Diseño de red WAN

Autor: **Gustavo Fabián Spadaro**

Titulación: **E.T.T. Telemática**

Consultor: **Miquel Font Rosselló**

Diciembre 2012

2. Resumen de unas 250 palabras. Palabras clave. Nombre del área de TFC.

Este proyecto se encuadra dentro del área Integración de redes telemáticas. Se ha desarrollado el diseño e implantación de una red WAN, para ofrecer múltiples servicios.

El diseño se adapta a las necesidades de cualquier operador con cobertura internacional, la infraestructura, tecnología e infraestructura seleccionada hace posible el despliegue de una red MPLS/IP a nivel mundial, convirtiéndose en un diseño ampliamente escalable tanto en capacidad como en número de nodos de red.

No es el ámbito de este trabajo compara las prestaciones de diferentes fabricantes, sino de acuerdo a la experiencia personal, y basándose en lo equipos actuales del mercado se proponen 2 fabricantes como proveedores de equipamiento tanto para el Core como el Acceso, evitando así de esta manera el condicionante de solo fabricante y la dependencia que pueda llegar a existir.

El proyecto abarca el diseño de la red, elección de equipamiento, justificación de la tecnología a utilizar, como así también el diseño de la red de gestión para la operación de los equipos.

A nivel de servicios se detallan las características de los servicios ofrecidos en todas sus modalidades (estos servicios no pretenden ser rígidos, sino que meramente son una guía de servicios, ya que gracias a la tecnología IP/MPLS utilizada pueden existir infinitas soluciones que se adapten a las necesidades de los cliente).

3. Índice de contenidos

1 Contenido

4. Índice de Figuras

5. Cuerpo de la Memoria

5.1.Introducción

Este proyecto corresponde al diseño de una red WAN, principalmente enfocado a la red de un proveedor de servicios de internet (ISP), de ámbito internacional, actualmente una red WAN debe estar preparada para poder transportar numerosos y variados servicios como ser :

- ✓ Voz sobre IP.
- ✓ Video conferencia y Telepresencia.
- ✓ STREAMING de Video.
- ✓ Redes privadas virtuales (VPN).
- ✓ Internet y muchos más**.**

Los proveedores de servicios de internet tanto en el ámbito local como en el extranjero disponen de una red muy semejante a la elaborada en este diseño, donde se pueden distinguir diferentes equipos y funciones dentro de la red.

Tenemos una capa de Core, esta capa se la conoce como núcleo o BACKBONE de red donde se ubican equipos cuyas características son la conmutación a alta velocidad, interfaces de alto ancho de banda (10Gbps, 100Gbps). En estos equipos se utiliza la conmutación por intercambio de etiquetas (MPLS).

La capa de Acceso es la que se encarga de agregar todo el trafico de los clientes e interconectarlo con los equipos de CORE, los equipos de Acceso suelen tener pocas interfaces de alta velocidad, y muchas densidad de puertos de varias tecnologías y anchos de bandas (FRAME-RELAY, ATM, HSSI, SDH, POS, ETHERNET, etc.).

Para poder interconectar los equipos de Acceso con los de Core, veremos que no solo es necesario disponer de conexiones físicas, sino también se realizarán interconexiones mediante circuitos lógicos llamados túneles, en los que se podrán definir la ingeniería de tráfico (MPLS-TE) para poder establecer caminos principales, secundarios, balanceo de tráfico y conmutación de caminos ante fallos.

Una red de estas características debe disponer de un sistema de gestión, y monitorización que suelen ser en banda y/o fuera de banda, en este caso se va a especificar una red fuera de banda y una red de gestión en banda (por una VPN de gestión), la red de gestión fuera de banda se utilizará en caso de fallos por que se podrá seguir operando y gestionando los equipos de red.

5.1.1. Justificación del TFC

El presente trabajo se realiza para describir paso a paso cómo y por qué se utilizan varias tecnologías y protocolos de encaminamiento en una red WAN de ámbito internacional. Donde se tiene como objetivo ofrecer múltiples servicios en la red. Utilizando los conocimientos adquiridos durante el transcurso de la carrera ITTT y además con la experiencia teórica y práctica de más de 15 años trabajando en el sector de las telecomunicaciones en redes de diferentes ámbitos, hacen posible la elaboración de este trabajo.

5.1.2. Objetivos

El objetivo general de este proyecto es dar a conocer las pautas para diseñar una red WAN que permita transportar múltiples servicios, para ello se utilizará MPLS, y la ingeniería de tráfico MPLS-TE (Ingeniería de Tráfico). En general se pueden identificar cuatro diferentes objetivos a lo largo de todo este proyecto.

El primer objetivo específico es formar una sólida base teórica sobre MPLS y TE (Ingeniería de Tráfico), entendiendo la razón de su existencia, funcionamiento y utilización en este diseño.

El segundo objetivo es poder diferenciar el funcionamiento de cada equipo dentro de la red (si en un equipo de CORE, o Acceso) para una vez identificado situarlo e interconectarlo con el resto de equipos.

El tercer objetivo, completar el diseño de la red, con su direccionamiento IP, normas de ingeniería de tráfico, y definir el portfolio de servicios soportados.

Por último establecer los procedimientos para la operación, provisión y mantenimiento de la red. Mecanismos de alta disponibilidad y prueba ante fallos.

5.1.3. Enfoque y método seguido

El enfoque y método seguido corresponde a un proyecto de despliegue de una red, en este caso es una red WAN y que consta de diferentes fases:

- Definición del caso de estudio (Red WAN)
- Especificación de la RED
    - Justificación de tecnología
    - Selección de equipamiento
    - Funcionalidad y finalidad de la RED
    - Coste económico.
- Definición de servicios
- Plantillas para la operación y manteniendo

5.1.4. Planificación del proyecto

Para la planificación del proyecto se realizo un estudio de tareas a realizar, verificando cuales puede ser ejecutada en paralelo y cuales guardan cierta dependencia de otras tareas.

Una vez identificadas las tareas se utilizo la herramienta de Microsoft Project plasmar en un diagrama de Gantt el tiempo de dedicación previsto para diferentes tareas o actividades en las que se divide este proyecto.

Ver anexo 8.1 (Diagrama de Gantt).

5.1.5. Productos obtenidos (Listado de equipamiento, Diseño de red, Diseño red fuera de banda, Direccionamiento IP, Normas de Ingeniería y plantillas de configuración).

Direccionamiento IP (ver punto 5.3.4)

Normas de Ingeniería (ver punto 5.5.2 y 5.5.3)

Plantillas de configuración (ver punto 5.6.3)

5.1.6. Breve descripción de los otros capítulos de la memoria.

En los capítulos posteriores se especificará la funcionalidad y finalidad de la red, debido al diseño funcional, esta red puede ofrecer infinidad de servicios IP/MPLS.

Se podrá conocer el rol de cada equipo, la función que cumple y como puede crecer en capacidad y trafico. Conocer en detalles los protocolos de encaminamiento que se encargarán de garantizar el correcto funcionamiento de la red.

Los servicios son será uno de los capítulos más importantes pro que en el ese podrá conocer como son los servicios, los enlaces y las diferentes modalidades de acceso que se pueden ofrecer.

5.2.Funcionalidad y Finalidad de la red

En el presente documento se intenta definir cómo y por que es necesario realizar una red IP MPLS para que un operador de Telecomunicaciones pueda brindar servicios IP de extremo a extremo de forma confiable y segura.

Para poder ofrecer estos servicios es necesario que el diseño de red deba ser funcional y se adapte a las necesidades del operador, permitiendo ofrecer un amplio abanico de servicios a múltiples clientes.

Se puede decir que la red es funcional cuando se puede crecer en número de nodos sin tener que modificar su diseño. En este caso se utiliza un esquema que permite crecer con total libertad en cuanto a número de nodos.

En la red se definen 3 o 4 tipos de equipos según su función y rol que van a desempeñar. Se pueden resumir alguna de sus características funcionales de la siguiente manera:

- ✓ Equipos del Núcleo o CORE: Son equipos que están dotados de interfaces de alta capacidad y permiten el intercambio de tráfico a velocidad superior a los 100Gbps, con la agrupación de varios de estos interfaces se puede tener una capacidad entorno a Tbit/s (1000Gbps).

- ✓ Equipos de Acceso: Son aquellos equipos que estarán ubicados entre el CORE y los equipos de cliente (EDC) con interfaces de mediana velocidad, alta densidad de puertos y tarjetas de múltiples en laces y capacidad).Interfaces típicas de conexión serán 10Gbps, 1Gbps, 100Mbps, E1, T1, E3, T3, RDSI, etc. **(En la sección 4.6.1 se amplía la información respecto a los tipos de enlaces)**

- ✓ Equipos de cliente: Son aquellos que se utilizan para interconectar los clientes con la red del proveedor de servicios por lo general estos equipos disponen de tarjetas WAN (Ethernet, FRAME-RELAY, ATM, RDSI, serial) para interconectarse con el proveedor del servicio y de una o varias interfaces LAN de mayor velocidad para proveer la conectividad a nivel local en las dependencias del cliente.

La finalidad de la red es permitir la interconexión de la mayor cantidad de clientes, desde su sedes remotas garantizando la prestación de los servicios extremo a extremo.

5.3.Diseño de red

5.3.1.Función de los equipos de red

Los equipos de red se suelen dimensionar de acuerdo a la función que van a cumplir en la red. En este caso se van a definir 3 tipos de equipos de red.

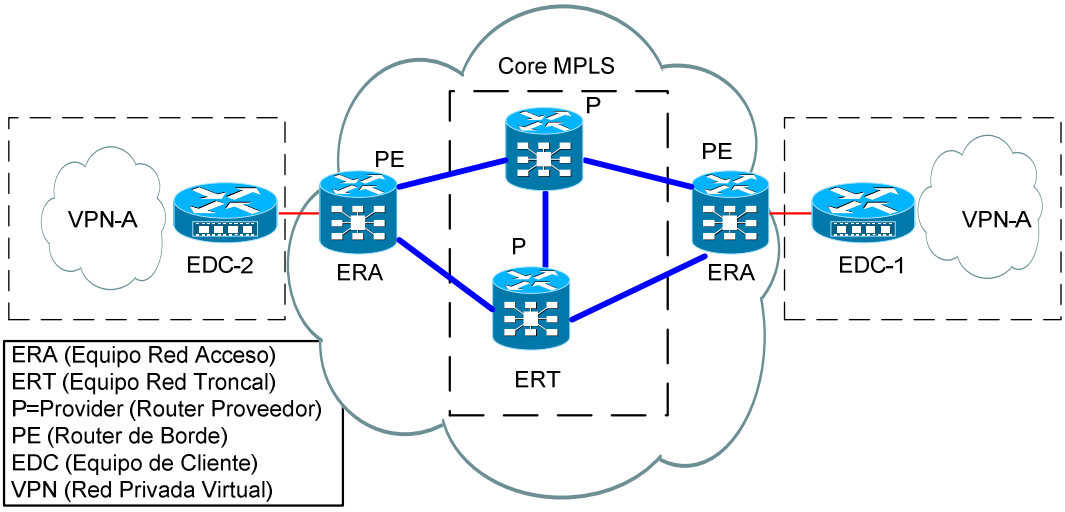


Figura: 1 Función de los equipos de Red

Equipos de Red Troncal: son aquellos equipos que estarán ubicados en el CORE o en el Backbone MPLS de la red, dentro de la nomenclatura de MPLS se los conoce P (Provider). Es un equipo cuyas características son: Interfaces de gran velocidad y ancho de banda.

Equipos de Red Acceso: son aquellos equipos que estarán ubicados entre el CORE y los equipos de cliente (EDC), dentro de la nomenclatura de MPLS se los conoce PE (Provider Edge). Es un equipo cuyas características son: Interfaces de mediana velocidad, tarjetas de múltiples en laces y ancho de banda).

Equipos de Red Gestión: son los equipos dedicados para acceso remoto mediante la utilización de un cable de consola que conecta directamente a los equipos ERT, ERA, permitiendo el acceso a estos por la red de gestión (VPN dedicada para gestión de equipos en banda o por la propia red).

También pueden garantizar el acceso mediante la utilización de una red (fuera de banda o por equipos diferentes y de otros proveedores) que garantizan una conexión de respaldo ante el fallo en nuestra propia red. La única finalidad de estos equipos es garantizar el acceso remoto a los equipos ERT, ERA ubicado en los CPD de los diferentes países.

Es un equipo cuyas características son: Interfaces baja velocidad, con acceso mediante RDSI y/o 3G para conexiones esporádicas en cado de pérdida de gestión de los equipos).

(En la sección 4.3.3.3 se muestra el tipo de conexión por consola utilizado y en la sesión 4.3.6 se detalla la red de gestión).

Equipos de Cliente (EDC): son aquellos equipos que pueden o no ser gestionados por el cliente, por lo general estos equipos disponen de tarjetas WAN (Ethernet, FRAME-RELAY, ATM, RDSI, serial) para interconectarse con la Red, y una o varias interfaces LAN de mayor velocidad (Giga bit Ethernet).

5.3.2. Elección y justificación de la tecnología a utilizar.

En la actualizad existen muchos y diferentes protocolos de encaminamiento que se podrían utilizar en una red IP/MPLS, desde el punto de vista de facilidad de manejo, escalabilidad, y tiempo de convergencia se utilizará el protocolo ISIS en el CORE de la red, LDP para la distribución e intercambio de etiquetas MPLS, y BGP para establecer las sesiones BGP entre los equipos PE de la red.

A continuación se definen las interfaces de Red de los equipos troncales (interconexión de equipos ERT), interfaces de los equipos de acceso (interconexión con equipos de cliente).

5.3.2.1. Protocolos de encaminamiento.

De los protocolos de encaminamiento disponible se decide utilizar IS-IS ya que es un protocolo de enrutamiento definido por la IETF , comúnmente utilizado en grande proveedores de servicios de internet (ISP) por su rápida convergencia y excelente escalabilidad, utiliza el algoritmo de SPF (Shortest Path First), es de los protocolos llamados link state (estado del enlace), estos protocolos se basan en la construcción de una mapa topológico de la red, conociendo exactamente el valor de cada enlace, permitiendo establecer múltiples caminos redundantes entre un origen y un destino concreto.

A diferencia de otros protocolos de estado de enlace ISIS opera en la capa 2 del modelo OSI.

Un mismo enrutador puede ejecutar múltiples instancias del protocolo de encaminamiento IS-IS cada uno de ellos se diferencia por un etiqueta o TAG.

Como se puede observar en la figura todos los equipos de red utilizan el protocolo de encaminamiento ISIS, tanto en los equipos de acceso como en los equipos del CORE.

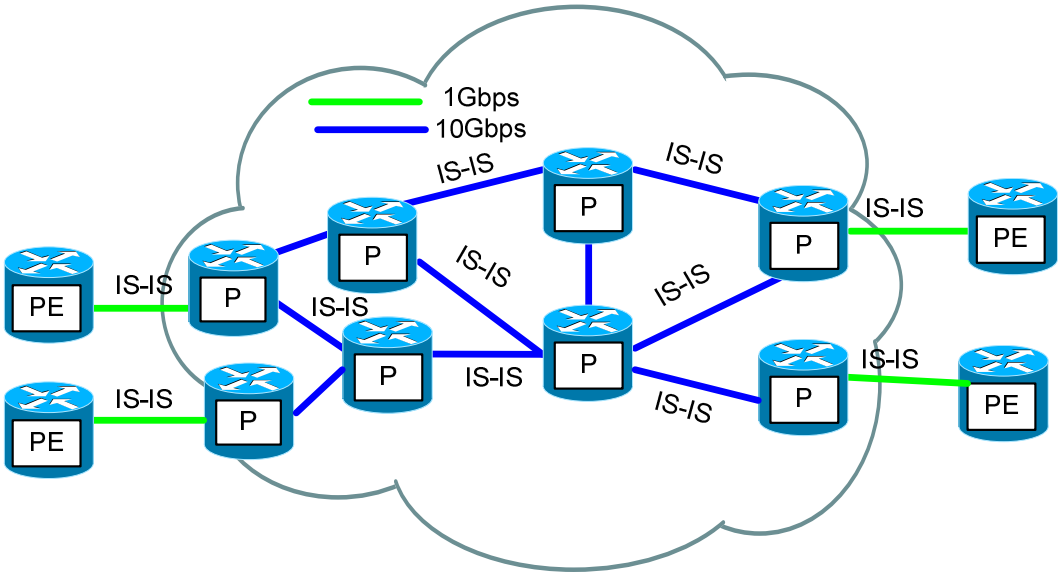


Figura: 2 Funcionamiento IS-IS

De esta manera cada equipo de la red tendrá un mapa topológico de toda la red, conociendo los caminos redundantes (aquellos que tienen un mismo coste desde un origen a un destino), y el estado de cada enlace, para que en caso de fallo de un enlace o la caída de un equipo el resto de equipos pueden re calcular el mapa topológico en cuestión de segundos, y de forma independiente.

Para la comunicación entre sistemas autónomos y/o para la comunicación entre VPN se utilizará el protocolo BGP, cuya función principal será intercambiar información en la red mediante el establecimiento de una sesión de comunicación entre los enrutadores de borde. BGP posee numerosos atributos que permiten la gestión o manipulación de tráfico de acuerdo a ciertos atributos, gracias a estos se puede definir diferentes políticas para el tráfico saliente y para el entrante.

La selección de rutas o caminos se puede hacer mediante la selección o manipulación de redes o rango de redes para poder escoger algunas como preferidas o principales, y propagar o anunciar algunas con métricas peores para que sean descartadas o marcadas como de respaldo.

Para ello se cuenta con un conjunto de atributos que dan información para la toma de decisión para filtrar o seleccionar rutas. Se definen a continuación dichos atributos:

- **ORIGIN**: Identifica el mecanismo por el cual se anunció el prefijo IP por primera vez. Se puede especificar como IGP (0), EGP (1) o INCOMPLETE (2). IGP indica que el prefijo IP se aprendió por un protocolo interior al sistema autónomo. EGP indica que el prefijo IP se aprendió por un protocolo exterior como podría ser BGP, por ejemplo puede ser debido a que se ha realizado agregación. Generalmente si el ORIGIN es INCOMPLETE es porque se ha aprendido de forma estática.

- **AS-PATH:** Este atributo almacena una secuencia de números de AS que identifican la ruta de los sistemas autónomos por los que ha pasado el anuncio. Cada vez que un enrutador de borde propaga una ruta hacia otro lado añade a este atributo su número de AS constituyendo así la lista de sistemas autónomos

- **NEXT-HOP:** Identifica la dirección IP del enrutador correspondiente al siguiente salto hacia el destino. Se debe tener en cuenta que un prefijo IP se anuncia fuera de un sistema autónomo, por lo que el next-hop es el destino que se conoce y al que hay que enviar el tráfico de los usuarios que quieran llegar a un destino final. En este caso los next-hop serán los PE de la red.

- **MULTI-EXIT-DISCRIMINATOR (MED):** Es utilizado cuando desde un sistema autónomo existen múltiples enlaces hacia un mismo sistema autónomo. Sirve para influir y elegir un camino con respecto a otro. Si se quisiera seleccionar una ruta por medio de este atributo se consideraría preferida la que tuviese un valor de MED menor.

- **LOCAL-PREF:** Este atributo dará preferencia al envío de tráfico por un enlace en concreto, por tanto solo tendrá sentido dentro de un mismo sistema autónomo, luego solo se transmite por IBGP. Se escogerá el envío de datos por el enlace que tenga un LOCAL-PREF más alto, siendo el LOCAL-PREF por defecto de valor 100.

- **COMMUNITY:** Se puede gestionar la distribución de información de ruteo a un grupo de destinatarios llamados COMMUNITIES. Existen diferentes tipos de communities, que permiten la ejecución de MP-BGP (Multi Protocol Border Gateway Protocol)

El proceso de decisión de BGP para determinar que ruta es preferente, debido a que todos los atributos pueden ser utilizados conjuntamente para el anuncio y manipulación de rutas, es por eso que debe existir el siguiente criterio para la selección de rutas,

1. Si el siguiente NEXT-HOP no está disponible se ignora la ruta.
2. Las rutas con menor LOCAL-PREF.
3. Las rutas con AS-PATH más largo.
4. Las rutas con ORIGIN más alto.
5. Las rutas con mayor MED.
6. Las rutas aprendidas por IBGP si las hay aprendidas por EBGP.
7. Las rutas con mayor coste hacia el NEXT-HOP.
8. Preferir la ruta que ha anunciado el router con menor identificador BGP (BGP ID).
9. Preferir la ruta recibida desde el interfaz con menor dirección para el vecino.

En la figura 3 se puede observar diferentes redes virtuales privadas (VPN-Green, VPN-Blue, VPN-Orange), para poder permitir la interconexión entre los PE's se establecen las sesiones IBGP, así de esta manera mediante los atributos de BGP como por ejemplo las community se puede establecer relaciones de redes y agruparlas todas en una misma tabla de encaminamiento perteneciente a una misma VPN.

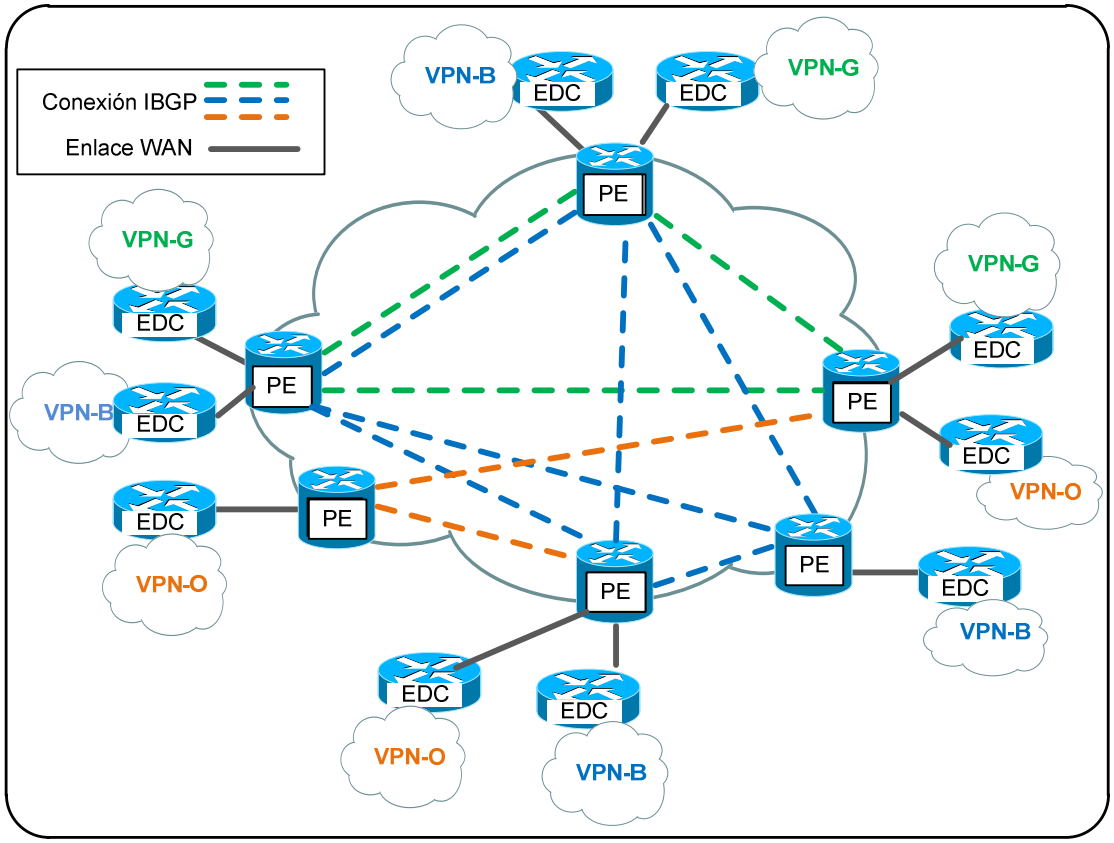


Figura: 3 Ejemplo de VPN

Como se puede apreciar en la figura 3 si una red contiene varias decenas de PE será necesario establecer una sesión BGP entre cada uno de ellos, digamos que si tenemos N PE el número de sesiones será N(N-1) con 60 equipos serán necesario configurar y establecer 3560 sesiones BGP Lo que se conoce como un full-mesh, lo que resulta muy difícil de manejar para evitar tener que crear y mantener tanta sesiones BGP, se utiliza uno o varios reflectores de rutas (es un equipo de la red que se encarga de establecer un única sesión BGP con cada PE para intercambiar todo cambio en las tablas BGP).

En la figura 4 se puede observar cómo se limita de forma considerable el número de sesiones BGP.

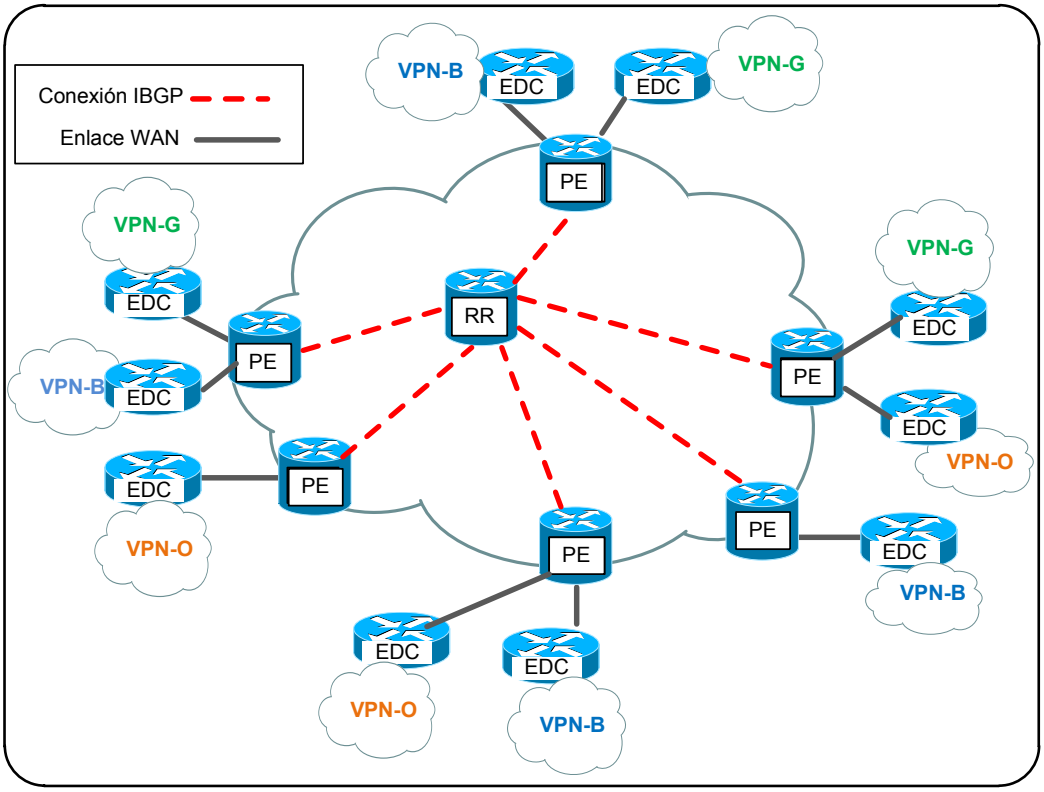


Figura: 4 Utilización de Reflector de Rutas

5.3.2.2. MPLS.

Está muy claro que MPLS es la tecnológica a utilizar como medio de transporte dentro del CORE de la red las ventajas que ofrece son:

- ✓ Reducción de costes (utilización de una infraestructura de red común).
- ✓ Mejor integración con antiguas tecnologías (ATM, FR, etc.).
- ✓ Un CORE de red rápido y robusto (Envío de tráfico basado en etiquetas).
- ✓ Fácil implementación de servicios IP (VOIP, Video, VPN, multicast).

MPLS (Multi Protocol Label switching) es un estándar creado por la IETF para definir el transporte de datos para redes basadas en la conmutación de circuitos y la conmutación de paquetes. Opera entre la capa de transporte y la capa de red del modelo OSI (normativa o estándar formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones).

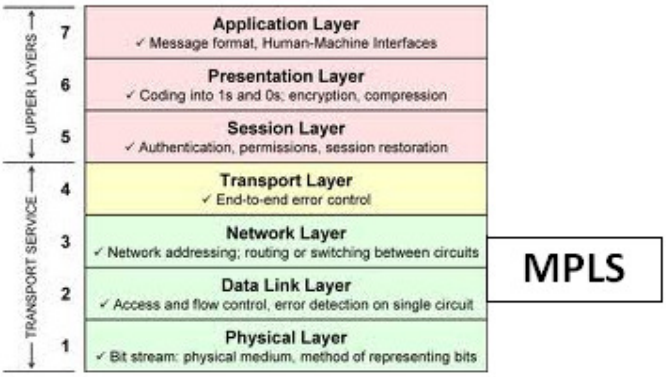


Figura: 5 MPLS en el modelo OSI

Una de las principales ventajas que tiene MPLS al operar entre la capa 2 y la capa 3 del modelo OSI, permite el intercambio de etiquetas en lugar de direcciones IP. Este intercambio se realiza en hardware realizándose a una velocidad muy alta. Al no poseer o no manejar direcciones puede transportar cualquier tipo de protocolo ya que permite etiquetar las tramas de nivel 2 (ATM, FR, Ethernet).

Los beneficios de utilizar MPLS en la red son:

La utilización de una infraestructura común y única: Al utilizar MPLS con IP no existe limitación con respecto al tipo de tecnología de nivel 2 (ATM, Frame Relay, HDLC, PPP, etc.) que se puede transportar por el core de la red. La técnica de etiquetar cualquier protocolo de nivel sobre MPLS se llama AToM (AnyTransport over MPLS). Esto permite ofrecer un servicio extremo a extremo independientemente del nivel 2 del enlace, utilizando una infraestructura común para su transporte.

Mejor integración de IP con ATM: En un principio se utilizo la RFC 1483 “Multiprotocol Encapsulation over ATM Adaptation Layer 5”, pero este estándar especificaba como configurar manualmente todas las interconexiones entre IP y los circuitos ATM. Por lo complejo en la

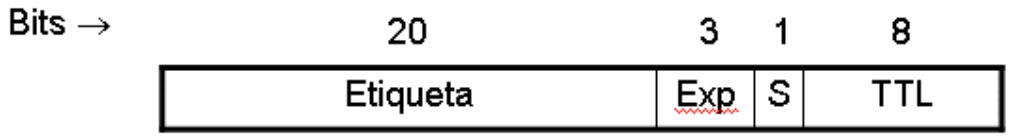
operación y el mantenimiento, se desarrollo otro método más dinámico como el de LAN Emulation (LANE), aun así fue muy popular en los equipos de Edge (equipo que agrega de equipos de cliente), pero no resulto ser muy estable y confiable para grandes proveedores de servicios. Finalmente Multiprotocol Over ATM (MPOA) fue la solución más utilizada pero continuaba siendo compleja de desplegar y manejar.

Tener un Core de Red sin BGP (solo se intercambian etiquetas): Siempre que se tiene que realizar el enrutamiento en los equipos de red se debe consultar la tabla de enrutamiento para determinar por qué interface encaminar el paquete a un destino determinado. Solamente los equipos del borde tendrán que ejecutar el protocolo BGP, para poder tener actualizada su tabla de enrutamiento global. Los equipos de Core solo intercambiarán etiquetas contra los equipos de borde sin necesidad de ejecutar el protocolo BGP, entonces no se verán afectados por los continuos cambios en la topología de red.

Modelo de MPLS VPN/VRF: El uso masivo de MPLS facilito el desarrollo de redes virtuales privadas (VPN). Este tipo de servicio permite la interconexión de redes de clientes. En la que un mismo equipo puede tener varias tablas virtuales de encaminamiento (VRF), digamos que tendrá una tabla de encaminamiento por VRF. De esta manera se puede utilizar un mismo equipo e interface para interconectar diferentes clientes, manteniendo separara la información correspondiente al encaminamiento, incluso varios clientes pueden compartir el mismo direccionamiento IP.

Arquitectura MPLS

MPLS (MultiProtocolLabelSwitching) Conmutación múltiple protocolo mediante etiquetas, una etiqueta MPLS tiene el siguiente formato de 4Bytes:



20 bits se utilizan para la etiqueta (valor numérico desde 0 hasta 1048572.
3 bits corresponden a los bits experimentales relacionados con la calidad de servicio (QoS).
1 Bit corresponde (0 para todas las etiquetas y 1 solo cuando se trata de una etiqueta final.
8 bits corresponden al tiempo de vida del paquete (TTL).

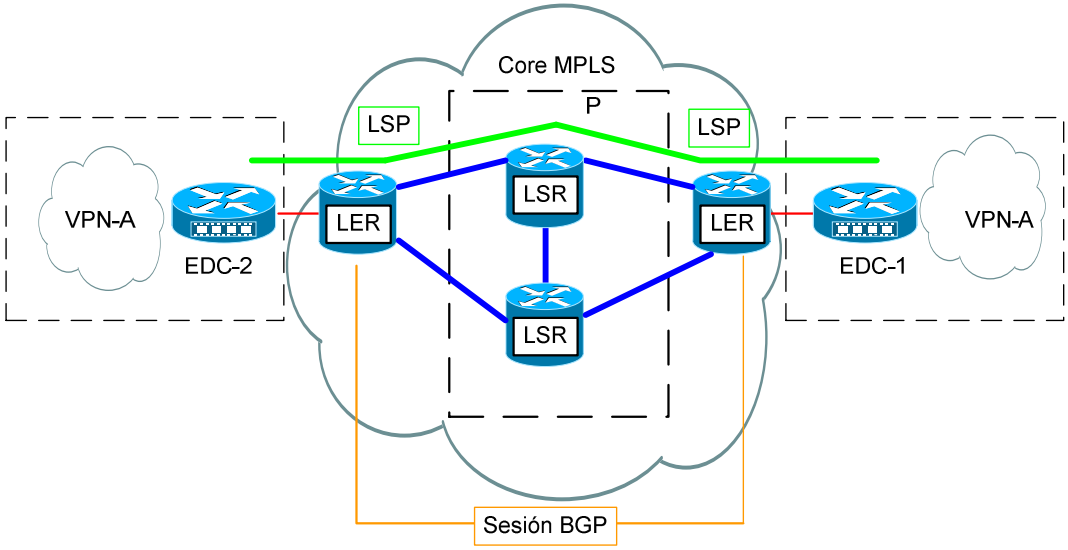


Figura: 6 Elementos de MPLS

Elementos de MPLS

- **LER (Label Edge Router):** elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router.
- **LSR (Label Switching Router):** elemento que conmuta etiquetas.
- **LSP (Label Switched Path):** nombre genérico de un camino MPLS (para cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. A tener en cuenta que un LSP es unidireccional.
- **LDP (Label Distribution Protocol):** un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- **FEC (Forwarding Equivalence Class):** nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

5.3.2.3. Definición de ingeniería de tráfico

Se conoce como ingeniería de tráfico, a la forma de dirigir el tráfico por la red, estableciendo circuitos virtuales para poder interconectar equipos de un extremo (PE) a otro extremo (PE) de la manera más óptima posible.

Para poder determinar el camino optimo, los protocolos de encaminamiento, disponen de métricas y costos asociados a los enlaces mediante la acumulación de estos costos se determina el mejor camino entre un origen y un destino. En general se suelen utilizar protocolos de encaminamiento que conocen el estado de los enlaces, y disponen un mapa general de toda la red estos protocolos son los llamados link-state (disponen de un tiempo de convergencia mucho menor).

Para poder establecer los TE-LSP (Túneles con ingeniería de tráfico) se utilizará el protocolo IS-IS, es un protocolo link-state. Se utiliza un protocolo de encaminamiento para poder mantener la topología de la red.

Para ello se crean LSP (Label Switched Path), que es un túnel lógico que atraviesa N conexiones físicas, se puede crear el LSP de forma dinámica, mediante la reserva de ancho de banda con el protocolo RSVP, o también se puede realizar de forma estática.

Según los requerimientos del servicio, se pueden utilizar un mismo TE-LSP para todos los servicios entre un origen y destino, o se pueden crear varios TE-LSP para servicios específicos entre un mismo origen y destino. Como así también se pueden tener varios TE-LSP con métrica igual para realizar el balanceo del tráfico.

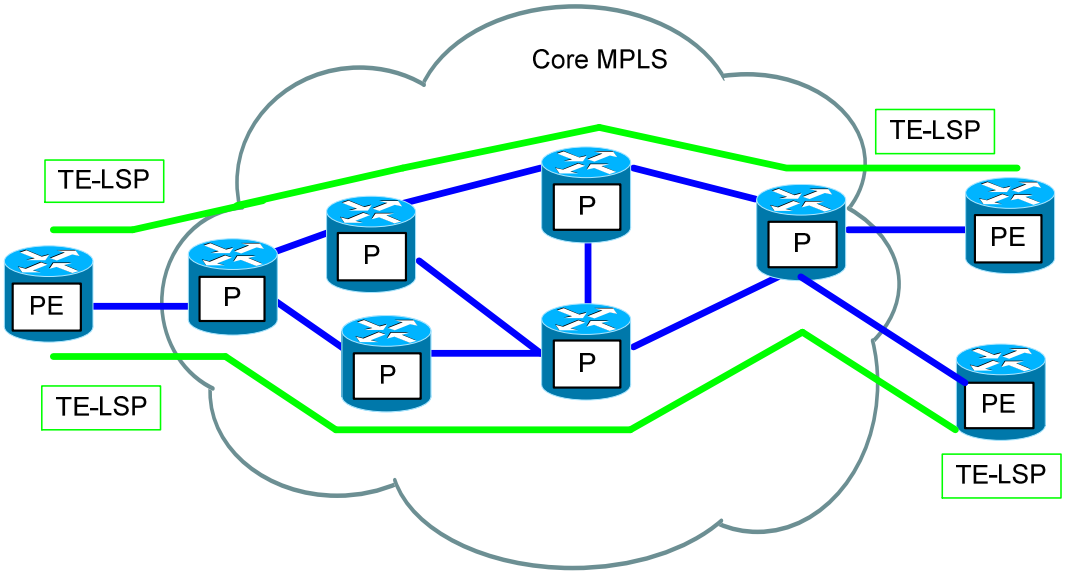


Figura: 7 Ejemplo TE_LSP

5.3.3. Elección de equipo según función.

5.3.3.1. Equipos de CORE

Para elegir los equipos de CORE tenemos varias opciones, pero voy a sugerir dos fabricantes que están presentes en la mayoría de los operadores de red. Ellos son Cisco y Juniper, el ámbito de este proyecto no es hacer una comparación exhaustiva en cuanto a performance.

Para los equipos de CORE se elige el equipo Carrier Class Routing (CRS) de Cisco modelo CRS-3 de 8 slots (si bien existen soluciones multi-chasis, no se tendrán en cuenta), dentro de las características se puede citar el tipo de interfaces disponibles para la conectividad.

- 1-port OC-768c/STM-256c packet over SONET (PoS)
- 4-port OC-192c/STM-64c PoS/Dynamic Packet Transport (DPT)
- 4/8-port 10 GE
- 1-port OC-768c/STM-256c Tunable WDMPoS
- 4-port 10 GE tunable WDMPHY
- 14/20-port 10 GE LAN/WAN PHY
- 1-port 100 GE
- Cisco CRS-1-SIP-800 Carrier Card
- 1-port OC-192c/STM-64c PoS/RPR SPA
- 1-port 10 GE SPA
- 2-port and 4-port Clear Channel T3/E3 SPAs
- 2-port, 4-port, and 8-port OC-12c/STM-4 PoS SPAs
- 1-port 10 GE LAN/WAN-PHY SPA

Performance	2.24-Tbps switching capacity
Conectividad	PoS, WDM, DPT, T3/E3, 100 GE, 10 GE, 1 GE
Fiabilidad y Disponibilidad	System redundancy: • Power-shelf redundancy 1:1 • Fan-tray redundancy 1:1 • Route-processor redundancy 1:1 • Fabric-card redundancy 1:4 • Dual homing with line cards • Support for APS Software features: • NSF using graceful restart for: IS-IS, OSPF, BGP, LDP, and RSVP • SONET APS 1:1 • Line-card OIR support • Fabric-card OIR support • Out-of-resource management • Process restartability • MPLS Fast Reroute (FRR) • Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP)

En cuanto al equipo para la red Troncal del fabricante Juniper, se elige el modelo T1600 de la serie T Core Network Routers (si bien existen soluciones multi-chasis, no se tendrán en cuenta). Dentro de las opciones de conectividad podemos citar:

- oC-192c/STM-64, 1-port
- oC-192c/STM-64, 1 and 4 port
- oC-12/STM-4, 1-port
- oC-3/STM-1
- 1-Gigabit Ethernet, 2-port SFP
- 1-Gigabit Ethernet, 4-port SFP
- 1-Gigabit Ethernet, 10-port SFP
- 10-Gigabit Ethernet, 1-port xenPaK
- 10-Gigabit Ethernet, 1-port dWdM
- 10-Gigabit Ethernet, 4-port xFP
- 1 100Gbps port
- dS3, 4-port
- e3 iQ, 4-port

T Series Core Network Routers

Performance	2.24-Tbps switching capacity
Conectividad	PoS, WDM, DPT, T3/E3, 100 GE, 40 GE, 10 GE, 1 GE
Fiabilidad y Disponibilidad	System redundancy: • Power-shelf redundancy 1:1 • Fan-tray redundancy 1:1 • Route-processor redundancy 1:1 • Fabric-card redundancy 1:4 • Dual homing with line cards • Software features: • Protocols IS-IS, OSPF, BGP, LDP, and RSVP • Line-card OIR support • Fabric-card OIR support • Process restart ability • MPLS Fast Reroute (FRR) • Virtual Router Redundancy Protocol (VRRP)

5.3.3.2. Equipos de Acceso.

Para elegir los equipos de Acceso se debe tener en cuenta que estos equipos deben tener múltiples tarjetas para poder realizar la agregación de todo tipo de tecnologías como ser (FRAME-RELAY, ATM, FastEthernet, Giga bit Ethernet, E1, E3, T1, T3, ISDN, etc.), por lo que deben poseer gran densidad de puertos y slots en los que se puedan insertar tarjetas de forma modular de acuerdo a las necesidades. Se eligen dos fabricantes que están presentes en la mayoría de los operadores de red, es conveniente disponer de más de un fabricante para garantizar una plataforma de red que no sea dependiente de una tecnología y orientada a conexiones estándar sin utilizar ningún tipo de protocolo o solución propietaria de un fabricante. Los fabricantes elegidos son Cisco y Juniper.

EL equipo seleccionado del fabricante Cisco es el 7600 (Aggregation Services Routers) de 10 slots. Dentro de las características se puede citar el tipo de interfaces disponibles para la conectividad.

Cisco 7613 System Features

- Total throughput: 720 Gbps
- Up to 400-Mpps distributed forwarding rate

- Slots 5 y 6 se utilizan para las tarjetas supervisoras.
- 11 slots restantes (se utilizan para tarjetas de líneas).

- SIP-200, SIP-400 y SIP-600 (SPA interface processors) Soporte para tarjetas modulares

SIP-400

A continuación se pueden observar el total de tarjetas de puertos (SPA) disponibles para insertar en la SIP-200, SIP-400, o SIP-600 cada una de estas SIP's utiliza 1 slot.

SIP-200	**ATM** • Cisco 2-Port OC-3c/STM-1c ATM Shared Port Adapter • Cisco 4-Port OC-3c/STM-1c ATM Shared Port Adapter POS/Channelized • Cisco 2-Port OC-3c/STM-1c POS Shared Port Adapter • Cisco 4-Port OC-3c/STM-1c POS Shared Port Adapter • Cisco 1-Port Channelized OC-3c/STM-1c POS Shared Port Adapter **Copper/Channelized** • Cisco 8-Port Channelized T1/E1 Shared Port Adapter • Cisco 2-Port Clear Channel T3/E3 Shared Port Adapter • Cisco 4-Port Clear Channel T3/E3 Shared Port Adapter • Cisco 2-Port Channelized T3 (DS0) Shared Port Adapter • Cisco 4-Port Channelized T3 (DS0) Shared Port Adapter • Cisco 4-Port Serial Shared Port Adapter **Fast Ethernet** • Cisco 4-Port Fast Ethernet Shared Port Adapter • Cisco 8-Port Fast Ethernet Shared Port Adapter
SIP-400	**Ethernet** • 2-port 1 GE SPA (V1 and V2) • 5 port 1 GE SPA (V2 only) • 1-port 10GbE SPA LAN PHY (V2 only) **ATM** • Cisco 2-Port OC-3c/STM-1c ATM SPA • Cisco 4-Port OC-3c/STM-1c ATM SPA • Cisco 1-Port OC-12c/STM-4c ATM SPA • Cisco 1-port OC48/STM16 ATM SPA **POS** • Cisco 2-Port OC-3c/STM-1c POS SPA • Cisco 4-Port OC-3c/STM-1c POS SPA • Cisco 1-Port OC-12c/STM-4c POS SPA • Cisco 1-Port OC-48/STM16-c POS/RPR SPA (POS mode only) **Serial/Channelized** • Cisco 8-port Channelized T1/E1 SPA • Cisco 2-port Channelized T3 to DS0 SPA • Cisco 4-port Channelized T3 to DS0 SPA • Cisco 2-port T3/E3 Serial SPA • Cisco 4-port T3/E3 Serial SPA • Cisco 1-port Channelized STM1/OC3 to DS0 SPA **CEoP/Channelized ATM SPA** • Cisco 24-port T1/E1 Circuit Emulation over Packet SPA (CEoP) • Cisco 1-port OC-3/STM-1 Circuit Emulation over Packet SPA • Cisco 2 port channelized T3 Circuit Emulation and channelized ATM SPA[1]
SIP-600	• Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter (pluggable IEEE LAN PHY XFP optics) • Cisco 10-Port Gigabit Ethernet Shared Port Adapter (SFP pluggable optics) • Cisco 5-Port Gigabit Ethernet Shared Port Adapter (SFP pluggable optics) • Cisco 1-Port OC-192/STM-64 POS Shared Port Adapter (XFP pluggable optics) • Cisco 1-Port OC-192/STM-64 POS Shared Port Adapter (long-reach fixed optics)

En cuanto al fabricante Juniper la elección corresponde a MX960 3D Universal Edge Router:

MX960 System Features

• Total throughput: 1,320 Gbps

- Slots 6 y76 se utilizan para las tarjetas supervisoras RSP.
- 12 slots restantes (se utilizan para tarjetas de líneas).
- Una FPC (Flexible PIC Concentrators) ocupa 2 slots
- FPC Soporta diferentes PIC Soporte para tarjetas modulares

FPC

A continuación se pueden observar el total de tarjetas de puertos (PICs) disponibles para insertar en las FPCs.

FPC	**Channelized OC12/STM4 Enhanced IQ (IQE) PIC with SFP** • PB-4CHOC12-STM4-IQE-SFP **Channelized OC48/STM16 Enhanced IQ (IQE) PIC with SFP** • PB-1CHOC48-STM16-IQE **SONET/SDH PICs** **SONET/SDH OC3/STM1 (Multi-Rate) PIC with SFP** • PB-4OC3-1OC12-SON2-SFP **SONET/SDH OC12/STM4 (Multi-Rate) PIC with SFP** • PB-4OC3-4OC12-SON-SFP **SONET/SDH OC48/STM16 Enhanced IQ (IQE) PIC with SFP** • PC-4OC48-STM16-IQE-SFP **SONET/SDH OC48/STM16 (Multi-Rate) PIC with SFP** • PB-1OC48-SON-B-SFP **SONET/SDH OC48/STM16 PIC with SFP** • PC-4OC48-SON-SFP **SONET/SDH OC192c/STM64 PIC** • PC-1OC192-SON-VSR **SONET/SDH OC192c/STM64 PIC with XFP** • PC-1OC192-SON-XFP

5.3.3.3. Equipos de Gestión.

Los requisitos para la elección de los equipos de Gestión son soporte a nivel mundial, recambio de piezas en 4hs, conexión mediante RDSI, y/o 3G. Estos equipos se utilizan como servidor de consolas (Conexión asíncrona RS232 con las consolas de los equipos), para acceso remoto y gestión de los equipo fuera de banda.

Figura: 8 cable asíncrono 8 puertos y HWIC-16A

No se necesitan características especiales en cuanto a la capacidad de tráfico, debido a que ancho de banda de la gestión fuera de banda se realizará por una interface RDSI.

5.3.4. Direccionamiento IP

El direccionamiento IP se va a dividir en 2 partes, la parte pública y la parte privada.

La parte publica será la que se utilice para la direcciones IP de los equipos de Red, es importante tener en cuenta la necesidad de que estas direcciones deben ser públicas para evitar el solapamiento del direccionamiento IP de otros proveedores

- Para las interfaces loopbacks (interface lógica que siempre permanece activa)
- Para las interfaces punto a punto (para establecer las interconexiones entre los equipos).
- Para los túneles TE-LSP (LSP de ingeniería de tráfico).
- Para la sesiones BGP Full mesh (interface Loopback 1)

Dirección	Mascara	Descripción	Utilización
200.200.0.0	255.255.254.0	Gestión Loopback 0	Gestión de Equipos
200.200.2.0	255.255.254.0	Reservado Uso Futuro	
200.200.4.0	255.255.254.0	Gestión Loopback 1	Conexión BGP
200.200.6.0	255.255.254.0	Reservado Uso Futuro	
200.200.8.0	255.255.254.0	Reservado Uso Futuro	
Dirección	**Mascara**	**Descripción**	**Utilización**
200.200.10.0	255.255.255.252	IP's TE (túnel TE-LSP)	
200.200.11.0	255.255.255.252	IP's TE (túnel TE-LSP)	
200.200.12.0	255.255.255.252	IP's TE (túnel TE-LSP)	
200.200.13.0	255.255.255.252	Reservado Uso Futuro	
200.200.14.0	255.255.255.252	Reservado Uso Futuro	
Dirección	**Mascara**	**Descripción**	**Utilización**
200.200.15.0	255.255.255.252	Conexión Punto a Punto	
200.200.16.0	255.255.255.252	Conexión Punto a Punto	
200.200.17.0	255.255.255.252	Conexión Punto a Punto	
200.200.18.0	255.255.255.252	Conexión Punto a Punto	
200.200.19.0	255.255.255.252	Conexión Punto a Punto	

El siguiente mapa de red pretende esquematizar un breve resumen del direccionamiento y como este se deberá configurar en los equipos de red. Donde se puede observar lo siguiente:

- Direccionamiento IP para la conexión Punto a Punto 200.200.15.0/30 correspondiente a la interconexión entre el PE y el P
- Direccionamiento IP de las loopbacks 0 (para gestión de los equipos)
- Direccionamiento IP para el túnel TE-LSP entre 2 PE de la red (200.200.10.0/30 y 200.200.10.4/30)

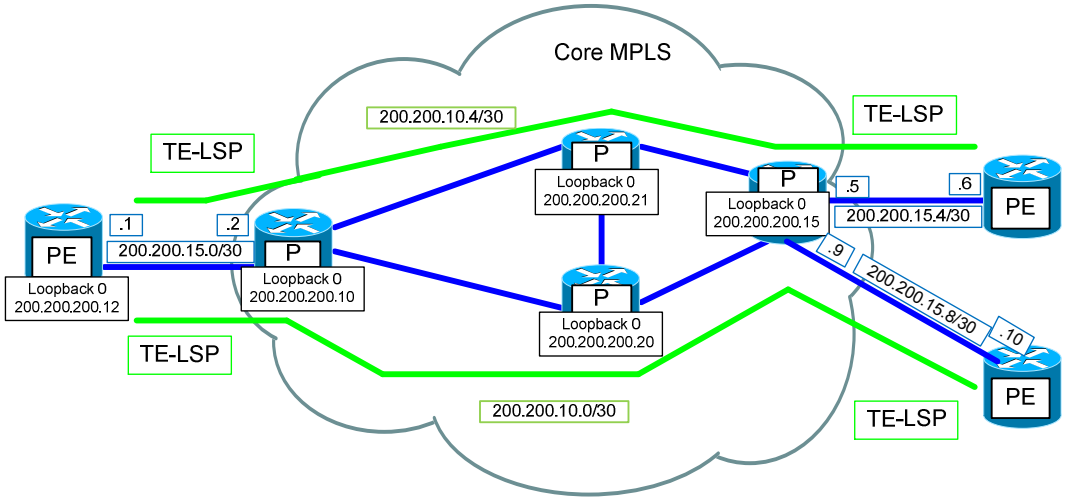


Figura: 9 Ejemplo direccionamiento publico

El direccionamiento privado se utiliza para la interconexión entre los PE de la red y los equipos de clientes (EDC's).

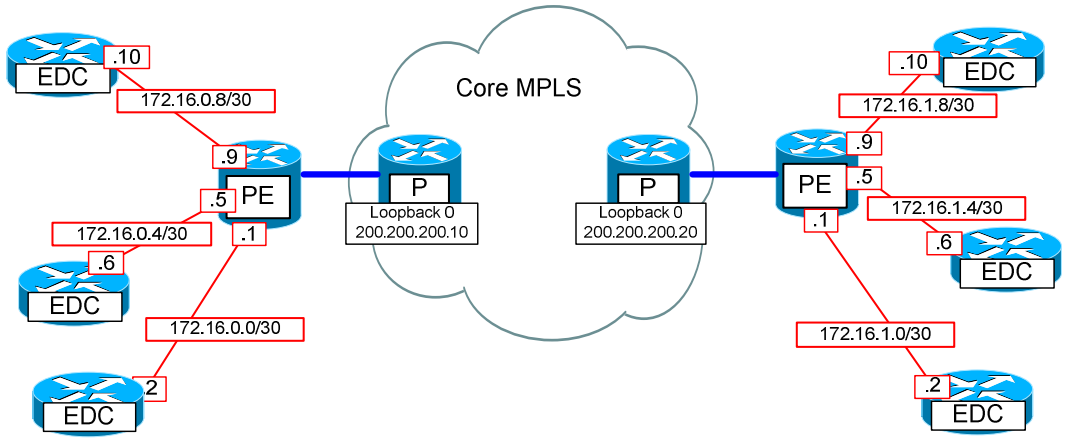


Figura: 10 Ejemplo direccionamiento Privad

5.3.5. Identificación de nombre de equipos

Para poder reconocer unívocamente los equipos de red, se debe crear una regla nemotécnica para definir el nombre de cada equipo dependiendo de su función (si es de un equipo de Gestión, de Acceso o Troncal). Para los equipos de cliente no se especifica ninguna regla ya que muchas veces estos son gestionados por otros.

La nomenclatura que utilizaremos será la siguiente:
ERAXXXNNYY **ERA** indica que es un **E**quipo de **R**ed **A**cceso
ERTXXXNNYY **ERT** indica que es un **E**quipo de **R**ed **T**roncal
ERGXXXNNYY **ERG** indica que es un **E**quipo de **R**ed **G**estion

XXX corresponde a la Ciudad (ej. PAR = Paris; BUE=Buenos Aires; BCN=Barcelona)
NN corresponde al housing o Centro de Datos (ej.NA =NAP Américas; IX=Interxion)
YY corresponde al número de equipo en el lugar (orden ascendente).

Por ejemplo para identificar unívocamente el primer equipo Troncal situado en el NAP de MIAMI sería **ERTMIANA01**, uno en Buenos Aires, en el data Center de Barracas correspondiente a la red de acceso sería **ERABUEBA01,** por ultimo si existe por lo menos 2 equipo de gestión de red, en Madrid en la central de Atocha nuevo equipo a instalar tendría la nomenclatura **ERGMADAT03.**

5.3.6. Diseño de red fuera de banda y vpn de gestión en banda

La finalidad de la red fuera de banda es garantizar conectividad (acceso remoto a los equipos) incluso ante fallos en la red o una incomunicación total. Para ello se debe utilizar una infraestructura de red alternativa (ya sea dedicada o por conexión de terceros) para tener siempre un acceso disponible a los equipos, ya sea por el direccionamiento de gestión o una conexión directa por consola).

Existen equipos específicos para permitir el acceso remoto por consola y se los denomina servidores de consola. Estos equipos suelen contar con una interface (RDSI, y/o 3G, o ADSL) con un direccionamiento IP publico accesible desde cualquier red y una serie de puertos de conexión asíncrona RS232 con las consolas de los equipos a ser gestionados.

Como se puede observar una Red típica de gestión fuera de banda, consta de una interconexión de los nodos de red (mediante el uso de una red específica, dedicada y diferente a la infraestructura a gestionar (en este caso se plante una red RDSI de cobertura internacional), y en cada CPD un equipo de gestión de los denominadas ERG, que hace sirve de interconexión entre la red RDSI y los equipos.

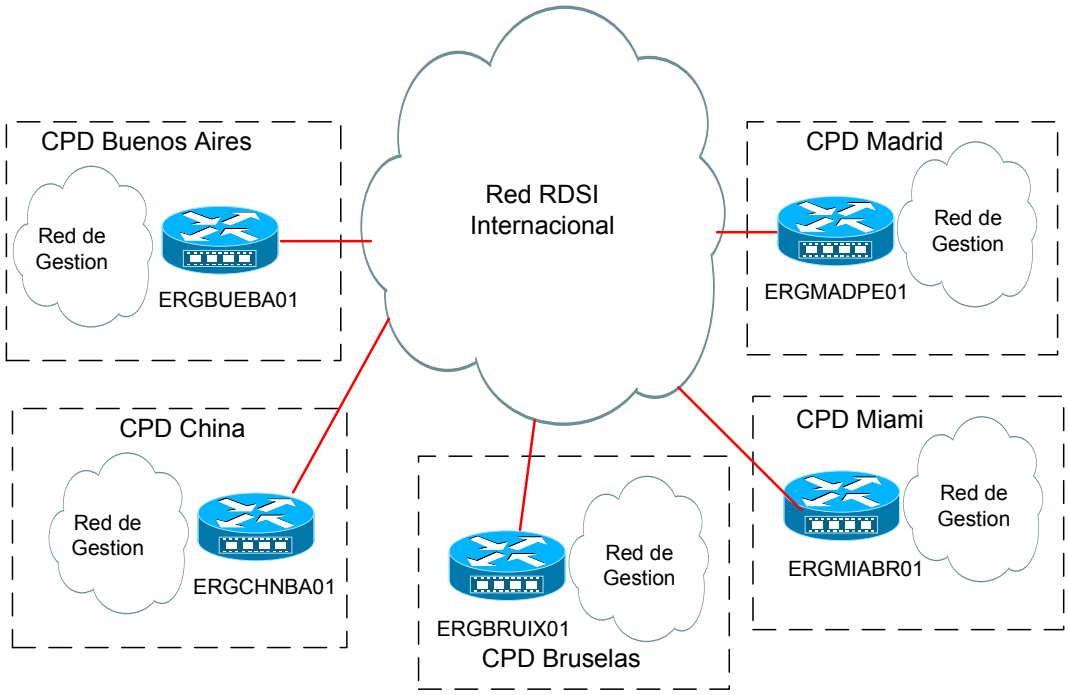


Figura: 11 Red de Gestion fuera de banda

En el esquema de red se puede observar como los equipos se intercomunican en caso de necesidad solamente cuando se pierde la gestión en banda (es la nube que aparece arriba como Red de Gestión) y es necesario conectarse a la consola a un equipo ubicado en un CPD. También este tipo de conexión se utiliza cuando se necesitan realizar una actualización del sistema operativo, y/o solucionar problemas de conectividad que dejaron al equipo aislado y no accesible desde la red de gestión en banda.

El funcionamiento es el siguiente desde el CPD de Madrid (centro de control, gestión y operación del operador) se llama al número RDSI del equipo ERG que se quiere conectar, una vez se establece la sesión.

Para poder establecer dicha sesión en realidad se utiliza el protocolo telnet o ssh y cuya dirección IP de destino es la dirección IP de la interface RDSI del equipo ERG ubicado en un sitio remoto. Una vez establecida la sesión en el caso de RDSI, es común la utilización del protocolo de punto a punto llamado PPP, que permite la utilización de la autenticación mediante el uso de un usuario y una contraseña para garantizar el acceso al equipo.

Una vez autorizado el acceso al equipo el usuario visualiza un menú de consolas para seleccionar el equipo al que se quiere conectar (cada número del menú corresponde a un puerto especifico del equipo remoto, y existe una conexión física entre el puerto de consolas por medio del cable RS-232).

Los pasos a seguir para establecer la conexión fuera de banda a un equipo remoto por ejemplo el equipo1 de Troncal de Madrid, y en concreto a la tarjeta supervisora activa serán los siguientes. Solamente es necesario conocer el equipo de gestión remoto que se quiere acceder (aquel que dispone las conexiones físicas a las consolas de los equipos)

1. Realizar el telnet o ssh a la dirección IP correspondiente
    a. Telnet ERGMADDE1 (en realidad se dispone de un servidor DNS para realizar la conversión de nombre a direcciones IP's).
2. Acceso al menú de consolas (para seleccionar el número que corresponde al equipo y Slot)
3. Ingreso del número correspondiente a la opción deseada (en este caso 5)
4. Ingresar usuario y contraseña para el acceso al equipo ERTMADDE1
5. Finalmente ya se está dentro del equipo para ejecutar los comandos deseados.

El menú de acceso puede tener la siguiente forma:

ROUTER Gestión remota ERGMADDE1

_____

Teclee un equipo

1	Libre
2	ERAMADDE1 (Slot6) RSP_standby
3	ERAMADDE1 (Slot5) RSP_activa
4	ERTMADDE1 (Slot6) RSP_standby
5	ERTMADDE1 (Slot5) RSP_activa
6	ERAMADDE2 (Slot6) RSP_standby
7	ERAMADDE2 (Slot5) RSP_activa
8	ERTMADDE2 (Slot6) RSP_standby
9	ERTMADDE2 (Slot5) RSP_activa
10	libre
11	SALIR

Donde por ejemplo con la opción 5 se puede acceder a la tarjeta supervisora activa del equipo de acceso ERTMADDE1 (Slot 5) RSP_activa.

5.4.Definición de mecanismos de redundancia y alta disponibilidad

5.4.1.Mecanismos de alta disponibilidad.

5.4.1.1. A nivel de equipo.

Ambos fabricantes para los equipos ERT y ERA disponen de los diferentes elementos redundantes para poder garantizar la alta disponibilidad ante un fallo simple.

Fuentes de alimentación: Cuatro fuentes de alimentación de las cuales son necesarias 3 para dar servicio al equipo completo de tarjetas (por lo que se contemple el fallo simple de una de las fuentes).

Tarjetas supervisoras: Todos los equipos se equipan con doble tarjeta de conmutación y procesamiento para que en caso de fallo de una de ellas la otra puede continuar con el envió y procesamiento del total del trafico (trabajan en forma activo /pasivo).

5.4.1.2. A nivel de enlace.

A nivel de enlace, se establecen caminos redundantes para poder garantizar el envío del tráfico ante un fallo simple. Existen varios mecanismos de redundancia de enlaces (protecciones de circuitos de transmisión, enlaces activo/standby, e incluso si es Ethernet el protocolo STP).

No se puede representar de forma general un único mecanismo de alta disponibilidad ya que existen muchas variables a tener en cuenta (Interoperabilidad entre fabricantes, tipo de enlace a utilizar Ethernet, FRAME-RELAY, ATM, etc.).

En este caso como es una red MPLS se trabaja con métricas que utilizan el protocolo IS-IS para establecer los túneles y los LSP.

La conmutación del tráfico se realiza en unos pocos milisegundos.

5.4.1.3. A nivel CPD.

A nivel de CPD, se debe tener en cuenta, en primer lugar el suministro eléctrico, si bien los equipos disponen de fuentes de alimentación redundantes, es necesario que se conecten a circuitos eléctricos diferentes para garantizar el correcto funcionamiento ante un fallo en alguno de los circuitos

5.4.2. Equilibrio entre coste y disponibilidad

Toda Red debe estar diseñado para poder brindar la mayor capacidad de transporte con el menor coste posible, donde la alta disponibilidad debe garantizar que ante un fallo se puede seguir transportando el mismo tráfico, con una interrupción mínima para los clientes.

En los apartados anteriores se pudo observar cómo se tiene en cuenta la redundancia a nivel de equipo, y de enlace.

A nivel de equipo está bien acotada la relación coste y disponibilidad, ya que como mínimo se debe redundar las fuentes de alimentación y las tarjetas supervisoras (que se encargan de realizar el procesamiento de todo el tráfico). La redundancia total a nivel de equipo se logra con la utilización de varios equipos para poder repartir la carga ante un fallo.

A nivel de enlace cabe señalar que un enlace por lo general es una línea que tiene un coste mensual y que se suele alquilar a un proveedor de servicios (Los grandes operadores tienen muchos enlaces propios, pero en determinadas ubicaciones deben arrendar enlaces a terceros). Este coste se va incrementando a medida que el ancho de banda es mayor, porque se entiende que además de arrendar un enlaces se alquila capacidad (por ejemplo no es lo mismo tener un acuerdo de capacidad por 1Mbps que por 10Gbps), ante un fallo la red del proveedor que nos ofrece el servicio debe estar preparada para garantizar nuestro enlace, incluso ante un fallo en su propia red.

Por esta razón ante circuitos propios y de alquilados a terceros se establecen la siguientes pautas para garantizar el trafico (cabe aclarar que a veces por razones de servicios y de acuerdos con clientes no se garantiza el 100% del tráfico).

- Protección de circuitos a nivel físico: Por lo general cuando se utiliza fibra óptica, si se dispone de equipos de transmisión propios, ante el corte de un tramo del circuitos si existe la posibilidad se encamina por medio de otro equipo de transmisión, para solventar el problema.

- Protección de nivel 2: Cuando se interconectan 2 equipos por medio de una red de nivel 2 (conmutadores) existe un mecanismo que evita que existan caminos redundantes (los caminos alternativos se quedan a la espera de ser utilizados). Este protocolo se llama STP (Spanning-Tree Protocol), que se ejecuta ante un cambio en la topología de red, entonces si un enlace principal falla, el enlace que estaba como respaldo se pone en funcionamiento.

- Protección de enlaces de Nivel 3: Puede existir múltiples enlaces (ATM, FRAME-RELAY, Ethernet) entre un origen y un destino, si se toma uno de ellos como principal (por razones del servicio no se quiere tener un balanceo de carga) entonces ante un fallo y perdida de conectividad el siguiente enlace (el enlace con mejor métrica) se utilizará para enviar el tráfico.

Es muy importante tener en cuenta el tipo de acuerdo que se firma con el proveedor y los clientes para poder garantizar el servicio a un coste razonable.

5.5.Previsión de crecimiento y adaptación a nuevas tecnologías

5.5.1.Escalabilidad

Se definieron los equipos según su función dentro de la red.

- Equipo de Red Troncal (ERT): Función interconectar los nodos de red.
- Equipo de Red Acceso (ERA): Función Agrupar conexiones de los clientes.
- Equipo de Cliente (EDC): Función interconectar la red del cliente.

Geográficamente según la necesidad se utiliza en un mismo POP (punto de presencia) un ERT y uno o más ERA, si es necesario ampliar un POP se podrán instalar más ERA que se interconecten con el ERT ya existente en ese POP, pero se debe tener en cuenta la alta disponibilidad ya que en caso de fallo de un ERT los demás ERA deben estar interconectados a otro ERT para no quedar aislados.

Pero como se puede observar la solución escala perfectamente si se pretende crecer tanto en número de POPs como en capacidad.

5.5.2.Normas de ingeniería para crecimiento por capacidad

La ampliación por capacidad suele realizarse cuando se pretende crecer en número de interfaces que interconectan con un equipo (ya sea ERT, ERA, o equipo de terceros).

Dependiendo de la tecnología a utilizar se puede realizar la unión lógica de varias interfaces físicas (todas del mismo tipo y ancho de banda)

- Ethernet LACP (Link Aggregation Control Protocol) es el estándar para la agregación de puertos Ethernet en una misma interface lógica.
- Multilink PPP (Multilink Point-to-Point Protocol) es el estándar para la agregación de puertos FRAME-RELAY, RDSI, ATM.

Como norma de ingeniería se estable que de ser posible siempre se utilicen puertos (de la misma velocidad y tipo) en tarjetas ubicadas en diferentes slots (para que en caso de fallo de una tarjeta por lo menos el resto de puertos que pertenecen a la interface lógica puedan seguir cursando tráfico).

5.5.3. Normas de ingeniería para aumento de nodos de red

Cuando se necesita crecer en cuanto a números de nodos de red, ya sea porque se desea tener presencia en un nuevo lugar geográfico y/o ampliar la presencia en un determinado lugar, siempre será necesario:

- Definir los acuerdos de SLA con los proveedores de los enlaces.
- Dar de alta en el inventario los circuitos (para ser identificados en caso de fallo o avería).
- Definir y aprovisionar los equipos ERT y ERA con la redundancia eléctrica, y de circuitos necesaria para garantizar la alta disponibilidad ante fallos.
- Dar de alta los contratos de mantenimiento con los fabricantes (detallando el equipamiento, el número de serie de cada una de las tarjetas instaladas)
- Configurar los equipos según las plantillas básicas de configuración y realizar las pruebas del equipo antes de la puesta en servicio.
- Dar de alta los nuevos nodos de red en las herramientas de gestión, monitorización y mantenimiento.
- Proveer acceso remoto a los nodos de Red, mediante la instalación de un equipo ERG con acceso 3G y/o RDSI.

5.5.4. Costes de crecimiento según función del equipo dentro de la red

El coste relacionado con el equipo según su función puede ser el siguiente:

Equipo de Red Troncal (ERT): Son aquellos equipos que estarán ubicados en el CORE o en el Backbone MPLS de la red, cuyas características son: Interfaces de gran velocidad y ancho de banda. Para definir un coste, se tiene en cuenta la siguiente arquitectura y configuración básica (Redundancia de tarjetas Procesadoras, Redundancia de Fuentes de Alimentación, 1 tarjetas de puertos de 10Gb o similar, 1 tarjeta de 100Gbps).

El coste de nodo ERT es de:

Juniper: €75.000

Cisco: € 70.000

Equipos de Red Acceso: son aquellos equipos que estarán ubicados entre el CORE y los equipos de cliente (EDC), cuyas características son: Interfaces de mediana velocidad, tarjetas de múltiples enlaces y ancho de banda).Para poder definir un coste, se tiene en cuenta la siguiente arquitectura y configuración básica (Redundancia de procesadoras y fuentes de alimentación, y solo 1 puerto de 10Ge en 1 slot con tarjetas de puertos SIP o FPC). No se define ninguna tarjeta de puertos ya que los requerimientos pueden variar en los diferentes POP, solo se contempla el Hardware necesario para interconectarse con un ERT.

El coste de nodo ERA es de:

Juniper: €40.000

Cisco: € 40.000

Equipos de Red Gestión: son aquellos equipos que estarán ubicados en la red fuera de banda, son equipos dedicados para acceso remoto a los equipos ubicados en los Data center o Housing. Es un equipo cuyas características son: Interfaces baja velocidad, con acceso mediante RDSI y/o 3G para conexiones esporádicas en caso de pérdida de gestión de los equipos). No se incluye el valor de la contratación del enlace

El coste de nodo ERG es de:

Cisco: € 2.500

Equipos de Cliente (EDC): son aquellos equipos que pueden o no ser gestionados por el cliente estos equipos los provee el cliente.

5.5.5.Adaptabilidad a nuevas tecnologías (implementaciones futuras).

En lo que se refiere a la adaptabilidad a nuevas tecnologías, en la actualidad los equipos están preparados para manejar interfaces de hasta 100Gbps (valor máximo en uso al momento de realizar este trabajo).

Como se eligieron equipos de los 2 principales fabricantes, se garantiza que cualquier cambio tecnológico podrá tener compatibilidad con el hardware actual. Tanto Cisco como Juniper proveen de cursos y seminarios donde informan sobre nuevas tendencias y tecnologías disponibles en los equipos, todos estos desarrollos están orientados a ser implementados en los equipos actuales.

5.6.Definición de los servicios ofrecidos y soportados

5.6.1.Portfolio de servicios

En cuanto al portfolio de servicios podemos realizar una subdivisión entre servicios gestionados (Gestión y mantenimiento del equipo del cliente) y no gestionados. También se puede contemplar el servicio STI (Servicio Tráfico Internet), pueden existir múltiples modalidades de las VPN como ser (conectividad de las sedes todas contra todas, todas contra una sola central, como así también accesos IPSec, etc.).

Para poder definir el tipo de servicio primer se debe tener en cuenta el tipo de acceso, y este se define de acuerda a la tecnología de acceso de interconexión entre el PE y el EDC. Es importante conocer y tener en cuenta el tipo de interfaces que se utilizan para interconectar los equipos (ya sea a nivel de red troncal como a nivel de servicios).

El CORE o equipos Troncales son los llamados P de la red de la nube MPLS, dichos equipos son los responsables de intercambiar los paquetes a la mayor velocidad posible, para ello se contemplas interfaces de 10Gbps y 100Gbps, mediante la utilización de LACP (Agregación lógica de enlaces físicos), se pueden tener enlaces lógicos de una capacidad del entorno de un Tera bit.

En los equipos de acceso, los PE de la red MPLS, dichos equipos se encargan de agrupar o agregar el tráfico proveniente de los equipos de clientes interconectándolo con la red MPLS.

Para ello es necesario que dichos equipos cuenten con interfaces que le permitan conectar con los equipos troncales como se 10Gbps y múltiples tipos de enlaces de menor capacidad, y diferentes tecnologías a continuación se comentan de forma resumida las características en cuanto a velocidad, tipo de conexión y capacidad de los diferentes tipos de enlaces que comúnmente se utilizan para la interconexión entre los equipos de cliente EDC y los equipos de acceso ERA:

- **Enlaces E1 / T1**: La trama E1 es un formato de transmisión digital. Incluye señalización de canales asociados (Channel Associated Signaling – CAS).

  La trama E1 consta en 32 divisiones (time slots) PCM (pulse code modulation) de 64k cada una, lo cual hace un total de 30 líneas de datos más 2 canales de señalización el ancho de banda de una enlaces E1 es de 32x64Kbps=2040bps.

  Para el caso de un T1 (se utiliza principalmente en USA, Japón y Corea del sur) consta de 24 divisiones (time slots) de 64Kbps + 8kbps de señalización, por que el ancho de banda de una T1=1544bps.

  Las tarjetas necesarias a instalar en los equipos de acceso serán:
  Cisco Módulos SPA (Shared Port Adapter) a insertar en el modulo SIP-400
  Cisco 8-port Channelized T1/E1 SPA
  Juniper Módulos PIC (Physical Interface Card) a insertar en el modulo FPC
  E1/T1-FPC I3 Board

- **Enlaces E3/T3:** en el caso de un trama E3 consta de una ancho de banda de 34.368Mbps y un T3 44.736Mbps.

  Las tarjetas necesarias a instalar en los equipos de acceso serán:
  Cisco Módulos SPA (Shared Port Adapter) a insertar en el modulo SIP-400
  Cisco 2/4-port Channelized T3 to DS0 SPA
  Cisco 2/4-port T3/E3 Serial SPA
  Juniper Módulos PIC (Physical Interface Card) a insertar en el modulo FPC
  E3/T3-FPC I3 Board

- **Tecnología SDH (STM-x):** Unidad de transmisión básica de la Jerarquía Digital Síncrona (SDH), correspondiente al primer nivel básico. Es una trama de 2430 bytes, distribuidos en 9 filas y 270 columnas. Las primeras nueve columnas contienen únicamente información de gestión y se distribuyen en tres campos (RSOH), filas 1-3 [27 bytes]; Puntero de la unidad administrativa, fila 4 [9 bytes]; (MSOH), filas 5-9 [45 bytes] Las columnas restantes (10-270) contienen carga útil. Normalmente, se trata de un contenedor virtual de nivel 4 (VC-4).

  Un contenedor virtual VC-4 y el puntero de la unidad administrativa conforman una unidad administrativa de nivel 4 (AU-4). Por lo tanto, se genera una trama STM-1 añadiendo a una AU-4 las taras RSOH y MSOH que le correspondan.

  La transmisión se realiza bit a bit en el sentido de izquierda a derecha y de arriba abajo. La trama se transmite a razón de 8.000 veces por segundo (cada trama se transmite en 125 µs,= 1/8000Hz). Por lo tanto el régimen binario es igual a:

  Los múltiplos de este ratio de transmisión (8.000) dan lugar a los enlaces STM-4, STM-16 y STM-64 y STM_256 descritos en el estándar SDH.

Bits por segundo	Capacidad	SDH	Capacidad SDH
51.84 Mbps	51 Mbps	STM-0	21 E1
155.52 Mbps	155 Mbps	STM-1	63 E1 o 1 E4
622.08 Mbps	622 Mbps	STM-4	252 E1 o 4 E4
2488.32 Mbps	2.4 Gbps	STM-16	1008 E1 o 16 E4
9953.28 Mbps	10 Gbps	STM-64	4032 E1 o 64 E4
39813.12 Mbps	40 Gbps	STM-256	16128 E1 o 256 E4

  Las tarjetas necesarias a instalar en los equipos de acceso serán:

  Cisco Módulos SPA (Shared Port Adapter) a insertar en el modulo SIP-400
  Cisco 2-Port OC-3c/STM-1c POS SPA
  Cisco 4-Port OC-3c/STM-1c POS SPA
  Cisco 1-Port OC-12c/STM-4c POS SPA
  Cisco 1-Port OC-48/STM16-c POS/RPR SPA (POS mode only)

Juniper Módulos PIC (Physical Interface Card) a insertar en el modulo FPC (Flexible PIC Concentrator)
SONET/SDH OC48/STM16 (Multi-Rate) PIC with SFP
SONET/SDH OC48/STM16 PIC with SFP
SONET/SDH OC192c/STM64 PIC
SONET/SDH OC192c/STM64 PIC with XFP

- **ATM:** Modo de Transferencia Asíncrona fue la apuesta de la industria tradicional de las telecomunicaciones por las comunicaciones de banda ancha. ATM es ampliamente utilizado allá donde se necesita dar soporte a velocidades moderadas, como es el caso de la ADSL.
  Se basa en el transporte de celdas como estructuras de datos de 53 bytes compuestas por dos campos principales:
  - Header, sus 5 bytes tienen tres funciones principales: identificación del canal, información para la detección de errores y si la celda es o no utilizada. Eventualmente puede contener también corrección de errores y un número de secuencia.
  - Payload, tiene 48 bytes fundamentalmente con datos del usuario y protocolos AAL que también son considerados como datos del usuario.
  - El ancho de banda del ATM están en torno a los enlaces de tecnología SDH

  Las tarjetas necesarias a instalar en los equipos de acceso serán:

  Cisco Módulos SPA (Shared Port Adapter) a insertar en el modulo SIP-400
  Cisco 2-Port OC-3c/STM-1c ATM SPA
  Cisco 4-Port OC-3c/STM-1c ATM SPA
  Cisco 1-Port OC-12c/STM-4c ATM SPA
  Cisco 1-port OC48/STM16 ATM SPA
  Juniper Módulos PIC (Physical Interface Card) a insertar en el modulo FPC (Flexible PIC Concentrator)
  OC3/STM1 (Multi-Rate) PIC with SFP
  OC12/STM4 PIC with SFP

- **FRAME-RELAY:** Es una técnica de comunicación de tramas para redes de circuitos virtuales. Las conexiones pueden ser del tipo permanente, (PVC, Permanent Virtual Circuit) o conmutadas (SVC, Switched Virtual Circuit).

  Al contratar un servicio Frame Relay, se contrata un ancho de banda determinado en un tiempo determinado. A este ancho de banda se le conoce como CIR (Commited Information Rate). Esta velocidad, surge de la división de Bc (Committed Burst), entre Tc (el intervalo de tiempo).

  Una de las características de Frame Relay es su capacidad para adaptarse a las necesidades de las aplicaciones, pudiendo usar una mayor velocidad de la contratada en momentos puntuales, resultando muy optimo para el tráfico del tipo en ráfagas. Los requisitos son que la media de tráfico en el intervalo Tc no deberá superar la cantidad estipulada Bc.

  Estos bits de Bc serán enviados de forma transparente. No obstante, cabe la posibilidad de transmitir por encima del CIR contratado, mediante el envío de

paquetes o ráfagas en exceso que son Be (Excess Burst). Estos datos que superan lo contratado, serán enviados en modo best-effort, activándose el bit DE de estas tramas, con lo que serán las primeras en ser descartadas en caso de congestión en algún nodo.

La siguiente imagen ayuda a comprender mejor el funcionamiento de FRAME RELAY

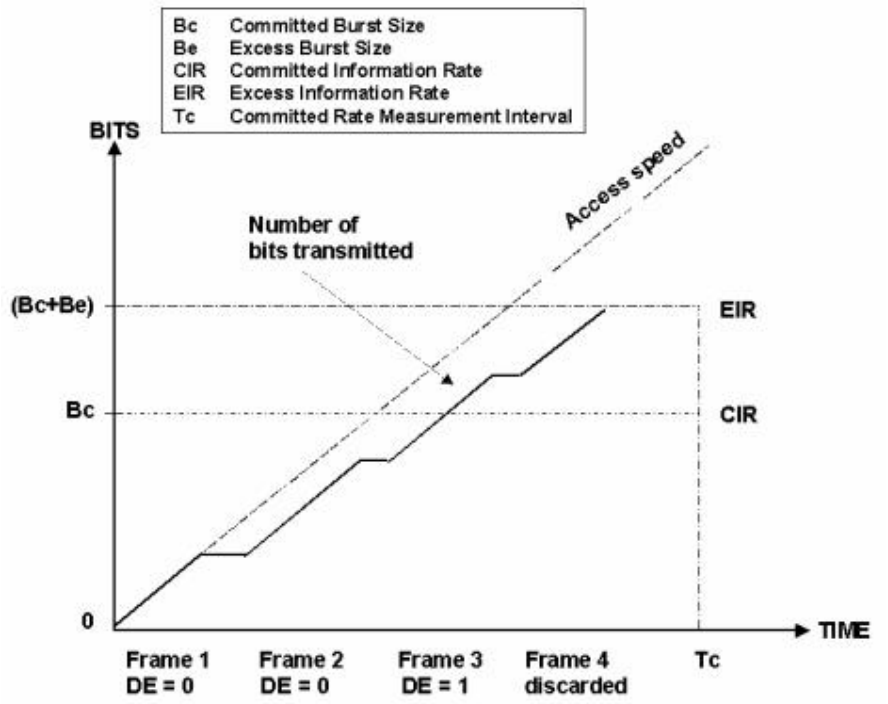


Figura: 12 conformado de tráfico Frame-Relay.

Como se puede observar las tramas que superen la cantidad de Bc+Be en el intervalo, serán descartadas directamente sin llegar a entrar en la red, sin embargo las que superan la cantidad Bc pero no Bc+Be se marcan como descartables (DE=1) para ser estas las primeras en ser eliminadas en caso de congestión.

Las tarjetas necesarias a instalar en los equipos de acceso serán:

Cisco Módulos SPA (Shared Port Adapter) a insertar en el modulo SIP-400 y SIP-200
8-Port Channelized T1/E1 SPA
2-Port and 4-Port Channelized T3 SPA
1-Port Channelized OC-3/STM-1 SPA
Juniper Modulo PIC (Physical Interface Card) a pinchar en el modulo FPC
E3/T3-FPC I3 Board
OC-3/STM1 PIC with SFP
E1/T1-FPC I3 Board

Ethernet (1Gbits, 100Mbits): Ethernet es el protocolo más utilizado en la actualidad y ampliamente reconocido aplicado a la capa física y de enlace en sus comienzos la velocidad de transmisión era de 10Mbps, posteriormente apareció FastEthernet que incrementó la velocidad de 10 a 100 megabits por segundo (Mbit/s).
Giga bit Ethernet fue la siguiente evolución, incrementando en este caso la velocidad hasta 1000 Mbit/s. En muchas redes LAN (Red Área local) actuales se utilizan 1000/100Mbits para la interconexión de equipos. Este tipo de interfaces se pueden agrupar mediante la utilización del protocolo LACP.
Como así también una misma red LAN se puede segmentar en redes LAN virtuales LAN, para ello se utiliza el protocolo 802.1Q (El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking)

Las tarjetas necesarias a instalar en los equipos de acceso serán:

Cisco Módulos SPA (Shared Port Adapter) a insertar en el modulo SIP-400 y SIP-200
Fast Ethernet (en SIP-200)
Cisco 4-Port Fast Ethernet Shared Port Adapter
Cisco 8-Port Fast Ethernet Shared Port Adapter
Ethernet (en SIP-400)
2-port 1 GE SPA (V1 and V2)
5 port 1 GE SPA (V2 only)
1-port 10GbE SPA LAN PHY (V2 only)
Tarjeta de línea de puertos:
WS-X6724-SFP
WS-X6748-SFP

Juniper Módulos PIC (Physical Interface Card) a insertar en el modulo FPC
1-Gigabit Ethernet, 2/4-port SFP
1-Gigabit Ethernet, 10-port SFP
1-Gigabit Ethernet, 24/48-port SFP
10-Gigabit Ethernet, 1-port xenPaK

Una vez definido el tipo de acceso, y su modalidad de servicio, se puede clasificar el portfolio de servicio según:

Servicio VPN: características que definen el tipo servicio, con el caso de un servicio VPN (se especifica el nombre de la VPN, los parámetros propios de la VRF como ser el RD (Identificador de equipo), comunidades de BGP propias de la VPN).

De forma general se pueden estandarizar los servicios de VPN, según la tecnología de acceso (FRAME-RELAY, ATM, Ethernet) y según la velocidad o capacidad contratada. De acuerdo a estas características tendrá diferentes clases de servicio.

Servicio	Gestionado	Acceso	Velocidad	Modalidad	Calidad de Servicio
VPN	Si / No	FR /ATM	512Kbps	VRF única	Oro/Plata/Bronce
VPN	Si / No	FR /ATM	1024Kbps	VRF única	Oro/Plata/Bronce
VPN	Si / No	FR /ATM	2048Kbps	VRF única	Oro/Plata/Bronce
VPN	Si / No	FR /ATM	4096Kbps	VRF única	Oro/Plata/Bronce
VPN	Si / No	Ethernet	10 Mbps	Mono o Multi VRF	Oro/Plata/Bronce
VPN	Si / No	Ethernet	100 Mbps	Mono o Multi VRF	Oro/Plata/Bronce
VPN	Si / No	Ethernet	1Gbps	Mono o Multi VRF	Oro/Plata/Bronce
VPN	Si / No	Ethernet	10Gbps	Mono o Multi VRF	Oro/Plata/Bronce

Servicio STI: En el caso se servicio STI se definen las políticas de importación y exportación de prefijos, y fundamentalmente se especifica si será necesario el acceso a internet mediante el anuncio de una ruta estática o anunciando el total de redes existentes en internet).

De forma general se pueden estandarizar los servicios de STI, según la tecnología de acceso (FRAME-RELAY, ATM, Ethernet) y según la velocidad o capacidad contratada. De acuerdo a estas características tendrá diferentes clases de servicio.

En la sección 4.6.2 se define en detalles la calidad de servicio Oro / Plata / Bronce

Servicio	Gestionado	Acceso	Velocidad	Modalidad	Calidad de Servicio
STI	Si / No	FR /ATM	512Kbps	VRF única	Oro/Plata/Bronce
STI	Si / No	FR /ATM	1024Kbps	VRF única	Oro/Plata/Bronce
STI	Si / No	FR /ATM	2048Kbps	VRF única	Oro/Plata/Bronce
STI	Si / No	FR /ATM	4096Kbps	VRF única	Oro/Plata/Bronce
STI	Si / No	Ethernet	10 Mbps	Mono o Multi VRF	Oro/Plata/Bronce
STI	Si / No	Ethernet	100 Mbps	Mono o Multi VRF	Oro/Plata/Bronce
STI	Si / No	Ethernet	1Gbps	Mono o Multi VRF	Oro/Plata/Bronce
STI	Si / No	Ethernet	10Gbps	Mono o Multi VRF	Oro/Plata/Bronce

STI = Servicio Trafico Internet

5.6.1.1. Características del servicio STI (servicio tráfico internet).

El servicio STI está pensado para dar conectividad a pequeñas y/o medianas empresas que necesitan acceso a internet con una velocidad garantizada mediante una conexión WAN (FRAME-RELAY, ATM, 100Mbps, 1Gbps, etc.) en dicha conexión entre PE-EDC se establece una sesión BGP y se envía una ruta por defecto (0.0.0.0/0) o se les envía el total de rutas existentes en internet (más de 300 mil redes), todo esto está condicionado a las necesidades el cliente y el tipo de equipo utilizado como EDC.

Otra variante a este servicio es la necesidad que tienen los clientes (mayormente empresas) que necesitan utilizar nuestra infraestructura de red para poder redes que se pueden encontrar en internet o en destinos fuera de nuestra red. En la figura se utilizan los colores para hacer referencia al servicio STI. Como se puede observar en el punto 5.6.1 se definen unos valores de referencia para la conexión WAN, con su calidad de servicio asociada.

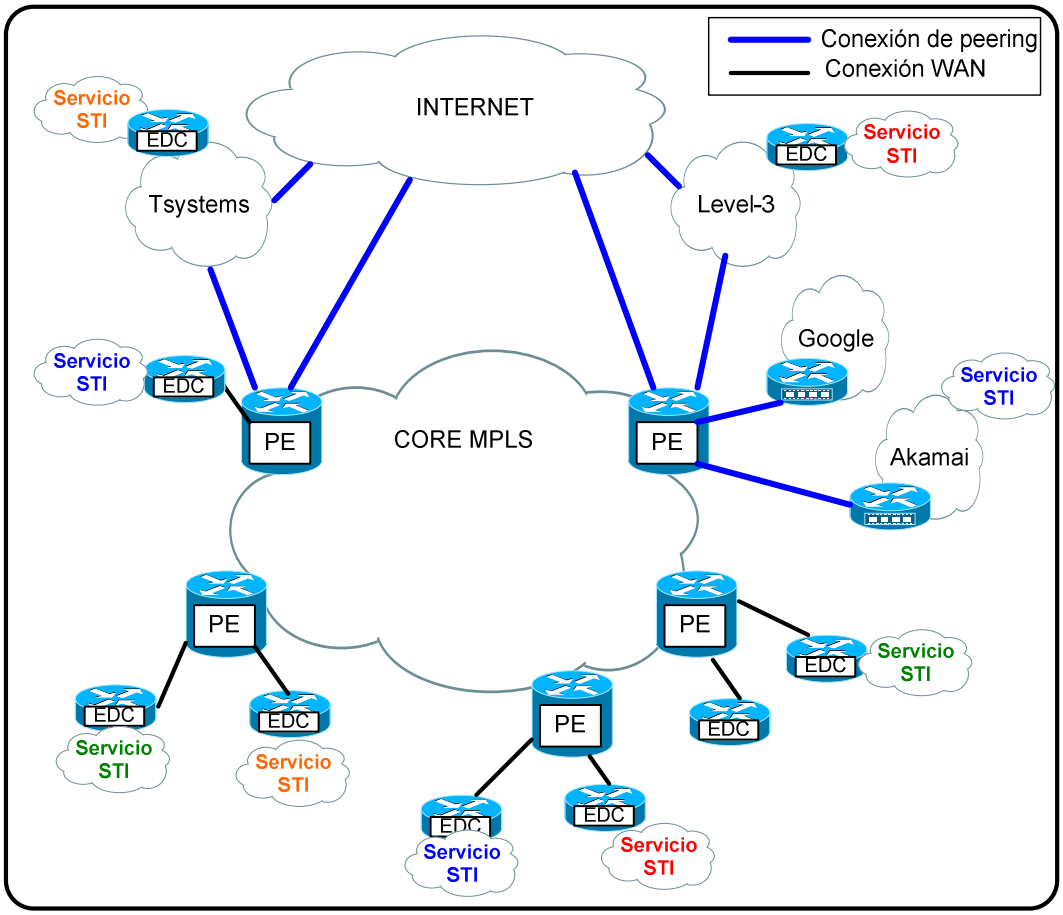


Figura: 13 Tráfico STI

5.6.1.2. Características del servicio VPN (Red Privada Virtual).

El servicio VPN está pensado para dar conectividad a pequeñas y/o medianas empresas que necesitan la interconectar de sus sedes (por ejemplo tiendas de ropa, que necesitan conocer al instante el volumen de venta y el stock).

Para ello es necesario establecer una conexión entre el EDC y el PE de nuestra red (esta conexión es del tipo WAN y con la velocidad y tipo de acceso definidos en el punto 5.6.1 según las necesidades del cliente). Se establece una sesión BGP (es importante recordar los atributos de BGP como se la community) que permiten definir los siguientes parámetros que serán únicos dentro de una VPN o VRF (Virtual Routing Forwarding), cabe aclarar que en los equipos PE van a existir una tabla de enrutamiento Global (para todo el trafico Internet y servicio STI) y también una tabla de enrutamiento por cada VPN o VRF.

En este contexto hace posible que el trafico de un cliente (pertenece a una VPN) permanezca aislado y solo sea conocidos por los miembros de esa misma VPN. El PE al tener una tabla individual por VRF puede tener incluso el mismo direccionamiento privado sin que se solapen por estar en contextos o tablas diferentes.

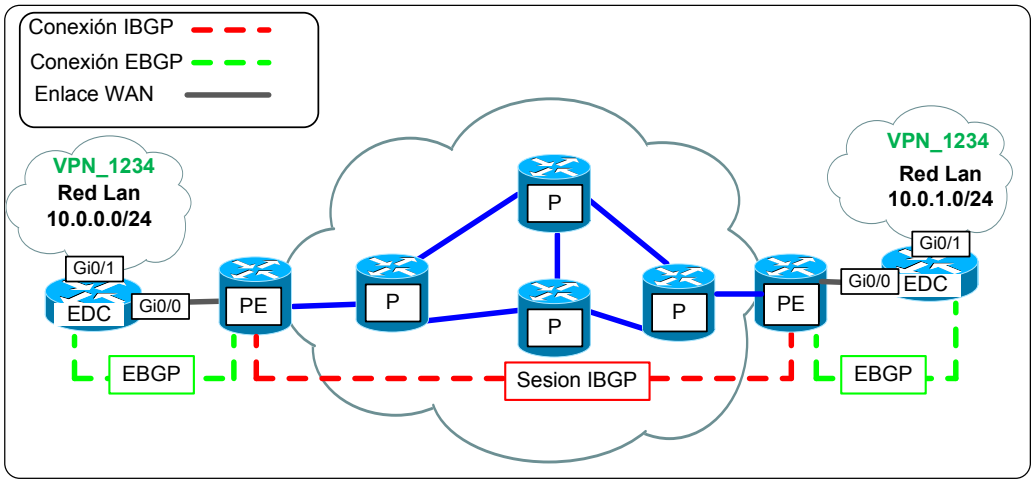


Figura: 14 Ejemplo de VPN

Como se puede observar en la figura 14 la vpn_1234 dispone de 2 EDC (Equipos de clientes) interconectando estas 2 sedes mediante la red IP/MPLS, el acceso a la red lo hacen mediante los enlaces EDC/PE a continuación se detalla la configuración necesaria en cada uno de los equipos de red.

1) Establecimiento de sesión eBGP entre el PE y el EDC.

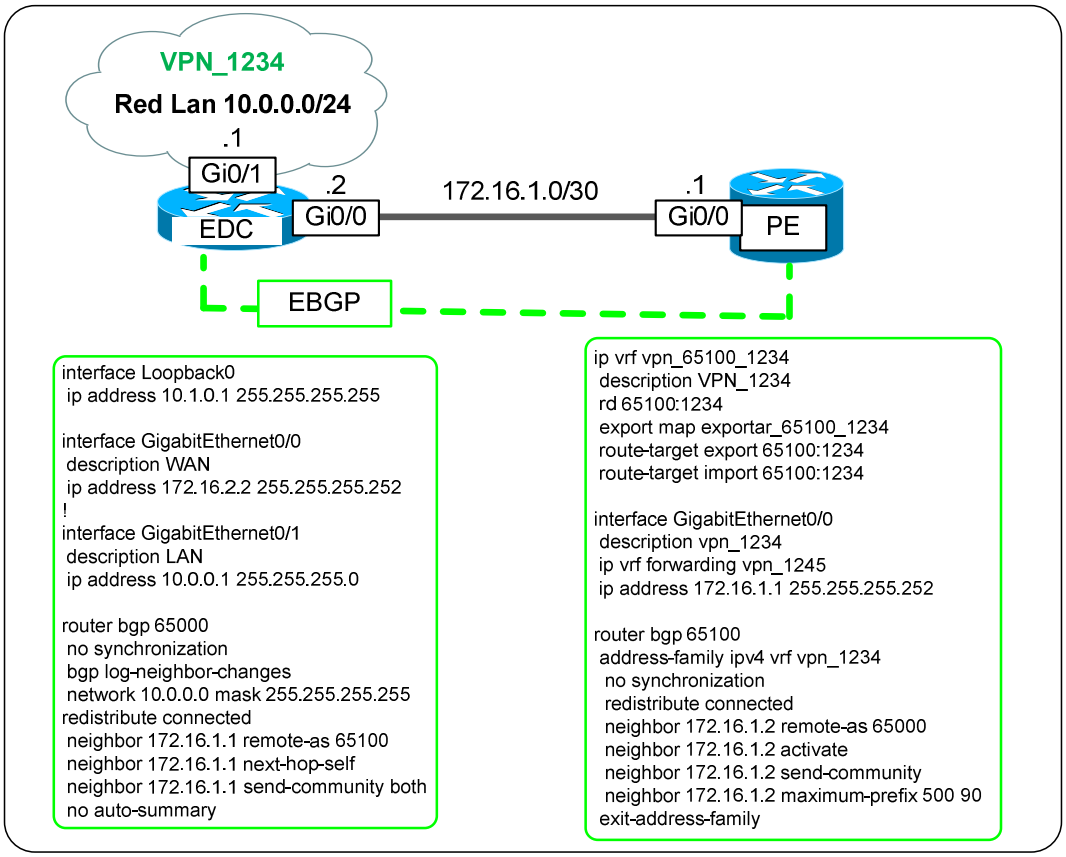


Figura: 15 Configuración sesión EBGP EDC y PE

En la figura 15, se puede observar que el EDC tiene directamente conectadas las redes 10.0.0.0/24 (interface GigabitEthernet 0/0), 10.1.0.1/32 (Interface Loopback 0) y la red 10.0.1.0/24 que aprende de la conexión EBGP con el PE (es la red LAN del EDC remoto)

2) Configuración IBGP PE-PE

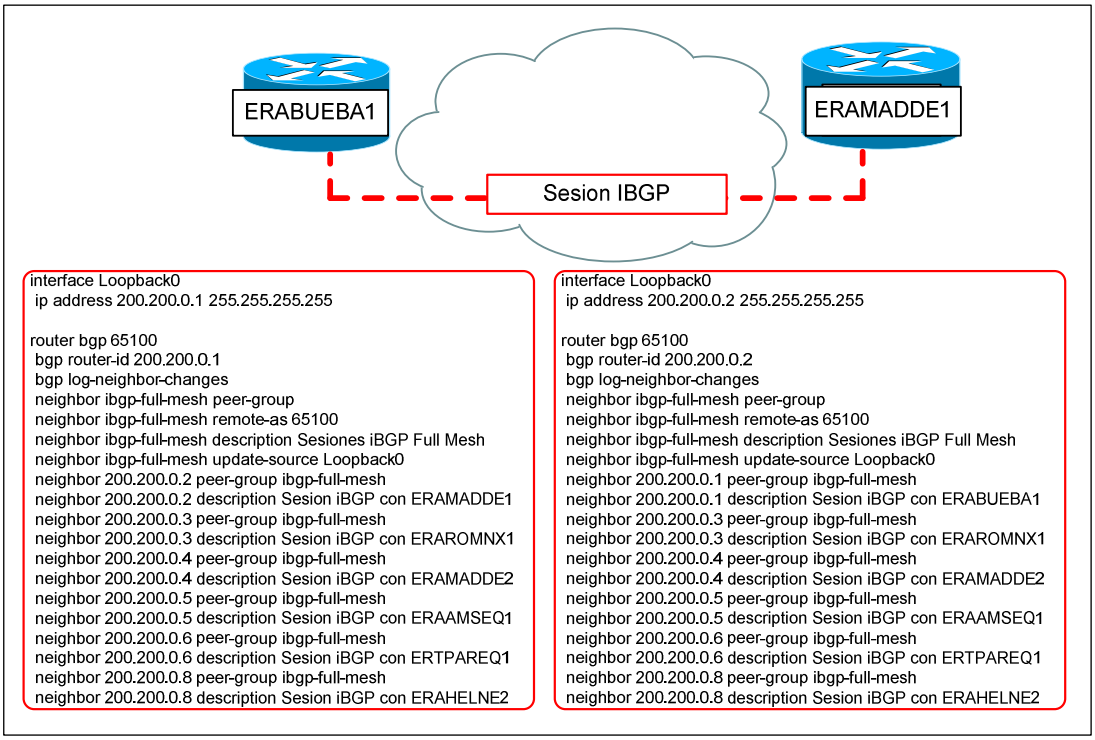


Figura: 16 Configuración sesión iBGP PE y PE

En el equipo ERAMADDE1, va a tener una sesión EBGP con el EDC por la interface y a nivel IBGP va a conocer la red 10.0.0.0/24 que le anuncia el router ERABUEBA2(200.200.0.1):

ERAMADDE1#sh ip bgp vpnv4 vrf vpn_65100_1234 **10.0.0.0**
BGP routing table entry for **65100:1234:10.0.0.0/24**, version 175199
Paths: (1 available, best #1, table **vpn_65100_1234**)
Advertised to update-groups:
746
200.200.0.1 (metric 85700) from **200.200.0.1 (200.200.0.1)**
Origin IGP, metric 1000, **localpref 100**, valid, internal, best
Community: 65100:1234
Extended Community: **RT:65100:1234**
mpls labels in/out nolabel/49

Con su correspondiente atributo de BGP community, LOCAL PREFERENCE, Metric , Origin. y las etiquetas MPLS 49

En el equipo ERABUEBA2, va a tener una sesión EBGP con el EDC por la interface y a nivel IBGP va a conocer la red 10.0.1.0/24 que le anuncia el router ERAMADDE1(200.200.0.2):

ERAMADDE1#sh ip bgp vpnv4 vrf vpn_65100_1234 **10.0.1.0**
BGP routing table entry for **65100:1234:10.0.1.0/24**, version 175199
Paths: (1 available, best #1, table **vpn_65100_1234**)
 Advertised to update-groups:
    746
  200.200.0.2 (metric 85700) from **200.200.0.2 (200.200.0.2)**
    Origin IGP, metric 1000, **localpref 100**, valid, internal, best
    Community: 65100:1234
    Extended Community: **RT:65100:1234**
    mpls labels in/out nolabel/59

Con su correspondiente atributo de BGP community, LOCAL PREFERENCE, Metric , Origin. y las etiquetas MPLS 59

sesiones EBGP establecidas
ERABUEBA2#**sh ip bgp vpnv4 vrf vpn_65100_1234 summary**
BGP router identifier 200.200.0.1, local AS number 65100
BGP table version is 11027365, main routing table version 11027365
440 network entries using 66880 bytes of memory
579 path entries using 30108 bytes of memory
13030/10622 BGP path/bestpath attribute entries using 1719960 bytes of memory
130 BGP rrinfo entries using 3120 bytes of memory
127741 BGP AS-PATH entries using 3862980 bytes of memory
33045 BGP community entries using 4227338 bytes of memory
2262 BGP extended community entries using 171688 bytes of memory
162 BGP route-map cache entries using 5832 bytes of memory
208 BGP filter-list cache entries using 3328 bytes of memory
BGP using 10091234 total bytes of memory
BGP activity 2696037/2123032 prefixes, 66948034/64109625 paths, scan interval 60 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
172.16.1.2	4	65000	14289	14303	11027365	0	0	1w1d	2

Rutas aprendidas por la session EBGP #### EDC-PE
ERABUEBA2#**sh ip bgp vpnv4 vrf vpn_65100_1234 neighbors 172.16.1.2 routes**
BGP table version is 11027914, local router ID is 200.200.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 65100:1234 (default for vrf vpn_65100_1234)					
*> 10.0.0.0/24	172.16.1.2			0	65000 i
*> 10.1.0.1/32	172.16.1.2			0	65000 i

Total number of prefixes 2

3) Configuración PE-EDC

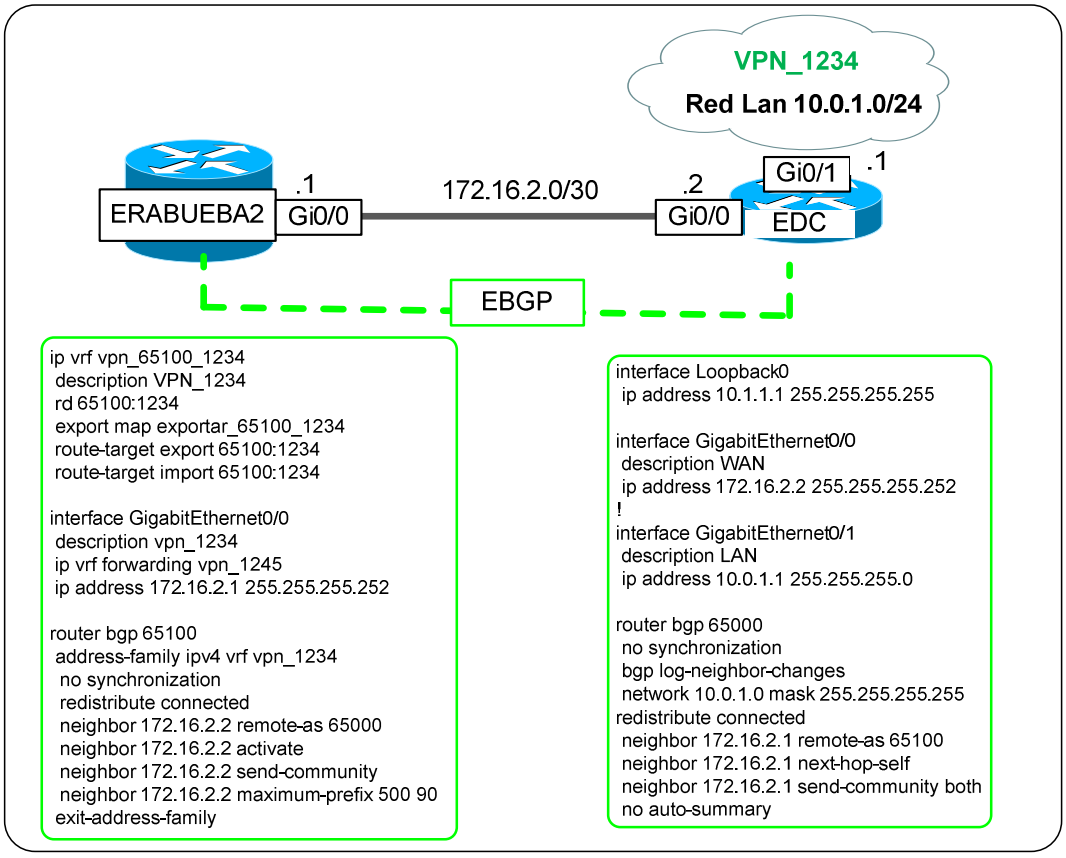


Figura: 17 Configuración sesión EBGP PE y EDC

Finalmente en el equipo remoto ubicado en Madrid, en la figura 17, se puede observar que el EDC tiene directamente conectadas las redes 10.0.1.0/24 (interface GigabitEthernet 0/0), 10.1.1.1/32 (Interface Loopback 0) y la red 10.0.0.0/24 que aprende de la conexión EBGP con el PE (es la red LAN del EDC remoto)

5.6.1.3. Diferencia entre servicio Gestionado y no Gestionado

El servicio no gestionado implica que el cliente es el encargado de mantener (verificar que el equipo está operativo los 365 días del año), para ellos debe disponer de un equipo de personas dedicados a monitorizar el o los EDC's para observar cualquier anomalía (generalmente se utilizan herramientas de gestión de alarmas, sondeo por SNMP para recibir y manejar las alarmas).

Un punto que siempre debe estar cubierto es el contrato de mantenimiento del equipo (este contrato vincula a la empresa con el fabricante del equipo) mediante el cual ante fallos software (los llamados BUGS que provocan inestabilidad en el equipo) o de hardware (fallo en tarjetas, fuentes de alimentación o cualquier elemento hardware que contiene el equipo) será solucionado por el vendedor a la mayor brevedad posible.

En cuanto a la línea (Conexión WAN que une el EDC con el PE), el cliente al ser un servicio no gestionado deberá responsabilizarse del mantenimiento (costo mensual del servicio de alquiler de línea, e incluso de gestión de averías con el proveedor ante fallos y/o perdidas de conectividad)

El servicio gestionado ofrece todo un servicio de los conocidos "llave en mano", el cliente solo será responsable de lo que ocurre apartar de la interface LAN del EDC, solo es responsable de su infraestructura propia y local de cada sede.

El contenido del servicio gestionado se pude resumir de la siguiente manera:

<u>Monitorización y gestión remota del equipamiento</u>

- Se le configura una dirección IP que pertenece a la red de gestión (así de esta manera se puede tener conectividad desde el centro de control, hasta el equipo)
- Se les configura una serie de parámetros a nivel SNMP, una comunidad de lectura y de escritura (Para poder recibir alarmas, ante fallos y/o superación de ciertos umbrales (, se monitoriza mediante SNMP el trafico entrante y saliente por el enlace, obteniendo graficas que ayudan a establecer la ocupación del enlace.
- Se le configura un servidor de LOGS (para detectar cualquier problema en el equipo) mediante la utilización de script que ayudan a filtrar la información de mensajes de error más críticos.
- Ante un fallo o avería en la línea se dispone de personal las 24hs del día que dispone de conocimientos para realizar la resolución de la incidencia. (Es equipo de personas es el mismo para todos los clientes) por lo que se conoce el entorno de red.
- Gestion del contrato de mantenimiento (garantía del fabricante), en caso de fallo HW posiblemente haya que gestionar el reemplazo Hardware (RMA), y para ellos hay que coordinar el envío y devolución de la pieza averiada. Si el cliente es de ámbito internacional se puede dar el caso de tener que manejar horas fuera del horario de trabajo local.

- En caso de fallos software, se puede realizar el cambio del sistema operativo del equipo, e incluso por la gran experiencia del equipo de gestión en cuanto a estabilidad de versiones de sistemas operativos se puede recomendar una versión en concreto (de acuerdo a los servicios necesarios por el cliente).

- Garantizar la recuperación del servicio en caso de fallo HW en 4hs, gracias a la gestión remota del equipo (se pueden obtener la configuración del equipo periódicamente), una vez restablecido el hardware dañado solamente se le copia la configuración previamente guardada.

- Disminución de costes en cuanto a mantenimiento y costes de líneas ya que como operador se pueden negociar mejor precio de líneas, también en cuanto a mantenimiento obtener un mejor tiempo de resolución ante fallos.

5.6.1.4. Script de gestión de LOGS.

Existen varias soluciones para la gestión de los syslog (repositorio en texto plano de mensajes de la consola de los equipos de red), utilizando o desarrollando script a medida para poder gestionar toda la información contenida en un texto plano. Para ello resulta útil realizar y tener en cuenta las siguientes recomendaciones:

- Disponer de un listado de equipos por Fabricantes (En nuestro caso disponer de el listado del nombre de equipos Cisco y Juniper)

- Tener todos los dispositivos sincronizados mediante NTP, para poder realizar el análisis de los logs de forma eficiente.

- Disponer de un listado de mensajes críticos para poder crear informes con mayor criticidad.

En el anexo 8.2 se puede observar el script propuesto realizado en Phyton, como así también un archivo plano de texto con el SYSLOG.txt y los 2 archivos Cisco_Log.txt y Juniper_Log.txt con los mensajes de cada unos de los fabricantes.

5.6.1.5. Plataforma de gestión de alarmas y monitorización de equipos.

Gestion SNMP: El protocolo SNMP es el protocolo de gestión más conocido y utilizado. Está definido en una serie de normas escritas por el IETF. Se refieren no sólo el propio protocolo, sino también el lenguaje de especificación de la MIB, SMI e incluso la arquitectura de cómo se deben implementar los agentes.

Componentes SNMP: Una red gestionada con SNMP, consta de tres componentes principales:

- **Dispositivo administrado:** Son todos los elementos de la red o dispositivos que contienen información susceptible de ser consultada, utilizan el protocolo SNMP y estos dispositivos administrados recogen y almacenan información que ponen a disposición de los gestores a través del protocolo SNMP. En una red WAN, se pueden encontrar ERT, ERA, ERG, conmutadores, firewalls, IDS o, en definitiva, cualquier elemento de red.

- **Un agente:** Es un módulo de software que reside en un dispositivo administrado. Un agente posee un conocimiento local de información de administración (memoria libre, número de paquetes IP recibidos, rutas, numero de rutas, etcétera), la cual es traducida a un formato compatible con SNMP y organizada en jerarquías MIB (Management Information Base).

- **Un gestor (NMS)**: Es el equipo que ejecuta aplicaciones que supervisan y controlan los dispositivos administrados. Los gestores proporcionan el total de los recursos necesario en cuanto a procesamiento y de memoria para realizar la gestión de la red. Pueden existir uno o más gestores de red.

Flujo de las peticiones SNMP

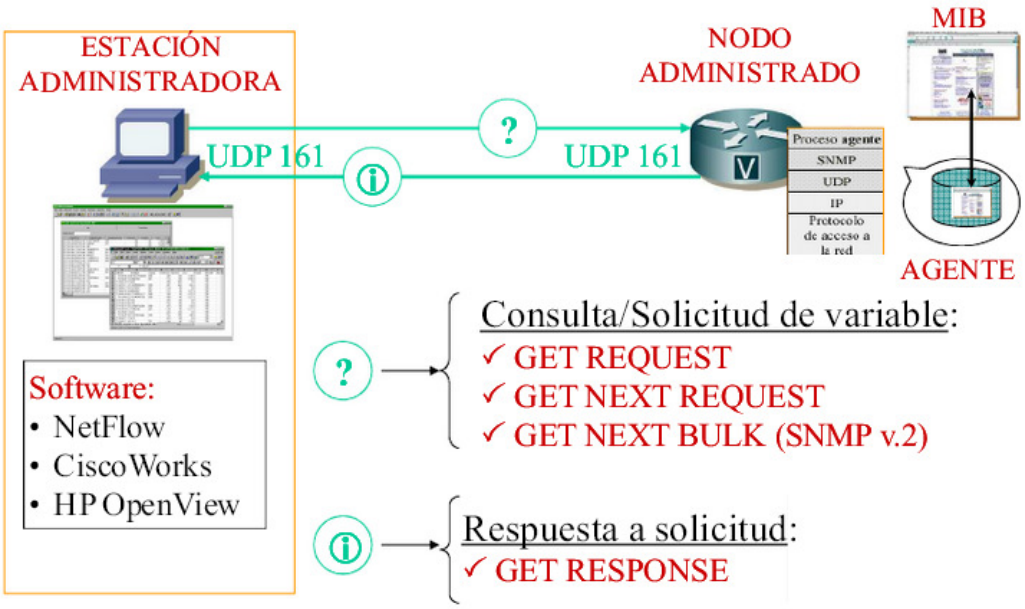


Figura: 18 Flujo de petición SNMP

Como se puede observar en la figura 18, el gestor o estación administradora se encarga de realizar las consultas mediante los mensajes GET REQUEST, GET NEXT REQUEST, GET NEXT BULK, para realizar el sondeo de determinada MIB con la intención de conseguir el valor especifico de una variable ubicada dentro del árbol de la MIB.

Este valor puede representar el valor del estado de uso de la CPU, memoria libre, puede representar también el valor del tráfico total que se está cursando en una interface determinada. Existen múltiples software para realizar este trabajo como ser NetFlow, Cisco Works, HP OpenView.

La información que se solicita desde el gestor hacia los dispositivos suele ir colectándose y almacenándose para poder calcular estadísticas.

Envío de TRAPS

Por otro lado ante un problema en un equipo (la caída de una interface, y/o la superación de un umbral predermindo) el equipo puede generar un trap (mensaje de notificación).

Como se puede observar en la figura 19, el dispositivo administrado envía un mensaje de interrupción o Trap al gestor.

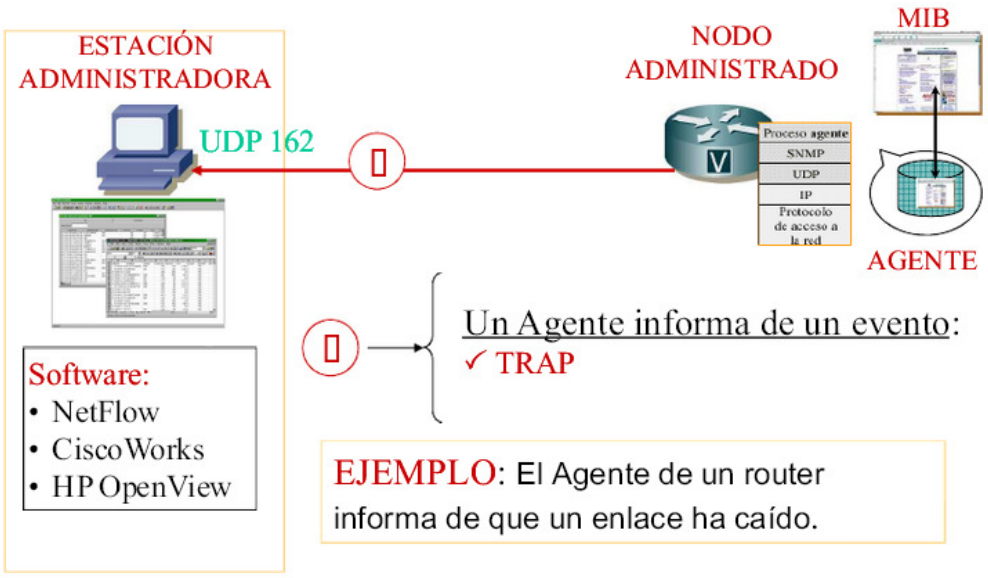


Figura: 19 Envío de TRAP SNMP

Herramientas para generar estadísticas

Por lo general el sondeo rutinario de interfaces y otros valores de las MIB de SNMP suele colectarse y almacenarse para poder generar informes y reportes estadísticos.

Las herramientas utilizadas suelen ser las llamadas RDtool es el acrónimo de Round Robin Database Tool . Se trata de una herramienta que trabaja con una base de datos que maneja planificación según Round-Robin. Esta técnica trabaja con una cantidad de datos fija, definida en el momento de crear la base de datos, y un puntero al elemento actual.

La base de datos se trata como si fuese un círculo, sobrescribiendo los datos almacenados con anterioridad una vez alcanzada la capacidad máxima de la misma. Esta capacidad máxima dependerá de la cantidad de información que se quiera conservar como historial.

Dentro de este tipo de herramientas podemos encontrar CACTI, MRTG, NSIM, etc. Como se puede ver en la figura 20 se puede representar la utilización de un determinado puerto o enlaces conociendo el tráfico actual entrante y saliente, como así también su valor máximo y

mínimo. Estas estadísticas pueden ser por hora, día, mes e incluso año dependiendo de la base de datos que se disponga.

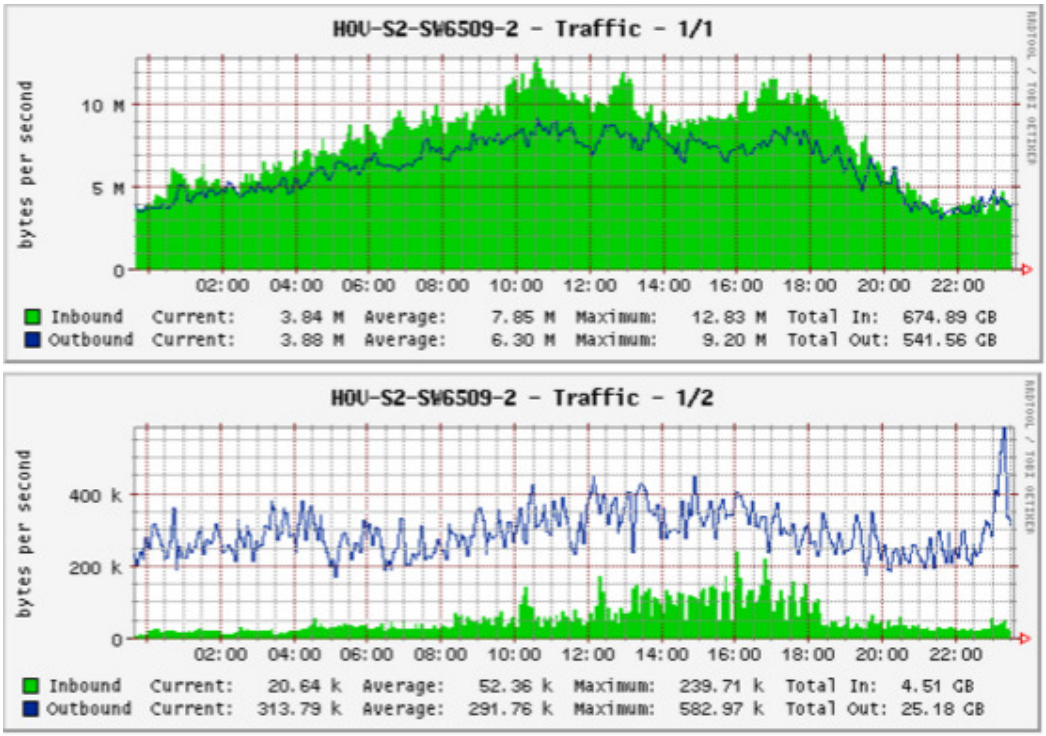


Figura: 20 Gráfico con RDDTool

Utilizando este tipo de herramienta se pueden establecer parámetros de servicios para conocer la ocupación real de un determinado enlace, los valores pico y valle de un enlaces, para determinar posibles rutas ante fallos.

Por otro lado es conveniente para poder establecer los puntos en los que existe un cuello de botella ya que posiblemente se vea reflejado en la grafica con una tipo de línea plano.

5.6.2. Definición de políticas de calidad de servicio en líneas de acceso.

Para poder garantizar en todo momento un ancho de banda fijo en una red de datos donde la infraestructura de red es compartida, es necesario aplicar calidad de servicio o QOS (Quality of Service), de esta manera se puede establecer patrones de acceso y diferentes niveles de calidad donde se pueda garantizar un determinado caudal aún durante congestión en la red.

Principalmente se definen dentro del portfolio de servicios 3 servicios de calidades de servicio:

- **Calidad de servicio Voz**: Es el trafico más importante dentro de la VPN del cliente, que debe ser tratado con mayor preferencia ya que seguramente es menos susceptible a retardos, jitter o delay este tipo de trafico suele ser el trafico (Voz sobre IP)

- **Calidad del servicio Video**: Es el tráfico de video o videoconferencia y/o telepresencia, como así también a tráfico Multimedia. Óptimo para aplicaciones sensibles al retardo, aplicaciones interactivas y, en general es tráfico que no puede ser retransmitido (tráfico UDP) que según el algoritmo de compresión suele ocupar mucho ancho de banda, cualquier problema de calidad o perdidas de paquetes se ve reflejado en la imagen como un pixelado o corte.

- **Calidad de servicio DATA ORO**: Es el tráfico más crítico dentro de la VPN del cliente, este tipo de tráfico se trata con la mayor prioridad, y ante congestión nunca será descartado. Generalmente Óptimo para aplicaciones críticas para el negocio del cliente.

- **Calidad de servicio DATA PLATA**: Es el tráfico de mediana criticidad dentro de la VPN del cliente, este tipo de tráfico se trata con mayor prioridad que el bronce, y ante congestión nunca será descartado, como se podrá observar se reserva un ancho de banda para él. Generalmente Óptimo para aplicaciones como ser el correo electrónico, trafico WEB y para conexión entre servidores no prioritarios para el negocio del cliente.

- **Calidad de servicio DATA BRONCE**: Es el tráfico de menor criticidad dentro de la VPN del cliente, pero que aún se considera necesario y que debe ser tratado con cierta prioridad para evitar que sea descartado en caso de congestión en la red. Se utiliza para la transferencia de archivo, descargas de contenido y actualización de servidores.

- **Clase DEFAULT**: Finalmente todo tráfico que no sea identificado y considerado necesario para alguna de las clases de calidad de servicio se marca como default y será el tráfico que se descartara en caso de congestión en la red se lo considera como best-effort.

5.6.3. Plantillas de configuración de la calidad de servicio.

Se entiende por calidad de servicio al mecanismo que se utiliza para identificar, marcar y garantizar un determinado tipo de tráfico con respecto al resto del tráfico que se va a transportar por un enlace, y que deberá ser enviado por la red.

El concepto de política de calidad de servicio (Service Policy) se aplica tanto para las interfaces de LAN (Red del cliente), como de WAN (interface de WAN que conecta el EDC con el PE de la red). Es importante establecer políticas de entrada como de salida para garantizar el correcto caudal por clase de tráfico (se definieron 3 clases ORO, PLATA, BRONCE de tráfico para ser priorizados con respecto al resto de tráfico). Todo tráfico que no sea identificado como ORO, PLATA, o BRONCE será marcado como trafico DEFAULT (trafico por defecto y no se prioriza se envía en modo best-effort).

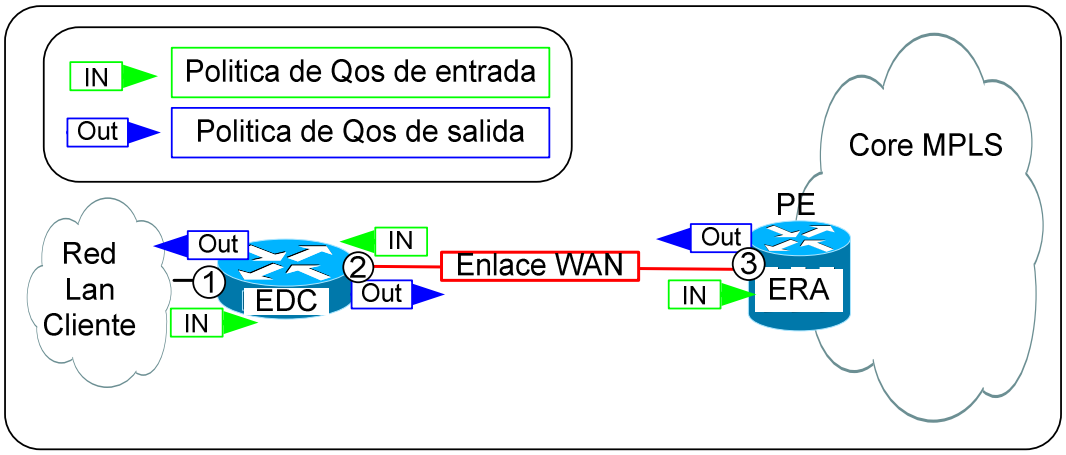


Figura: 21 Políticas de calidad de servicio

Según se puede observar en la figura 15, van a existir diferentes políticas de entrada y salida dependiendo del tipo interface que se hace referencia por ejemplo:

Interface LAN del cliente (1)

Va a existir una **política de entrada de tráfico**, que se va a encargar de identificar el trafico (esta identificación de trafico se puede realizar mediante la utilización de listas de acceso ACL, por rango de puertos TCP o UDP, o por parámetros de COS (marcado de trafico de nivel 2), o por la IP PRECEDENCE, o DSCP, etc.).

En esta política se va a marcar todo el tráfico que será colocado en cada una de las clases definidas (ORO, PLATA, BRONCE) y si no cumple con las condiciones de ese tráfico ira a la clase DEFAULT menos prioritaria y sin garantía de no ser descartada en caso de congestión de la red.

También deberá existir una **política de salida de tráfico** en la misma interface, para realizar el remarcado si fuera necesario. No se suele utilizar esta política para priorizar el tráfico, porque se entiende que no va existir congestión en la LAN del cliente.

Interface WAN del cliente (2)

Va a existir una **política de entrada de tráfico**, esta interface WAN es la que interconecta la LAN del cliente con la Red del proveedor. Muchas veces ocurre que el proveedor en su red remarca o utiliza otros parámetros de calidad de servicio (Diferente IP PRECEDENCE, o DSCP) por lo que a veces es necesario remarcar el trafico que nos envía el proveedor para que se adecue a la política de la LAN.

También deberá existir una **política de salida de tráfico** en la misma interface WAN, para realizar el marcado y priorización en el enlace WAN (recordar que el enlace WAN es de una velocidad menor que la LAN) por lo tanto es necesario la priorización para garantizar que el trafico realmente importante sea transportado por la red MPLS con la garantía que no será descartado si existe congestión en algún tramo de la red.

Interface WAN del PE (3)

Finalmente hay que analizar cómo será el tráfico de entrada en el lado WAN de la interface del PE donde va a existir una **política de entrada de tráfico**, esta política se va a encargar de realizar el conformado de tráfico, donde se va a limitar la entrada de trafico para que se adapte al caudal contratado (todo trafico que se sobrepase ese límite puede ser o bien marcado como DEFAULT para ser descartado en caso de congestión o se puede llegar a descartar directamente sin ser remarcado).

Como el proveedor es el administrador de todos los recursos compartidos por los que debe circular el tráfico de todos los clientes y servicios debe asegurar que el conformado de tráfico sea el correcto en cada acceso.

Igualmente como en el resto de interfaces, va a existir una **política de salida de tráfico** en la misma interface WAN, para realizar el marcado y priorización en el enlace WAN (recordar que el enlace WAN es de una velocidad menor que el resto de la red) por lo tanto es necesario la priorización para garantizar que el trafico realmente importante sea transportado por el enlace WAN y que solo será descartado en caso de congestión el menos prioritario.

En el portfolio de servicios se definieron unos Accesos de una velocidad de (512kbps, 1024Kbps, 2048Kbps, 4096Kbps y desde los 10Mbps hasta los 10Gbps), todos ellos también tiene predefinida 3 clases de servicios para poder priorizar y garantizar un ancho de banda mínimo por clase.

Estos accesos son independientes del tipo de tecnología utilizada en el enlace (FRAME-RELAY, ATM, ETHERNET)

Los accesos definidos en el portfolio tienen una calidad de servicio asociada y son los siguientes (estos valores son por defecto y puede ser modificados según las necesidades del cliente)

Tipo	Acceso	Oro	Plata	Bronce	Default
FR /ATM	512Kbps	320Kbps	128Kbps	48Kbps	16Kbps
FR /ATM	1024Kbps	640Kbps	256Kbps	96Kbps	32Kbps
FR /ATM	2048Kbps	1280Kbps	512Kbps	192Kbps	64Kbps
FR /ATM	4096Kbps	2560Kbps	1024Kbps	384Kbps	128Kbps
Ethernet	10 Mbps	6Mbps	3Mbps	0,75Mbps	0,25Mbps
Ethernet	100 Mbps	60Mbps	30Mbps	7,5Mbps	2,5Mbps
Ethernet	1Gbps	600Mbps	300Mbps	75Mbps	25Mbps
Ethernet	10Gbps	6Gbps	3Gbps	0,75Gbps	0,25Gbps

Plantilla genérica (para todos los caudales, y tipos de contratos) de configuración para el Equipo de Cliente (EDC).

Los EDC Cisco crean por defecto la clase ***class-default,*** y asocia a esta clase todo el tráfico que no haya sido clasificado en ninguna de las demás clases.

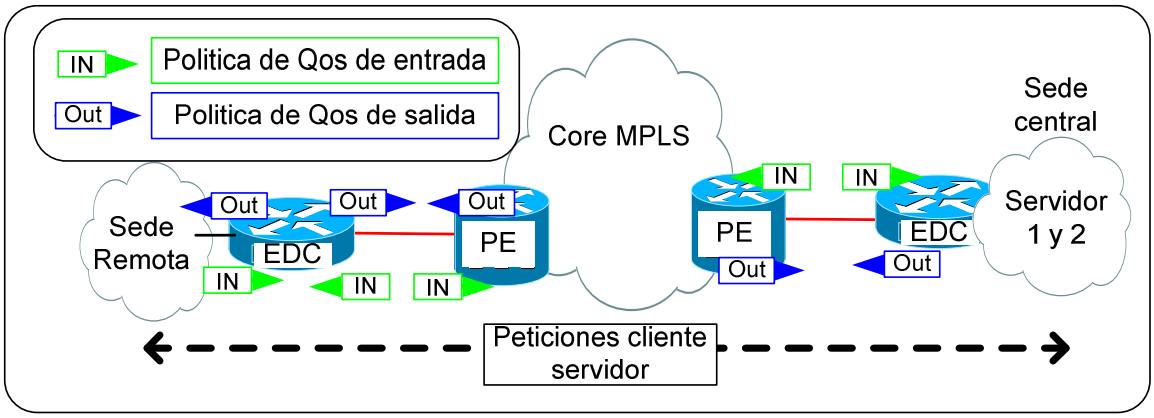


Figura: 22 Ejemplo de calidad de servicio extremo a extremo

Como se puede observar en la figura 16, desde la sede remota se quiere priorizar el tráfico que tiene como destino el servidor 1 y 2 de la sede central.

Para ello es necesario:

1) **Identificar el trafico mediante listas de acceso o por IP PRECEDENCE o DSCP.**

Para poder identificar el trafico que se considera interesante y que cumple las condiciones necesarias para ser asignada a una clase determinada (como ser Oro / Plata / Bronce), se utilizan ACL (Listas de control de acceso) en realidad estas listas de acceso, son filtro que permiten especificar o seleccionar el trafico (por IP origen y/o IP destino, Puerto TCP y/o UDP de Origen, Puerto TCP y/o UDP de destino).

A nivel de línea de comando del sistema operativo de Cisco (IOS), se configura de la siguiente manera:
Access-list <Numero> Accion Protocolo Origen Destino
Numero: Específica el número de lista de acceso para el tráfico que cumplirá con las condiciones para la clasificación de tráfico oro.
Acción: Permitir o denegar el trafico identificado, en este caso permit.
Protocolo: En este caso es IP (por lo que contiene tanto a UDP/TCP).
Origen: Mismos valores posibles que en destino, en nuestro caso se configura any (cualquier rango de direcciones).
Destino: valores posibles any, rango de direcciones (por ejemplo 10.0.0.0 0.0.0.255 corresponde la clase 10.0.0.0/24 donde 0.0.0.255 es la máscara inversa de la red o Wildcard), en nuestro caso es la dirección IP concreta de un solo equipos por lo que se configura con la palabra host y su dirección IP.

Entonces se pude utilizar la siguiente plantilla de configuración para poder identificar el tráfico y luego se deberá asignar a una clase especifica. Cabe aclarar que la identificación de tráfico se puede realizar también por la condición match de la clase, que se verá en el punto 2.

SEDES REMOTAS (sedes en las que no está el servidor 1 o 2)
access-list **<num acl Oro>** permit ip any host <dir_IP_servidor1>
access-list **<num acl Oro>** permit ip any host <dir_IP_servidor2>
access-list **<num acl Plata>** permit ip any host <dir_IP_servidor1>
access-list **<num acl Plata>** permit ip any host <dir_IP_servidor2>
access-list **<num acl Bronce>** permit ip any host <dir_IP_servidor1>
access-list **<num acl Bronce>** permit ip any host <dir_IP_servidor2>

SEDE CENTRAL (sede en la que se encuentre el servidor 1 o 2)
access-list **<num acl Oro>** permit ip host <dir_IP_servidor1> any
access-list **<num acl Oro>** permit ip host <dir_IP_servidor2> any
access-list **<num acl Plata>** permit ip host <dir_IP_servidor1> any
access-list **<num acl Plata>** permit ip host <dir_IP_servidor2> any
access-list **<num acl Bronce>** permit ip host <dir_IP_servidor1> any
access-list **<num acl Bronce>** permit ip host <dir_IP_servidor2> any

Se adjunta una tabla donde se puede observar la correspondencia entre las calidades de servicio predefinidas (Oro, Plata y Bronce) con su correspondiente valor de DSCP y Precedencia IP.

DSCP	Binario	Decimal	IP precedence	QoS
CS0	000 000	0	0	DATA(DEFAULT)
CS1	001 000	8	1	DATA(BRONCE)
AF11	001 010	10	1	DATA(BRONCE)
AF12	001 100	12	1	DATA(BRONCE)
AF13	001 110	14	1	DATA(BRONCE)
CS2	010 000	16	2	DATA(PLATA)
AF21	010 010	18	2	DATA(PLATA)
AF22	010 100	20	2	DATA(PLATA)
AF23	010 110	22	2	DATA(PLATA)
CS3	011 000	24	3	DATA(ORO)
AF31	011 010	26	3	DATA(ORO)
AF32	011 100	28	3	DATA(ORO)
AF33	011 110	30	3	DATA(ORO)
CS4	100 000	32	4	VIDEO
AF41	100 010	34	4	VIDEO
AF42	100 100	36	4	VIDEO
AF43	100 110	38	4	VIDEO
CS5	101 000	40	5	VOZ
EF	101 110	46	5	
CS6	110 000	48	6	
CS7	111 000	56	7	

2) Definición de la clase de servicio:

Se debe definir la clase de servicio, una vez identificado y marcado el tráfico, se deberá asignar a una de las 3 clases de servicio predefinidas.

En este caso en la clase ORO se va a completar con el trafico que cumpla con las condiciones de la lista de acceso `access-list` **`<num acl Oro>,`** y también con el trafico que tenga como IP precedence 3. Esta condición se cumple por que en el class-map existe la condición match-any.

class-map match-any ORO
    match access-group **<num acl Oro>**
    match ip precedence 3
class-map match-any PLATA
    match access-group **<num acl Plata>**
    match ip precedence 2
class-map match-any BRONCE
    match access-group **<num acl Bronce>**
    match ip precedence 1

3) Definir la política de servicio para el marcado del tráfico según QoS en la interfaz conectada a la interface LAN del cliente-

interface Ethernet <id interfaz LAN EDC>

```
        service-policy input Set_Precedencia_IN

policy-map Set_Precedencia_IN
class ORO
        set ip precedence 3
class PLATA
        set ip precedence 2
class BRONCE
        set ip precedence 1
class class-default
        set ip precedence 0
```

4) **Definir la política de servicio para la interface WAN en salida (si el trafico ya fue marcado en la interface LAN, puede no ser necesario volver a marcar el trafico con la precedence, pero si es necesario realizar el conformado de tráfico**.

A continuación se especifican la plantilla de configuración para cada tipo de enlaces (FRAME-RELAY, ATM, ETHERNET).

Enlace < caudal> Kbps (FRAME-RELAY) caudal (512kbps, 1024kbps, 2048kbps,4098kbps)

```
Interface serial  <id interfaz>
        frame-relay traffic-shaping

interface Serial  <id interfaz>.<numero subinterfaz> point-to-point
        no cdp enable
        frame-relay interface-dlci <dlci>
                class <tipo contrato>
                map-class frame-relay <tipo contrato>
                frame-relay cir <caudal total bps>
                frame-relay mincir <caudal total bps>
                frame-relay bc <caudal total bps/100>
                service-policy output QoS_Out  (política de salida en el enlace WAN)
                service-policy input QoS_In  (política de entrada en el enlace WAN)
                frame-relay fragment <Tamaño fragmento>
```

Enlace de Acceso E1 (G.703 o V.35), E3/T3 caudal (512kbps, 1024kbps, 2048kbps,4098kbps)

(Se especifica caudal por que la utilización del E3/T3 es compartido por varios clientes)

```
#Se define la política de QoS DE SALIDA WAN#
policy-map QoS_Out
class ORO
        priority <caudal ORO Kbps>
        police <caudal  bps> <ráfaga ORO> <ráfaga max ORO> conform-action set-precedence-transmit 5 exceed-action drop
```

class PLATA
bandwidth <caudal PLATA Kbps>
police <caudal Prec4 bps> <ráfaga PLATA> <ráfaga max PLATA> conform-action set-prec-transmit 4 exceed-action set-prec-transmit 4
class BRONCE
bandwidth <caudal BRONCE Kbps>
random-detect
police <caudal BRONCE bps> <ráfaga BRONCE> <ráfaga max BRONCE> conform-action set-prec-transmit 3 exceed-action set-prec-transmit 3
class class-default
bandwidth <caudal DEFAULT Kbps>
random-detect
police <caudal Prec0 bps> <ráfaga Prec0 > <ráfaga max Prec0 > conform-action set-prec-transmit 0 exceed-action set-prec-transmit 0
 # Se define la política de QoS DE ENTRADA WAN#
policy-map QoS_In
class ORO
set ip precedence 3
class PLATA
set ip precedence 2
class BRONCE
set ip precedence 1
class class-default
set ip precedence 0
#se aplica la política a la interface que conecta con el PE#
interface serial<id interfaz>:<timeslot>
service-policy output QoS_Out
service-policy input QoS_In
max-reserved-bandwith 100

Acceso ATM

interface Ethernet <id interfaz LAN EDC>
service-policy input Set_Precedencia

policy-map QoS_Out
class ORO
bandwidth <caudal_ORO kbps>
set ip precedence 6
class PLATA
PRORITY <caudal_PLATA kbps>
police <caudal PLATA bps> <ráfaga PLATA> <ráfaga max PLATA> conform-action set-precedence-transmit 5 exceed-action drop
class BRONCE
bandwidth <caudal_BRONCE kbps>
set ip precedence 4
class class-default
bandwidth <caudal Prec0 Kbps>
random-detect
set ip precedence 0

 # Se define la política de QoS DE ENTRADA WAN#
policy-map QoS_In
class ORO
set ip precedence 3
class PLATA
set ip precedence 2
class BRONCE
set ip precedence 1
class class-default
set ip precedence 0

#se aplica la política a la interface que conecta con el PE#
interface ATM <id interfaz>.<número subinterfaz> point-to-point
pvc <itv>/<icv>
vbr-nrt <pico> <media> <rafaga>
encapsulation aal5snap
service-policy output QoS_Out
service-policy input QoS_In
max-reserved-bandwith 100

Multilink PPPoATM

```
vc-class atm SALIDA_PPPOA
protocol ppp Virtual-Template1
  vbr-nrt <pico> <media> <ráfaga>
  encapsulation aal5snap
interface Multilink1
          ip address <DIR_IP_WAN_CPE > <MASCARA_IP_WAN_CPE>
           load-interval 30
           ppp multilink
          ppp multilink interleave
           ppp multilink group 1
          ppp multilink fragment delay 10
          max-reserved-bandwidth 100
           service-policy input QoS_In
          service-policy output QoS_Out

interface ATM<id interfaz>
          description <descripcion interfaz>
          no ip address
           no ip proxy-arp
          no ip mroute-cache
          load-interval 30
           no atm ilmi-keepalive
          dsl operating-mode auto
          max-reserved-bandwidth 100

interface ATM<id interfaz>.<numero subinterfaz> point-to-point
          pvc <vpi>/<vci>
           class-vc SALIDA_PPPOA
            tx-ring-limit <valor tx-ring>
           oam-pvc manage
            oam retry <celulas perdidas> <celulas en espera> <tiempo>
 !
interface Virtual-Template1
           no ip address
          ppp multilink
          ppp multilink group 1
           max-reserved-bandwidth 100
```

Acceso Fast Ethernet/GigabitEthernet (Ejemplo Acceso Ethernet 10Mpbs)

En el caso de accesos Ethernet, se define un policer (para poder conformar el tráfico salida, de cada una de las clases)
A nivel línea de comando la estructura del policer es la siguiente:

Police ***<caudal clase_bps> <ráfaga_ clase> <ráfaga max_clase>*** conform-action set-precedence-transmit ***clase*** exceed-action drop
Donde:
<caudal_clase_bps> : Define el mínimo de ancho de banda garantizado para la clase de servicio correspondiente. (ORO=6Mbps, PLATA=3Mbps, BRONCE=768Kbps, default=256kbps)

<ráfaga_clase>: Se define el tráfico a ráfagas que podrá soportar y guardar en el buffer para garantizar el ancho de banda (las ráfagas pueden ser de 7,2Mbps) de los 7,2Mbps son 6Mbps de banda mínimo garantizado + 1,2Mbps de ráfaga).

<ráfaga_max_clase>: Valor máximo de ráfaga que podrá soportar y guardar en el buffer para garantizar el ancho de banda de la clase (el valor máximo será de 8,4Mbps) de los 8,4Mbps son 6Mbps de Ancho de banda mínimo garantizado + 2,4 Mbps de pico máximo de ráfaga.

```
interface Fast Ethernet <id interfaz> / GigatEthernet <id interfaz>
        description <descripcion interfaz>
        ip address <dir IP WAN EDC> 255.255.255.252
         ip mtu 1500
         no ip redirects
        no ip directed-broadcast
        no ip proxy-arp
         full-duplex
         no cdp enable
        no shutdown
        service-policy input QoS_In
        service-policy output Qos_Out
        exit

policy-map QoS_Out
 class ORO
   bandwith 6144
   police 6144000 1152000 2304000 conform-action set-prec-transmit 3 exceed-action    drop
violate-action drop
 class PLATA
   bandwith 3072
   police 3072000 576000 1152000 conform-action set-prec-transmit 2 exceed-action drop
violate-action drop
 class BRONCE
   bandwith 768
   police 768000 144000 288000 conform-action set-prec-transmit 1 exceed-action drop
violate-action drop
 class class-default
   bandwidth 256
   police 256000 48000 96000 conform-action set-prec-transmit 0 exceed-action drop  violate-
action drop
```

```
policy-map QoS_In
 class ORO
  set precedence 3
 class PLATA
  set precedence 2
 class BRONCE
  set precedence 1
 class class-default
  set ip precedence 0
```

<u>Acceso GigabitEthernet</u> (multiple VRF's y con Vlans) Para acceso 100Mbps

En el caso de accesos Ethernet, se define un policer (para poder conformar el tráfico salida, de cada una de las clases)
A nivel línea de comando la estructura del policer es la siguiente:

Police ***<caudal clase_bps> <ráfaga_ clase> <ráfaga max_clase>*** conform-action set-precedence-transmit ***clase*** exceed-action drop
Donde:
<caudal_clase_bps>: Define el mínimo de ancho de banda garantizado para la clase de servicio correspondiente. (ORO=60Mbps, PLATA=30Mbps, BRONCE=7680Kbps, default=2560kbps).

<ráfaga_clase>: Se define el tráfico a ráfagas que podrá soportar y guardar en el buffer para garantizar el ancho de banda (las ráfagas pueden ser de 72Mbps) de los 72Mbps son 60Mbps de banda mínimo garantizado + 12Mbps de ráfaga).

<ráfaga_max_clase>: Valor máximo de ráfaga que podrá soportar y guardar en el buffer para garantizar el ancho de banda de la clase (el valor máximo será de 84Mbps) de los 84Mbps son 60Mbps de Ancho de banda mínimo garantizado + 24 Mbps de pico máximo de ráfaga.

```
interface GigatEthernet <id interfaz>.<id Vlan>
        description <descripcion interfaz>
        ip address <dir IP WAN EDC> 255.255.255.252
        encapsulation dot1q id.vlan
         ip mtu 1500
        no shutdown
        service-policy input QoS_In
        service-policy output Qos_Out
        exit

policy-map QoS_Out
 class ORO
   bandwith 61440
   police 61440000 11520000 23040000 conform-action set-prec-transmit 3 exceed-action
drop   violate-action drop
 class PLATA
   bandwith 30720
   police 30720000 5760000 11520000 conform-action set-prec-transmit 2 exceed-action drop
violate-action drop
 class BRONCE
   bandwith 7680
   police 7680000 1440000 2880000 conform-action set-prec-transmit 1 exceed-action drop
violate-action drop
 class class-default
   bandwidth 2560
   police 2560000 480000 960000 conform-action set-prec-transmit 0 exceed-action drop
violate-action drop

policy-map QoS_In
 class ORO
  set precedence 3
 class PLATA
```

```
 set precedence 2
class BRONCE
 set precedence 1
class class-default
 set IP precedence 0
```

5.6.3.1. Configuración adicional para EDC gestionados.

- ✓ Plantilla de configuración para equipos de clientes (EDC) de servicios VPN **Gestionados.**

En los EDC gestionados además hay que incluir estos parámetros para poder tener acceso desde el centro de gestión.

#Acceso por gestión SNMP desde el centro de servicios

Para recibir las alarmas de SNMP, y poder realizar el sondeo de interfaces y demás parámetros del EDC es necesario establecer community de lectura y escritura

```
snmp-server community <nombre_comunidad_escritura> RW <lista-acceso-snmp>
snmp-server community <nombre_comunidad_lectura> RO <lista-acceso-snmp>

access-list <lista-acceso-snmp> permit IP <red_gestion_EDCs>
```

Se garantiza el acceso desde un origen (Centro de gestión) mediante una lista de acceso
#Acceso por telnet desde el centro de gestión

```
access-list <lista-filtro telnet> permit host <dir_IP_WAN_PE>
access-list <lista-filtro telnet> permit <red_gestion_EDCs> <máscara>
line vty 0 4
        access-class <lista-filtro telnet> in
```

- ✓ Plantilla de configuración para equipos de clientes (EDC) de servicios STI (Servicio de trafico internet)

Las plantillas de configuración del servicio STI son iguales a los EDC no gestionados.

5.6.4. Plantillas de configuración en los PE's CISCO.

5.6.4.1. Configuración ATM 4096Kbps.

4096Kbps(2560Kbps ORO, 1024Kbps PLATA, 384Kbps BRONCE, 128Kbps DEFAULT)

Configuración para enlace ATM de 4096Kbps (como se puede observar la calidad de servicio se aplica en el PVC)

```
interface ATM 7/0/0.<Nro_subinterface> point-to-point
        description <descripcion interfaz_VPN>
        bandwidth 4096
        ip vrf forwarding <VPN_XXXXX>
        ip address <IP_WAN_PE>
        no ip redirects
        snmp trap link-status
        no atm enable-ilmi-trap
        pvc VC/VCI
                vbr-nrt  4096 4096 1
                oam-pvc manage
                oam retry 3 3 5
                encapsulation aal5snap
                service-policy in QoS_In_7/0/0. <Nro_subinterface>
                service-policy out QoS_Out_7/0/0. <Nro_subinterface>

#Se definen las clases de servicio y se clasifica el trafico##
class-map match-all ORO
 match ip precedence 3
class-map match-all PLATA
 match ip precedence 2
class-map match-all BRONCE
 match ip precedence 1

#Se define la política de QOS de entrada y salida #
policy-map QoS_In_7/0/0.<Nro_subinterface>
 class ORO
  police cir 2560000 bc 480000 be 960000 conform-action set-mpls-exp-imposition-transmit 3
exceed-action drop violate-action drop
 class PLATA
  police cir 1024000 bc 192000 be 384000 conform-action set-mpls-exp-imposition-transmit 2
exceed-action drop violate-action drop
 class BRONCE
  police cir 394000 bc 74000 be 148000 conform-action set-mpls-exp-imposition-transmit 1
exceed-action drop violate-action drop
 class class-default
  police cir 131000 bc 24000 be 49000 conform-action set-mpls-exp-imposition-transmit 0
exceed-action drop violate-action drop
```

```
policy-map QoS_Out_7/0/0.<Nro_subinterface>
 class ORO
  police cir 2560000 bc 480000 be 960000 conform-action transmit exceed-action drop
violate-action drop
 class PLATA
  police cir 1024000 bc 192000 be 384000 conform-action transmit exceed-action drop
violate-action drop
 class BRONCE
  police cir 394000 bc 74000 be 148000 conform-action transmit exceed-action drop violate-
action drop
 class class-default
  police cir 131000 bc 24000 be 49000 conform-action transmit exceed-action drop violate-
action drop
```

5.6.4.2. Configuración FRAME-RELAY 512kbps.

512Kbps (320Kbps ORO, 128Kbps PLATA, 48Kbps BRONCE, 16Kbps DEFAULT)

Ejemplo de configuración para enlace FRAME-RELAY de 512Kbps (como se puede observar la calidad de servicio se aplica en el PVC)

```
interface Serial1/3/0.18 point-to-point
 description <descripcion interfaz_VPN>
 bandwidth 256
 ip vrf forwarding <Datos_VPN>
 ip address <IP_Wan_PE>
 no ip proxy-arp
 no cdp enable
 frame-relay interface-dlci 18
  class FR_1/3/0.18
        map-class frame-relay FR_1/3/0.18
        service-policy input QoS_In_1/3/0.18
        service-policy output Shaping_1/3/0.18

#Se define la política de QOS de entrada y salida #
policy-map QoS_In_1/3/0.18
 class ORO
  police cir 320000 bc 60000 be 120000 conform-action set-mpls-exp-imposition-transmit 3
exceed-action drop violate-action drop
 class PLATA
  police cir 128000 bc 24000 be 48000 conform-action set-mpls-exp-imposition-transmit 2
exceed-action drop violate-action drop
 class BRONCE
  police cir 48000 bc 9000 be 18000 conform-action set-mpls-exp-imposition-transmit 1
exceed-action drop violate-action drop
 class class-default
  police cir 16000 bc 3000 be 6000 conform-action set-mpls-exp-imposition-transmit 0
exceed-action drop violate-action drop

#Se definen las clases de servicio y se clasifica el trafico##
class-map match-all ORO
```

```
 match ip precedence 3
class-map match-all PLATA
 match ip precedence 2
class-map match-all BRONCE
 match ip precedence 1
```

5.6.4.3. Configuración Ethernet.100Mbps

100Mbps (60Mbps ORO, 30Mbps PLATA, 7,5Mbps BRONCE, 2,4Mbps DEFAULT).

```
interface Fast Ethernet <id interfaz> / GigatEthernet <id interfaz>
        description <descripcion interfaz>
        ip address <dir IP WAN PE> 255.255.255.252
         ip mtu 1500
         no ip redirects
        no ip directed-broadcast
        no ip proxy-arp
         full-duplex
         no cdp enable
        no shutdown
        service-policy input QoS_In
        service-policy output Qos_Out
        exit

policy-map QoS_Out
 class ORO
   bandwith 61440
   police 61440000 11520000 23040000 conform-action set-prec-transmit 3 exceed-action
drop   violate-action drop
 class PLATA
   bandwith 30720
   police 30720000 5760000 11520000 conform-action set-prec-transmit 2 exceed-action drop
violate-action drop
 class BRONCE
   bandwith 7680
   police 7680000 1440000 2880000 conform-action set-prec-transmit 1 exceed-action drop
violate-action drop
 class class-default
   bandwidth 2560
   police 2560000 480000 960000 conform-action set-prec-transmit 0 exceed-action drop
violate-action drop

policy-map QoS_In
 class ORO
  set precedence 3
 class PLATA
  set precedence 2
 class BRONCE
  set precedence 1
 class class-default
  set IP precedence 0
```

5.6.5. Plantillas de configuración en los PE's JUNIPER.

5.6.5.1. Configuración ATM 4096Kbps.

4096 Kbps(2560Kbps ORO, 1024Kbps PLATA, 384Kbps BRONCE, 128Kbps DEFAULT).

```
#Se aplica el policy en la subinterface#

configuration interfaces at-7/2/0.1790
description "<descripcion interfaz>";
vci 17.90;
shaping {
   vbr peak 4096000 sustained 4096000 burst 4200;
}
atm-scheduler-map atm_7/2/0.1790;
family inet {
   mtu 1500;
   filter {
      input-list QOS_IN_7/2/0.1790;
      output-list QOS_OUT_7/2/0.1790;
   }
   address <IP_WAN_PE>/30;
}
family mpls;

#Se define la política QOS de salida#
configuration firewall family inet filter QOS_OUT_7/2/0.1790
term limitar {
   then {
      policer Total_QoS_OUT_7/2/0.1790;
      next term;
   }
}

term ORO {
   from {
      precedence 3;
   }
   then {
      policer  ORO_QoS_OUT_7/2/0.1790;
      loss-priority high;
      forwarding-class expedited-forwarding;
      accept;
   }
}
term PLATA {
   from {
      precedence 2;
   }
   then {
      policer  PLATA_QoS_OUT_7/2/0.1790;
      loss-priority high;
```

```
      forwarding-class expedited-forwarding;
      accept;
   }
}
term BRONCE {
   from {
      precedence 1;
   }
   then {
      policer  BRONCE_QoS_OUT_7/2/0.1790;
      loss-priority high;
      forwarding-class expedited-forwarding;
      accept;
   }
}
term DEFAULT {
   then {
      policer  DEFAULT_QoS_OUT_7/2/0.1790;
      loss-priority low;
      forwarding-class best-effort;
      accept;
   }
}

configuration firewall policer ORO_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 2560k;
   burst-size-limit 256k;
}
configuration firewall policer PLATA_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 1024k;
   burst-size-limit 102k;
}
configuration firewall policer BRONCE_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 384k;
   burst-size-limit 38k;
}
configuration firewall policer DEFAULT_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 128k;
   burst-size-limit 12k;
}

configuration firewall policer Total_QoS_OUT_7/2/0.1790
if-exceeding {
   bandwidth-limit 4096k;
   burst-size-limit 4096000;
}
then discard;
```

5.6.5.2. Configuración FRAME-RELAY 512kbps.

512 Kbps (320Kbps ORO, 128Kbps PLATA, 48Kbps BRONCE, 16Kbps DEFAULT)

```
show configuration interfaces e3-0/1/0.16
description "descripcion";
dlci 16;
family inet {
   mtu 1500;
   filter {
      input QOS_IN_0/1/0.16;
      output QOS_OUT_0/1/0.16;
   }
   address <IP_WAN_PE>/30;
}
family mpls;

#Se define la política de QOS de ENTRADA #
show configuration firewall family inet filter QOS_IN_0/1/0.16
term limitar {
   then {
      policer TOTAL_IN_0/1/0.16;
      next term;
   }
}
term ORO {
   from {
      precedence 3;
   }
   then {
      count trafico_ORO_input_0/1/0.16;
      loss-priority high;
      forwarding-class assured-forwarding;
      accept;
   }
}
term PLATA {
   from {
      precedence 2;
   }
   then {
      count trafico_PLATA_input_0/1/0.16;
      loss-priority low;
      forwarding-class assured-forwarding;
      accept;
   }
}
term BRONCE {
   from {
      precedence 2;
   }
```

```
   then {
      count trafico_PLATA_input_0/1/0.16;
      loss-priority low;
      forwarding-class assured-forwarding;
      accept;
   }
}

term DEFAULT {
   then {
      count trafico_DEFAULT_input_0/1/0.16;
      loss-priority low;
      forwarding-class assured-forwarding;
      accept;
   }
}

#Se define la política de QOS de SALIDA #

show configuration firewall family inet filter QOS_OUT_0/1/0.16
term ORO {
   from {
      precedence 3;
   }
   then {
      policer ORO_out_0/1/0.16;
      count trafico_ORO_output_0/1/0.16;
      loss-priority low;
      forwarding-class expedited-forwarding;
      accept;
   }
}
term PLATA {
   from {
      precedence 2;
   }
   then {
      policer PLATA_out_0/1/0.16;
      count trafico_PLATA_output_0/1/0.16;
      loss-priority low;
      forwarding-class expedited-forwarding;
      accept;
   }
}
term BRONCE {
   from {
      precedence 1;
   }
   then {
      policer BRONCE_out_0/1/0.16;
      count trafico_BRONCE_output_0/1/0.16;
      loss-priority low;
```

```
      forwarding-class assured-forwarding;
      accept;
   }
}

term DEFAULT {
   then {
      count trafico_DEFAULT_output_0/1/0.16;
      loss-priority low;
      forwarding-class best-effort;
      accept;
   }
}

#Se define el conformado de tráfico o policer#
configuration firewall policer ORO_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 320k;
   burst-size-limit 32k;
}
configuration firewall policer PLATA_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 128k;
   burst-size-limit 12k;
}
configuration firewall policer BRONCE_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 48k;
   burst-size-limit 4k;
}
configuration firewall policer DEFAULT_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 16k;
   burst-size-limit 2k;
}
```

5.6.5.3. Configuración Ethernet.1000Mbps

1 Gbps (600Mbps ORO, 300Mbps PLATA, 75Mbps BRONCE, 25Mbps DEFAULT).

```
#Se aplica el policy en la subinterface#
interfaces ge-3/2/0.131
description "<descripcion interfaz>";
vlan-id 131;
family inet {
   mtu 1500;
   filter {
      input QoS_IN_3/2/0.131;
      output QoS_OUT_3/2/0;
   }
   address <IP_WAN_PE/30>;
}
family mpls;

#Se define la política QOS de entrada#
configuration firewall family inet filter QoS_IN_3/2/0.131

term ORO {
   from {
      precedence 3;
   }
   then {
      policer  ORO_QoS_OUT_3/2/0;
      loss-priority high;
      forwarding-class expedited-forwarding;
      accept;
   }
}
term PLATA {
   from {
      precedence 2;
   }
   then {
      policer  PLATA_QoS_OUT_3/2/0;
      loss-priority high;
      forwarding-class expedited-forwarding;
      accept;
   }
}

term BRONCE {
   from {
      precedence 1;
   }
   then {
      policer  BRONCE_QoS_OUT_3/2/0;
      loss-priority high;
```

```
      forwarding-class assured-forwarding;
      accept;
   }
}
term DEFAULT {
   then {
      policer  DEFAULT_QoS_OUT_3/2/0;
      loss-priority low;
      forwarding-class best-effort;
      accept;
   }
}
#Se define el conformado de tráfico o policer#
configuration firewall policer ORO_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 600m;
   burst-size-limit 60m;
}
configuration firewall policer PLATA_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 300m;
   burst-size-limit 30m;
}
configuration firewall policer BRONCE_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 75m;
   burst-size-limit 8m;
}
configuration firewall policer DEFAULT_QoS_OUT_3/2/0
if-exceeding {
   bandwidth-limit 25m;
   burst-size-limit 3m;
}
```

5.6.6. Plantillas de configuración de la VPNs.

#creación de una VPN en un PE (Cisco)#

```
IP vrf vpn_<NumeroAS>_<idVPN>
 description "Nombre del Cliente"
 rd NumeroAS:NroVRF
 export map exportar_ NumeroAS_NroVRF
 route-target export NumeroAS_NroVRF
 route-target import NumeroAS_NroVRF
 route-target import  NuestroAS:VRF_Gestión
 maximum routes Contratadas 90
!
```

<Numero AS>= Numero de AS por ejemplo AS3352 (Telefónica de España)
<idVPN>= Valor interno que se provee por los sistemas de gestión.

#Asignación de una VPN a un interface en un PE (Cisco)#

```
 interface <tipo interfaz><id interfaz>
 ip vrf forwarding vpn_<AS>_<id vpn>
 ip address <dir IP WAN EDC> 255.255.255.252
exit
```

#Configuración del address-family en un PE (Cisco)#

```
router bgp <NuestroAS>
 bgp router-id < loopback0>
 bgp log-neighbor-changes
 bgp deterministic-med
 neighbor ibgp-full-mesh peer-group
 neighbor ibgp-full-mesh remote-as XXXX
 neighbor ibgp-full-mesh description Sesiones iBGP Full Mesh
 neighbor ibgp-full-mesh update-source Loopback0

address-family ipv4 vrf VPN_<NumeroAS>_<idVPN>
  no synchronization
  bgp aggregate-timer 0
  redistribute static
  redistribute connected route-map connected2bgp-gestion
  neighbor <XX.XX.XX.XX> remote-as< AS_vecino>
  neighbor <XX.XX.XX.XX> activate
  exit-address-family
```

6. Conclusiones.

Al finalizar el proyecto se puede decir que se han alcanzado satisfactoriamente los objetivos específicos que se contemplaban para el Diseño de una Red WAN, que consistían en realizar un diseño de una red para un operador de nivel internacional.

Durante el proyecto se justifico la necesidad de la utilización de MPLS para proveer a la red un de CORE capaz de transportar de manera veloz y eficiente gran volumen de tráfico desde los 10Gbps hasta más de 1Tbps.

Si se toma como valor de referencia 2Mbps (Valor medio del servicio de VPN) para analizar la capacidad de la red en cuanto a número de clientes (Al ser un operador Mundial su foco no son usuarios finales sino interconectar y ofrecer servicios a empresas), se puede calcular con una redundancia del 100%(2 enlaces troncales 1 Tbps con una ocupación máxima del 50%), la red es capaz de dar servicio a mas de 50.000 VPN's y transportar mas de 1Tbps de tráfico.

Su diseño permite escalar en cuanto a equipamiento por ampliación de nuevas zonas geográficas y/o también por necesidad de crecimiento por capacidad, ya sea en enlaces troncales como así también en cuanto a número de equipos de CORE.

7. Bibliografía.

http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps5103/product_data_sheet09186a008015cfeb_ps368_Products_Data_Sheet.html

http://www.cisco.com/en/US/prod/collateral/routers/ps5763/CRS-3_8-Slot_DS.html

http://www.cisco.com/en/US/products/ps5854/index.html

http://www.juniper.net/us/en/products-services/routing/t-tx-series/t640/#literature

http://www.juniper.net/us/en/products-services/routing/mx-series/mx960/

http://es.wikipedia.org/wiki/STM-1

http://www.cisco.com/en/US/prod/collateral/modules/ps2831/ps4370/product_data_sheet09186a0080092241_ps368_Products_Data_Sheet.html

http://es.wikipedia.org/wiki/E1

http://www.cisco.com/en/US/products/hw/routers/ps368/products_relevant_interfaces_and_modules.html

http://en.wikipedia.org/wiki/Digital_Signal_1

http://www.juniper.net/techpubs/en_US/junos12.2/information-products/topic-collections/config-guide-network-interfaces/book-config-guide-network-interfaces-channelized.pdf#search=%22E1%2FT1%20pic%20MX960%22

http://www.speedguide.net/articles/bits-bytes-and-bandwidth-reference-guide-115

http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_Digital_Plesi%C3%B3crona

http://es.wikipedia.org/wiki/Frame_Relay

http://es.wikipedia.org/wiki/Gigabit_Ethernet

http://es.wikipedia.org/wiki/IEEE_802.1Q

http://es.wikipedia.org/wiki/BGP

http://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol

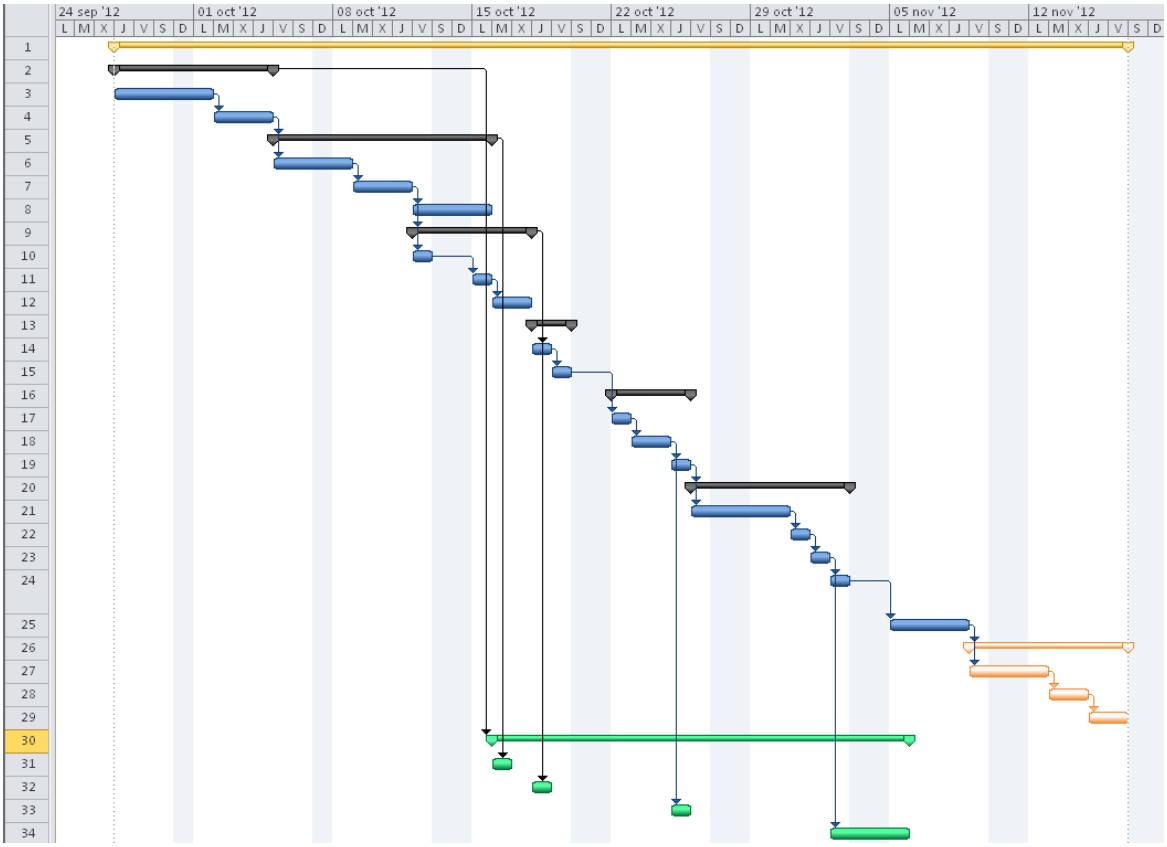
http://es.wikipedia.org/wiki/MRTG

http://www.cacti.net/

8. ANEXOS.

8.1.(Diagrama de Gantt)

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	**Planificación del proyecto**	**39 días**	**jue 27/09/12**	**vie 16/11/12**	
2	**Justificación del TFC**	**7 días**	**jue 27/09/12**	**jue 04/10/12**	
3	Definición Objetivos	4 días	jue 27/09/12	lun 01/10/12	
4	Enfoque y método seguido	3 días	mar 02/10/12	jue 04/10/12	3
5	**Funcionalidad y Finalidad de la red**	**8 días**	**vie 05/10/12**	**lun 15/10/12**	**4**
6	Eleccion de equipamiento	3 días	vie 05/10/12	lun 08/10/12	4
7	Justificacion de la tecnologia a utilizar	3 días	mar 09/10/12	jue 11/10/12	6
8	Caracteristicas del trafico y Normas de Ingeniería	2 días	vie 12/10/12	lun 15/10/12	7
9	**Diseño de Red**	**4 días**	**vie 12/10/12**	**mié 17/10/12**	**7**
10	Mapa topologico	1 día	vie 12/10/12	vie 12/10/12	7
11	Direccionamiento IP	1 día	lun 15/10/12	lun 15/10/12	10
12	Diseño de red fuera de banda y VPN de gestión	2 días	mar 16/10/12	mié 17/10/12	11
13	**Definicion de mecanismos de alta disponibilidad**	**2 días**	**jue 18/10/12**	**vie 19/10/12**	
14	Mecanismos de Alta disponiblidad	1 día	jue 18/10/12	jue 18/10/12	9
15	Equilibrio entre coste y disponibilidad	1 día	vie 19/10/12	vie 19/10/12	14
16	**Crecimiento y Nuevas tecnologias**	**4 días**	**lun 22/10/12**	**jue 25/10/12**	
17	Normas de Ingeniería para crecimiento en capacidad	1 día	lun 22/10/12	lun 22/10/12	15
18	Normas de Ingeniería para aumento de nodos de red	2 días	mar 23/10/12	mié 24/10/12	17
19	Estimación de costes por crecimiento	1 día	jue 25/10/12	jue 25/10/12	18
20	**Definición de Servicios**	**6 días**	**vie 26/10/12**	**vie 02/11/12**	**19**
21	Creación del portfolio de servicios	3 días	vie 26/10/12	mar 30/10/12	19
22	Politicas de calidad de servicios	1 día	mié 31/10/12	mié 31/10/12	21
23	Creación de plantillas de configuración	1 día	jue 01/11/12	jue 01/11/12	22
24	Politicas de filtrado, importación y exportación de prefijos en VRF's	1 día	vie 02/11/12	vie 02/11/12	23
25	Conclusiones	4 días	lun 05/11/12	jue 08/11/12	24
26	**Anexos**	**6 días**	**vie 09/11/12**	**vie 16/11/12**	**25**
27	Caracteristicas del hardware	2 días	vie 09/11/12	lun 12/11/12	25
28	Configuración Basica de gestion SNMP	2 días	mar 13/11/12	mié 14/11/12	27
29	Bibliografia y referencias tecnicas	2 días	jue 15/11/12	vie 16/11/12	28
30	**<Productos Obtenidos "Entregables">**	**15 días**	**mar 16/10/12**	**lun 05/11/12**	**2**


24 sep '12
01 oct '12
08 oct '12
15 oct '12
22 oct '12
29 oct '12
05 nov '12
12 nov '12
L M X J V S D
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34

8.2.(Script de análisis de Logs)

```
#!/usr/bin/python
import sys

def greet(name):
   print 'Hello', name
def loadDevicesDb(devicesFileName):
   db = {}
   f = open(devicesFileName, 'r')
   lines = f.readlines();
   for i, l in enumerate(lines):
      fields = l.split();
      devName = fields[0]
      brand   = fields[1]
      if db.has_key(devName):
         print "Warning: Duplicate name:", devName, "in:",
         print  devicesFileName, "line #", i
         continue
      db[devName] = brand;
   return db


def processSysLog(devDb, syslogFileName, brandSel, deviceSel):
   f = open(syslogFileName, 'r')
   lines = f.readlines();
   brandAll = brandSel == "all"
   devAll   = deviceSel == "all"
   for i, l in enumerate(lines):
      fields = l.split();
      if len(fields) < 3:
         print "Warning: Invalid syslog line#:", str(i+1), l
         continue
      devName = fields[3]
      if not devDb.has_key(devName):
         print "Warning: Device", devName, "in line#", str(i+1), "on syslog, can't be found in
devices file"
         continue
      brand = devDb[devName]
      if brandAll or brandSel == brand:
         if devAll or deviceSel == devName:
            print l.strip()
# Make sure we get all params - USAGE
if len(sys.argv) != 5:
   print "Usage: ./gus.py SYSLOG.LOG DEVICES.DB DEVICE_SELECTION";
   sys.exit(3)
```

```
syslogFileName  = sys.argv[1]
devicesFileName = sys.argv[2]
brandSel        = sys.argv[3]
deviceSel       = sys.argv[4]

devDb = loadDevicesDb(devicesFileName);
processSysLog(devDb, syslogFileName, brandSel, deviceSel)
```

El script realiza la función de leer un archivo plano con todos los mensajes del syslog (syslog.log) y también lee de un listados los equipos (nombre de host ejemplo ERAMADDE1, ERTBUEBA2, etc.) para luego crear 1 archivo por fabricante, y también puede crear un archivo por equipo y por marca (esto lo realiza mediante la redirección a un archivo), a continuación se muestra como se ejecuta el script.

- Creando un archivo especifico por equipo, donde:

gus.py: es el script a ejecutar

syslog.log: es el archivo de texto plano que debe leer

devices.db: es el archivo con el nombre de los equipos y el fabricante correspondiente (en este caso el script se encargará de recoger todos los logs correspondiente al equipo Cisco con nombre eramadad1).

>>: Se redirige el estándar out (salida por pantalla) al archivo eramadad1.log

./gus.py sys.log devices.db Cisco eramadad1 >> eramadad1.log

- Creando un archivo por marca de equipo, donde:

gus.py: es el script a ejecutar

syslog.log: es el archivo de texto plano que debe leer

devices.db: es el archivo con el nombre de los equipos y el fabricante correspondiente (en este caso el script se encargará de recoger todos los logs correspondiente solamente a los equipos definidos en devices.db como Cisco).

>>: Se redirige el estándar out (salida por pantalla) al archivo Cisco_log.log

./gus.py syslog.log devices.db Cisco all >> Cisco_log.log

./gus.py syslog.log devices.db Juniper all >> Juniper_log.log **(Aquí hace lo mismo para los Juniper)**

- Creando un archivo con todos los equipos en el listado device.db (cabe aclarar que en dicho syslog.log pueden existir mensajes de EDC (equipos de cliente).

gus.py: es el script a ejecutar

syslog.log: es el archivo de texto plano que debe leer

devices.db: es el archivo con el nombre de los equipos y el fabricante correspondiente (en este caso el script se encargará de recoger todos los logs correspondiente a los equipos de Red, y descartará todos los logs de los EDC).

>>: Se redirige el estándar out (salida por pantalla) al archivo eramadad1.log

./gus.py syslog.log devices.db all all >> Cisco_Juniper.log

Ejemplo del archivo devices.db

```
ertmiana2 Juniper
erastoix1 Juniper
erafraix2 Juniper
eraguatc3 Juniper
ertparix3 Juniper
eramadpe2 Juniper
eralontc1 Juniper
erabueba2 Cisco
eramadad1 Cisco
eramadde1 Cisco
eramiatc2 Cisco
eramiana1 Cisco
eraparix3 Cisco
eraccsmv1 Cisco
eradaleq1 Cisco
```

Ejemplo del archivo Cisco_log.log

Oct 13 00:01:10 **eramadde1** 486809: Oct 13 00:01:08: %BGP-4-MAXPFX: Number of prefixes received from 172.31.239.190 vpn vrf vpn_3352_1291 (afi 4) reaches 428, max 500
Oct 13 00:01:17 **eramadad1** 774336: RP/0/RP0/CPU0:Oct 13 00:01:16 : SSHD_[65746]: disconnect_session: sshd.state:10
Oct 13 00:03:06 **eraparix3** 14224: Oct 13 00:03:05: %CONTROLLER-5-UPDOWN: Controller E1 3/3/7, changed state to down
Oct 13 00:03:16 **eraparix3** 14225: Oct 13 00:03:15: %CONTROLLER-5-UPDOWN: Controller E1 3/3/7, changed state to up
Oct 13 00:03:22 **eraparix3** 14226: Oct 13 00:03:21: %CONTROLLER-5-UPDOWN: Controller E1 3/3/7, changed state to down
Oct 13 00:03:32 **eraparix3** 14227: Oct 13 00:03:31: %CONTROLLER-5-UPDOWN: Controller E1 3/3/7, changed state to up
Oct 13 00:06:00 **eradaleq1** 1195852: Oct 13 00:05:59: %IPRT-3-ROUTELIMITEXCEEDED: IP routing table limit exceeded - vpn_6147_10
Oct 13 00:06:02 eramadad1 774337: RP/0/RP0/CPU0:Oct 13 00:06:02 : SSHD_[65746]: disconnect_session: sshd.state:10
Oct 13 00:06:02 eramiatc2 92309: Oct 13 00:06:01: %IPRT-3-ROUTELIMITEXCEEDED: IP routing table limit exceeded - vpn_6147_10
Oct 13 00:07:19 eraparix3 14228: Oct 13 00:07:18: %CONTROLLER-5-UPDOWN: Controller E1 3/3/7, changed state to down
Oct 13 00:07:29 eraparix3 14229: Oct 13 00:07:28: %CONTROLLER-5-UPDOWN: Controller E1 3/3/7, changed state to up
Oct 13 00:11:07 eramadde1 486810: Oct 13 00:11:06: %IPRT-3-ROUTELIMITWARNING: IP routing table limit warning - vpn_3352_131800
Oct 13 00:11:09 eramadde1 486811: Oct 13 00:11:08: %IPRT-3-ROUTELIMITWARNING: IP routing table limit warning - vpn_3352_131800
Oct 13 00:11:17 eramadad1 774338: RP/0/RP0/CPU0:Oct 13 00:11:17 : SSHD_[65746]: disconnect_session: sshd.state:10
Oct 13 00:12:39 eramadde1 486812: Oct 13 00:12:38: %BGP-4-MAXPFX: Number of prefixes received from 172.31.239.190 vpn vrf vpn_3352_1291 (afi 4) reaches 396, max 500
Oct 13 00:12:39 eramadde1 486813: Oct 13 00:12:38: %IPRT-3-ROUTELIMITWARNING: IP routing table limit warning - vpn_3352_1291
Oct 13 00:15:02 eraccsmv1 1287: Oct 13 00:15:01: %FR-5-DLCICHANGE: Interface Serial8/2/0 - DLCI 53 state changed to INACTIVE
Oct 13 00:15:12 eraccsmv1 1288: Oct 13 00:15:01: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial8/2/0.53, changed state to down
Oct 13 00:15:12 eraccsmv1 1289: Oct 13 00:15:02: %BGP-5-ADJCHANGE: neighbor 172.31.144.134 vpn vrf vpn_108429_37892 Down Interface flap
Oct 13 00:15:12 eraccsmv1 1290: Oct 13 00:15:02: %BGP_SESSION-5-ADJCHANGE: neighbor 172.31.144.134 IPv4 Unicast vpn vrf vpn_108429_37892 topology base removed from session Interface flap
Oct 13 00:16:09 eramadad1 774339: RP/0/RP0/CPU0:Oct 13 00:16:02 : SSHD_[65746]: disconnect_session: sshd.state:10
Oct 13 00:16:42 eraccsmv1 1291: Oct 13 00:16:41: %FR-5-DLCICHANGE: Interface Serial8/2/0 - DLCI 53 state changed to ACTIVE
Oct 13 00:16:43 eraccsmv1 1292: Oct 13 00:16:41: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial8/2/0.53, changed state to up
Oct 13 00:17:00 eraccsmv1 1293: Oct 13 00:16:59: %BGP-5-ADJCHANGE: neighbor 172.31.144.134 vpn vrf vpn_10429_3792 Up

```
Oct 13 00:18:07 eraparix3 14230: Oct 13 00:18:06: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to down
Oct 13 00:18:24 eraparix3 14231: Oct 13 00:18:23: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to up
Oct 13 00:18:28 eraparix3 14232: Oct 13 00:18:27: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to down
Oct 13 00:18:40 eraparix3 14233: Oct 13 00:18:39: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to up.
Oct 13 00:24:26 eraparix3 14243: Oct 13 00:24:25: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to up
Oct 13 00:24:34 eraparix3 14244: Oct 13 00:24:33: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to down
Oct 13 00:24:44 eraparix3 14245: Oct 13 00:24:43: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to up
Oct 13 00:25:41 eraparix3 14246: Oct 13 00:25:40: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to down
Oct 13 00:25:51 eraparix3 14247: Oct 13 00:25:50: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to up
Oct 13 00:25:54 eraparix3 14248: Oct 13 00:25:53: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to down
Warning: Device ERAMADMOS1  in line 100X on syslog, can't be found in devices file
Oct 13 00:26:08 eramadad1 774341: RP/0/RP0/CPU0:Oct 13 00:26:02 : SSHD_[65746]:
disconnect_session: sshd.state:10
Oct 13 00:26:14 eraparix3 14249: Oct 13 00:26:13: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to up
Oct 13 00:26:23 eraparix3 14250: Oct 13 00:26:22: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to down
Oct 13 00:26:43 eraparix3 14251: Oct 13 00:26:42: %CONTROLLER-5-UPDOWN: Controller E1
3/3/7, changed state to up
```

En el contenido se puede observar los equipos ERAXXXX que coinciden con los equipos que figuran en el archivo devices.db y los que no figuran salen con el mensaje de error **"Warning: Device devName in line XX on syslog, can't be found in devices file"**

Donde **devName** será el nombre del equipo que aparece en el archivo syslog.log pero que no aparece en el listado de devices.db

Line XX es el número de línea en el que aparece en el syslog.

Ejemplo del contenido del archive Juniper.log.

Oct 13 00:51:10 L0-eraguatc3 /kernel: e1-2/1/7 down:
send=0x0072bff1/reflected=0x50a5ee6d sequence numbers differ by 3 or more
Oct 13 00:51:19 L0-eramadpe2 rpd[90235]: 172.120.16.234 (External AS 13352): Configured maximum prefix-limit threshold(1485) exceeded for inet-unicast nlri: 1492
Oct 13 00:51:19 L0-eramadpe2 rpd[90235]: 172.131.150.90 (External AS 13352): Configured maximum prefix-limit threshold(2700) exceeded for inet-unicast nlri: 2986
Oct 13 00:51:20 L0-eraguatc3 /kernel: e1-2/1/7 down: send=0x50a4165f/reflected=0x0072bff1 sequence numbers differ by 3 or more
Oct 13 00:51:20 L0-eramadpe2 rpd[90235]: RPD_RT_PREFIX_LIMIT_REACHED: Number of prefixes (1500) in table vpn_3352_131800.inet.0 still exceeds or equals configured maximum (1500)
Oct 13 00:51:20 L0-eraguatc3 mib2d[1938]: SNMP_TRAP_LINK_DOWN: ifIndex 633, ifAdminStatus up(1), ifOperStatus down(2), ifName ce1-2/1/0
Oct 13 00:51:15 L0-erastoix1 Slot: 4, PIC Slot 0) last message repeated 94 times
Oct 13 00:51:30 L0-erafraix2 rpd[1578]: 134.252.250.98 (External AS 1286): Configured maximum prefix-limit threshold(450) exceeded for inet-unicast nlri: 469
Oct 13 00:51:30 L0-eraguatc3 /kernel: e1-2/1/7 down:
send=0x0072b76f/reflected=0x50a4165f sequence numbers differ by 3 or more
Oct 13 00:51:28 L0-eramadpe2 Slot: 6, PIC Slot 0) last message repeated 46 times
Oct 13 00:51:37 L0-eraguatc3 mib2d[1938]: SNMP_TRAP_LINK_DOWN: ifIndex 635, ifAdminStatus up(1), ifOperStatus down(2), ifName ce1-2/1/2
Oct 13 00:51:40 L0-eraguatc3 /kernel: e1-2/1/7 down:
send=0x50a40e5d/reflected=0x0072b76f sequence numbers differ by 3 or more
Oct 13 00:51:41 L0-ertmiana2 mgd[11722]: UI_TACPLUS_ERROR: TACACS+ failure: Network read timed out
Oct 13 00:51:49 L0-ertparix3 root: invoke-commands: Executed /tmp/evt_cmd_CaWRkG, output to /tmp/evt_op_muOkHT in text format
Oct 13 00:51:43 L0-ertmiana2 root: invoke-commands: Executed /tmp/evt_cmd_IuhlLG, output to /tmp/evt_op_WAZPtQ in text format
Oct 13 00:51:49 L0-eramadpe2 rpd[90235]: 172.20.16.234 (External AS 3352): Configured maximum prefix-limit threshold(1485) exceeded for inet-unicast nlri: 1492
Oct 13 00:51:49 L0-eramadpe2 rpd[90235]: 172.31.150.90 (External AS 3352): Configured maximum prefix-limit threshold(2700) exceeded for inet-unicast nlri: 2986
Oct 13 00:51:50 L0-eraguatc3 /kernel: e1-2/1/7 down:
send=0x0072bf49/reflected=0x50a40e5d sequence numbers differ by 3 or more
Oct 13 00:51:50 L0-eramadpe2 rpd[90235]: RPD_RT_PREFIX_LIMIT_REACHED: Number of prefixes (1500) in table vpn_3352_131800.inet.0 still exceeds or equals configured maximum (1500)
Oct 13 00:51:53 L0-eraguatc3 mib2d[1938]: SNMP_TRAP_LINK_DOWN: ifIndex 633, ifAdminStatus up(1), ifOperStatus down(2), ifName ce1-2/1/0
Oct 13 00:51:56 L0-eraguatc3 mib2d[1938]: SNMP_TRAP_LINK_DOWN: ifIndex 635, ifAdminStatus up(1), ifOperStatus down(2), ifName ce1-2/1/2
Oct 13 00:52:08 L0-eramadpe2 rpd[90235]: RPD_RT_PREFIX_LIMIT_WARNING: Number of prefixes (16785) in table vpn_33352_186900.inet.0 reached warning threshold (90 percent of configured maximum 18000)
Oct 13 00:52:08 L0-ertparix3 rpd[32773]: 2001:1498:1:300::2e (External AS 3257): Configured maximum prefix-limit threshold(2800) exceeded for inet6-unicast nlri: 2841

Oct 13 00:52:10 L0-eraguatc3 /kernel: e1-2/1/7 down:
send=0x0072b778/reflected=0x50a4369f sequence numbers differ by 3 or more
Oct 13 00:52:10 L0-eraguatc3 mib2d[1938]: SNMP_TRAP_LINK_DOWN: ifIndex 635,
ifAdminStatus up(1), ifOperStatus down(2), ifName ce1-2/1/2
Oct 13 00:52:19 L0-eramadpe2 rpd[90235]: 172.21.110.90 (External AS 13352): Configured
maximum prefix-limit threshold(2700) exceeded for inet-unicast nlri: 2986
Oct 13 00:52:20 L0-eraguatc3 /kernel: e1-2/1/7 down:
send=0x50a42e83/reflected=0x0072b778 sequence numbers differ by 3 or more
Oct 13 00:52:20 L0-eramadpe2 rpd[90235]: RPD_RT_PREFIX_LIMIT_REACHED: Number of
prefixes (1500) in table vpn_33152_1318100.inet.0 still exceeds or equals configured
maximum (1500)
Oct 13 00:52:22 L0-erafraix2 rpd[1578]: RPD_RT_PREFIX_LIMIT_WARNING: Number of prefixes
(16809) in table vpn_33152_181600.inet.0 reached warning threshold (90 percent of
configured maximum 18000)
Oct 13 00:52:22 L0-erastoix1 rpd[2075]: RPD_RT_PREFIX_LIMIT_WARNING: Number of
prefixes (16789) in table vpn_3352_18600.inet.0 reached warning threshold (90 percent of
configured maximum 18000)
Oct 13 00:52:28 L0-erastoix1 rpd[2075]: bgp_read_message: peer 172.120.10.10 (External AS
13292): Notification arrived, expected Open
Oct 13 00:52:29 L0-eraguatc3 mib2d[1938]: SNMP_TRAP_LINK_DOWN: ifIndex 635,
ifAdminStatus up(1), ifOperStatus down(2), ifName ce1-2/1/2
Oct 13 00:52:37 L0-eralontc1 kmd[45029]: KMD_PM_PHASE2_POLICY_LOOKUP_FAIL: Unable
to retrieve policy for Phase 2 from responder (Phase 1 local peer
ipv4(udp:500,[0..3]=211.130.32.43), remote peer ipv4(udp:500,[0..3]=116.71.111.66); Phase 2
local peer ipv4_subnet(any:0,[0..7]=0.0.0.0/0), remote peer
ipv4_subnet(any:0,[0..7]=0.0.0.0/0))
ipv4(udp:500,[0..3]=116.91.121.58); Phase 2 local peer ipv4_subnet(any:0,[0..7]=0.0.0.0/0),
remote peer ipv4_subnet(any:0,[0..7]=0.0.0.0/0))
Oct 13 00:52:45 L0-eralontc1 kmd[45029]: KMD_PM_PHASE2_POLICY_LOOKUP_FAIL: Unable
to retrieve policy for Phase 2 from responder (Phase 1 local peer
ipv4(udp:500,[0..3]=212.110.22.43), remote peer ipv4(udp:500,[0..3]=195.48.11.194); Phase 2
local peer ipv4_subnet(any:0,[0..7]=0.0.0.0/0), remote peer
ipv4_subnet(any:0,[0..7]=0.0.0.0/0))
Oct 13 00:53:40 L0-eralontc1 cscript: Thermomib: clearing idp:cpu:sp-
0/0/0:ipsec_3352_467000_000051100 type integer timestamp 07 dc 0c 17 00 2f 3b 00 2b 00
00
Oct 13 00:53:40 L0-eraguatc3 /kernel: e1-2/1/7 down:
send=0x50a4987e/reflected=0x007ae639 sequence numbers differ by 3 or more
Oct 13 00:55:42 L0-eraguatc3 mib2d[1938]: SNMP_TRAP_LINK_DOWN: ifIndex 635,
ifAdminStatus up(1), ifOperStatus down(2), ifName ce1-2/1/2
Oct 13 00:55:44 L0-eraguatc3 mib2d[1938]: SNMP_TRAP_LINK_DOWN: ifIndex 633,
ifAdminStatus up(1), ifOperStatus down(2).

9. Glosario (Acrónimos).

3G	*Tercera generación de transmisión de voz y datos*
802.1Q	*Especifica como implementar varias VLAN en un mismo puerto*
ACL	*Listas de control e acceso*
ATM	*Modo de Transferencia Asíncrona*
AToM	*Cualquier protocolo sobre MPLS*
BACKBONE	*Equipos troncales de la Red*
BC	*Caudal comprometido*
BE	*Caudal en exceso*
BEST-EFFORD	*Entrega con el menor esfuerzo*
BGP	*Protocolo de encaminamiento de Borde*
CAS	*Señalización por canal asociado*
CIR	*Ancho de banda determinado en un tiempo determinado*
COMMUNITY	*Atributo de BGP*
CORE	*Equipos troncales de la Red*
CPD	*Centro de Procesamiento de Datos*
DE	*Elegible de ser Descartado*
DELAY	*Retardo*
DWDM	*Multiplicación por división de frecuencia*
E1	*Trama E1 de 2048Kbps*
E3	*Trama E3 de 34Mbps*
EDC	*Equipo de Cliente*
ERA	*Equipo de Red Acceso*
ERG	*Equipo de Red de Gestión*
ERT	*Equipo de Red Troncal*
FEC	*Clase equivalente de envió de trafico*
FPC	*Concentrador Flexible de PIC*
FRAME	*Trama*
FRAME-RELAY	*Protocolo de transmisión de tramas para redes de circuitos virtuales*
GATEWAY	*Puerta de enlace*
HEADER	*Cabecera*
HOUSING	*Lugar físico donde se alojan equipos*
HSSI	*Interface Serial de Alta Velocidad*
IETF	*Internet Engineering Task Force*
IGP	*Protocolo de encaminamiento Interior*
IPSEC	*Protocolo Seguro para Internet*
ISIS	*Protocolo de Encaminamiento*
ISP	*Proveedor de Servicios de Internet*
JITTER	*variabilidad del tiempo de ejecución de los paquetes*
LACP	*Protocolo de Agregación y Control de Enlaces*
LAN	*Red de Área Local*
LABEL	*Etiqueta*

LDP	*Protocolo para Distribución e intercambio de Etiquetas*
LER	*Elemento que inicia o termina el túnel*
LINK STATE	*Estado del enlace*
LOCAL-PREF	*Atributo de BGP*
LOOPBACK	*Interface Virtual siempre accesible*
LSP	*Camino por conmutación de etiquetas*
LSR	*Elemento que conmuta etiquetas*
MED	*Atributo de BGP*
MPLS	*Conmutación por intercambio de etiquetas*
MPLS-TE	*Ingeniería de Tráfico para MPLS*
MPOA	*Multi protocolo sobre ATM*
MPPP	*Varios enlaces PPP*
NEXT-HOP	*Próximo Salto*
OSI	*Modelo de interconexión de sistemas abiertos*
P	*Equipo de Red Troncal*
PCM	*Condigo de Modulación por Pulso*
PE	*Equipo del Proveedor*
PIC	*Physical Interface Card*
POS	*Packet Over Sonet*
PPP	*Protocolo punto a punto*
PVC	*Conexión Permanente Virtual*
QOS	*Calidad de Servicio*
RDSI	*Red Digital de Servicios Integrados*
RS232	*Estándar para el intercambio de una serie de datos binarios*
SERVICE-POLICY	*Servicio de politica de QOS*
SFP	*Small Factor Port*
SIP	*SPA Interface Processor*
SNMP	*Protocolo de Gestión de Red*
SPA	*Shared Port Adapter*
SPF	*Shortest Path First (Primero el Camino más corto)*
STI	*Servicio de Transito Internet*
STP	*Protocolo para evitar bucles*
STREAMING	*Distribución*
SVC	*Circuito Virtual Conmutado*
T1	*Trama T1 1.544Mbps*
T3	*Trama T3 44.736Mbps*
TAG	*Etiqueta*
TBit	*Terabit 1000Gbps/s*
TTL	*Time-To-Live o tiempo de vida*
VCI	*Identificador del Canal Virtual*
VOIP	*Voz sobre IP*
VPI	*Identificador del camino Virtual*
VPN	*Red Virtual Privada*
VRF	*Tabla Virtual de Encaminamiento*