UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

TRABAJO DE SUFICIENCIA PROFESIONAL

INTEGRACION DE DOS REDES MPLS PARA OPTIMIZAR LA GESTIÓN FUERA DE BANDA EN UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES.

PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

ELABORADO POR:

CESAR VICENTE SALAS RIMAC

ASESOR

ING. ALFREDO EFRAIN RODRIGUEZ GUTIERREZ

LIMA – PERÚ

2021

INTEGRACION DE DOS REDES MPLS PARA OPTIMIZAR LA GESTIÓN FUERA DE BANDA EN UN PROVEEDOR DE SERVICIOS DE TELECOMUNICACIONES.

DEDICATORIA

A Dios por haberme dado la vida y permitir desarrollarme profesionalmente, a mi madre y abuelo por su guía y apoyo constante en las etapas iniciales de mi vida.

RESUMEN

En el presente informe se explica la Integración de dos redes MPLS, cómo el método para optimizar la gestión fuera de banda en un proveedor de servicios de Telecomunicaciones.

La metodología aplicada es el análisis de un caso de estudio que involucra a un proveedor de servicios que cuenta con dos redes MPLS de gestión fuera de banda independientes pero que necesita aprovechar de mejor manera los recursos físicos y lógicos con los que cuenta. Para lograr esto, en el presente informe se explica cómo funcionan ambas redes MPLS de gestión fuera de banda por separado, utilizando luego esta información como base para definir las características de la Integración de redes MPLS. De manera extensiva, se presenta también cómo la implementación de esta solución optimiza los costos de inversión y operación.

El desarrollo de este Informe de Suficiencia Profesional beneficiará la adquisición de conocimientos y experiencias para futuros ingenieros de la carrera de Ingeniería de Telecomunicaciones y afines, ya que muestra los procedimientos y criterios utilizados en la industria cuando se ejecuta una integración de redes MPLS además de los resultados obtenidos en indicadores clave que muestran cómo la solución logra resolver el problema inicial del proveedor de servicios.

ABSTRACT

This report explains the Integration of two MPLS networks, as the method to optimize out-of-band management in a Telecommunications service provider.

The methodology applied is the analysis of a case study that involves a service provider that has two independent MPLS out-of-band management networks, but that needs to improve the use of the physical and logical resources it has. To achieve this, it is explained how both MPLS out-of-band management networks work separately: That information, is used then as a basis to define the characteristics of MPLS network integration. In an extensive way, it is also presented how the implementation of this solution optimizes investment and operating costs.

The development of this Professional Sufficiency Report will benefit the acquisition of knowledge and experiences for future engineers of the Telecommunications Engineering career and related, since it shows the procedures and criteria used in the industry when an integration of MPLS networks is executed, in addition, the key indicators results obtained show how the solution manages to solve the initial problem of the service provider.

ÍNDICE

PRÓLOGO

En el presente informe se presenta la Integración de dos redes MPLS de Gestión Fuera de Banda en un proveedor de servicios de Telecomunicaciones como la solución a un problema de ingeniería aplicada en el campo de las redes de datos.

La elaboración de este informe es el producto de la experiencia laboral práctica del autor en el campo de la Ingeniería de Telecomunicaciones y la recopilación de material bibliográfico, revistas técnicas, manuales utilizados para el diseño de redes de datos para proveedores de servicios y ha sido escrito como parte de los requisitos para obtener el Título Profesional de Ingeniero de Telecomunicaciones de la Facultad de Ingeniería Eléctrica y Electrónica de la Universidad Nacional de Ingeniería.

El presente informe está dividido en cinco capítulos:

En el Capítulo 1, se identifica el problema de ingeniería y se precisan cuáles son los objetivos generales y específicos de la solución.

En el Capítulo 2, se describen los conceptos y definiciones de la tecnología a utilizar para el despliegue de la red MPLS con servicios L3VPN con propósitos de Gestión Fuera de Banda incluyendo también los elementos que conforman el sistema de gestión de red de datos, la tecnología utilizada en el núcleo y acceso de la red MPLS, los planos de operación de la infraestructura y los mecanismos de calidad de servicio.

En el Capítulo 3, se realiza la ingeniería necesaria para definir la solución al problema inicial. Esto es dividido en tres secciones: Situación Inicial, para describir la manera en que funcionaban inicialmente las redes de gestión fuera de banda que utilizaba el proveedor de servicios. En la segunda sección, Red MPLS a Implementar, se detalla el funcionamiento de la solución propuesta en el núcleo y acceso de la red MPLS, la red LAN y la implementación de mecanismos de calidad de servicio. En la tercera sección se presenta un programa de implementación para ejecutar la Integración de las Redes MPLS.

En el Capítulo 4, se realiza un análisis de los resultados obtenidos para demostrar que la solución propuesta logra resolver el problema de Ingeniería y el impacto sobre los costos de inversión y operación con los que se puede reservar el presupuesto destinado para implementar la solución.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

1.1 Descripción del problema

A nivel mundial, la utilización de redes de gestión fuera de banda es una característica esencial en empresas que, por su giro de negocio, exigen que sus centros de datos cuenten con una alta disponibilidad tales como la industria financiera, proveedores de servicios o similares. El impacto económico de la caída de una red se encuentra estimado globalmente en un valor promedio $300 mil dólares por hora. En el caso de ciberataques, el costo para las organizaciones, víctimas de este tipo de ataques, en el año 2018 se estima en $45 billones de dólares, mientras que el mercado global, de herramientas de monitoreo que ayudan tener visibilidad de estos eventos está pronosticado en $11 billones de dólares para el año 2024. [1].

En la región, el uso de redes de gestión fuera de banda está orientado principalmente al sector de proveedores de servicios por la gran cantidad de equipamiento que suelen desplegar geográficamente y los niveles de disponibilidad y calidad de servicio o SLA's (*Service Level Agreement*) de los contratos que celebran con sus clientes. Esta característica es común a clientes del sector privado como del sector estatal, y su incumplimiento trae como consecuencia penalidades que se traducen en pérdidas económicas, además de dañar la imagen de la compañía.

En el Perú es importante anotar también que la calidad de los servicios públicos de telecomunicaciones está supervisada por OSIPTEL, que como ente regulador del estado aplica sanciones que se reflejan en multas e incluso hasta la inhabilitación para seguir comercializando los servicios. Según los informes de OSIPTEL, el primer semestre del año 2018, los montos de devolución a clientes en los 4 principales operadores llegaron a sumar casi S/. 1,46 millones de soles para los servicios de Telefonía Móvil, Internet Fijo y Tv Paga [2], mientras que si consideramos sólo las multas a la empresa operadora Telefónica del Perú por incumplir compromisos de mejora de calidad entre los años 2016 y 2017 estas llegaron a sumar más de S/. 35 millones de soles [3].

Ante el escenario antes descrito, los proveedores de servicio se ven obligados a implementar estrategias para mitigar el riesgo de fallas en el servicio, tales como la redundancia física y/o geográfica de enlaces, utilizar equipos con *hardware* redundante,

planes de recuperación de servicios en el menor tiempo posible y el uso de redes de gestión fuera de banda.

En el proveedor de servicios elegido para este informe, las redes de gestión fuera de banda instaladas son dos redes MPLS independientes que son utilizadas por el personal de operación y mantenimiento de distintas áreas para ejecutar tareas de monitorización, administración y recuperación de los servicios de red en alguna de las redes de servicios, sin embargo su utilización requiere optimizarse pues cada red MPLS de gestión fuera de banda cuenta con topologías diferentes de nodos MPLS WAN y LAN que deben ser unificadas, así como también asegurar la alta disponibilidad, permitir el crecimiento en cantidad de dispositivos de cada una de las redes de servicios y considerar los ciclos de vida útil de los dispositivos de red para renovar los dispositivos en la última fase de su ciclo de vida. Las capacidades de hardware y software de los nuevos equipos deben ser aprovechados evitando la subutilización de recursos, e incluyendo la capacidad de diferenciar entre tipos de tráfico.

El uso de una gestión fuera de banda no representa un servicio de valor agregado facturable al cliente final. Por tanto, los directivos del proveedor de servicios consideran que mantener dos redes MPLS de gestión fuera de banda en producción, es un gasto que debe optimizar, para evitar asignar partidas anuales diferentes en su presupuesto anual para los gastos de Inversión (CapEx) y de Operación (OpEx) que cubran los requerimientos de renovación tecnológica y ampliación de capacidades por cada red de gestión fuera de banda.

1.2 Formulación del Problema

Consiste en:

1.2.1. Problema General

¿De qué manera la Integración de dos redes MPLS permite optimizar la gestión fuera de banda de dispositivos de red en un proveedor de servicios de telecomunicaciones?

1.2.2. Problemas Específicos

Los problemas específicos son:

1. ¿Cómo la Integración de las dos redes MPLS de gestión fuera de banda aprovecha las capacidades de hardware y software de los equipos a renovar para evitar la subutilización de estos recursos en el proveedor de servicios?
2. ¿Cómo la Integración de las dos redes MPLS de gestión fuera de banda mejora la disponibilidad a nivel WAN y LAN de esta red en el proveedor de servicios?
3. ¿Cómo la Integración de las dos redes MPLS de gestión fuera de banda optimiza la topología, la cantidad de enlaces y equipos requeridos además de la cobertura de las redes de gestión fuera de banda?

4. ¿De qué manera la Integración de las dos redes MPLS de gestión fuera de banda puede optimizar los gastos realizados en costos de Inversión (CapEx) y de mantenimiento y operación (OpEx) que realiza el proveedor de servicios al mantener en producción ambas redes?

1.3 Objetivos

1.3.1. Objetivo General

Integrar dos redes MPLS para optimizar la gestión fuera de banda de dispositivos de red en un proveedor de servicios de telecomunicaciones

1.3.2. Objetivos Específicos:

1. Implementar la integración de las dos redes MPLS para aprovechar las capacidades de hardware y software de los equipos de gestión fuera de banda en el proveedor de servicios.
2. Implementar protocolos de red en la integración de las dos redes MPLS de gestión fuera de banda que mejoren la disponibilidad a nivel WAN y LAN de la nueva red MPLS de gestión fuera de banda en el proveedor de servicios.
3. Definir una topología de red única en la integración de las dos redes MPLS de gestión fuera de banda que optimice la cantidad de enlaces y equipos requeridos además de la cobertura de las redes de gestión fuera de banda.
4. Demostrar que la integración de las dos redes MPLS de gestión fuera de banda puede optimizar los gastos realizados en costos de Inversión (CapEx) y operación (OpEx) que realiza el proveedor de servicios al mantener en producción las dos redes de gestión fuera de banda.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

2.1. Planos de operación de un Dispositivo de Red

Para entender la gestión de los dispositivos de red requiere de abstraer sus funciones en tres planos de operación:

2.1.1. Plano de Control (Control Plane)

El plano de control permite procesar el tráfico que es utilizado para el funcionamiento de los conmutadores y enrutadores de la infraestructura de red. Este plano consta de las aplicaciones y los protocolos entre dispositivos de red, tales como STP, BGP, EIGRP, OSPF, IS-IS, etc.

2.1.2. Plano de Datos (Data Plane)

El plano de datos permite reenviar los paquetes a través de un dispositivo de red. No incluye el tráfico enviado al enrutador o conmutador local.

2.1.3. Plano de Administración (Management Plane)

El plano de gestión procesa el tráfico enviado al enrutador o al conmutador, y está formado por aplicaciones y protocolos para las funciones de administración, tales como telnet, Secure Shell (SSH), Simple Network Management Protocol (SNMP), Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) y HTTP Secure (HTTPS).

En la figura 2.1 se muestran los planos de operación y los protocolos que son considerados dentro de cada plano de control.

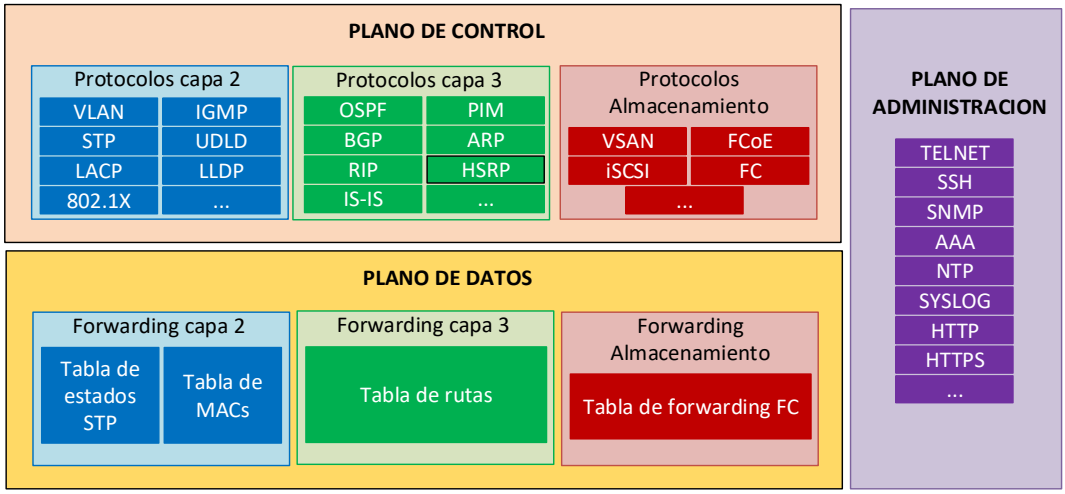


Figura 2.1 Planos de operación. (Fuente: Elaboración propia)

2.2. Sistemas de Gestión de redes de datos

2.2.1. Definición

Un sistema de gestión de red de datos está definido como el conjunto de elementos, que puede incluir a dispositivos físicos, programas de software, protocolos y las actividades que son utilizadas por los administradores de red para realizar las labores de control, planificación, coordinación, asignación y monitoreo de los recursos de la red, ayudando a los mismos a mantener la red de datos en un óptimo estado de funcionamiento durante el tiempo máximo posible, minimizando los tiempos de falla y por ende el impacto sobre las capacidades brindadas por la red de datos.

2.2.2. Red de Gestión

En este contexto, las redes de gestión son un elemento esencial para asegurar la disponibilidad tanto física como lógica de la red de datos, por lo tanto, su complejidad y capacidades requeridas estarán determinadas por las necesidades del negocio al cual atiende la red de datos de servicio. En tal sentido, una red de gestión de una red pequeña requiere únicamente de capacidades de gestión en banda, mientras que una red grande y de alta criticidad por el tipo de negocio al que atiende (finanzas & banca, proveedor de servicios, etc.) requiere de una red de gestión dedicada que es conocida como fuera de banda.

2.2.3. Tipos de Sistema de Gestión de redes de datos

a) Gestión en banda

La gestión en banda consiste en el control y acceso de la infraestructura de TI mediante la propia red. Esta es la forma más común de administrar una red. Sin embargo, para redes grandes o críticas para el negocio, la administración de la red en banda muchas veces no es suficiente pues si una parte de la red fallase, no puede ser utilizada para llegar a los dispositivos afectados y resolver el problema. La solución es utilizar una ruta de acceso alternativa o secundaria para solucionar o para acceder a la fuente del problema, que es esencialmente lo que proporciona la Gestión fuera de banda.

b) Gestión fuera de banda

La gestión fuera de banda tiene como uso principal, el acceso y control de la infraestructura de TI mediante un acceso alternativo a la red de producción en caso este no se encuentre disponible debido a fallas en la red. El tipo de activos que requieren gestionarse en modo fuera de banda incluye normalmente a los enrutadores, conmutadores, KVM, servidores, almacenamiento y dispositivos de misión crítica que sirven como la columna vertebral de la infraestructura de TI.

En la figura 2.2 se muestra una topología de una red con gestión en banda y fuera de banda.

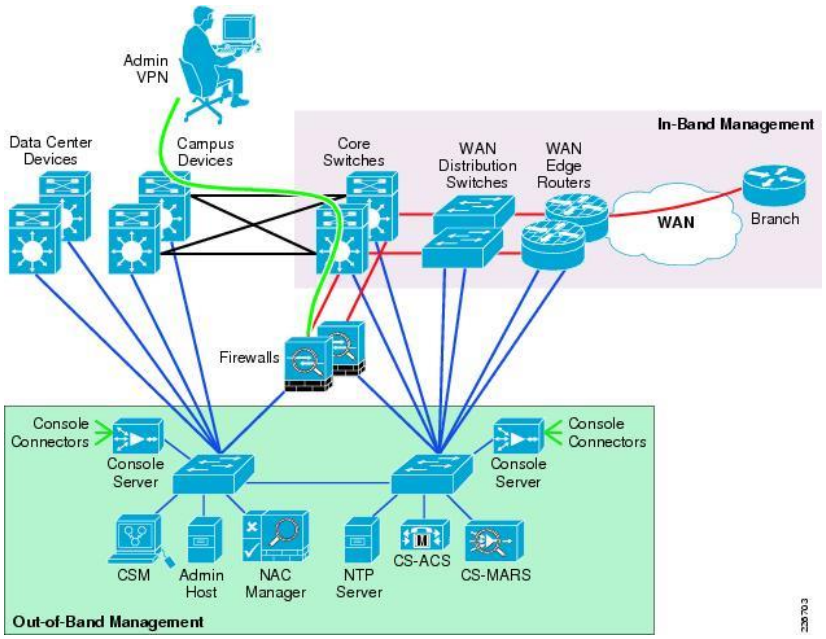


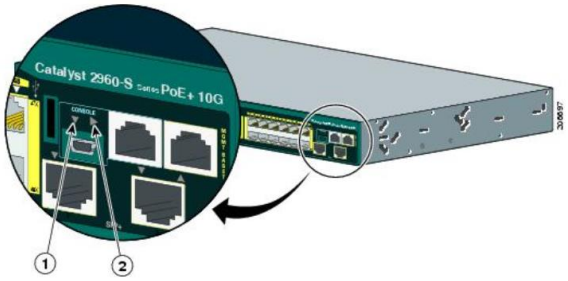
Figura 2.2 Gestión en banda y fuera de Banda. (Fuente: Ref. [4])

2.2.4. Métodos de Gestión

Los métodos de acceso local para la administración de un dispositivo incluyen métodos de acceso local y remoto.

a) Gestión Local

El acceso local para las tareas de administración de un dispositivo se realiza utilizando una conexión directa mediante un puerto especial denominado usualmente puerto de consola. Cada fabricante elije el tipo de puerto a utilizar, siendo los más comunes los puertos seriales que siguen la norma EIA/TIA-232 con terminales RJ-45 aunque es posible encontrar otros tales como los USB mini tipo B de 5 pines, DB9 y otros. En la figura 2.3 se muestra un equipo con puertos de consola serial RJ45 y USB.



1	USB console LED
2	RJ-45 console LED

Figura 2.3 Equipo con puertos consola serial RJ45 y USB. (Fuente: Ref. [5])

Para poder acceder desde una PC es necesario contar con una aplicación de emulación de terminal (Ej. Microsoft Windows Hyperterminal, Putty, Secure CRT) con los parámetros de configuración del puerto serial adecuados para comunicarse con el puerto de consola del dispositivo. Estos parámetros son la velocidad de conexión (en baudios), número de bits de datos (data bits) en cada carácter, cantidad de bits de parada, bit de detección de paridad y control de flujo. En la figura 2.4 se muestra una laptop conectada mediante un cable a un equipo con puertos de consola serial USB con propósitos de gestión.

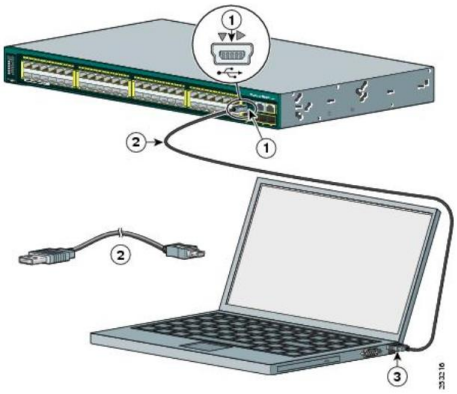


Figura 2.4 Conexión física a puerto serial (Fuente: Ref. [5]).

b) Acceso Remoto

El acceso remoto es realizado mediante la red haciendo posible que los operadores no se encuentren físicamente en el mismo lugar que los equipos que se pretenden administrar, sino que se concentren en un único centro de gestión conocido como NOC (Network Operation Center). En la figura 2.5 se muestra un operador conectado de manera remota a un dispositivo de red (enrutador).

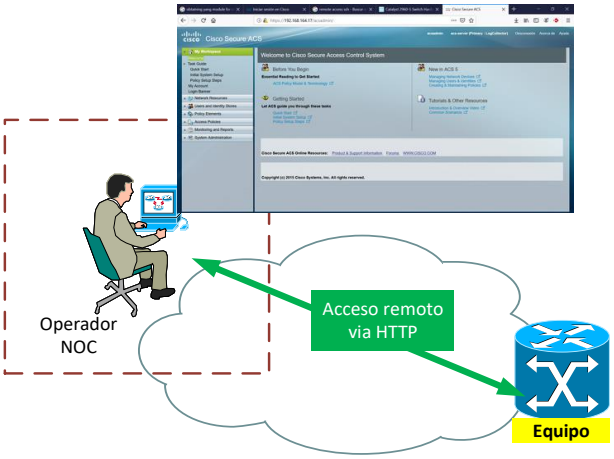


Figura 2.5 Conexión remota a un equipo vía HTTP (Fuente: Elab. propia).

Las aplicaciones utilizadas para este fin permiten la emulación de terminales de forma remota mediante protocolos como telnet y ssh que utilizan poco ancho de banda. Otras

opciones disponibles, consiste en la utilización de aplicaciones estándar o propietarias que usan protocolos (tales como snmp, http, https, rdp, etc.) que permiten recolectar información que luego es mostrada mediante la inclusión de tableros gráficos (*dashboard*) que muestran la información en formato más fácil de interpretar por los administradores de red. En la figura 2.6 se muestra un NMS que muestra información obtenida a través del protocolo SNMP.

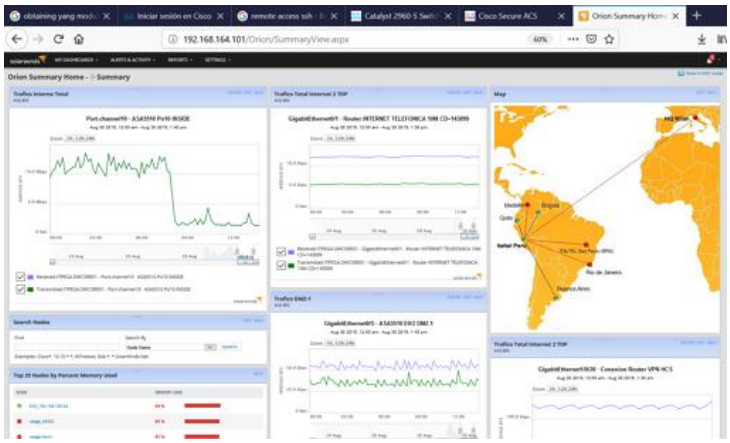


Figura 2.6. NMS con información obtenida vía SNMP. (Fuente: Elab. propia).

Adicionalmente también es posible utilizar servidores de acceso vía consola que combinan el acceso remoto hasta el servidor con el acceso local a los puertos de consola a través de telnet reverso utilizando cables asíncronos. En la figura 2.7 se muestra la forma en que un operador de NOC puede gestionar dispositivos de red utilizando un servidor de acceso.

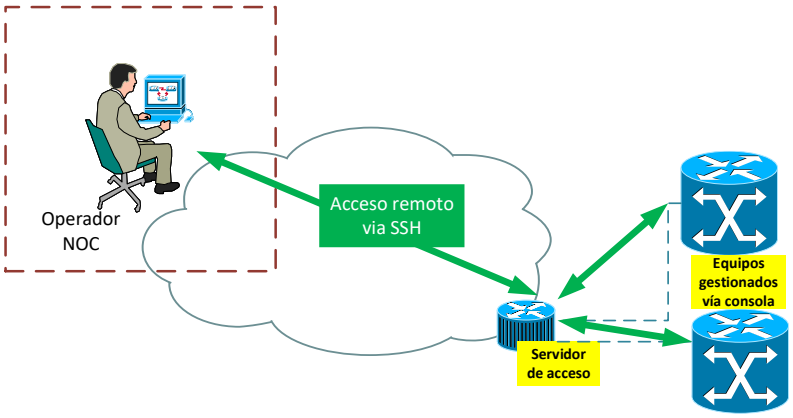


Figura 2.7. Acceso vía servidor de acceso vía consolas. (Fuente: Elab. propia).

2.2.5. Protocolos de Gestión

a) AAA

AAA (Authentication, Autorization and Accounting) es el marco de referencia que incluye a una familia de protocolos para llevar a cabo los procesos de autenticación, autorización y contabilidad, que son utilizado para garantizar el acceso seguro a los dispositivos de red.

- **Autenticación:** Se refiere al proceso de identificación único de cada usuario en el sistema, generalmente utilizando un nombre de usuario y contraseña.
- **Autorización:** Se refiere al proceso de aceptar o denegar el acceso de un usuario a un dispositivo de red y sus recursos. Cada usuario recibe un nivel de autorización diferente que limita su acceso a la red, los cambios que puede realizar y los recursos asociados en función de alguna condición que es elegida por los administradores del sistema (Por ejemplo, el rol del trabajador, el área donde trabaja, etc.).
- **Contabilidad:** La contabilidad se refiere uso de registros para brindar seguimiento a las actividades que los usuarios realizan en una red informática. Esto puede incluir: la fecha y hora en que el usuario ha accedido a la red, los equipos a los cuales accedió, datos de inicio de sesión permitiendo realizar un análisis de capacidad y tendencias de uso.

Los protocolos que se pueden utilizar para la implementación de AAA en una red son TACACS+, Radius, Kerberos o Diameter.

- **TACACs+**

TACACS+ (Terminal Access Controller Access-Control System Plus) es un protocolo de control de acceso desarrollado inicialmente por Cisco, pero liberado posteriormente como un protocolo abierto estándar en 1993 en la RFC 1492. TACACS+ maneja los procesos de AAA como servicios por separado. Utiliza el puerto 49 de TCP y encripta toda la carga útil TCP, que incluye tanto el nombre de usuario y contraseña.

- **Radius:**

RADIUS (Remote Authentication Dial-In User Service) realiza los procesos de AAA mediante dos paquetes: Access-Request (solicitud de acceso) que maneja los procesos de Autenticación y Autorización y Accounting-Request (solicitud de contabilidad) que maneja la contabilidad. Adicionalmente Radius puede utilizar TCP/UDP mediante el puerto 1812 pero a diferencia de TACACS sólo cifra la contraseña enviada a través de la red dejando el resto de la información en texto plano.

b) SNMP

SNMP (*Simple Network Management Protocol*) es un protocolo abierto que utiliza tablas con índices conocidos como MIB (*Management Information Base*) o Base de información de administración para administrar y conseguir información de los dispositivos de red. Existe una gran cantidad de MIBs estándar que pueden ser utilizados para este propósito además de las MIB privadas para la gestión de dispositivos específicos que son definidas por cada fabricante.

SNMP cuenta con distintas versiones:

SNMPv1: Es la versión inicial de este protocolo, considera contadores de 32-bits.

SNMPv2C: Considera mejoras en el método de operación y es compatible con SNMPv1.

SNMPv3: Añade características de seguridad tales como autenticación y encriptación.

Los softwares de administración de red, conocidos como NMS (*Network Management System*) o Sistema de Administración de Red, utilizan SNMP para consultar a los dispositivos que gestionan, a fin de poder recolectar los datos necesarios para construir los diagramas, tablas y gráficos que presentan en un solo tablero o *dashboard*. En la figura 2.8 se muestra un NMS obteniendo información de un dispositivo de red a través del protocolo SNMP.

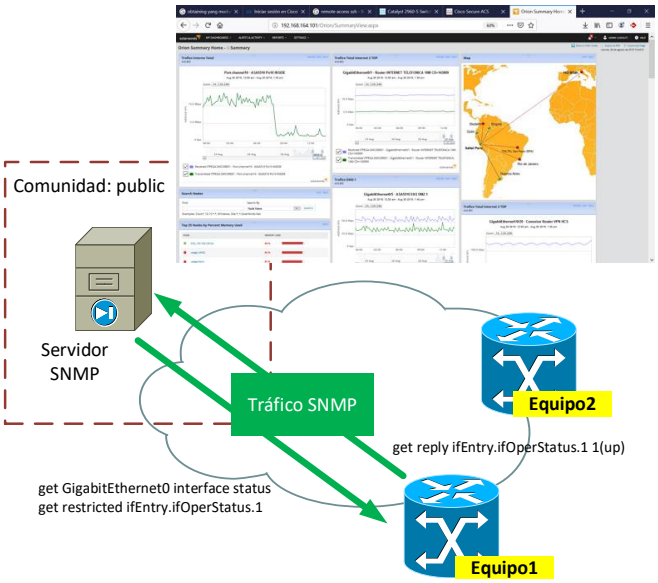


Figura 2.8. NMS obteniendo información vía SNMP. (Fuente: Elab. propia).

c) Protocolos de Acceso Remoto

Los protocolos de acceso remoto más utilizados son los siguientes:

- **Telnet**

Telnet (*Telecommunication Network*) es el protocolo que permite acceder remotamente a un dispositivo con el objetivo de realizar tareas de administración vía una terminal de consola virtual. Utiliza el puerto 23 de TCP.

- **SSH**

SSH (*Secure Shell*) es un protocolo que cumple con el mismo objetivo que Telnet, pero de manera segura, pues usa una conexión es encriptada. Adicionalmente, SSH permite realizar la copia de archivos de manera segura, gestionar claves RSA (evitando escribir las contraseñas durante la conexión). SSH utiliza el puerto 22 de TCP.

- **HTTP/HTTPS**

El acceso vía web es otra alternativa para realizar las tareas de configuración en un dispositivo evitando la complejidad de los comandos CLI. El acceso vía web es realizado a través de los protocolos HTTP o HTTPS (HTTP seguro).

d) Syslog

Syslog, definido en la RFC 5424, permite realizar el almacenamiento de los registros de eventos (logs) ocurridos en el equipo en un servidor de la red con propósitos de solución de problemas, investigaciones de seguridad o análisis posterior. Usa normalmente el puerto 514 de UDP y transfiere los registros en texto plano.

Facilidades y Severidades:

La RFC 5424 sugiere una lista de 23 facilidades (*facilities*) para identificar los tipos de logs. En la figura 2.9 se muestran las facilidades sugeridas en la RFC 5424.

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Figura 2.9. Lista de facilidades Syslog. (Fuente: Ref. [6])

La RFC5424 define también la siguiente lista de severidades (*severity*) para los eventos que se registran. Esta lista es de uso común entre los fabricantes. En la figura 2.10 se listan las severidades definidas por la RFC5424.

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Figura 2.10. Lista de Severidades Syslog. (Fuente: Ref. [6])

e) NTP

NTP (Protocolo de Tiempo de red) es el protocolo estándar que permite sincronizar los relojes de sistema de los dispositivos de red con una fuente centralizada permitiendo la

correlación de información de todos los dispositivos con propósitos de solución de problemas, investigaciones de seguridad o análisis del entorno tecnológico.

NTP utiliza una estructura jerarquizada basada en estratos o *Stratum*. El nivel más alto lo tienen los servidores del *Stratum* 1 (conectados directamente a relojes atómicos o GPS). Los servidores *Stratum* 2 obtienen su tiempo de un servidor *Stratum* 1. Los servidores del *Stratum* 3 lo obtienen de servidores *Stratum* 2 y así sucesivamente. En la figura 2.11 se muestra varios dispositivos de red sincronizando su reloj con un servidor NTP.

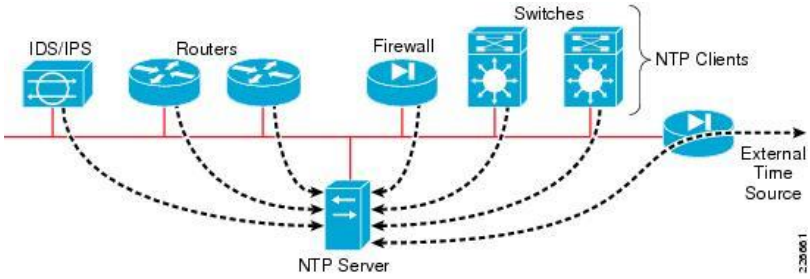


Figura 2.11. Conexiones NTP para dispositivos de red. (Fuente: Ref. [4])

2.3. Tecnologías de Transporte

Las tecnologías de transporte a utilizar consideran únicamente medios guiados o alámbricos, que son los que se describen a continuación:

2.3.1. Fibra Óptica:

Los cables de fibra óptica utilizan fibras de vidrio como medio de transmisión para el envío de datos digitales modulados en forma de ondas de luz. La principal ventaja de los cables de fibra óptica respecto a otros tipos de medio es la gran cantidad de ancho de banda y, por lo tanto, su mejor rendimiento a la hora de transportar datos. Además, los cables de fibra óptica son más ligeros e inmunes a interferencias electromagnéticas y *crosstalk*, aunque son más frágiles que los cables de metal.

a) Funcionamiento:

En una fibra óptica, las señales se transmiten sobre una única fibra de pocos micrómetros de diámetro, rodeada de un recubrimiento que puede ser otro cristal o plástico de diferentes propiedades ópticas.

En la figura 2.12 se muestra tres haces de luz que inciden inicialmente en el límite de las superficies aire/sílice con ángulos $\propto_1$, $\propto_2$ y $\propto_3$ y los haces refractados correspondientes según β_1, β_2 y β_3. La fibra óptica propaga el haz de luz dentro del cable de fibra óptica bajo el principio de reflexión total de la ley de Snell, según el cual, para valores del ángulo de incidencia del haz de luz mayores a un valor crítico, se obtiene que toda la luz es reflejada internamente quedando atrapada dentro de cable de fibra óptica como se muestra en la figura final.

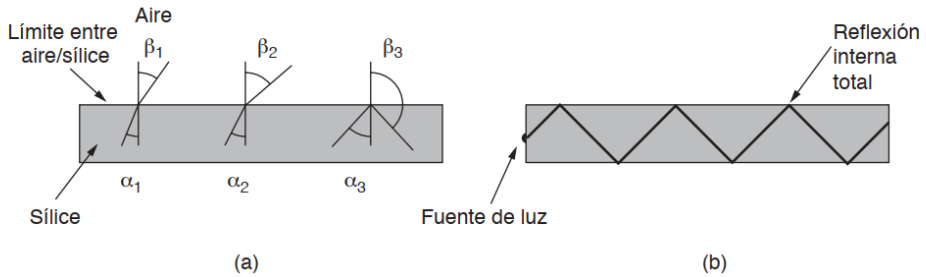


Figura 2.12 (a) Tres rayos de luz incidiendo sobre el límite entre aire y sílice a distintos ángulos. (b) Luz atrapada por reflexión interna total. (Fuente: Ref. [7]).

Cada uno de los haces reflejados es denominado modo. Si se tienen múltiples rayos reflejados la fibra es multimodo y si se tiene un solo haz que se propaga en línea recta la fibra es monomodo.

b) Cables de Fibra Óptica:

Los cables de fibra óptica contienen un núcleo de vidrio, a través del cual se propaga la luz. El grosor del núcleo en una fibra multimodo es de 62.5 o 50 micrómetros mientras que en una fibra monomodo es de 9 micrómetros. El núcleo es rodeado por un revestimiento de vidrio, con índice de refracción más bajo, para permitir la reflexión total del haz de luz hacia el núcleo y posteriormente se coloca una cubierta de plástico para proteger el revestimiento. En caso de llevar más de una fibra, se coloca una funda que permite agruparlas y llevarlas como un solo cable.

En la figura 2.13 se muestra la vista lateral de una fibra y de un cable conteniendo tres fibras al interior.

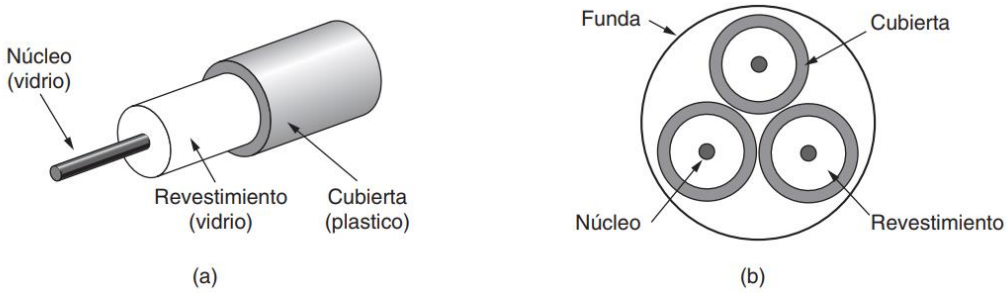


Figura 2.13 (a) Vista lateral de una fibra. (b) Vista de extremo de un cable con tres fibras. (Fuente: Ref. [7]).

En la figura 2.14 se muestra los modos de propagación en cables multimodo y monomodo. Observar los valores de diámetro del núcleo y revestimiento en cada caso.

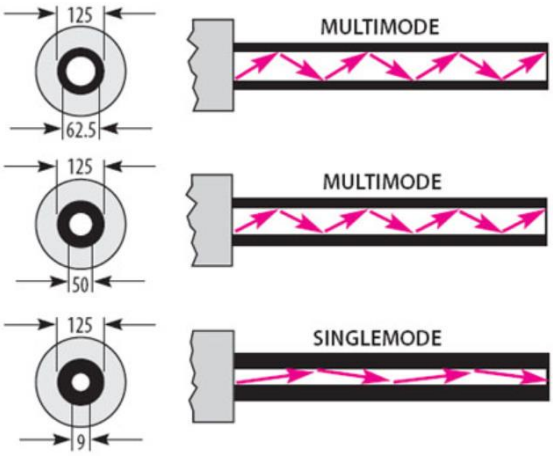


Figura 2.14 Modos de propagación en cables de fibra óptica (Fuente: Ref. [8])

c) Fuentes de Luz Óptica:

Las fuentes utilizadas para producir señales LED son de dos tipos: Diodos Emisores de Luz (LED, Ligth Emitting Diodes) y láseres semiconductores. En la figura 2.15 se muestra un cuadro que resume las características de cada tipo de fuente:

Característica	LED	Láser semiconductor
Tasa de datos	Baja	Alta
Tipo de fibra	Multimodo	Multimodo o monomodo
Distancia	Corta	Larga
Tiempo de vida	Vida larga	Vida corta
Sensibilidad a la temperatura	Poca	Considerable
Costo	Bajo	Elevado

Figura 2.15. Características de fuentes LED y Láser. (Fuente: Ref. [7])

La longitud de onda utilizada en la fuente de luz puede corresponder a una de tres regiones o ventanas de longitudes de onda centradas en: primera ventana (850 nm), segunda ventana (1300 nm) y tercera ventana (1550 nm). Las pérdidas por atenuación son menores cuanto mayor es la longitud de onda, por lo que la primera ventana es utilizada en enlaces de corta distancia (usualmente menores a 250m) y mientras que la tercera ventana es utilizada para distancias de varios kilómetros. La figura 2.16 muestra los valores de atenuación típicos en una fibra óptica de acuerdo con la longitud de onda del haz de luz.

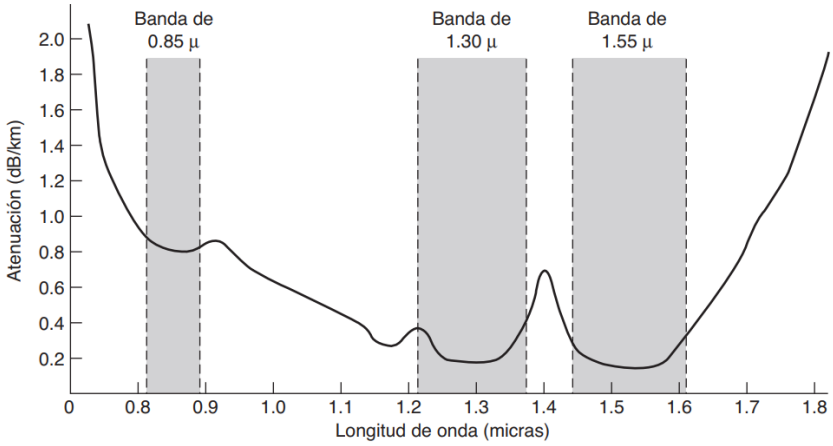


Figura 2.16 Atenuación de la luz dentro de una fibra óptica. (Fuente: Ref. [7])

d) Métodos de conexión

Los métodos de conexión para un cable de fibra óptica son tres:

- Conectores: Los cables son terminados en conectores que son insertados en puertos, transceptores o clavijas de fibra óptica, con una pérdida entre 10-20% de la potencia óptica. En la figura 2.17 se muestran los tipos de conectores más comunes:

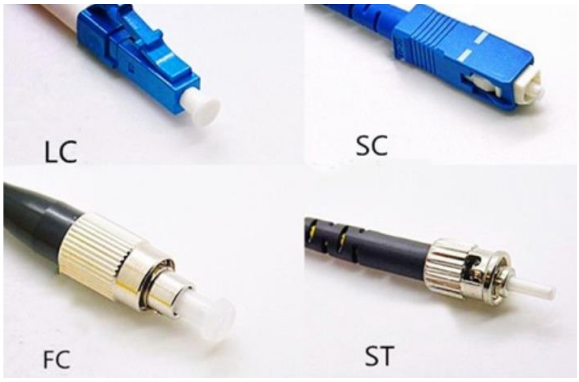


Figura 2.17 Conectores de cable de fibra óptica. (Fuente: Ref. [9])

- Empalmes mecánicos: Se acomodan los dos extremos cortados de fibra óptica utilizando una manga especial que los mantiene alineados. La pérdida en este tipo de empalmes es de 10%.

- Fusión: Los extremos de la fibra óptica son fusionados (fundidos) para conseguir una conexión sólida, con pérdidas muy pequeñas, siendo casi tan buenos como una sola fibra.

2.3.2. Cables de Par trenzado:

El cable de par trenzado es uno de los medios de transmisión más antiguos y utilizados hasta la actualidad. Consta de dos cables de cobre aislados y trenzados en forma helicoidal para cancelar la radiación electromagnética de ambos cables en el par, ofreciendo incluso inmunidad frente a ruidos externos. Los cables de par trenzado son utilizados usualmente en el sistema telefónico, pero también para transmitir datos, logrando anchos de banda importantes en distancias cortas. En la figura 2.18 se muestra un cable de par trenzado.

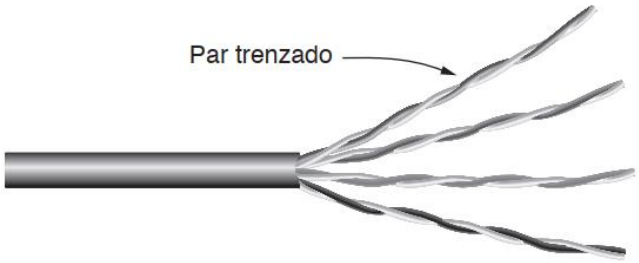


Figura 2.18 Cable de par trenzado. (Fuente: Ref. [7])

a) Tipos de Cables:

Los cables de par trenzado pueden identificarse según el nivel de blindaje utilizado en la construcción:

- *Unshielded twisted pair* (UTP) o cable de par trenzado sin blindaje, de bajo costo y de fácil uso, pero más susceptible a errores que otros tipos de cable y tiene limitaciones en la distancia soportada.

- *Foiled twisted pair* (FTP) o cable de par trenzado apantallado: Contiene pares trenzados, todos rodeados de una cubierta protectora global hecha de aluminio.

- ***Shielded twisted pair* (STP)** o cable de par trenzado blindado, con pares trenzados y rodeados en pares por una cubierta protectora de aluminio.

En la figura 2.19 se muestran los tipos de cable de par trenzado según el nivel de blindaje utilizado.

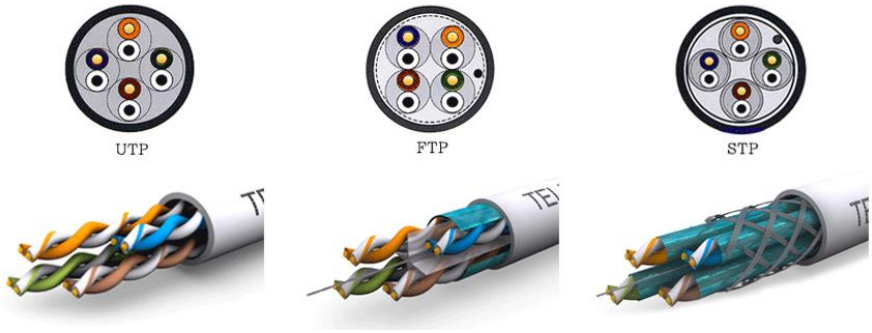


Figura 2.19 Cables de par trenzado UTP, FTP y STP. (Fuente: Ref. [10])

b) Categorías:

La norma más utilizada para transmisión de datos en las redes actuales es Categoría 6, que soporta la transmisión según la norma 1000BASE-T Ethernet a una distancia de 90 metros. Sin embargo, existen otras categorías de cableado que son mostradas en la figura 2.20 al igual que los casos de uso para los cuales fueron diseñados.

Name	Cable Type	Max. Data Rate	Bandwidth	Application
Cat1	Twisted Pair	1 Mbps	0.4 MHz	Telephone and modem lines
Cat2	Twisted Pair	4 Mbps	4 MHz	Older terminal systems, e.g. IBM 3270
Cat 3	Twisted Pair	10 Mbps	16 MHz	10BASE-T and 100BASE-T4 Ethernet
Cat 4	Twisted Pair	16 Mbps	20 MHz	16Mbit/s Token Ring
Cat 5	Twisted Pair	100 Mbps	100 MHz	100BASE-TX & 1000BASE-T Ethernet
Cat5e	Twisted Pair	1 Gbps	100 MHz	100BASE-TX & 1000BASE-T Ethernet
Cat 6	Twisted Pair	10 Gbps	250 MHz	10GBASE-T Ethernet
Cat 6a	Twisted Pair	10 Gbps	500 MHz	10GBASE-T Ethernet
Cat 7	Twisted Pair	10 Gbps	600 MHz	10GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable
Cat 7a	Twisted Pair	10 Gbps	1000 MHz	10GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable
Cat 8/8.1	Twisted Pair	40 Gbps	1600-2000 MHz	40GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable
Cat 8.2	Twisted Pair	40 Gbps	1600-2000 MHz	40GBASE-T Ethernet or POTS/CATV/1000BASE-T over single cable

Figura 2.20. Categorías de cables de par trenzado. (Fuente: Ref. [11])

c) Conectores:

Los cables de par trenzado de datos utilizan el conector RJ45. Este conector cuenta con 8 posiciones para los pines que son utilizados para terminar el cable de par trenzado. Existen dos normas reconocidas por ANSI TIA y EIA que definen la terminación de los cables Ethernet: T568A y T568B. Aunque, por su popularidad, la norma T568B es considerada como el esquema por defecto en cualquier conexión. En la figura 2.21 se muestra el código de colores definido en ambas normas T-568A y T-568B.

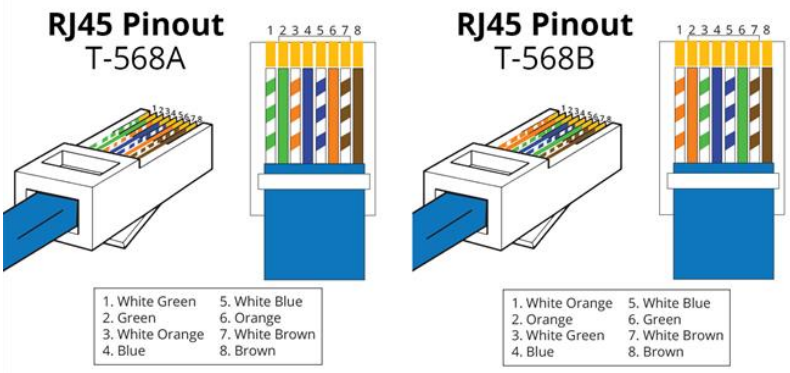


Figura 2.21. Normas T-568A y T-568B. (Fuente: Ref. [12])

- Cables Directos (*Straigth-through*): Los cables directos son utilizados en redes de datos para conectar una computadora a un conmutador. En un cable directo el orden de los pines coincide, utilizando una sola norma ya sea T-568A o T-568B. En la figura 2.22 se muestra un cable directo que utiliza T-568B en ambos extremos del cable.

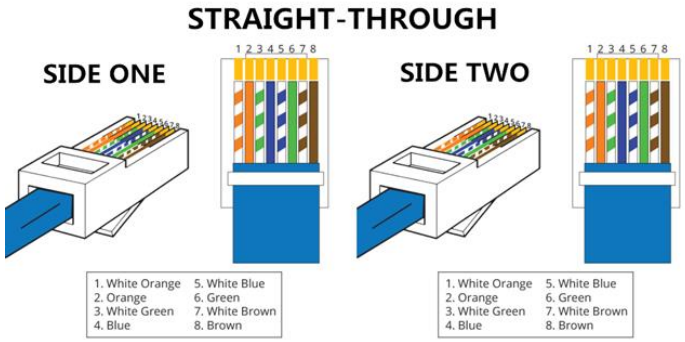


Figura 2.22. Conectores en un cable directo con T-568B. (Fuente: Ref. [12])

- Cables Cruzados (*Crossover*): A diferencia del cable directo, los cables cruzados usan diferentes normas en los conectores de cada extremo. Este tipo de cable era utilizado inicialmente de manera exclusiva para conectar dos computadoras entre sí, sin embargo, los dispositivos actuales usan capacidades MDI/MDI-X para reconocer al dispositivo remoto y cambiar la disposición de las señales eléctricas y utilizar cualquier tipo de cable, por lo que en la actualidad no es tan utilizado. En la figura 2.23 se muestra un cable cruzado que diferentes normas en los extremos del cable.

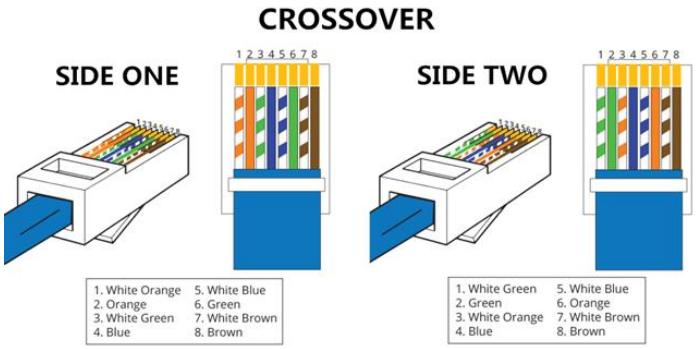


Figura 2.23 Conectores en un cable cruzado. (Fuente: Ref. [12])

2.3.3. Transceptores:

Los transceptores ópticos son utilizados usualmente como interfaz en los dispositivos de red pues brindan la posibilidad de recibir un conector de fibra óptica o de cobre según sea uno desee, bastando solamente con cambiar el tipo de transceptor.

La mayoría de los transceptores utiliza los siguientes códigos y ventanas de transmisión de luz óptica para indicar la distancia máxima que pueden soportar:

- **SR - 850 nm**, para un máximo de 300 m
- **LR - 1310 nm**, para distancias hasta 10 km
- **ER - 1550 nm**, para distancias hasta 40 km
- **ZR - 1550 nm**, para distancias hasta 80 km

Los transceptores más conocidos (SFP y XFP) son descritos a continuación.

a) SFP:

Conocido también como Small Form Pluggable, fue desarrollado en el marco de un acuerdo entre fabricantes de la industria de telecomunicaciones conocido como SFP MSA (SFP Multi Source Agreement) para soportar SONET, GigabitEthernet, FibreChannel, PON, etc. Aunque inicialmente estaba limitados a 1Gbps, se desarrollaron otras versiones que permiten alcanzar mayores velocidades, tales como:

- ***Enhanced Small Form Pluggable*** **(SFP+)**, versión mejorada que se denomina que soporta 8 Gbit/s Fibre Channel, 10 Gigabit Ethernet y el OTN standard OTU2. Tiene las mismas dimensiones que un SFP.
- **25 Gbit/s SFP28,** evolucionó de interfaces 100Gbps que utilizaban 4xSFP 25Gbps. Soporta 25Gpbs y hasta 28Gbps con sobrecosto (overhead).
- ***Compact Small form-factor pluggable*** **(cSFP),** una versión de SFP que permite usar un par de puertos SFP para tener 2 flujos bidireccionales con distintas longitudes de onda, obteniendo un lógicamente un puerto SFP 2xGE.
- ***Quad Small form-factor pluggable*** **(QSFP)**, desarrollado inicialmente para llevar 4 canales Gigabit Ethernet, 4GFC (Fiber Channel) soportando hasta 4Gbps. Su versión mejorada, QSFP+, soporta 40Gbps (4 canales de 10 Gigabit Ethernet o 10G Fibre Channel). También existen versiones para llevar mayor cantidad de tráfico tales como: 100 Gbit/s QSFP28 (100 Gigabit Ethernet o 32G Fibre Channel) y 200 Gbit/s QSFP56 (200 Gigabit Ethernet o 64G Fibre Channel).

En la figura 2.24 se muestra transceptores ópticos de tipo SFP 1GE y QSFP 40GE.

Figura 2.24 Transceptores SFP: a) SFP Óptico 1GE b) QSFP 40GE (Fuente: Ref. [13])

b) XFP:

De manera similar al SFP, fue desarrollado por un grupo de fabricantes conocido como XFP MSA. El módulo XFP es un transceptor diseñado para soportar 10 GigabitEthernet, 10Gbit/s FibreChannel, SONET OC-192, STM-64, 10Gbit/s OTN OTU-2. En la figura 2.25 se muestra un transceptor XFP 10GE

Figura 2.25 XFP 10Gigabit Ethernet (Fuente: Ref. [13])

2.4. Tecnologías de Capa de Enlace de Datos

2.4.1. Ethernet

Ethernet es considerado como una tecnología clave que propició el surgimiento de las redes de datos actuales incluyendo a Internet, y se encuentra prácticamente en todos los dispositivos de red actuales debido a su confiabilidad, facilidad para mantener, economía en los dispositivos utilizados, interacción con TCP/IP y su rápida adaptación para soportar velocidades cada vez mayores.

a) Historia

Ethernet fue desarrollado inicialmente para resolver el problema de control de acceso múltiple a un medio de transmisión compartido entre varios dispositivos bajo un protocolo conocido como DIX en 1978 (desarrollado por Dell, Intel y Xerox) y que luego pasó a convertirse en la norma IEEE 802.3 en 1983. Bajo esta norma se desarrolló la primera versión de Ethernet 10BASE5 conocida como Ethernet gruesa (*thick Ethernet*), por el cable coaxial de 9.5 mm al que las computadoras eran conectadas a través de adaptadores de red y le siguió la 10BASE2, también llamada Ethernet delgada (*thin Ethernet)* que utilizaba cables coaxiales. Estas versiones de Ethernet tenían una longitud máxima de transmisión y usaban repetidores para amplificar la señal y superar estas distancias. En la figura 2.26 se muestra la arquitectura de una red Ethernet clásica.

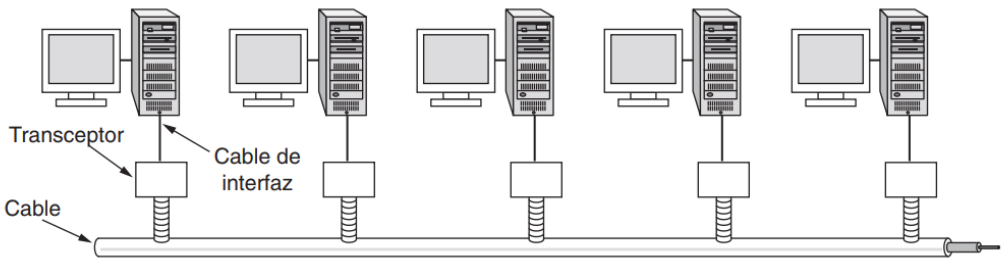


Figura 2.26 Arquitectura de red Ethernet clásica (Fuente: Ref. [7])

Al usar un medio compartido es necesario la utilización del algoritmo de Acceso Múltiple al Medio con Sensibilidad de Portadora con Detección de Colisiones (CSMA/CD) que monitorea el canal para detener la transmisión si hay colisiones en el momento en que se envía la información y volver a enviarla después de un tiempo aleatorio cuando el medio se encuentre disponible.

Posteriormente Ethernet evolucionó con el desarrollo de otros dispositivos que ayudaron a dejar de lado la arquitectura de un solo cable extenso de la norma inicial. Primero se incorporaron a la arquitectura, *hubs* (concentradores) que conectan eléctricamente los cables de los dispositivos como si estuvieran soldados en conjunto y, finalmente los conmutadores (*switches*), que crean el concepto de Ethernet conmutada en el cual se tiene un plano posterior (*backplane*) que interconecta a todos los dispositivos, pero la información es enviada únicamente al puerto donde se encuentra el dispositivo destino. En la figura 2.27 se muestra la representación de la arquitectura de un *hub* concentrador y conmutador.

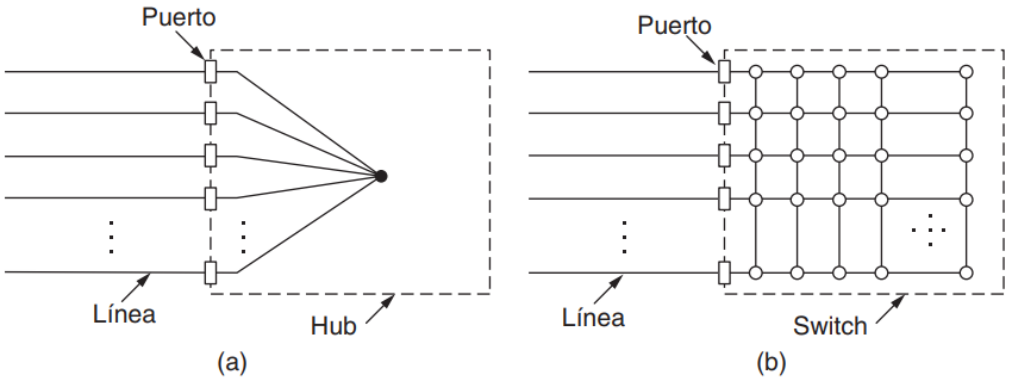


Figura 2.27 Representación de un a) Hub b) Conmutador (Fuente: Ref. [7])

Actualmente los dispositivos que ha prevalecido son los conmutadores pues permiten llegar a altas velocidades de transmisión sin los inconvenientes de colisiones que presentaban los dispositivos anteriores.

b) Normas IEEE 802.3

Ethernet se encuentra definido bajo el conjunto de normas IEEE 802.3. Estas definen la capa física y de enlace de datos, indicando el tipo de cableado permitido y las características de la información transmitida.

Las normas Ethernet tienen una nomenclatura que sigue una estructura general: xBASE-Z. El primer número x, indica la velocidad en Mbps sobre el canal, BASE se refiere a "*Baseband modulation*", que es el método de modulación empleado y la última cifra (o letra) Z, señala la longitud máxima del cable en centenares de metros, o el tipo de tecnología: Ejemplo: T: par trenzado (*Twisted pairs*), F: fibra óptica (*Fiber*), etc. En la tabla 2.1 se muestra un resumen de las normas Ethernet más conocidas:

Tabla 2.1 Normas Ethernet IEEE 802.3 (Fuente: Elab. propia)

Nombre IEEE	Nombre corto IEEE	Cable	Velocidad
802.3	10BASE-5	Cable coaxial grueso	10 Mbps
802.3a	10BASE-2	Cable coaxial delgado	10 Mbps
802.3i	10BASE-T	Cable de par trenzado	10 Mbps
802.3u	100Base-T4	UTP CAT. 3	100 Mbps
802.3u	100Base-TX	UTP CAT. 5	100 Mbps
802.3u	100Base-FX	Fibra óptica	100 Mbps
802.3z	1000Base-X	Fibra óptica	1 Gbps
802.3ab	1000Base-TX	UTP CAT.5	1 Gbps
802.3an	10GBASE-T	UTP CAT-6A o CAT-7	10 Gbps
802.3ae	10GBASE-X	Fibra óptica	10 Gbps
802.3ba	40GBASE-X	Fibra óptica	40 Gbps
802.3ba	100GBASE-X	Fibra óptica	100 Gbps

c) Formato de la trama Ethernet

En el momento de la publicación de la norma 802.3 por parte de la IEEE, ya existían muchos dispositivos en el mercado que seguían otra definición denominada Ethernet II. Sin embargo, IEEE decidió realizar algunas concesiones en el campo Longitud para soportar la compatibilidad con Ethernet II. Por tanto, se aceptan los dos formatos de tramas: Ethernet II y 802.3. La estructura de los campos en la trama Ethernet es la siguiente:

Preámbulo de 8 bytes, contiene un patrón repetido de bits 10101010 (a excepción del último, en el que los últimos 2 bits son 11). El último byte se llama delimitador de Inicio de trama en el 802.3 (SFD, *Start Frame Delimiter*) e indica al receptor que está a punto de empezar el resto de la trama.

Direcciones MAC Destino y Origen, de 6 bytes y globalmente únicas. Los 3 primeros bytes son un Identificador Único Organizacional (OUI, *Organizationally Unique Identifier*) que corresponde al fabricante (asignado por IEEE) y los últimos 3 bytes corresponden a un valor asignado por el fabricante al momento de su fabricación.

Tipo o Longitud, si el valor es menor o igual a 0x600 (1536) se puede interpretar como Longitud (IEEE 802.3), y si es mayor de 0x600 se interpreta como Tipo (Ethernet II).

Datos (*payload*), con longitud mínima de 46 bytes (se necesitan al menos 64 bytes desde la dirección de destino a la suma de verificación para que funcione la detección de colisiones). Si la porción de datos es menor que 46 bytes se utiliza un **relleno** para completar la trama al tamaño mínimo. El tamaño máximo según la norma es 1500 bytes.

Suma de verificación, un CRC de 32 bits usado para determinar si los bits de la trama se recibieron correctamente. Sólo realiza detección de errores y la trama se desecha si se detecta un error.

En la figura 2.28 se muestran ambos tipos de trama

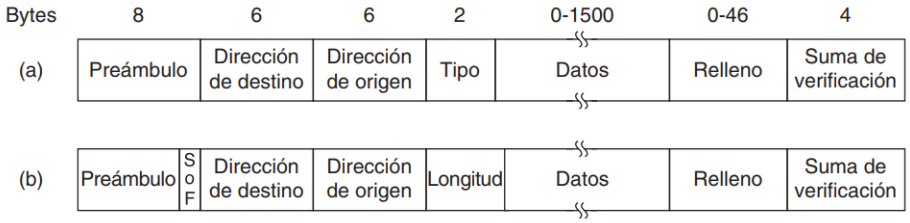


Figura 2.28 Formatos de trama a) Ethernet II b) IEEE 802.3 (Fuente: Ref. [7])

2.4.2. VLAN

Una VLAN (Virtual LAN), es la segmentación lógica de un dominio de broadcast en un conmutadora de capa 2 y se utilizan para dividir redes que son muy grandes o que requieran de una organización específica. Los dispositivos que se encuentran en VLANs diferentes comparten la misma infraestructura, pero funcionan como si estuvieran en su propia LAN (Red de Área Local) independiente.

En la figura 2.29 se muestra una red LAN segmentada con VLANs y troncales 802.1Q.

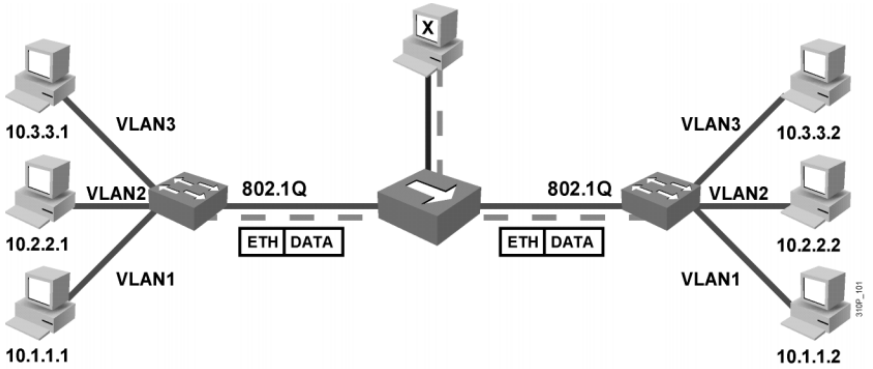


Figura 2.29 Red LAN segmentada con VLANs y troncales Ethernet 802.1Q (Fuente: Ref. [14])

2.4.3. Troncales Ethernet y IEEE 802.1q

Un enlace troncal de VLANs es un enlace físico que transporta simultáneamente el tráfico de varias VLANs. El tráfico es enviado por dispositivos de red (conmutadores, enrutadores o PC's con NIC adecuadas) que cuentan con esa capacidad.

IEEE 802.1Q, también conocido como **dot1q** es el protocolo desarrollado por la IEEE para etiquetar las tramas en una troncal de VLANs. Este protocolo muestra el siguiente formato:

- TPID (*Tag Protocol ID* - Identificador de Etiqueta de Protocolo): 2 bytes con un valor fijo de 0x8100, indica que es una trama con etiqueta de VLAN.

- TCI (*Tag Control Information* - Información de Control de Etiqueta): 2 bytes con 3 subcampos:

○ PCP (*Priority Code Point*): 3 bits, indicador de prioridad.

○ DEI (*Drop Eligibility Indicator*): 1 bit, indicador de descarte.

○ VID (VLAN ID): 12 bits, identificador de VLAN en el rango 1-4094.

En la figura 2.30 se muestran los campos de dot1q dentro de una trama Ethernet.

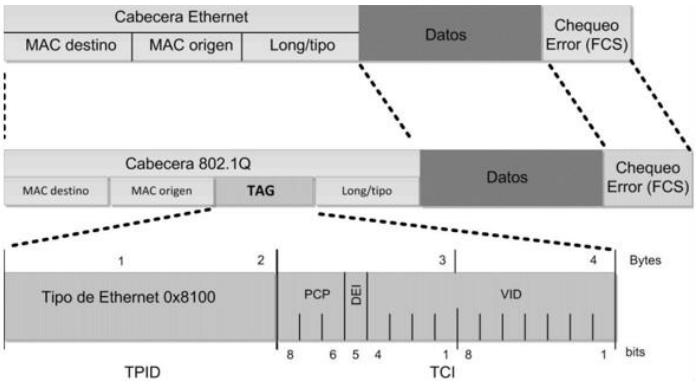


Figura 2.30 Posición del tag 802.1Q en la trama ethernet. (Fuente: Ref. [14])

2.4.4. Spanning Tree

El protocolo de Árbol de Expansión o *Spanning-Tree* (STP), definido originalmente en la norma 802.1d de la IEEE, es útil para construir topologías libres de bucles de capa 2 previniendo de esa manera las tormentas de tráfico de difusión (*broadcast storm*). Una tormenta de tráfico de difusión se da cuando estas tramas se quedan circulando indefinidamente en la red, consumiendo de manera progresiva todo el ancho de banda disponible, pues al no existir un campo TTL (*Time To Live*) en la capa 2, el tráfico de difusión seguirá en la red indefinidamente hasta que alguien apague uno de los conmutadores o rompa un enlace. STP ejecuta el Algoritmo de Árbol de Expansión (STA, *Spanning Tree Algorithm*), entre todos los conmutadores para encontrar una topología libre de bucles tomando como punto de referencia llamado puente raíz *(root bridge*) y los enlaces disponibles hacía él. STP evalúa si existen más de un enlace, seleccionando el mejor y bloqueando los demás como se puede observar en la figura 2.31.

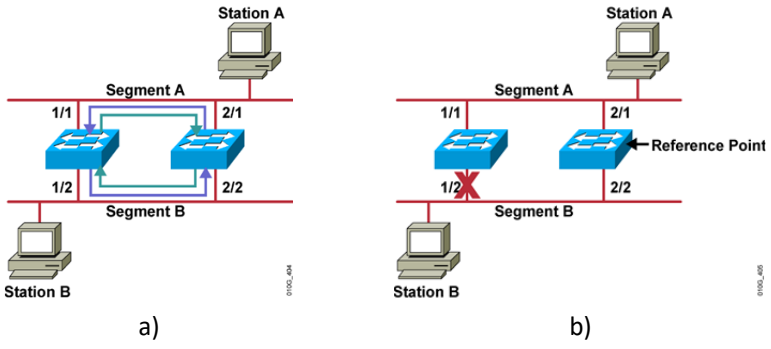


Figura 2.31 Bucle eliminado con STP. (Fuente: Ref. [15])

a) Funcionamiento

El protocolo STP hace uso extensivo de varios conceptos claves:

- **Bridge ID (ID de *Bridge*)**, identifica cada conmutador de manera única. En la norma original 802.1D, el Bridge ID estaba formado por la Prioridad y la MAC del conmutador, además de utilizar un único árbol de expansión común o CST (*Common Spanning Tree*) para todas las VLANs. Sin embargo, el Bridge ID fue modificado añadiendo un campo VLAN-ID, soportando otras versiones de STP que requieren también el valor de VLAN para poder crear una topología STP por cada VLAN. En la figura 2.32 se muestran los formatos original y extendido del bridge-id.

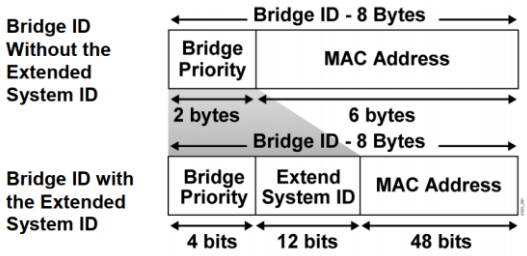


Figura 2.32 Formato extendido del ID de Bridge (Fuente: Ref. [15])

- **El costo del Enlace o Ruta**, utilizado para evaluar el camino a otros conmutadores. En la tabla 2.2 se muestran los costos por defecto de varios tipos de enlace según las normas 802.1d y 802.1t. Notar que los costos están definidos de manera no lineal y que los valores fueron actualizados de su valor original para soportar anchos de banda más grandes.

Tabla 2.2 Costos STP por defecto (Fuente: Elab. propia)

Velocidad	802.1d (Original)	802.1d	I802.1t
10 Mbps	100	100	2000000
100 Mbps	10	19	200000
1 Gbps	1	4	20000
10 Gbps	1	2	2000
100 Gbps	1	1	200
1 Tbps	1	1	20
10 Tbps	1	1	2

- **BPDU** (*Bridge Protocol Data Units* - Unidad de Datos de Protocolo de Bridge), son enviados hacia todos los conmutadores vecinos por cada puerto del conmutador conteniendo la información requerida para el cálculo de STP. En la figura 2.33 se muestra el formato utilizado en los BPDUs:

Bytes	Campo
2	ID de protocolo
1	Version
1	Tipo de mensaje
1	Flags
8	ID de Raíz
4	Costo de paso
8	ID de Bridge
2	ID de Puerto
2	Tiempo del mensaje
2	Tiempo máximo
2	Tiempo de Hello
2	Retardo de transmisión

Figura 2.33 Formato de mensajes de STP. (Fuente: Ref. [14])

Existen dos tipos de BPDU:

✓ BPDU de configuración o *Configuration* BPDU, usado durante el cálculo de STP.

✓ BPDU de Notificación de Cambios en la Topología o *Topology Change Notification* (TCN) BPDU, utilizado para anunciar cambios en la topología de la red.

b) Operación

El algoritmo STP realiza 4 acciones para converger en una topología sin bucles:

1. **Elección del Conmutador Raíz (*Root Bridge*)**, el proceso inicia con todos los conmutadores enviando BPDUs de configuración. Se elige al conmutador con el menor Bridge ID como Conmutador Raíz (*Root*).
2. **Elección de los Puertos Raíz (*Root Ports*),** se elige el puerto con menor costo al *Root* en cada uno de los demás conmutadores. El costo desde un puerto hacia el *root* se halla sumando los costos en cada enlace hasta llegar al *Root*. En caso de existir más de un puerto con la misma distancia se usan las siguientes reglas en orden:
   - ✓ Bridge ID de transmisor menor (*Lowest Sender* BID).
   - ✓ Prioridad de puerto menor (*Lowest Port Priority*).
   - ✓ ID de puerto menor (*Lowest Port* ID).
3. **Elección de los Puertos Designados (*Designated Ports*)** en cada segmento seleccionando el puerto con menor costo de ruta al root. El conmutador que contiene el Puerto Designado es denominado como conmutador designado (*designated switch*) para ese segmento. En caso de requerir un desempate se siguen las siguientes reglas:
   - ✓ BID de transmisor menor (*Lowest Sender* BID).
   - ✓ Prioridad de puerto menor (*Lowest Port Priority*).
   - ✓ ID de puerto menor (*Lowest Port* ID).
4. **Bloquear los puertos no elegidos como designados (*Non-designated Ports*) o *root port***, lo cual permite la prevención de lazos de STP.

c) Estado de los puertos en STP

Al participar en STP, cada puerto del conmutador pasa por varios estados hasta llegar al estado final en el que puede reenviar tráfico. Estos estados son los siguientes:

- **Deshabilitado (*Disabled*),** puertos apagados administrativamente.
- **Bloqueado (*blocking*),** el puerto no puede recibir ni transmitir datos, tampoco puede agregar direcciones MAC a su tabla de direcciones, pero se permite que reciba BPDUs para que pueda escuchar a otros conmutadores vecinos. Este es el estado inicial de un puerto al momento de inicializar de modo que no se pueden formar bucles.
- **Escucha (*listening*),** el puerto aún no puede enviar o recibir tráfico, sin embargo, puede recibir y enviar BPDUs participando activamente en el proceso de STP. Aquí, el puerto puede convertirse en un puerto raíz o puerto designado. Si el puerto pierde su estado de puerto raíz o puerto designado, volverá al estado de bloqueo.
- **Aprendizaje (*learning*),** después de un período de tiempo denominado retardo de reenvío (*Forward Delay*) en el estado de escucha, el puerto pasa al estado de aprendizaje. El puerto sigue enviando y recibiendo BPDUs y adicionalmente puede aprender nuevas direcciones MAC. Sin embargo, el puerto todavía no puede enviar ninguna trama de datos.
- **Retransmisión (*forwarding*),** después de otro período de tiempo de retardo de reenvío en el estado de aprendizaje, el puerto pasa al estado de reenvío. El puerto ahora podrá enviar y recibir tramas de datos, recopilar direcciones MAC, enviar y recibir BPDUs.

En la figura 2.34 se muestra una topología libre de bucles de capa 2 resultante luego de la convergencia del protocolo STP.

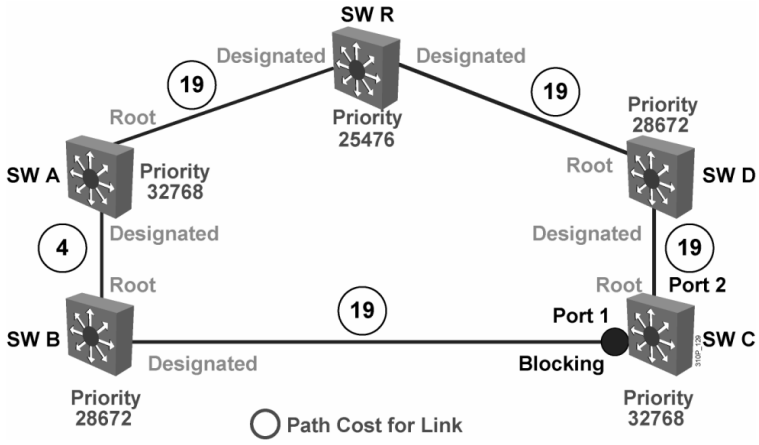


Figura 2.34 Ejemplo de topología STP. (Fuente: Ref. [15])

d) Evolución del protocolo STP

El protocolo STP ha evolucionado desde su versión original en la norma 802.1d.

- **RSTP (*Rapid Spanning Tree Protocol*),** sigue la norma IEEE 802.1w y alcanza una convergencia más rápida. RSTP tiene estados de puertos distintas como: Alternativo

(*Alternate*) y Resguardo (*Backup*). Los puertos que no participan en el Árbol de Expansión se conocen como Puertos de Borde (*Edge Ports*). RSTP es compatible con 802.1d y el formato de la trama BPDU es el mismo, excepto que el campo de Versión se indica con 2.

- **Múltiple Árbol de Expansión (*Multiple Spanning Tree* – MST)**, sigue la norma IEEE 802.1s, es una versión más reciente de STP que extiende la norma IEEE 802.1w RSTP a múltiples instancias de STP. El principal propósito de MST es reducir el número total de instancias de árboles de expansión que se pueden plantear en una topología física de red, y así reducir los ciclos de CPU de un conmutador utilizando un número mínimo de instancias STP.

También, existen versiones propietarias del protocolo desarrollados por varios fabricantes como las siguientes:

- ***Per-VLAN** Spanning **Tree*** **(PVST+)** de Cisco, crea una instancia de STP 802.1D por cada VLAN configurada en la red.
- ***Rapid Per-VLAN Spanning Tree*** **(Rapid PVST+)** de Cisco, que proporciona una instancia separada de 802.1w por VLAN.
- ***Virtual Spanning-Tree*** **(**VSTP**)** de Juniper, es compatible con PVST+ y Rapid PVST+.

2.4.5. Agregación de Enlaces mediante LACP

La agregación de enlaces permite combinar varias interfaces Ethernet y tratarlos como una sola interfaz lógica para aumentar la capacidad disponible del enlace. Agregando además redundancia y balanceo de tráfico entre todos los enlaces del grupo.

La norma IEEE 802.3ax define el Protocolo de Control de Agregación de Enlaces o ***Link Aggregation Control Protocol*** **(LACP)** para controlar el establecimiento y operación de los grupos de enlaces agregados (*Link Aggregation Group*, LAG) a través del intercambio de unidades de datos de protocolo de LACP (LACPDU) para monitorear los enlaces entre dispositivos vecinos. En la figura 2.35 se muestra un dispositivo de red con interfaces formando un enlace agregado.

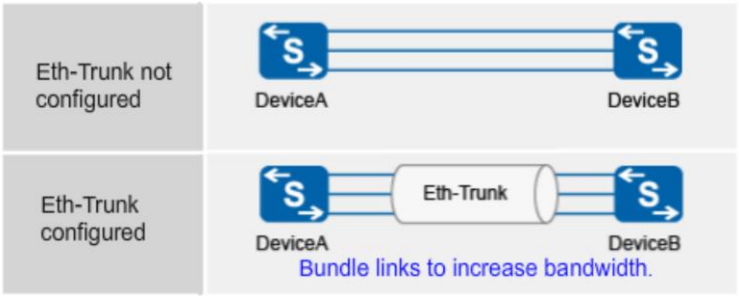


Figura 2.35 Enlaces agregados en un dispositivo de red. (Fuente: Ref. [16])

a) Tipos de puerto:

- **Puerto pasivo:** El puerto solo transmitirá LACPDUs cuando su homólogo use LACP activo (no participa en la conversación a menos que otro la inicie).
- **Puerto activo:** el puerto transmite LACPDUs independientemente de si su contraparte inicia la conversación o no.

b) Operación:

El proceso de establecimiento de sesiones LACP es el siguiente:

5. Ambos dispositivos envían LACPDU's entre ellos.
6. Se elige al dispositivo Actor, que es el dispositivo con mayor prioridad de sistema (*system priority*), numéricamente es el de menor valor. Si ambos tienen la misma prioridad se usa la MAC de menor valor.
7. El Actor elige a los enlaces activos que forman parte del LAG, considerando sólo a los que tengan mayor prioridad (menor valor numérico) que su contraparte. Los otros serán colocados en espera (*standby*).

En la figura 2.36 se muestra el proceso de establecimiento de las sesiones LACP.

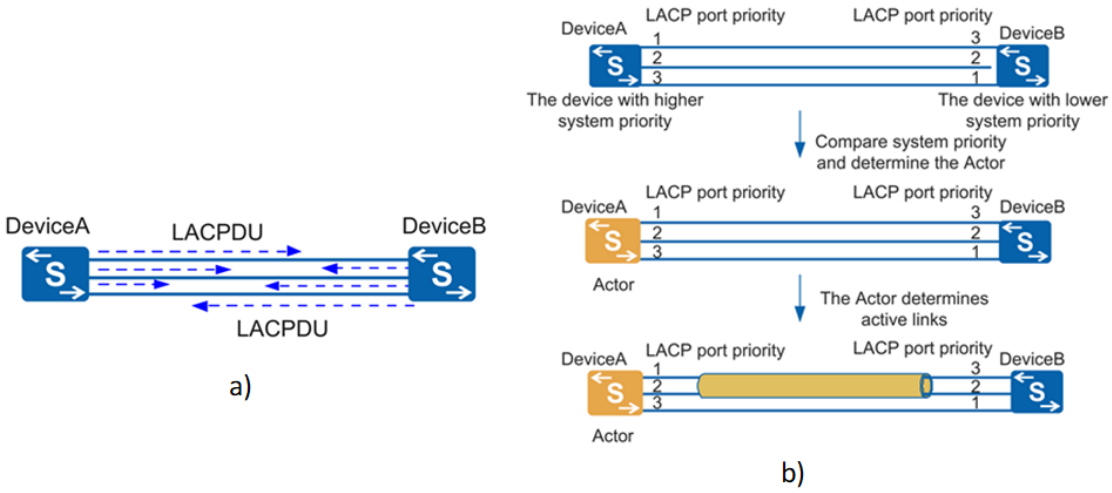


Figura 2.36 Operación de LACP. a) Envío de LACPDUs b) Elección de actor y puertos activos (Fuente: Ref. [16])

c) Modos de Balanceo.

Es posible usar los siguientes modos de equilibrio de carga según el tipo de red:

- Basado en las direcciones MAC de origen y/o destino de paquetes
- Basado en las direcciones IP de origen y/o destino de los paquetes.
- Basado en el resultado OR exclusivo de las direcciones MAC de origen y destino.
- Basado en el resultado OR exclusivo de las direcciones IP de origen y destino.

d) Interoperabilidad con STP.

Desde la perspectiva del protocolo STP solo existe una interfaz lógica que representa a todo el LAG por la que se envían BPDUs pues los puertos individuales no son parte de la topología STP. Gracias a esto, se puede aprovechar la capacidad total de todos los enlaces sin el bloqueo de algún puerto como sucedería al aplicarse las reglas habituales de STP.

- **Implementaciones propietarias**

Existen otros protocolos desarrollados por fabricantes de equipo para el establecimiento de un LAG, que son mostrados en la tabla 2.3:

Tabla 2.3 Algunas implementaciones de LAG. (Fuente: Elab. propia)

Fabricante	Nombre de la Implementación
Cisco	EtherChannel and Port Aggregation Protocol
Juniper	Aggregated Ethernet
Huawei	Eth-Trunk
Windows	Windows NIC Teaming
Red Hat	LACP bonding
Solaris	Dladm aggr

2.4.6. MC-LAG

MC-LAG, o grupo de agregación de enlaces de múltiples chasis, es un tipo de grupo de agregación de enlaces (LAG) entre puertos que se encuentran en equipos diferentes, principalmente con el propósito de proporcionar redundancia en caso de que falle uno de los equipos. Las implementaciones del MC-LAG son propietarias y difieren en cuanto al protocolo existente entre los equipos para sincronizar y negociar conmutaciones automáticas (*failover*), pero deben ser compatibles con LACP y la norma 802.1ax (LACP). En 2012, el IEEE creó una alternativa estandarizada para MC-LAG en IEEE 802.1aq (puente de ruta más corta). En la tabla 2.4 se muestran algunas implementaciones de MC-LAG propietarias de los fabricantes más conocidos:

Tabla 2.4 Algunas implementaciones de MC-LAG. (Fuente: Elab. propia)

Fabricante	Nombre de la Implementación
Cisco Catalyst 6500 - VSS	Multichassis Etherchannel (MEC)
Cisco Catalyst 9000	StackWise Virtual
Cisco Nexus	Virtual PortChannel (vPC)
Cisco IOS-XR	mLACP
Dell Networking	Virtual Link
Fortinet	MC-LAG (Multi Chassis Link Aggregation Group)
HPE/Aruba	Distributed Trunking
Juniper	MC-LAG
ZTE	MC-LAG
Huawei	M-LAG

a) Cisco Virtual Portchannel

En esta sección se elige a vPC de Cisco para explicar el funcionamiento típico de los mecanismos utilizados por los fabricantes de equipos para implementar MC-LAG. Luego se revisan de manera resumida las implementaciones de Juniper y Huawei.

Cisco desarrolló vPC para implementar MC-LAG en sus equipos Nexus con software NX-OS. vPC permite que los enlaces que están conectados a dos equipos Nexus diferentes, se vean como un solo Port-channel (término de Cisco para definir un LAG).

El elemento más importante de un vPC es el ***peerlink*** que se utiliza para tener un solo plano de control reenviando BPDU's, sincronizando información de LACP, direcciones MAC, entradas IGMP, transporte para tráfico multicast y también paquetes HSRP (protocolo FHRP de Cisco). Adicionalmente, se usan enlaces dedicados con la función de vPC ***peer-keepalive*** para resolver escenarios dual-active cuando se pierde la conectividad del *peerlink*. El *peer-keepalive* puede utilizar enlaces físicos directos o equipos intermedios como una red de gestión fuera de banda. En la figura 2.37 se muestra como la utilización de vPC agrupa enlaces físicos de equipos diferentes en un solo enlace lógico.

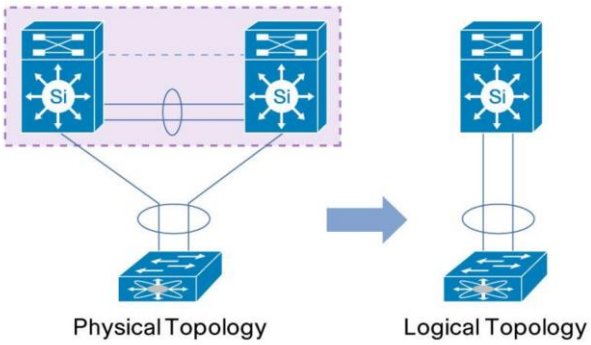


*Figura 2.*37 *Cisco vPC (Fuente: Ref.* [17]*)*

Terminología vPC:

- **vPC**: Port-channel combinado entre los vPC *peers* y el dispositivo *downstream*.
- **vPC *peer device*:** uno de los dispositivos los cuales están conectados con el puerto especial conocido como vPC Peer-link.
- **vPC *peer-link***: el enlace usado para sincronizar los estados entre los VPC *peers*. Ambas interfaces deben ser interfaces de 10GE.
- **vPC *domain***: Este dominio está formado por los 02 dispositivos que configuran el vPC peer-link.
- **vPC *peer-keepalive link***: el enlace *peer-keepalive* entre los vPC *peers* aseguran que ambos equipos estén UP. El enlace *peer-keepalive* envía mensajes de *keepalive* periódicos entre los equipos conectados por el vPC *peer-link*. Esto puede realizarse a través de los puertos de gestión (*management*).
- **vPC *member port***: Interfaces que pertenecen a la vPC.

- **vPC VLAN**: es una de las VLANs llevadas sobre el enlace peer-link y es usado para comunicarse vía vPC con otro dispositivo.
- **Non-vPC VLAN**: uno de los STP VLANs que no son llevados sobre el peer-link.
- **CFS**: Cisco Fabric *services protocol*, usados para sincronización de estados y validación de configuración entre los vPC *peer devices.*

En la figura 2.38 se muestran los elementos que conforman un vPC.

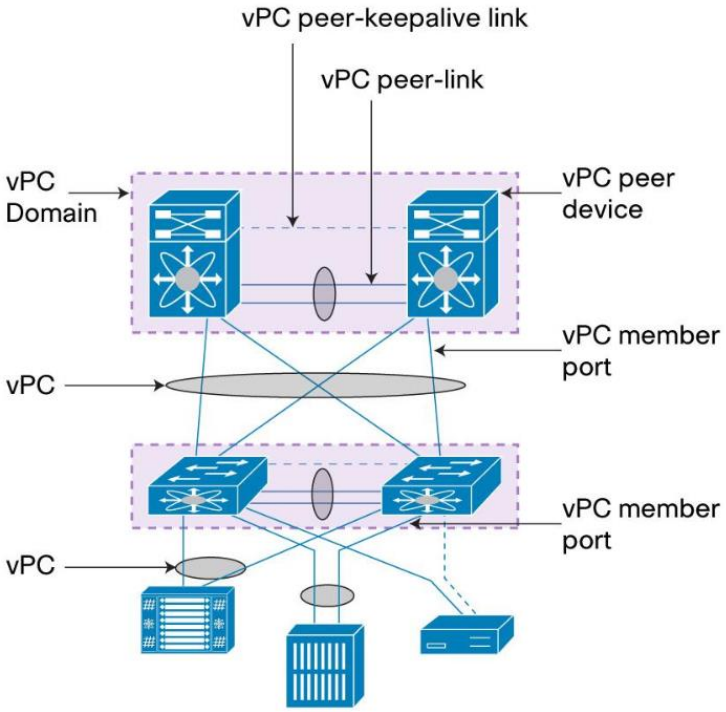


*Figura 2.*38 *Topología de Red vPC. (Fuente: Ref.* [17]*)*

Parámetros de configuración

Los siguientes parámetros de configuración deben ser idénticos, caso contrario el VPC cambiará al modo suspendido:

- Modo de PortChannel (on, off, o active)
- Velocidad de los enlaces
- Modo Dúplex
- Modo de troncal de VLANs
- Estado de VLAN
- Configuraciones globales *de Spanning Tree Protocol* y específicas de interfaz.
- Parámetros de calidad de servicio (QoS)

Los siguientes parámetros deberían ser idénticos, pero esto no es estrictamente necesario:

- Tiempo de envejecimiento dirección MAC.
- Entradas estáticas de dirección MAC.

- Configuraciones de Access-list (ACL) y parámetros
- Configuraciones de interfaces de STP.

- **Juniper MC-LAG**

La implementación MC-LAG de Juniper utiliza un protocolo para intercambio de información y coordinación entre los dispositivos llamado *Interchassis Control Protocol* (ICCP) para asegurar que el tráfico es enviado apropiadamente mediante una interfaz agregada dedicada para este propósito.

Adicionalmente se hace uso del *Interchassis Link* (ICL) también conocido como *Interchassis Link-Protection Link* (ICL-PL), se utiliza para reenviar el tráfico de datos a través de los vecinos MC-LAG. Este enlace proporciona redundancia cuando se produce una falla de enlace (por ejemplo, una falla del troncal MC-LAG) en uno de los enlaces activos. La ICL puede ser una sola interfaz Ethernet física o una interfaz Ethernet agregada. En la figura 2.39 se muestra una topología con los elementos de un MC-LAG de Juniper.

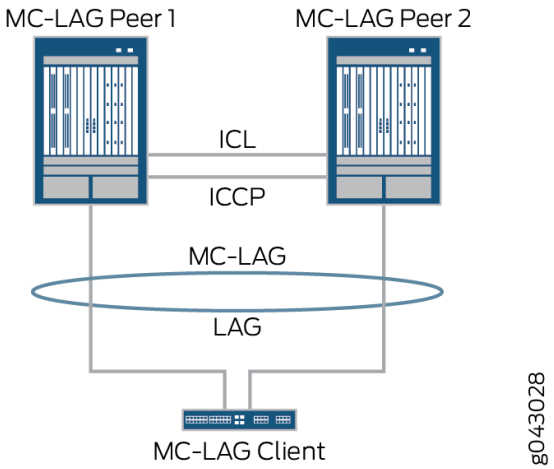


*Figura 2.*39 *Topología Juniper MC-LAG. (Fuente: Ref.* [18] *)*

- **Huawei M-LAG**

La implementación de Huawei es llamada M-LAG y utiliza algunos conceptos similares a los utilizados por Cisco vPC como los siguientes:

- **Grupo Dynamic Fabric Service (DFS):** Usado para emparejar dispositivos M-LAG. Los dispositivos M-LAG utilizan el protocolo de grupo DFS para sincronizar información como el estado de la interfaz y las entradas.
- **DFS *master device*,** dispositivo configurado con M-LAG en estado maestro.
- **DFS *backup device*,** dispositivo configurado con M-LAG en estado de backup.
- **Enlace Dual Active Detection (DAD)**: utilizado para que los dispositivos M-LAG master y backup intercambien paquetes DAD en la Capa 3.

- ***Peer-link***, se utiliza para intercambiar paquetes de negociación y transmitir parte del tráfico. Se recomienda utilizar varios enlaces agregados.
- **M-LAG *member port***, son las interfaces pertenecientes a M-LAG en los dispositivos de respaldo y maestro M-LAG que están conectados al host o k del lado del usuario.
- Las interfaces de los miembros de M-LAG también funcionan en modo *master*/*backup*. Cuando las interfaces de los miembros locales y remotos sincronizan la información, la interfaz que levanta primero se convierte en la interfaz M-LAG master, y la otra interfaz se convierte en la interfaz M-LAG *backup*.

En la figura 2.40 se muestra la topología básica de M-LAG de Huawei.

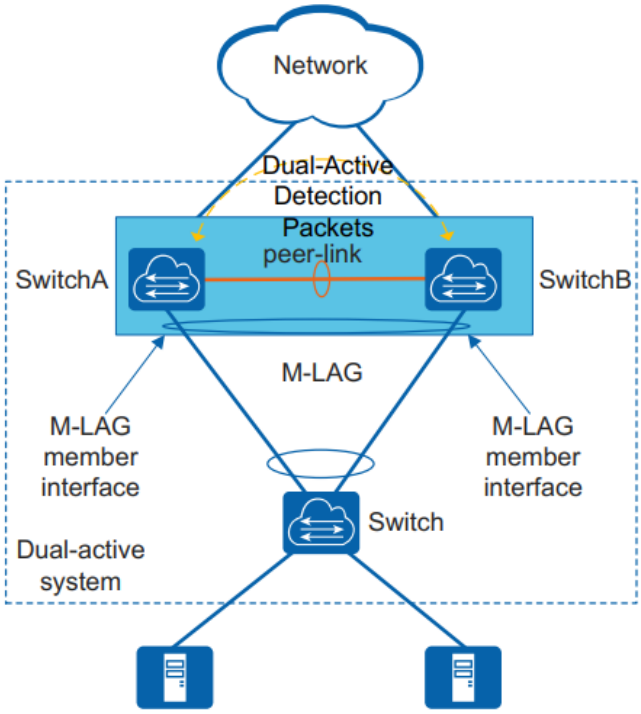


*Figura 2.*40 *Topología Huawei M-LAG. (Fuente: Ref.* [16]*)*

2.5. Tecnologías de Capa de Red

En esta sección se describe el funcionamiento de los protocolos de capa de red a utilizar en el presente proyecto.

2.5.1. IS-IS

El protocolo *Intermediate System to Intermediate System* (IS-IS) forma parte del conjunto de protocolos OSI. IS-IS fue desarrollado inicialmente a finales de la década de 1980 por Digital Equipment Corporation (DEC) para luego ser estandarizado por ISO en la norma ISO/IEC 10589 como un protocolo de enrutamiento para el protocolo ISO de redes sin conexión o *Connectionless Network Protocol* (CLNP). El protocolo fue modificado posteriormente por la IETF para soportar el protocolo IP en la RFC 1195 en una versión llamada Dual IS-IS.

a) Terminología ISO

Para entender el funcionamiento de IS-IS es necesario comentar algunos términos que la nomenclatura ISO utiliza para describir los mismos elementos que IETF denomina de otra manera:

- Un enrutador es un sistema intermedio (*Intermediate-System*, IS) y un host es un sistema final (*End System*, ES).
- Punto de conexión de subred (*Sub Network Point of Attachment*, SNPA) es una interfaz conectada a una subred que define el punto en el que se proporciona un servicio de subred.
- Servicio No Orientado a Conexión (*Connectionless Network Service*, CLNS) es el servicio OSI en la capa de red para la transferencia de información entre dos puntos.
- Unidad de datos de protocolo o *Protocol Data Unit* (PDU) es la unidad de datos que es compartida entre nodos diferentes de la misma capa OSI. Por ejemplo, una trama de capa 2 es un PDU de enlace de datos (*Data Link* PDU, DLPDU), y un paquete es una PDU de red (*Network* PDU, NPDU). También se cuenta con los PDU que describen el estado de un enlace (*Link State* PDU, LSP) que viene a ser la función equivalente a los LSA de OSPF.

b) Áreas IS-IS

En IS-IS, un dominio de enrutamiento se puede dividir en grupos más pequeños denominados áreas, donde los enrutadores o sistemas se encuentran organizados jerárquicamente en dos: Nivel 1 (L1) y Nivel 2 (L2). Los sistemas nivel 1 son utilizados cuando el enrutamiento es realizado al interior de un área; y el nivel 2 cuando el destino se encuentra fuera de un área. En la figura 2.41 se muestran un dominio de enrutamiento IS-IS con áreas y sistemas L1 y L2.

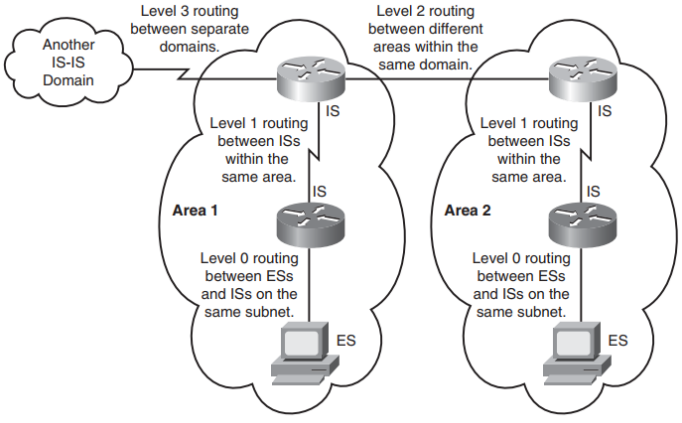


Figura *2.*41 Areas IS-IS y sistemas L1/L2. (Fuente: Ref. [19])

c) Direccionamiento NSAP

IS-IS utiliza direcciones de red ISO donde cada dirección identifica un punto de conexión a la red, tal como una interfaz de enrutador, y se denomina punto de acceso al servicio de red (NSAP).

Un sistema final (ES) puede tener varias direcciones NSAP, en cuyo caso las direcciones solo difieren en el último byte (denominado selector-n). Cada NSAP representa un servicio que está disponible en ese nodo. Además de tener múltiples servicios, el nodo puede pertenecer a múltiples áreas.

Los enrutadores (IS) también tienen una dirección de red especial que es denominada título de entidad de red o *Network Entity Title* (NET). Estructuralmente, una NET es idéntica a una dirección NSAP, pero tiene un n-selector de 00.

Las direcciones NET son hexadecimales y tienen una longitud variable de 8-20 bytes. En general, su formato consta de un campo de:

- Autoridad e Identificador de Formato o *Authority and Format Identifier* **(AFI):** 1 byte,
- ID de dominio (*domain ID*): longitud variable
- ID de área (*area ID*): 0-12 bytes
- Identificador de sistema (*system-id*): 6 bytes
- Selector: 1 byte

El formato más simple omite el ID de dominio y tiene una longitud de 10 octetos. Por ejemplo, en la figura 2.42 se muestra la dirección NET 49.0001.1921.6800.1001.00 y las partes que la conforman:

AFI	ID AREA	ID Sistema	SEL
49	. 0001 .	1921 . 6800 . 1001	. 00
1 byte	0-12 bytes	6 bytes	1 byte

Figura 2.42 Ejemplo dirección NET IS-IS. (Fuente: Elab. propia)

d) Niveles de enrutamiento en IS-IS

IS-IS realiza el enrutamiento de manera jerárquica según el tipo de área donde se encuentra cada enrutador.

- **Nivel 1**, los enrutadores comparten información de enrutamiento dentro del área y mantiene un base de datos de estados de enlace (LSDB) de todos los sistemas de nivel 1. Su función es equivalente en OSPF al de los enrutadores internos diferentes del área 0.
- **Nivel 2**, los enrutadores comparten información de rutas Inter área únicamente con los enrutadores de nivel 2 y mantiene una LSDB de todos estos. Su equivalente en OSPF es el área 0.
- **Nivel 1-2,** los enrutadores que tienen interfaces en ambos niveles realizan el enrutamiento intra e inter-área, y mantienen una LSDB por separado para cada nivel. Cuando un enrutador L1 necesite enviar un paquete a un destino de área diferente enviará el paquete al enrutador L1-2 más cercano, para seguir con el proceso de reenvío en L2 hasta llegar al área destino donde el paquete finalmente será reenviado en nivel 1.

En la figura 2.43 se muestran un ejemplo de las posibles adyacencias por nivel para los enrutadores en el mismo segmento de red.

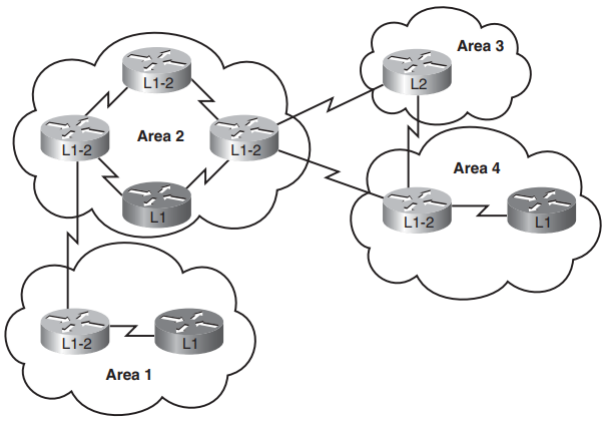


Figura 2.43 Adyacencias por nivel L1, L2 IS-IS. (Fuente: Ref. [19])

e) Paquetes IS-IS

IS-IS intercambia información entre los enrutadores a través de PDU's.

A continuación, se indican los tipos de PDU utilizados.

- **IIH (*Intermediate System-to-Intermediate System Hello* PDUs),** se intercambian entre vecinos IS con el protocolo IS-IS habilitado. Los IIH incluyen ID del sistema, direcciones de área y *system*-id de los vecinos conocidos por el IS emisor.

Hay tres tipos de IIHs:

- Punto a punto (*point-to-point*): se envían en circuitos punto a punto.
- Nivel 1 LAN (*Level* 1 LAN): en circuitos de acceso múltiple cuando el IS es de nivel 1.
- Nivel 2 LAN (*Level* 2 LAN): en circuitos de acceso múltiple cuando el IS es de nivel 2.
- **LSP (*Link State* PDUs),** utilizado por un enrutador para anunciar a sus vecinos, las redes que tiene directamente conectadas. Los LSP permiten que IS-IS obtenga información de toda la topología tanto a nivel 1 como a nivel 2.
- ***Sequence Number* PDUs (SNPs)**, contienen una descripción resumida de uno o más LSP. Son usados para mantener sincronizadas todas las LSDB.

  ○ ***Complete Sequence Number* PDUs (CSNPs),** contiene una lista completa de todos los LSP. Son enviados periódicamente en todos los enlaces para actualizar y sincronizar LSDB.

  ○ ***Partial Sequence Number* PDUs (PSNPs),** es enviado cuando se detecta que falta un LSP o la LSDB esta desactualizada en un segmento de acceso múltiple o también para indicar que se recibió la información en un segmento P2P.

f) Métricas IS-IS

La norma ISO 10589 especifica las siguientes métricas (una requerida y tres opcionales) para calcular la ruta más corta:

- **Métrica predeterminado o default,** esta métrica debe ser compatible y entendida por cada enrutador IS-IS.
- **Retardo o delay** (opcional) refleja el retardo de tránsito de una subred.
- **Gastos o expense** (opcional) refleja el costo de usar la subred.
- **Error,** (opcional) refleja la probabilidad de error de la subred, similar a la métrica de confiabilidad de IGRP / EIGRP.

g) Proceso de elección de rutas

Una vez que los PDU compartidos han creado la LSDB, el proceso de decisión utiliza esta información para calcular la mejor ruta utilizando el algoritmo SPF por separado para L1 y como para L2. Se toma en cuenta el número de LSP para evitar obtener un enrutamiento incorrecto por falta de información.

Las rutas se clasifican en L1 o L2, y también en internas o externas. Estas indican si la ruta pertenece a un destino dentro del dominio IS-IS o no. Sólo las rutas L2 pueden ser internas o externas, mientras que las rutas L1 son internas (se puede hacer que una ruta L1 sea externa mediante políticas especiales, pero debe hacerse con una buena justificación y con cuidado). En caso de tener múltiples rutas posibles hacia un destino, se prefiere una ruta L1 sobre una ruta L2. Dentro de cada nivel, se prefiere una ruta que admita las métricas opcionales sobre una ruta que solo admita la métrica predeterminada. Dentro de cada nivel de soporte de métricas, se prefiere la ruta con la métrica más baja. Si el proceso de decisión encuentra múltiples rutas de igual costo y nivel, se ingresan todas en la tabla de rutas. En la figura 2.44 se muestra una red con enrutamiento IS-IS.

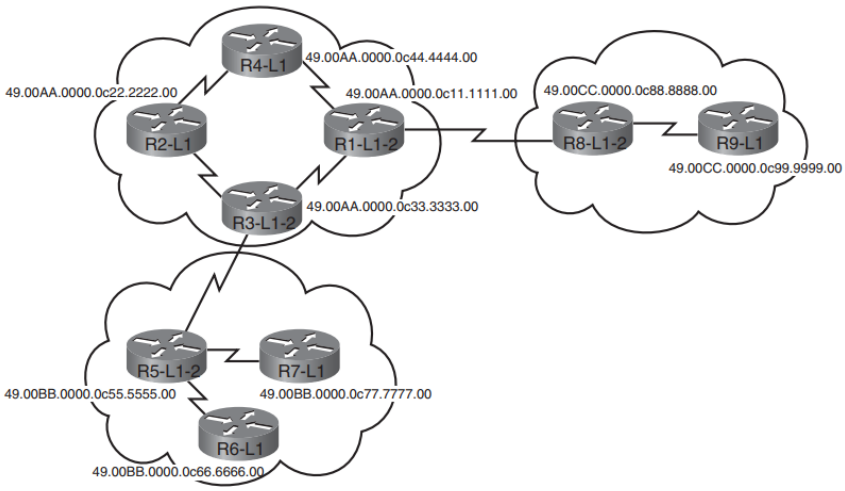


Figura 2.44 Enrutamiento con IS-IS. (Fuente: Ref. [19])

2.5.2. MPLS

Multiprotocol Label Switching (MPLS) es una tecnología que surgió a principios de este siglo, siendo definida en la RFC 3031, para mejorar el proceso de enrutamiento de

paquetes del protocolo IP utilizando únicamente etiquetas para proceso de conmutación. Esto aligera la conmutación de paquetes ya que el protocolo IP contiene mayor cantidad de información y su procesamiento toma mayor tiempo y recursos de hardware. Sin embargo, MPLS también añadió otras capacidades tales como:

- Capacidad de transportar cualquier tecnología de acceso (ATM, ethernet, frame relay).
- Elimina la necesidad de implementar BGP en el núcleo de la red.
- VPN's en el modelo Peer-to-peer.
- Flujos óptimos de tráfico.
- Ingeniería de tráfico.

a) Estructura básica de una red MPLS

La estructura típica de una red MPLS está compuesta por enrutadores conocidos como LSR (*Label Switching Router*) y pueden realizar las operaciones de inserción, intercambio o retiro de etiquetas. Los LSR se pueden clasificar en:

- **Ingress LSR (LSR de ingreso):** Recibe paquetes sin etiqueta desde enrutadores que no forman parte del dominio MPLS e inserta **(*push*)** una etiqueta.
- ***Egress* LSR (LSR de egreso):** Recibe paquetes etiquetados y retira **(*pop*)** las etiquetas antes de enviarlos a enrutadores que no forman parte del dominio MPLS.
- ***Intermediate* LSR (LSR intermedio):** Recibe y envía paquetes etiquetados realizando la operación de intercambio **(swap)** de etiquetas en el proceso.

En la figura 2.45 se muestran los elementos de una red MPLS.

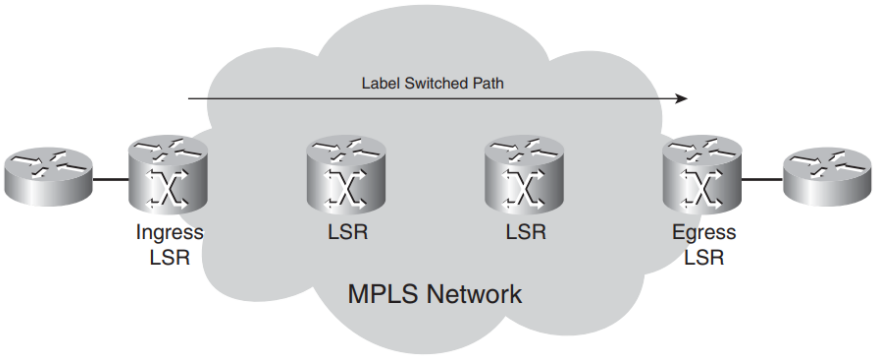


Figura 2.45 Elementos de una red MPLS. (Fuente: Ref. [20])

b) Arquitectura MPLS

La arquitectura MPLS está dividida en dos componentes principales:

- **Plano de Control (*Control Plane*):** Genera y mantiene la información de enrutamiento y las etiquetas utilizadas.

○ La tabla base de información de enrutamiento (*Routing Information Base*, RIB): es generada por los protocolos de ruteo IP y es utilizada para seleccionar las rutas. Para este fin es posible utilizar protocolos IGP tales como OSPF, IGRP, EIGRP, IS-IS, RIP y BGP.

o La tabla de información base de etiquetas (*Label Information Base*, LIB): es generada por los protocolos de distribución de etiquetas tales como LDP, BGP o RSVP. LIB es la base de datos utilizada por LDP donde se le asigna una etiqueta de significancia local que es mapeado a un prefijo IP y etiqueta que fueron aprendido desde un LSR vecino en sentido descendente.

- **Plano de Datos (*Data Plane*):** Encargado del reenvío de los paquetes IP y MPLS.

o La tabla base de información de reenvío (*Forwarding Information Base*, FIB): es obtenida de la RIB y es la base de datos utilizada para reenviar los paquetes IP. Un paquete con destino a una dirección IP será reenviado con una etiqueta si es que existe una etiqueta previamente asignada, de lo contrario será reenviado sin etiquetar.

o La tabla base de información de reenvío de etiquetas (*Label Forwarding Information Base*, LFIB): es derivada de la LIB y utilizada para reenviar los paquetes con etiqueta MPLS. La LFIB contiene las etiquetas locales (anunciadas previamente a los vecinos en sentido ascendente) que son asignadas a las etiquetas de siguiente salto que se recibieron de los vecinos en sentido descendente.

A continuación, en la figura 2.46 se muestra el funcionamiento de los componentes de la arquitectura MPLS en un enrutador.

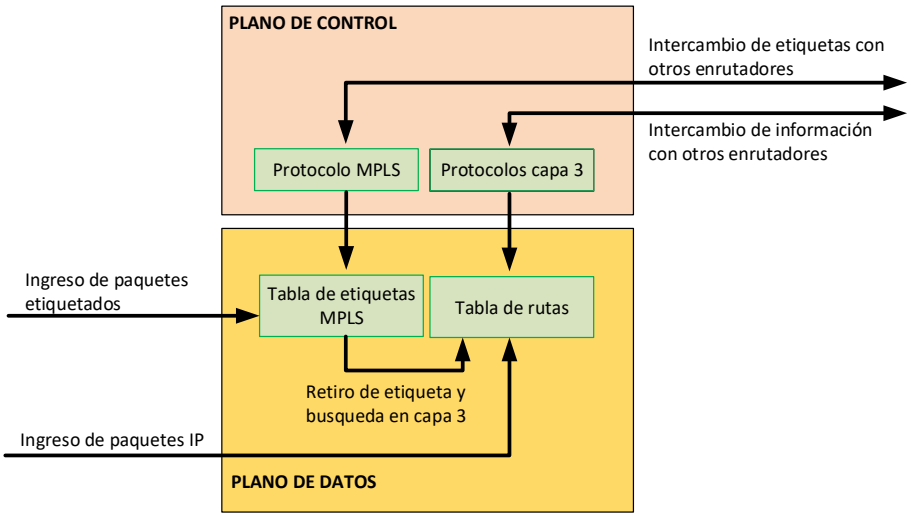


Figura 2.46 Funcionamiento de MPLS en un enrutador. (Fuente: Elab. Propia)

Las combinaciones de reenvío de paquetes en cualquiera de los LSR pertenecientes al dominio MPLS son las siguientes:

- Se recibe un paquete IP, se analiza la información de la IP destino y se reenvía como un paquete IP.
- Se recibe un paquete IP, se analiza la información de la IP destino y se reenvía luego de insertar una etiqueta MPLS.

- Se recibe un paquete que contiene una etiqueta MPLS se analiza la información de la etiqueta. La etiqueta es reemplazada por otra y el paquete es reenviado con la nueva etiqueta.
- Se recibe un paquete que contiene una etiqueta MPLS se analiza la información de la etiqueta. La etiqueta es retirada y el paquete es reenviado como un paquete IP.

c) Etiquetas MPLS

De acuerdo con la definición brindada por la RFC 3031, una etiqueta MPLS es un identificador significativo, corto, de longitud fija y local que se utiliza para identificar y representar una clase de equivalencia de reenvío (*Forwarding Equivalence Class*, FEC) a la cual pertenece un paquete. Una FEC es un grupo de paquetes IP con características similares y que se reenvían de la misma manera, por la misma ruta y con el mismo tratamiento.

- **Campos de una etiqueta,** las etiquetas MPLS tienen 4 bytes de longitud y contienen 4 campos de acuerdo con lo definido en la RFC 3032.

  ○ **Etiqueta (Label):** Campo de 20 bits que indica el valor de la etiqueta asignada.

  ○ **Experimental (Exp):** 3-bit, de uso no definido en la RFC 3032. Es utilizado usualmente como un campo para indicar el nivel de calidad de servicio (*class of service*).

  ○ **Indicador de Apilamiento (1-bit Botton-of-Stack)**: MPLS soporta el anidamiento de múltiples etiquetas. Este campo tiene 1 bit de longitud que se establece en 1 cuando se trata de la última entrada de la pila de etiquetas (es decir, para la parte inferior de la pila) y 0 para todas las demás entradas de la pila de etiquetas.

  ○ **TTL (time to live).** Campo de 8-bit que indica cuantos saltos puede pasar un paquete antes de ser descartado.

En la figura 2.47 se muestran los campos de una etiqueta MPLS.

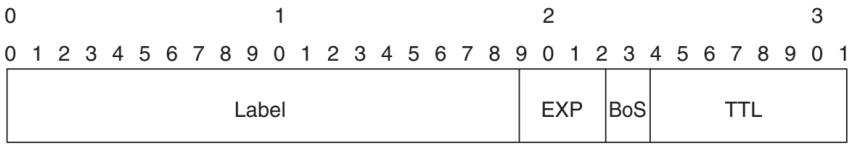


Figura 2.47 Campos de una etiqueta MPLS. (Fuente: Ref. [20])

- **Apilamiento de etiquetas**

Para algunas aplicaciones, tales como VPN basadas en MPLS e ingeniería de tráfico, es necesario utilizar más de una etiqueta encima del paquete para enrutar un paquete a través de la red MPLS. Esto se hace empaquetando las etiquetas en una pila (stacking). La primera etiqueta en la pila se llama la etiqueta superior, y la última etiqueta se llama la etiqueta inferior. En el medio, puede tener cualquier número de etiquetas. En la figura 2.48 se muestra cómo se ubican las etiquetas MPLS cuando son apiladas.

Figura 2.48 Apilamiento o stacking de etiquetas MPLS. (Fuente: Ref. [20])

- **Ubicación de las etiquetas**

En general, las etiquetas MPLS (ya sea una sola etiqueta o de una pila de etiquetas) se insertan entre entre el encabezado de IP (capa 3) y el encabezado de Control de enlace lógico (LLC) de capa 2, utilizando un identificador de protocolo que indica que el protocolo transportado es MPLS (labeled IP multicast): PID=0x8848. En la figura 2.49 se muestra la ubicación de una etiqueta MPLS dentro de un paquete.

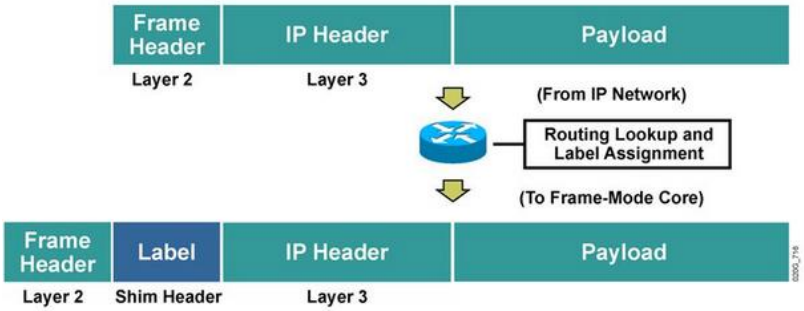


Figura 2.49 Ubicación de la etiqueta MPLS dentro de un paquete (Fuente: Ref. [21])

- **Etiquetas reservadas:** Las etiquetas del 0 al 15 son etiquetas reservadas. Un LSR no puede usarlos en el caso normal para reenviar paquetes ya que tienen una función específica asignada para cada una.

○ **La etiqueta NULL implícita (*Implicit NULL Label*)** con un valor de 3, es asignada por el LSR de egreso para que el penúltimo LSR realice la operación de retiro de etiqueta, (en lugar del último) optimizando el proceso de reenvío. Este procedimiento es denominado PHP (*penultimate hop popping*).

○ **Etiqueta NULL explícita o *Explicit NULL label*** con un valor de 0. El penúltimo LSR reemplaza la etiqueta por una con valor 0 pero manteniendo los otros campos intactos. De esta manera se conserva el tratamiento de QoS hasta el último LSR.

○ **Etiqueta de Alerta del enrutador o *Router Alert label*,** con un valor de 1. Alerta al LSR de que el paquete necesita un análisis más detallado. Por lo tanto, el paquete no se reenvía en hardware, sino que se analiza mediante un proceso de software.

○ **Etiqueta de alerta OAM o *OAM Alert Label*,** con un valor de 14, también conocido como *Operation and Maintenance* (OAM) según lo descrito en la Recomendación UIT-T

Y.1711 y RFC 3429. Se usa básicamente para la detección de fallas, la localización y el monitoreo del rendimiento.

d) Forward Equivalence Class

Una Clase de equivalencia de reenvío o *Forward Equivalence Class* (FEC) es un grupo o flujo de paquetes que se reenvían a lo largo de la misma ruta y se tratan de la misma manera al momento de reenviarse. Todos los paquetes que pertenecen a la misma FEC tienen la misma etiqueta. Sin embargo, no todos los paquetes que tienen la misma etiqueta pertenecen a la misma FEC, ya que sus valores de EXP pueden diferir (QoS diferente) y por tanto pertenecer a una FEC diferente. El enrutador que decide qué paquetes pertenece a qué FEC es el LSR de ingreso.

e) Label Switched Path

Una ruta de conmutación de etiquetas o *Label Switched Path* (LSP) es la secuencia de LSR que llevan un paquete etiquetado a través de una red MPLS o parte de una red MPLS. Básicamente, el LSP es la ruta a través de la red MPLS o una parte de ella que toman los paquetes. Los LSP son unidireccionales por lo cual es necesario crear otro LSP para el tráfico de retorno de una FEC en particular.

f) Tratamiento de los paquetes en una red MPLS

Cuando un paquete IP llega a borde de un dominio MPLS, el *Ingress* LSR analiza el paquete para ver qué ruta MPLS debe seguir, y coloca la etiqueta correspondiente. Una vez dentro de la red MPLS, esta etiqueta es utilizada para reenviar el paquete a través de los LSR intermedios hasta llegar al otro extremo de la red. En este punto la etiqueta ya ha cumplido su propósito y es retirada para descubrir el paquete IP y enviarlo al siguiente enrutador como se muestra en la figura 2.50.

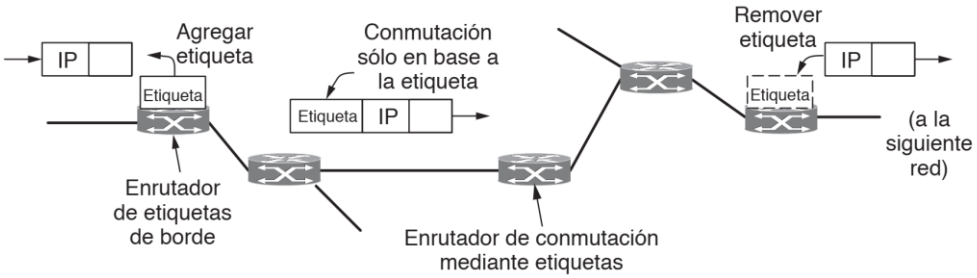


Figura 2.50 Proceso de reenvío de un paquete en una red MPLS. (Fuente: Ref. [7])

2.5.3. LDP

El protocolo LDP es el encargado de proporcionar los medios para que los LSR intercambien las etiquetas MPLS asignadas a un LSP asociado a una FEC. El protocolo LDP permite el descubrimiento de vecinos, el establecimiento y mantenimiento de sesiones LDP, el anuncio y limpieza de etiquetas MPLS.

a) Descubrimiento de Vecinos:

Los mecanismos de descubrimiento de vecinos LDP hace uso de los mensajes *Hello* que puede variar dependiendo del tipo de adyacencia.

- **Mecanismo básico de descubrimiento:** Utilizado cuando los LSR están directamente conectados. Los mensajes *Hello* de LDP son enviados utilizando como destino a la IP multicast 224.0.0.2 y puerto destino (UDP y TCP) 646. Un identificador LDP (LDP ID) de 6 bytes es enviado indicando un TLV que identifica el enrutador (primeros cuatro bytes) y el espacio de la etiqueta (últimos dos bytes). En la figura 2.51 se muestra el contenido de los mensajes *Hello* durante el descubrimiento de vecinos.

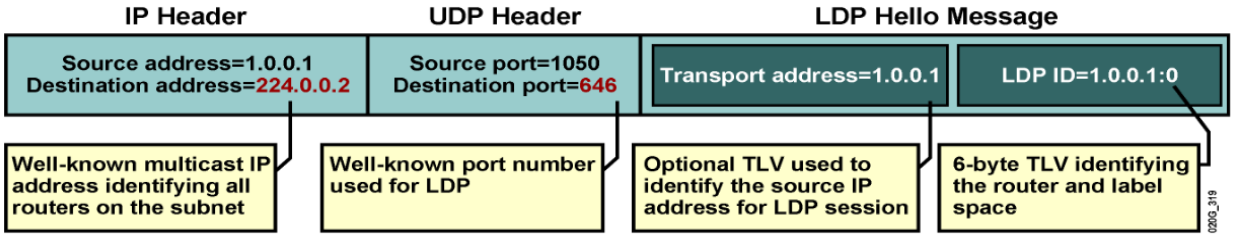


Figura 2.51 Contenido de los mensajes LDP *Hello* (Fuente: Ref. [21])

- **Mecanismo Extendido de descubrimiento:** Utilizado cuando los LSR no se encuentran directamente conectados. Los mensajes *Hello* son dirigidos como paquetes UDP unicast al LSR con el cual se desea establecer la sesión (LDP targeted Hello).

b) Proceso de Establecimiento de una sesión LDP:

1. **Establecer una sesión TCP:** Ambos LSR identifican que LSR debe iniciar la conexión (dirección IP de transporte más alta).
2. **Intercambio inicial de mensajes de Inicialización:** El LSR ganador del paso 1 enviará un mensaje de Inicialización para negociar los parámetros a utilizar en la sesión LDP. Si el otro LSR acepta los parámetros también enviará un mensaje de Inicialización, sino deberá enviar un mensaje de Notificación para detener el proceso. Junto con el envío del mensaje de inicialización el LSR remoto deberá enviar también un *Keepalive*
3. **Intercambio inicial de mensajes *Keepalive*:** Si el primer LSR acepta la respuesta al mensaje de inicialización también responderá con un mensaje de *Keepalive* o sino enviará una notificación para detener el proceso.
4. Ambos LSR intercambiaran etiquetas para todos los prefijos.

En la figura 2.52 se muestra el proceso de establecimiento de una sesión LDP:

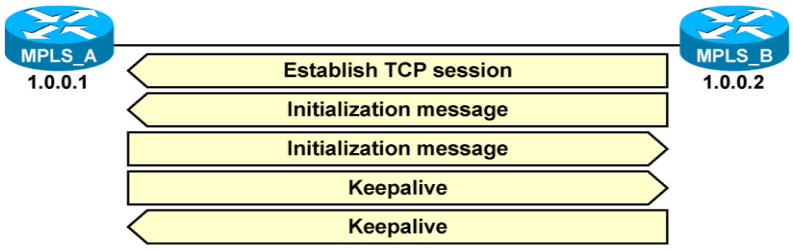


Figura 2.52 Establecimiento de una sesión LDP (Fuente: Ref. [21])

c) Modos de trabajo de LDP

Un LSR puede usar diferentes modos al distribuir y mapear etiquetas a un FEC dependiendo del modo de trabajo de LDP utilizado y que son explicados en los siguientes párrafos:

- **Modos de distribución de etiquetas,** se tienen dos modos:

1. **Distribución de etiquetas en sentido descendente (*Downstream-on-Demand*, DoD)**: Un LSR distribuye etiquetas a un FEC específico solo después de haber recibido mensajes de solicitud de etiquetas de su LSR vecino ascendente.
2. **Distribución de etiquetas no solicitadas en sentido descendente (*Unsolicited Downstream*, UD) mode**: Un LSR distribuye etiquetas a un FEC específico sin tener que recibir mensajes de solicitud de etiquetas desde otro LSR.

- **Modos de retención de etiqueta**, se refieren a la forma en que los LSR procesan las etiquetas recibidas antes de ser utilizadas. Se tienen dos modos para retener etiquetas:

1. **Retención de liberal (*Liberal Label Retention mode*, LLR):** El LSR retiene en su LIB todas las etiquetas recibidas de los LSR vecinos independientemente de si se trata del siguiente salto. La LFIB solo utiliza las etiquetas que corresponden al LSR del siguiente salto. Esto ayuda a actualizar rápidamente la LFIB en caso de caída de algún enlace o equipo ya que la información se encuentra disponible en la LIB.
2. **Retención conservadora (*Conservative Label Retention*, CLR):** El LSR retiene en su LIB únicamente los mapeos de etiquetas recibidos del LSR vecino que corresponde al siguiente salto, demanda menor cantidad de recursos.

- **Modos de control para el establecimiento de un LSP**

Estos modos se refieren a la forma en que se asignan las etiquetas en un LSR durante el proceso de establecimiento del LSP correspondiente a una FEC. Para esto, los LSR tienen dos maneras:

1. **LSP independiente (*independent* LSP)**: El LSR puede realizar la asignación de una etiqueta para un FEC independientemente de los otros LSR e informarla a otros LSR vecinos ascendentes. Por lo general, esto significa que el prefijo para el FEC está en su tabla de enrutamiento.

2. **LSP ordenado (*ordered* LSP)**: En el modo de control LSP ordenado, un LSR solo asigna la etiqueta para un FEC si reconoce que es el LSR de egreso para el FEC o si el LSR ha recibido una etiqueta desde el LSR de próximo salto. La desventaja es que algunos LSR comienzan a etiquetar los paquetes antes de que el LSP completo se configure de extremo a extremo y por tanto podría reenviarse incorrectamente.

d) Proceso de asignación y distribución de etiquetas:

El proceso de asignación y distribución de etiquetas sigue los siguientes pasos:

1. Intercambio de información de enrutamiento (a través de OSPF, IS-IS, EIGRP, etc.).
2. Generación de etiquetas locales a cada destino IP que se encuentra en la tabla de enrutamiento principal y se almacena en la tabla LIB.
3. Propagación de etiquetas locales a enrutadores adyacentes

En la figura 2.53 se muestra cómo se asignan y propagan las etiquetas MPLS entre dos enrutadores PE.

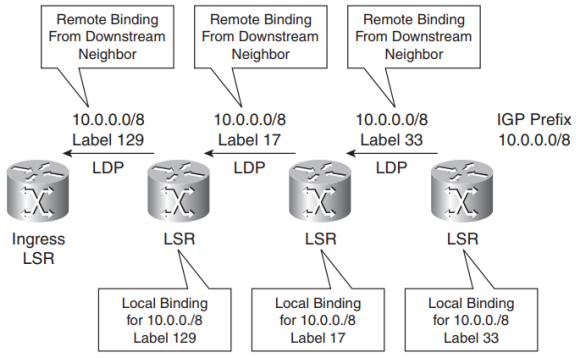


Figura 2.53 Asignación y propagación de etiquetas en LDP (Fuente: Ref. [20])

2.5.4. VPN MPLS

a) VPN

Una red privada virtual o Virtual Private Network (VPN) es una red que provee conectividad entre los múltiples sitios de un cliente utilizando una infraestructura compartida, pero con las mismas políticas de acceso o seguridad que en una red privada. Existen dos modelos para llevar esto a cabo:

- **Modelo de superposición (*overlay model*),** el proveedor de servicios proporciona un servicio de enlaces punto a punto o circuitos virtuales a través de su red. Los enrutadores del proveedor de servicios se mantienen aislados pues nunca ven las rutas de los clientes. Estos servicios pueden ser de Capa 1, 2 o incluso 3. Ej. en capa 1: Enlaces dedicados E1, E3, SONET y SDH; capa 2: circuitos virtuales X.25 o Frame Relay; capa 3: túneles GRE. En la figura 2.54 se muestra un ejemplo de VPN *overlay* con servicios de capa 2 utilizando Frame Relay.

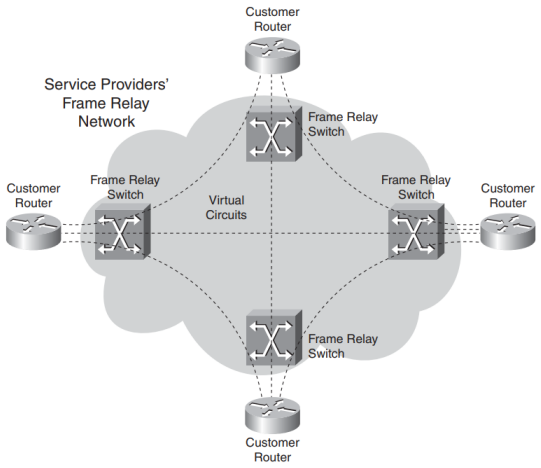


Figura 2.54 Ejemplo de red privada virtual overlay con Frame-Relay (Fuente: Ref. [20])

- **Modelo de igual a igual (*peer-to-peer model***), el proveedor de servicios transporta los datos del cliente a través de la red, pero también participa en el enrutamiento. En otras palabras, se forman adyacencias del protocolo de enrutamiento entre el cliente y el proveedor de servicios. En la figura 2.55 se muestra un ejemplo de vpn peer-to-peer.

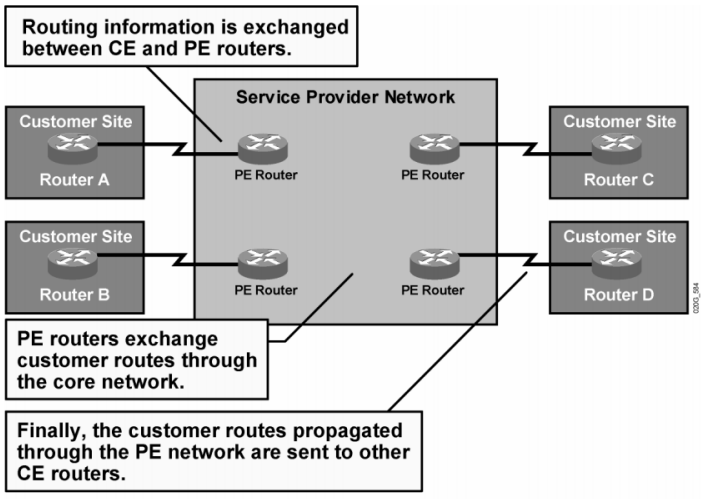


Figura 2.55 Red privada virtual peer-to-peer (Fuente: Ref. [21])

b) Modelo VPN MPLS

VPN MPLS combina los beneficios del modelo de superposición (seguridad y el aislamiento) pero añade simplicidad al enrutamiento del modelo igual a igual. En el modelo de VPN MPLS se pueden encontrar los siguientes elementos:

- Enrutador de borde del proveedor (*Provider Edge router*, PE), con conexión directa en capa 3 al enrutador CE del cliente. Los PE son LSR de ingreso o egreso.
- Enrutador del proveedor (*Provider router*, P), sin conexión directa con ningún enrutador CE del cliente. Los PE son LSR intermedios.
- Enrutador de borde del cliente (*Customer Edge router*, CE), con conexión directa en capa 3 al enrutador PE del proveedor.

En la figura 2.56 se muestra un diagrama con los elementos explicados anteriormente para las VPN MPLS de dos clientes distintos.

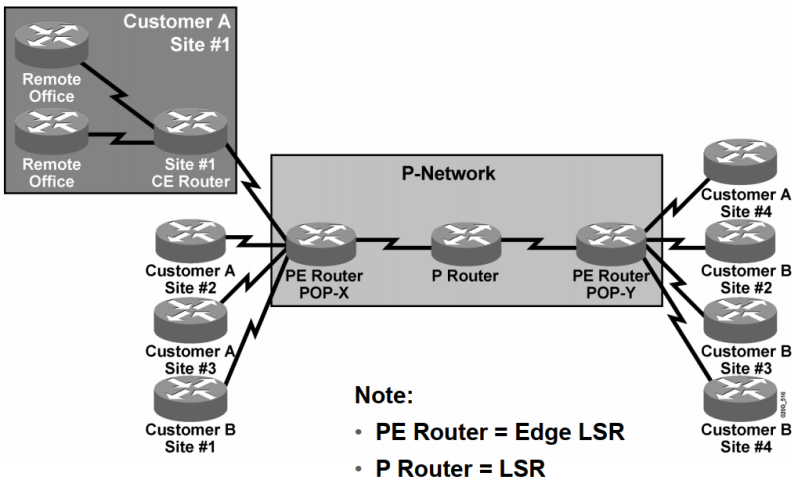


Figura 2.56 Elementos de una VPN MPLS (Fuente: Ref. [21])

c) Arquitectura de una VPN MPLS

- ***Virtual Routing Forwarding*** **(Instancia virtual de ruteo y envío)**, es el conjunto de una tabla de rutas, interfaces y parámetros que mantienen la independencia de una VPN en un PE. Según la RFC 4364: Cada PE mantiene tablas de reenvío separadas, siendo una de ellas conocida como la "tabla de reenvío global" y las otras como "tablas de enrutamiento y reenvío de VPN" o "VRFs". En la figura 2.57 se representa un enrutador PE con dos tablas de enrutamiento y una tabla global.

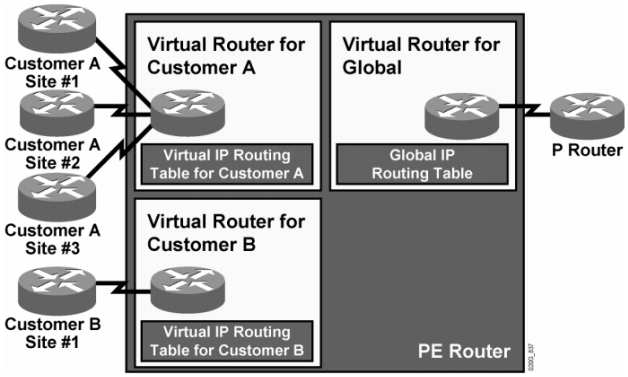


Figura 2.57 Tablas de reenvío en un PE: VRF's y tabla global (Fuente: Ref. [21])

- ***Route Distinguisher*** **(RD),** es un número único local que identifica a los prefijos pertenecientes a la VPN de un cliente de manera que los prefijos de varios clientes no se traslapen entre ellos. Un RD es un número de 64-bits que puede tener dos formatos:

- **AS-número: número**, donde AS-número es el número de sistema autónomo (AS) con un valor de 2 bytes en el rango de 1-65535, y número es un valor de 4 bytes.

- **Dirección-IP: número**, donde dirección-IP es una dirección IP con un valor de 4 bytes (usualmente el router-id de LSR) y número es un valor de 2 bytes.

- **Prefijos VPNv4,** es la combinación del RD con el prefijo IPv4 resultando en una dirección de 96 bits. Por ejemplo, para el prefijo IPv4 10.1.1.0/24 y un RD 1:1 (primer formato) tendríamos como dirección vpnv4: 1:1:10.1.1.0/24. Si se usara como RD 192.168.1.1:1(segundo formato) tendríamos: 192.168.1.1:1:10.1.1.0/24.
- ***Router Target*** **(RT)**, es una comunidad extendida de BGP que indica qué rutas deben importarse desde MP-BGP a una VRF bajo estas operaciones:

1. **Exportación de RT (RT *export*),** la ruta vpnv4 será anunciada en BGP luego de añadirle el RT en el PE de ingreso como comunidad extendida de BGP.
2. **Importar un RT (RT *import*),** el PE de egreso importa la ruta vpnv4 recibida desde MP-BGP si coincide con una de las comunidades extendida configuradas en el PE y la añade a la tabla de enrutamiento de la VRF como una ruta IPv4.

En la figura 2.58 se muestra cómo se utilizan los RT en una MPLS VPN.

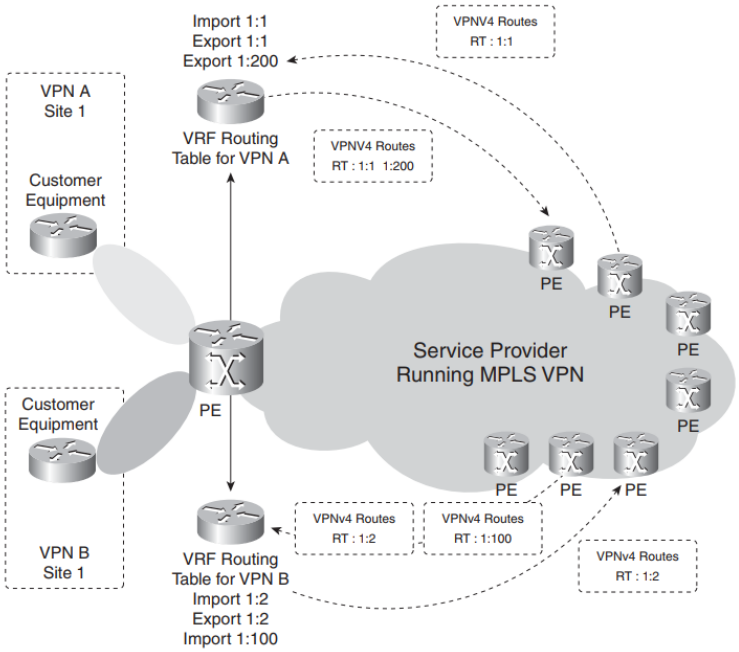


Figura 2.58 Manejo de RD, RT en MPLS VPN (Fuente: Ref. [20])

- **MP-BGP,** se utiliza el protocolo BGP con su extensión definida en la RFC 4760 para soportar múltiples protocolos. MP-BGP añade dos atributos: NLRI multiprotocolo accesible (MP_REACH_NLRI) y NLRI multiprotocolo inalcanzable (MP_UNREACH_NLRI). El primero se usa para llevar el conjunto de destinos accesibles junto con la información del siguiente salto que se usará para reenviar a estos destinos. Mientras que el segundo se utiliza para llevar el conjunto de destinos inalcanzables. Ambos atributos son opcionales y no transitivos, de esta manera que si un enrutador no admite estas capacidades ignora la información contenida y no se envía a otros enrutadores BGP. Los atributos MP_REACH_NLRI y MP_UNREACH_NLRI tienen dos campos: el Identificador de familia

de direcciones o *Address Family Identifier* (AFI) de 2 bytes de longitud y el Identificador de familia de direcciones subsiguientes o *Subsequent Address Family Identifier* (SAFI) de 1 byte de longitud. Juntos, describen exactamente qué tipos de rutas lleva BGP.

Los valores de AFI y SAFI utilizados en MPLS VPN para IPv4 son 1 y 128 respectivamente. En las tablas 2.5 y 2.6 se visualizan algunos valores de AFI y SAFI para distintos protocolos.

Tabla 2.5. Algunos de los números AFI y sus descripciones. (Fuente: Elab. propia)

AFI	Descripción
0	Reservado
1	IP (versión 4)
2	IPv6
11	IPX
12	Apple Talk

Tabla 2.6 Algunos de los números SAFI y sus descripciones. (Fuente: Elab. propia)

SAFI	Descripción
1	NLRI para Unicast Forwading
2	NLRI para Multicast Forwarding
3	NLRI para Unicast y Multicast Forwarding
4	NLRI con etiquetas MPLS
128	NLRI para direcciones MPLS VPN etiquetadas

MP-BGP distribuye las rutas VPN-IPv4 entre los PE, correspondientes a los extremos de una VPN MPLS, mediante una conexión iBGP entre ellas. En la figura 2.59 se muestra como las rutas son intercambiadas entre los enrutadores CE y PE cuando utiliza una MPLS VPN. Opcionalmente también se puede considerar la utilización de reflectores de ruta (router reflectors, RR) de BGP.

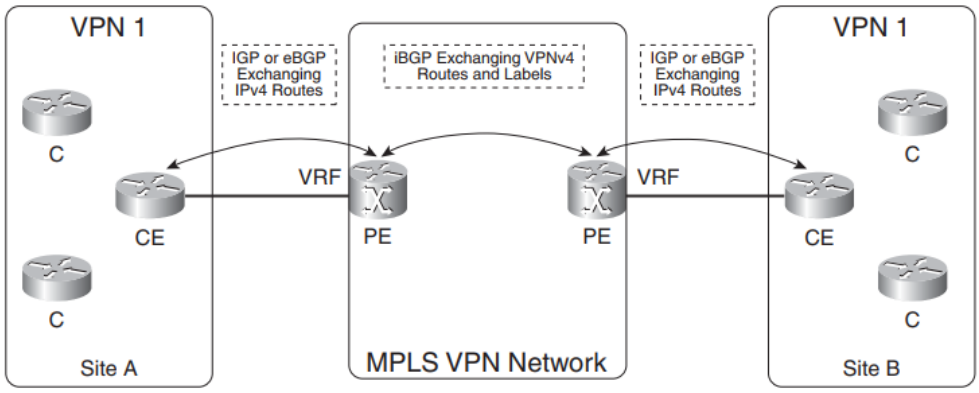


Figura 2.59 Intercambio de rutas en una MPLS VPN (Fuente: Ref. [20])

d) Proceso de propagación de rutas en una VPN MPLS

La propagación de prefijos vpnv4 en una VPN MPLS son los siguientes:

1. El enrutador PE de ingreso recibe los prefijos IP desde el CE a través de un protocolo de enrutamiento PE-CE (Ej. eBGP, OSPF).
2. Los prefijos son colocados en la tabla de enrutamiento de la VRF correspondiente.
3. Se añade el RD a los prefijos para convertirlos en rutas vpnv4 y se redistribuyen en MP-BGP. Adicionalmente se añaden los RT de exportación.
4. MP-BGP se encarga de distribuir estas rutas vpnv4 a todos los enrutadores PE.
5. El enrutador PE de salida revisa que los prefijos coincidan con el RT de importación y de ser así son aceptados. El RD es retirado del prefijo vpnv4 quedando sólo el prefijo IP.
6. Se colocan los prefijos en la tabla de enrutamiento de la VRF.
7. Finalmente, las rutas son anunciadas en el PE de salida hacia el CE a través de protocolo PE-CE.

La figura 2.60 muestra el proceso de propagación de los prefijos VPNv4 en una VPN MPLS.

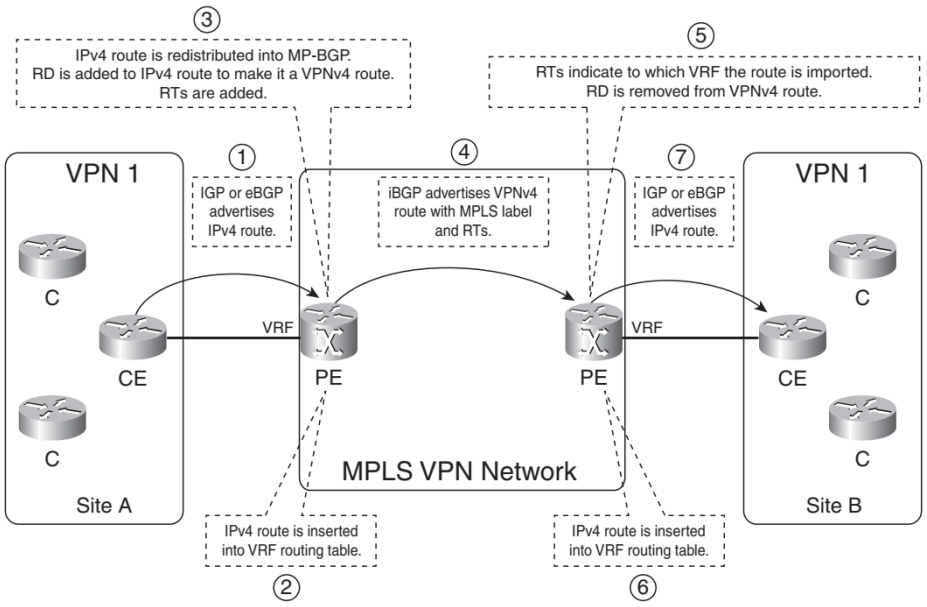


Figura 2.60 Propagación de prefijos VPNv4 en una VPN MPLS (Fuente: Ref. [20])

e) Proceso de reenvío de paquetes en una VPN MPLS

Durante el proceso de reenvío de paquetes, el paquete ingresa al enrutador PE en una interfaz de la VRF como un paquete IPv4. Esta es reenviada a través de la red MPLS con dos etiquetas: la etiqueta superior del IGP (distribuida por LDP o RSVP para TE entre todos los P y PE, salto por salto), y la etiqueta inferior de VPN (distribuida por BGP). Los enrutadores P reenvían el paquete utilizando la etiqueta superior que es intercambiada en cada salto. Las etiquetas son eliminadas en el enrutador de egreso PE utilizando la etiqueta inferior para identificar la VRF correspondiente y el paquete se reenvía como un paquete IPv4 en la interfaz de VRF hacia el enrutador CE. La figura 2.61 muestra el proceso de

reenvío de paquetes en una VPN MPLS en el cual se puede apreciar que las etiquetas MPLS son utilizadas únicamente dentro del dominio MPLS.

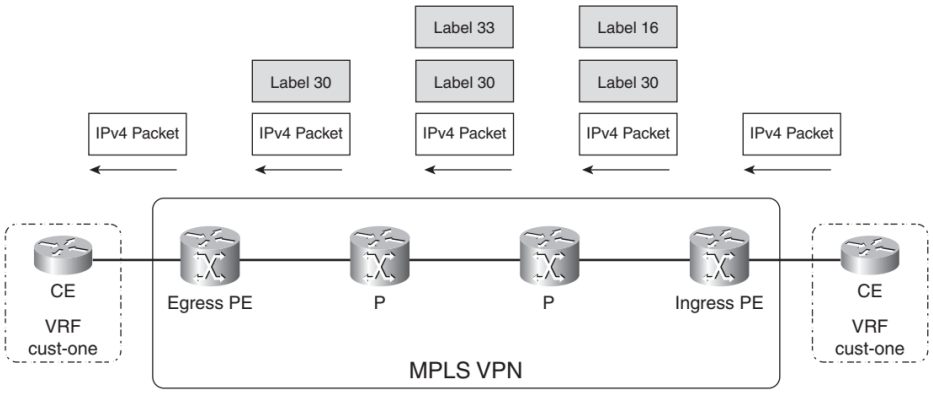


Figura 2.61 Reenvío de paquetes en la red VPN MPLS (Fuente: Ref. [20])

2.5.5. Protocolos de enrutamiento PE-CE

Un protocolo de enrutamiento PE-CE es necesario para que un PE pueda aprender los prefijos desde enviados por el CE de un cliente y luego redistribuirlos en MP-BGP, para ser anunciados a través de una VPN MPLS. A continuación, se indican brevemente los protocolos más utilizados:

a) Enrutamiento Estático

Es el más sencillo de configurar, pero complicado de mantener en topologías complejas durante la fase de operación.

b) RIP

Es un protocolo de enrutamiento dinámico del tipo vector distancia en el que la métrica de una ruta está determinada por cantidad de saltos hasta el destino. Su uso está limitado a 15 saltos como máximo.

c) OSPF

OSPF es utilizado como protocolo PE-CE añadiendo algunas reglas al modelo clásico.

- Se introduce un tercer nivel de jerarquía: VPN *superbackbone*, que se suma a los dos niveles de jerarquía (un área *backbone* 0 y N x áreas *non-backbone*).
- Los enrutadores PE se anuncian como enrutadores de borde de área. El *superbackbone* aparece como otra área para los enrutadores CE.
- Las rutas redistribuidas en MP-BGP aparecerán como rutas inter-área en los sitios remotos si la ruta original era una ruta interna o inter-área, y como rutas externas si la ruta original también lo era. Se introduce un Identificador de Dominio OSPF (OSPF *Domain* ID) como opcional para preservar los tipos de ruta de OSPF, caso contrario se aplican las reglas de una redistribución tradicional.

- Los siguientes atributos de OSPF son transportados directamente en MP-BGP a través de comunidades extendidas de forma que la ruta puede reconstruirse en el PE de salida: Tipo de Ruta OSPF, número de área, identificador de enrutador, Identificador de Dominio y tipo de métrica de OSPF.

La figura 2.62 muestra el proceso descrito anteriormente en dos condiciones: a) identificadores de dominio iguales donde el tipo de ruta es conservado (el PE de egreso es el ABR que genera un LSA tipo 3) y b) con identificadores de dominio diferentes cambiando el tipo de ruta cambia a externo (el PE de salida genera un LSA tipo 5).

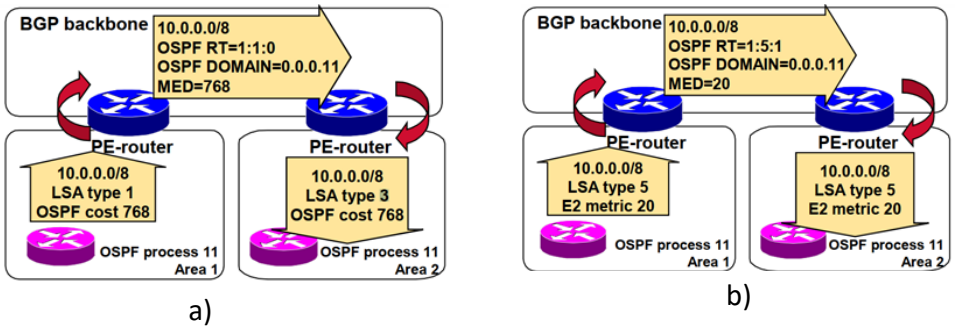


Figura 2.62 Propagación de rutas en protocolo PE-CE OSPF a) mismo Domain ID b) Domain ID diferente (Fuente: Ref. [21])

Finalmente es posible utilizar un enlace-simulado (*sham-link*) cuando dos sitios pertenecen a la misma área y mantienen un enlace de respaldo (*backdoor*), pero de menor capacidad que los enlaces hacia la MPLS. Bajo las reglas normales de OSPF, el enlace de menor capacidad será preferido puesto que la ruta aprendida por ese enlace es de tipo intra-área mientras que la aprendida por la MPLS es de tipo inter-área. Con el enlace simulado se establece un enlace lógico intra-área a través del *superbackbone* donde los dos PE serán los puntos finales y los enlaces MPLS serán elegidos como preferentes. En la figura 2.63 se muestra cómo se utiliza un enlace-simulado para optimizar el flujo de tráfico prefiriendo enviar el tráfico a través de la red MPLS en lugar del enlace directo de baja velocidad.

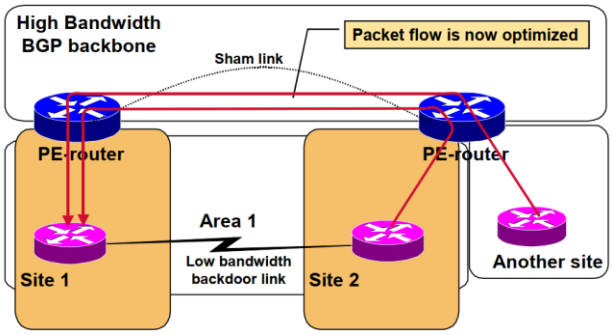


Figura 2.63 Enlace simulado sham-link OSPF (Fuente: Ref. [21])

d) BGP

Usar BGP como protocolo PE-CE tiene la ventaja de que no es necesario realizar una redistribución de protocolos de enrutamiento en el PE para anunciar los prefijos vía vpnv4, sin embargo, hay que tener en cuenta el mecanismo de prevención de bucles de *as-path*. Si cada uno de los CE del cliente tiene números diferentes de AS, BGP podrán operar sin problemas, pero si el cliente tiene el mismo número de AS en diferentes sitios, el PE de salida deberá reemplazar el número de AS del cliente con el suyo antes de enviarlo al CE destino, para prevenir que este descarte la ruta. Esto es conocido como *as-override*.

En el ejemplo de la figura 2.64: a) el CE rechaza la ruta enviada por PE de salida por ver su AS en el as-path b) El PE reemplaza el as-path a [65115] en lugar de [65213], ahora el CE procede a aceptar esta ruta porque ya no ve su propio AS en el as-path.

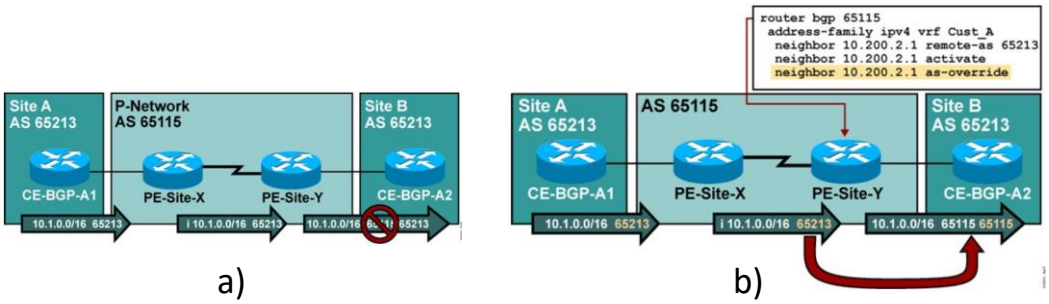


Figura 2.64 BGP como protocolo PE-CE a) sin as-override
b) con as-override (Fuente: Ref. [21])

2.5.6. FHRP

Los protocolos de redundancia de primer salto (*First Hop Redundancy Protocol*, FHRP) proteger la puerta de enlace de un segmento de red brindando la posibilidad de que dos o más enrutadores proporcionen una sola dirección IP virtual como puerta de enlace. A continuación, se explican a los protocolos HSRP y VRRP puesto que son los protocolos FHRP más utilizados.

a) HSRP

Desarrollado por Cisco, usa un mecanismo basado en prioridades (se elige al enrutador con el valor más alto) para determinar qué dispositivo HSRP tendrá el rol de activo y será el encargado de enviar el tráfico dirigido a la IP virtual. Además, utiliza una MAC virtual para terminar de resolver los mensajes de ARP de los hosts finales. Para configurar un dispositivo como activo, se le asigna una prioridad más alta que los otros dispositivos. La prioridad por defecto es 100.

- **Estados de HSRP,** los enrutadores tienen los siguientes estados en HSRP.
  - **Inicial (*Initial*):** Este es el estado al inicio. En este estado HSRP no se ejecuta.

○ **Aprendizaje (*Learn*)**: el enrutador no ha determinado la dirección IP virtual y aún no ha visto un mensaje *Hello* del enrutador activo.

○ **Escucha (*Listen*):** el enrutador conoce la dirección IP virtual, pero no es el enrutador activo ni standby. Además, escucha los mensajes *Hello* de otros enrutadores.

○ **Hablando (Speak):** el enrutador envía mensajes *Hello* periódicamente y participa activamente en la elección del enrutador activo y/o *standby*.

○ **En espera (*Standby*):** el enrutador es un candidato para convertirse en el siguiente enrutador activo y envía mensajes *Hello* periódicamente.

○ **Activo (*Active*):** el enrutador activo reenvía los paquetes que se envían a la dirección MAC virtual del grupo. El enrutador envía mensajes de saludo periódicos.

En la figura 2.65 se muestra un grupo de enrutadores con HSRP que son utilizados como puerta de enlace para los hosts finales.

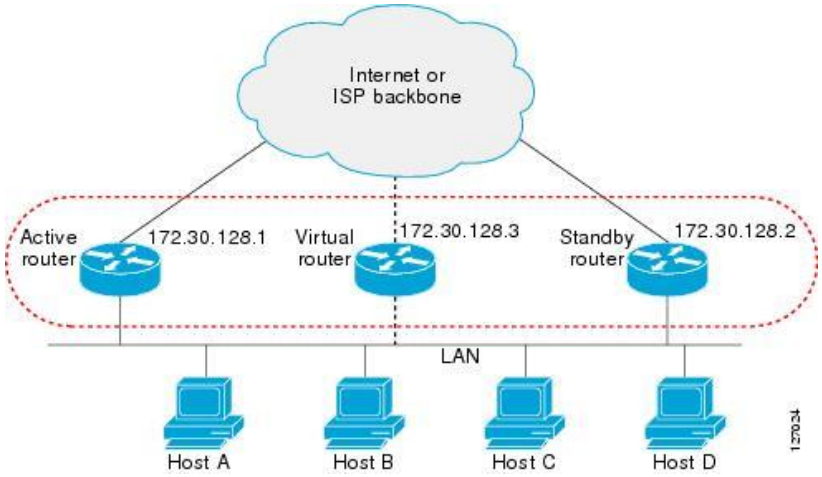


Figura 2.65 Componentes de HSRP. (Fuente: Ref. [22])

- **Versiones,** HSRP tiene dos versiones con las siguientes características:

○ **HSRP versión 1:**

✓ Los mensajes *Hello*, enviados por el enrutador activo con destino a la IP multicast 224.0.0.2, a un intervalo de 3 segundos por defecto y se declaran como muertos a los 10 segundos.

✓ La prioridad más alta es 255. (predeterminado 100).

✓ Se acepta hasta 255 grupos HSRP por puerto.

✓ La MAC virtual es 0000. 0C07.ACxx, donde xx es el grupo HSRP en hexadecimal.

✓ La dirección IP virtual debe estar en la misma subred que las interfaces y diferente de cualquier dirección IP de otro enrutador.

✓ Admite la autenticación de texto claro y MD5.

○ **HSRP versión 2:**

Añade las siguientes características:

✓ Valores de temporizador de milisegundos.

✓ Usa la IP multicast destino 224.0.0.102 y el rango de dirección MAC 0000. 0C9F.F000-0000.0C9F.FFFF.

✓ Expande el rango de números de grupo de 0 a 4095.

✓ Provee soporte para IPv6.

b) VRRP

El Protocolo de redundancia de enrutador virtual o *Virtual Router Redundancy Protocol* (VRRP) está definido por IETF en la RFC 5798 y permite que un grupo de enrutadores forme un solo enrutador virtual con su correspondiente IP y MAC virtuales, pero a diferencia de HSRP es *multivendor*. VRRP tiene las siguientes características:

✓ Cada virtual *router*, representa un grupo de enrutadores que es identificado a través de un grupo VRRP. Soporta hasta 255 grupos.

✓ VRRP elige al enrutador con la prioridad más alta como como el enrutador virtual maestro. El enrutador virtual maestro puede tener la misma dirección IP del grupo de enrutadores virtuales.

✓ Los enrutadores que no tienen el rol de master funcionan como enrutadores de respaldo (backup). Varios enrutadores pueden funcionar como enrutadores de respaldo.

✓ VRRP tiene la opción de *preemption* activada por defecto, así un enrutador master que fue reiniciado recuperará el rol después de terminar de *bootear*.

✓ Utiliza la IP multicast destino 224.0.0.18 y una dirección MAC virtual multicast 0000.5E00.01xx, donde xx es el número de grupo VRRP hexadecimal.

En la figura 2.66 se muestra un grupo de enrutadores con VRRP que son utilizados como puerta de enlace para los hosts finales.

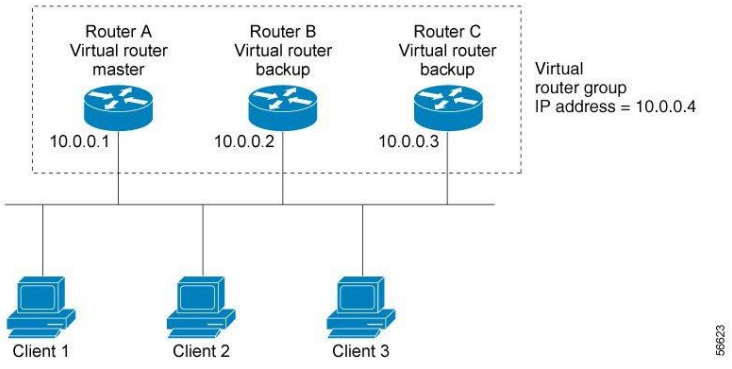


Figura 2.66 Componentes de VRRP. (Fuente: Ref. [22])

2.6. Mecanismos de Calidad de Servicio

Los mecanismos de calidad de servicio (QoS) son entendidos como el conjunto de tecnologías utilizadas en una red para asegurar que el rendimiento de esta cubra los requerimientos mínimos ancho de banda, variaciones de latencia (*jitter*) y latencia incluso

cuando la red se encuentre congestionada. Los mecanismos conocidos para brindar QoS son:

2.6.1. Mejor Esfuerzo (*Best-Effort*)

No se utiliza ningún tratamiento para diferenciar o priorizar ninguno de los paquetes, sino que son tratados al mejor esfuerzo.

2.6.2. Servicios Integrados (IntServ)

IntServ es definido por la IETF y utiliza el protocolo RSVP para señalar explícitamente las necesidades de QoS del tráfico de una aplicación en todos los dispositivos a lo largo del camino entre el origen y el destino utilizando el plano de control. La aplicación sólo empezará a transmitir si cada dispositivo puede reservar el ancho de banda necesario. IntServ es definido en las RFC 1633 (*Integrated Services in the Internet Architecture: an Overview*) y 2205 (*Resource ReSerVation Protocol*, RSVP).

2.6.3. Servicios Diferenciados (DiffServ)

DiffServ también es definido por la IETF, pero en cambio, la configuración de QoS se realiza en cada punto de la red y define un campo llamado DiffServ (DS) que reemplaza el campo ToS de IPv4 para tomar decisiones de comportamiento por salto (PHB). Estos campos son utilizados por cada fabricante para implementar técnicas de manejo de colas en base a este campo. Los mecanismos utilizados en Diffserv son utilizados en el plano de datos impactando directamente al comportamiento de los paquetes y son implementados usualmente por los fabricantes utilizando hardware de uso específico.

En la figura 2.67 se muestra cómo se aplica la calidad de servicio al utilizar Diffserv.

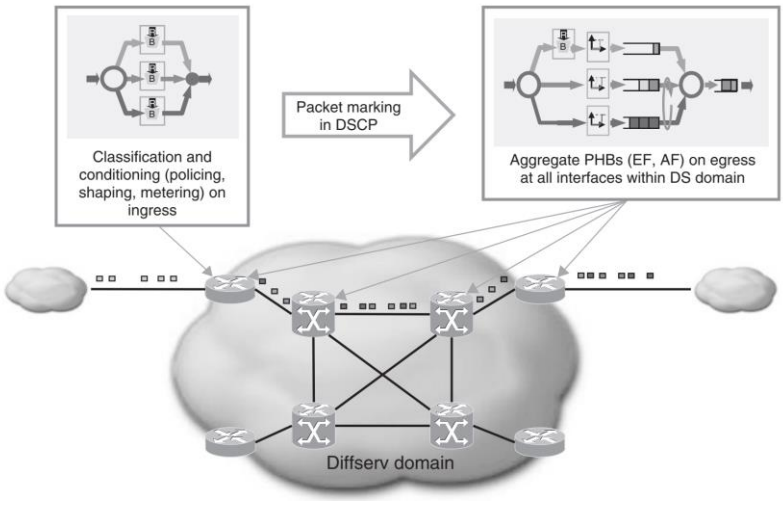


Figura 2.67 Aplicación de QoS mediante DiffServ en una red (Fuente: Ref. [23])

Las acciones comprendidas en Diffserv comprenden:

a) Clasificación:

Es la acción de categorizar el tráfico en un número determinado de colas, cada una de ellas, correspondiente a una clase de servicio de forma que luego se pueda ejecutar una acción o política de QoS sobre cada paquete. En la figura 2.68 se muestra como los paquetes son clasificados al ingresar a la interfaz de un enrutador donde se tiene configurada una política de calidad de servicio.

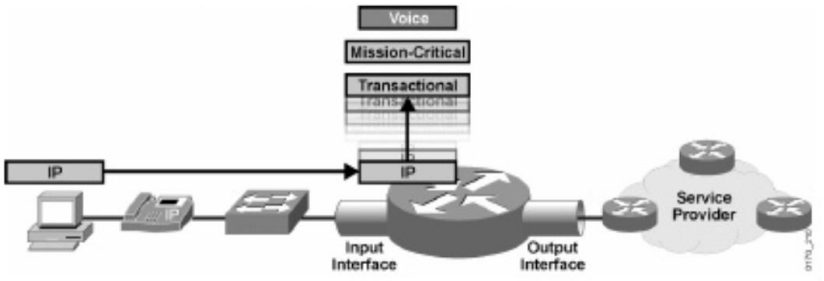
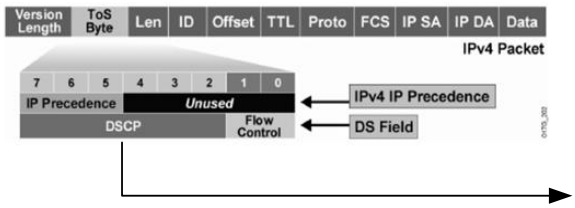


Figura 2.68 Proceso de clasificación de paquetes (Fuente: Ref. [24])

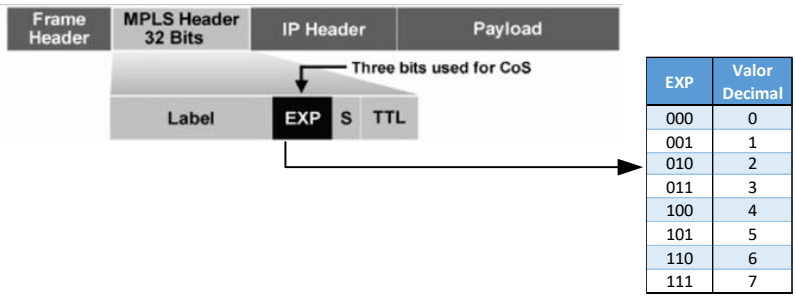
Paquetes IPv4, la clasificación en un paquete IPv4 se realiza utilizando el campo Diffserv en la cabecera IP a través de los campos de DSCP y ECN. También es posible utilizar la definición original de Byte de Tipo de Servicio (ToS). En la figura 2.69 se muestran el campo Diffserv dentro de un paquete IPv4 y los valores que puede tomar el DSCP.



DSCP	Valor Decimal	Significado	Probabilidad de descarte	IP Precedence equivalente
000 000	0	Best Effort	-	000 - Routine
001 000	8	CS1	-	001 - Priority
001 010	10	AF11	Low	001 - Priority
001 100	12	AF12	Medium	001 - Priority
001 110	14	AF13	High	001 - Priority
010 000	16	CS2	-	010 - Immediate
010 010	18	AF21	Low	010 - Immediate
010 100	20	AF22	Medium	010 - Immediate
010 110	22	AF23	High	010 - Immediate
011 000	24	CS3	-	011 - Flash
011 010	26	AF31	Low	011 - Flash
011 100	28	AF32	Medium	011 - Flash
011 110	30	AF33	High	011 - Flash
100 000	32	CS4	-	100 - Flash Override
100 010	34	AF41	Low	100 - Flash Override
100 100	36	AF42	Medium	100 - Flash Override
100 110	38	AF43	High	100 - Flash Override
101 000	40	CS5	-	101 - Critical
101 110	46	EF	-	101 - Critical
110 000	48	CS6	-	110 - Internet
111 000	56	CS7	-	111 - Network

Figura 2.69 Definición del campo Diffserv en la cabecera IP (Fuente: Ref. [24])

- Paquetes MPLS, los paquetes MPLS utilizan un campo de 3 bits definido inicialmente en la cabecera del paquete MPLS para uso experimental. La RFC 3270, designa este campo para ser utilizado en el marcado de los paquetes MPLS y permitir de esta manera el soporte del modelo Diffserv en MPLS. En la figura 2.70 se muestran el campo EXP dentro de una etiqueta MPLS y los valores que puede tomar este campo.



EXP	Valor Decimal
000	0
001	1
010	2
011	3
100	4
101	5
110	6
111	7

Figura 2.70 Campo EXP en una etiqueta MPLS (Fuente: Ref. [24]).

b) Marcado

Es la acción explícita de colorear o marcar un paquete, implica la acción de cambiar los bits del campo Diffserv en el paquete IP o EXP en MPLS para poder identificarlo en el siguiente salto de la red. En la figura 2.71 se muestra un enrutador realizando el proceso de marcado del campo Diffserv.

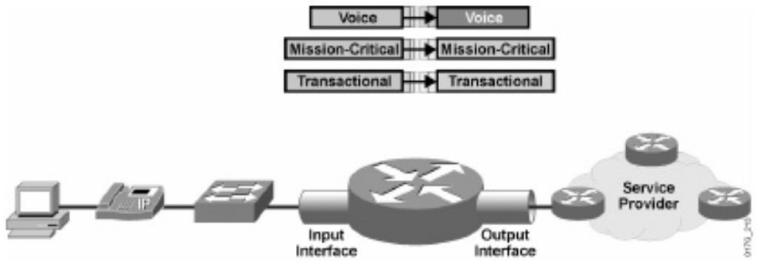


Figura 2.71 Proceso de marcado de paquetes (Fuente: Ref. [24])

El marcado de un paquete puede ser realizado en dos momentos:

- **En el origen**: El marcado es realizado por la aplicación y/o plataforma que origina el paquete. Es necesario que los equipos por los que el paquete transitará luego extremo-a-extremo reconozcan y acepten este marcado como confiable.
- **En un dispositivo intermedio:** El marcado es realizado por un nodo al cual intermedio en el trayecto extremo-a-extremo. Esto es realizado cuando la aplicación o plataforma que origina el paquete no tiene la capacidad de marcar el paquete o cuando el nodo, al cual el paquete está ingresando, no considera este proceso de marcado como confiable.

c) Control de ancho de banda y congestión

Es la acción de limitar la cantidad de ancho de banda máximo, que pueden utilizar una clase o conjunto de clases de servicio. Los mecanismos que se pueden utilizar son: *shaping* y *policing*. En la figura 2.72 se muestra un enrutador aplicando un mecanismo de control de ancho de banda y congestión de paquetes en su interfaz de salida.

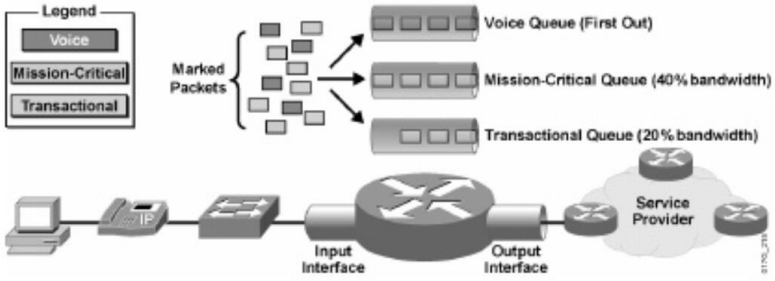


Figura 2.72 Control de ancho de banda y congestión (Fuente: Ref. [24])

- Policing, es utilizado para asegurar que el tráfico no sobrepase en ningún momento la tasa máxima asignada para un flujo de tráfico. Para visualizar este proceso se utiliza un modelo matemático de baldes y tokens o fichas, donde los tokens representan la cantidad de recursos disponibles para enviar datos en una interfaz y que se van reponiendo en el balde a una velocidad determinada y el balde representa la capacidad de contener un número específico de estas fichas o tokens. Al llegar un paquete toma una cantidad de tokens del depósito de acuerdo con el tamaño del paquete. En caso no haya suficientes tokens en el balde, el mecanismo de policing decide esperar a que se acumulen suficientes tokens en el balde o descartar el paquete.

A modo de ejemplo, se describe el mecanismo de Policing con una cubeta de fichas simple (Single Token Bucket). Este mecanismo uutiliza un único balde de fichas al que los tokens van llegando a una tasa de arribo y los paquetes son atendidos sólo si existen tokens disponibles. El flujo de tráfico en este caso es definido por estos parámetros:

✓ Tasa de información comprometida (*Committed Information Rate*, CIR): Tasa de tráfico promedio a la que el cliente puede enviar tráfico a la red.

✓ Tamaño de ráfaga comprometido (*Committed Burst Size*, Bc): Cantidad máxima de paquetes que un cliente puede enviar en un solo bloque.

✓ Intervalo de tiempo comprometido (*Committed time Interval*, Tc): Periodo de tiempo en el que se envía una ráfaga Bc a una tasa CIR.

La relación matemática entre estos parámetros es: $CIR_{bps} = Bc_{bits}/Tc_{seg}$.

La figura 2.73 muestra el comportamiento de *policing* sobre un enrutador a modo de ejemplo en dos situaciones: a) En T=0, llegan 500 Bytes, cuando se tienen disponibles 600 Bytes en el balde. La acción por ejecutar en este caso será transmitir los paquetes, dejando 100 bytes en el balde. b) En T=Tc=1.4 seg, llegan 700 Bytes, pero el balde cuenta con 600 tokens (100 + 500 tokens nuevos), por tanto, el paquete es descartado.

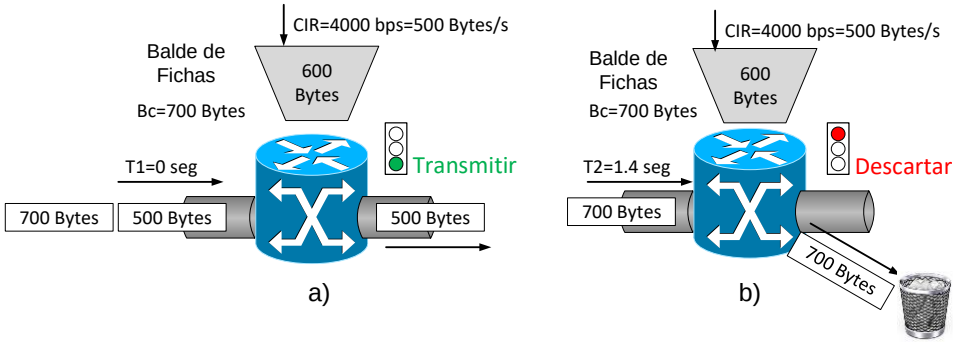


Figura 2.73 *Policing* con una Cubeta de fichas simple (Fuente: Ref. Elab. propia)

○ *Shaping*, a diferencia de *policing* el exceso de tráfico no se descarta, sino que es almacenado temporalmente para ser transmitido cuando se tengan recursos disponibles. Otra diferencia importante, es que los tokens son repuestos en el balde cada vez que un paquete es procesado o en intervalos de tiempo regulares utilizando un valor de bits por segundo (bps). El flujo de tráfico está definido por estos parámetros:

✓ Tasa de información comprometida (*Committed Information Rate*, CIR)

✓ Tamaño de ráfaga comprometido (*Committed Burst Size*, Bc)

✓ Intervalo de tiempo comprometido (*Committed time Interval*, Tc)

La relación matemática entre estos valores es: $CIR_{bps} = Bc_{bits}/Tc_{seg}$.

El uso más común del mecanismo de *shaping* es restringir la cantidad de ancho de banda a utilizar en una interfaz física o lógica, para ofrecer un servicio contratado. Ejemplo, un cliente que contrata 10Mbps, pero la interfaz del enrutador con el que es atendido es 1Gbps. En la figura 2.74 se ilustra como el proceso de *shaping* es utilizado para restringir el ancho de banda a la salida del *scheduler* y antes de llegar a la interfaz de un dispositivo de red.

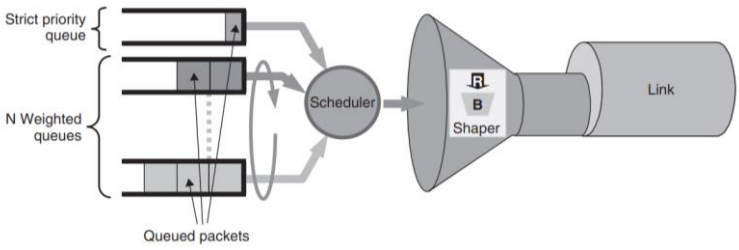


Figura 2.74. *Shaping* en interfaz para restringir el ancho de banda (Fuente: Ref. [23])

d) Encolamiento y Programación de colas

Los procesos de encolamiento (*queuing*) y programación de colas (*scheduling*) definen la forma en que se gestiona el ingreso y salida de los paquetes en un equipo en situaciones de congestión de tráfico. Los enrutadores utilizan un modelo de cola tipo FIFO (*First Input First Output*) por defecto en sus interfaces, sin embargo, es posible utilizar un programador

(*scheduler*) para priorizar la atención de los paquetes que requieran un tratamiento especial. El proceso lógico de encolamiento y agendamiento es mostrado en la figura 2.75, donde los paquetes llegan a las colas del equipo para luego pasar por el programador, antes de ser enviados por la interfaz física del equipo.

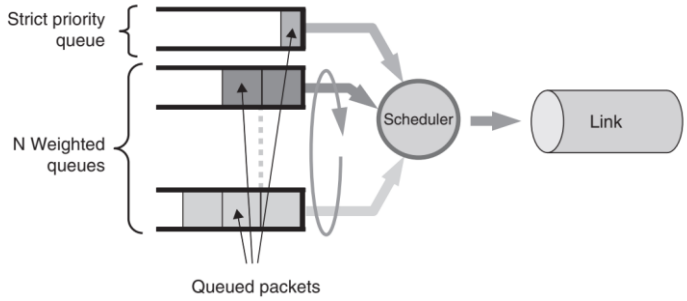


Figura 2.75 Programador de recursos en un enrutador [23]

A continuación, se describen los tipos de programación existentes:

- Programación Priorizada, usualmente utilizada en servicios que tienen poca tolerancia a retardos como la voz y video. Esto asegura que los paquetes tengan un retardo limitado y no sean afectados por fluctuaciones de fase (*jitter*). Además, es común, que se le asigne un ancho de banda de manera estricta para controlar el tráfico que ingresa a la cola priorizada de forma que no afecte a las otras colas.
- Programación ponderada por ancho de banda, el programador atenderá generalmente buscando realizar una ponderación efectiva en función del ancho de banda asignado a cada cola. Esto permite controlar el impacto de los retrasos en las colas y se puede diferenciar el servicio relativo a esas colas conforme a requisitos comunes de SLA demandados por el cliente final. Algunos ejemplos de este tipo de programación son los siguientes:

  ○ ***Weighted Round Robin*** **(WRR),** la distribución total de recursos de una interfaz a cada cola se realiza en función del peso asignado a la cola.

  ○ ***Weighted Fair Queuing*** **(WFQ),** similar a la anterior, sin embargo, la cantidad de recursos de cada cola es distribuida entre los flujos que maneja esa cola. Esto hace que el manejo de los paquetes en el enrutador sea más complejo puesto que debe mantener información de la cantidad de bits transmitidos en cada momento.

  ○ ***Deficit Round Robin*** **(DRR),** modifica WRR para tener las funcionalidades de WFQ sin la complejidad de está utilizando un contador de déficit de recursos (quantums) por cola. Busca calcular y acomodar los recursos necesarios para poder enviar los paquetes que no se pudieron enviar en el siguiente intento.

- **Interfaces FIFO**, el programador de un enrutador no coloca los paquetes directamente sobre la interfaz física, sino que previamente hace uso de una cola de tipo FIFO llamada

interfaz FIFO o buffer de anillo de transmisión (tx-ring). Esta cola permite aprovechar de mejor manera los recursos de la interfaz física y maximizar la cantidad de información transmitida en esta. El tamaño de esta cola debe ser lo suficientemente grande como para recibir los paquetes a una tasa más alta que la de los paquetes que llegan en la interfaz física pero no tan grande que introduzca un retardo apreciable en los paquetes.

En la figura 2.76 se muestra el funcionamiento del programador en una interfaz tipo FIFO.

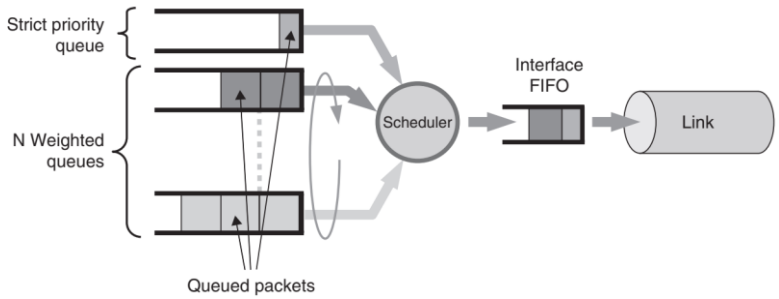


Figura 2.76 Interfaz FIFO en el programador (*scheduler*) de un enrutador [23]

e) Mecanismos para evitar la congestión

Los mecanismos para evitar la congestión realizan el descarte temprano de paquetes TCP para disminuir la cantidad de flujos que se envían por una interface, evitando el efecto de sincronización global de TCP, que ocurre cuando muchos flujos dejan de transmitirse al mismo tiempo durante periodos de congestión debido a la falta de QoS en la red troncal de un proveedor de servicios. Esto ayuda a algunas aplicaciones, como las de VoIP, al descartar el paquete y no tener que esperar que toda la cola se llene antes de ser transmitida aumentando el retardo.

- **Caída de Cola (*Tail Drop*):** Establece un límite estricto de tamaño para todas las colas a partir del cual los paquetes son descartados con una probabilidad del 100%.
- **Caída de Cola Ponderada (*Weigthed Tail Drop*):** Similar al anterior, con la ventaja de utilizar valores diferentes para el límite por cada cola.
- **Detección Temprana Aleatoria (*Random Early Detection*):** Establece dos limites: un valor inferior (qminth) a partir del cual los paquetes son descartados aleatoriamente con una tasa de probabilidad de descarte creciente desde 0 hasta pmax al llegar al límite superior de la cola (qmaxth). A partir de ese punto se descartan todos los paquetes serán descartados.
- **Detección Temprana Aleatoria Ponderada (*Weighted Random Early Detection*):** Extiende el concepto básico de RED, usando un perfil de RED diferente por cola.

En la figura 2.77 se muestra la probabilidad de descarte de paquetes en cada uno de estos mecanismos con el objetivo de manejar la congestión en una interfaz.

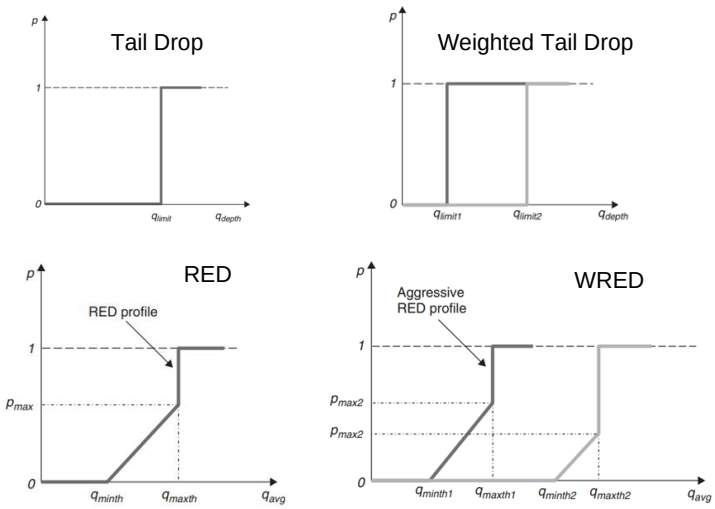


Figura 2.77 Probabilidad de descarte de paquetes en mecanismos para evitar congestión (Fuente: Ref. [23])

RED y WRED permiten la detección temprana del desborde de tráfico para evitar el efecto de "sincronización global" de sesiones TCP. En la figura 2.78 se muestra el comportamiento del tráfico TCP antes y después de aplicar RED.

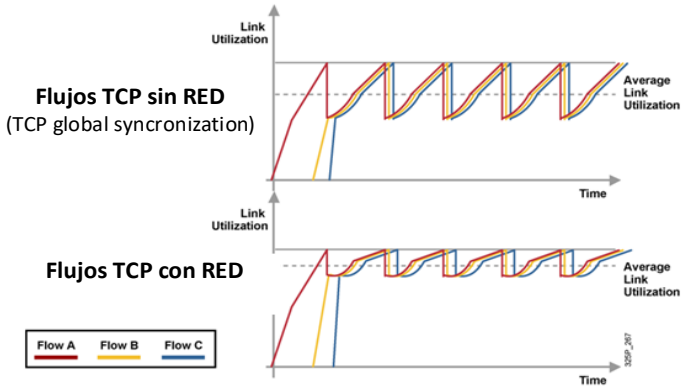


Figura 2.78 Efecto de RED sobre la sincronización global de TCP (Fuente: Ref. [24])

CAPÍTULO III
INTEGRACIÓN DE LAS REDES MPLS

En el presente capítulo se evalúa la información obtenida en la fase de relevamiento de información de la situación inicial de ambas redes MPLS, a fin de identificar los problemas de fondo que se deben resolver y decidir la solución a implementar definiendo los protocolos y normas a aplicar en la solución. Finalmente se indica el plan de implementación con las actividades principales a ejecutar durante el proyecto.

3.1. Situación Inicial

Las características principales de ambas redes identificadas durante la fase de relevamiento de información son indicadas a continuación:

- **Equipamiento en fase de obsolescencia.**

La MPLS GOB cuentan con enrutadores y conmutadores en la última etapa de su ciclo de vida tecnológico (declarado por el fabricante de estos) que deben renovarse en el corto plazo puesto que ya no cuentan con soporte técnico del fabricante. El tiempo de vida media de los equipos existentes en esta red es mayor a 6 años y parte de los equipos ya se encuentran cercanos a su fin de vida (anuncios de End-of-Sale and End-of-Support del fabricante).

- **Problemas de cobertura de la red.**

La MPLS GOB cuenta con menor cantidad de enrutadores PE (menor cantidad de puntos de presencia de nodos MPLS), pero mayor cantidad de dispositivos en su acceso MPLS y LAN a diferencia de la red MPLS DCN. Es posible mejorar las capacidades de ambas redes de Gestión Fuera de Banda aprovechando las topologías iniciales y los recursos existentes (enlaces, disposición geográfica de los nodos y salas de equipos) para lograr sinergias entre ambas redes.

- **Trafico sin diferenciación ni nivel de prioridad**.

No existe ningún mecanismo de calidad de servicio implementado que permita diferenciar y/o priorización de los distintos tipos de tráfico.

- **Equipos críticos sin redundancia que representan puntos de falla importantes**.

Los conmutadores de concentración principales de la MPLS GOB (nodos principales, centros de datos y centro de gestión) representan un punto de falla, ya que no cuentan con redundancia de equipo. Además, se confía únicamente en el diseño del protocolo STP, para evitar tormentas de tráfico broadcast. Era necesario mejorar la alta disponibilidad de

los sistemas existentes reduciendo el riesgo de caídas, que en este caso representan la imposibilidad de reaccionar ante fallas de la red que atiende a los servicios a clientes finales.

- **No se aprovechan las capacidades totales del equipamiento instalado**.

Los enrutadores PE de ambas redes MPLS por sus características pueden soportar mayor cantidad de sesiones BGP, nodos en el protocolo IGP, capacidad de reenvío de paquetes, número de L3VPN, etc., pero esto no es aprovechado.

- **Topologías de red similares en ambas redes MPLS y la necesidad de interconexión de ambas redes.**

Se identifica que el diseño de ambas redes es similar, al utilizar protocolos similares. Adicionalmente se identifica que existen requerimientos para interconectar ambas redes para propósitos de gestión de algunos equipos.

- **Personal encargado de la gestión de los equipos no capacitado o con foco en otras tecnologías**.

Se identificó que el equipo encargado de las tareas de gestión de la red MPLS DCN, contaba con mayores conocimientos de las tecnologías de transporte tales como DWDM, SDH, microondas, etc., por ser la red de servicios, que tenían cargo, pero no tenían mucha experiencia con tecnologías IP/MPLS. En el caso de la red MPLS GOB, el personal a cargo de la gestión no tenía este problema puesto que al trabajar con redes de servicio IP/MPLS para clientes finales tenían la suficiente experiencia para trabajar con esta.

- **Crecimiento de la red de gestión fuera de banda a 5 años.**

El requerimiento para ampliar las capacidades de gestión debe soportar el crecimiento de los próximos 5 años de nuevos equipos en las redes de servicios.

- **Duplicidad de costos de inversión**

Atender los requerimientos de ampliación de cobertura y capacidades de ancho de banda por separado en cada red de gestión fuera de banda representa la adquisición de equipos, cableados, adecuaciones en los nodos y servicios profesionales por cada red duplicando la inversión. La sinergia entre ambas redes mejora la capacidad y disponibilidad de ambas redes además de conseguir ahorros en los costos de Inversión (CapEx) y de mantenimiento y operación (OpEx).

3.1.1. Red MPLS GOB

La red MPLS GOB cuenta con puntos de presencia o POP (*Point of Presence*) en los lugares más relevantes de la red de servicios, lo cual brinda un método de gestión resiliente a fallas en los enlaces de la red.

En la Tabla 3.1, se indica la relación de equipos encontrados como parte del dominio MPLS y la nomenclatura a utilizar para el presente informe:

Tabla 3.1 Situación Inicial MPLS GOB: Relación de equipos (Fuente: Elab. propia)

N°	Región	Lugar	Sala	Tipo	Equipo
1	Lima	Washington	Datos	Enrutador	PE_GOB_01
2	Lima	San Isidro 1	Datos	Enrutador	PE_GOB_02
3	Lima	Surquillo	Datos 1	Enrutador	PE_GOB_03
4	Lima	Surquillo	Datos 2	Enrutador	PE_GOB_04
5	Lima	La Victoria	Celular	Enrutador	PE_GOB_05
6	Lima	San Isidro 2	Celular	Enrutador	PE_GOB_06
7	Lima	Monterrico	Datos	Enrutador	PE_GOB_07
8	Lima	Miraflores	Datos	Enrutador	PE_GOB_08
9	Provincia Norte	Trujillo	Datos	Enrutador	PE_GOB_09
10	Provincia Sur	Arequipa	Datos	Enrutador	PE_GOB_10
11	Lima	Washington	Datos	Conmutador	SWC_GOB_01
12	Lima	San Isidro 1	Datos	Conmutador	SWC_GOB_02
13	Lima	Surquillo	Datos 1	Conmutador	SWC_GOB_03
14	Lima	Surquillo	Datos 2	Conmutador	SWC_GOB_04
15	Lima	La Victoria	Celular	Conmutador	SWC_GOB_05
16	Lima	San Isidro 2	Celular	Conmutador	SWC_GOB_06
17	Lima	Monterrico	Datos	Conmutador	SWC_GOB_07
18	Lima	Miraflores	Datos	Conmutador	SWC_GOB_08

a) Topología

En la figura 3.1 se muestra la topología física inicial de la red MPLS GOB:

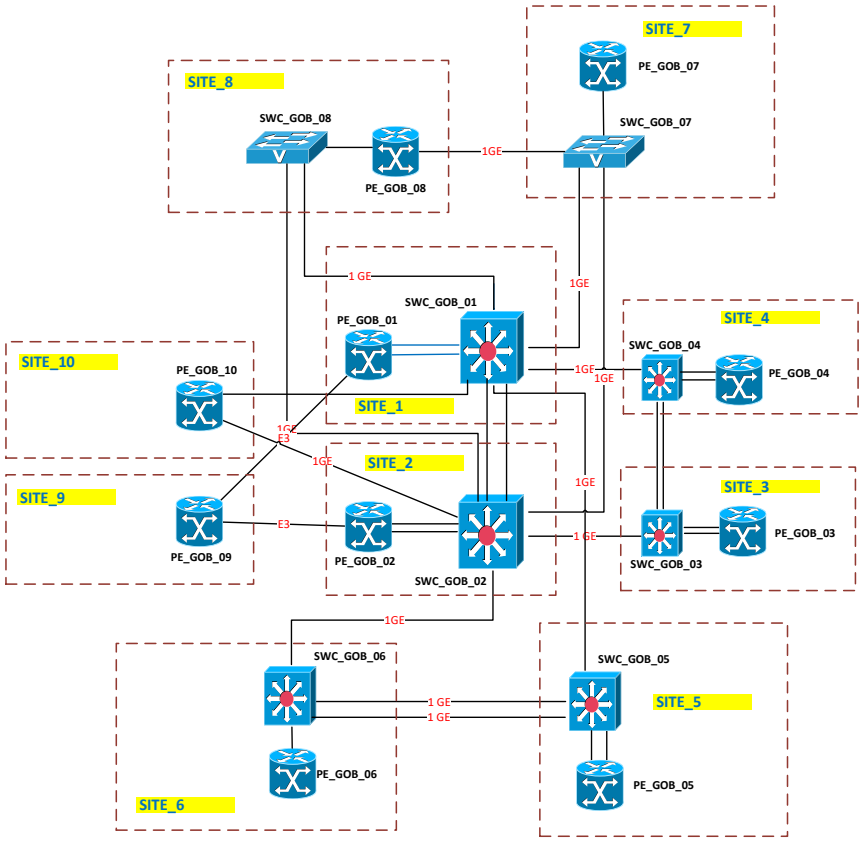


Figura 3.1. Situación Inicial MPLS GOB: Topología Física (Fuente: Elab. propia)

b) Topología Lógica

La conectividad L3 entre enrutadores no es directa, sino mediante la extensión de VLANs, a través de conmutadores intermedios, que permiten el paso de las VLANs para establecer conectividad entre los PE. En la figura 3.2 se muestra la topología de conectividad L3 entre PE_GOB_01, 02 y 06 utilizando VLANs extendidas.

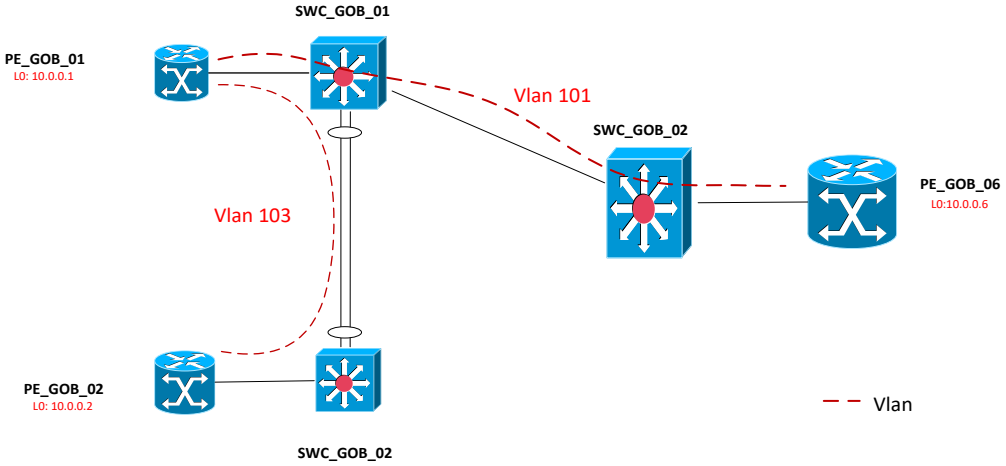


Figura 3.2. Situación Inicial MPLS GOB: Topología conectividad L3 entre PE_GOB_01, 02 y 06 (Fuente: Elaboración propia)

La topología lógica resultante, al mapear estas conexiones es mostrada en la figura 3.3:

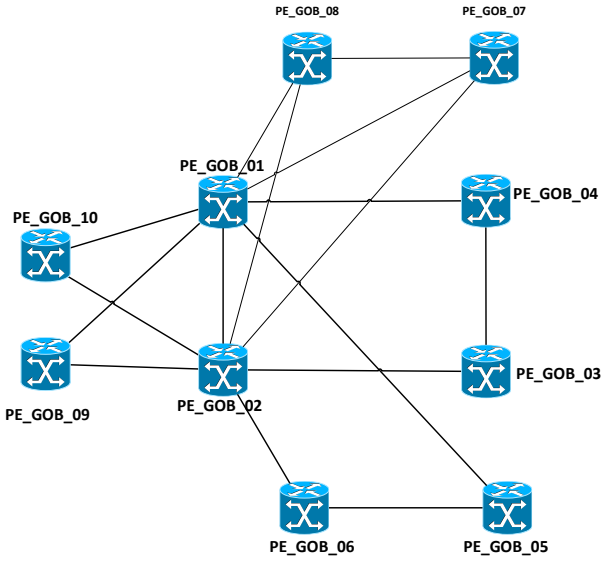


Figura 3.3. Situación Inicial MPLS GOB: Topología Lógica (Fuente: Elab. propia)

c) Protocolo IGP:

El protocolo *Intermediate System – Intermediate System* (IS-IS) es utilizado como IGP para el enrutamiento de prefijos internos a la MPLS que incluye a los enlaces WAN y *loopbacks*. Todos los enrutadores se encontraban en un solo área y bajo la misma jerarquía

de nivel 2. No se utiliza la jerarquía de nivel 1. En la figura 3.4 se muestra la topología de adyacencias de IS-IS encontrado:

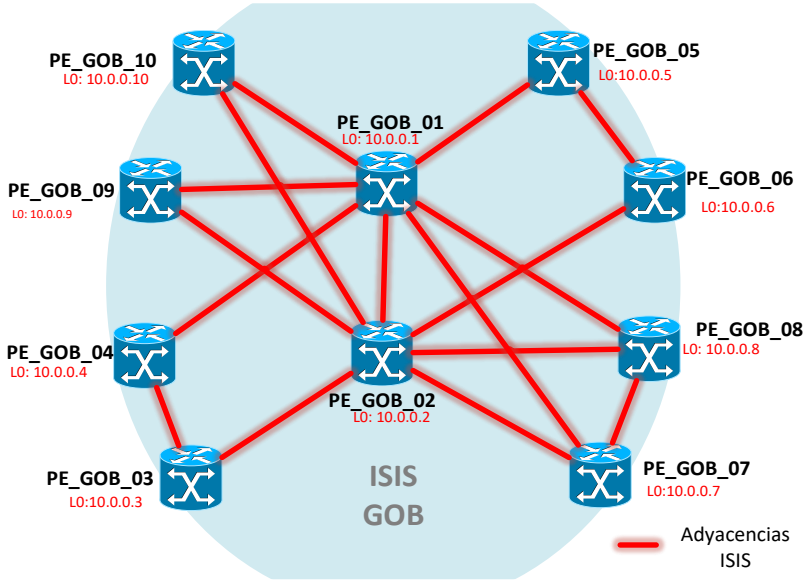


Figura 3.4 Situación Inicial MPLS GOB: Adyacencias IGP IS-IS (Fuente: Elab. propia)

En el Anexo A, tabla A.1 se muestra la lista de adyacencias IS-IS encontradas en los enrutadores PE de la MPLS GOB.

d) MPLS:

La topología MPLS encontrada es de tipo colapsada, por tanto, todos los enrutadores cumplen con la función de PE.

A continuación, se muestra el diagrama de adyacencias de IS-IS en la figura 3.5:

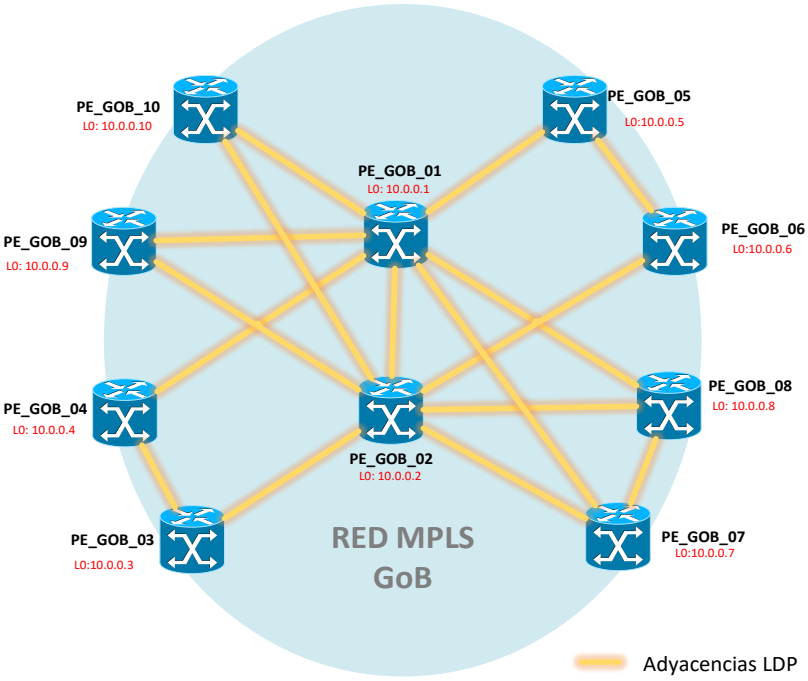


Figura 3.5. Situación Inicial MPLS GOB: Adyacencias LDP (Fuente: Elab. propia)

En la tabla 3.2 se muestra la lista de adyacencias LDP formadas entre los enrutadores PE de la MPLS GOB.

Tabla 3.2 Situación Inicial MPLS GOB: Adyacencias ISIS y LDP (Fuente: Elab. propia)

PE1	PE2	Tipo	Tipo ISIS	Estado ISIS	Estado LDP
PE_GOB_01	*PE_GOB_02*	1G	L2	UP	UP
PE_GOB_01	*PE_GOB_04*	1G	L2	UP	UP
PE_GOB_01	*PE_GOB_05*	1G	L2	UP	UP
PE_GOB_01	*PE_GOB_07*	1G	L2	UP	UP
PE_GOB_01	*PE_GOB_08*	1G	L2	UP	UP
PE_GOB_01	*PE_GOB_09*	1G	L2	UP	UP
PE_GOB_01	*PE_GOB_10*	1G	L2	UP	UP
PE_GOB_02	*PE_GOB_03*	1G	L2	UP	UP
PE_GOB_02	*PE_GOB_06*	1G	L2	UP	UP
PE_GOB_02	*PE_GOB_07*	1G	L2	UP	UP
PE_GOB_02	*PE_GOB_08*	1G	L2	UP	UP
PE_GOB_02	*PE_GOB_09*	1G	L2	UP	UP
PE_GOB_02	*PE_GOB_10*	1G	L2	UP	UP
PE_GOB_03	*PE_GOB_04*	1G	L2	UP	UP
PE_GOB_05	*PE_GOB_06*	1G	L2	UP	UP
PE_GOB_07	*PE_GOB_08*	1G	L2	UP	UP

Los parámetros de configuración de LDP presentan las siguientes características:

- Usa interfaces lógicas *loopback* (bucle de retorno) como *router-id*
- Los modos de trabajo utilizados para LDP en esta red son:
  - ✓ Modo de distribución de etiquetas: no solicitadas en sentido descendente o UD
  - ✓ Modo de retención de liberal o LLR
  - ✓ Modo de control LSP independiente
- Las adyacencias de LDP están autenticadas.
- Se permiten la formación de adyacencias remotas mediante mensajes *Hello* dirigidos.

e) Sesiones BGP:

Los enrutadores PE_GOB_01 y PE_GOB_02 funcionan como RR. Los demás enrutadores ejecutan mantienen sesiones BGP activas con estos RR. El sistema autónomo que utilizan es de tipo privado (65001). Las sesiones BGP se establecen utilizando interfaces *loopback*. Las familias habilitadas son IPv4 (AFI 1 y SAFI 1) y VPNv4 (AFI 1 y SAFI 128).

En la tabla 3.3 se listan las sesiones BGP formadas entre los enrutadores PE y los RR encontradas.

Tabla 3.3 Situación Inicial MPLS GOB: Sesiones BGP - PEs y RRs (Fuente: Elaboración propia)

PE	RR	Descripción
PE_GOB_03	*PE_GOB_01*	RR1
	PE_GOB_02	RR2
PE_GOB_04	*PE_GOB_01*	RR1
	PE_GOB_02	RR2
PE_GOB_05	*PE_GOB_01*	RR1
	PE_GOB_02	RR2
PE_GOB_06	*PE_GOB_01*	RR1
	PE_GOB_02	RR2
PE_GOB_07	*PE_GOB_01*	RR1
	PE_GOB_02	RR2
PE_GOB_08	*PE_GOB_01*	RR1
	PE_GOB_02	RR2
PE_GOB_09	*PE_GOB_01*	RR1
	PE_GOB_02	RR2
PE_GOB_10	*PE_GOB_01*	RR1
	PE_GOB_02	RR2

En la figura 3.6 se muestran las sesiones BGP establecidas entre los PE y los RR:

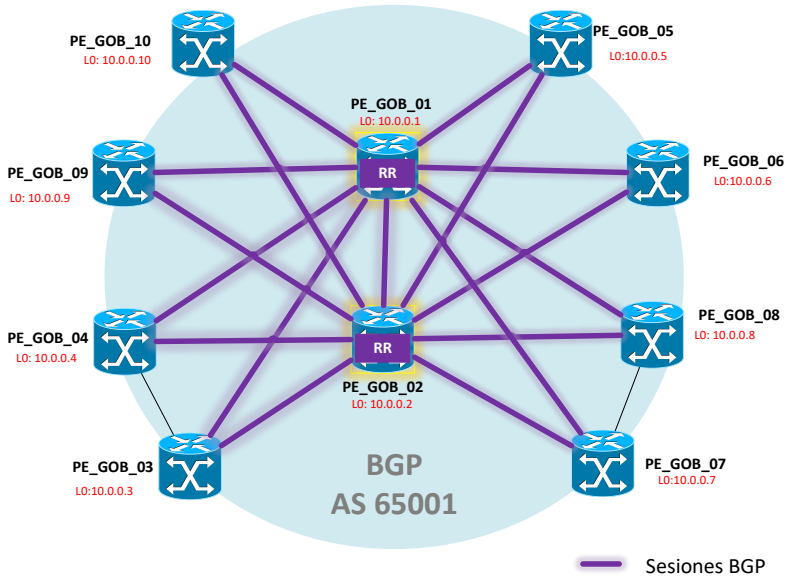


Figura 3.6. Sit. Inicial MPLS GOB: Sesiones BGP – PEs y RRs (Fuente: Elab. propia)

3.1.2. Acceso MPLS GOB:

Este bloque define funcionalmente la manera como los enrutadores de acceso de la red MPLS se interconectan con la red de cada cliente que hace uso de los servicios L3VPN.

a) VRF:

Las VRF's encontradas segmentan las tablas de enrutamiento por el tipo de red a la que pertenecen las plataformas. En la tabla 3.4 se lista las VRF existentes en enrutadores PE y sus valores de RD, RT *Import* y RT *Export*.

Tabla 3.4 Sit. Inicial MPLS GOB: VRFs (Fuente: Elab. propia)

Tipo de Red de Gestión	VRF	RD	RT	
			Import	Export
Equipos Red Empresas	vrf_GOB_1	65001:1	65001:1	65001:1
Equipos Red BA	vrf_GOB_2	65001:2	65001:2	65001:2
Equipos Red Móvil	vrf_GOB_3	65001:3	65001:3	65001:3
Equipos Seguridad	vrf_GOB_4	65001:4	65001:4	65001:4
Equipos Interconexión	vrf_GOB_5	65001:5	65001:5	65001:5

b) Conexiones PE-CE:

Las conexiones hacia la red MPLS GOB muestran dos tipos de topología:

1. PE y CE interconectados a través de VLANs.
2. Conexión CE-PE directa a través de enlaces TDM E1.

En la figura 3.7 se muestra ambas topologías:

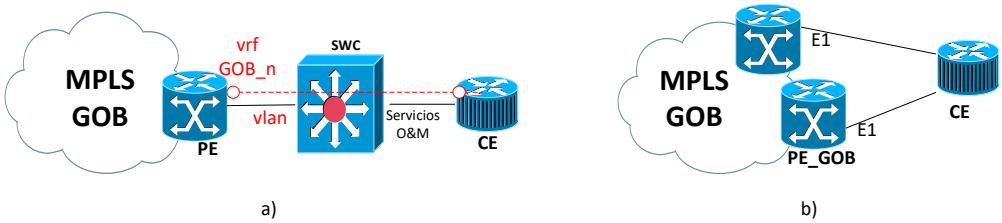


Figura 3.7. Sit. Inicial MPLS GOB: Conexión PE–CE a) mediante conmutador b) directamente con enlace TDM E1 (Fuente: Elab. propia)

En la tabla 3.5 se muestra la relación de equipos con enlaces PE-CE directos mediante enlace E1 y el BW asignado inicialmente:

Tabla 3.5 Sit. Inicial MPLS GOB: Enlaces PE-CE mediante E1 (Fuente: Elab. propia)

CE	PE	Tipo	BW
CE_GOB11_1	PE_GOB_06	E1 Datos	2048 kbps
CE_GOB11_1	PE_GOB_05	E1 Datos	2048 kbps
CE_GOB12_1	PE_GOB_06	E1 Datos	2048 kbps
CE_GOB12_1	PE_GOB_05	E1 Datos	2048 kbps
CE_GOB13_1	PE_GOB_06	E1 Datos	2048 kbps
CE_GOB13_1	PE_GOB_05	E1 Datos	2048 kbps
CE_GOB14_1	PE_GOB_06	E1 Datos	2048 kbps
CE_GOB14_1	PE_GOB_05	E1 Datos	2048 kbps
CE_GOB15_1	PE_GOB_06	E1 Datos	2048 kbps
CE_GOB15_1	PE_GOB_05	E1 Datos	2048 kbps
CE_GOB16_1	PE_GOB_06	E1 Datos	2048 kbps
CE_GOB16_1	PE_GOB_05	E1 Datos	2048 kbps
CE_GOB17_1	PE_GOB_06	E1 Datos	2048 kbps
CE_GOB17_1	PE_GOB_05	E1 Datos	2048 kbps

En el Anexo B figura B.1 se muestra la topología de las redes de acceso existentes en cada POP.

c) Enrutamiento PE-CE:

A continuación, se describen los tipos de enrutamiento PE-CE existentes en el acceso a la MPLS GOB.

- BGP. Es el tipo de enrutamiento más utilizado. Los enrutadores PE y CE tienen una sesión eBGP en cada VRF utilizando el AS vecino correspondiente a cada red de plataformas. En la figura 3.8 se muestra cómo se establecen las sesiones BGP entre PE y CE.

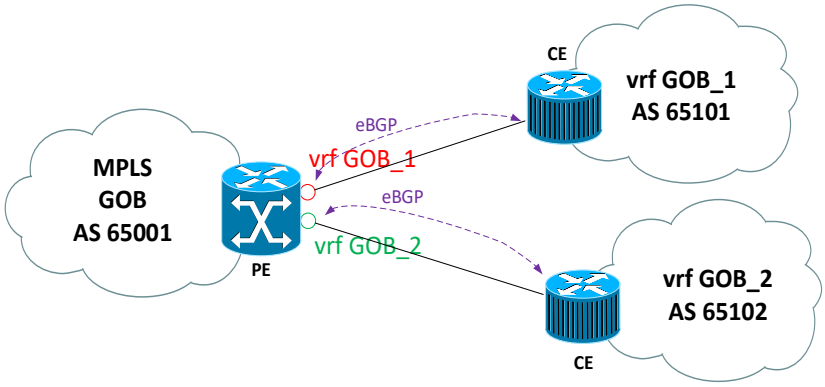


Figura 3.8 Sit. Inicial MPLS GOB: BGP como protocolo PE-CE. (Fuente: Elab. propia)

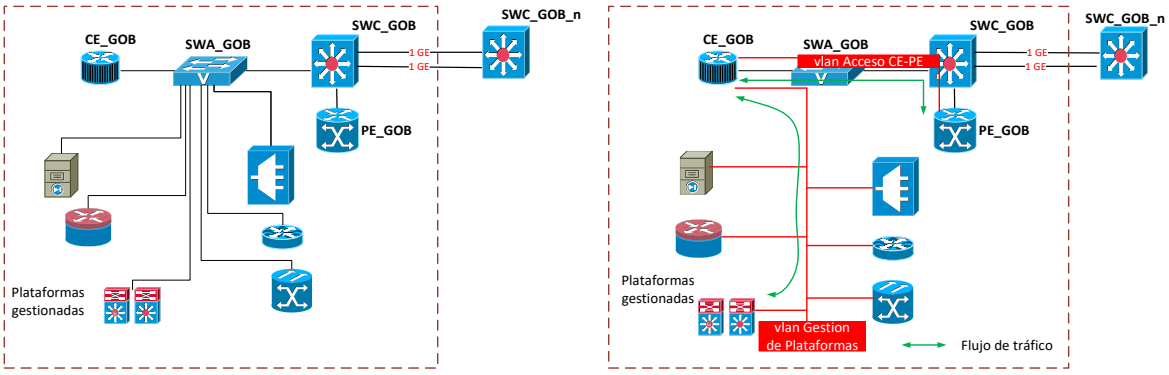
- Enrutamiento Estático, utilizado cuando no es posible utilizar enrutamiento dinámico.

3.1.3. Acceso LAN GOB:

Se pudo identificar los siguientes tipos de nodos:

a) Nodo Primario:

Un nodo primario atiende la gestión de nodos con la mayor cantidad de dispositivos y plataformas de red (sin considerar a los Centros de Datos ni los Centros de Gestión) y mantiene una distribución jerárquica de conmutadores de acceso y concentración. A nivel lógico la puerta de enlace es mantenida sobre el CE, quien a su vez mantiene una VLAN que se extiende por los conmutadores de acceso y concentración hacia el PE. La topología física y lógica de los nodos primarios son mostradas en la figura 3.9:



a) Topología Física

b) Topología Lógica

Figura 3.9 Situación Inicial MPLS GOB: Topologías Física y Lógica en nodos primarios. (Fuente: Elab. propia)

También se dispone de gestión vía interfaces seriales asíncronas en el enrutador CE, que hace las veces de servidor de acceso con el protocolo telnet reverso, como se observa en la figura 3.10.

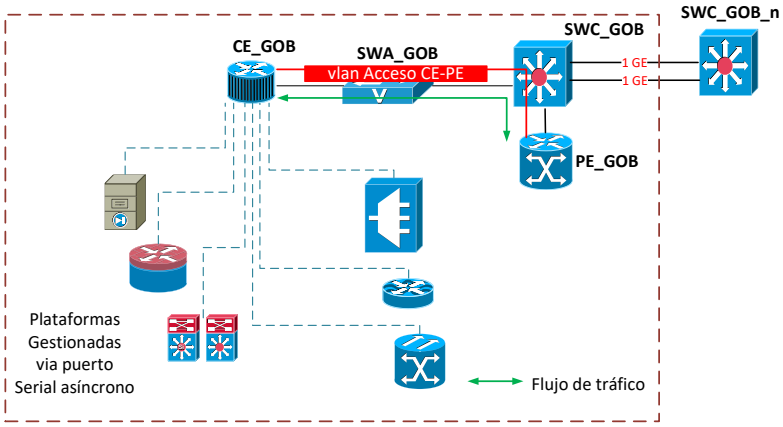


Figura 3.10 Situación Inicial MPLS GOB: Topologías Gestión vía puerto serial asíncrono. (Fuente: Elab. propia)

b) Nodo Secundario

Un nodo secundario atiende una cantidad menor de equipos que los nodos principales, y suelen concentrar todas las conexiones de los equipos y plataformas a gestionar en un conmutador de acceso. A nivel lógico la puerta de enlace se mantiene sobre el CE, quien a su vez mantiene una VLAN que se extiende por los conmutadores de acceso hacia el PE. La topología física y lógica de los nodos secundarios es mostrada en la figura 3.11:

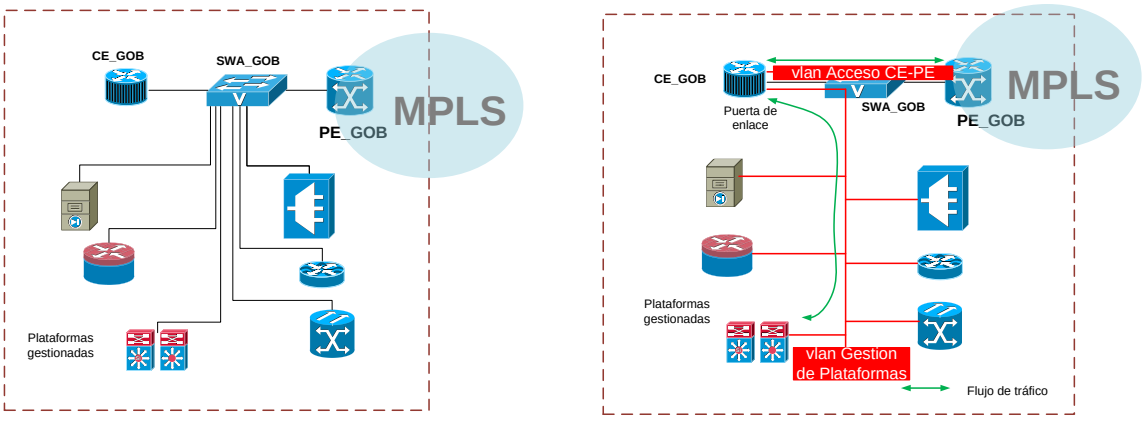
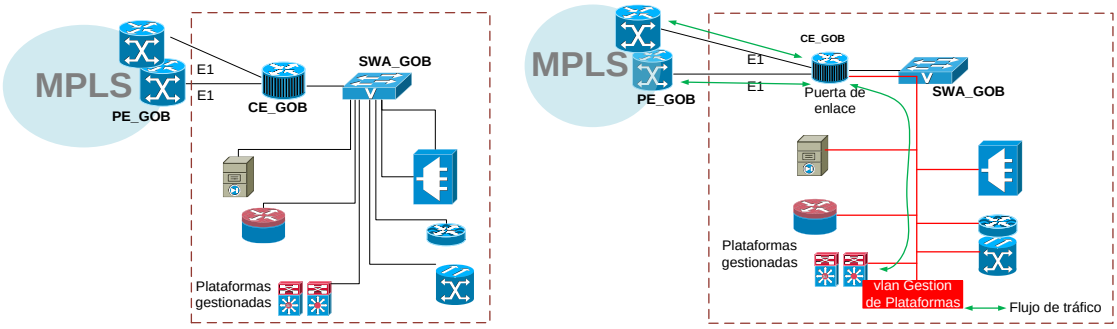


Figura 3.11 Situación Inicial MPLS GOB: Topologías Física y Lógica en nodos secundarios. (Fuente: Elab. propia)

La gestión vía interfaces seriales asíncronas se mantiene en el enrutador CE, que hace las veces de servidor de acceso con el protocolo telnet reverso.

c) Nodos Remotos:

Los nodos remotos se encuentran en zonas alejadas y contienen menos equipos que los nodos principales y secundarios. No cuentan con enlaces PE-CE Ethernet, sino que utilizan enlaces TDM E1. A nivel lógico mantienen una topología similar a los nodos secundarios con un solo conmutador de acceso y puerta de enlace en el enrutador CE. La topología física y lógica de los nodos remotos es mostrada en la figura 3.12:



a) Topología Física

b) Topología Lógica

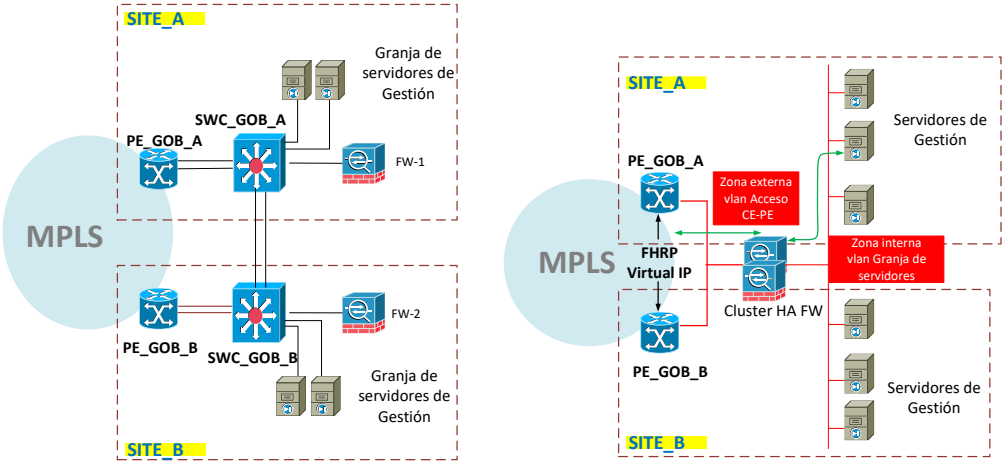
Figura 3.12 Situación Inicial MPLS GOB: Topologías Física y Lógica en nodos remotos. (Fuente: Elab. propia)

La gestión vía interfaces seriales asíncronas se mantiene en el enrutador CE, que hace las veces de terminal server con el protocolo telnet reverso.

d) Centro de Datos:

El Centro de Datos es el lugar donde se ubican los servidores y plataformas de la red de servicio y de gestión fuera de banda. Los Centros de Datos cuentan con redundancia en zonas geográficas diferentes para asegurar la alta disponibilidad del servicio, con servidores que se instalan en más de un centro de datos.

A nivel lógico, cuentan con alta disponibilidad utilizando un protocolo FHRP en los enrutadores de borde PE MPLS. Estos a su vez tienen colapsados la función de CE. La puerta de enlace se encuentra en un clúster de *firewalls* que provee alta disponibilidad y seguridad a los servidores. Las topologías física y lógica de un centro de datos se muestran en la figura 3.13:

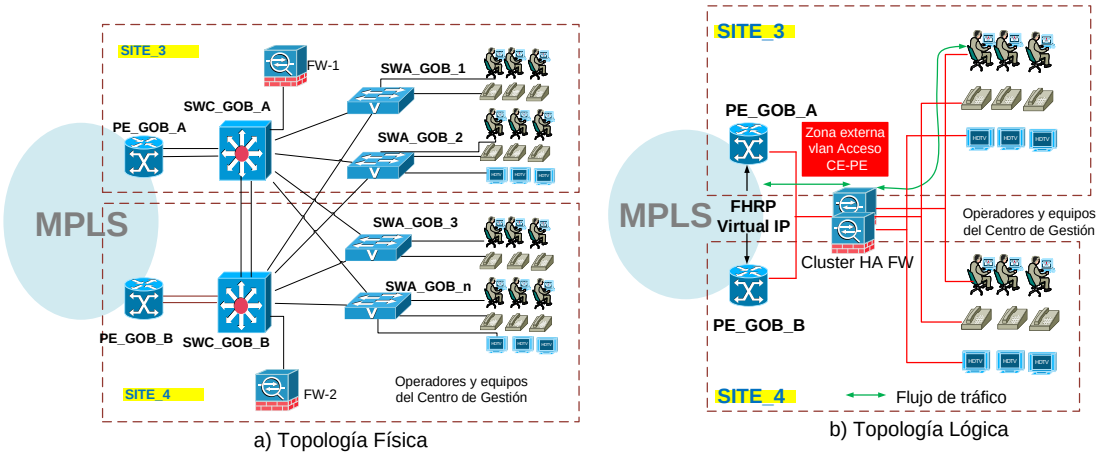


a) Topología Física b) Topología Lógica

Figura 3.13 Situación Inicial MPLS GOB: Topologías Física y Lógica en Centro de Datos. (Fuente: Elab. propia)

e) Centro de Gestión:

El Centro de Gestión es considerado como uno de los puntos más importantes de la red pues es el lugar donde se ubican físicamente los agentes y operadores de la red para realizar las tareas de monitoreo, solución de problemas e implementar mejoras continuas en la red. El acceso LAN de esta sede es similar a un centro de datos, pero ubicado en los nodos SITE_3 y SITE_4. En la figura 3.14 se muestra la topología física y lógica en un Centro de Gestión



a) Topología Física b) Topología Lógica

Figura 3.14 Situación Inicial MPLS GOB: Topologías Física y Lógica en Centro de Gestión. (Fuente: Elab. propia)

3.1.4. Red MPLS DCN

A diferencia de la MPLS GOB, esta red MPLS cuenta con puntos de presencia casi en todos los lugares coincidentes con la red de servicios. El tiempo de vida media de los equipos existentes en la red es menor a 2 años y cuentan con contratos de soporte activos con los fabricantes de estos.

a) Topología

Los enrutadores de la red MLS DCN se encuentran interconectados por enlaces directos 1G. La topología física de equipos de la red MPLS DCN es mostrada en el Anexo C figura C.1. En la tabla 3.6 se muestra la relación de equipos encontrados y la nomenclatura a utilizar para el presente informe:

Tabla 3.6. Situación Inicial MPLS DCN: Relación de enrutadores (Fuente: Elab. Propia)

N°	Región	PoP	Nodos	Router ID
1	Lima	Surquillo 1	PE_TX_01	11.0.0.1
2		Surquillo 1	PE_TX_02	11.0.0.2
3		Washington	PE_TX_03	11.0.0.3
4		Lince	PE_TX_04	11.0.0.4
5		Higuereta	PE_TX_05	11.0.0.5
6		Lurín	PE_TX_06	11.0.0.6
7		La Victoria	PE_TX_07	11.0.0.7
8		San Isidro	PE_TX_08	11.0.0.8
9		Monterrico	PE_TX_09	11.0.0.9
10	Provincia Zona Norte	Trujillo	PE_TX_10	11.0.0.10
11		Cajamarca	PE_TX_11	11.0.0.11
12		Chiclayo	PE_TX_12	11.0.0.12
13		Piura	PE_TX_13	11.0.0.13
14		Tarapoto	PE_TX_14	11.0.0.14
15		La Oroya	PE_TX_15	11.0.0.15
16		Chimbote	PE_TX_16	11.0.0.16
17		Huaraz	PE_TX_17	11.0.0.17
18		Tumbes	PE_TX_18	11.0.0.18
19		Jaén	PE_TX_19	11.0.0.19
20		Tingo Maria	PE_TX_20	11.0.0.20
21		Pucallpa	PE_TX_21	11.0.0.21
22	Provincia Zona Sur	Huancayo	PE_TX_22	11.0.0.22
23		Ayacucho	PE_TX_23	11.0.0.23
24		Cusco	PE_TX_25	11.0.0.25
25		Ica	PE_TX_26	11.0.0.26
26		Juliaca	PE_TX_27	11.0.0.27
27		Puno	PE_TX_28	11.0.0.28
28		Desaguadero	PE_TX_29	11.0.0.29
29		Arequipa	PE_TX_30	11.0.0.30
30		Tacna	PE_TX_31	11.0.0.31
31		Moquegua	PE_TX_32	11.0.0.32

b) Protocolo IGP

La red MPLS DCN también utiliza IS-IS como IGP para el enrutamiento de prefijos internos (enlaces WAN y *loopbacks*) con una configuración de parámetros similar a la

MPLS GOB. No se utiliza jerarquía nivel 1, así que todos los enrutadores se encuentran en un solo área y bajo jerarquía de nivel 2. En la figura 3.15 se muestra el diagrama de adyacencias IS-IS.

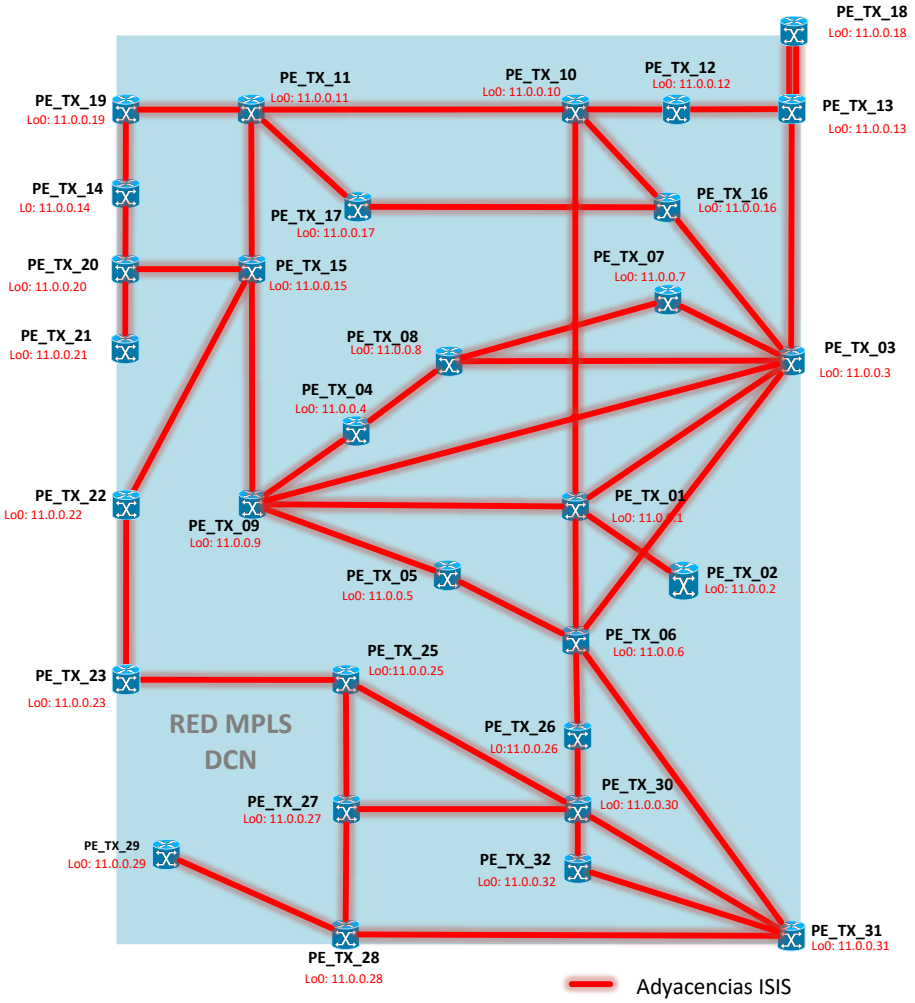


Figura 3.15 Sit. Inicial MPLS DCN: – Adyacencias IGP IS-IS (Fuente: Elab. Propia)

En la tabla C.1 del Anexo C se muestra la lista de adyacencias IS-IS encontradas en los enrutadores PE de la MPLS DCN.

c) Protocolo de Distribución de etiquetas MPLS:

De características similares a la MPLS GOB, la red MPLS DCN utiliza LDP como protocolo de distribución de etiquetas:

- Usa interfaces lógicas *loopback* (bucle de retorno) como *router-id*
- Los modos de trabajo utilizados para LDP en esta red son:
  - ✓ Modo de distribución de etiquetas: no solicitadas en sentido descendente o UD
  - ✓ Modo de retención de liberal o LLR
  - ✓ Modo de control LSP independiente
- Las adyacencias de LDP están autenticadas.
- Se permiten la formación de adyacencias remotas mediante mensajes *Hello* dirigidos.

En el Anexo C, tabla C.1 muestra la lista de adyacencias LDP formadas entre los enrutadores PE de la red MPLS DCN, mientras que el diagrama de adyacencias LDP en mostrado en la figura 3.16.

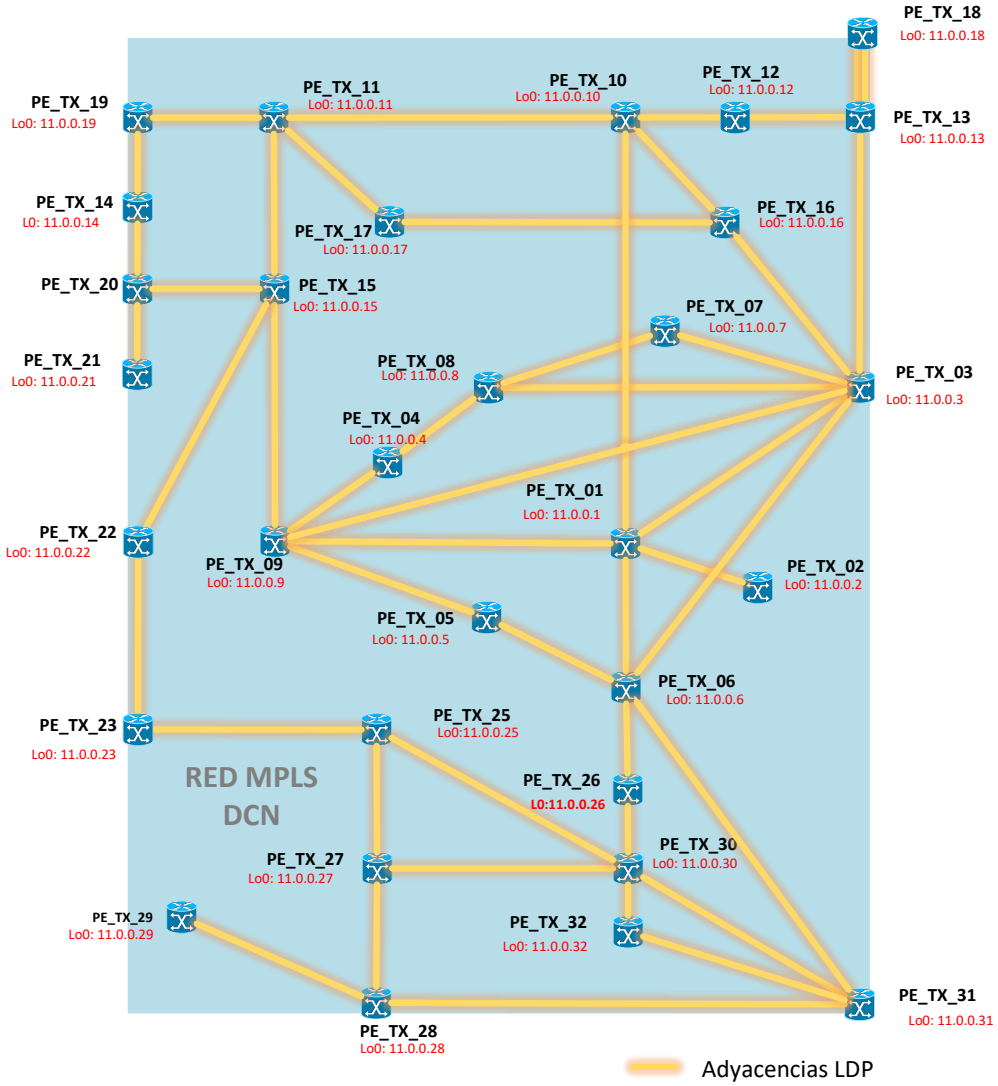


Figura 3.16 Situación Inicial MPLS DCN: Adyacencias LDP (Fuente: Elab. Propia)

d) Sesiones BGP:

Las funciones de reflector de ruta de BGP recaen en PE_TX_03 y PE_TX_06. El sistema autónomo considerado es de tipo privado (65002). Las sesiones BGP se establecen utilizando las interfaces *loopback* habilitando las familias correspondientes a IPv4 (AFI 1 y SAFI 1) y VPNv4 (AFI 1 y SAFI 128).

Las sesiones BGP entre los PE y los RRs de la MPLS DCN son listadas en el Anexo C Tabla C.2 y se muestran gráficamente en la figura 3.17:

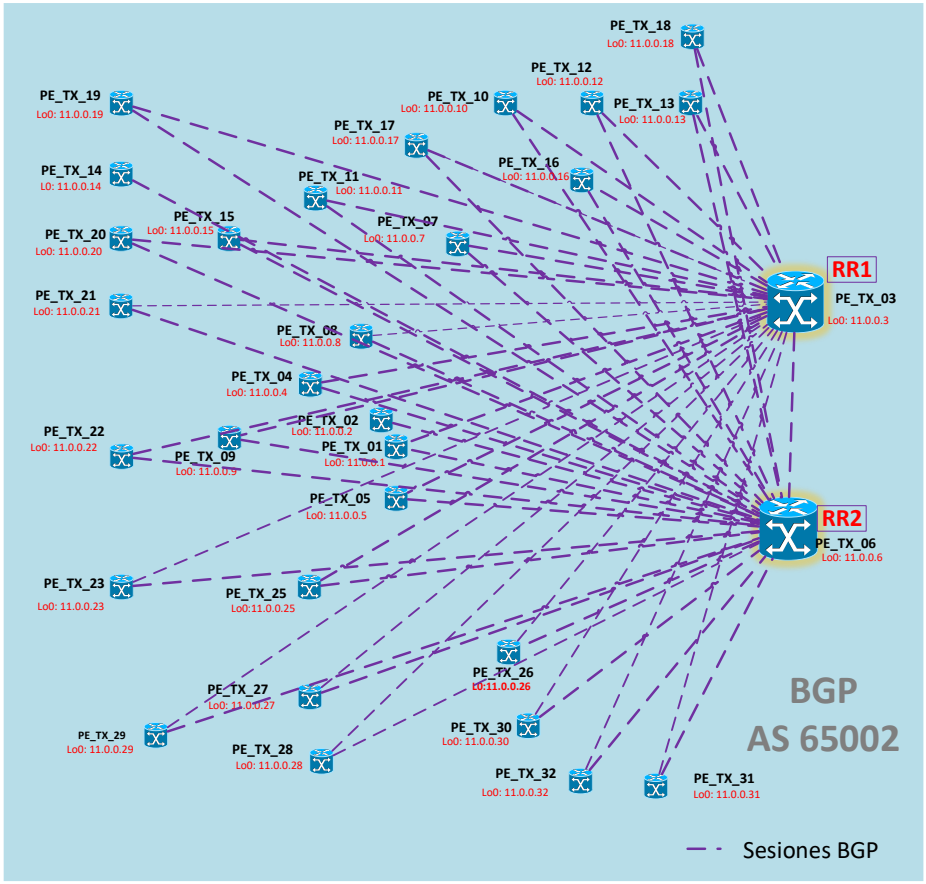


Figura 3.17. Sit. Inicial MPLS DCN: Sesiones BGP - PEs y RRs (Fuente: Elab. Propia)

3.1.5. Acceso MPLS y LAN DCN:

a) VRF

Las VRF's creadas para separar el tráfico de gestión segmentan el enrutamiento por tipo de plataforma/fabricante de los equipos de Transmisión existentes en la red. En la tabla 3.7 se muestran las VRFs existentes y sus valores de RD y RT *Import*, *Export*.

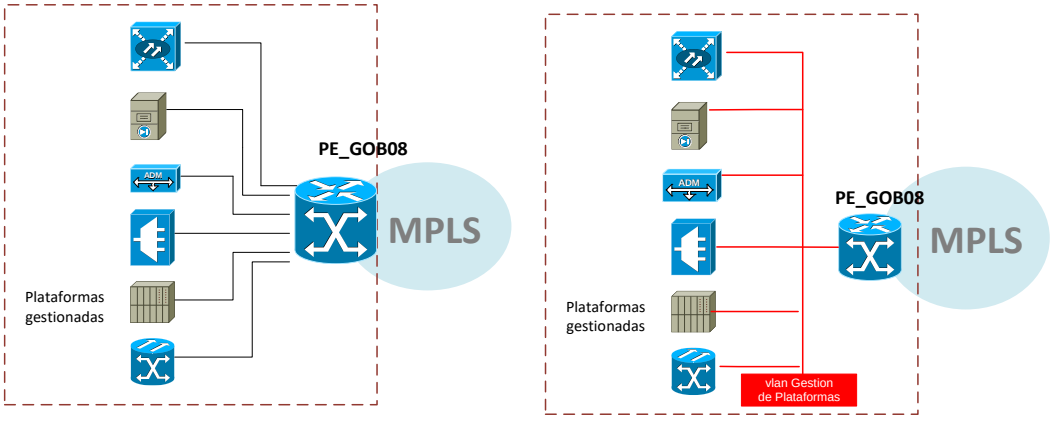
Tabla 3.7 Sit. Inicial MPLS DCN: VRFs (Fuente: Elab. propia)

Tipo de Red de Gestión	VRF	RD	RT	
			Import	Export
Gestión Equipos Fabricante Huawei	vrf_DCN_1	65002:1	65002:1	65002:1
Gestión Equipos Fabricante Alcatel	vrf_DCN_2	65002:2	65002:2	65002:2
Gestión Equipos Plataformas Radio	vrf_DCN_3	65002:3	65002:3	65002:3
….	…	..	65002:4	65002:4
Gestión Equipos Fabricante 10	vrf_DCN_10	65002:10	65002:10	65002:10

b) Red de Acceso MPLS y LAN:

La red de acceso MPLS y LAN están colapsadas sobre el mismo enrutador. En los nodos DCN los enrutadores tienen la capacidad de funcionar como conmutador de acceso a través de tarjetas de línea insertadas en el equipo. A nivel lógico, todas las plataformas

utilizan como puerta de enlace al enrutador de borde PE/CE y están sobre la misma VLAN de gestión, como se observa en la figura 3.18.



a) Topología Física b) Topología Lógica

Figura 3.18 Situación Inicial MPLS DCN: Acceso MPLS y LAN (Fuente: Elab. Propia)

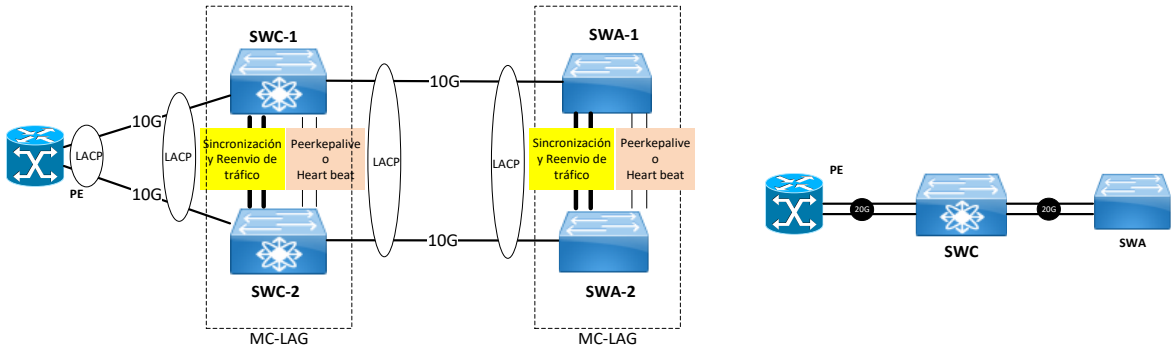
3.2. Solución propuesta

3.2.1. Red MPLS

Resultado del análisis realizado sobre ambas redes MPLS se decide fusionar ambas redes MPLS y mejorar las tecnologías de acceso LAN tomando en cuenta lo siguiente:

a) Conmutadores en nodos Primarios:

Se utiliza MC-LAG para implementar la redundancia y alta disponibilidad en los conmutadores de concentración y acceso usando enlaces agregados de puertos ubicados en diferentes chasis. Según lo que se detalló en la capitulo II, los requerimientos físicos para la implementación de MC-LAG pueden varias según el fabricante, pero por lo general consisten en al menos un cable adicional entre los chasis de ambos equipos para sincronizar la información de los protocolos y envío de tráfico entre ambos equipos, y otro a modo de keepalive para monitorear ambos equipos y evitar un escenario de dual-active. Con motivo de redundancia, se utilizarán dos cables por cada uno de estos. Las topologías física y lógica tipo son observadas en la figura 3.19.



a) Topología Física b) Topología Lógica

Figura 3.19 Topologías física y lógica tipo MC-LAG (Fuente: Elab. propia)

b) Enrutadores MPLS

A fin de optimizar recursos, se decide integrar las funciones de los enrutadores PE's GOB en los PE's DCN. Esto debido a que la red DCN cuenta con mayor cantidad de enrutadores MPLS desplegados en ubicaciones que corresponden con los nodos principales de la red de Transmisiones, que es la que provee los enlaces físicos, salvo estas excepciones:

- PE_GOB_04 debe mantenerse para contar con geo redundancia, puesto que tanto PE_TX_01 como PE_TX_02 se encuentran en el mismo nodo. Este equipo pasará a llamarse PE_TX_33
- PE_GOB_08 debe mantenerse puesto que la red DCN no cuenta con un punto de presencia en este lugar. Este equipo pasará a llamarse PE_TX_34.
- PE_GOB_02 es retirado debido a que el nodo en que fue instalado dejara de funcionar. Sus capacidades serán migradas hacia PE_TX_08 que es el más cercano geográficamente.

Las conexiones internodales entre conmutadores de los nodos principales de la ciudad de Lima son conservadas para mantener la posibilidad de extender las VLANs entre puntos de presencia contiguos. A nivel jerárquico los equipos seguirán formando en una red Core/Acceso MPLS colapsada de enrutadores PE's.

En la tabla 3.8 se muestran las migraciones a ejecutar por cada enrutador PE en la Integración de las redes MPLS.

Tabla 3.8 Solución propuesta: Migración PEs GOB a PE DCN (Fuente: Elab. propia)

PE Origen			PE Destino		
PoP	Sala	Nodos	PoP	Sala	Nodos
Surquillo	Datos 1	PE_GOB_03	Surquillo	Transmisiones	PE_TX_01
Washington	Datos	PE_GOB_01	Washington	Transmisiones	PE_TX_03
La Victoria	Celular	PE_GOB_05	La Victoria	Transmisiones	PE_TX_07
San Isidro 2	Celular	PE_GOB_06	San Isidro 2	Transmisiones	PE_TX_08
Monterrico	Datos	PE_GOB_07	Monterrico	Transmisiones	PE_TX_09
Trujillo	Datos	PE_GOB_09	Trujillo	Transmisiones	PE_TX_10
Arequipa	Datos	PE_GOB_10	Arequipa	Transmisiones	PE_TX_30
Miraflores	Datos	PE_GOB_08	DCN no cuenta con este POP, se debe mantener. El equipo pasará a llamarse PE_TX_34		
Surquillo	Datos 2	PE_GOB_04	Se mantiene para contar con geo redundancia. El equipo pasará a llamarse PE_TX_33		
San Isidro 1	Datos	PE_GOB_02	Se dará de baja (fusionar con PE_TX_08)		

c) Enlaces físicos:

La capacidad de enlaces internodales 1G es ampliada a 10G vía fibra óptica directa entre los nodos principales de Lima para mejorar la capacidad actual de la red y permitir crecimiento a futuro de los servicios de gestión. Los enlaces y SFP a utilizar para los nuevos

enlaces 10G intermodal cumplen con las normas: 10GBASE-SR (enlaces hasta 400m en Multi-Mode OM4), 10GBASE-LR (10Km) o 10GBASE-ER (40Km) según a la distancia entre las ubicaciones físicas de los enrutadores.

En la figura 3.20 se muestra la topología resultante en los nodos primarios.

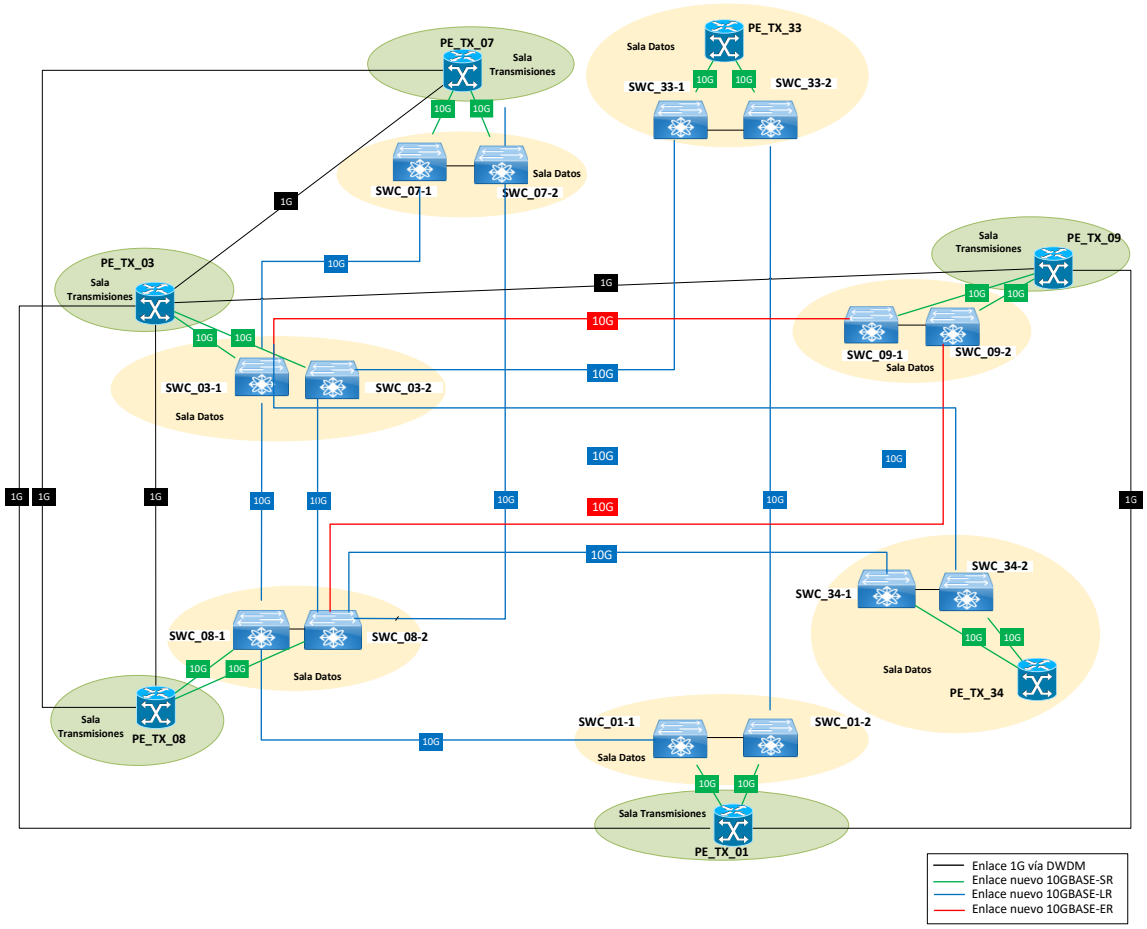


Figura 3.20. Topología Física propuesta en nodos primarios (Fuente: Elab. propia)

Se instalan nuevos enlaces 1G entre PE_TX_10 y PE_TX_30 hacia los conmutadores de concentración: SWC_03-1, SWC_03-2, SWC_08-1, SWC_08-2 cuyo transporte será la red DWDM y a utilizarse en las adyacencias de ISIS y LDP con PE_TX_03 y PE_TX_08.

Otros nodos conservarán los enlaces 1G de la MPLS DCN, cuyo transporte es usa una red de transmisiones DWDM. La relación de nuevos enlaces requeridos para la conectividad en base a la distancia entre nodos es mostrada en el Anexo D, tabla D.1.

En la figura 3.21 se muestra la topología resultante con los nuevos enlaces 1G en PE_TX_10 y PE_TX_30.

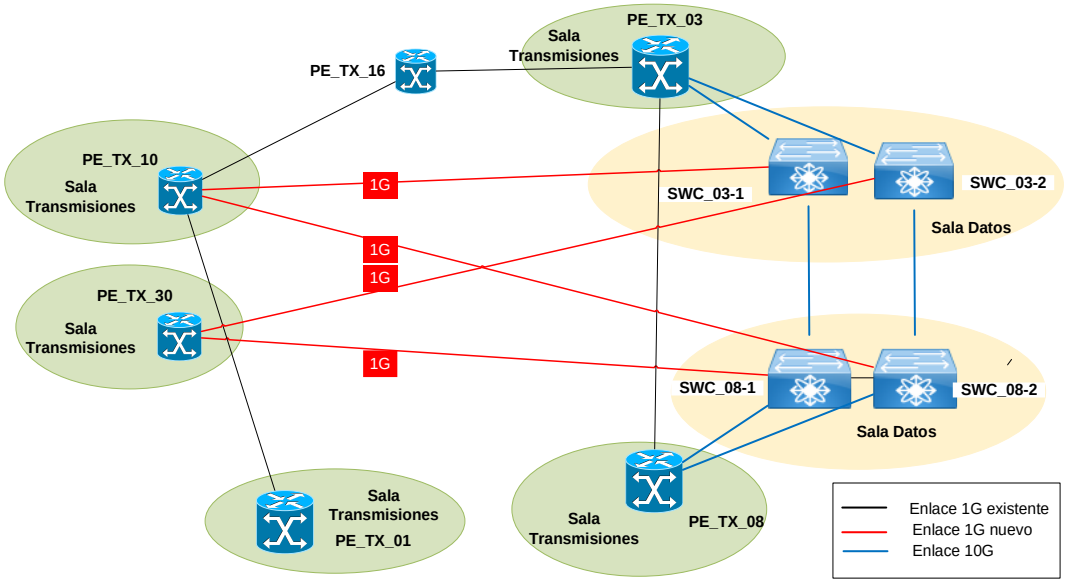


Figura 3.21. Topología propuesta: Nuevos enlaces 1G en PE_TX_10 y PE_TX_30 (Fuente: Elab. propia)

d) IGP:

El protocolo de enrutamiento interno elegido es IS-IS en jerarquía de nivel 2, homologando las direcciones NET, los parámetros de autenticación MD5 por interfaz/área y los temporizadores que controlan los paquetes hello (para el mantenimiento de las adyacencias), el comportamiento de los LSP y del algoritmo SPF. En el Anexo D, Tabla D.2 se indican los Router-ID y las direcciones NET de IS-IS a utilizar en los PE.

El análisis de métricas IS-IS toma en cuenta estos lineamientos:

- La elección de los nodos principales está relacionada con la ubicación geográfica de nodos de la red MPLS GOB más importantes, siguiendo una topología que ya es conocida para la identificación de fallas en la red de servicios.
- Las adyacencias de IS-IS en los nodos principales se realiza a través de VLANs extendida permitiendo simular conexiones punto a punto según lo mostrado en la figura 3.22.
- El tráfico debe transmitirse a través de los enlaces 10G en lugar de los enlaces 1G siempre que sea posible, de forma que los enlaces 1G queden como respaldo de los enlaces 10G.
- El tráfico debe enviarse a través de enrutadores que tengan la menor distancia geográfica incluso cuando tengan la misma cantidad de saltos intermedios hacia los nodos principales.
- Las métricas de IS-IS se asignan de manera simétrica en ambos sentidos de cada enlace buscando usar valores comunes. En este caso se usarán: 10, 50 y 20.

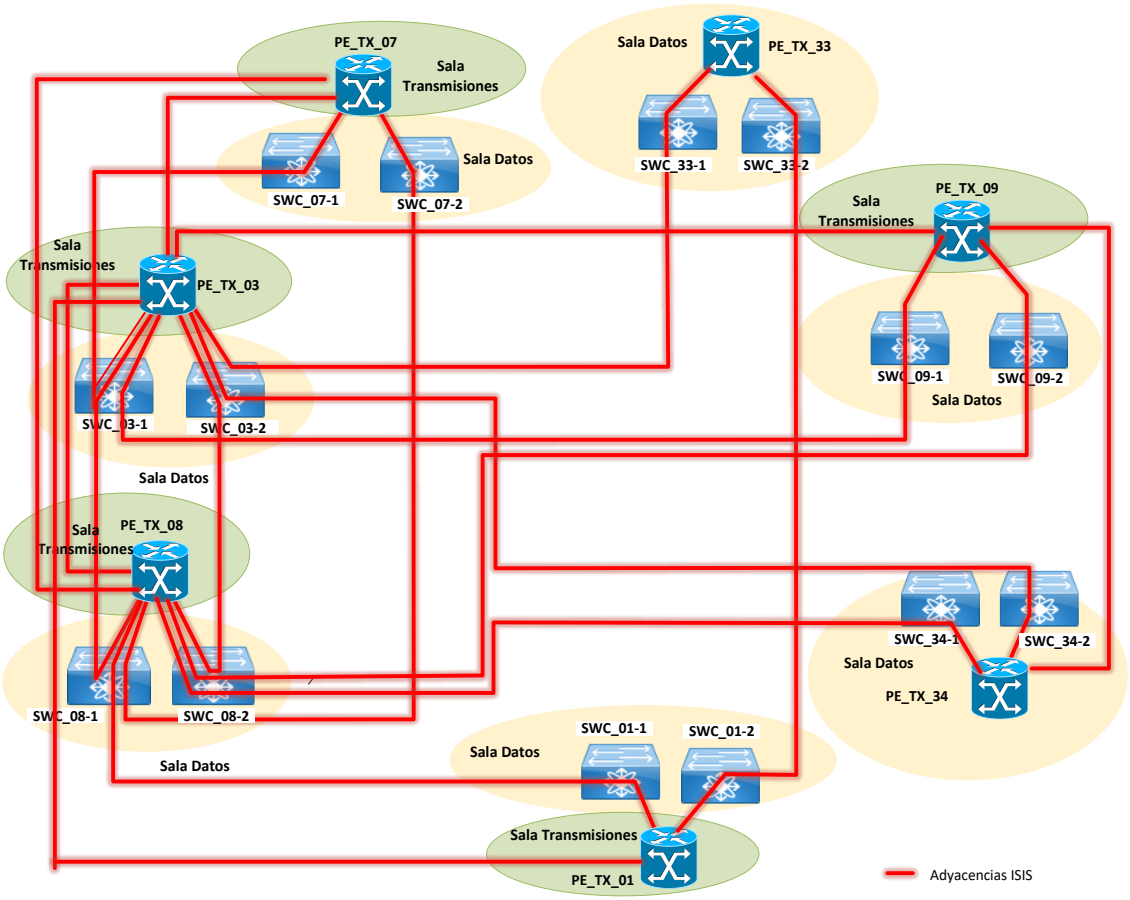


Figura 3.22. Solución propuesta: Topología adyacencias IS-IS (Fuente: Elab. propia)

En la figura D.1 del Anexo D se muestra la topología de IS-IS con las métricas resultado del análisis realizado.

e) VLANs MPLS

Se define un rango (1200-1299) para la asignación de VLANs que simulan conexiones punto a punto en los nodos primarios para llevar las sesiones IS-IS. Estas VLANs deben ser extendidas únicamente entre las troncales que las necesiten y filtrados en cualquier otra troncal. La topología de árbol de STP para estas VLANs no cuenta con la definición específica de un root STP, y se prefiere utilizar el algoritmo STP para la elección del mejor candidato (mejor Bridge-id). En la figura 3.23 se muestra las VLANs utilizadas para simular los enlaces punto a punto:

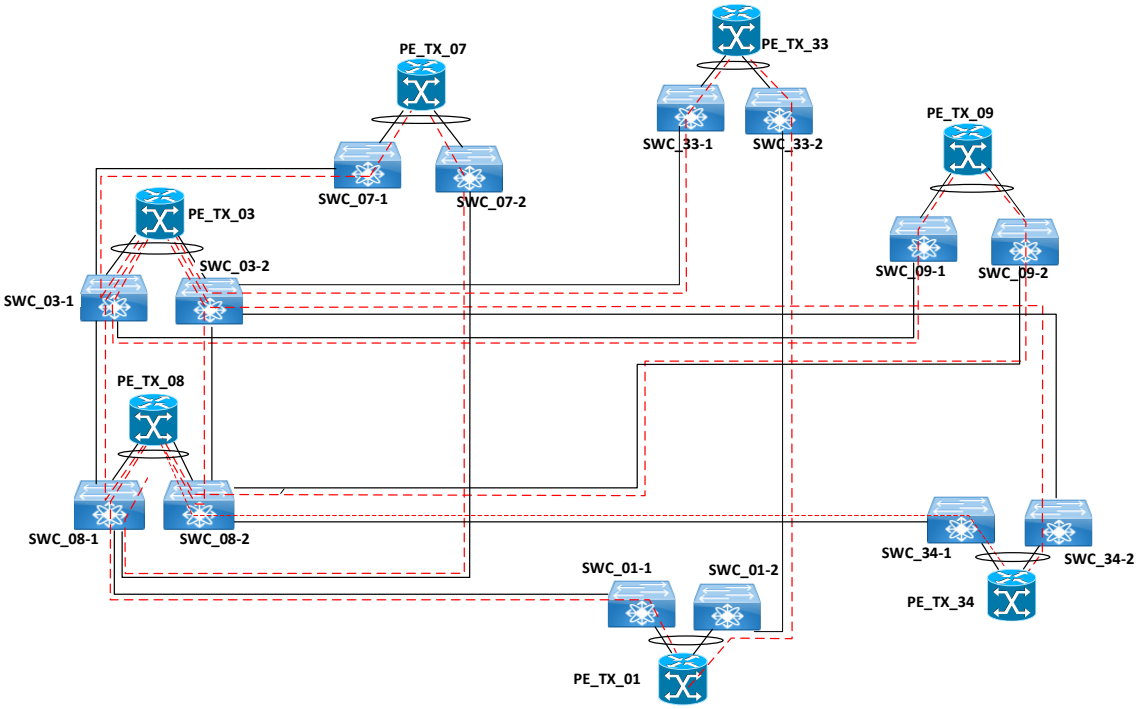


Figura 3.23. Solución propuesta: Topologías VLANs MPLS IS-IS (Fuente: Elab. propia)

En la tabla 3.9 se lista las VLANs consideradas para adyacencias IS-IS en nodos primarios.

Tabla 3.9 Solución propuesta: VLANs adyacencias IS-IS - nodos primarios (Fuente: Elab. propia)

PE Origen	PE Destino	VLAN	Tipo
PE_TX_03	*PE_TX_08*	1201	p2p-wan-isis
PE_TX_03	*PE_TX_33*	1202	p2p-wan-isis
PE_TX_03	*PE_TX_07*	1203	p2p-wan-isis
PE_TX_03	*PE_TX_09*	1204	p2p-wan-isis
PE_TX_03	*PE_TX_34*	1205	p2p-wan-isis
PE_TX_01	*PE_TX_08*	1206	p2p-wan-isis
PE_TX_01	*PE_TX_33*	1207	p2p-wan-isis
PE_TX_07	*PE_TX_08*	1208	p2p-wan-isis
PE_TX_08	*PE_TX_09*	1209	p2p-wan-isis
PE_TX_08	*PE_TX_34*	1210	p2p-wan-isis

La topología resultante del protocolo de enrutamiento interno IS-IS luego de aplicar estos cambios en la nueva red MPLS es mostrada en la figura 3.24.

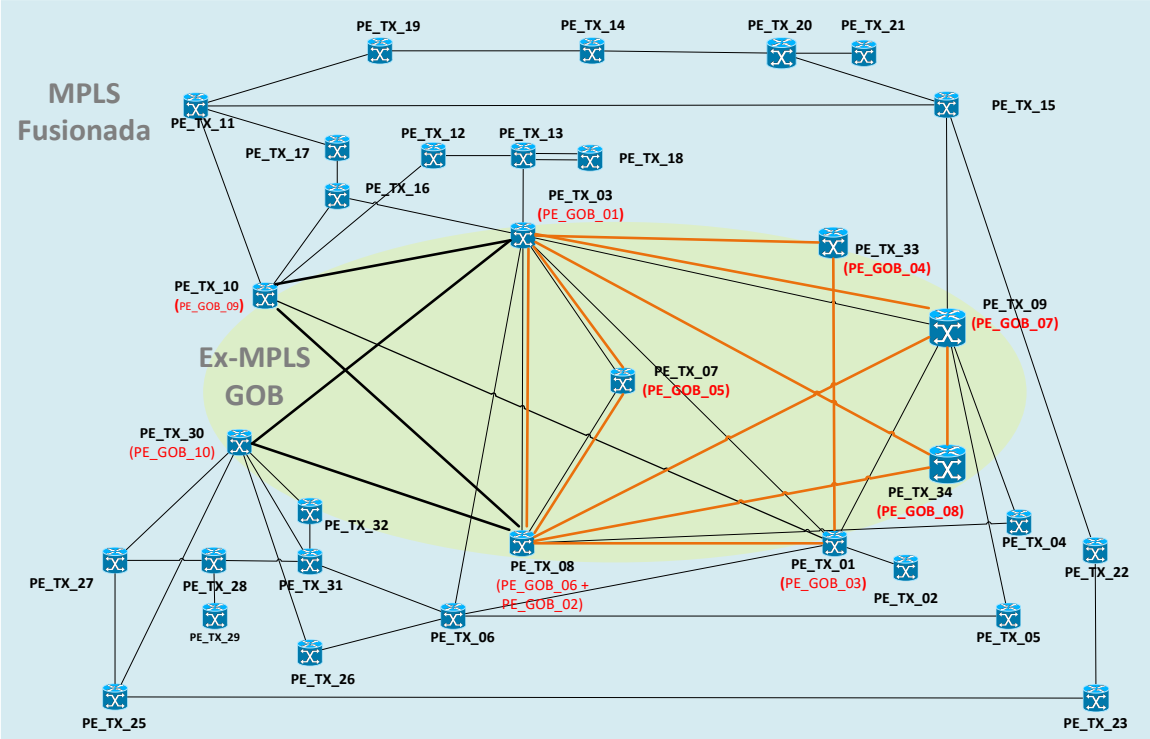


Figura 3.24. Solución propuesta: IS-IS resultante MPLS Fusionada (Fuente: Elab. propia)

f) Protocolo de Distribución de etiquetas MPLS:

Se utiliza LDP como protocolo de distribución de etiquetas homologando los parámetros de configuración ya descritos en las secciones 3.1.1 y 3.1.4.

- Usa interfaces lógicas *loopback* (bucle de retorno) como router-id
- Los modos de trabajo utilizados para LDP en esta red son:
  - ✓ Modo de distribución de etiquetas: no solicitadas en sentido descendente o UD
  - ✓ Modo de retención de liberal o LLR
  - ✓ Modo de control LSP independiente
- Las adyacencias de LDP deben estar autenticadas.
- Se permitirá la formación de adyacencias remotas mediante mensajes Hello dirigidos.

En el Anexo D, tabla D.3 muestra la lista de adyacencias LDP formadas entre los enrutadores PE de la red MPLS DCN, mientras que en la figura 3.25 se muestra el diagrama de adyacencias LDP.

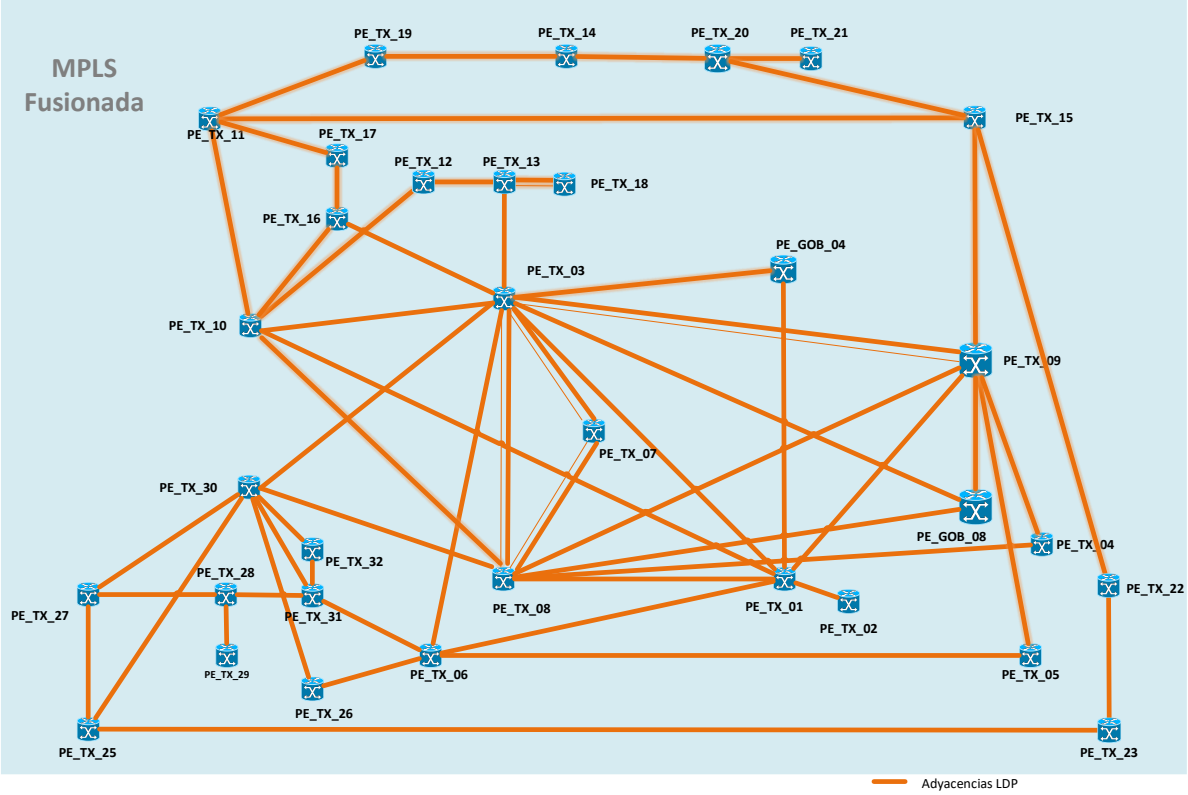


Figura 3.25 Solución propuesta: Adyacencias LDP (Fuente: Elab. propia)

g) BGP:

La función de reflector de rutas de BGP se traslada hacia PE_TX_03 y PE_TX_08 por su ubicación céntrica en las topologías MPLS resultante a nivel lógico/geográfico. Se utiliza el sistema autónomo de la MPLS GOB (AS 65001) debido a que su utilización no impacta a las sesiones BGP existentes con los enrutadores CE, evitando la necesidad de realizar cambios en estos enrutadores. Las sesiones BGP se establecen entre las interfaces *loopback* asignadas a cada enrutador dejando habilitadas las familias IPv4 y VPNV4. Adicionalmente, se implementan reflectores de ruta regionales para las zonas: Norte-Centro (en PE_TX_10) y Sur (en PE_TX_30) que servirán de contingencia en situaciones de desastre o *disaster recovery*) ante la pérdida de conectividad de los PE remotos de provincias con los RR de Lima.

Los enrutadores PE's tendrán 03 sesiones BGP: 02 con los reflectores de rutas de Lima además de 01 sesión BGP con su correspondiente RR regional. La relación total de sesiones BGP a implementar es listada en el Anexo D Tabla D.4. En la figura 3.26 se muestra el esquema de sesiones BGP para los PE y sus reflectores de ruta.

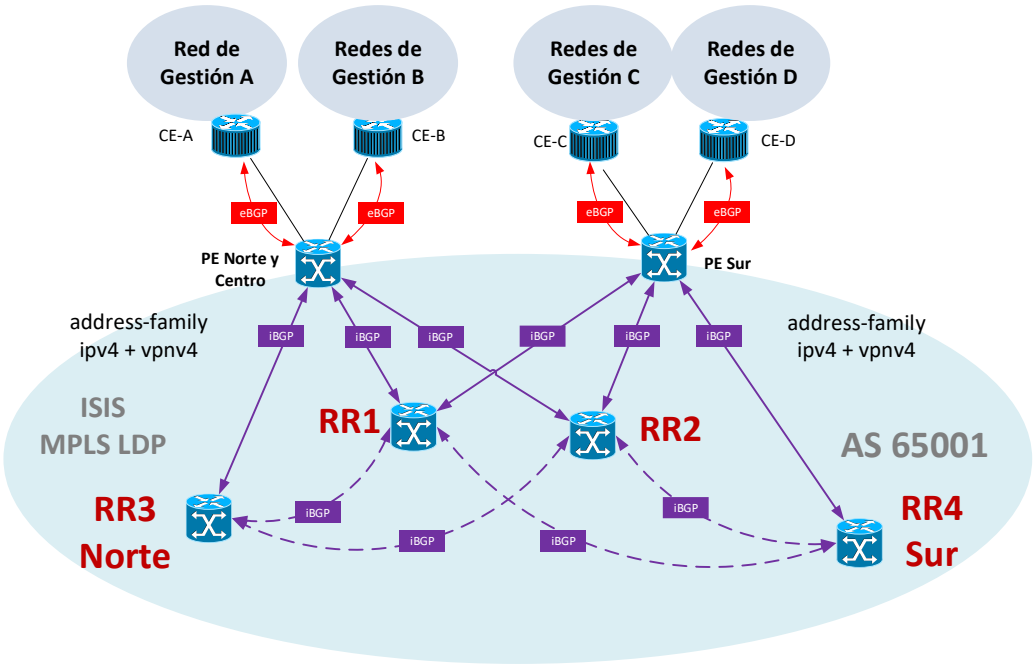


Figura 3.26 Solución propuesta: Sesiones BGP por PE (Fuente: Elab. propia)

En la figura 3.27 se muestra el diagrama de sesiones BGP resultante entre los enrutadores PE y los RR PE-TX_01 y PE_TX_08.

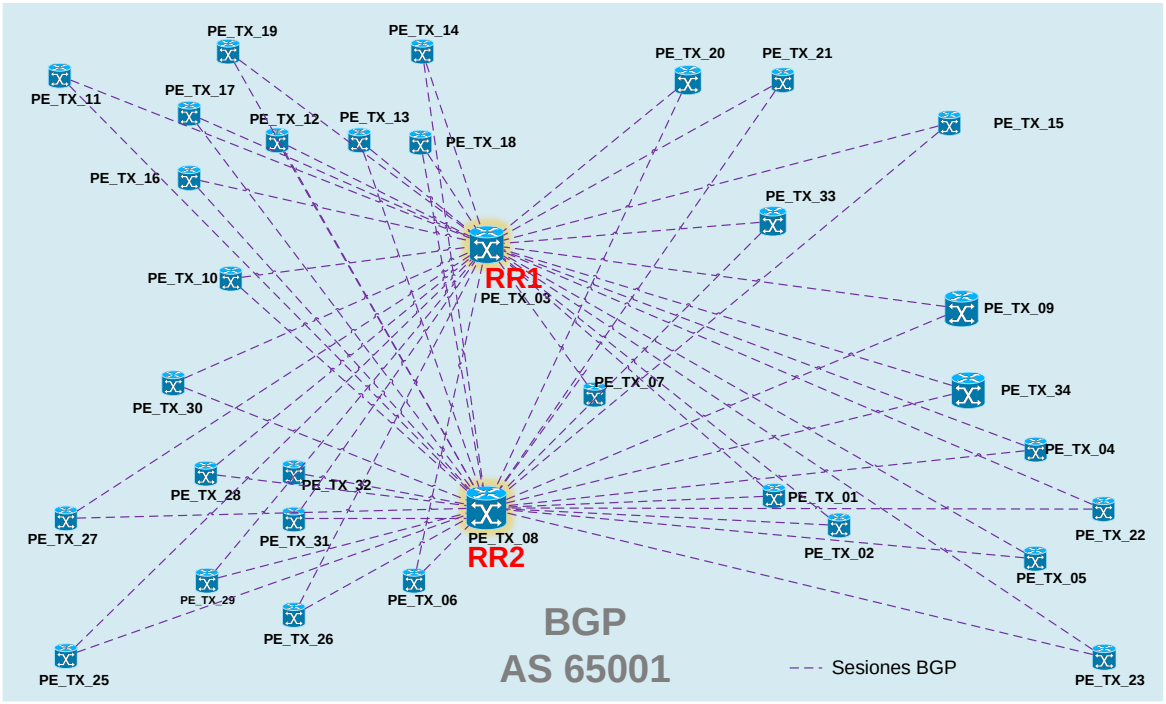


Figura 3.27 Solución propuesta: Adyacencias BGP (Fuente: Elab. propia)

En la figura 3.28 se muestra las sesiones BGP entre los enrutadores PE y los RR regionales Norte y Sur, obviando las sesiones con los RR1 y RR2 Lima.

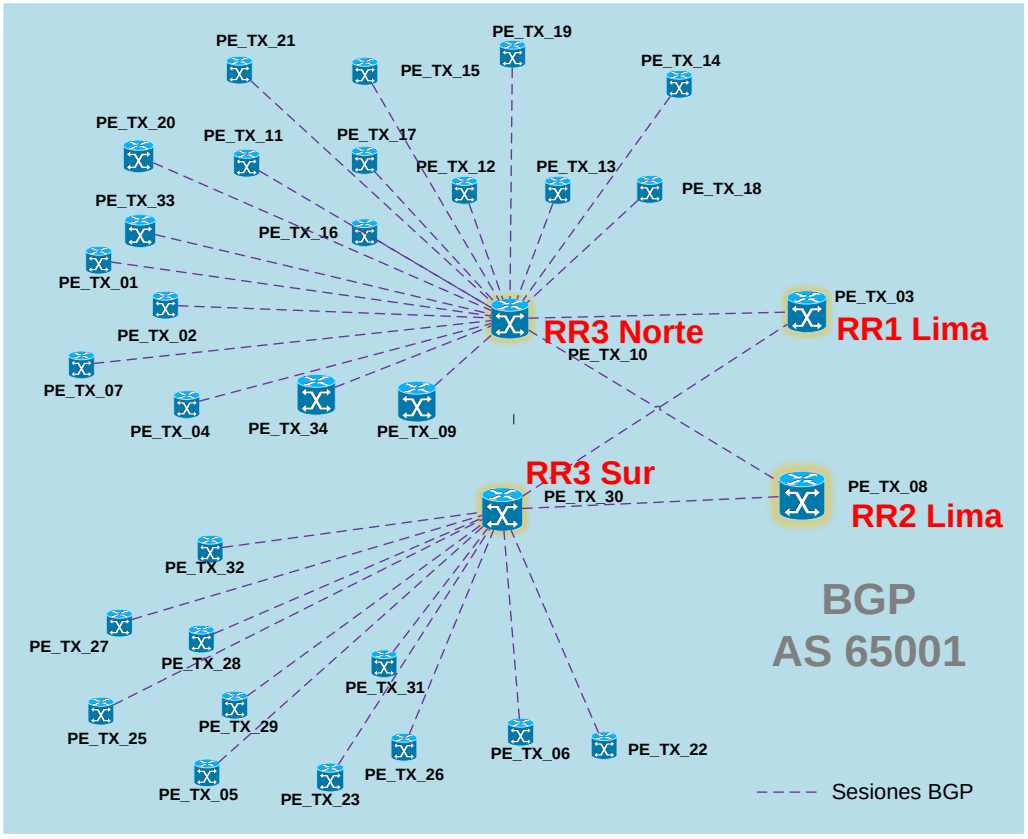


Figura 3.28 Solución propuesta: Sesiones BGP con RR Norte y Sur (Fuente: Elab. propia)

3.2.2. Acceso MPLS

a) VRFs:

Las instancias de enrutamiento, VRFs, existentes no serán modificadas de forma que los servicios de gestión y el tráfico se siga comportando de la misma manera. Por tanto, los enlaces que se encuentren en los PE a darse de baja se migran a enrutadores PE que consolidan todos los enlaces y VRFs a las que pertenecen. En la figura 3.29 se muestra un enrutador PE_TX de la MPLS Fusionada que consolida las VRF's GOB y DCN.

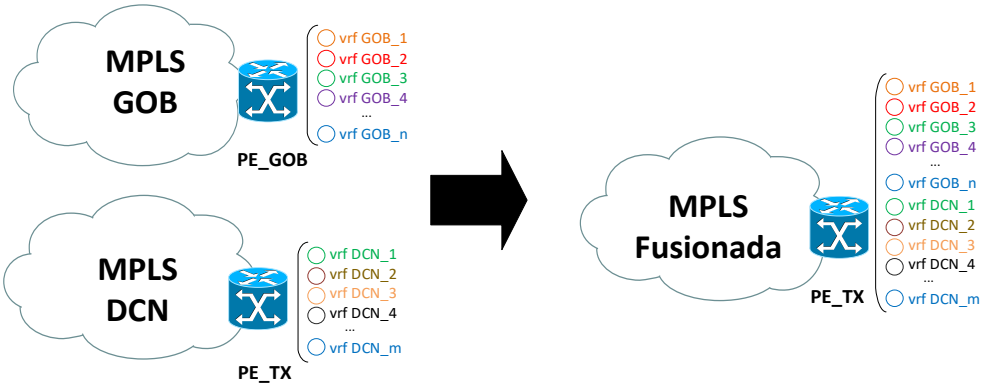
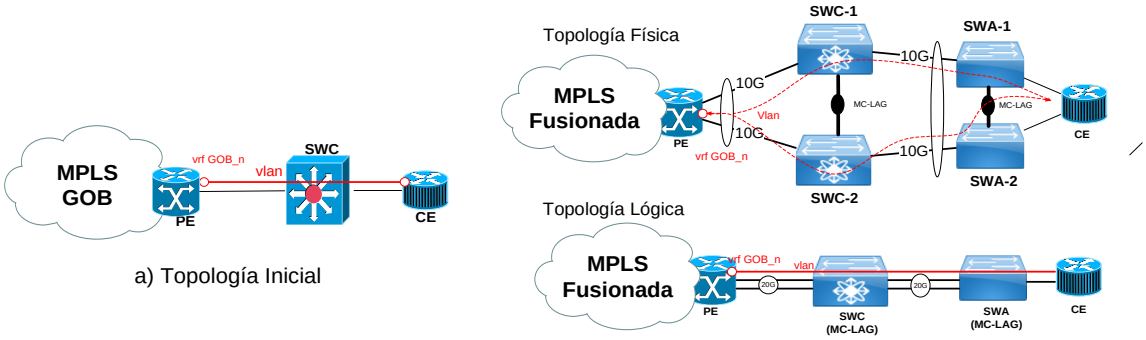


Figura 3.29 Integración de VRFs – GoB y DCN (Fuente: Elab. propia)

b) Acceso PE-CE:

Los escenarios observados son migrados tomando en cuenta la mejor distribución de enlaces para contar con alta disponibilidad del servicio.

- **PE y CE interconectados a través de una VLAN extendida**. En este escenario, se reemplaza el conmutador existente por un par de conmutadores usando MC-LAG. En los nodos primarios se añaden también conmutadores de acceso con MC-LAG. El comportamiento lógico de este escenario es el equivalente a la inicial, pero implementado redundancia y mayor capacidad de enlaces logrando anchos de banda de hasta 20G. En la figura 3.30 se muestran la topología inicial y final de conexiones PE-CE.



a) Topología Inicial

b) Topología Final

Figura 3.30 Solución propuesta: conexión PE-CE mediante VLAN (Fuente: Elab. propia)

- **PE y CE interconectados a través de enlaces físicos TDM.** En los casos donde existe un enrutador PE cercano geográficamente a un CE, se migran los enlaces PE-CE con TDM E1 hacia enlaces ethernet 1Gbps conectados a PE's más cercanos. En la tabla 3.10 se muestra la lista de nuevos enlaces, que se migran bajo este criterio de optimización:

Tabla 3.10 Solución propuesta: Enlaces PE-CE migrados a Ethernet (Fuente: Elab. propia)

CE	SWC	PE	Tipo	BW
CE_GOB11_1	SWC_30	PE_TX_30	Ethernet	1Gbps
CE_GOB12_1	SWC_30	PE_TX_30	Ethernet	1Gbps
CE_GOB13_1	SWC_10	PE_TX_10	Ethernet	1Gbps
CE_GOB14_1	SWC_10	PE_TX_10	Ethernet	1Gbps
CE_GOB15_1	SWC_34	PE_TX_34	Ethernet	1Gbps
CE_GOB16_1	-	PE_TX_08	E1 Datos	2048 kbps
CE_GOB16_1	-	PE_TX_07	E1 Datos	2048 kbps
CE_GOB17_1	-	PE_TX_08	E1 Datos	2048 kbps
CE_GOB17_1	-	PE_TX_07	E1 Datos	2048 kbps

La topología final propuesta es mostrada en el Anexo D, figura D.2:

c) Enrutamiento PE-CE:

Los protocolos de enrutamiento PE-CE existentes se migran a los enrutadores PE_TX. Los tipos de enrutamiento a utilizar son descritos a continuación.

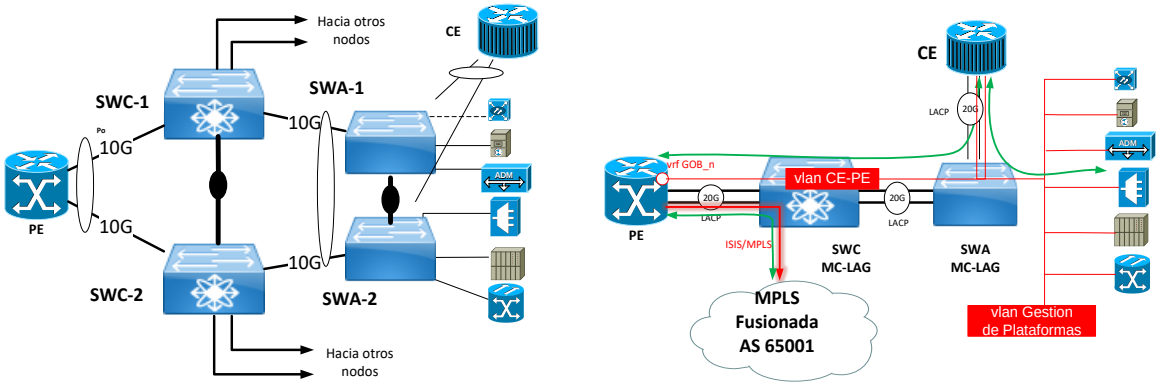
- **BGP**, al mantenerse el sistema autónomo utilizado en la MPLS GOB (AS 65001) se puede conservar, sin alterar, los sistemas autónomos utilizados en cada CE al igual que las políticas configuradas en cada uno de ellos.
- **Enrutamiento Estático,** se mantiene la configuración (siguiente salto, rótulos y configuración de interfaz de salida).

3.2.3. Acceso LAN:

En este bloque se consideran los escenarios posibles de optimización en los nodos utilizando un modelo jerárquico de Core/Distribución colapsado en los conmutadores de acceso.

a) Nodos Primario:

En los nodos primarios se implementa una jerarquía de conmutadores de concentración y acceso. Las conexiones físicas de las plataformas gestionadas son conectadas directamente a los conmutadores de acceso. Los enlaces entre los equipos conmutadores de concentración, acceso, enrutadores PE y CE utilizan MC-LAG y LACP para realizar la agregación de enlaces de 10G a un solo enlace lógico 20G. A nivel lógico, la puerta de enlace se mantiene en el CE, que mantiene conectividad con el PE a través de una VLAN extendida a través del conmutador de concentración. En la figura 3.31 se muestran la topología física y lógica de acceso LAN en un nodo primario.



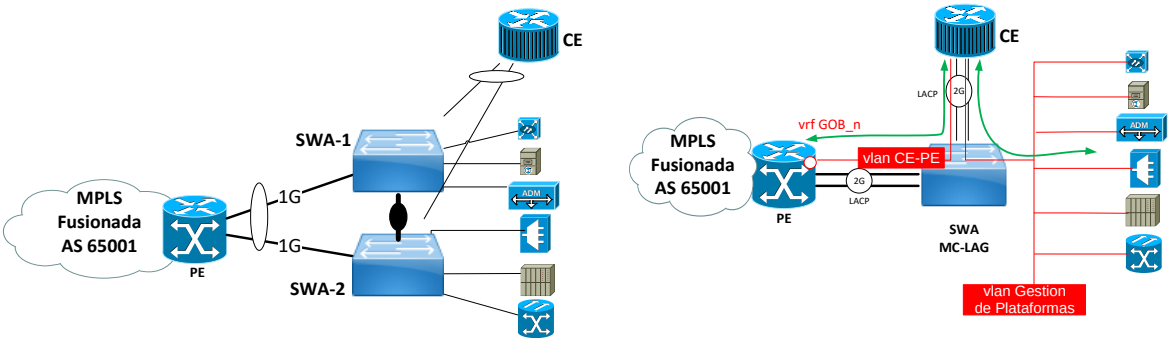
a) Topología Física b) Topología Lógica

Figura 3.31 Solución propuesta: Topologías a) física y b) lógica – Acceso LAN Nodo primario (Fuente: Elab. propia)

b) Nodo Secundario:

En nodos secundarios, las conexiones físicas de las plataformas gestionadas son conectadas directamente a los conmutadores de acceso que cuentan con enlaces directos

al PE del nodo donde se encuentran. Los conmutadores de acceso usan MC-LAG y LACP siempre que sea posible (la implementación de los conmutadores de acceso con MC-LAG están fuera del alcance del proyecto). A nivel lógico, la puerta de enlace se mantiene en el CE, que mantiene conectividad con el PE a través de una VLAN. En la figura 3.32 se muestra las topologías física y lógica de acceso en nodos secundarios usando MC-LAG.



a) Topología Física b) Topología Lógica

Figura 3.32 Solución propuesta: a) Topologías física y b) lógica acceso LAN nodo secundario (Fuente: Elaboración propia)

c) Nodos DCN:

Los nodos DCN que cuentan conexiones físicas directas al enrutador, se convierten en nodos secundarios manteniendo la misma topología de conexión vía un conmutador de acceso con MC-LAG. La implementación de los conmutadores de acceso para los nodos DCN están fuera del alcance del proyecto.

d) Nodos Remotos:

Los nodos remotos no sufren variación en el modo de acceso LAN, manteniendo la misma topología de acceso LAN mediante un conmutador de acceso y una puerta de enlace en el enrutador CE.

e) Centro de Datos:

En los centros de datos se implementa una topología redundante de conmutadores de concentración con conexiones físicas hacia los firewalls y conmutadores de acceso con MAC-LAG. A nivel lógico, la alta disponibilidad incluye la utilización de un protocolo FHRP en los enrutadores de borde PE MPLS con siguiente salto en el clúster de firewalls, para proveer la capa de seguridad alta y servir también como puerta de enlace de las VLANs de servidores. Los enlaces entre conmutadores de concentración y acceso, enrutadores PE y CE utilizan LACP para realizar la agregación de enlaces de 10G a un solo enlace lógico 20G. En la figura 3.33 se muestra las topologías física y lógica de acceso en los centros de datos.

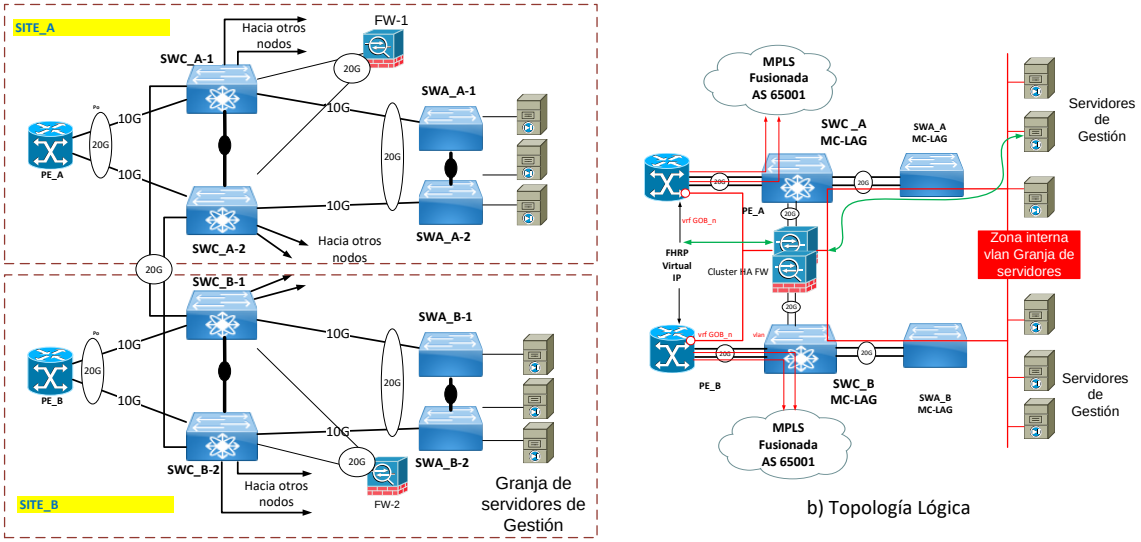


Figura 3.33 Solución propuesta: Topologías a) física y b) lógica acceso LAN Centro de Datos (Fuente: Elaboración propia)

f) Centro de Gestión:

Se implementa una jerarquía de conmutadores de concentración y acceso con MC-LAG. Las conexiones físicas de las plataformas gestionadas son conectadas a los conmutadores de acceso. A nivel lógico la alta disponibilidad incluye la utilización de un protocolo FHRP en los enrutadores de borde PE MPLS conectados a un clúster de firewalls para proveer alta disponibilidad y una capa de seguridad.

En la figura 3.34 se muestra las topologías física y lógica de acceso en el Centro de Gestión.

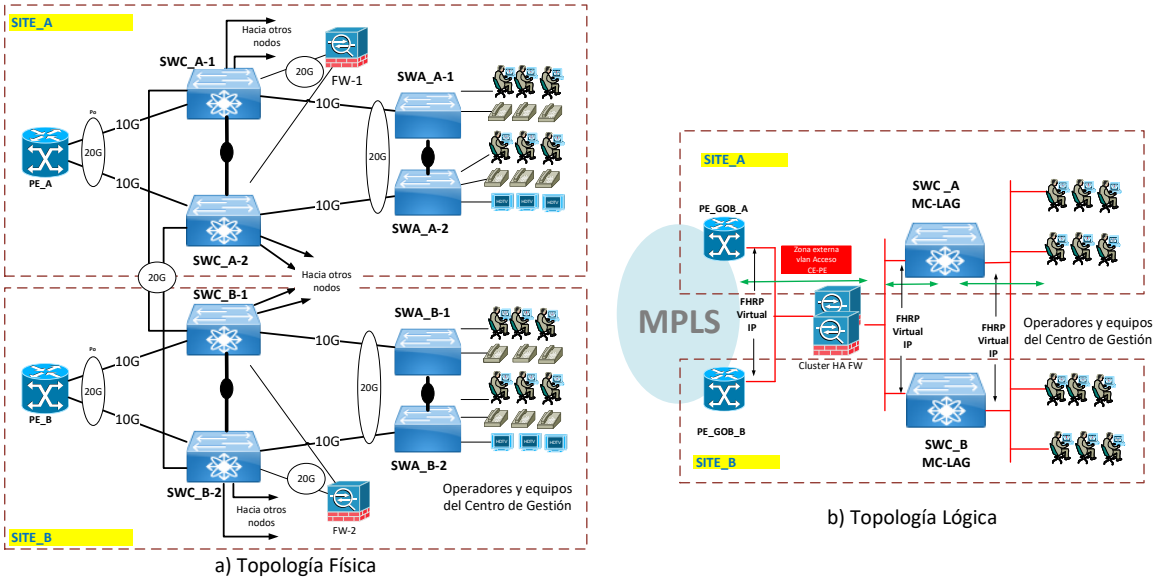


Figura 3.34 Solución propuesta: Topologías a) física y b) lógica acceso LAN Centro de Gestión (Fuente: Elaboración propia)

Los conmutadores de concentración son el siguiente salto en capa 3 usando un protocolo FHRP para proveer una IP virtual como puerta de enlace de las VLANs internas. Los enlaces entre los equipos conmutadores de concentración, acceso, enrutadores PE y CE utilizan LACP logrando enlaces lógicos de 20G.

3.2.4. *Spanning-Tree*:

Esta sección define los lineamientos de configuración de *Spanning-Tree* pues se considera como parte de los requerimientos iniciales la posibilidad de extender las VLANs pertenecientes a los servidores de los Centros de Datos y/o las del Centro de Gestión entre los nodos primarios formando un solo dominio de capa 2. En la figura 3.35, se muestra la topología de capa 2 formada por los conmutadores existentes en los nodos primarios

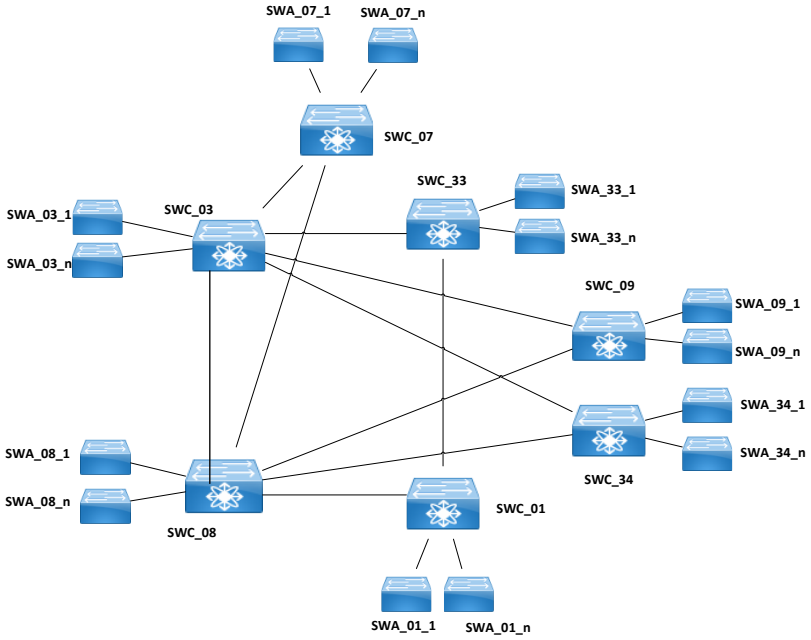


Figura 3.35 Solución propuesta: *Dominio capa 2 en nodos primarios* (Fuente: Elab. propia)

a) VLANs Centro de Datos

En las VLANs de Centro de Datos se elige Raíz del árbol de STP al conmutador SWC_03 y Raíz Secundaría a SWC_08 puesto que los servidores mantienen como puerta de enlace al firewall en modo clúster cuyo chasis con el rol activo se encuentra en SWC_03 y contingencia en SWC_08. Esto permite mantener un flujo de traficó de capa 3 por el camino óptimo hacia la puerta de enlace en la capa 2. Los enlaces redundantes desde conmutadores de concentración remotos son bloqueados de manera automática o manual (utilizando costos configurados sobre las interfaces correspondientes) para contar con la menor cantidad de puntos de paso para llegar a la raíz. En caso de la caída del conmutador raíz de STP, este rol será asumido por la Raíz secundaria SWC_08. En la figura 3.36 se

muestran las topologías de STP incluyendo a los *Root port* y puertos bloqueados bajo estas consideraciones en a) situación normal y b) cuando existe una caída del conmutador raíz.

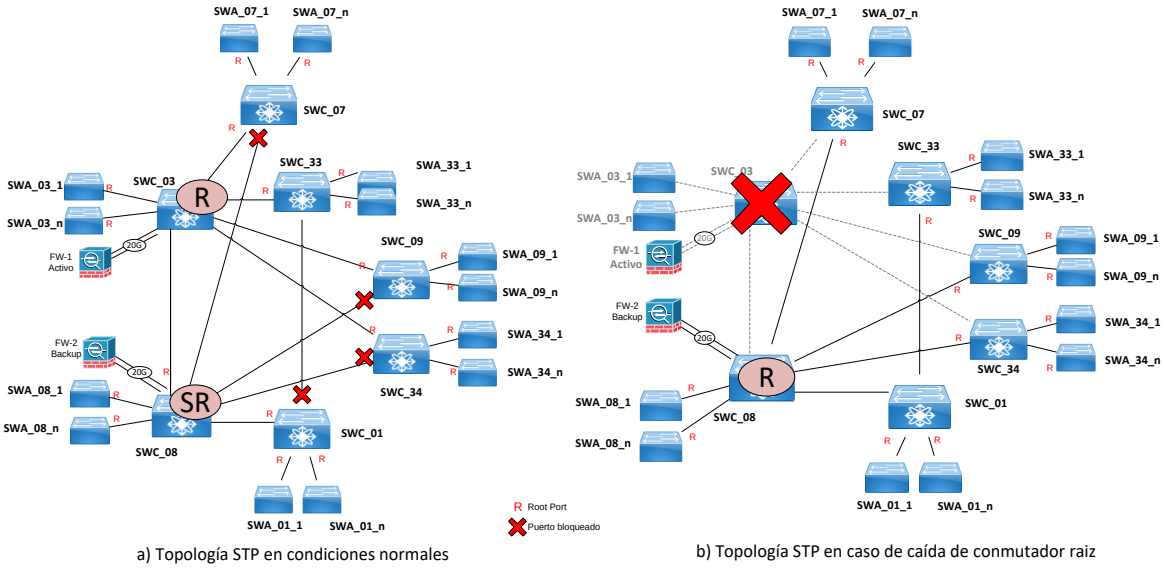


Figura 3.36 Topologías STP en VLANs Centro de Datos (Fuente: Elab. propia)

b) VLANs Centro de Gestión

En las VLANs de Centro de Gestión, se elige como Raiz del árbol de STP a SWC_33 y Raíz Secundaría a SWC_01 puesto que el siguiente salto de capa 3 luego de la puerta de enlace se encuentra el firewall en modo clúster cuyo chasis con el rol activo se encuentra en SWC_33 y contigencia en SWC_01. Esto permite mantener un flujo de traficó óptimo en la capa 2. En caso de la caída del conmutador raíz de STP SWC_33, este rol será asumido por SWC_01. En la figura 3.37 se muestran las topologías de STP incluyendo a los *Root port* y puertos bloqueados bajo estas consideraciones en a) situación normal y b) cuando existe una caída del conmutador raíz.

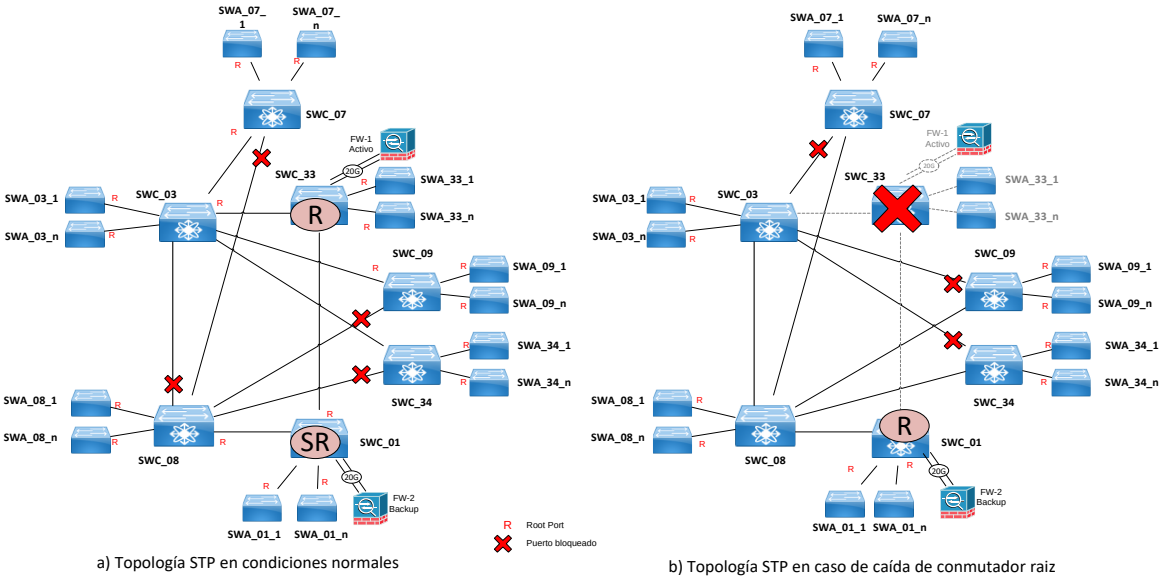


Figura 3.37 Topologías STP en VLANs Centro de Datos (Fuente: Elab. propia)

3.2.5. Calidad de Servicio

En esta sección se describen las consideraciones utilizadas para la definición de calidad de servicio del tráfico cursante, utilizando los siguientes pasos:

- Identificación de los requerimientos de ancho de banda del tráfico
- Definición de Colas de Servicio
- Distribución del Ancho de Banda por Colas de Servicio en enlaces PE-CE:
- Encolamiento y programación de cola
- Mecanismos para evitar congestión.

a) Identificación de los requerimientos de ancho de banda del tráfico

No existe una definición previa en la red, por tanto, el primer paso es identificar y definir los valores de tráfico que deseamos asegurar, lo cual debe ser realizado en conjunto con los administradores de red. Los requerimientos de ancho de banda para las aplicaciones cursantes varían de acuerdo con el tipo e importancia del nodo a considerar.

- **Centro de Gestión:**

En la tabla 3.11 se indican las aplicaciones identificadas como las más importantes para el desempeño del centro de gestión y por ende a asegurar. También se identifican el ancho de banda (BW) promedio utilizado por cada sesión, la cantidad de usuarios y sesiones en promedio con las que trabaja cada usuario habitualmente con para calcular del ancho de banda demandados. La demanda de ancho de banda total por aplicación en el Centro de Gestión es calculada siguiendo la fórmula (3.1):

$$BW_{\substack{Mbps\ Total \\ Centro\ Gestion}} = (BW_{Kbps\ x\ sesión} \times \#\ Sesiones_{usuario} \times \#\ Usuarios) \times (\frac{1\ Kbps}{1000\ Mbps}) \quad (3.\ 1)$$

Los valores obtenidos son utilizados en la definición de colas de los enlaces MPLS.

Tabla 3.11 Requerimiento de Ancho de banda en Centro de Gestión (Fuente: Elab. propia)

Aplicación	BW (Kbps) x sesión	Sesiones por usuario	Cantidad de Usuarios	BW total (Mbps)	Observación
Telnet/SSH	9.6	5	100	4.8	Texto plano a 9600 baudios
HTTP/HTTPS	512	4	100	204.8	Pagina web de 1MB cargada en 2 seg
RDP/Herramientas de Colaboración	2048	2	50	204.8	Requerimiento referencial recomendado para telepresencia: https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meetings/white_paper_c11-691351.html
VoIP	119.28	1	100	11.9	Llamadas con codec G729 (64Kbps) y payload 80 Bytes Ref https://cway.cisco.com/tools/vccalc/#result
Transferencia de archivos	4000	3	20	240	4 Mbps por sesión, transferencia de archivos: - 200MB en 7 min - 500MB en 17.5 min - 1GB en 36 min
			Total Mbps	666.3	

El requerimiento de ancho de banda en los enlaces PE-CE es estimado como la quinta parte del valor total por cada instancia virtual de ruteo. Esta distribución es la misma a utilizar en los enlaces MPLS.

- **Centro de Datos:**

En la tabla 3.12 se indican las aplicaciones identificadas como necesarias en los Centros de Datos, el ancho de banda utilizado por cada sesión, la cantidad de sesiones que se estima cada servidor atiende en sus actividades diarias y el ancho de banda total por cada aplicación. La demanda de ancho de banda total por aplicación en el Centro de Datos es calculada en la fórmula (3.2):

$$BW_{\substack{Mbps\ Total \\ Centro\ de\ Datos}} = (BW_{Kbps\ x\ sesión} \times \#\ Sesiones) \times (\frac{1\ Kbps}{1000\ Mbps}) \qquad (3.\ 2)$$

Tabla 3.12 Requerimientos de Ancho de banda en Centro de Datos (Fuente: Elab. propia)

Aplicación	BW (Kbps) x sesión	Cant. de sesiones	BW total (Mbps)	Observación
Telnet/SSH	25	100	2.5	valor medido experimentalmente
SNMP	100	1000	100	consulta típica de snmp walk: Ref. https://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/install/reference/ins_discobandwidthreq.html
Syslog	8	2000	16	Mensaje tipico de 100 bytes. 10 mensajes por seg por log
NTP	0.024	2000	0.048	Ref. https://networking.ringofsaturn.com/Protocols/ntp.php
HTTP/HTTPS	512	200	102.4	Pagina web de 1MB cargada en 2 seg
AAA	50	1000	50	valor medido exprimentalmente en la red
VoIP	119.28	100	11.9	Llamadas con codec G729 (64Kbps) y payload 80 Bytes Ref https://cway.cisco.com/tools/vccalc/#result
RDP/Herramientas de Colaboración	2048	100	204.8	Video interactivo
Transferencia de archivos	4096	50	204.8	4 Mbps por sesión, transferencia de archivos: - 200MB en 7 min - 500MB en 17.5 min - 1GB en 36 min
		Total Mbps	692.5	

El requerimiento de ancho de banda de los enlaces PE-CE es estimado como la quinta parte del valor total estimado utilizando la misma distribución que los enlaces MPLS.

- **Nodo Primario:**

En la tabla 3.13 se muestra los valores estimados para definir el tráfico que cursa para un nodo primario considerando que debe albergar en promedio a 500 dispositivos. Estos valores serán utilizados durante la definición de las colas de los enlaces MPLS.

La demanda de ancho de banda total por aplicación en un Nodo Primario es calculada en la fórmula (3.3):

$$BW_{\substack{Mbps\ Total \\ Nodo\ Primario}} = (BW_{Kbps\ x\ sesión} \times \#\ Sesiones\ ) \times (\frac{1\ Kbps}{1000\ Mbps}) \qquad (3.\ 3)$$

Tabla 3.13 Requerimientos de Ancho de banda en un Nodo primario (Fuente: Elab. propia)

Aplicación	BW (Kbps) x sesión	Cant. de sesiones	BW total (Mbps)	Observación
Telnet/SSH	9.6	100	0.96	valor medido experimentalmente
SNMP	100	250	25	consulta típica de snmp walk: Ref. https://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/install/reference/ins_discobandwidthreq.html
Syslog	8	500	4	Mensaje tipico de 100 bytes. 10 mensajes por seg por log
NTP	0.024	500	0.01	Ref. https://networking.ringofsaturn.com/Protocols/ntp.php
HTTP/HTTPS	512	100	51.2	Pagina web de 1MB cargada en 2 seg
AAA	50	250	12.5	valor medido experimentalmente
Transferencia de archivos	4096	10	41	4 Mbps por sesión, transferencia de archivos: - 200MB en 7 min - 500MB en 17.5 min - 1GB en 36 min
		Total Mbps	134.6	

Al igual que en el caso anterior se estima que los requerimientos de ancho de banda de los enlaces PE-CE serán iguales a la quinta parte del valor total estimado utilizando la misma distribución que los enlaces MPLS.

- **Nodo Secundario:**

En la tabla 3.14 se muestra los valores estimados para definir el tráfico que cursa para un nodo secundario considerando que alberga en promedio a 200 dispositivos. La demanda de ancho de banda total por aplicación en un Nodo Secundario es calculada utilizando la fórmula (3.4):

$$BW_{\substack{Mbps\ Total \\ Nodo\ Secundario}} = (BW_{Kbps\ x\ sesión} \times \#\ Sesiones) \times \left(\frac{1\ Kbps}{1000\ Mbps}\right) \qquad (3.\ 4)$$

Tabla 3.14 Requerimientos de Ancho de banda en un Nodo secundario (Fuente: Elab. propia)

Aplicación	BW (Kbps) x sesión	Cant. de sesiones	BW total (Mbps)	Observación
Telnet/SSH	9.6	50	0.5	valor medido experimentalmente
SNMP	100	100	10	consulta típica de snmp walk: Ref. https://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/install/reference/ins_discobandwidthreq.html
Syslog	8	200	1.6	Mensaje tipico de 100 bytes. 10 mensajes por seg por log
NTP	0.024	200	0.005	Ref. https://networking.ringofsaturn.com/Protocols/ntp.php
HTTP/HTTPS	512	25	12.8	Pagina web de 1MB cargada en 2 seg
AAA	50	100	5	valor medido experimentalmente
Transferencia de archivos	4096	5	20.5	4 Mbps por sesión, transferencia de archivos: - 200MB en 7 min - 500MB en 17.5 min - 1GB en 36 min
		Total Mbps	50.4	

El ancho de banda utilizado por los enlaces PE-CE será igual a la quinta parte del valor total estimado utilizando la misma distribución que los enlaces MPLS.

- **Nodo Remoto:**

En la tabla 3.15 se muestra los valores estimados para definir el tráfico que debería cursar en un nodo de este tipo considerando que debe albergar en promedio a 50 dispositivos. La demanda de ancho de banda total por aplicación en un Nodo Remoto es calculada con la fórmula (3.5):

$$BW_{\substack{Kbps\ Total \\ Nodo\ Remoto}} = (BW_{Kbps\ x\ sesión} \times \#\ Sesiones) \qquad (3.\ 5)$$

Tabla 3.15 Requerimientos de Ancho de banda en un Nodo remoto (Fuente: Elab. propia)

Aplicación	BW (Kbps) x sesión	Cant. de sesiones	BW total (Kbps)	Observación
Telnet/SSH	9.6	5	48	valor medido experimentalmente
SNMP	100	3	300	consulta típica de snmp walk: Ref. https://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/install/reference/ins_discobandwidthreq.html
Syslog	8	20	160	Mensaje tipico de 100 bytes. 10 mensajes por seg por log
NTP	0.024	20	0.48	Ref. https://networking.ringofsaturn.com/Protocols/ntp.php
HTTP/HTTPS	256	1	256	Pagina web de 1MB cargada en 4 seg
AAA	50	5	250	valor medido experimentalmente
Transferencia de archivos	128	1	128	128Kbps por sesión, transferencia de archivos: - 10MB en 11 min - 20MB en 21 min - 25MB en 27 min
		Total	1142.5	

b) Definición de Colas de Servicio

Para la definición de las colas de servicio se utilizará 7 colas cuyo origen está basado en un modelo de 8 colas (Ref. [25]) para identificar a todos los tipos de tráfico que la red podría cursar y sobre las que se mapearan las aplicaciones identificadas en la sección anterior. Las colas estarán definidas según:

- Control de red
- Tiempo Real (Voz)
- Video
- Datos críticos
- Datos transaccionales
- Datos masivos
- Best effort
- Datos no importantes

De estas colas se decide juntar las clases “Datos masivos” y “Datos no importantes” en una sola clase para simplificar el modelo dado que estos tipos de tráfico son considerados con el mismo nivel de importancia para los administradores y usuarios de la red. Esto es mostrado a continuación en la tabla 3.16. Los valores de DSCP serán utilizados en los paquetes IP, mientras que los MPLS Experimental bit serán utilizados en los paquetes que usan etiquetas MPLS.

Tabla 3.16 Definición de colas de Servicio (Fuente: Elab. propia)

Cola	Tipo de Aplicación	DSCP	MPLS EXP bit
NETWORK-CONTROL	Network Control	CS7	7
	Internetwork Control	CS6	6
REALTIME	Voz	EF	5
VIDEO	Video Interactivo	AF41	4
	Video Streaming	CS4	4
DATOS-CRITICOS	Datos Críticos	AF31	3
	Call Signaling	CS3	3
DATOS-TRANSACCIONALES	Datos transaccionales	AF21	2
	Gestión de Equipos	CS2	2
DATOS-MASIVOS	Datos voluminosos	AF11	1
	Datos no importantes	CS1	1
DEFAULT	Best Effort	0	0

Las aplicaciones identificadas anteriormente en cada nodo según las tablas 3.11, 3.12, 3.13, 3.14 y 3.15 son mapeadas y relacionadas con las colas definidas en la tabla 3.16. El mapeo resultante es mostrado en la tabla 3.17.

Tabla 3.17 Mapeo de aplicaciones a Colas de Servicio (Fuente: Elab. propia)

Aplicación	Cola
Telnet/SSH	DATOS-TRANSACCIONALES
HTTP/HTTPS	DATOS-TRANSACCIONALES
RDP/Herramientas de Colaboración	VIDEO
VoIP	REALTIME
Transferencia de archivos	DATOS-MASIVOS
Syslog	DATOS-TRANSACCIONALES
NTP	NETWORK-CONTROL
AAA	NETWORK-CONTROL
Transferencia de archivos	DATOS-MASIVOS
SNMP	DATOS-TRANSACCIONALES

Esto permite relacionar el requerimiento de ancho de banda por aplicación con el valor de ancho de banda por cola de servicio. El ancho de banda requerido por cada clase es calculado como la suma de anchos de banda requeridos por las aplicaciones que se

corresponden con esa clase. En la tabla 3.18 se muestra el ancho de banda requerido para un Centro de Gestión.

Tabla 3.18 Req. de ancho de banda por clase Centros de Gestión (Fuente: Elab. propia)

Clases	Aplicación	DSCP	EXP	BW (Mbps) por aplicación	BW total (Mbps) por clase
REALTIME	VoIP	EF	5	11.9	11.928
VIDEO	RDP/Herramientas de Colaboración	AF41	4	204.8	204.8
DATOS-TRANSACCIONALES	Telnet/SSH	CS2	2	4.8	209.6
	HTTP/HTTPS	AF21		204.8	
DATOS-MASIVOS	Transf. de archivos	AF11	1	240	240
			Total, Mbps	666.3	666.3

En la tabla 3.19 se muestra el ancho de banda requerido para un Centro de Datos.

Tabla 3.19 Req. de ancho de banda por clase en Centros de Datos (Fuente: Elab. propia)

Clases	Aplicación	DSCP	EXP	BW (Mbps) por aplicación	BW total (Mbps) por clase
REALTIME	VoIP	EF	5	11.9	11.9
NETWORK-CONTROL	NTP	CS6	6	0.048	50.0
	AAA	CS6		50	
VIDEO	RDP/Herramientas de Colaboración	AF41	4	204.8	204.8
DATOS-TRANSACCIONALES	HTTP/HTTPS	AF21	2	102.4	220.9
	Telnet/SSH	CS2		2.5	
	SNMP	CS2		100	
	Syslog	CS2		16	
DATOS-MASIVOS	Transf. de archivos	AF11	1	204.8	204.8
			Total, Mbps	692.5	692.5

En la tabla 3.20 se muestra el requerimiento de ancho de banda para un nodo principal.

Tabla 3.20 Req. de ancho de banda por clase en Nodo Principal (Fuente: Elab. propia)

Clases	Aplicación	DSCP	EXP	BW (Mbps) por aplicación	BW total (Mbps) por clase
NETWORK-CONTROL	NTP	CS6	6	0.012	12.5
	AAA	CS6		12.5	
DATOS-TRANSACCIONALES	Telnet/SSH	CS2	2	0.96	81.2
	SNMP	CS2		25	
	Syslog	CS2		4	
	HTTP/HTTPS	AF21		51.2	
DATOS-MASIVOS	Transf. de archivos	AF11	1	40.96	41.0
			Total, Mbps	134.6	134.6

En la tabla 3.21 se muestra el requerimiento de ancho de banda para un nodo secundario.

Tabla 3.21 Req. de ancho de banda por clase en Nodo Secundario (Fuente: Elab. propia)

Clases	Aplicación	DSCP	EXP	BW (Mbps) por aplicación	BW total (Mbps) por clase
NETWORK-CONTROL	NTP	CS6	6	0.0048	5.0
	AAA	CS6		5	
DATOS-TRANSACCIONALES	Telnet/SSH	CS2	2	0.48	24.9
	SNMP	CS2		10	
	Syslog	CS2		1.6	
	HTTP/HTTPS	AF21		12.8	
DATOS-MASIVOS	Transf. de archivos	AF11	1	20.48	20.5
			Total, Mbps	50.4	50.4

En la tabla 3.22 se muestra el requerimiento de ancho de banda para un nodo remoto.

Tabla 3.22 Req. de ancho de banda por clase en Nodo Remoto (Fuente: Elab. propia)

Clases	Aplicación	DSCP	BW (Kbps) por aplicación	BW total (Kbps) por clase
NETWORK-CONTROL	NTP	CS6	0.48	250.48
	AAA	CS6	250	
DATOS-TRANSACCIONALES	Telnet/SSH	CS2	48	764
	SNMP	CS2	300	
	Syslog	CS2	160	
	HTTP/HTTPS	AF21	256	
DATOS-MASIVOS	Transf. de archivos	AF11	128	128
		Total, Kbps	1598.48	1142.5

c) Distribución del Ancho de Banda por Colas de Servicio

En esta sección se explican los criterios utilizados para la distribución del ancho de banda en cada enlace. Como buena práctica, se busca que los valores elegidos puedan utilizarse a manera de plantilla sobre enlaces de características similares.

- **Enlaces 10Gbps**

Los enlaces 10Gbps son agregados formando enlaces lógicos de 20Gbps en los nodos Principales, Centro de Datos y Centro de Gestión. Estos enlaces llevan tanto enlaces troncales MPLS como enlaces PE-CE separadas mediante VLANs, por lo cual es necesario aplicar un mecanismo de *shaping* que asegure y limite el ancho de banda consumido por cada VLAN de enlace MPLS y enlace PE-CE bajo las siguientes consideraciones:

- El ancho de banda elegido para cada enlace lógico MPLS es 2.5 Gbps. Utilizar este valor permite distribuir el ancho de banda disponible de los enlaces lógicos agregados (20 Gbps) soportando a los nodos con mayor cantidad de enlaces MPLS (PE_TX_03 y

PE_TX_08 con 5 enlaces cada uno). En la figura 3.38 se muestra la distribución de los enlaces lógicos en los nodos principales, Centro de Datos y Centro de Gestión.

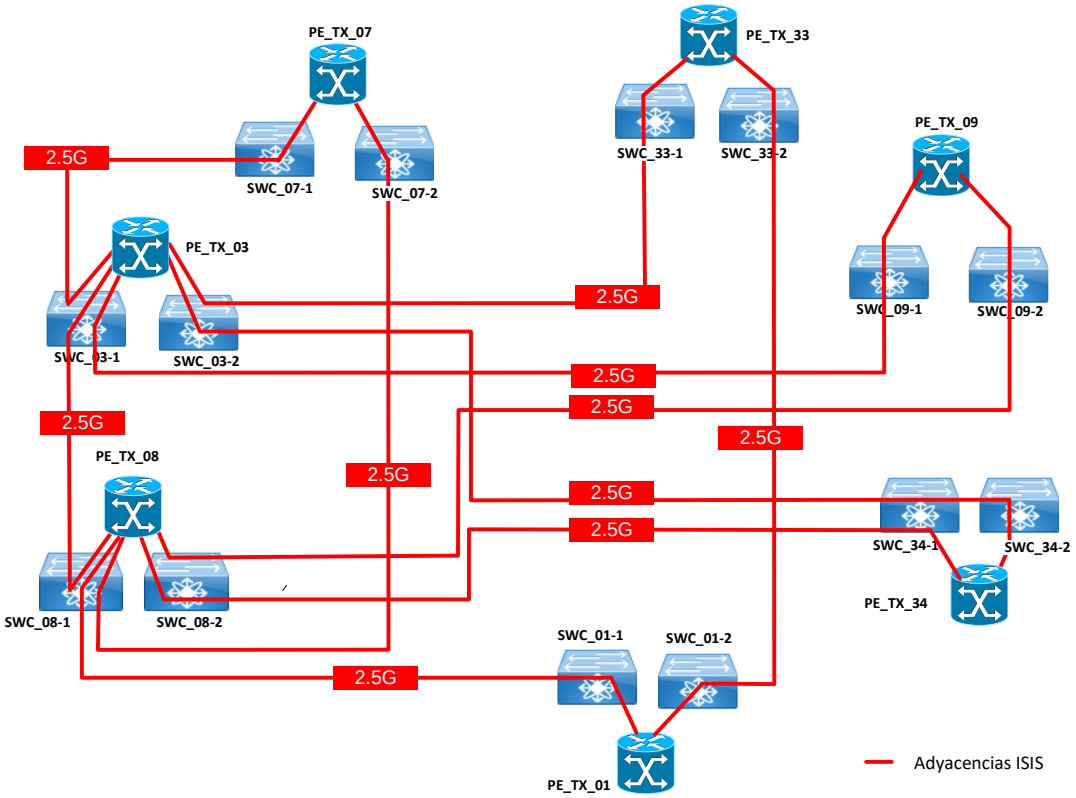


Figura 3.38 Solución propuesta: Enlaces MPLS con BW 2.5G (Fuente: Elab. propia)

- Todos los nodos principales tienen una concurrencia de al menos 10 accesos PE-CE. Se estima que por cada VRF se necesitará al menos la décima parte del valor máximo en los enlaces MPLS por lo cual se asignará un valor de *shaping* a cada uno de 250 Mbps = 2,5 Gbps / 10 accesos. El consumo estimado total de BW a utilizar en enlaces PE-CE correspondiente al valor máximo de 15 VRFs es de 3.75 Gbps = 250 Mbps x 15.

- Los 02 Centros de Gestión (uno por GOB y otro por DCN) se ubican en los nodos correspondientes a PE_TX_01 y PE_TX_33. Se estima necesario al menos la quinta parte del ancho de banda de los enlaces MPLS por lo cual se asignará un valor de *shaping* a cada uno de 500 Mbps = 2,5 Gbps / 5 accesos. El consumo estimado total de BW a utilizar en enlaces PE-CE correspondiente al valor máximo de 15 VRFs es de 7.5 Gbps = 500 Mbps x 15.

- Los 02 Centro de Datos (uno por GOB y otro por DCN) se ubican en los nodos correspondientes a PE_TX_03 y PE_TX_08. Se estima necesario también al menos la quinta parte del ancho de banda de los enlaces MPLS por lo cual se asignará un valor de *shaping* de 500 Mbps = 2,5 Gbps / 5 accesos. El consumo estimado total de BW a utilizar en enlaces PE-CE para 15 VRFs es de 7.5 Gbps = 500 Mbps x 15.

En la tabla 3.23 se consolidan estos datos, mostrando el ancho de banda agregado, los estimados para usar en enlaces MPLS, enlaces PE-CE y el que quedaría disponible para crecimiento futuro, que es calculado según la fórmula (3.6):

$$BW(Gbps)_{\substack{Disponible\\crecimiento}} = BW(Gbps)_{\substack{Enlace\\agregado}} - (BW(Gbps)_{\substack{utilizado\\Enl.\ MPLS}} + BW(Gbps)_{\substack{utilizado\\Enl.\ PE-CE}}) \quad (3.6)$$

Tabla 3.23 BW utilizado y disponible en enlaces 10G (Fuente: Elab. propia)

PE	Conmutador	Enlace Físico (Gbps)	BW enlace Agregado (Gbps)	BW utilizado enlaces MPLS (Gbps)	BW utilizado Enlaces PE-CE (Gbps)	BW disponible Crecimiento (Gbps)
PE_TX_03	*SWC_03-1*	10	20	12.5	7.5	0
PE_TX_03	*SWC_03-2*	10				
PE_TX_08	*SWC_08-1*	10	20	12.5	7.5	0
PE_TX_08	*SWC_08-2*	10				
PE_TX_07	*SWC_07-1*	10	20	5	3.75	11.25
PE_TX_07	*SWC_07-2*	10				
PE_TX_33	*SWC_33-1*	10	20	5	7.5	7.5
PE_TX_33	*SWC_33-2*	10				
PE_TX_01	*SWC_01-1*	10	20	5	7.5	7.5
PE_TX_01	*SWC_01-2*	10				
PE_TX_09	*SWC_09-1*	10	20	5	3.75	11.25
PE_TX_09	*SWC_09-2*	10				
PE_TX_34	*SWC_34-1*	10	20	5	3.75	11.25
PE_TX_34	*SWC_34-2*	10				

Enlaces MPLS en Nodos Principales:

En la tabla 3.24 se muestra la distribución de ancho de banda propuesto para cada una de las clases definidas para los enlaces MPLS, en base al bit Experimental con respecto al valor de *shaping* 2.5Gbps.

Tabla 3.24 Distribución de BW enlaces MPLS 2.5G Nodo Principal (Fuente: Elab. propia)

Clases	EXP	BW (%)
REALTIME	5	**5%**
NETWORK-CONTROL	6,7	15% (del BW restante)
VIDEO	4	5% (del BW restante)
DATOS-CRITICOS	3	10% (del BW restante)
DATOS-TRANSACCIONALES	2	20% (del BW restante)
DATOS-MASIVOS	1	15% (del BW restante)
DEFAULT	0	35% (del BW restante)

Al aplicar esta distribución se cubren los requerimientos de ancho de banda demandados incluso para el peor caso que se da cuando se utiliza la cola REALTIME al máximo de su capacidad (según lo indicado por los administradores actualmente no existe este tráfico por lo que esta cola no consume ancho de banda).

El ancho de banda ofrecido es calculado según las fórmulas (3.7) y (3.8):

- BW máximo ofrecido en la clase REALTIME:

$$BW_{MAX\ REAL\ TIME} = BW_{REALTIME}(\%) \times BW_{Enlace} \quad (3.7)$$

Donde: BW_{Enlace}= 2500 Mbps y $BW_{REALTIME}(\%) = 5\%$

Resultado: $BW_{MAX\ REALTIME}$= 125 Mbps

- BW ofrecido en otras clases:

$$BW_{Clase} = (BW_{Enlace} - BW\ usado_{REALTIME}) \times BW_{Clase}(\%) \quad (3.8)$$

Donde: BW_{Enlace}= 2500 Mbps

Para el cálculo de la Situación Actual se considera: $BW\ usado_{REALTIME}$= 0 Mbps

Para el peor caso se considera: $BW\ usado_{REALTIME}$= 125 Mbps

En la tabla 3.25 se muestra una comparación entre los valores de ancho de banda requerido y el ofrecido para los enlaces MPLS en los nodos principales.

Tabla 3.25 BW requerido vs ofrecido en Nodos principales - enlaces MPLS 2.5G (Fuente: Elab. propia)

		BW(Mbps) requerido	**BW (Mbps) ofrecido por cola con *shaping* 2.5G**	
Clases	**EXP**	**Nodo Principal**	**Situación actual**	**Cola real-time al Max**
REALTIME	5	0	0	125
NETWORK-CONTROL	6,7	12.5	375	356.3
VIDEO	4	0	125	118.8
DATOS-CRITICOS	3	0	250	237.5
DATOS-TRANSACCIONALES	2	81.2	500	475
DATOS-MASIVOS	1	41.0	375	356.25
DEFAULT	0	0	875	831.25
Total		134.6		

Enlaces PE-CE en Nodos Principales:

La asignación de ancho de banda por cola en los enlaces PE-CE de los nodos principales sigue la distribución definida en la tabla 3.24 pero considerando un límite de 250 Mbps (1/10 del valor de BW para un enlace MPLS: 2.5Gbps). Esta distribución cubre los requerimientos de ancho de banda demandados incluso para el peor caso, cuando se

utiliza la cola REALTIME al máximo de su capacidad (actualmente no existe este tráfico por lo que esta cola no consume ancho de banda).

El ancho de banda ofrecido es calculado según las fórmulas (3.9) y (3.10):

- BW máximo ofrecido en la clase REALTIME:

$$BW_{MAX\ REAL\ TIME} = BW_{REALTIME}(\%) \times BW_{Enlace} \quad (3.\ 9)$$

Donde: BW_{Enlace}= 2500 Mbps y $BW_{REALTIME}(\%) = 5\%$

Resultado: $BW_{MAX\ REALTIME}$= 125 Mbps

- BW ofrecido en otras clases:

$$BW_{Clase} = (BW_{Enlace} - BW\ usado_{REALTIME}) \times BW_{Clase}(\%) \quad (3.\ 10)$$

Donde: BW_{Enlace}= 250 Mbps

Para el cálculo de la Situación Actual se considera: $BW\ usado_{REALTIME}$= 0 Mbps

Para el peor caso se considera: $BW\ usado_{REALTIME}$= 12.5 Mbps

En la tabla 3.26 se muestra una comparación entre los valores de ancho de banda requerido y el ofrecido para los enlaces PE-CE en los nodos principales.

Tabla 3.26 BW requerido vs ofrecido en Nodos principales - enlaces PE-CE (Fuente: Elab. propia)

		BW(Mbps) requerido enlace PE-CE Nodo principal	**BW (Mbps) ofrecido en colas - *shaping* 250Mbps**	
Clases	**DSCP**		**Situación actual**	**Cola real-time al Max**
REALTIME	CS7, CS6	0.0	0.0	12.5
NETWORK-CONTROL	EF	2.5	37.5	35.6
VIDEO	AF41, CS4	0.0	12.5	11.9
DATOS-CRITICOS	AF31, CS3	0.0	25	23.8
DATOS-TRANSACCIONALES	AF21, CS2	16.2	50	47.5
DATOS-MASIVOS	AF11, CS1	8.2	37.5	35.6
DEFAULT	0	0.0	87.5	83.1
Total		26.9	250	250

Enlaces MPLS en Centro de Datos y Centro de Gestión:

La asignación de ancho de banda por cola requiere una distribución diferente debido al uso de las colas VIDEO y DATOS-MASIVOS.

En la tabla 3.27 se muestra la distribución de BW por colas propuesto para el Centro de Datos y Centro de Gestión.

Tabla 3.27 Distribución de BW en enlaces MPLS 10G (Fuente: Elab. propia)

Clases	BW (%)
REALTIME	5%
NETWORK-CONTROL	15% (del BW restante)
VIDEO	10% (del BW restante)
DATOS-CRITICOS	10% (del BW restante)
DATOS-TRANSACCIONALES	20% (del BW restante)
DATOS-MASIVOS	20% (del BW restante)
DEFAULT	25% (del BW restante)

Esta distribución cubre los requerimientos de ancho de banda demandados incluso para el peor caso que se da cuando se utiliza la cola REALTIME al máximo de su capacidad. En la tabla 3.28 se muestra una comparación entre los valores de ancho de banda requerido y el ofrecido en los enlaces MPLS para el Centro de Datos y Centro de Gestión. El ancho de banda ofrecido es calculado según las fórmulas (3.11) y (3.12):

Tabla 3.28 BW requerido vs ofrecido en Centro de Datos y Centro de Gestión - enlaces MPLS 2.5G (Fuente: Elab. propia)

		BW(Mbps) requerido total		BW (Mbps) ofrecido por cola en enlace 2.5G Nodo principal	
Clases	EXP	Centro de Gestion	Centro de Datos	Situación actual	Cola real-time al Max
REALTIME	5	11.9	11.9	0	125
NETWORK-CONTROL	6,7	0	50	375	356.3
VIDEO	4	204.8	204.8	250	237.5
DATOS-CRITICOS	3	0	0	250	237.5
DATOS-TRANSACCIONALES	2	209.6	220.9	500	475
DATOS-MASIVOS	1	240.0	204.8	500	475
DEFAULT	0	0	0	625	593.75
Total		666.3	692.5	2500	2500

Enlaces PE-CE en Centro de Datos y Centro de Gestión:

La asignación de ancho de banda por cola en los enlaces PE-CE de los nodos principales sigue la distribución definida en la tabla 3.24 pero con un *shaping* de 500 Mbps (1/5 del valor de BW para un enlace MPLS: 2.5Gbps). Al aplicar esta distribución podremos observar que se cubren los requerimientos de ancho de banda demandados incluso con la cola REALTIME ocupada al máximo de su capacidad. El ancho de banda ofrecido es calculado según las fórmulas 3.11 y 3.12:

- BW máximo ofrecido en la clase REALTIME:

$$BW_{MAX\ REAL\ TIME} = BW_{REALTIME}(\%) \times BW_{Enlace} \quad (3.\ 11)$$

Donde: BW_{Enlace}= 500 Mbps y $BW_{REALTIME}(\%) = 5\%$

Resultado: $BW_{MAX\ REALTIME}$= 25 Mbps

- BW ofrecido en otras clases:

$$BW_{Clase} = (BW_{Enlace} - BW\ usado_{REALTIME}) \times BW_{Clase}(\%) \quad (3.\ 12)$$

Donde: BW_{Enlace}= 500 Mbps

Para el cálculo de la Situación Actual se considera: $BW\ usado_{REALTIME}$= 0 Mbps

Para el peor caso se considera: $BW\ usado_{REALTIME}$= 25 Mbps

En la tabla 3.29 se muestra una comparación entre los valores de ancho de banda requerido y el ofrecido para los enlaces PE-CE en un Centro de Datos y Centro de Gestión.

Tabla 3.29 BW requerido vs ofrecido en Centro de Datos y Centro de Gestión - enlaces PE-CE (Fuente: Elab. propia)

		BW(Mbps) requerido en enlace PE-CE		BW (Mbps) por cola usando shaping 500Mbps	
Clases	DSCP	Centro de Gestion	Centro de Datos	Situación actual	Cola real-time al Max
REALTIME	CS7, CS6	2.3856	2.3856	0	25
NETWORK-CONTROL	EF	0	10.0096	75	71.25
VIDEO	AF41, CS4	40.96	40.96	50	47.5
DATOS-CRITICOS	AF31, CS3	0	0	50	47.5
DATOS-TRANSACCIONALES	AF21, CS2	41.92	44.18	100	95
DATOS-MASIVOS	AF11, CS1	48	40.96	100	95
DEFAULT	0	0	0	125	118.75
Total		133.2656	138.4952	500	500

- **Enlaces 1Gbps:**

Los enlaces MPLS 1G no necesitan de un mecanismo de *shaping*.

En la tabla 3.30 se muestra la distribución de ancho de banda definido por clase de servicio para los enlaces MPLS, en base al bit Experimental:

Tabla 3.30 Distribución de BW en enlaces MPLS 1G (Fuente: Elab. propia)

Clases	Experimental	BW (%)
REALTIME	5	**5%**
NETWORK-CONTROL	6,7	15% (del BW restante)
VIDEO	4	5% (del BW restante)
DATOS-CRITICOS	3	10% (del BW restante)
DATOS-TRANSACCIONALES	2	20% (del BW restante)
DATOS-MASIVOS	1	15% (del BW restante)
DEFAULT	0	35% (del BW restante)

El ancho de banda ofrecido es calculado según las fórmulas (3.13) y (3.14):

- BW máximo ofrecido en la clase REALTIME:

$$BW_{MAX\ REAL\ TIME} = BW_{REALTIME}(\%) \times BW_{Enlace} \quad (3.\ 13)$$

Donde: BW_{Enlace}= 1000 Mbps y $BW_{REALTIME}(\%) = 5\%$

Resultado: $BW_{MAX\ REALTIME}$= 50 Mbps

- BW ofrecido en otras clases:

$$BW_{Clase} = (BW_{Enlace} - BW\ usado_{REALTIME}) \times BW_{Clase}(\%) \quad (3.\ 14)$$

Donde: BW_{Enlace}= 1000 Mbps

Para el cálculo de la Situación Actual se considera: $BW\ usado_{REALTIME}$= 0 Mbps

Para el peor caso se considera: $BW\ usado_{REALTIME}$= 50 Mbps

En la tabla 3.31 se muestran los valores de ancho de banda requeridos por clase de servicio en los nodos de tipo Principal y Secundario con acceso a la MPLS 1G.

Tabla 3.31 BW requerido vs ofrecido - enlaces MPLS 1G (Fuente: Elab. propia)

		BW(Mbps) requerido total		BW (Mbps) ofrecido por cola en enlace 1G	
Clases	**EXP**	**Nodo Principal**	**Nodo Secundario**	**Situación normal**	**Cola real-time al Max**
REALTIME	5	0	0	0	50
NETWORK-CONTROL	6,7	12.5	5	150	142.5
VIDEO	4	0	0	50	47.5
DATOS-CRITICOS	3	0	0	100	95
DATOS-TRANSACCIONALES	2	81.2	24.9	200	190
DATOS-MASIVOS	1	41.0	20.5	150	142.5
DEFAULT	0	0		350	332.5
Total		134.7	50.4	1000	1000

Los requerimientos son cubiertos y es posible atender incluso una demanda mayor de tráfico.

Enlaces PE-CE en nodo remoto:

En los nodos remotos se define una distribución de BW que no incluye las colas REALTIME y VIDEO por el bajo valor de ancho de banda disponible: 2.048 Mbps. Por tanto, todo el tráfico se redistribuye entre las clases restantes.

En la tabla 3.32 se muestra la distribución de ancho de banda por clase de servicio en los enlaces de los nodos remotos.

Tabla 3.32 Distribución de BW en enlaces PE-CE Nodos remotos (Fuente: Elab. propia)

Clases	**BW (%)**

NETWORK-CONTROL	20%
DATOS-TRANSACCIONALES	45%
DATOS-MASIVOS	25%
DEFAULT	10%

El ancho de banda ofrecido es calculado según la fórmula (3.15):

$$BW_{Clase} = BW_{Enlace} \times BW_{Clase}(\%) \quad (3.15)$$

Donde: BW_{Enlace}= 2048 Kbps

En la tabla 3.33 se muestra una comparación entre los valores de ancho de banda requerido y el ofrecido. Los requerimientos son cubiertos y es posible atender incluso una demanda mayor de tráfico.

Tabla 3.33 BW requerido vs ofrecido – enlaces PE-CE nodos remotos (Fuente: Elab. propia)

Clases	**DSCP**	**BW(Kbps) requerido en enlace PE-CE Nodos remotos**	**BW (Kbps) por cola**
NETWORK-CONTROL	CS6, CS7	250.5	409.6
DATOS-CRITICOS	AF31, CS3	0	
DATOS-TRANSACCIONALES	AF21, CS2	764	921.6
DATOS-MASIVOS	AF11, CS1	128	512
DEFAULT	0	0	204.8
Total, Kbps		1598.48	2048

d) Definición del Encolamiento

- **Disciplinas de Encolamiento:**

Se usa un Cola de Prioridad (PQ) para el tráfico de Voz (cola REALTIME) que utiliza una cola de prioridad estricta, pero cuyo ancho de banda asignado que no puede ser sobrepasado puesto que usa *policing* para controlar este ancho de banda. El resto de las colas de tráfico usará *Weigthed Fair Queuing* (WFQ) buscando asegurar un ancho de banda por cada cola en caso de congestión, pero a la vez se debe permitir usar todo el ancho de banda disponible en la interfaz.

En los casos donde se requiere restringir el ancho de banda a un valor menor que el del enlace físico (ej. En los enlaces lógicos a 2.5Gbps) se utiliza *shaping* previamente para controlar el ancho de banda máximo a utilizar.

- **Colas utilizadas sobre interfaces:**

A continuación, se indican las características del encolamiento por cada tipo de enlace.

○ **Enlaces PE-PE:**

Colas de salida: realizan marcado de MPLS EXP y control de ancho de banda por cola.

Colas de Ingreso: no realiza cambios.

En enlaces compartidos (VLANs) se utiliza *shaping* previamente en ambos sentidos para limitar el ancho de banda a 2.5G. En la figura 3.39 se muestran las colas en enlaces MPLS 10G y 1G MPLS y las acciones que estas ejecutarán en un enrutador PE.

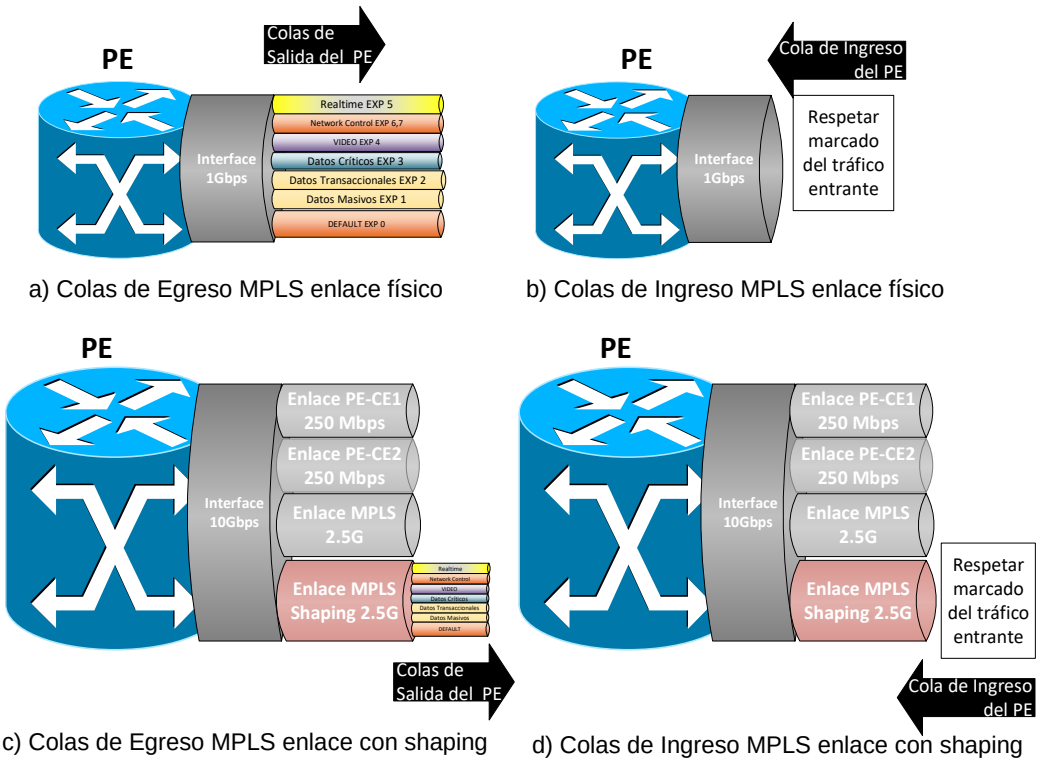


Figura 3.39 Encolamiento PE-PE (Fuente: Elab. propia)

○ **Enlaces PE-CE:**

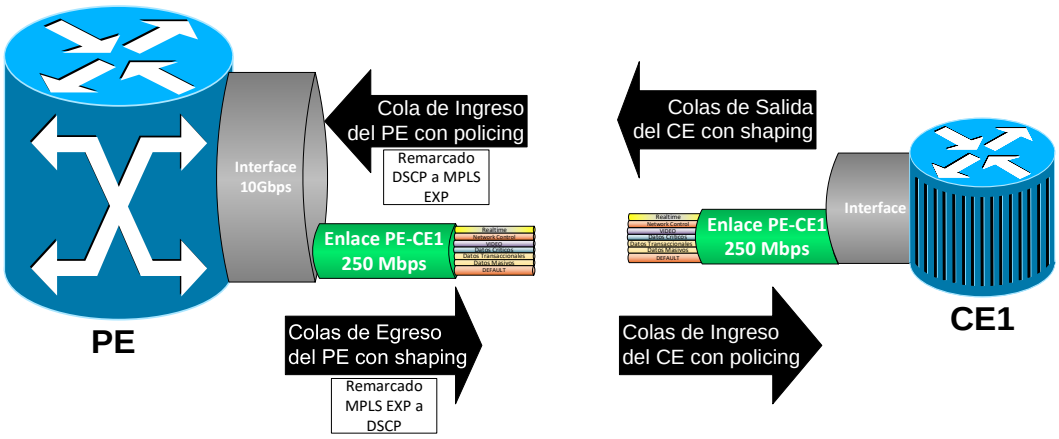
Colas de salida en el PE: remarcado de MPLS EXP a DSCP y control de ancho de banda por cola.

Colas de Ingreso en el PE: remarcado de DSCP a MPLS EXP y control de ancho de banda por cola.

Colas de salida en el CE: control de ancho de banda por cola.

Colas de Ingreso en el PE: control de ancho de banda por cola. También requiere de la utilización de *shaping* en ambos sentidos para el control de ancho de banda total.

En la figura 3.40 se muestran las colas en enlaces PE-CE y acciones que ejecutaran.



a) Colas PE en enlace PE-CE

b) Colas CE en enlace PE-CE

Figura 3.40 Encolamiento de enlaces PE-CE en el a) PE y b) CE (Fuente: Elab. propia)

e) Mecanismos para evitar congestión.

El mecanismo de congestión WRED es utilizado para evitar los efectos de la sincronización global de TCP con los límites inferior y superior descritos en la tabla 3.34.

Tabla 3.34 Definición de límites WRED (Fuente: Elab. propia)

Clases	EXP	DSCP	Límite Inferior	Límite Superior	Prob. de Descarte
NETWORK-CONTROL	6,7	CS7, CS6	32	80	1/10
REALTIME	5	EF	30	80	1/10
VIDEO	4	AF41, CS4	28	80	1/10
DATOS-CRITICOS	3	AF31, CS3	26	80	1/10
DATOS-TRANSACCIONALES	2	AF21, CS2	24	80	1/10
DATOS-MASIVOS	1	AF11, CS1	22	80	1/10
DEFAULT	0	0	20	80	1/10

3.2.6. Gestión

La gestión de la red de Gestión Fuera de Banda será realizada en banda. Los sistemas de gestión a utilizar para el monitoreo y gestión de los equipos de la nueva red de Gestión Fuera de Banda de red serán los de la red MPLS GOB. Esto incluye a los servidores SNMP, AAA, NTP, syslog y el acceso vía SSH desde el centro de gestión con el direccionamiento IP asignado para este propósito. Para tal efecto, los equipos se cambiará la configuración en los equipos provenientes de la MPLS DCN para utilizar los nuevos servidores.

En la figura 3.41 se observa cómo se establecerán los flujos de tráfico desde los equipos hacia los servidores de gestión, ubicados en los centros de datos y hacia el centro de gestión donde se encuentran los operadores de red.

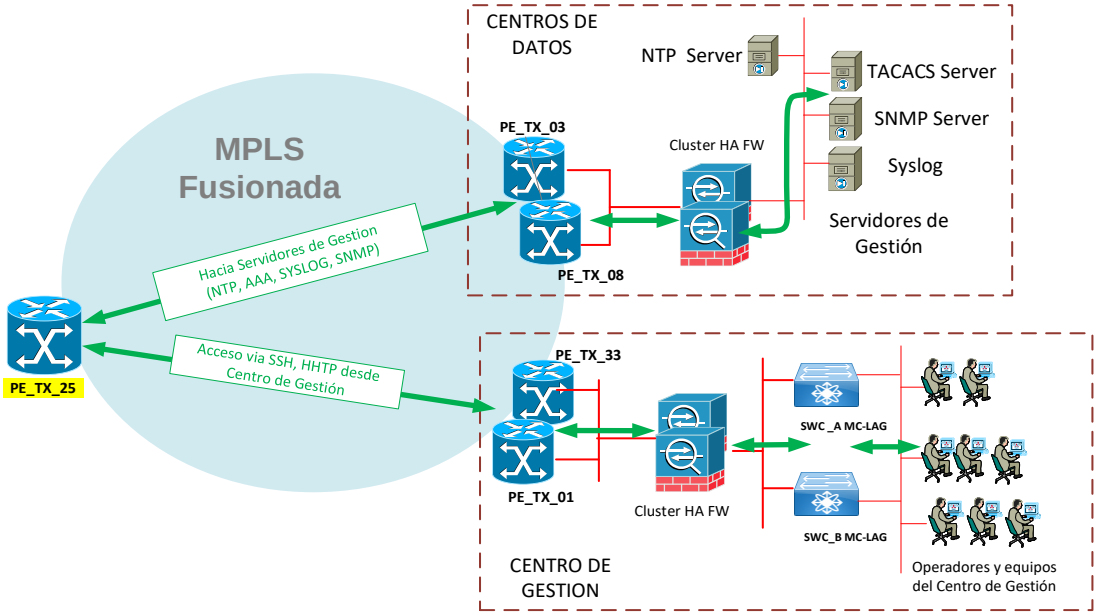


Figura 3.41 Solución propuesta: Gestión de equipos MPLS (Fuente: Elab. propia)

3.3. Programa de Implementación

Planificación de la solución

Etapa en la cual el proveedor de servicios define la propuesta de la red que integrará las dos redes MPLS y que cumplirá con los requerimientos de la solución.

Gestión de Compra

Donde se elige al integrador que realizará la implementación de la solución y se realiza la compra del equipamiento y servicios necesarios para la implementación.

Entrega de Equipos

Es el tiempo que toma desde la puesta de la orden de compra al integrador y recibir el equipamiento. Incluye los tiempos de fabricación de los equipos y la logística necesaria para transporte desde fabrica al almacén del proveedor de servicios.

Diseño de la solución

Etapa donde se realiza el diseño de Ingeniería del proyecto y se consiguen los recursos para su ejecución. Consta de las siguientes actividades:

- Site Survey, para identificar la ubicación en que se instalará el nuevo equipamiento y si es necesario realizar adecuaciones.

- Entrega de recursos de Energía, considera los tiempos para conseguir la asignación de llaves de energía para el nuevo equipamiento a instalar.

- Entrega de recursos de Transmisión (fibra óptica), considera los tiempos para conseguir los nuevos enlaces internodales, incluyendo las gestiones para la asignación de nuevos perfiles de fibra óptica y posiciones a utilizar en los ODFs.

- Elaboración de Documentos de Diseño de alto (descripción de los componentes de la solución y la manera en que interactúan) y bajo nivel (ingeniería de detalle).

- Ejecución de pruebas de equipamiento adquirido en laboratorio, para validar la operatividad del equipamiento adquirido e identificar fallas de fábrica, en cuyo caso se solicitará un cambio de equipo vía un RMA (Return Merchandise Authorization)

Ejecución:

Etapa donde se ejecutan las actividades de implementación en ventanas de mantenimiento programadas. Se identifican 2 fases:

Fase1: Fusión MPLS, comprende estas actividades:

Elaboración de Documento Plan de Implementación, para detallar las actividades a realizar en las ventanas de mantenimiento.

Tendido de cableados, utilizando los recursos de transmisión obtenidos en la fase de diseño.

Ejecución de ventanas de mantenimiento, siguiendo los pasos detallados en el documento Plan de Implementación.

Fase 2: Despliegue de equipos en nodos, comprende estas actividades:

Elaboración de Documento Plan de Implementación, ídem a la fase1.

Instalación y Energización del equipamiento adquirido, utilizando los recursos de energía y obtenidos en la fase de diseño.

Tendido de cableados, ítem a la fase1.

Integración con la red en producción, incluye las actividades de configuración e integración a la red, de los equipos adquiridos. En esta fase se incluye también la integración con los servidores de gestión NTP, SNMP, AAA, syslog y el acceso remoto desde el centro de gestión.

Migración de servicios, siguiendo los pasos en el documento Plan de implementación.

Ejecución de Protocolo de Pruebas de Aceptación, para validar la operatividad de la solución bajo condiciones normales y también en caso de caída de equipos y/o enlaces.

Cierre del proyecto:

Es la fase final del proyecto luego de haberse terminado las actividades de ejecución del proyecto.

Elaboración de Documentos de Cierre del Proyecto, se elaboran los últimos entregables del proyecto: Informe Final, topologías, actas de conformidad, etc. que son expuestas en una reunión a todos los interesados del proyecto.

Entrega a Operaciones (Día 1), se realiza la transferencia de información al equipo de operaciones que se encargará de las actividades de soporte de la red.

La figura 3.42 muestra un cronograma tentativo mostrando las tareas a realizar. Los tiempos estimados para cada actividad están basados en la experiencia de proyectos similares del proveedor de servicios.

Nombre de tarea	Duraci	Comienzo	Fin
Planificación de la solución	30 días	lun 7/01/19	vie 15/02/19
Gestión de Compra	10 días	lun 18/02/19	vie 1/03/19
Entrega de Equipos	45 días	lun 4/03/19	vie 3/05/19
Diseño de la solución	**45 días**	**lun 4/03/19**	**vie 3/05/19**
Site Survey	20 días	lun 4/03/19	vie 29/03/19
Entrega de Recursos de Energía	45 días	lun 4/03/19	vie 3/05/19
Entrega de recursos de Tx (fibra optica)	45 días	lun 4/03/19	vie 3/05/19
Elaboración de Documentos de Diseño alto y bajo nivel	21 días	lun 1/04/19	lun 29/04/19
Ejecución de pruebas de equipamiento adquirido en lab.	10 días	lun 1/04/19	vie 12/04/19
Ejecución:	**128 días**	**mar 30/04/19**	**jue 24/10/19**
Fase1: Fusión MPLS	**28 días**	**mar 30/04/19**	**jue 6/06/19**
Elaboración de Documento Plan de Implementación	5 días	mar 30/04/19	lun 6/05/19
Tendido de cableados	3 días	mar 7/05/19	jue 9/05/19
Ejecución de ventanas de mantenimiento	20 días	vie 10/05/19	jue 6/06/19
Fase 2: Despliegue de equipos en nodos	**100 días**	**vie 7/06/19**	**jue 24/10/19**
Elaboración de Documento Plan de Implementación	20 días	vie 7/06/19	jue 4/07/19
Instalación de equipamiento adquirido	10 días	vie 7/06/19	jue 20/06/19
Energización de equipamiento adquirido	10 días	vie 21/06/19	jue 4/07/19
Tendido de cableados	10 días	vie 21/06/19	jue 4/07/19
Integración con la red en produción	20 días	vie 5/07/19	jue 1/08/19
Migración de servicios	60 días	vie 2/08/19	jue 24/10/19
Ejecución de Protocolo de Pruebas de Aceptación	10 días	vie 25/10/19	jue 7/11/19
Cierre del proyecto	**10 días**	**vie 8/11/19**	**jue 21/11/19**
Elaboración de Documentos de Cierre del Proyecto	5 días	vie 8/11/19	jue 14/11/19
Entrega a Operaciones (Día 1)	5 días	vie 15/11/19	jue 21/11/19

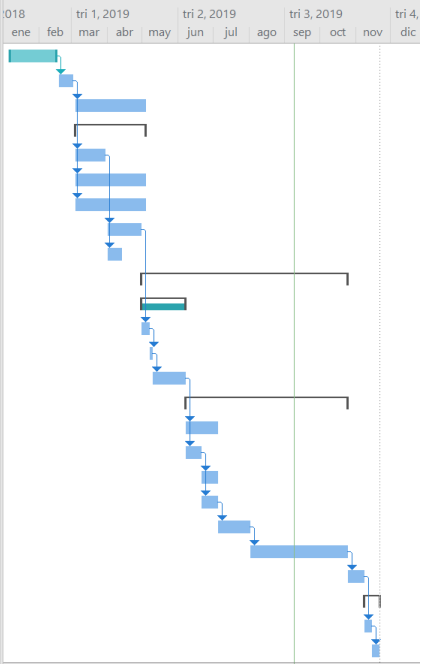


Figura 3.42 Cronograma de Implementación (Fuente: Elaboración propia)

CAPÍTULO IV
ANALISIS DE RESULTADOS Y COSTOS

En este capítulo se realiza el análisis de los resultados obtenidos, además de los aspectos económicos del proyecto tomando en consideración los costos de inversión y los de operación a utilizar en el proyecto.

4.1. Análisis de Resultados

Se eligen cinco características de las redes de gestión fuera de banda como indicadores a evaluar cuando se mantienen separadas las redes MPLS y cuando se implementa la Integración de las redes MPLS.

Los indicadores escogidos para la evaluación son los siguientes:

- Cantidad de equipos requeridos
- Utilización de capacidades de los equipos adquiridos
- Cantidad de enlaces requeridos
- Cobertura geográfica
- Confiabilidad de la red

4.1.1. Cantidad de equipos requeridos.

La comparación de equipos requeridos considera que se dará de baja un nodo MPLS (San Isidro) y la implementación de alta disponibilidad en los conmutadores de concentración y acceso. La implementación de alta disponibilidad en los conmutadores requiere incluir dos equipos para su funcionamiento.

En la tabla 4.1 se muestra la cantidad de equipos requeridos a instalar en caso se mantengan separadas ambas redes MPLS de gestión fuera de banda en el proveedor de servicios.

Tabla 4.1 Equipos a instalar con redes MPLS de gestión fuera de banda separadas (Fuente: Elab. propia)

Equipos	Situación Inicial	Redes MPLS separadas
Enrutadores MPLS GOB	10	9
Conmutadores MPLS GOB	16	28
Enrutadores MPLS DCN	31	31
Conmutadores MPLS DCN	0	0
Total, Equipos requeridos	57	68

En la tabla 4.2 se muestra la cantidad de equipos requeridos a instalar con la Integración de las redes MPLS fuera de banda en el proveedor de servicios.

Tabla 4.2 Equipos a instalar en la Integración de redes MPLS fuera de banda (Fuente: Elab. propia)

Equipos	Cantidad
Enrutadores MPLS Fusionada	31
Conmutadores MPLS Fusionada	28
Total, Equipos requeridos	59

El resultado obtenido muestra que de implementar la Integración de las dos redes MPLS la cantidad de equipos requeridos para el despliegue disminuye en 10, lo cual optimiza en 15% la cantidad de equipos a adquirir para las redes de gestión fuera de banda.

4.1.2. Utilización de capacidades de los equipos adquiridos.

La utilización de capacidades se calcula tomando como referencia la capacidad máxima soportada por el enrutador Cisco ASR903 con supervisora A900-RSP2A-128, de acuerdo con la hoja de datos del fabricante [26], en 4 funcionalidades clave a utilizar en la implementación: Cantidad de VPNS MPLS, rutas IPv4, etiquetas MPLS e interfaces de capa 3. Estos valores son comparados luego con los requerimientos de los enrutadores de las redes MPLS GOB, MPLS DCN y MPLS Fusionada para obtener luego los porcentajes de capacidad sin utilizar en cada caso. El resultado obtenido muestra que cuando se mantienen separadas las redes MPLS GOB y MPLS DCN el porcentaje de capacidad desaprovechado es mayor que cuando se implementa la Integración de las dos redes MPLS de gestión fuera de banda. El valor de optimización en este indicador muestra un aprovechamiento de hasta en 15% en la cantidad de etiquetas MPLS en un enrutador de la MPLS Fusionada con respecto a un enrutador utilizado en la MPLS GOB.

En la tabla 4.3 se muestra los valores de capacidad máxima soportada por el equipo de referencia (Cisco ASR903) y las capacidades requeridas por los enrutadores de cada red MPLS.

Tabla 4.3 Requerimientos por funcionalidad clave en enrutadores MPLS y cantidad máxima soportada por el equipo (Fuente: Elab. propia)

Enrutador ASR903 con supervisora A900-RSP2A-128	Capacidad máxima del equipo	Requerido MPLS GOB	Requerido MPLS DCN	Requerido MPLS Fusionada
MPLS VPN	128	5	10	15
Rutas IPv4	20000	2000	2500	4500
Etiquetas MPLS	15994	2000	2500	4500
Interfaces L3	1000	15	20	35

En la tabla 4.4 se muestra el porcentaje de capacidad sin utilizar por cada tipo de enrutador con respecto al valor máximo soportado por el equipo de referencia en cada funcionalidad evaluada.

Tabla 4.4 Equipos a instalar en la Integración de redes MPLS fuera de banda (Fuente: Elab. propia)

Enrutador ASR903 con supervisora A900-RSP2A-128	% Capacidad sin utilizar MPLS GOB	% Capacidad sin utilizar MPLS DCN	% Capacidad sin utilizar MPLS Fusionada	% Optimización Mejora
MPLS VPN	96	92	88	8
Rutas IPv4	90	88	78	12
Etiquetas MPLS	87	84	72	15
Interfaces L3	99	98	97	2

4.1.3. Cantidades de enlaces requeridos.

Se comparan la cantidad de enlaces requeridos en caso de mantener separadas ambas redes MPLS y cuando se implementa la integración.

En la tabla 4.5 se muestra la cantidad de enlaces 1G y 10G requeridos en caso se mantengan separadas ambas redes MPLS de gestión fuera de banda en el proveedor de servicios.

Tabla 4.5 Enlaces requeridos con redes MPLS de gestión fuera de banda separadas (Fuente: Elab. propia)

Enlaces	Requerido MPLS GOB	Requerido MPLS DCN	Total Requerido
Enlaces 1G	32	50	82
Enlaces 10G	30	0	30
Total			112

En la tabla 4.6 se muestra la cantidad de enlaces 1G y 10G requeridos con la Integración de las redes MPLS fuera de banda en el proveedor de servicios.

Tabla 4.6 Equipos a instalar en la Integración de redes MPLS fuera de banda (Fuente: Elab. propia)

Enlaces	Requerido MPLS Fusionada
Enlaces 1G	32
Enlaces 10G	30
Total	62

El resultado obtenido muestra que de implementar la Integración de las dos redes MPLS la cantidad de enlaces 1G requeridos disminuye en 50, optimizando en 44% la cantidad de enlaces 1G en las redes de gestión fuera de banda.

4.1.4. Cobertura geográfica.

La cobertura geográfica es evaluada comparando la cantidad de nodos a través de los cuales una VRF's puede extenderse para atender conexiones de gestión en caso de mantener separadas ambas redes MPLS y cuando se implementa la integración.

En la tabla 4.7 se muestra la cantidad de nodos por los que cada vrf puede extenderse.

Tabla 4.7 Cobertura de las VRF's (Fuente: Elab. propia)

Tipo de Red de Gestión	VRF	Redes MPLS Separadas	Redes MPLS Fusionada
Equipos Red Empresas	vrf_GOB_1	9	30
Equipos Red BA	vrf_GOB_2	9	30
Equipos Red Móvil	vrf_GOB_3	9	30
Equipos Seguridad	vrf_GOB_4	9	30
Equipos Interconexión	vrf_GOB_5	9	30
Gestión Equipos Fabricante Huawei	vrf_DCN_1	30	30
Gestión Equipos Fabricante Alcatel	vrf_DCN_2	30	30
Gestión Equipos Plataformas Radio	vrf_DCN_3	30	30
….			
Gestión Equipos Fabricante 10	vrf_DCN_10	30	30

El resultado obtenido muestra que de implementar la Integración de las dos redes MPLS, las VRFs que pertenecen a la red MPLS GOB aumentan su cobertura de 9 a 30 nodos, lo cual representa un incremento de cobertura del 230%.

4.1.5. Confiabilidad de la red.

Se analiza el impacto de la implementación de protocolos de alta disponibilidad sobre la confiabilidad de la red, comparando el valor de la confiabilidad del sistema inicial y el que se obtiene luego de implementar la solución sobre un segmento de red utilizado para la comunicación entre un equipo gestionado de un nodo principal y un servidor de gestión.

En la figura 4.1 se muestra el segmento de red cuya confiabilidad será evaluada.

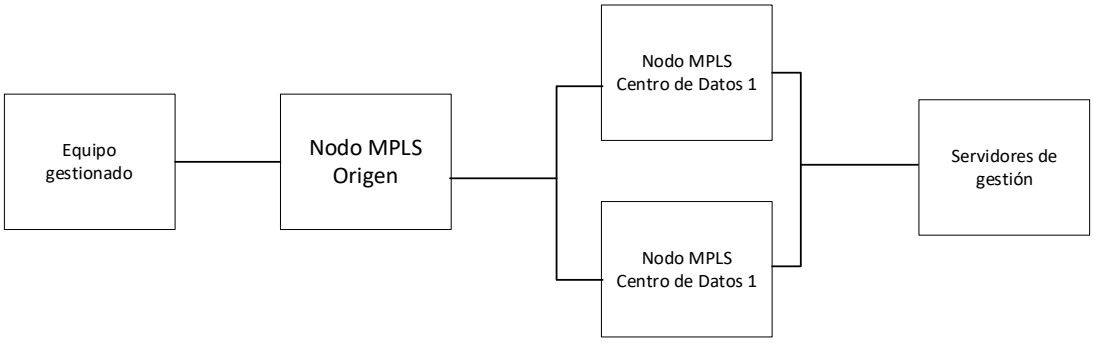


Figura 4.1 Segmento de red a evaluar (fuente. Elab. Propia)

Confiabilidad inicial de la red

Se calcula primero la confiabilidad en un nodo, para esto se esquematizan los equipos y conexiones en el nodo. En la figura 4.2 se muestra el esquema resultante de los equipos y conexiones existentes en un nodo principal sin ningún protocolo de alta disponibilidad.

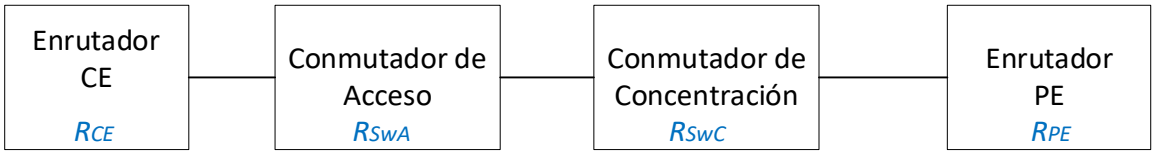


Figura 4.2 Sistema inicial en un nodo (fuente. Elab. Propia)

En la fórmula (4.1) se muestra la relación a utilizar para el cálculo de la confiabilidad del sistema de la figura 4.2.

$$R_N = R_{CE} \times R_{SwA} \times R_{SwC} \times R_{PE} \quad (4.1)$$

Donde:

R_N = Confiabilidad del sistema en un nodo

R_{CE} = Confiabilidad del enrutador CE

R_{SwA} = Confiabilidad del conmutador de acceso

R_{SwC} = Confiabilidad del conmutador de concentración

R_{PE} = Confiabilidad del enrutador PE

El cálculo de la confiabilidad de cada dispositivo se obtiene según la fórmula (4.2)

$$R = \frac{MTBF}{MTBF + MTTR} \quad (4.2)$$

Donde:

R = Confiabilidad del dispositivo

$MTBF$ = Tiempo medio antes de falla

$MTTR$ = Tiempo medio de recuperación

Para el caso de estudio, se utilizan los mismos valores de $MTBF$ y $MTTR$ en todos los equipos, por tanto $R = R_{CE} = R_{SwA} = R_{SwC} = R_{PE}$.

$MTTR = 8\ horas$ (tiempo promedio para detectar un equipo averiado y reemplazarlo)

$MTBF = 8752\ horas$ (tiempo de funcionamiento del equipo sin fallas)

Remplazando estos valores en la fórmula (4.2) se obtiene $R = 0{,}9991$.

Luego al reemplazar el valor de R en la fórmula (4.1) obtenemos: $R_N = 0{,}9964$.

Para la evaluación de la confiabilidad del segmento de red, se utiliza el esquema mostrado en la figura 4.3, donde N_1 representa al nodo principal mientras que N_2 y N_3 representan a los Centros de Datos en alta disponibilidad.

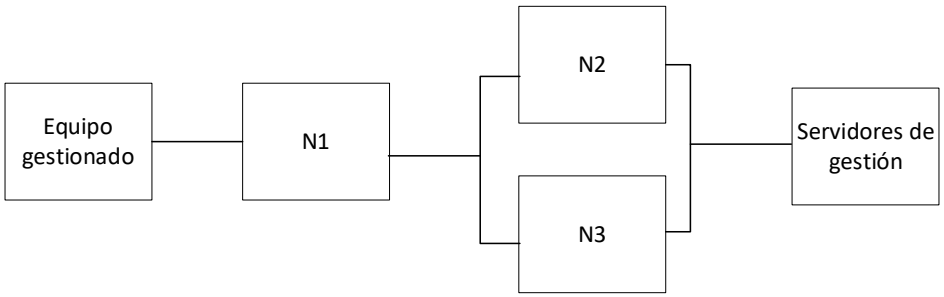


Figura 4.3 Sistema con alta disponibilidad en un nodo (fuente. Elab. Propia)

En la fórmula (4.3) se muestra la relación a utilizar para el cálculo de la confiabilidad del sistema de la figura 4.3.

$$R_S = R_{N1} \times R_{N2+N3} \quad (4.3)$$

Donde:

R_S = Confiabilidad del segmento de red evaluado

R_{N1} = Confiabilidad del nodo 1

R_{N2+N3} = Confiabilidad del nodo 2 y 3 en alta disponibilidad

El cálculo de la confiabilidad en un sistema con alta disponibilidad se obtiene según la fórmula (4.4)

$$R_{A+B} = 1 - [(1 - R_A) \times (1 - R_B)] \quad (4.4)$$

Donde:

R_{A+B} = Confiabilidad del sistema en alta disponibilidad A+B

R_A = Confiabilidad del sistema A

R_B = Confiabilidad del sistema B

Reemplazando el valor de $R_N = R_{N1} = R_{N2} = R_{N3} = 0{,}9964$ en la fórmula (4.4) y luego en la fórmula (4.3) se obtiene $R_S = 0{,}9963$, equivalente a una confiabilidad del 98,63%.

Confiabilidad de la red implementando la solución.

Se calcula primero la confiabilidad de un nodo principal luego de implementar la solución con protocolos de alta disponibilidad.

En la figura 4.4 se muestra el esquema resultante de los equipos y conexiones existentes en un nodo principal luego de implementar protocolos de alta disponibilidad.

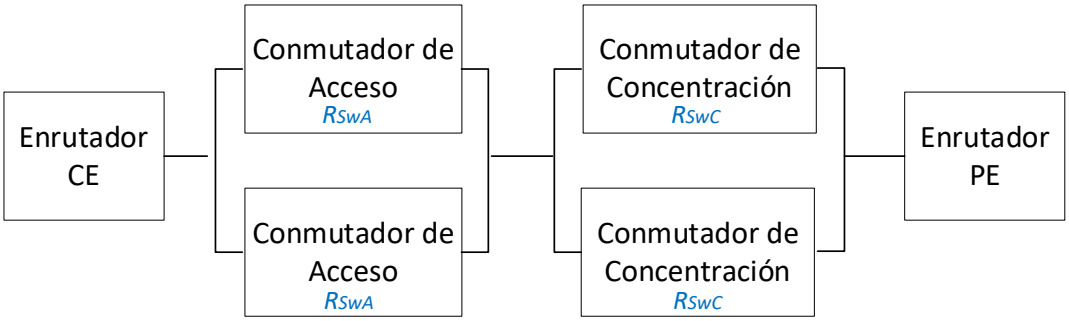


Figura 4.4 Sistema con alta disponibilidad en un nodo (fuente. Elab. Propia)

En la fórmula (4.5) muestra la relación a utilizar para el cálculo de la confiabilidad del sistema de la figura 4.4.

$$R_N = R_{CE} \times R_{SwA+SwA} \times R_{SwC+SwC} \times R_{PE} \quad (4.5)$$

Donde:

R_N = Confiabilidad de un nodo

R_{CE} = Confiabilidad del enrutador CE

$R_{SwA+SwA}$ = Confiabilidad del conmutador de acceso en alta disponibilidad

$R_{SwC+SwC}$ = Confiabilidad del conmutador de concentración en alta disponibilidad

R_{PE} = Confiabilidad del enrutador PE

Al considerar las mismas condiciones que en el caso anterior:

$MTTR = 8\ horas$

$MTBF = 8752\ horas$

Con estos valores y la fórmula (4.4) en la fórmula (4.5) se obtiene: $R_N = 0{,}9991$.

Finalmente, al reemplazar el valor de $R_N = R_{N1} = R_{N2} = R_{N3} = 0{,}9982$ en las fórmulas (4.4) y (4.3) se obtiene $R_S = 0{,}9982$, equivalente a una confiabilidad del 99,82%.

El resultado obtenido en este indicador muestra una mejora en la disponibilidad de las redes de gestión fuera de banda, que pasa del 98,63% al 99,82%, que equivale a pasar de un tiempo de indisponibilidad anual de 32 horas a 16 horas optimizando el tiempo de indisponibilidad en un 50%.

4.1.6. Resumen de resultados.

El análisis de los resultados muestra que al implementar la Integración de las redes MPLS en el proveedor se servicios se mejoran los indicadores escogidos de las redes de gestión fuera de banda cumpliendo con el requerimiento de optimización.

En la tabla 4.8 se muestran los porcentajes de optimización obtenidos por cada indicador.

Tabla 4.8 Resultados obtenidos por indicador (Fuente: Elab. propia)

Indicador	Mejora	% Optimizacion
Cantidad de equipos requeridos (Disminuye la cantidad total de equipos requeridos)	SI	15
Utilización de capacidades de los equipos adquiridos (Mejora el aprovechamiento de recursos de los enrutadores)	SI	15
Cantidad de enlaces requeridos (Disminución de enlaces 1G requeridos)	SI	44
Cobertura geográfica (Aumento de cobertura de nodos Red MPLS GOB)	SI	230
Confiabilidad de la red (Disminuye el tiempo de indisponibilidad de la red)	SI	50

4.2. Análisis de Costos

En el análisis de costos se comparan los Costos de Inversión y los Costos de Operación en caso de mantener ambas redes separadas y cuando se implementa la Integración.

Los Costos de Inversión, conocidos también como Gastos de Capital (CAPEX, *Capital Expenditure*), son los gastos realizados por una empresa al adquirir bienes a modo de inversión en el negocio y se deprecian durante el ciclo de vida del activo.

Los costos de operación o gastos operativos (OPEX, *Operation Expenditure*), son los gastos incurridos durante la operación diaria del negocio incluyendo gastos generales, administrativos, investigación y desarrollo, etc.

4.2.1. Costos al mantener las redes separadas

Costos de Inversión

Para el cálculo del CAPEX se considera la compra de enrutadores, conmutadores, cableados, adecuaciones físicas y servicios profesionales para desplegar el proyecto.

En la tabla 4.9 se muestra los Costos de Inversión al mantener separadas las redes MPLS de gestión fuera de banda.

Tabla 4.9 Costos de Inversión con redes MPLS separadas (Fuente: Elab. propia)

Ítem	Cant.	Precio USD	Total USD
Equipamiento			
Enrutadores	9	43550	391950
Conmutadores Concentración	14	20000	280000
Conmutadores de Acceso	14	8900	124600
Transceptores 10G SR	36	995	35820
Transceptores 10G LR	18	3995	71910
Transceptores 10G ER	4	10000	40000
Transceptores 1G LX/LH	64	995	63680
Cableados			
Fibra Óptica Dúplex Monomodo - long.prom. 40m.	80	63	5040
Fibra Óptica Dúplex Multimodo - long. 5m.	20	28	560
Cableado UTP RJ45 Categoría 6 - caja 305m.	25	200	5000
Cableado Coaxial - long. prom. 50 m	4	50	200
Cableado para Energía y aterramiento 12AWG (rollos 100m por colores)	50	35	1750
Adecuaciones para el cableado	18	400	7200
Servicios Profesionales	1		30000
Total (USD)			**1057710**

Costos de Operación

Para el cálculo del OPEX se incluye el costo de Soporte y Mantenimiento realizado por personal propio del proveedor (NOC), la Asistencia Técnica de la empresa que implementa la solución y el Contrato de soporte con el fabricante. El costo de Soporte y Mantenimiento

se estima en un valor de 5% del gasto realizado en la adquisición del nuevo equipamiento. El valor obtenido se suma al OPEX de la planta existente estimado en 250 mil dólares.

En la tabla 4.10 se muestran el Costo de Operación al mantener separadas las redes MPLS de gestión fuera de banda.

Tabla 4.10 Costos de operación con redes MPLS separadas (Fuente: Elab. propia)

Detalles	Precio USD
Costos de Soporte y Mantenimiento	51386
Asistencia Técnica con el Proveedor	10000
Contratos de Soporte con el Fabricante	60000
OPEX Anual equipamiento nuevo	**121386**
OPEX planta existente	250000
OPEX Anual Total	**371386**

4.2.2. Costos de la Integración de redes MPLS fuera de banda

Costos de Inversión

Incluye: Compra de equipamiento, Instalación física y cableados y los servicios profesionales para el desarrollo del proyecto. El costo por concepto de servicios profesionales aumenta por la complejidad de las tareas a realizar.

En la tabla 4.11 se muestran los costos de Inversión al implementar la Integración de redes MPLS gestión fuera de banda.

Tabla 4.11 Costos de Inversión e Instalación (Fuente: Elab. propia)

Ítem	Cant.	Precio USD	Total USD
Equipamiento			
Enrutadores (solo tarjetas)	9	8000	72000
Conmutadores Concentración	14	20000	280000
Conmutadores de Acceso	14	8900	124600
Transceptores 10G SR	36	995	35820
Transceptores 10G LR	18	3995	71910
Transceptores 10G ER	4	10000	40000
Transceptores 1G LX/LH	64	995	63680
Cableados			
Fibra Óptica Dúplex Monomodo - long.prom. 40m.	80	63	5040
Fibra Óptica Dúplex Multimodo - long. 5m.	20	28	560
Cableado UTP RJ45 Categoría 6 - caja 305m.	25	200	5000
Cableado Coaxial - long. Prom. 50 m	4	50	200
Cableado para Energía y aterramiento 12AWG (rollos 100m por colores)	50	35	1750
Adecuaciones para el cableado	18	400	7200
Servicios Profesionales del Integrador	1		50000
Total			**757760**

Otros costos tales como la construcción de nuevas instalaciones, sistemas de energía de corriente continua, adecuaciones de sala de datos, aire acondicionado, sistemas contra incendios no se toman en cuenta puesto que son parte de la infraestructura existente.

Costos de Operación

Se incluye el costo de Soporte y Mantenimiento realizado por personal propio del proveedor (NOC), la Asistencia Técnica de la empresa que implementa la solución y el Contrato de soporte con el fabricante. El costo de Soporte y Mantenimiento se estima en un valor de 5% del gasto realizado en la adquisición del nuevo equipamiento. El valor obtenido se suma al OPEX de la planta existente estimado en 200 mil dólares puesto que se apagarán los equipos cuyo rol es asumido por equipos de la MPLS DCN.

No se consideran los costos de alquiler de local, pago de licencias a las municipalidades, seguridad física, entre otros pues ya son asumidos por el proveedor de servicios en otras partidas contables.

En la tabla 4.12 se muestran los costos de OPEX al implementar la Integración de redes MPLS gestión fuera de banda.

Tabla 4.12 Costos de operación (Fuente: Elab. propia)

Detalles	Precio USD
Costos de Operación y Mantenimiento	35388
Asistencia Técnica con el Proveedor	10000
Contratos de Soporte con el Fabricante	30000
OPEX Anual	**75388**
OPEX planta existente	200000
OPEX Anual total	**275388**

4.2.3. Resultado del Análisis de Costos.

El resultado obtenido muestra un ahorro en gastos de CAPEX de aprox. 300 mil dólares (ahorro del 28,4%) y OPEX anual, en aprox. 96 mil dólares anuales (ahorro del 25,8%).

En la tabla 4.13 se muestran los costos de CAPEX y OPEX al mantener separadas las redes MPLS y con la Integración de las redes MPLS y los ahorros obtenidos.

Tabla 4.13 Costos de CAPEX y OPEX (Fuente: Elab. propia)

	Redes Separadas	Integración	Ahorro	
	(USD)	(USD)	(USD)	%
CAPEX	757760	1057710	299950	28,4
OPEX (1 año)	275388	371386	95998	25,8

CONCLUSIONES

1. En el presente informe se concluye que la Integración de las dos redes MPLS permite optimizar la gestión fuera de banda de dispositivos de red en el proveedor de servicios de telecomunicaciones.
2. Se concluye, basado en el caso de estudio, que la Integración de las dos redes MPLS aprovecha de mejor manera las capacidades de hardware y software de los equipos de gestión fuera de banda que cuando las redes MPLS se mantienen separadas.
3. Se concluye, basado en el caso de estudio, que la Integración de las dos redes MPLS mejora la disponibilidad a nivel WAN y LAN de las redes de gestión fuera de banda en el proveedor de servicios.
4. Se concluye, basado en el caso de estudio, que la Integración de las dos redes MPLS unifica las topologías aumentando las capacidades de cobertura, ancho de banda y enlaces de las redes de gestión fuera de banda en el proveedor de servicios.
5. Se concluye, basado en el caso de estudio, que la Integración de las dos redes MPLS optimiza los gastos en costos de Inversión (CapEx) y operación (OpEx) que realiza el proveedor de servicios en las redes de gestión fuera de banda.

RECOMENDACIONES

1. Las actividades de implementación deben involucrar al personal encargado de las tareas de operación y mantenimiento de las plataformas para las validaciones antes, durante y después de las ventanas de mantenimiento.
2. La fase de diseño es de vital importancia y el personal a cargo de la elaboración de los documentos de diseño de alto y bajo nivel debe contar con los conocimientos suficientes para su elaboración, además de la participación de las distintas áreas del proveedor de servicios que ellos convoquen a fin de mapear todos los requerimientos y considerarlos en la ingeniería de detalle.
3. El cronograma inicial del proyecto debe tomar en cuenta los periodos de congelamiento de la planta por feriados, festividades o eventos importantes dentro del plan de implementación.
4. Los recursos de energía en los nodos y fibra óptica internodal deben ser solicitados en las fases iniciales del proyecto pues son recursos vitales para la implementación y en caso de no existir será necesario solicitar otro proyecto al área encargada lo cual podría significar demoras de hasta algunos meses para todo el proyecto.
5. El equipo de operación monitorear y revisar periódicamente la definición de políticas de QoS para hacer ajustes en las mismas puesto que las necesidades del tráfico pueden variar a lo largo del tiempo.
6. Las actividades de operación y mantenimiento de la red MPLS final de Gestión Fuera de Banda deben quedar bajo responsabilidad del equipo de operaciones de la red Core IP/MPLS de servicios pues es el que tiene mayor experiencia y conocimientos sobre las tecnologías implementadas.
7. El proyecto debe contar con el respaldo e interés de las gerencias responsables de la Ingeniería y Operación de las plataformas que la usan para evitar demoras en el tiempo de implementación por no contar con su aprobación para la ejecución de ventanas de mantenimiento.

BIBLIOGRAFIA

[1] betterbuys.com, «Compare Top Network Monitoring Tools Software,» 2018. https://www.betterbuys.com/network-monitoring/.

[2] OSIPTEL, «Resultados de Mediciones de Calidad de los Servicios Públicos de Telecomunicaciones (ENE-JUN 2019),» 2019.

[3] Andina, «Agencia Peruana de Noticias,» 2019. https://andina.pe/agencia/noticia-osiptel-sanciono-a-telefonica-multa-mas-s-35-millones-750836.aspx.

[4] Cisco Systems, Cisco SAFE Reference Guide, California, USA, 2010.

[5] Cisco Systems, Catalyst 2960-S Switch Hardware Installation Guide, 2019.

[6] R. Gerhards, The Syslog Protocol, RFC 5424, Marzo 2009.

[7] A. Tanenbaum y D. Wetherall, Redes de Computadoras, México: PEARSON EDUCACIÓN, 2012.

[8] Infinite Cables Inc., «Fiber Optic Cables & Couplers,» 2003. https://www.ira.inaf.it/Computing/tecnica/FIBRE/fiber.html.

[9] C. Lopez, «Cuatro tipos comunes de conectores de fibra óptica,» medium.com, 2017. https://medium.com/@clopez.stark/cuatro-tipos-comunes-de-conectores-de-fibra-%C3%B3ptica-4ada21a95541.

[10] F. Gumiel, «Diferencias entre los cables de par trenzado UTP, STP y FTP,» Telecocable.com, 2017. https://www.telecocable.com/blog/diferencias-entre-cable-utp-stp-y-ftp/1374.

[11] F. Official, «UTP vs STP Cables for 10GBASE-T Network?,» fs.com, 2017. https://www.fs.com/utp-or-stp-cables-for-10gbase-t-network-aid-580.html.

[12] Cables-Solutions, «Difference of Straight Through and Crossover Cable,» Cables-Solutions.com, 2016. http://www.cables-solutions.com/difference-between-straight-through-and-crossover-cable.html.

[13] Cisco Systems, «Cisco Transceiver Modules,» 2019.

https://www.cisco.com/c/en/us/products/interfaces-modules/transceiver-modules/index.html.

[14] S. Perez y H. Facchini, DISPOSITIVOS Y PROTOCOLOS DE REDES LAN Y WAN, Mendoza, Argentina: UTN Regional Mendoza, 2017.

[15] Cisco Systems Learning, Building Cisco Multilayer Switched Networks Volume I v3.0, 2006.

[16] Huawei Technologies, CloudEngine 8800, 7800, 6800, and 5800 V200R005C10 Configuration Guide - Ethernet Switching, 2019.

[17] Cisco Systems, Design and Configuration Guide:Best Practices for Virtual Port Channels (vPC) on Cisco Nexus 7000 Series Switches, 2006.

[18] Juniper Networks, JunOS Multichassis Link Aggregation Feature Guide for EXSeries, MXSeries, and QFX Series Devices, USA, 2019.

[19] D. Teare y C. Paquet, Authorized Self Study Guide Building Scalable Cisco Internetworks, USA: Cisco Press, 2006.

[20] L. D. Ghein, MPLS Fundamentals, IN, USA: Cisco Press, 2007.

[21] Cisco Systems Learning, Implementing Cisco MPLS v2.2 Course Student Guide Volumes I & II, USA: Cisco Systems Learning, 2006.

[22] Cisco Systems, First Hop Redundancy Protocols Configuration Guide, Cisco IOS XERelease 3S, USA, 2017.

[23] J. Evans y C. Filsfils, Deploying IP and MPLS QOS for Multiservice Networks, Theory and Practice, USA: Morgan Kaufmann Publishers, 2007.

[24] Cisco Systems, Implementing Cisco Quality of Service Volume I v2.2, 2006.

[25] Cisco Systems, Next Generation Enterprise MPLS VPN-Based MAN Design and Implementation Guide, CA: http://www.cisco.com, 2006.

[26] Cisco Systems, «Cisco ASR 900 Series Route Switch Processor Data Sheet,» https://www.cisco.com/c/en/us/products/collateral/routers/asr-903-series-aggregation-services-routers/datasheet-c78-738339.html.

[27] W. Stallings, «MPLS,» *The Internet Protocol Journal,* vol. 4, nº 3, pp. 2-14, Setiembre 2011.

[28] I. Pepelnjack y J. Guichard, MPLS and VPN Architectures, USA: Cisco Press, 2001.

[29] T. Bates, R. Chandra, D. Katz y R. Yakov, Multiprotocol Extensions for BGP-4, RFC 4760, Enero 2007.

[30] Global Knowledge, «How to Secure Cisco Routers and Switches,» 2018. https://www.globalknowledge.com/us-en/resources/resource-library/articles/how-to-secure-cisco-routers-and-switches/.

[31] J. Doyle y J. Carrell, CCIE Professional Development Routing TCP/IP, Volume I, Second Edition, Cisco Press, 2005.

[32] T.-C. Publishing's, «Queuing and Scheduling (QOS-Enabled Networks), what-when-how,» The-Crankshaft Publishing's. http://what-when-how.com/qos-enabled-networks/queuing-and-scheduling-qos-enabled-networks-part-1/.

[33] Cisco Systems, «Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting,» Cisco Systems, 2014. https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-policing/19645-policevsshape.html.

[34] P. Lapukhov, «Understanding Single-Rate and Dual-Rate Traffic Policing,» INE Inc., 2011. https://blog.ine.com/2011/05/22/understanding-single-rate-and-dual-rate-traffic-policing.

ANEXO A
GLOSARIO DE TERMINOS

AAA	Authorization Authorization Accounting
Best Effort	Mejor esfuerzo
BPDU	Bridge Protocol Data Unit
CAPEX	Capital Expenditures
CRC	Cyclic redundancy check
Delay	Retardo o latencia
DiffServ	Servicios Diferenciados
E1	Formato de transmisión digital 2048 Mbps
IGP	Interior Gateway Protocol
IntServ	Servicios Integrados
IP	Internet Protocol
IS-IS	Intermediate System-to-Intermediate System
ITU-T	International Union for Telecommunications, Telecommunications
Jitter	Variación en el retardo
LACP	Link Aggregation Control Protocol
LAG	Link Agregarían Group
LAN	Local Area Network
LLQ	Low Latency Queuing
Log	Registro de información
Loopback	Interfaces lógicas de bucle de retorno
MCR	Minimum Cell Rate
MIB	Management Information Base
MPLS	Multi Protocol Label Switching
MQC	Modular QoS CLI
NTP	Network Time Protocol
ODF	Optical Distribution Frame
OPEX	Operational Expenditures
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PCR	Peak Cell Rate
PHB	Per-Hop Behavior
QoS	Quality of Service
Queuing	Encolamiento
RFCs	Request for Comments
RMA	Return Merchandise Authorization
RMON	Remote Monitoring
Router	Enrutador
RSVP	Resource Reservation Protocol
Scheduler	Programador
SLA	Service Level Agreement
STP	Spanning Tree Protocol
SVC	Switched Virtual Circuit
Switch	Conmutador Ethernet
TCP	Transfer Control Protocol

TDM	Time Division Multiplexing
ToS	Type of Service
TSS	Technnical Site Survey
UDP	User Datagram Protocol
VoIP	Voice over IP
WRED	Weighted Randomly Early Detected

ANEXO B
SITUACION INICIAL MPLS GOB:
TOPOLOGÍA ACCESO PE-CE

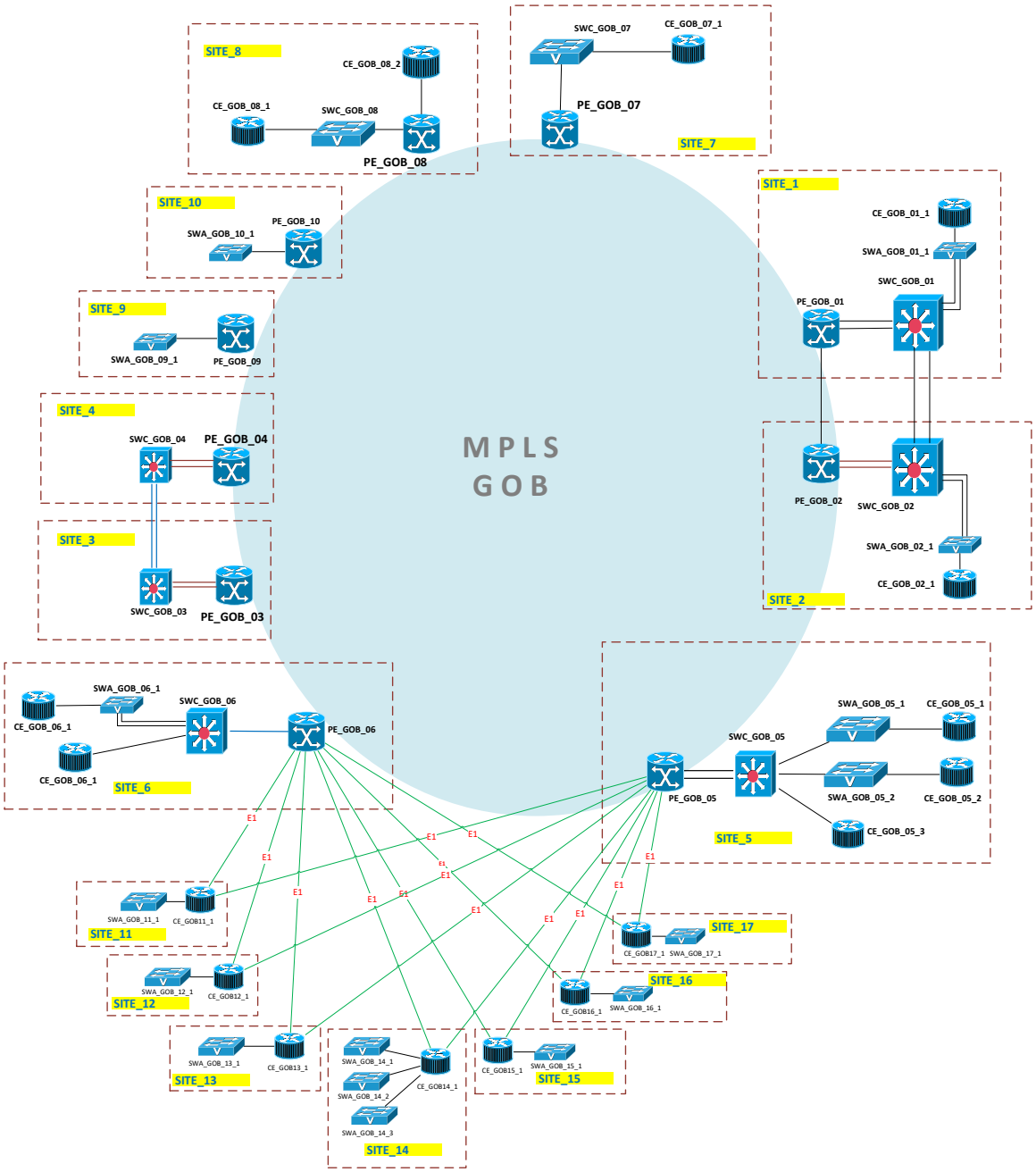


Figura B.1 Situación Inicial MPLS GOB: Topología Acceso PE-CE (Fuente: Elab. propia)

ANEXO C
SITUACION INICIAL MPLS DCN: ADYACENCIAS IS-IS, LDP Y SESIONES BGP

Tabla C.1 Situación Inicial MPLS DCN: Adyacencias ISIS y LDP (Fuente: Elab. propia)

PE	Neighbor System Id	Tipo	Type ISIS	State ISIS	State LDP
PE_TX_01	PE_TX_02	1G	L2	UP	UP
PE_TX_01	PE_TX_03	1G	L2	UP	UP
PE_TX_01	PE_TX_06	1G	L2	UP	UP
PE_TX_01	PE_TX_09	1G	L2	UP	UP
PE_TX_01	PE_TX_10	1G	L2	UP	UP
PE_TX_03	PE_TX_06	1G	L2	UP	UP
PE_TX_03	PE_TX_07	1G	L2	UP	UP
PE_TX_03	PE_TX_08	1G	L2	UP	UP
PE_TX_03	PE_TX_09	1G	L2	UP	UP
PE_TX_03	PE_TX_13	1G	L2	UP	UP
PE_TX_03	PE_TX_16	1G	L2	UP	UP
PE_TX_04	PE_TX_08	1G	L2	UP	UP
PE_TX_04	PE_TX_09	1G	L2	UP	UP
PE_TX_05	PE_TX_06	1G	L2	UP	UP
PE_TX_05	PE_TX_09	1G	L2	UP	UP
PE_TX_06	PE_TX_26	1G	L2	UP	UP
PE_TX_06	PE_TX_31	1G	L2	UP	UP
PE_TX_07	PE_TX_08	1G	L2	UP	UP
PE_TX_09	PE_TX_15	1G	L2	UP	UP
PE_TX_10	PE_TX_11	1G	L2	UP	UP
PE_TX_10	PE_TX_12	1G	L2	UP	UP
PE_TX_10	PE_TX_16	1G	L2	UP	UP
PE_TX_11	PE_TX_15	1G	L2	UP	UP
PE_TX_11	PE_TX_17	1G	L2	UP	UP
PE_TX_11	PE_TX_19	1G	L2	UP	UP
PE_TX_12	PE_TX_13	1G	L2	UP	UP
PE_TX_13	PE_TX_18	1G	L2	UP	UP
PE_TX_13	PE_TX_18	1G	L2	UP	UP
PE_TX_14	PE_TX_19	1G	L2	UP	UP
PE_TX_14	PE_TX_20	1G	L2	UP	UP
PE_TX_15	PE_TX_20	1G	L2	UP	UP
PE_TX_15	PE_TX_22	1G	L2	UP	UP
PE_TX_16	PE_TX_17	1G	L2	UP	UP
PE_TX_20	PE_TX_21	1G	L2	UP	UP
PE_TX_22	PE_TX_23	1G	L2	UP	UP
PE_TX_23	PE_TX_25	1G	L2	UP	UP
PE_TX_25	PE_TX_27	1G	L2	UP	UP
PE_TX_25	PE_TX_30	1G	L2	UP	UP
PE_TX_26	PE_TX_30	1G	L2	UP	UP
PE_TX_27	PE_TX_28	1G	L2	UP	UP
PE_TX_27	PE_TX_30	1G	L2	UP	UP
PE_TX_28	PE_TX_29	1G	L2	UP	UP
PE_TX_28	PE_TX_31	1G	L2	UP	UP
PE_TX_30	PE_TX_31	1G	L2	UP	UP
PE_TX_30	PE_TX_32	1G	L2	UP	UP
PE_TX_31	PE_TX_32	1G	L2	UP	UP

Tabla C.2 Situación Inicial MPLS DCN: Sesiones BGP (Fuente: Elab. propia)

PE	RR	Descripción	PE	RR	Descripción
PE_TX_01	PE_TX_03	RR1 Lima	PE_TX_18	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_02	PE_TX_03	RR1 Lima	PE_TX_19	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_04	PE_TX_03	RR1 Lima	PE_TX_20	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_05	PE_TX_03	RR1 Lima	PE_TX_21	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_07	PE_TX_03	RR1 Lima	PE_TX_22	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_08	PE_TX_03	RR1 Lima	PE_TX_23	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_09	PE_TX_03	RR1 Lima	PE_TX_25	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_11	PE_TX_03	RR1 Lima	PE_TX_26	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_12	PE_TX_03	RR1 Lima	PE_TX_27	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_13	PE_TX_03	RR1 Lima	PE_TX_28	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_14	PE_TX_03	RR1 Lima	PE_TX_29	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_15	PE_TX_03	RR1 Lima	PE_TX_31	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_16	PE_TX_03	RR1 Lima	PE_TX_32	PE_TX_03	RR1 Lima
	PE_TX_06	RR2 Lima		PE_TX_06	RR2 Lima
PE_TX_17	PE_TX_03	RR1 Lima			
	PE_TX_06	RR2 Lima			

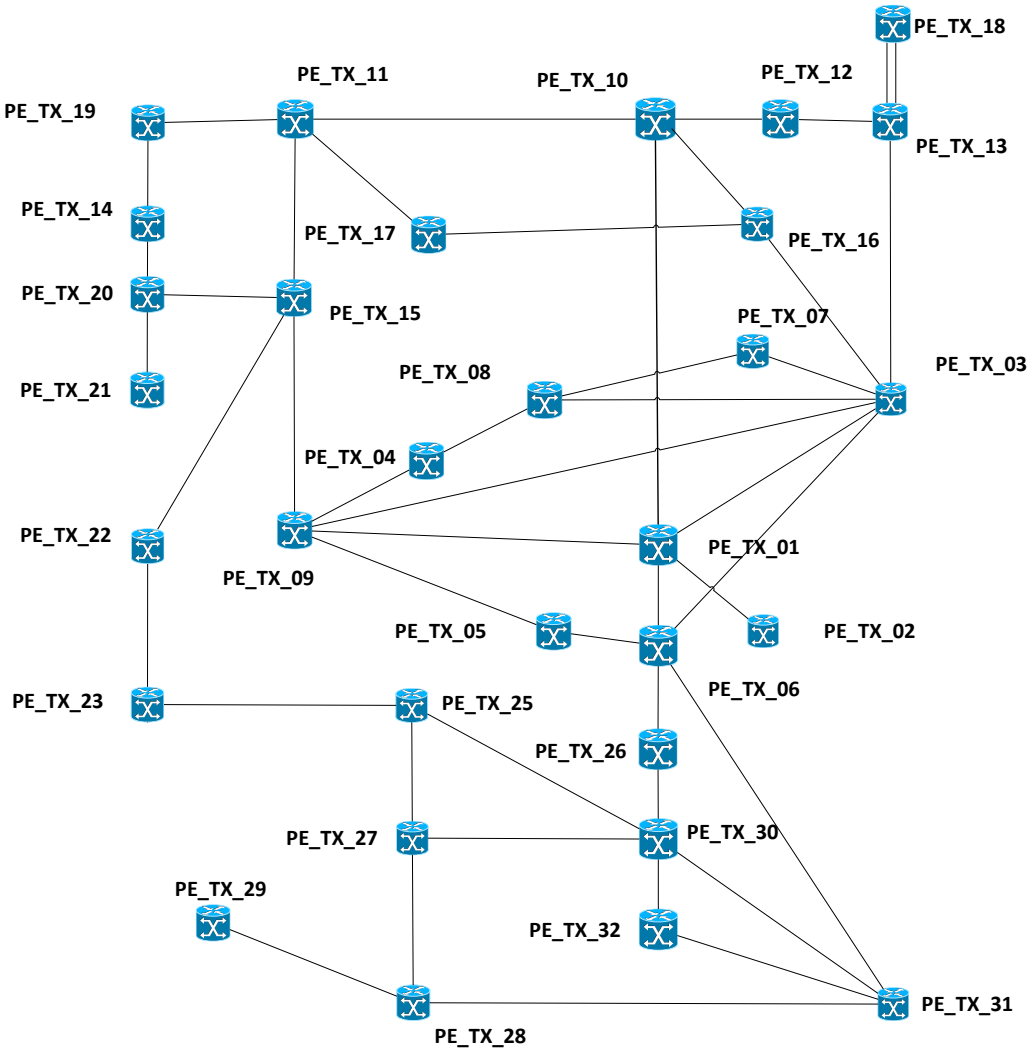


Figura C.1. Situación Inicial MPLS DCN: Topología física (Fuente: Elab. propia)

ANEXO D
SOLUCIÓN PROPUESTA MPLS FUSIONADA

Tabla D.1 Solución propuesta MPLS Fusionada: Enlaces requeridos (Fuente: Elab. propia)

Enlace	Cable	Longitud de Onda	Distancia	Norma
PE_TX_01 <> SWC_01-1	multimodo	850 nm	< 300m	10GBASE-SR
PE_TX_01 <> SWC_01-2				
PE_TX_03 <> SWC_03-1				
PE_TX_03 <> SWC_03-2				
PE_TX_07 <> SWC_07-1				
PE_TX_07 <> SWC_07-2				
PE_TX_08 <> SWC_08-1				
PE_TX_08 <> SWC_08-2				
PE_TX_09 <> SWC_09-1				
PE_TX_09 <> SWC_09-2				
PE_TX_33 <> SWC_33-1				
PE_TX_33 <> SWC_33-2				
PE_TX_34 <> SWC_34-1				
PE_TX_34 <> SWC_34-2				
SWC_01-1 <> SWC_08-1	monomodo	1310 nm	< 10Km	10GBASE-LR
SWC_01-2 <> SWC_33-2				
SWC_03-1 <> SWC_08-1				
SWC_03-2 <> SWC_08-2				
SWC_03-1 <> SWC_07-1				
SWC_03-1 <> SWC_34-2				
SWC_03-2 <> SWC_33-1				
SWC_07-2 <> SWC_08-2				
SWC_08-2 <> SWC_34-1				
SWC_09-2 <> SWC_34-2				
SWC_03-1 <> SWC_09-1	monomodo	1550 nm	< 40Km	10GBASE-ER
SWC_08-2 <> SWC_09-2				
PE_TX_10 <> SWC_03-1	monomodo	1310 nm	-	1000BASE-LX (el transporte intermedio es DWDM)
PE_TX_10 <> SWC_08-2				
PE_TX_30 <> SWC_03-2				
PE_TX_30 <> SWC_08-1				

Tabla D.2 Solución propuesta: Relación de IS-IS Direcciones NET (Fuente: Elab. propia)

		NSAP		
Nodos	**Router ID**	**Área**	**System ID**	**NSEL**
PE_TX_01	11.0.0.1	47.0000 .	0b00.0001 . 0200 .	00
PE_TX_02	11.0.0.2	47.0000 .	0b00.0002 . 0200 .	00
PE_TX_03	11.0.0.3	47.0000 .	0b00.0003 . 0200 .	00
PE_TX_04	11.0.0.4	47.0000 .	0b00.0004 . 0200 .	00
PE_TX_05	11.0.0.5	47.0000 .	0b00.0005 . 0200 .	00
PE_TX_06	11.0.0.6	47.0000 .	0b00.0006 . 0200 .	00
PE_TX_07	11.0.0.7	47.0000 .	0b00.0007 . 0200 .	00
PE_TX_08	11.0.0.8	47.0000 .	0b00.0008 . 0200 .	00
PE_TX_09	11.0.0.9	47.0000 .	0b00.0009 . 0200 .	00
PE_TX_10	11.0.0.10	47.0000 .	0b00.000a . 0200 .	00
PE_TX_11	11.0.0.11	47.0000 .	0b00.000b . 0200 .	00
PE_TX_12	11.0.0.12	47.0000 .	0b00.000c . 0200 .	00
PE_TX_13	11.0.0.13	47.0000 .	0b00.000d . 0200 .	00
PE_TX_14	11.0.0.14	47.0000 .	0b00.000e . 0200 .	00
PE_TX_15	11.0.0.15	47.0000 .	0b00.000f . 0200 .	00
PE_TX_16	11.0.0.16	47.0000 .	0b00.0010 . 0200 .	00
PE_TX_17	11.0.0.17	47.0000 .	0b00.0011 . 0200 .	00
PE_TX_18	11.0.0.18	47.0000 .	0b00.0012 . 0200 .	00
PE_TX_19	11.0.0.19	47.0000 .	0b00.0013 . 0200 .	00
PE_TX_20	11.0.0.20	47.0000 .	0b00.0014 . 0200 .	00
PE_TX_21	11.0.0.21	47.0000 .	0b00.0015 . 0200 .	00
PE_TX_22	11.0.0.22	47.0000 .	0b00.0016 . 0200 .	00
PE_TX_23	11.0.0.23	47.0000 .	0b00.0017 . 0200 .	00
PE_TX_25	11.0.0.25	47.0000 .	0b00.0019 . 0200 .	00
PE_TX_26	11.0.0.26	47.0000 .	0b00.001a . 0200 .	00
PE_TX_27	11.0.0.27	47.0000 .	0b00.001b . 0200 .	00
PE_TX_29	11.0.0.28	47.0000 .	0b00.001c . 0200 .	00
PE_TX_29	11.0.0.29	47.0000 .	0b00.001d . 0200 .	00
PE_TX_30	11.0.0.30	47.0000 .	0b00.001e . 0200 .	00
PE_TX_31	11.0.0.31	47.0000 .	0b00.001f . 0200 .	00
PE_TX_32	11.0.0.32	47.0000 .	0b00.0020 . 0200 .	00
PE_TX_33	11.0.0.33	47.0000 .	0b00.0021 . 0200 .	00
PE_TX_34	11.0.0.34	47.0000 .	0b00.0022 . 0200 .	00

Tabla D.3 Solución propuesta: Adyacencias ISIS y LDP (Fuente: Elab. propia)

PE	Neighbor System Id	Tipo	Type ISIS	State ISIS
PE_TX_01	PE_TX_02	1G	L2	UP
PE_TX_01	PE_TX_03	1G	L2	UP
PE_TX_01	PE_TX_06	1G	L2	UP
PE_TX_01	PE_TX_08	10G (vlan)	L2	UP
PE_TX_01	PE_TX_09	1G	L2	UP
PE_TX_01	PE_TX_10	1G	L2	UP
PE_TX_01	PE_TX_33	10G (vlan)	L2	UP
PE_TX_03	PE_TX_06	1G	L2	UP
PE_TX_03	PE_TX_07	1G	L2	UP
PE_TX_03	PE_TX_07	10G (vlan)	L2	UP
PE_TX_03	PE_TX_08	10G (vlan)	L2	UP
PE_TX_03	PE_TX_08	1G	L2	UP
PE_TX_03	PE_TX_09	10G (vlan)	L2	UP
PE_TX_03	PE_TX_09	1G	L2	UP
PE_TX_03	PE_TX_10	1G	L2	UP
PE_TX_03	PE_TX_13	1G	L2	UP
PE_TX_03	PE_TX_16	1G	L2	UP
PE_TX_03	PE_TX_30	1G	L2	UP
PE_TX_03	PE_TX_33	10G (vlan)	L2	UP
PE_TX_03	PE_TX_34	10G (vlan)	L2	UP
PE_TX_04	PE_TX_08	1G	L2	UP
PE_TX_04	PE_TX_09	1G	L2	UP
PE_TX_05	PE_TX_06	1G	L2	UP
PE_TX_05	PE_TX_09	1G	L2	UP
PE_TX_06	PE_TX_26	1G	L2	UP
PE_TX_06	PE_TX_31	1G	L2	UP
PE_TX_07	PE_TX_08	10G (vlan)	L2	UP
PE_TX_07	PE_TX_08	1G	L2	UP
PE_TX_08	PE_TX_09	10G (vlan)	L2	UP
PE_TX_08	PE_TX_10	1G	L2	UP
PE_TX_08	PE_TX_30	1G	L2	UP
PE_TX_08	PE_TX_34	10G (vlan)	L2	UP
PE_TX_09	PE_TX_15	1G	L2	UP
PE_TX_09	PE_TX_34	10G (vlan)	L2	UP
PE_TX_10	PE_TX_11	1G	L2	UP
PE_TX_10	PE_TX_12	1G	L2	UP
PE_TX_10	PE_TX_16	1G	L2	UP
PE_TX_11	PE_TX_15	1G	L2	UP
PE_TX_11	PE_TX_17	1G	L2	UP
PE_TX_11	PE_TX_19	1G	L2	UP
PE_TX_12	PE_TX_13	1G	L2	UP
PE_TX_13	PE_TX_18	1G	L2	UP
PE_TX_13	PE_TX_18	1G	L2	UP
PE_TX_14	PE_TX_19	1G	L2	UP
PE_TX_14	PE_TX_20	1G	L2	UP
PE_TX_15	PE_TX_20	1G	L2	UP
PE_TX_15	PE_TX_22	1G	L2	UP
PE_TX_16	PE_TX_17	1G	L2	UP
PE_TX_20	PE_TX_21	1G	L2	UP
PE_TX_22	PE_TX_23	1G	L2	UP
PE_TX_23	PE_TX_25	1G	L2	UP
PE_TX_25	PE_TX_27	1G	L2	UP
PE_TX_25	PE_TX_30	1G	L2	UP
PE_TX_26	PE_TX_30	1G	L2	UP
PE_TX_27	PE_TX_28	1G	L2	UP
PE_TX_27	PE_TX_30	1G	L2	UP
PE_TX_28	PE_TX_29	1G	L2	UP
PE_TX_28	PE_TX_31	1G	L2	UP
PE_TX_30	PE_TX_31	1G	L2	UP
PE_TX_30	PE_TX_32	1G	L2	UP
PE_TX_31	PE_TX_30	1G	L2	UP
PE_TX_31	PE_TX_32	1G	L2	UP

Tabla D.4 Solución propuesta: sesiones BGP (Fuente: Elab. propia)

PE	RR	Descripción	PE	RR	Descripción
PE_TX_01	PE_TX_03	RR Lima	PE_TX_18	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_10	RR Norte
PE_TX_02	PE_TX_03	RR Lima	PE_TX_19	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_10	RR Norte
PE_TX_04	PE_TX_03	RR Lima	PE_TX_20	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_10	RR Norte
PE_TX_05	PE_TX_03	RR Lima	PE_TX_21	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_30	RR Sur		PE_TX_10	RR Norte
PE_TX_06	PE_TX_03	RR Lima	PE_TX_22	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_30	RR Sur		PE_TX_30	RR Sur
PE_TX_07	PE_TX_03	RR Lima	PE_TX_23	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_30	RR Sur
PE_TX_09	PE_TX_03	RR Lima	PE_TX_25	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_30	RR Sur
PE_TX_11	PE_TX_03	RR Lima	PE_TX_26	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_30	RR Sur
PE_TX_12	PE_TX_03	RR Lima	PE_TX_27	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_30	RR Sur
PE_TX_13	PE_TX_03	RR Lima	PE_TX_28	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_30	RR Sur
PE_TX_14	PE_TX_03	RR Lima	PE_TX_29	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_30	RR Sur
PE_TX_15	PE_TX_03	RR Lima	PE_TX_31	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_30	RR Sur
PE_TX_16	PE_TX_03	RR Lima	PE_TX_32	PE_TX_03	RR Lima
	PE_TX_08	RR Lima		PE_TX_08	RR Lima
	PE_TX_10	RR Norte		PE_TX_30	RR Sur
PE_TX_17	PE_TX_03	RR Lima			
	PE_TX_08	RR Lima			
	PE_TX_10	RR Norte			

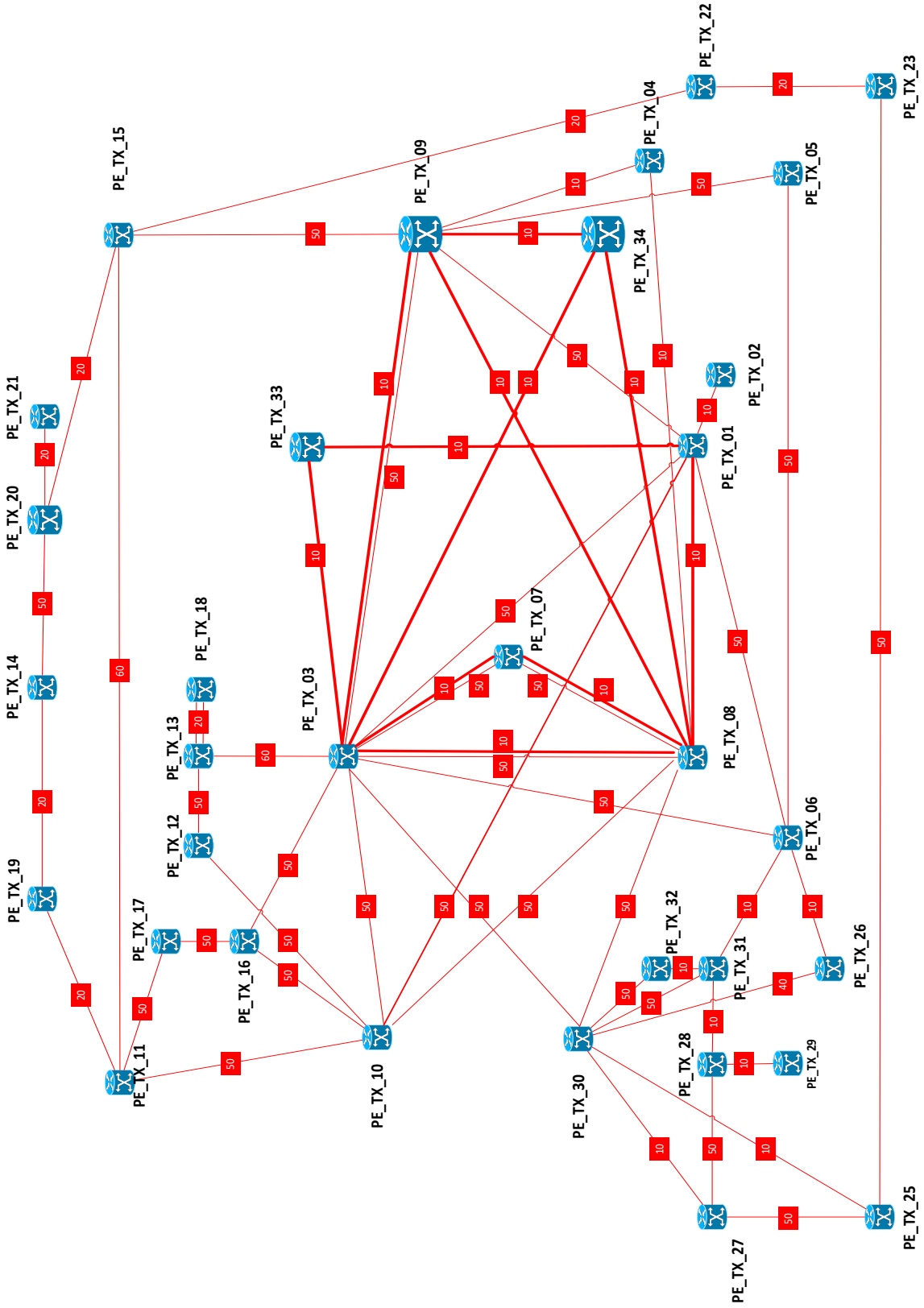


Figura D.1. Solución propuesta: Métricas IS-IS

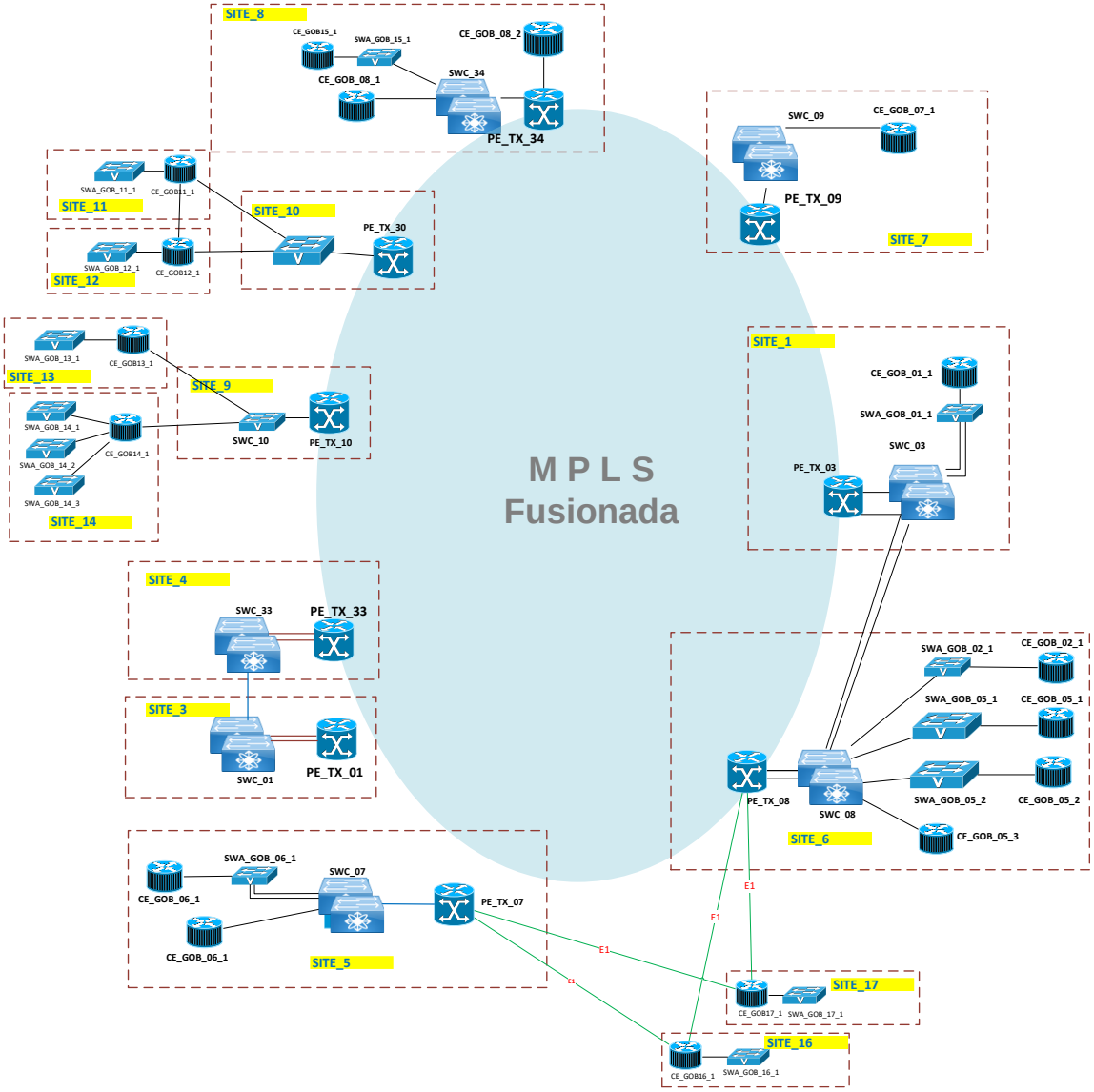


Figura D.2. Solución propuesta: Topología enlaces PE-CE