una configuración compleja y la tendencia al decrecimiento, han sido las premisas para que las soluciones *Legacy* sean migradas a soluciones Metroethernet, donde se manejan grandes capacidades de tráfico, es escalable y la configuración es más sencilla.

- Las redes Metroethernet al ser redes de acceso de alta disponibilidad, e interconectadas al *backbone* IP/MPLS, son una combinación eficiente y escalable que el usuario busca para sus aplicaciones en un proveedor de servicio.

- Las redes Metroethernet a nivel de acceso de última milla están soportadas principalmente por medios de transmisión guiados, como son el cobre y la fibra óptica. Sin embargo, es posible brindar soluciones de radio en banda licenciada, cubriendo de esta manera la solución a cualquier sector urbano.

- Metroethernet basa su funcionamiento en apilar de forma consecutiva dos etiquetas VLAN, una VLAN para el proveedor (*Service* VLAN S-VLAN) y otro para el cliente (*Costumer* VLAN C-VLAN). La S-VLAN permite que el proveedor identifique individualmente las redes de sus clientes, mientras que la C-VLAN identifica las VLANs utilizadas en la red del cliente. El encapsulamiento de las C-VLAN mediante una S-VLAN vendrá determinado por el servicio que el cliente solicitó al proveedor. La red del proveedor emula la función de un conmutador LAN para conectar todos los UNI del cliente, de esta manera formar una única VLAN.

- REP es el protocolo de protección en redes Metroethernet que operan con equipos *Cisco*. En este diseño se ha escogido REP, ya que los tiempos de respuesta de conmutación no son comparables a *Spanning Tree* puesto que son muchísimo menores; sin embargo, puede convivir sin causar inconvenientes pero tomando las debidas precauciones al respecto.

- Para la implementación en el diseño se escogió el protocolo REP por su capacidad de respuesta de conmutación en el orden de los milisegundos en situaciones de falla.

- De lo que se puede observar en este Proyecto, especificados los parámetros de configuración, cada segmento REP es modular, con lo cual la red puede ampliarse manteniendo la eficiencia de la red; pero se debe considerar el

aumento de tráfico que cruzará por el anillo principal de agregación, para un estudio y ampliación del ancho de banda a futuro así como la implementación con equipos de la serie ME3800 con interfaces TenGigabitEthernet.

- La red puede pasar por la administración de diferente personal por lo que es necesaria una correcta depuración de configuraciones. El establecimiento de plantillas de configuración y una documentación actualizada se torna esencial; además esta información debe estar disponible en una base de datos corporativa.

- Una red Metroethernet puede interconectarse por medio de una red *Long-Haul* con otras redes Metroethernet de otras ciudades y se puede dar servicio a nivel de capa 2 sin ingresar a los *routers* de borde.

- Tomando como referencia un protocolo de rápida conmutación ante fallas, un diseño se puede implementar por medio del protocolo RPR (*Resilient Packet Ring*), tecnología que se sugiere que sea estudiada para ser implementada.

- El diseño que se ha presentado en el presente Proyecto de Titulación, tiene parámetros de manera general para que sea usado como referencia de implementación para los proveedores de servicios.

- Los *switches* principales deben estar concentrados en *Datacenters* o Telepuertos con la infraestructura necesaria para minimizar los riesgos de falla, además del control estricto del ingreso y manipulación física por parte de personal técnico autorizado. Esto en vista de que un error humano por manipulación incorrecta en el cableado, puede producir la caída total de la red.

- Al realizar migración de un cliente desde una red *Legacy* hacia una red IP conlleva una gran inversión por el equipamiento al inicio del proyecto, pero es de fácil recuperación en el transcurso de los primeros años.

- Equipos finales a ser instalados en las sedes del cliente, como el *router Cisco* 881, puede ser reemplazados por otros equipos similares de la marca *Huawei* o *Juniper* que son un 20% y 30% más económicos con la negociación directa con el fabricante.

- La implementación de recursos de fibra óptica empleado en el diseño, en lugar de recursos de cobre, es estratégica tanto en costos de mantenimiento que conllevaria el mantener operativa una red de cobre, así como el alinearse con las políticas actuales que promueve el gobierno hacia el desarrollo de tecnologías que provean una mayor velocidad y capacidad.

- Las configuraciones de las políticas en cuanto a calidad de servicio dentro de la red *Metroethernet* se ha diseñado en función de la capacidad del puerto, regularizando de esta manera las configuraciones para cuando se presente un incidente, poder realizar un *troubleshooting* apropiado y certero.

5.2 RECOMENDACIONES

- Como se ha visto en el modelamiento de red realizado, no se recomienda implementar segmentos REP con varios *switches* ubicados físicamente en las sedes de los clientes, ya que un apagado de los equipos por parte del usuario final, pone en vulnerabilidad a los demás equipos del segmento.

- Es importante el monitoreo de los diferentes segmentos de la red y la depuración en la configuración de las VLANs, esto con el objetivo de que en operación la red Metroethernet no presente configuraciones innecesarias.

- El protocolo REP es propietario de *Cisco*, y es importante mantener el soporte con el fabricante para la actualización en caso de ser necesario, en las versiones de IOS de los *switches Cisco* ME3XXX.

- Como se ha podido verificar en el modelamiento realizado, la apertura de un segmento por un corte en el recurso de fibra óptica es protegido por el protocolo REP, mientras que la caída de un *switch* ME3400 implica la caída de todos los servicios vinculados a éste. Por esta razón, es importante las condiciones y el mantenimiento de los respaldos eléctricos en los nodos, así como la disponibilidad inmediata de equipos de reposición.

- Algo a tomar en cuenta en la configuración es el filtrado de los paquetes, tormentas de *broadcast* y la verificación de la publicación de *mac-address,* ya que una *mac–address* duplicada puede generar *loops*, produciendo que se sobrecargue la red y como resultado que la misma llegue a “caerse”.

- La carga del IOS debe ser homologado y previamente probado en un laboratorio, ya que un IOS diferente puede producir que el equipo no funcione apropiadamente o presentar *bugs*, con lo que el equipo no trataría correctamente los paquetes, produciendo el reinicio del equipo.

- La actualización o cambio de solución que involucre equipos de última milla de tecnología *Legacy* a IP por parte del proveedor, incentiva en la fidelidad de los clientes. Esto se afianza más ya que al disponer del suficiente *stock* de repuestos, el soporte técnico es oportuno.

- En cuanto a la perspectiva de crecimiento a mayores velocidades por parte del cliente, se recomienda el uso de equipos Juniper sxr100 ya que soportan, a menor costo, hasta 30 Mbps. El equipo *Cisco* 881 solo soporta un máximo de 20 Mbps.

REFERENCIAS BIBLIOGRÁFICAS

CAPÍTULO 1

[1] https://learningportal.juniper.net/core/user_scorm_launch.aspx

[2] http://es.wikipedia.org/wiki/Ethernet

[3] https://learningportal.juniper.net/juniper/user_activity_info.aspx?id=769

[4] http://www.textoscientificos.com/redes/ethernet/ethernet-vs-ieee8023

[5] http://www.textoscientificos.com/redes/redes-virtuales

[6] http://sistemac.carnet.hr/node/671?device=mobile

[7] http://metroethernetforum.org/

[8] http://corporateportal.gcintranet.net/netdev/Technical%20Specification%20Documents/Current%20Releases/Advanced-switching-systems-Ethernet-2.0.12x.pdf

[9] Metro Ethernet, Sam Halabi, Cisco, 2003 Pag. 66

[10] www.tonet.jazztel.es/docs/cbxc_wans.pdf

[11] biblioteca.pucp.edu.pe/docs/./07_Alcocer_2000_Redes_Cap_07.pdf

[12] http://tools.ietf.org/html/rfc3748

[13] http://www.cisco.com/c/dam/en/us/products/collateral/switches/me-3400-series-ethernet-access-switches/prod_white_paper0900aecd806ec6fa.pdf

[14] http://ccieordie.com/wp-content/uploads/2013/02/tos_dscp.png

[15] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html#pgfId-46447

[16] http://www.cisco.com/cisco/web/support/LA/7/73/73469_dscpvalues.pdf

[17] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html#pgfId-46092

[18] http://es.wikipedia.org/wiki/Jitter

[19] http://tools.ietf.org/html/rfc2475#section-2.3.3.3

[20] http://tools.ietf.org/html/rfc4594#page-8

[21] http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf

[22] Implementing Cisco Quality of Service Volume 1 Version 2.1 Pag. 102 QOS21StudentGuide_Vol1.pdf

[23] http://es.wikipedia.org/wiki/Reflect%C3%B3metro_de_dominio_de_tiempo

[24] http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094195.shtml

[25] http://mars.tekkom.dk/mediawiki/images/b/b5/ScreenShot742.jpg

[26] http://giret.ufps.edu.co/cisco/descargas/Presentaciones/Modulo2_capitulo10.pdf

[27] http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html

[28] http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a3e6f.shtml

[29] http://bibing.us.es/proyectos/abreproy/11359/fichero/BGP%252F5.+Fundamentos+de+BGP.pdf

[30] Multiprotocol Label Switching (MPLS), Ing. Pablo Hidalgo, Julio 2014

[31] http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo2.pdf

[32] https://globalcrossing.skillport.com/skillportfe/login.action

[33] http://www.scribd.com/doc/830503/MPLS-Concepts

[34] ishare.edu.sina.com.cn/download.php?fileid=6920688

[35] http://www.4shared.com/office/voWc3v4C/CiscoPressMPLS_and_VPN_Archite.html

[36] http://tools.ietf.org/html/rfc4364

[37] https://es.scribd.com/doc/92188638/Arquitectura-Redes-Mpls-Ver7

[38] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/VPNQoS.html

CAPÍTULO 2

[39] www.cisco.com/cisco/web/support/LA/7/73/73295_bwidth_consume.html

[40] www.cisco.com/cisco/web/support/LA/102/.../1026685_video-qos.pdf

[41] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html#pgfId-46626

CAPÍTULO 3

[42] TSD (Technical Specification Document) http://corporateportal.gcintranet.net/netdev/Technical%20Specification%20Documents/Current%20Releases/Metro%20and%20Long%20Haul%20Ethernet%20TSD%20v2.1.1.pdf

[43] http://www.juniper.net/techpubs/en_US/junos13.3/topics/reference/configuration-statement/vlan-id-range-edit-interfaces.html

[44] http://es.wikipedia.org/wiki/IEEE_802.16

[45] http://www.modulo0tutoriales.com/ofdm-multiplexacion-por-division-de/

[46] Manual FibeAir IP-10G ETSI Product Description for I6.8(RevF).pdf PAg. 122

[47] https://sites.google.com/site/stigestionydesarrollo/recuperacion/desarrollo-1/tema11/8---propiedades-y-tipos-de-conectores-de-fibra-optica

[48] http://www.cisco.com/c/en/us/products/collateral/switches/me-3400-series-ethernet-access-switches/prod_bulletin0900aecd8052f3d5.html

[49] Contabilidad de Costos, ChrlesT. Horngren, Décima Edición, Pag. 751.

[50] *www.ecotec.edu.ec/...de.../1619_2010_CEE_LSOLEDISPA_05.pdf*

[51] http://www.consejo.org.ar/coltec/astrella.htm

[52] Contabilidad de Costos, ChrlesT. Horngren, Décima Edición, Pag. 752

ACRÓNIMOS

ACL	*(Access Control List)*	Lista de Control de Acceso
ADI	*(Access Dedicated Internet)*	Acceso Dedicado a Internet
AF	*(Assured Forwarding)*	Reenvío Asegurado
AGC	*(Automatic Gain Control)*	Control Automático de Ganancia
AS	*(Antonomous Sistem)*	Sistema Autónomo
ASN	*(Autonomous System Number)*	Número de Sitema Autonomo
ATM	*(Asynchronous Transfer Mode)*	Modo de Transferencia Asíncrona
ATPC	*(Automatic Transmit Power Control)*	Control Control de Transmision de Potencia
BA	*(Behavior Aggregate)*	Comportamiento Agregado
BER	*(Bit Error Rate)*	Tasa de Error de Bit
BGP	*(Border Gateway Protocol)*	Protocolo *Gateway* de Borde
BIP	*(Bit Interleaved Parity)*	Paridad Intercalada de Bits
BPDU	*(Bridge Protocol Data Units)*	Unidad de Datos de Protocolo Puente
BPON	*(Broadband PON)*	Red Óptica Pasiva de Banda Ancha
BSDU	*(Base Station Distribution Unit)*	Unidad de Distribución de la Estación Base
BSR	*(Base Station Radio)*	Estación base de Radio
CBWFQ	*(Class-Based Weighted Fair Queueing)*	Clase Basada en Colas de Peso Justo
CE	*(Customer Equipment)*	Equipo del Cliente
CFI	*(Canonical Format Indicator)*	Indicador de Formato Canónico
CIDR	*(Classless Inter-Domain Routing)*	Enrutamiento entre Dominios sin Clases
CIR	*(Commited Information Rate)*	Información de Tasa Comprometida
CoS	*(Class Of Service)*	Clase de Servicio
CPE	*(Customer Premises Equipment)*	Equipo Local del Cliente
CQ	*(Custom Queueing)*	Encolamiento Personalizado
CRC	*(Cyclic Redundancy* Code)	Código de Redundancia Cíclica
CRC	*(Cyclic Redundancy Check)*	Comprobación de Redundancia Cíclica
CR-LDP	*(Constraint-Based Routing Label Distribution Protocol)*	Protocolo de Enrutamiento de Distribución de Etiquetas basado en restricciones
CRTP	*(Compressed Real-Time Transport Protocol)*	Protocolo de Transporte de Tiempo Real Comprimido
CS	*(Class selector)*	Seleccionador de Clase
CSMA/CD	*(Carrier Sense Multiple Access with Collision Detection)*	Acceso Múltiple con Escucha de Portadora y Detección de Colisiones

CSMA/CD	*(Carrier Sense Multiple Access With Collision Detection)*	Acceso Múltiple con Detección de Colisiones de Carrier Sense
C-VLAN	*(Customer VLAN)*	VLAN de Cliente
DLCI	*(Data Link Connection Identifier)*	Identificador de Conexión de Enlace de Datos
DSCP	*(Differentiated Services Code Point)*	Punto de Código de Servicios Diferenciados
DSLAM	*(Digital Subscriber Line Access Multiplexer)*	Multiplexor de Línea de Acceso de Abonado Digital
DSP	*(Digital signal processor)*	Procesador de Señales Digitales
DWDM	*(Dense Wavelength Division Multiplexing)*	Multiplexación por División de Longitudes de Onda Densa
EAPS	*(Ethernet Automatic Protection Switching)*	Conmutación de Protección Automática Ethernet
EBGP	*(External BGP)*	BGP Externo
ECN	*(Explicit Congestion Notification)*	Notificación de Congestion Explicita
EF	*(Expedited Forwarding)*	Reenvío Acelerado
EFM	*(Ethernet in the First Mile)*	Ethernet en la Primera Milla
EGP	*(Exterior Gateway Protocol)*	Protocolos de *Gateway* Exterior
EIGRP	*(Enhanced Interior Gateway Routing Protocol)*	Protocolo de Enrutamiento Mejorado de *Gateway* Interior
EIR	*(Excess Information Rate)*	Tasa de Exceso de Información
E-LAN	*(Ethernet Lan Service)*	Servicio Ethernet LAN
E-LINE	*(Ethernet Line Service)*	Servicio Ethernet *Line*
ENNIs	*(Ethernet Network To Network Interface)*	Red Ethernet a Interfaces de Red
EPL	*(Servicio Ethernet Private Line)*	Servicio de Línea Privada de Internet
EPLAN	*(Ethernet Private Lan)*	Ethernet LAN Privada
EVC	*(Ethernet Virtual Connectio)*	Conexión Virtual Ethernet
EVPL	*(Servicio Ethernet Virtual Private Line)*	Servicio Ethernet de Línea Virtual Privada
EVPLAN	*(Ethernet Virtual Private Lan)*	LAN Privada Ethernet
FCS	*(Frame Check Sequence)*	Comprovador de Secuencia de Trama
FDD	*(Frequency Division Duplex)*	Duplexación por División de Frecuencia
FEC	*(Forwarding Equivalence Class)*	Equivalencia de Clases de Reenvío
FIB	*(Forwarding Information BasE)*	Reenvío de Base de Información
FIFO	*(First In First Out)*	Primero Ingresa-Primero Sale
FR	*(Frame Relay)*	Frame Relay
FXO	*(Foreign Exchange Office)*	Oficina de Intercambio Foráneo
FXS	*(Foreign Exchange Station)*	Estación de Intercambio Foráneo
GPON	*(Gigabit Passive Capacity Optical Network)*	Red Óptica Pasiva con Capacidad de Gigabit

GRE	*(Generic Routing Encapsulation)*	Encapsulación de Enrutamiento Genérico
HDSL	*(High Bit Rate Digital Subscriber Line)*	Línea de Abonado Digital de Alta Velocidad Binaria.
HTTP	*(Hypertext Transfer Protocol)*	Protocolo deTransferencia de Hipertexto
I-BGP	*(Internal BGP)*	BGP Interno
IDU	*(Indoor unit)*	Unidad Interna
IEEE	(Institute of Electrical and Electronics Engineers)	Instituto de Ingenieros Eléctricos Y Electrónicos
IETF	*(Internet Engineering Task Force)*	Grupo de Trabajo de Ingeniería de Internet
IF	*(Intermediate Frequency)*	Frecuencia Intermedia
IFC	*(IF Combining)*	Combinación IF
IGP	*(Interior Gateway Protocol)*	Protocolo De *Gateway* Interior
IGRP	*(Interior Gateway Routing Protocol*	Protocolo de Enrutamiento de *Gateway* Interior
IP ECN	*(Explicitcongestion Notification)*	Notificación de Congestión Explícita
IPP	*(Precedencia* IP)	IP Precedence
IPX	*(Internetwork Packet Exchang)*	Intercambio de Paquetes Interred
IS-IS	*(Intermediate System-To-Intermediate System)*	Sistema Intermedio a Sistema Intermedio
ISP	*(Internet Service Provider)*	Proveedor de Servicio de Internet
ITU	*(International Telecommunication Union)*	Unión Internacional de Telecomunicaciones
LAN	*(Local area network)*	Red de Area Local
LDP	*(Label Distribution Protocol)*	Protocolo de Distribución de Etiquetas
LER	*(Label Edge Router)*	Router de Etiqueta de Borde
LFI	*(Link Fragmentation And Interleaving)*	Enlace Fragmentación e Intercalado
LFIB	*(Label Forwarding Information Base)*	Base de Información de Reenvío de Etiquetas
LIB	*(Label Information Base)*	Base de Información de Envío
LLQ	*(Low Latency Queuing)*	Encolamiento de Baja Latencia
LOS	*(Loss Of Signal)*	Pérdida de Señal
LSA	*(Link State Advertisement)*	Paquetes de Estado-Enlace
LSP	*(Label Switching Path)*	Ruta de Acceso de Conmutación de Etiquetas
LSR	*(Label Switching Router)*	Router de Etiqueta de Cambio
MAC	*(Media Access Control)*	Control de Acceso al Medio
MAN	*(Metropolitan Area Network)*	Red de Área Metrolitana
MEF	*(Metro Ethernet Forum)*	Foro Metro Ethernet
MEN	*(Metro Ethernet Network)*	Red Metro Ethernet
MOS	(Mean Opinion Score)	Opinión Media de Puntuación
MP-BGP	*(Multiprotocol BGP)*	Multiprotocolo BGP

MPLS	*(Multiprotocol Label Switching)*	Conmutación Multi-Protocolo Mediante Etiquetas
MRC	*(Monthly Recurrent Charge)*	Carga Recurrente Mensual
MRMC	*(Multi Rate Multi Coding)*	Codificación de Tasa Múltiple
MSE	*(Mean Square Error)*	Error Cuadrático Medio
MSTP	*(Multiple Spanning Tree Protocol)*	Multiple *Spanning Tree*
MTU	*(Maximum Transfer Unit)*	Unidad Máxima de Transferencia
NBAR	*(Network-Based Application Recognition)*	Aplicación de Reconocimiento Basada en la Red
NIC	*(Network Interface Card)*	Tarjeta de Interfaz de Red
NLoS	*(Non line-of-sight)*	Sin Línea de Visión
NNI	*(Network-Network Interface)*	Red Interfaz de Red
NRC	*(Non Recurrent Charge)*	Cargo No Recurrente
OAM	*(Operations, Administration, and Maintenance)*	Operación, Administración y Mantenimiento
ODR	*(On Demand Routing)*	Ruteo Bajo Demanda
OFDM	*(Orthogonal Frequency Division Multiplexing)*	Multiplexación por División de Frecuencia Octogonal
OSPF	*(Open Short Path First)*	El Camino Más Corto Primero
PDU	*(Protocol Data Unit)*	Unidad de Datos de Protocolo
PE	*(Provider Edge)*	Router de Borde del Proveedor
PHB	*(Per Hop Behavior)*	Comportamiento por Salto
PHP	*(Hypertext Pre-Processor)*	Hipertexto Pre-Procesado
PID	*(Protocol Identifier)*	Identificador de Protocolo
PIM	*(Protocol Independent Multicast)*	Protocolo Multicast Independiente
PON	*(Passive Optical Network)*	Red Óptica Pasiva
POTS	*(Plain Old Telephone Service)*	Servicio Telefónico Ordinario
PPP	*(Point To Point Protocol)*	Protocolo Punto a Punto
PQ	*(Priority Queuing)*	Cola de Prioridad
PSK	*(Phase Shift Keying)*	Modulación por desplazamiento de Fase
QAM	*(Quadrature Amplitude Modulation)*	Modulación en Amplitud de Quaratura
QoS	*(Quality of service)*	Calidad de Servicio
RD	*(Route Distinguishers)*	Distinguidor de Ruta
RED	*(Random Early Detection)*	Detección Temprana Aleatoria
REP	*(Resilient Ethernet Protocol)*	Protocolo Ethernet Resistente
RF	*(Radio Frequency)*	Radio Frecuencia
RFC	*Request for Comments*	Solicitud de Comentarios
RFU	*(Radio Frequency Unit)*	Unidad de Radio Frecuencia
RIB	*(Routing Information Base)*	Base de Información de Etiquetas
RIP	*(Routing Information Protocol)*	Protocolo de Información de Enrutamiento
RPR	*(Resilient Packet Ring)*	Anillo de Recuperación de Paquetes

RSL	*(Received Signal Level)*	Nivel de Señal Recibida
RSVP	*(Resource Reservation Protocol)*	Protocolo de Reserva de Recurso
RT	*(Route Target)*	Objetivo de Rutas
RTP	*(Real-Time Transport Protocol)*	Protocolo de Tiempo Real de Transporte
SDA	*(Suscriber Data Adapter)*	Adaptador de Datos del Suscriptor
SDH	*(Synchronous Digital Hierarchy)*	Multiplexación por División en Longitudes de Onda Densas
SDM	*(Switch Database Management)*	Switch de Administración de Base de Datos
SLA	*(Service - Level Agreement)*	Acuerdo del Nivel de Servicio
SONET	*(Synchronous Optical Network)*	Red Óptico Sincrónico
SPR	*(Suscriber Personal Radio)*	Antena de Radio del Suscriptor
STCN	*(Segment Topology Change Notification)*	Notificación de Cambio de Topología del Segmento
STDM	*(Statistical Time Division Multiplexing)*	Multiplexación por División de Tiempo Estadístico
STP	(*Spanning Tree Protocol)*	Protocolo de Árbol de Expansión
S-VLAN	*(Service VLAN)*	VLAN de Servicio
SWAP	*(Shared Wireless Access Protocol)*	Protocolo Acceso Inalámbrico Compartido
TCP	*(Transmission Control Protocol)*	Protocolo de Control de Transmisión
TDD	*(Time Division Duplex)*	Duplexación por División de Tiempo
TDM	*(Time Division Multiplexing)*	Multiplexación
TDR	*(Optical Time Domain)*	Reflectómetro de Dominio del Tiempo
TIR	*(Internal Rate Of Return)*	Tasa Interna de Rendimiento
ToS	*(Type Of Service)*	Tipo de Servicio
TPID	*(Tag Protocol Identifier)*	Identificador de Protocolo de Etiqueta
TS	*(Traffic Shaping)*	Catalogación de Tráfico
TSD	*(Technical Specification Document)*	Especificaciones Técnicas del Documento
TSL	*(Transmission Signal Level)*	Nivel de Transmición de Señal
UDP	*(User Datagram Protocol)*	Protocolo de Datagrama de UsuariO
UIT	(The *International* Telecommunication *Union)*	Unión Internacional de Telecomunicaciones
UNI	*(User To Network Interface)*	Usuario de Interfaz de Red
UTP	*(Unshielded Twisted Pair)*	Par Trenzado No Blindado
VAN	*(Net present value)*	Valor Actual Neto
VCI	*(Virtual Channel Identifier)*	Identificador de Canal Virtual
VLAN	*(Virtual LAN)*	Red de Área Local Virtual
VLAN ID	*(VLAN Identification)*	Identificación de la VLAN
VLSM	*(Variable Length Subnet Mask)*	Máscara de Longitud Variable

VMPS	*(VLAN Management Policy Server)*	Servidor de Políticas y Administración de VLAN
VoIP	(Voice over IP)	Voz sobre IP
VPI	*(Virtual Path Identifier)*	Identificador de Ruta Virtual
VPN	*(Virtual Private Network)*	Red Privada Virtual
VRF	*(Virtual Routing And Forwarding Table)*	Tabla Virtual de Enrutamiento y Reenvío
WACC	*(Weighted Average Cost Of Capital)*	Coste Medio Ponderado de Capital
WAN	*(Wide Area Network)*	Rede de Area Extendida
WDM	*(Wavelength Division Multiplexing)*	Multiplexación por División de Longitud de Onda
WFQ	*(Weighted fair queuing)*	Espera Equitativa Ponderada
WHIP	*WHIP (World Hardiest IP Network)*	Red Mundial IP
WIMAX	(*Worldwide Interoperability for Microwave Access)*	Interoperabilidad Mundial para Acceso por Microondas
WRED	*(Weighted Random Early Detection)*	Detección Temprana Aleatoria Ponderada

ANEXOS

ANEXO A RADIO SAF
ANEXO B MODEM MUSIC 200
ANEXO C RADIO DMC CLASSIC II
ANEXO D RADIO MICROMAX AIRSPAN
ANEXO E RADIO CERAGON
ANEXO F CONVERSOR DE F.O. CTC
ANEXO G CONVERSOR DE F.O. TP-LINK
ANEXO H *ROUTER* CISCO 2821
ANEXO I *ROUTER* CISCO 881
ANEXO J *SWITCH* CISCO ME3400
ANEXO K EQUIPOS DE VIDEOCONFERENCIA POLYCOM
ANEXO L EQUIPO AUDIOCODE MEDIANT 1000
ANEXO M EQUIPO AUDIOCODE MP 11X
ANEXO N CONFIGURACIÓN SEGMENTOS REP

ANEXO A

RADIO SAF

(CD ADJUNTO)

ANEXO B

MODEM MUSIC 200

(CD ADJUNTO)

ANEXO C

RADIO DMC CLASSIC II
(CD ADJUNTO)

ANEXO D

RADIO MICROMAX AIRSPAN
(CD ADJUNTO)

ANEXO E

RADIO CERAGON
(CD ADJUNTO)

ANEXO F

CONVERSOR DE F.O. CTC
(CD ADJUNTO)

ANEXO G

CONVERSOR DE F.O. TP-LINK
(CD ADJUNTO)

ANEXO H

ROUTER CISCO 2821

(CD ADJUNTO)

ANEXO I

ROUTER CISCO 881

(CD ADJUNTO)

ANEXO J

SWITCH CISCO ME3400

(CD ADJUNTO)

ANEXO K

EQUIPOS DE VIDEOCONFERENCIA POLYCOM
(CD ADJUNTO)

ANEXO L

EQUIPO AUDIOCODE MEDIANT 1000

(CD ADJUNTO)

ANEXO M

EQUIPO AUDIOCODE MP 11X

(CD ADJUNTO)

ANEXO N

CONFIGURACIÓN SEGMENTOS REP 62 - 66

Configuración segmento REP 62

La S-VLAN 62 se configura para el segmento REP.

```
vlan 7          name BBONE:GYE:BKP
vlan 8          name BBONE:GYE
vlan 49         name MGMT:METRO_GYE
vlan 62         name ADMIN_REP_62
```

Los siguientes parámetros se configuran en las interfaces correspondientes al segmento REP 62.

```
port-type nni
switchport trunk native vlan 62
switchport trunk allowed vlan 7,8,,49,62
switchport mode trunk
bandwidth 100000
load-interval 30
udld port aggressive
rep preempt delay 45
storm-control broadcast level 1.00
storm-control multicast level 10.00
storm-control action trap
service-policy input GX-Ingress-GE
service-policy output GX-Egress-GE
```

Switch Cisco SWME3400-1 10.5.80.1 ME3400EG-12CS

```
interface GigabitEthernet0/10
description TRUNK: SWME3400-13:G0/2
rep segment 62 edge primary
rep stcn segment 60
rep block port id 0002A40CC3E92C80 vlan 1-4094
```

Switch Cisco SWME3400-13 10.5.80.33 ME3400EG-2CS

```
interface GigabitEthernet0/2
description TRUNK:SWME3400-1:G0/10
rep segment 62

interface GigabitEthernet0/1
description TRUNK:SWME3400-14:G0/2
rep segment 62
!
interface Vlan49
ip address 10.5.80.33 255.255.255.0
```

```
!
ip default-gateway 10.5.80.254
```

Switch Cisco SWME3400-14 10.5.80.34 ME3400EG-2CS

```
interface GigabitEthernet0/2
description TRUNK:SWME3400-13:G0/1
rep segment 62 preferred

interface GigabitEthernet0/1
description TRUNK:SWME3400-2:G0/10
rep segment 62
!
interface Vlan49
ip address 10.5.80.34 255.255.255.0
!
ip default-gateway 10.5.80.254

SWME3400-14#sh int g0/2 rep detail
GigabitEthernet0/2   REP enabled
Segment-id: 62 (Preferred)
PortID: 0002A40CC3E92C80
Preferred flag: Yes
Operational Link Status: TWO_WAY
Current Key: 000A8CB64F740680F245
Port Role: Alternate
Blocked VLAN: 1-4094
Admin-vlan: 62
Preempt Delay Timer: 45 sec
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
```

Switch Cisco SWME3400-2 10.5.80.2 ME3400EG-12CS

```
interface GigabitEthernet0/10
description TRUNK:SWME3400-14
rep segment 62 edge
rep stcn segment 60
```

Se verifica que el segmento REP 62 este configurado correctamente.

```
SWME3400-1#sh rep topology segment 62
REP Segment 62
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-1   Gi0/10     Pri  Open
```

SWME3400-13 Gi0/2 Open
SWME3400-13 Gi0/1 Open
SWME3400-14 Gi0/2 Alt
SWME3400-14 Gi0/1 Open
SWME3400-2 Gi0/10 Sec Open

Configuración segmento REP 63

La S-VLAN 63 se configura para el segmento REP.

vlan 7 name METRO_GYE_BKP
vlan 8 name METRO_GYE
vlan 49 name MGMT:METRO_GYE
vlan 63 name ADMIN_REP_63

Los siguientes parámetros se configuran en las interfaces correspondientes al segmento REP 63.

port-type nni
switchport trunk native vlan 63
switchport trunk allowed vlan 7,8,49,63
switchport mode trunk
bandwidth 1000000
load-interval 30
udld port aggressive
rep preempt delay 45
storm-control broadcast level 1.00
storm-control multicast level 10.00
storm-control action trap
service-policy input GX-Ingress-GE
service-policy output GX-Egress-GE

Switch Cisco SWME3400-3 10.5.80.3 ME3400EG-12CS

interface GigabitEthernet0/12
description TRUNK:SW2.CC1.GYE.EC:GE0/16
rep segment 63 edge primary
rep stcn segment 60
rep block port id 000C1CAA07C9A000 vlan 1-4094

Switch Cisco sw2.cc1.gye.ec 10.5.80.20 ME3400EG-12CS

interface GigabitEthernet0/16
description TRUNK:SWME3400-3:GE0/12
rep segment 63

```
interface GigabitEthernet0/12
description TRUNK:SWME3400-6:GE0/12
media-type sfp
rep segment 63 preferred

interface Vlan49
ip address 10.5.80.20 255.255.255.0
!
ip default-gateway 10.5.80.254

sw2.cc1.gye.ec#sh int g0/12 rep detail
GigabitEthernet0/12   REP enabled
Segment-id: 63 (Preferred)
PortID: 000C1CAA07C9A000
Preferred flag: Yes
Operational Link Status: TWO_WAY
Current Key: 000C8CB64F3A4A809218
Port Role: Alternate
Blocked VLAN: 1-4094
Admin-vlan: 63
Preempt Delay Timer: 45 sec
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none

Switch Cisco  SWME3400-6  10.5.80.5     ME3400EG-12CS

interface GigabitEthernet0/12
description TRUNK:SW2.CC1.GYE.EC:GE0/12
rep segment 63 edge
rep stcn segment 60
```

Se verifica que el segmento REP 63 este configurado correctamente

```
SWME3400-3#sh rep topology segment 63
REP Segment 63
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-3   Gi0/12     Pri  Open
SWME3400-15   Gi0/16          Open
SWME3400-15   Gi0/12          Alt
SWME3400-6   Gi0/12     Sec  Open
```

Configuración segmento REP 64

La S-VLAN 64 se configura para el segmento REP.

```
vlan 7          name METRO_GYE_BKP
vlan 8          name METRO_GYE
vlan 49         name MGMT:METRO_GYE
vlan 64         name ADMIN_REP_64
```

Los siguientes parámetros se configuran en las interfaces correspondientes al segmento REP 64.

```
port-type nni
switchport trunk native vlan 64
switchport trunk allowed vlan 7,8 ,49,64
switchport mode trunk
bandwidth 48000
load-interval 30
udld port aggressive
rep preempt delay 45
storm-control broadcast level 1.00
storm-control multicast level 10.00
storm-control action trap
service-policy input GX-Ingress-GE
service-policy output GX-Egress-GE
```

Switch Cisco SWME3400-1 10.5.80.1 ME3400EG-12CS

```
interface GigabitEthernet0/9
description TRUNK:SWME3400-16:GE0/16
switchport vlan mapping 329 332
rep segment 64 edge primary
rep stcn segment 60
rep block port id 000C1CAA07C99880 vlan 1-4094
```

Switch Cisco SWME3400-16 10.5.80.21 ME3400EG-12CS

```
interface GigabitEthernet0/16
description TRUNK:SWME3400-1:GE0/9
rep segment 64

interface GigabitEthernet0/12
description TRUNK:SWME3400-9:GE0/9 [CERAGON 48MBPS]
media-type rj45
speed 100
duplex full
rep segment 64 preferred
!
interface Vlan49
ip address 10.5.80.21 255.255.255.0
```

```
!
ip default-gateway 10.5.80.254

SWME3400-16#sh int g0/12 rep detail
GigabitEthernet0/12   REP enabled
Segment-id: 64 (Preferred)
PortID: 000C1CAA07C99880
Preferred flag: Yes
Operational Link Status: TWO_WAY
Current Key: 00098CB64F74068078BD
Port Role: Alternate
Blocked VLAN: 1-4094
Admin-vlan: 64
Preempt Delay Timer: 45 sec
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
```

Switch Cisco SWME3400-9 10.5.80.8 ME3400EG-12CS

```
interface GigabitEthernet0/9
description TRUNK:SWME3400-16:GE0/12 [ECLIPSE 48MBPS]
media-type rj45
speed 100
duplex full
rep segment 64 edge
rep stcn segment 60
```

Se verifica que el segmento REP 64 este configurado correctamente

```
SWME3400-1#sh rep topology segment 64
REP Segment 64
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-1    Gi0/9      Pri     Open
SWME3400-16   Gi0/16           Open
SWME3400-16   Gi0/12            Alt
SWME3400-9    Gi0/9      Sec  Open
```

Configuración segmento REP 65

La S-VLAN 65 se configura para el segmento REP.

```
vlan 7-8,49,65
```

Los siguientes parámetros se configuran en las interfaces correspondientes al segmento REP 65

```
port-type nni
switchport trunk native vlan 65
switchport trunk allowed vlan 7,8,49,65
switchport mode trunk
bandwidth 1000000
load-interval 30
speed 1000
duplex full
udld port aggressive
rep preempt delay 45
storm-control broadcast level 1.00
storm-control multicast level 10.00
storm-control action trap
service-policy input GX-Ingress-GE
service-policy output GX-Egress-GE
```

Switch Cisco SWME3400-15 10.5.80.20 ME3400EG-12CS

```
interface GigabitEthernet0/10
description RESERVADO
TRUNK:SW1.LATINOMEDICAL.MTX.ALBORADA.GYE.EC:GE:G0/1
media-type rj45
rep segment 65 edge primary
rep stcn segment 63
rep block port id 00016C9CEDC17480 vlan 1-4094
```

Switch Cisco SWME3400-17 10.5.80.36 ME3400EG-12CS

```
interface GigabitEthernet0/1
description TRUNK:SWME3400-15:GE0/10
media-type rj45
rep segment 65 preferred
!
interface GigabitEthernet0/2
description TRUNK:SWME3400-7:GE0/10
media-type rj45
rep segment 65

interface Vlan49
ip address 10.5.80.36 255.255.255.0
!
ip default-gateway 10.5.80.254

SWME3400-17#sh int g0/1 rep detail
GigabitEthernet0/1   REP enabled
Segment-id: 65 (Preferred)
PortID: 00016C9CEDC17480
```

Preferred flag: Yes
Operational Link Status: TWO_WAY
Current Key: 000A1CAA07C9A0008F63
Port Role: Alternate
Blocked VLAN: 1-4094
Admin-vlan: 65
Preempt Delay Timer: 45 sec
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none

Switch Cisco SWME3400-7 10.5.80.6 ME3400EG-12CS

interface GigabitEthernet0/10
description RESERVADO
TRUNK:SW1.LATINOMEDICAL.MTX.ALBORADA.GYE.EC:GE:G0/4
media-type sfp
rep segment 65 edge
rep stcn segment 60

Se verifica que el segmento REP 65 este configurado correctamente

```
SWME3400-7#sh rep topology segment 65
REP Segment 65
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
SWME3400-15   Gi0/10     Pri  Open
SWME3400-17- Gi0/1          Alt
SWME3400-17- Gi0/2          Open
SWME3400-7   Gi0/10     Sec  Open
```

Configuración segmento REP 66

La S-VLAN 66 se configura para el segmento REP.

```
vlan 7              name METRO_GYE_BKP
vlan 8              name METRO_GYE
vlan 49             name MGMT:METRO_GYE
vlan 66             name ADMIN_REP_66
```

Los siguientes parámetros se configuran en las interfaces correspondientes al segmento REP 66

port-type nni
switchport trunk native vlan 66

switchport trunk allowed vlan 7,8 ,49,66,
switchport mode trunk
bandwidth 1000000
load-interval 30
udld port aggressive
rep preempt delay 45
storm-control broadcast level 1.00
storm-control multicast level 10.00
storm-control action trap
service-policy input GX-Ingress-GE
service-policy output GX-Egress-GE

Switch Cisco SWME3400-1 10.5.80.1 ME3400EG-12CS

interface GigabitEthernet0/8
description TRUNK:SWME3400-18:GE0/3
media-type sfp
rep segment 66 edge primary
rep stcn segment 60
rep block port id 000408CC68979300 vlan 1-4094

Switch Cisco SWME3400-18 10.5.80.96 ME3400EG-2CS

interface GigabitEthernet0/3
description TRUNK:SWME3400-1:GE0/8
rep segment 66

interface GigabitEthernet0/4
description TRUNK:SWME3400-16:GE0/8
rep segment 66 preferred

interface Vlan49
ip address 10.5.80.96 255.255.255.0
!
ip default-gateway 10.5.80.254

SWME3400-18#sh int g0/4 rep detail
GigabitEthernet0/4 REP enabled
Segment-id: 66 (Preferred)
PortID: 000408CC68979300
Preferred flag: Yes
Operational Link Status: TWO_WAY
Current Key: 00088CB64F740680C6F9
Port Role: Alternate
Blocked VLAN: 1-4094
Admin-vlan: 66
Preempt Delay Timer: 45 sec
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: none

Configured Load-balancing Block VLAN: none
STCN Propagate to: none

Switch Cisco SWME3400-16 10.5.80.21 ME3400EG-12CS

interface GigabitEthernet0/8
description TRUNK:SWME3400-18:GE0/4
rep segment 66 edge
rep stcn segment 64

Se verifica que el segmento REP 66 este configurado correctamente.

SWME3400-1#sh rep topology segment 66
REP Segment 66
BridgeName PortName Edge Role
---------- ---------- ---- ----
SWME3400-1 Gi0/8 Pri Open
SWME3400-18 Gi0/3 Open
SWME3400-18 Gi0/4 Alt
SWME3400-16 Gi0/8 Sec Open