



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Implementación de servicios “Carrier Ethernet” EP-Line y EVP-Line del estándar MEF sobre la red de transporte MPLS de un Proveedor de Servicios local para la conectividad en capa 2 de clientes finales en un entorno simulado

AUTOR:

Ing. Geovanny Marcelo Avendaño Castro

**Trabajo de titulación previo a la obtención del grado de
Magister en Telecomunicaciones**

TUTOR:

Ing. Romero Paz Manuel de Jesús, MSc.

Guayaquil, a los 2 días del mes de febrero año 2018



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por Geovanny Marcelo Avendaño Castro como requerimiento parcial para la obtención del Título de Magíster en Telecomunicaciones.

TUTOR

MSc. Manuel Romero Paz

DIRECTOR DEL PROGRAMA

MSc. Manuel Romero Paz

Guayaquil, a los 2 días del mes de febrero año 2018



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES**

DECLARACIÓN DE RESPONSABILIDAD

YO, GEOVANNY MARCELO AVENDAÑO CASTRO

DECLARÓ QUE:

El trabajo de Titulación “**Implementación de servicios “Carrier Ethernet” EP-Line y EVP-Line del estándar MEF sobre la red de transporte MPLS de un Proveedor de Servicios local para la conectividad en capa 2 de clientes finales en un entorno simulado**” previo a la obtención del Título de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 2 días del mes de febrero año 2018

EL AUTOR

Ing. Geovanny Marcelo Avendaño Castro



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES**

AUTORIZACIÓN

YO, GEOVANNY MARCELO AVENDAÑO CASTRO

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación**, en la biblioteca de la institución del Trabajo de Titulación de Titulación, **“Implementación de servicios “Carrier Ethernet” EP-Line y EVP-Line del estándar MEF sobre la red de transporte MPLS de un Proveedor de Servicios local para la conectividad en capa 2 de clientes finales en un entorno simulado”** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 2 días del mes de febrero año 2018

EL AUTOR

Ing. Geovanny Marcelo Avendaño Castro

REPORTE DE URKUND

Documento: [AVENDANO GEOVANNY V1 - 4 \(3\).docx](#) (D34321171)

Presentado: 2018-01-03 11:35 (-05:00)

Presentado por: orlandophilco_7@hotmail.com

Recibido: orlando.philco.ucsg@analysis.orkund.com

Mensaje: trabajo de titulación [Mostrar el mensaje completo](#)

1% de estas 57 páginas, se componen de texto presente en 1 fuentes.

Categoría	Enlace/nombre de archivo
	Caso Estudio MPLS para ESPCTLLC Omar Armas.pdf
	1471914844_612_PROYECTO%2528MPLS%2528CON%2528GNS3.pdf
	TESIS DE MAESTRIA LEONEL MORAN RIVERA.docx
	Memoria Tecnica de Tesis Final.docx
Fuentes alternativas	TESIS DE MAESTRIA LEONEL MORAN RIVERA.docx

Interconexión de Servicio (SI-NN – Service Interworking Network-Network Interface) 332.3.2. Metro Ethernet Forum. 34 2.3.1. Carrier Ethernet CE 2.0 35 2.3.1.1. Características CE 2.0 35 Detección de Fallas 37 Verificación y Aislamiento de Fallas 37 2.3.1.2. Servicios CE 2.0 37 E-Line 38 E-LAN 40 E-Tree 42 E-Access 45 Capítulo 3: Simulación de red con servicios CE2.0. 46 3.1. Introducción. 46 3.2. Software GNS3. 47 3.3. Equipamiento a utilizar. 50 3.4. Diseño de la red del Proveedor de Servicios. 53 3.4.1. Planificación de la topología de red 54 3.4.2. Planificación de los recursos para los equipos de red 56 3.4.2.1. Definición del Nombre del Equipo (Hostname) 56 3.4.2.2. Definición del Direccionamiento de Sistema del Equipo 59 3.4.2.3. Definición de enlaces de red 60 3.4.3. Planificación del protocolo IGP para la red 68 3.4.4. Planificación de MPLS y RSVP-TE 71 3.4.5. Planificación para MP-BGP 75 3.4.6. Planificación para Servicios del Cliente 79 3.4.6.1. Servicio 1: Conectividad entre dos sitios mediante una L3VPN 80 3.4.6.2. Servicio 2: Conectividad entre dos sitios mediante varias L3VPN 88 3.5. Planificación para migrar servicios utilizando servicios basados en CE2.0 98 3.5.1. Migración de Servicio 1 utilizando un esquema EP-Line 98 3.5.2. Migración de Servicio 2 utilizando un esquema EVP-Line 105 Conclusiones 113 Recomendaciones 114 Referencias Bibliográficas 115 Glosario de Términos 117

INDICE FIGURAS Figura 1. 1: Ejemplo de redes de comunicación en el pasado 17 Figura 1. 2: Ejemplo de redes de comunicación en el presente 18 Figura 1. 3: Ejemplo de redes de...

El análisis Urkund al Trabajo de Titulación **“Implementación de servicios “Carrier Ethernet” EP-Line y EVP-Line del estándar MEF sobre la red de transporte MPLS de un Proveedor de Servicios local para la conectividad en capa 2 de clientes finales en un entorno simulado”** a cargo del **Ing. Geovanny Marcelo Avendaño Castro**, está al 1% de coincidencias.

Agradecimientos

Agradezco a Dios por haberme otorgado la bendición para cumplir esta meta en mi vida.

A mis padres Rosendo y Narsisa por haber dedicado sus vidas a inculcar lo mejor de ellos en mí, por haber tenido la paciencia y la fortaleza para impulsarme a conseguir este logro.

A mis hermanos Paola, Karla y Fausto quienes me han servido de ejemplo y motivación.

Al Ing. Manuel Romero por haberme brindado su guía en la elaboración del presente trabajo de titulación.

A Marcelo Lopez quien ha sido un amigo infalible y un apoyo constante durante estos dos años de estudio.

Geovanny Marcelo Avendaño Castro.

Dedicatoria

Este trabajo de titulación está dedicado a mis padres Rosendo y Narsisa quienes han sido mi guía, mi ejemplo y mi soporte para caminar en la vida.

A mis hermanos Paola, Karla y Fausto quienes me han apoyado de manera incondicional y han estado presentes en cada paso que doy.

A Michelle, por el apoyo, la paciencia y el sacrificio que significó este logro.

Geovanny Marcelo Avendaño Castro.



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ROMERO PAZ MANUEL DE JESÚS

TUTOR

f. _____

PHILCO ASQUI ORLANDO

REVISOR

f. _____

CORDOVA RIVADENEIRA LUIS

REVISOR

f. _____

ROMERO PAZ MANUEL DE JESÚS

DIRECTOR DEL PROGRAMA

CONTENIDO

Resumen.....	14
Abstract	15
Capítulo 1: Descripción del Proyecto de Intervención.	16
1.1. Introducción.....	16
1.2. Antecedentes.....	20
1.3. Definición del problema	21
1.4. Justificación del Problema a Investigar.	22
1.5. Objetivos	23
1.5.1. Objetivo General:.....	23
1.5.2. Objetivos específicos:	23
1.6. Hipótesis	24
1.7. Metodología de investigación.....	24
Capítulo 2: Fundamentación Teórica.....	25
2.1. Introducción a Ethernet.....	25
2.1.1. Historia de Ethernet.	26
2.1.2. Beneficios de Ethernet.	26
2.1.3. Futuro de Ethernet.	28
2.2. MEN (Metro Ethernet Network).	28
2.2.1. Modelo de referencia para redes MEN.....	28
2.2.2. Modelo de capas para redes MEN.	29
2.2.2.1. Capa de Servicios Ethernet (ETH Layer).....	30
2.2.2.2. Capa de Servicios de Transporte (TRAN Layer)	30
2.2.2.3. Capa de Servicios de Aplicación (APP Layer).....	31
2.2.3. Puntos de referencia en redes MEN.....	31
2.2.3.1. Interface Usuario – Red (UNI – User-Network Interface)	31
2.2.3.2. Interface Red – Red Externa (E-NNI – External Network-Network Interface) .	32
2.2.3.3. Interface Red – Red Interconexión de Red (NI-NNI – Network Interworking	
Network-Network Interface)	33
2.2.3.4. Interface Red – Red Interconexión de Servicio (SI-NNI – Service Interworking	
Network-Network Interface)	33
2.3. Metro Ethernet Forum.....	33

2.3.1. Carrier Ethernet CE 2.0	35
2.3.1.1. Características CE 2.0	35
Detección de Fallas	36
Verificación y Aislamiento de Fallas	37
2.3.1.2. Servicios CE 2.0	37
E-Line	38
E-LAN	40
E-Tree	43
E-Access	45
Capítulo 3: Simulación de red con servicios CE2.0	47
3.1. Introducción	47
3.2. Software GNS3	48
3.3. Equipamiento a utilizar	51
3.4. Diseño de la red del Proveedor de Servicios	54
3.4.1. Planificación de la topología de red	55
3.4.2. Planificación de los recursos para los equipos de red	56
3.4.2.1. Definición del Nombre del Equipo (Hostname)	57
3.4.2.2. Definición del Direccionamiento de Sistema del Equipo	60
3.4.2.3. Definición de enlaces de red	61
3.4.3. Planificación del protocolo IGP para la red	68
3.4.4. Planificación de MPLS y RSVP-TE	72
3.4.5. Planificación para MP-BGP	75
3.4.6. Planificación para Servicios del Cliente	79
3.4.6.1. Servicio 1: Conectividad entre dos sitios mediante una L3VPN	80
3.4.6.2. Servicio 2: Conectividad entre dos sitios mediante varias L3VPN	89
3.5. Planificación para migrar servicios utilizando servicios basados en CE2.0	98
3.5.1. Migración de Servicio 1 utilizando un esquema EP-Line	99
3.5.2. Migración de Servicio 2 utilizando un esquema EVP-Line	105
Conclusiones	113
Recomendaciones	114
Referencias Bibliográficas	115
Glosario de Términos	117

INDICE FIGURAS

Figura 1. 1: Ejemplo de redes de comunicación en el pasado	17
Figura 1. 2: Ejemplo de redes de comunicación en el presente	18
Figura 1. 3: Ejemplo de redes de comunicación en el futuro.....	19
Figura 1. 4: Ejemplo de servicios con terminales físicos y virtuales	20
Figura 2. 1: Modelo básico de referencia para redes MEN.....	29
Figura 2. 2: Modelo de capas para redes MEN.....	30
Figura 2. 3: Interface UNI dentro de una red MEN	32
Figura 2. 4: Puntos de referencia en una red MEN	34
Figura 2. 5: Esquema de Arquitectura OAM	37
Figura 2. 6: Servicio EP-Line.....	38
Figura 2. 7: Servicio EVP-Line.....	39
Figura 2. 8: Ejemplo Servicios EVP-Line.....	40
Figura 2. 9: Servicio EP-LAN.....	41
Figura 2. 10: Servicio EVP-LAN.....	42
Figura 2. 11: Ejemplo Servicios EVP-LAN.....	42
Figura 2. 12: Servicio EP-Tree.....	43
Figura 2. 13: Servicio EVP-Tree.....	44
Figura 2. 14: Ejemplo Servicios EVP-Tree	45
Figura 2. 15: Servicio E-Access: Interconexión entre proveedor y operador ..	45
Figura 3. 1: Logo de Software GNS3.....	49
Figura 3. 2: Logo de Software GNS3.....	51
Figura 3. 3: Imagen de equipo C2691 para simulación.	53
Figura 3. 4: Imagen de equipo C7200 para simulación.	54
Figura 3. 5: Imagen de equipo C7200 IOS15.X para simulación.	54
Figura 3. 6: Topología de red a Simular	56
Figura 3. 7: Patrón de Nomenclatura para equipos de Red.....	58
Figura 3. 8: Diagrama de conexión de equipos de red.....	62
Figura 3. 9: Ingeniería del cliente – Servicio 1	82
Figura 3. 10: Ingeniería del cliente – Servicio 2	91

INDICE DE TABLAS

Tabla 2-1. Servicios CE 2.0	38
Tabla 3-1. Requerimientos mínimos GNS3	50
Tabla 3-2. Requerimientos recomendados GNS3	50
Tabla 3-3. Routers soportados en GNS3	52
Tabla 3-4. Requerimientos de simulación CISCO7200	52
Tabla 3-5. Requerimientos de simulación CISCO2691	53
Tabla 3-6. Recursos de equipamiento asignado por Sitio	59
Tabla 3-7. Direccionamiento de sistema asignado	60
Tabla 3-8. Interfaces asignadas enlaces CORE	61
Tabla 3-9. Interfaces asignadas enlaces AGREGACIÓN	62
Tabla 3-10. Descripción de interfaces origen para enlaces CORE	63
Tabla 3-11. Descripción de interfaces destino para enlaces CORE	63
Tabla 3-12. Descripción de interfaces origen para enlaces AGREGACIÓN ..	63
Tabla 3-13. Descripción de interfaces destino para enlaces AGREGACIÓN ..	64
Tabla 3-14. Direccionamiento asignado para enlaces CORE	64
Tabla 3-15. Direccionamiento asignado para enlaces AGREGACIÓN	65
Tabla 3-16. Plantilla de configuración inicial GALSRAP01 y GALSRBP02 ..	65
Tabla 3-17. Plantilla de configuración inicial GALSRCPP03 y GALSRDP04 ..	66
Tabla 3-18. Plantilla de configuración inicial GALEREE01 y GALERFE02 ..	67
Tabla 3-19. Plantilla de configuración inicial GALERGE03 y GALERHE04 ..	68
Tabla 3-20. Recursos asignados para ISIS	69
Tabla 3-21. Plantilla de configuración inicial ISIS	70
Tabla 3-22. Recursos asignados para MPLS y RSVP-TE	72
Tabla 3-23. Plantilla de configuración MPLS y RSVP-TE equipos CORE	73
Tabla 3-24. Plantilla de configuración MPLS y RSVP-TE equipos AGREGACIÓN	74
Tabla 3-25. Recursos asignados para BGP	76
Tabla 3-26. Plantilla de configuración BGP equipos RR	77
Tabla 3-27. Plantilla de configuración BGP para la red	78
Tabla 3-28. Recursos asignados para Servicio1 Cliente_A en equipos del	81
Tabla 3-29. Recursos asignados para Servicio1 Cliente_A en equipos del Cliente	82

Tabla 3-30. Configuración Servicio1 en red del Proveedor.....	83
Tabla 3-31. Configuración Servicio 1 en equipos del Cliente	84
Tabla 3-32. Recursos asignados Servicio 2 para GALERFE02.....	89
Tabla 3-33. Recursos asignados Servicio 2 para GALERHE04	90
Tabla 3-34. Recursos asignados Servicio 2 para equipos del Cliente.....	90
Tabla 3-35. Configuración Servicio 2 en red del Proveedor.....	91
Tabla 3-36. Configuración Servicio 2 en red del Cliente.....	93
Tabla 3-37. Recursos asignados para EP-Line Servicio1 en el Proveedor	100
Tabla 3-38. Recursos asignados para EP-Line Servicio1 en el Cliente	101
Tabla 3-39. Recursos asignados para EVP-Line Servicio2 en GALERFE02	106
Tabla 3-40. Recursos asignados para EVP-Line Servicio2 en GALERHE04	107
Tabla 3-41. Recursos asignados para EVP-Line Servicio2 en el Cliente	107

Resumen

El trabajo de titulación a continuación consiste en simular una red de transporte IP/MPLS (Internet Protocol / Multi-Protocol Label Switching) bajo un ambiente controlado de un típico Proveedor de Servicios sobre la cual se va a configurar VPN (Virtual Private Network) de capa 3 como método actual de aprovisionamiento y servicios Carrier Ethernet (E-Line) como nueva tendencia de aprovisionamiento hacia el cliente final, con el objetivo de optimizar los recursos en la red del proveedor y brindar al cliente un servicio en base al nuevo paradigma que se maneja en las redes de comunicación a nivel mundial. Se presentará a manera de introducción un análisis de los servicios Carrier Ethernet así como el despliegue de redes Metro Ethernet para la provisión de estos servicios, indicando las ventajas de Ethernet sobre las tecnologías antecesoras, sus características, funcionalidades, estándares de configuración y estándares de interacción entre redes, siendo el MEF (Metro Ethernet Forum) el motor de la implementación de estos estándares con la visión a futuro, al relacionar tecnologías como SDN (Software Defined Networks), NFV (Network Function Virtualization), LSO (Lifecycle Service Orchestration) que apuntan a brindar este tipo de servicios de red NaaS (Network-as-a-Service).

Palabras Claves:

IP, MPLS, VPN, Ethernet, Carrier Ethernet, MEF, SDN, NaaS, NFV, LSO.

Abstract

The titling work below consists of simulating an IP / MPLS (Internet Protocol / Multi-Protocol Label Switching) transport network under a controlled environment of a typical Service Provider on which to configure Layer 3 VPNs (Virtual Private Network) as the current provisioning method and Carrier Ethernet services (E-Line) As a new supply trend towards the end customer, with the objective of optimizing the resources in the network of the supplier and providing the customer with a service based on the new paradigm that is managed in the communication networks worldwide. An analysis of the Carrier Ethernet services as well as the deployment of Metro Ethernet networks for the provision of these services will be presented as an introduction, indicating the advantages of Ethernet over the predecessor technologies, their characteristics, functionalities, configuration standards and interaction standards Between networks, with the MEF (Metro Ethernet Forum) being the engine of the implementation of these standards with the future vision to relate technologies like SDN (Software Defined Networks), NFV (Network Function Virtualization), LSO (Lifecycle Service Orchestration) that aim to provide This type of network-as-a-service (NaaS) network services.

Key words:

IP, MPLS, VPN, Ethernet, Carrier Ethernet, MEF, SDN, NaaS, NFV, LSO.

Capítulo 1: Descripción del Proyecto de Intervención.

En el Capítulo 1 se expone al lector la introducción, antecedentes, problema, justificación, objetivos generales y específicos, hipótesis y metodología de investigación que se utilizará para el desarrollo del trabajo de titulación.

1.1. Introducción.

El desarrollo del tema a tratar en este documento, pretende mostrar al lector la importancia de Ethernet como el principal protocolo de transporte en las redes de comunicación de un proveedor de servicios local, al permitir la extensión de los dominios de redes LAN (Local Area Network) hacia entornos WAN (Wide Area Network) con la optimización en cuanto al uso compartido de servicios privados definidos por el estándar MEF a nivel mundial, beneficiando de esta manera al Proveedor de Servicios al optimizar los recursos sobre su red de comunicación y al cliente final al proporcionarle un servicio con visión al futuro que le permita su administración, operación y control bajo su demanda.

Hoy en día la mayoría del tráfico que se genera en las redes de telecomunicaciones a nivel mundial son IP (Internet Protocol) y Ethernet, convirtiendo de esta manera a la segunda mencionada, como la tecnología para redes convergentes en cuanto a protocolo de transporte. La ventaja de Ethernet sobre sus competidores, ha sido la habilidad de aprovechar su gran volumen de despliegue a nivel mundial, debido a su dominio a nivel de redes empresariales, su popularidad, y de la extraordinaria capacidad de crecimiento en cuanto a las capacidades de tráfico que logra manejar, teniendo en la actualidad interfaces de hasta 100Gbps, a través de un largo proceso de adaptación que ha crecido por más de 30 años y dejando en el pasado a tecnologías TDM (Time Division Multiplexing) como transporte de redes de comunicación, figura 1.1.

Las redes WAN se encuentran en un cambio de paradigma debido a la alta y continua demanda por anchos de banda cada vez mayores, sin un aparente límite a través del tiempo. Las demandas de incremento de ancho de banda crecen día a

día, lo que obliga a proveedores de servicio a brindar expectativas de aumento inmediato bajo demanda.



Figura 1. 1: Ejemplo de redes de comunicación en el pasado

Fuente: (MEF, y otros, An Industry Initiative for Third Generation Network and Services, 2016)

Usuarios de redes de telecomunicaciones demandan servicios Carrier Ethernet que sean altamente confiables, escalables, administrables y que ofrezcan calidad de servicio. Impulsando de esta manera al mercado de servicios que ha superado los \$40 billones en el 2014 y que se proyecta, para el 2018, la suma de \$60 billones, figura 1.2. (MEF, Carrier Ethernet and SDN Part 1 : An Industry Perspective, 2014).

Los proveedores de servicios deben preparar sus redes para proveer aplicaciones para la demanda de manera dinámica, ofreciendo la disponibilidad del servicio en minutos, y brindando al cliente la posibilidad de administrar/modificar su servicio en demanda.

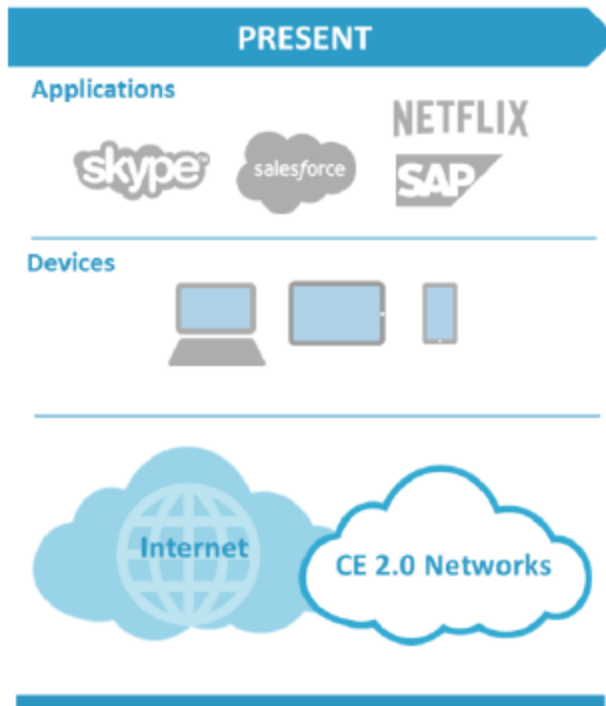


Figura 1. 2: Ejemplo de redes de comunicación en el presente

Fuente: (MEF, y otros, An Industry Initiative for Third Generation Network and Services, 2016)

El MEF ha trabajado en la estandarización de los servicios Carrier Ethernet, que se pueden brindar a través de una red de proveedor de servicios, expandiéndose incluso a la estandarización de servicios entre redes de diferentes proveedores, con el fin de proporcionar servicios “end-to-end” transparentes para los clientes a través de la denominada “La Tercera Red” (The Third Network).

Esta es la era de transformación para las redes de telecomunicaciones, que acelerará la capacidad de proveedores para ofrecer servicio bajo demanda, con conexión a la nube y auto-servicio por parte de clientes a través de redes interconectadas. Las redes de nueva generación permitirán servicios de redes ágiles, confiables y orquestadas para potenciar a la economía digital y el mundo hiper-conectado con el control del cliente sobre los recursos de la red y la conectividad con la nube, figura 1.3.

La transformación de las redes de telecomunicaciones, además de la adopción de Ethernet como su transporte, adiciona nuevos conceptos como SDN, NFV y LSO.

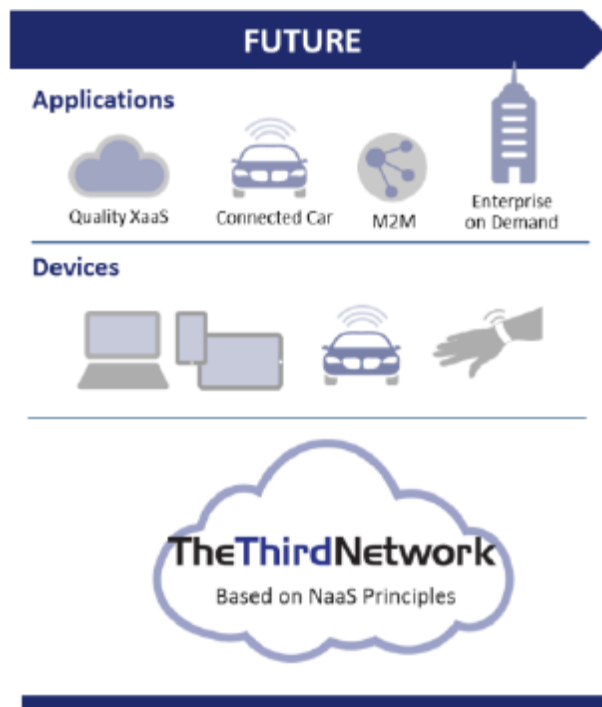


Figura 1. 3: Ejemplo de redes de comunicación en el futuro

Fuente: (MEF, y otros, An Industry Initiative for Third Generation Network and Services, 2016)

Ethernet junto con los conceptos de SDN, NFV, LSO llegan a formar redes interconectadas, virtuales y automáticas para la provisión de servicios en tiempo real, con calidad de servicio, seguridad del tráfico y la integración de redes NaaS como valor agregado, que no solo se limitan al aprovisionamiento en interfaces físicas UNI (User-Network Interface), sino en la entrega dentro del rack de servidores que pertenecen a máquinas virtuales o servicios en la nube como muestra la figura 1.4. (MEF, y otros, An Industry Initiative for Third Generation Network and Services, 2016).

La visión, a nivel de industria, de “La Tercera Red” se basa en los principios de NaaS al permitir al usuario tener una perspectiva de tener el control de su propia red, a través de servicios de valor agregado en su conexión física. Esto permite a los administradores de red tener el control y crear servicios según sea necesario bajo la demanda, modificarlos o en su defecto eliminarlos. Se maneja un concepto similar en IaaS (Infrastructure as a Service) en los Data Center al permitir a usuarios crear, modificar o eliminar de manera dinámica recursos de cómputo y almacenamiento.

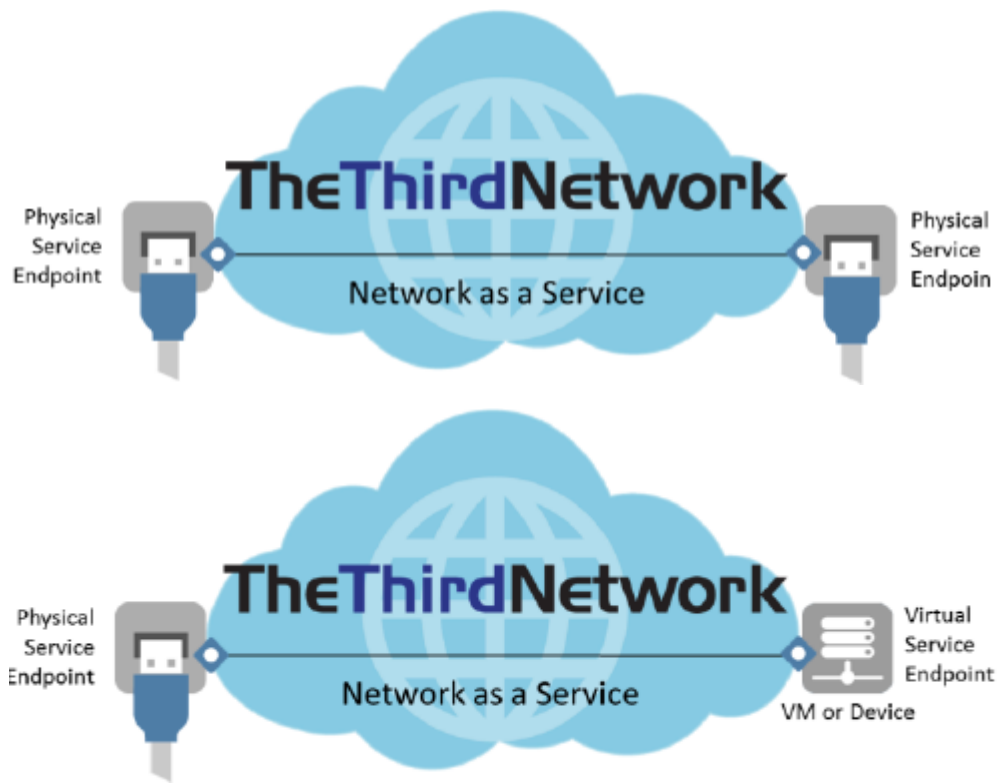


Figura 1. 4: Ejemplo de servicios con terminales físicos y virtuales

Fuente: (MEF, y otros, An Industry Initiative for Third Generation Network and Services, 2016)

Al iniciar el desarrollo del presente documento se definirá el problema que se desea tratar junto con los objetivos generales y específicos.

1.2. Antecedentes.

La aceptación de Ethernet como estándar de conectividad física ha ido creciendo de una manera notable desde su aparición al inicio de la década de los 70s, las diferentes empresas que proveen servicios de telecomunicaciones han ido migrando paulatinamente sus redes de estándares antiguos como Frame Relay o ATM (Asynchronous Transfer Mode) hacia Ethernet como principal método de transporte. (NTT, 2010)

Ethernet fue concebido para proveer conectividad a redes pequeñas, denominadas de área local, las mismas que consistían en un grupo de equipos distribuidos en un área geográfica pequeña, como una casa, edificio, etc. y que no se necesitaba de un proveedor de servicios para proveer de conectividad entre los diferentes

dispositivos. Las velocidades a las que trabaja Ethernet han ido creciendo desde sus inicios con 3Mbps hasta velocidades de 40Gbps o 100Gbps en la actualidad, proporcionando un despunte importante con respecto a otras tecnologías como Frame Relay o ATM que no pueden ostentar un crecimiento tan significativo. (NTT, 2010)

Dada la gran demanda que se ha generado con respecto al contenido que se transmite en las redes de comunicación, tales como voz y video de alta definición, ha ocasionado que los proveedores de servicio adopten a Ethernet como su medio de transporte preferido ya que proporciona las características y los costos adecuados para poder brindar este tipo de servicios a los usuarios finales.

Con los estándares predecesores, en términos de transporte WAN, en caso de que un usuario requiera un circuito dedicado privado se solían proveer de circuitos físicos dedicados para cada cliente, los mismos que tenían limitaciones en cuanto a la capacidad de transmisión que manejaban, como a los elevados costos que representaba para el cliente final. Los proveedores de servicio han optado por extender los dominios de las áreas locales que utilizaban Ethernet, brindando de esa manera una conectividad WAN para el usuario final, a través del bien conocido estándar Ethernet ya implementado por las redes de área local.

MEF es un consorcio formado principalmente para poder estandarizar los diferentes servicios y prestaciones que se pueden explotar con el estándar Ethernet y que los mismos sean aplicados de manera ordenada entre diferentes proveedores de servicio, con el fin de brindar una experiencia transparente para el usuario final en términos de conectividad a nivel físico, sin la necesidad de intercambiar/publicar el enrutamiento propio de cada red del cliente. En el presente documento se expondrán los conceptos básicos para brindar al lector un panorama claro con respecto a los servicios Ethernet y se sustentará con una simulación de los mismos en un ambiente controlado.

1.3. Definición del problema

Los proveedores de servicio locales han optado por implementar redes de transporte IP/MPLS para la provisión de diferentes servicios, tales como internet fijo, telefonía fija, telefonía móvil y datos en general hacia su red de abonados, a través de la configuración L3VPN (Layer 3 Virtual Private Network) para cada uno de ellos.

Este tipo de provisión de servicios demanda elevados recursos de procesamiento y capacidad de la red al tener que almacenar y replicar un elevado número de rutas para cada nodo, ocasionando un problema de falta de memoria en los equipos del Proveedor de Servicios limitando su crecimiento.

La implementación de servicios Carrier Ethernet EP-Line y EVP-Line, permite reducir los recursos de rutas que se requiere en los equipos de la red del proveedor de servicios, permitiendo así optimizar los recursos de la red sin que sea necesario una fuerte inversión en cambio de equipamiento, y a la vez proporcionando al usuario final las características de dichos servicios (servicios estandarizados, calidad de servicio, escalabilidad, administración de servicios, confiabilidad).

La provisión de los servicios Carrier Ethernet dentro de una red de un Proveedor de Servicios, promueve la tendencia a nivel mundial de adopción de Ethernet como tecnología de transporte, permitiendo preparar la red para la adopción de los nuevos paradigmas que se plantean en cuanto a las redes de comunicación a nivel mundial.

1.4. Justificación del Problema a Investigar.

Con la implementación de servicios Metro Ethernet sobre una red de transporte de un proveedor, se pretende brindar conectividad a nivel de capa 2 del modelo OSI (Open System Interconnection) a los clientes finales a través del protocolo de mayor popularidad, crecimiento y despliegue; ya sean estos clientes residenciales, corporativos, gubernamentales o incluso otro proveedor de servicios, con el fin de proporcionar un medio transparente mediante la extensión de servicios Ethernet a través de una red WAN.

De esta manera se le permite al usuario final tener el control total de la conexión solicitada a través del Proveedor de servicios, ya que se trata de la extensión de su dominio Ethernet en capa 2. Los usuarios no requieren intercambiar tablas de ruteo, ni adaptarse o modificar sus protocolos de enrutamiento para acoplarse a la red del proveedor, se da la total autonomía e independencia a los usuarios.

Este trabajo pretende demostrar, mediante una simulación, la manera de implementar los servicios Ethernet que se estandarizan a través del MEF en una red multi-servicios MPLS de un proveedor de servicios. Se mostrará el ambiente recreado para conseguir este objetivo junto con las configuraciones y consideraciones necesarias para su completa implementación.

1.5. Objetivos

Dentro del presente trabajo de titulación se plantean los siguientes objetivos generales y específicos.

1.5.1. Objetivo General:

Simular en un entorno controlado mediante el software GNS3 la implementación de servicios “Carrier Ethernet” EP-Line y EVP-Line del estándar MEF sobre la red de transporte multiservicios MPLS de un Proveedor de Servicios local para la conectividad en capa 2 de clientes.

1.5.2. Objetivos específicos:

- ✓ Exponer los conceptos que se definen bajo el estándar MEF para los servicios EP-Line y EVP-Line enmarcado en un contexto de servicio sobre una red multi-servicio MPLS.
- ✓ Presentar las características, consideraciones, recursos y planificación que se requiere para simular una red de un Proveedor de Servicios bajo un entorno controlado, así como la implementación de servicios para clientes con el uso de L3VPN.

- ✓ Exponer el procedimiento, recursos y consideraciones para migrar los servicios de los clientes utilizando los esquemas “Carrier Ethernet” EP-Line y EVP- Line en un entorno simulado de red de un Proveedor de Servicios.
- ✓ Analizar los resultados obtenidos de la simulación y exponer las conclusiones y recomendaciones que guíen a la implementación de estos servicios sobre una red en producción.

1.6. Hipótesis

La implementación de los servicios EP-Line y EVP-Line permiten una gran flexibilidad al proveedor de servicios para ofrecer conectividad a sus clientes sin la necesidad de intercambiar direcciones IP ni protocolos de enrutamiento, brindando un total control y aislamiento de los clientes dentro de una red multi-servicios MPLS a nivel de capa 2 que permite ofrecer un servicio estandarizado, con calidad de servicio, escalable, administrable y confiable, optimizando los recursos del proveedor y acoplándose al nuevo paradigma en las redes de comunicación.

1.7. Metodología de investigación.

Para el desarrollo de este trabajo se utilizará un método experimental, basado en un diseño aplicado a un caso de estudio, donde se recrea una red de un proveedor de servicios sobre la cual se implementará los servicios EP-Line y EVP-Line. Adicionalmente se tendrá un enfoque descriptivo de los criterios teóricos y de diseño utilizados para el desarrollo.

Para concluir la investigación se utilizará un análisis explicativo de los resultados obtenidos en la implementación del diseño para demostrar el cumplimiento de los objetivos planteados.

Capítulo 2: Fundamentación Teórica.

En el Capítulo 2 se expone al lector la fundamentación teórica respecto a los conceptos necesarios para entender los diferentes servicios Carrier Ethernet 2.0 que han sido definidos por el MEF.

2.1. Introducción a Ethernet.

Ethernet ha sido un estándar que desde sus inicios ha presentado un notable crecimiento y despliegue dentro de las redes de telecomunicaciones de los proveedores a nivel mundial. Solamente en Norte América ha presentado cifras de dos dígitos de crecimiento, lo que no puede manifestarse de tecnologías precedentes como Frame Relay o ATM, ya que poco a poco han sido migradas a la tecnología Ethernet para conectividad de redes WAN. (NTT, 2010)

Las razones por las que las empresas de telecomunicaciones se encuentran migrando sus tecnologías hacia Ethernet, van desde la reducción de sus costos de implementación y de operación, hasta la comodidad de brindar un servicio transparente y ampliamente usado en redes de área local por los diferentes usuarios.

Ethernet permite la conectividad de redes a lo largo de múltiples localidades a nivel mundial, permitiendo brindar velocidades de 100 Mbps hasta 100Gbps dependiendo de los requerimientos, ya que los mismos varían de cliente a cliente. La constante demanda de mayores tasas de transferencia por parte del tráfico que cursa en la red, ha sido un punto crucial para elegir a Ethernet por encima de tecnologías como Frame Relay y ATM ya que estas últimas presentan un mayor grado de complejidad, así como un elevado costo en relación a Ethernet. (NTT Communications, 2010)

2.1.1. Historia de Ethernet.

Ethernet nace en el año 1973, con una velocidad de transmisión de 3Mbps, orientado a la conexión de redes LAN, las mismas que se caracterizaban por depender de un proveedor de servicios para su conectividad, ya que se desplegaban dentro de un área geográfica reducida como hogares, oficinas o un pequeño conjunto de edificios. Para la interconexión entre estas redes LAN que se situaban geográficamente distantes, era necesario utilizar tecnologías como Leased Lines (Líneas arrendadas), Frame Relay o ATM. (NTT, 2010)

Por lo general Frame Relay y Leased Lines no otorgaban un ancho de banda suficiente para el transporte del tráfico de aplicaciones en tiempo real o transferencia de archivos entre las redes LAN. Las demandas en cuanto a tasas de transmisión para usuarios de PC (Personal Computer) han escalado desde los 10Mbps en los años 80s hasta 100Mbps (dentro de un ambiente característico de hogar) o incluso 10Gbps Full-Duplex. Los proveedores de servicio para poder atender esta creciente demanda, se han visto en la obligación de proveer una solución para llevar este tráfico bajo un esquema transparente para el usuario. Ethernet ha evolucionado en conjunto con los requerimientos descritos, e incluso permite tener una percepción de usuario de estar directamente conectado hacia su otro extremo requerido como una conexión local, a pesar de encontrarse geográficamente separados.

Al convertirse Ethernet en el estándar predominante para conexiones WAN, los servicios prestados en Ethernet no han sido estandarizados. Los servicios que se pueden brindar pueden ser privados, virtuales, punto a punto, multipunto, híbrido, MPLS o VPN. (NTT, 2010)

2.1.2. Beneficios de Ethernet.

Las principales ventajas que se destacan para Ethernet giran en torno a los costos de operación e implementación, la escalabilidad, la disponibilidad, etc. A continuación se describen las principales ventajas, que permiten tener una mejor

visualización de su superioridad con respecto a tecnologías predecesoras. (NTT, 2010)

- El uso de la tecnología Ethernet para conectar redes LAN a otras MAN (Metropolitan Area Network) o WAN, ayuda a reducir los gastos de inversión y operación ya que es una tecnología con gran penetración a nivel mundial, lo que abarata sus costos.
- Se trata de una tecnología que, debido a su desarrollo y presencia inclusive en redes LAN, es bien conocida por los profesionales que operan las redes, permitiendo una mejor adaptación sin la necesidad de una inversión en capacitación experta.
- Ethernet se encuentra implementada en, prácticamente, todos los productos de redes, lo que abarata sus costos.
- Se puede incrementar el ancho de banda conforme requiera el cliente, permitiendo realizar pagos por lo que el usuario utiliza únicamente. Brinda de ésta manera una mayor aceptación en cuanto a requerimientos de los clientes hacia los proveedores de servicios.
- Los cambios en cuanto al servicio prestado al cliente, en términos de ancho de banda, pueden ser aplicados en breves instantes de tiempo, sin la necesidad de la adquisición de nuevos equipos para adoptar las nuevas velocidades de transmisión.
- No se requiere un protocolo de capa 3 del modelo OSI entre el cliente y el proveedor de servicios, lo que se traduce en flexibilidad y privacidad para las redes de los clientes.
- Es fácil y rápido de implementar. Permite la adición de nuevos servicios de una manera ágil en cuanto ya se tenga la infraestructura base en las instalaciones del cliente.
- La confiabilidad que ofrece se hereda de la confiabilidad que tienen los enlaces WAN dentro del proveedor de servicios, dicho de otra manera, el cliente adopta la red del proveedor como parte de su WAN. Se implementan SLAs (Service Level Agreement) para asegurar tiempos de falla.

2.1.3. Futuro de Ethernet.

Los ya mencionados beneficios de Ethernet no solo han provocado que sea la tecnología adoptada para transmisión de redes WAN, en reemplazo de Frame Relay o ATM, sino que han posicionado a Ethernet como el método banda ancha preferido a nivel mundial. Con el continuo crecimiento del mercado, ha ido creciendo a la par con las tasas de transferencia que ahora soporta Ethernet, llegando así a tener velocidades de 40Gbps y 100Gbps Full-Duplex permitiendo prever un futuro dominante aún sobre otras tecnologías. (NTT, 2010)

Mediante la estandarización de los servicios que se prestan sobre una red Ethernet de un proveedor de servicios, se pueden brindar servicios que trasciendan las barreras de un único proveedor, y permitiendo el transporte del tráfico de un usuario a través de puntos de interconexión Ethernet, entre diferentes proveedores de servicio. Un proveedor pequeño puede alquilar infraestructura a uno más grande, para poder alcanzar lugares distantes mediante un transporte en L2, lo que simplifica su implementación y reduce sus costos. (NTT, 2010)

2.2. MEN (Metro Ethernet Network).

La arquitectura que se presentará en este trabajo para las redes MEN, está enmarcada en el modelo genérico definido por el MEF para indicar, en un modelo de capas, los servicios Ethernet, los servicios de transporte y los servicios de aplicación.

2.2.1. Modelo de referencia para redes MEN.

En la figura 2.1 se presenta el modelo básico referencial para redes MEN, en el cual se destaca sus dos componentes principales: el equipamiento del cliente y la infraestructura de red MEN del proveedor.

El punto de referencia T indica los límites de las redes del proveedor y del cliente, también se lo denomina UNI, la misma que será descrita con más detalle en el

desarrollo del presente trabajo, dada la gran importancia dentro del modelo de red presentado. El punto de referencia S, demarca los límites del equipamiento de red del cliente y el del usuario final que genera el flujo de las tramas Ethernet.

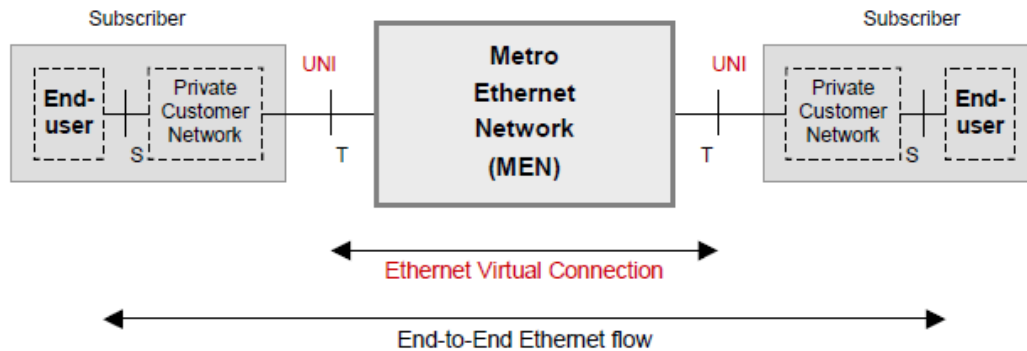


Figura 2. 5: Modelo básico de referencia para redes MEN

Fuente: (MEF, MEF 4 Metro Ethernet Network Architecture Framework - Part 1: Generic Framework, 2004)

En el caso de que no exista el equipamiento intermedio entre el del proveedor y el usuario terminal, los puntos S y T coinciden en el mismo punto dentro del esquema lógico. Un flujo Ethernet representa una sucesión de tramas Ethernet, no necesariamente consecutivas/contiguas, que comparten un trato común para el propósito de transferir los datos del usuario a través de la red MEN. (MEF, MEF 4 Metro Ethernet Network Architecture Framework - Part 1: Generic Framework, 2004)

El EVC (Ethernet Virtual Circuit) es la arquitectura que se construye con el fin de asociar las interfaces UNI de referencia, entre los dos puntos de la red MEN donde se requiere la comunicación a nivel de capa 2. Puede existir más de un flujo asociado a un EVC en particular dentro de la infraestructura del proveedor. El mapeo entre los flujos Ethernet y los EVCs se especifica dentro de los modelos de servicio de las especificaciones MEF. Tanto los EVC y los modelos de servicio MEF serán introducidos de manera clara en los temas siguientes.

2.2.2. Modelo de capas para redes MEN.

El modelo de capas para redes MEN especificado a continuación se divide así:

- Capa de Servicios Ethernet
- Capa de Servicios de Transporte
- Capa de Servicios de Aplicación

El modelo de capas se basa en una relación cliente/proveedor, en donde cada capa se compone de sus respectivos planos de datos, control y administración. La figura 2.2 muestra el modelo de capas para redes MEN.

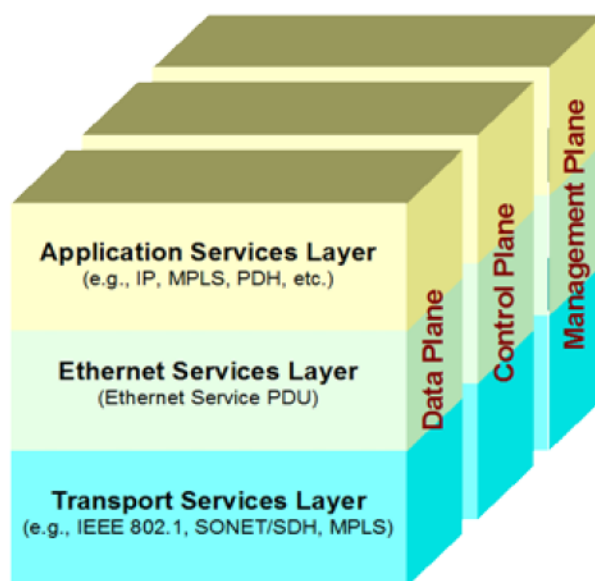


Figura 2. 6: Modelo de capas para redes MEN

Fuente: (MEF, MEF 4 Metro Ethernet Network Architecture Framework - Part 1: Generic Framework, 2004)

2.2.2.1. Capa de Servicios Ethernet (ETH Layer)

Es la responsable de la creación de instancias de servicios de conectividad orientada a través de MAC (Media Access Control) Ethernet y a la entrega de tramas de servicio Ethernet presentados a través de interfaces internas y externas.

También es responsable de todos los aspectos asociados a los flujos MAC Ethernet, los mismos que incluyen la operación, administración, aprovisionamiento y mantenimiento para la conectividad de los servicios Ethernet.

2.2.2.2. Capa de Servicios de Transporte (TRAN Layer)

Soporta la conectividad para la capa Ethernet de una manera independiente. Se requiere varios criterios de interconexión y tecnologías de red, para soportar los requerimientos de la capa de Servicios Ethernet. Dentro de los ejemplos que se puede citar para la capa de transporte se incluye IEEE 802.3 PHY, SONET/SDH, MPLS LSP (Label Switched Path), etc.

2.2.2.3. Capa de Servicios de Aplicación (APP Layer)

Soporta aplicaciones transportadas en los servicios Ethernet a través de una red MEN. Varios servicios de aplicaciones pueden ser soportados sobre Ethernet en su capa de servicios. Un ejemplo de los servicios es el uso de la ETH Layer como una TRAN Layer para otra capa de la red como IP, MPLS, PDH (Plesiochronous Digital Hierarchy), etc. Adicionalmente incluye funciones adicionales para complementar los servicios de la ETH Layer. Este modelo será aplicado de manera recursiva en la capa de aplicación.

2.2.3. Puntos de referencia en redes MEN.

Los puntos de referencia en las redes MEN son utilizados para demarcar bordes administrativos en el enlace, los mismos que son interfaces definidas por el MEF. Los puntos de referencia pueden ser varios e indican la separación entre la red del suscriptor y del proveedor de servicios, o en su defecto el borde entre dos redes MEN, en el caso de que se encuentren involucrados más de un proveedor para brindar el servicio.

2.2.3.1. Interface Usuario – Red (UNI – User-Network Interface)

La interface UNI es el punto de demarcación donde se conecta el suscriptor con su equipamiento de red, con el proveedor de la red de servicios MEN. Esto quiere decir que en este punto la responsabilidad del proveedor de servicios termina, para que empiece la del suscriptor del servicio. Las interfaces UNI, al ser punto de

demarcación de la red MEN, se encuentran del lado del proveedor (UNI-N) y del cliente (UNI-C) como se puede apreciar en la figura 2.3.

La interface UNI-C soporta las funcionalidades para intercambiar información en los planos de control, datos y administración del lado del suscriptor hacia el proveedor de servicios, la cual está en la entera administración del suscriptor/cliente.

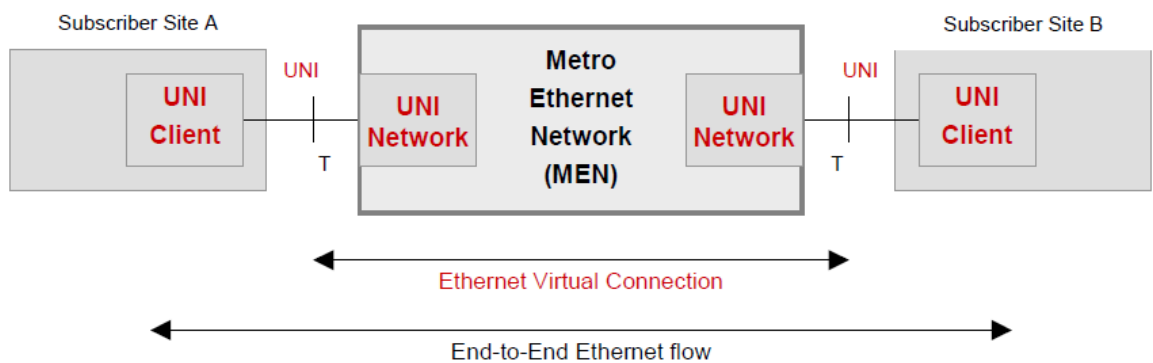


Figura 2. 3: Interface UNI dentro de una red MEN

Fuente: (MEF, MEF 4 Metro Ethernet Network Architecture Framework - Part 1: Generic Framework, 2004)

La interface UNI-N, de igual manera que la UNI-C, soporta todas las funcionalidades en los planos de control, datos y administración y se encuentra dirigida por el proveedor de servicios.

2.2.3.2. Interface Red – Red Externa (E-NNI – External Network-Network Interface)

Se trata de una interface abierta, la cual es tratada como un punto de demarcación entre dos redes MEN de proveedores de servicios distintos, que intercambian un punto de conexión a través de ésta interface. Una interface E-NNI es un punto de demarcación para los servicios Ethernet entre dos proveedores y su equipamiento.

2.2.3.3. Interface Red – Red Interconexión de Red (NI-NNI – Network Interworking Network-Network Interface)

Una interface NI-NNI es un punto de demarcación entre dos redes MEN, que brinda las facilidades para la extensión de servicios Ethernet y EVCs asociados a través de una red de transporte externa que no esté directamente involucrada en la provisión del servicio end-to-end. La red de transporte puede ser pública OTN (Optical Transport Network), SDH (Synchronous Digital Hierarchy)/SONET (Synchronous Optical Network), ATM, Frame Relay, etc.

2.2.3.4. Interface Red – Red Interconexión de Servicio (SI-NNI – Service Interworking Network-Network Interface)

La interface SI-NNI soporta la interoperabilidad, de un servicio MEF con otros provistos por diferentes tecnologías como ATM, IP, Frame Relay, etc. Se trata de un punto de demarcación entre redes MEN, interconectadas a través de una red de transporte (OTN, ATM, IP, Frame Relay, etc.), que no se encuentra directamente involucrada en la provisión del servicio Ethernet end-to-end.

En la figura 2.4 se representa las diferentes interfaces mencionadas y su grado de interacción, con el fin de identificar los diferentes puntos de demarcación que pueden estar presentes en la provisión de servicios Ethernet end-to-end. Se toma como referencia a redes MEN de diferentes proveedores de servicios para la ilustración. (MEF, MEF 4 Metro Ethernet Network Architecture Framework - Part 1: Generic Framework, 2004).

2.3. Metro Ethernet Forum.

El MEF es un consorcio que se enfoca en la adopción de redes y servicios Carrier Ethernet. Está compuesto por diferentes entidades, dentro de las cuales están proveedores de servicios y equipamiento, operadoras y otras compañías de telecomunicaciones que comparten interés en redes MEN.

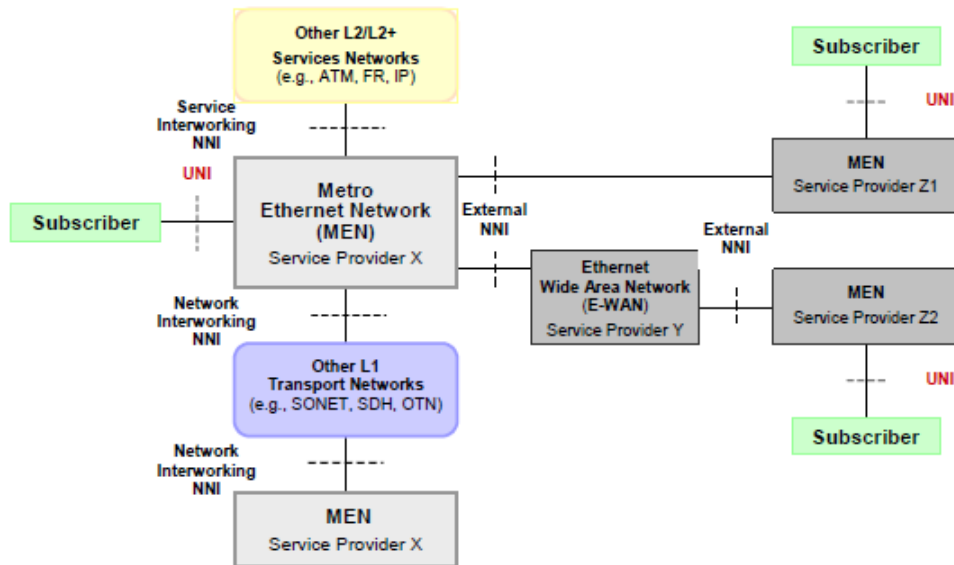


Figura 2. 4: Puntos de referencia en una red MEN

Fuente: (MEF, MEF 4 Metro Ethernet Network Architecture Framework - Part 1: Generic Framework, 2004)

A diferencia de la IEEE (Institute of Electrical and Electronics Engineers) o la IETF (Internet Engineering Task Force), MEF no se centra en definir protocolos de red, sino en definir como todos los componentes dentro de las redes Ethernet son estandarizados para su implementación. MEF define arquitecturas de red, escenarios de despliegue y de prueba para la conectividad Ethernet entre cliente y proveedor. (Mizrahi & Safrai, 2015)

Se aprovecha el gran ancho de banda proporcionado por Ethernet, para proveer conectividad dedicada/privada para el usuario final, a través de un enlace de un circuito de capa 2. Las interfaces usadas normalmente son 10/100/1000 Mbps. La conectividad capa 2 Ethernet permite implementar diferentes servicios en la misma conexión, con lo que aquellos como el almacenamiento, VoIP (Voice over IP), Seguridad, etc., coexisten en una única interfaz para el cliente y el proveedor.

MEF utiliza los siguientes cinco atributos para definir a Ethernet como Carrier Class:

- Servicios estandarizados
- Calidad de Servicio

- Escalabilidad
- Administración de servicios
- Confiabilidad.

Los servicios Carrier Ethernet pueden ser desplegados a través de Ethernet nativo, Ethernet sobre SDH/SONET, Ethernet sobre MPLS. (Cisco, Cisco CPT Configuration Guide–CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01), 2014)

2.3.1. Carrier Ethernet CE 2.0

Se trata de la segunda generación de redes y servicios definidos por el MEF para poder cumplir con los retos que presentan los proveedores de servicios en la década actual.

La funcionalidad de CE 2.0 se define a través de tres características principales y 8 servicios.(Mizrahi & Safrai, 2015)

2.3.1.1. Características CE 2.0

Las tres principales características son:

- Interconexión

El modelo referencial de MEF se centra en dos entidades cliente/proveedor. En CE 2.0 se añade una tercera entidad denominada “operador”, la misma que se define por quien presta interconexión al proveedor, en caso de que no pueda alcanzar todas las localidades del cliente.

- Multi-CoS

El tráfico se envía sobre múltiples clases de servicio CoS (Class of Service), las mismas que están asociadas con los objetivos y niveles de rendimiento definidos por el MEF, lo que permite una calidad constante del servicio a través de múltiples proveedores.

- Administración

CE 2.0 incluye mejoras en las capacidades de detectar fallas y errores de configuración, para monitorear el desempeño de la red. Adicionalmente provee políticas para el tratamiento del tráfico dentro de los parámetros del SLA, todo lo que caiga fuera de lo estipulado en él, es descartado (Mizrahi & Safrai, 2015).

La IEEE y la ITU (International Telecommunication Union) trabajan en la estandarización de OAM (Operations, administration and maintenance) para redes Metro Ethernet, teniendo como componente principal a CFM (Connectivity Fault Management), IEEE 802.1ag, en donde se especifican protocolos, procedimientos y objetos a ser administrados. Estos elementos facilitan la verificación y el descubrimiento de los caminos que toma el tráfico a través de LANs y la detección y aislamiento de una falla de conectividad específica.

CFM establece objetos llamados Asociaciones de Mantenimiento (MA – Maintenance Association), para brindar una estructura en el intercambio de mensajes CFM. El alcance de la MA es determinada por el Dominio de Mantenimiento (MD – Maintenance Domain), el cual describe una región de la red donde la conectividad y el desempeño son administrados. Cada MA asocia dos o más Puntos Finales de Asociación (MEP – Maintenance Endpoints) y permite Puntos intermedios de Asociación de Mantenimiento (MIP – Maintenance Intermediate Points) para soportar la detección de fallas y su aislamiento como se indica en la figura 2.5 (Green, Monette, Olsson, Saltsidis, & Takács, 2007).

Detección de Fallas

La detección de fallas utiliza un protocolo de verificación continua, para las fallas de conectividad y aquella no deseada entre MA. Cada MEP puede transmitir de manera periódica, un CCM (Connectivity Check Message) en multicast y verificar CCMs recibidos por otros MEP en la MA. Un mensaje CCM puede detectar cross-conexión de servicio, configuraciones duplicadas de MEP, pérdida de datos y jitter. (Green, Monette, Olsson, Saltsidis, & Takács, 2007)

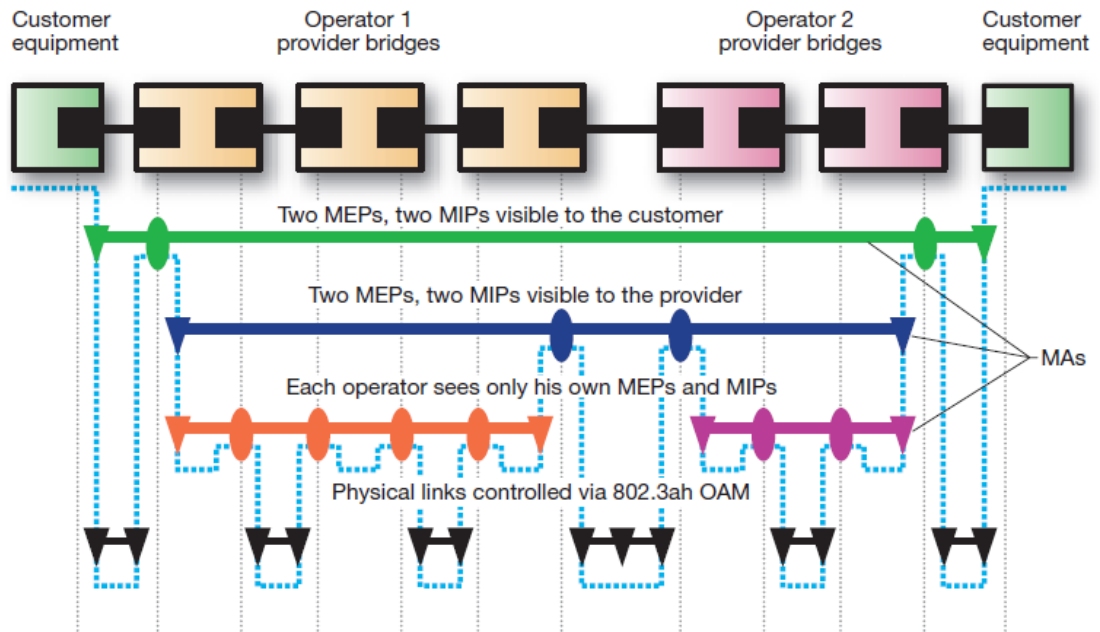


Figura 2. 5: Esquema de Arquitectura OAM
Fuente: (Green, Monette, Olsson, Saltsidis, & Takács, 2007)

Verificación y Aislamiento de Fallas

La verificación y el aislamiento de una falla son acciones administrativas, que por lo general se ejecutan después de haber detectado una falla, las cuales confirman una iniciación o recuperación de la conectividad de manera exitosa. El administrador utiliza un protocolo de lazo (loopback) para verificar la falla, enviando un alto volumen de mensajes de este protocolo se puede verificar el ancho de banda, la confiabilidad y el jitter. (Green, Monette, Olsson, Saltsidis, & Takács, 2007)

2.3.1.2. Servicios CE 2.0

Se definen 8 servicios dentro de MEF los mismos que se listan a continuación en la Tabla 2-1.

Tabla 2-1. Servicios CE 2.0

Tipo de Servicio	Servicios Basados en Puertos	Servicios Basados en VLAN (Virtual Local Area Network)
E-Line	EPL	EVPL
E-LAN	EP-LAN	EVP-LAN
E-Tree	EP-Tree	EVP-Tree
E-Access	Access EPL	Access EVPL

Fuente: (Green, Monette, Olsson, Saltsidis, & Takács, 2007)

En el presente trabajo no se abarcan los 4 tipos de servicios que se definen en el MEF, únicamente se hará énfasis en la implementación de los servicios E-Line basado en Puertos y basado en VLAN. A continuación se indica a breves rasgos los 4 tipos de servicios antes mencionados.

E-Line

Es un EVC punto a punto que conecta dos UNIs, el cual puede ser basado en puerto (EPL - Ethernet Private Line) figura 2.6 o basado en VLAN (EVPL - Ethernet Virtual Private Line) figura 2.7.

Cuando el servicio E-Line es basado en un puerto (EPL) se dice que todo el tráfico enviado por un puerto determinado del CE (Client Edge) se encapsula en un único EVC. Figura 2.6.

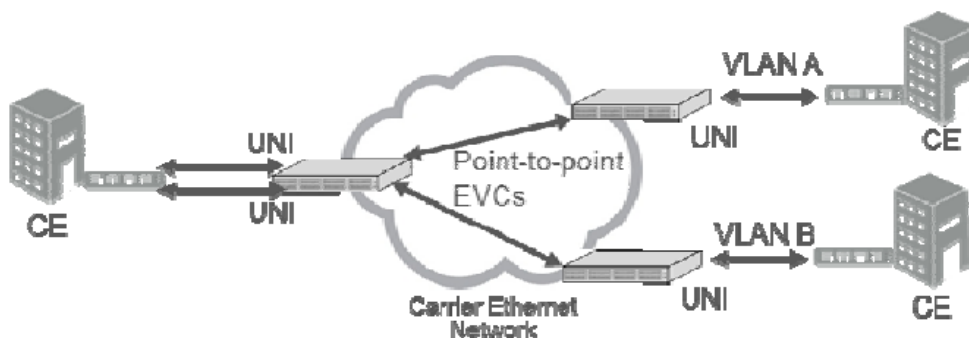


Figura 2. 6: Servicio EP-Line

Fuente: (Mizrahi & Safrai, 2015)

Por otro lado cuando un servicio E-Line se basa en VLANs (EVPL), se realiza una multiplexación de los servicios en el puerto del equipo del cliente CE encapsulándolos en distintos EVC. Figura 2.7

Un servicio EPL se puede configurar con el fin de atravesar diferentes redes Metro Ethernet, es decir, se puede concatenar varios servicios EPL entre redes de distintos proveedores, con el fin de brindar el servicio al cliente. (MEF, MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer, 2014)

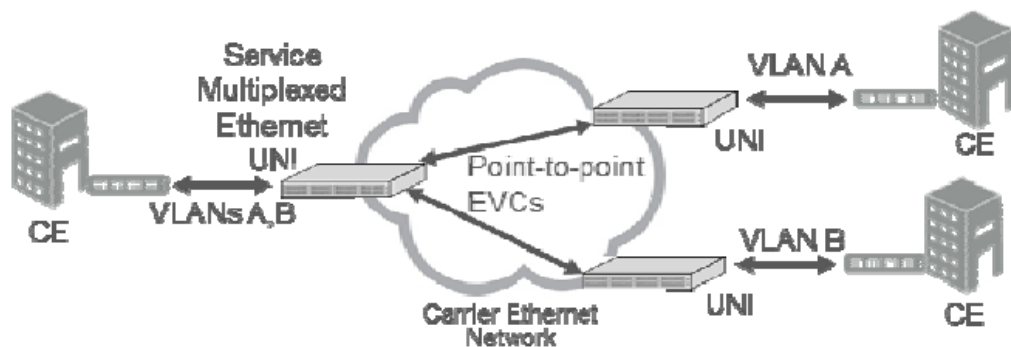


Figura 2. 7: Servicio EVP-Line
Fuente: (Mizrahi & Safrai, 2015)

En la figura 2.8 se puede apreciar que en la red Metro Ethernet de cada proveedor se configura un EVC haciendo uso de interfaces UNI, para la conexión hacia el cliente, y de una interface ENNI para la interconexión de los EVC en cada una de las redes de los distintos proveedores.

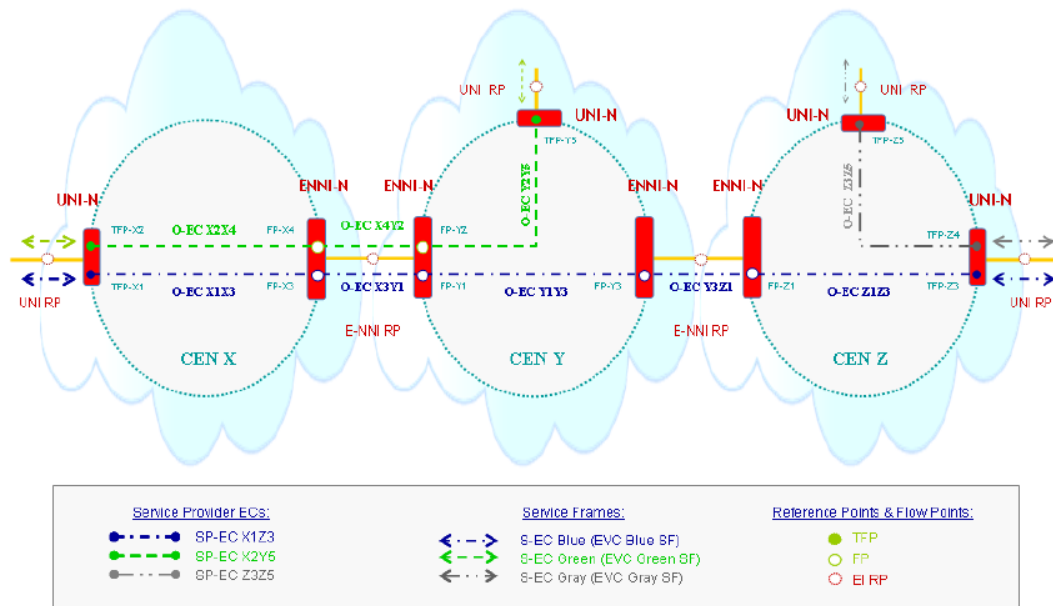


Figura 2. 8: Ejemplo Servicios EVP-Line

Fuente: (MEF, MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer, 2014)

Se tienen dos servicios EPL configurados en la figura 2.8, los mismos que interconectan interfaces de usuario UNI en la red del mismo proveedor, para el caso del servicio que interconecta los puntos de referencia Z4 – Z5 (gris), o atravesando redes de distintos proveedores a través de interfaces ENNI, para el caso del servicio que interconecta los puntos de referencia X2 – Y5 (verde).

Para el servicio Z4 – Z5 (gris) se utiliza la un EVP-Line entre los puntos Z4 y Z5 de la red Metro Ethernet del proveedor Z. Para el servicio X2 – Y5 (verde) se utiliza un EVP-Line entre los puntos X2 – X4 dentro del proveedor X, concatenando un servicio X4 – Y2 en la interconexión entre operadores (interface ENNI) y un servicio Y2 – Y5 en la red Metro Ethernet del proveedor Y.

E-LAN

Es un EVC multipunto a multipunto para conectar diversas UNI del cliente. Puede ser basado en puerto (EP-LAN) figura2.9 o basado en VLAN (EVP-LAN) figura2.10.

De la misma manera que en los servicios E-Line, para los servicios E-LAN basados en puerto, implica que todo el tráfico del puerto del CE se encapsula en un EVC, con lo que se podría brindar únicamente este servicio en el puerto indicado. Un ejemplo se muestra en la figura 2.9 en donde un único EVC se encarga de brindar el servicio E-LAN utilizando los puertos en los tres sitios del cliente.

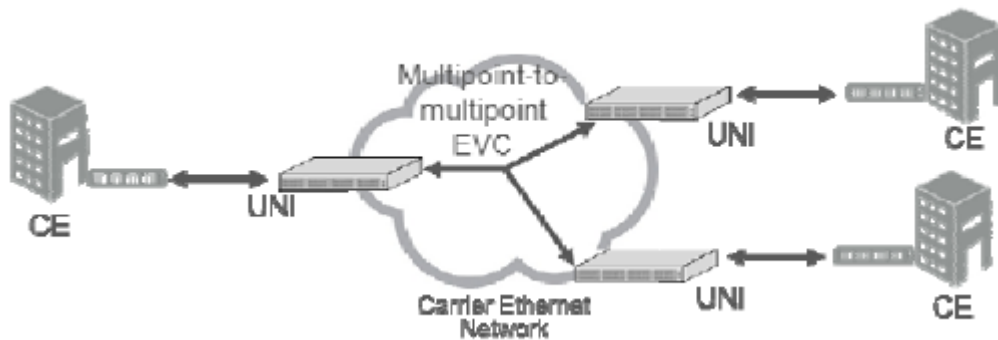


Figura 2. 9: Servicio EP-LAN

Fuente: (Mizrahi & Safrai, 2015)

En un servicio E-LAN basado en VLAN (EVP-LAN), realiza una multiplexación de los servicios en el puerto del equipo CE en el lado del cliente, permitiendo de esta manera diferenciar los servicios y enlazarlos con distintos EVC. En la figura 2.10 se indica un ejemplo, en donde el sitio 1 del cliente se configura el CE para permitir varios servicios diferenciados por VLAN, en donde un EVC se configura como una EVP-LAN con los sitios 3 y 4 y un segundo EVC se configura como un EVP-Line con el sitio 2 utilizando el mismo puerto del lado del CE.

Los servicios E-LAN pueden ser configurados para atravesar redes Metro Ethernet de varios proveedores, utilizando concatenación de EVCs en las redes de cada uno para cumplir con la topología necesaria del servicio a brindar.

En la figura 2.11 se ejemplifica el caso de un servicio EVP-LAN que atraviesa dos redes de proveedores de servicio, utilizando la concatenación de un EVC configurado como EVP-Line en la red de un proveedor, y un EVC multipunto EVP-LAN configurado en la red del segundo proveedor.

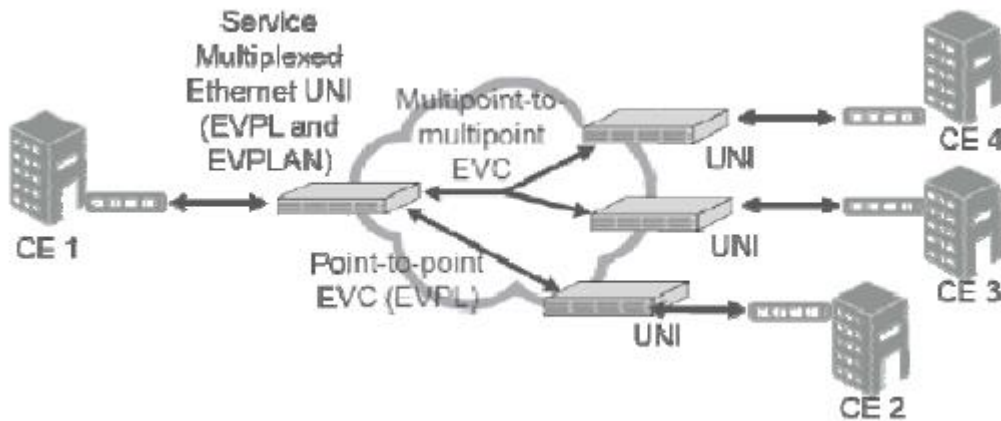


Figura 2. 10: Servicio EVP-LAN
Fuente: (Mizrahi & Safrai, 2015)

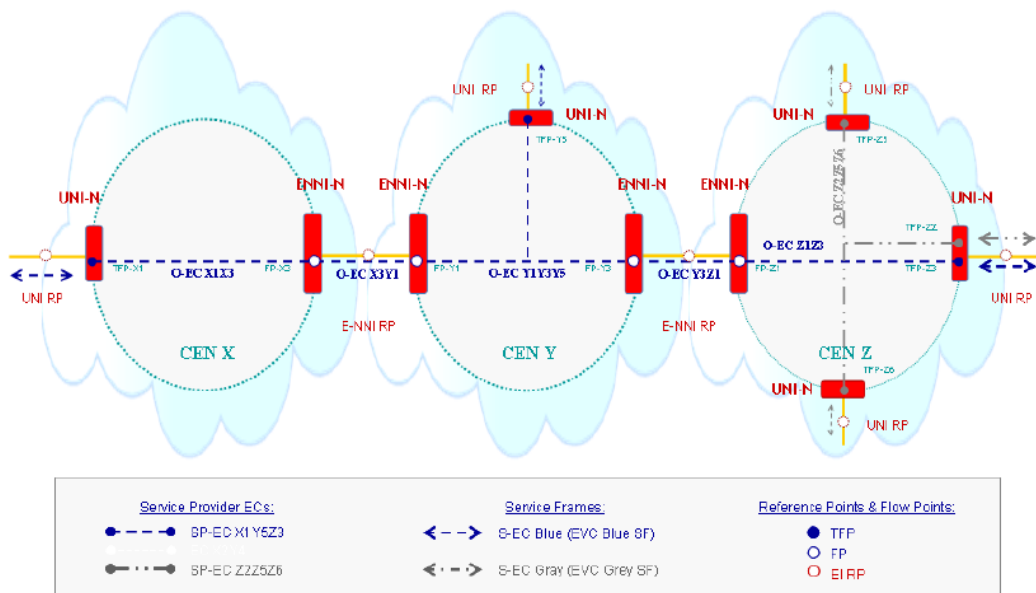


Figura 2. 11: Ejemplo Servicios EVP-LAN

Fuente: (MEF, MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer, 2014)

El servicio EVP-LAN configurado sirve para interconectar los puntos X1, Y5 y Z3 (azul) a nivel de un servicio Ethernet. El servicio se forma con la concatenación de un EVC configurado como EVP-Line para los puntos X1 y X3 dentro de la red del proveedor X concatenado con un servicio X3 – Y1, a través de una interface ENNI entre los proveedores, dentro de la red del proveedor Y se utiliza un EVP-LAN para conectar los puntos Y1-Y3-Y5 y se concatena con el

servicio Y3-Z1 por la interface ENNI, finalmente en la red del proveedor Z se configura un EVC como EVP-Line entre los puntos Z1-Z3. (MEF, MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer, 2014)

E-Tree

Se trata de un EVC multipunto con raíz (root), en donde una UNI es la raíz y es la única permitida para enviar y recibir tráfico a otras UNI hojas (leaves) o raíces. La comunicación entre interfaces UNI hojas no está permitida.

Se puede basar su arquitectura en puerto (EP-Tree) figura 2.12 o en VLAN (EVP-Tree) figura 2.13

Un servicio EP-Tree utiliza un único EVC, por lo que el puerto en el CE del lado del cliente se lo configura con el fin de que todo el tráfico que se envíe por el mismo forme parte del EVC. Figura 2.12. Se puede complementar su composición con el uso de EP-Line para cuando se requiere extender su alcance hacia redes de otros Proveedores de Servicios.

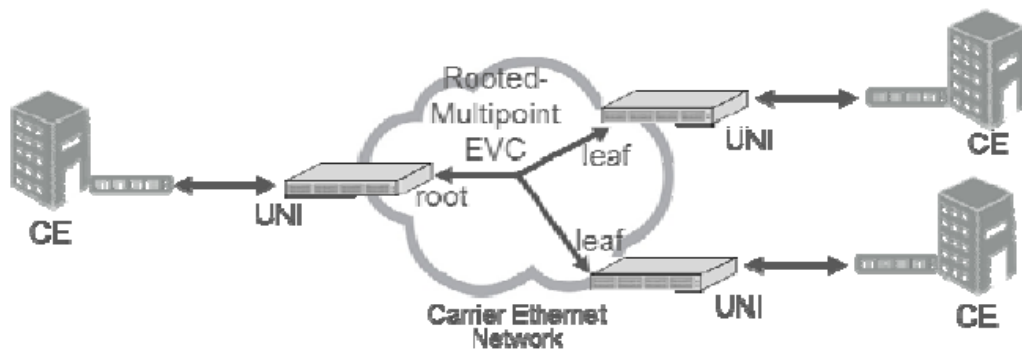


Figura 2. 12: Servicio EP-Tree

Fuente: (Mizrahi & Safrai, 2015)

Para el caso de un EVP-Tree, el puerto en el CE se configura para permitir la multiplexación de servicios mediante VLAN, logrando de esa manera identificar los servicios como se indica en la figura 2.13, en la que un EVC se utiliza para la configuración de un EVP-Tree y un segundo EVC para la configuración de una EVP-Line.

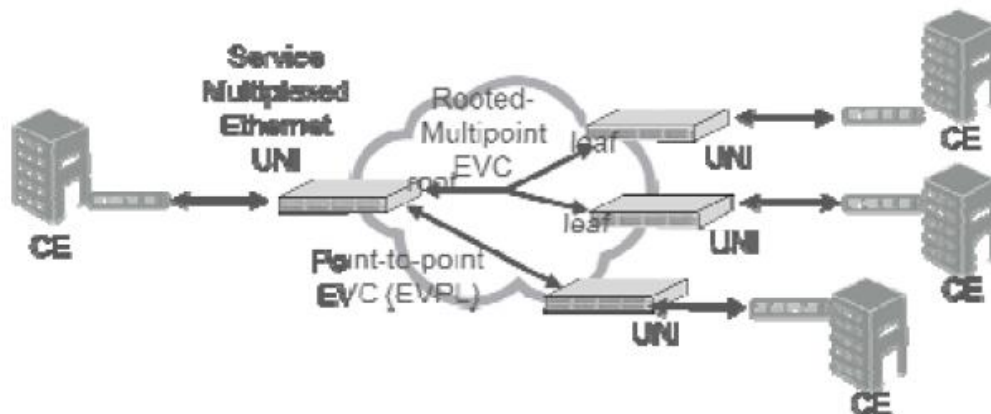


Figura 2. 13: Servicio EVP-Tree
Fuente: (Mizrahi & Safrai, 2015)

Un servicio E-TREE se puede configurar para atravesar redes Metro Ethernet de diferentes proveedores, utilizando interface ENNI. De manera adicional se introducen los conceptos de un EVC Troncal (trunk) o Rama (branch).

Un EVC Troncal es el responsable del transporte de ETH PDU (Protocol Data Unit) de un UNI raíces hacia otras UNI raíces o UNI hojas. Un EVC Rama es el encargado de transportar ETH PDU de UNI hojas hacia UNI raíces. Con las definiciones indicadas se definen nuevos puntos de flujo para tener un mejor entendimiento de la formación del servicio, los cuales son:

- Troncal – a – Hoja (TL-FP)
- Hoja – a – Rama (LB-FP)
- Rama – a – Raíz (BR-FP)

En la figura 2.14 se ejemplifica el caso de un servicio E-TREE, que atraviesa dos redes de proveedores, utilizando en la red de cada uno de ellos un EVC Troncal y un EVC Rama, para las conexiones hacia las interfaces UNI Raíz y UNI Hoja respectivamente. Para la concatenación de los EVC Troncal y Rama en las redes Metro Ethernet de cada proveedor, se utiliza la configuración de un servicio EVC EP-Line en las interfaces ENNI para su respectiva concatenación. (MEF, MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer, 2014)

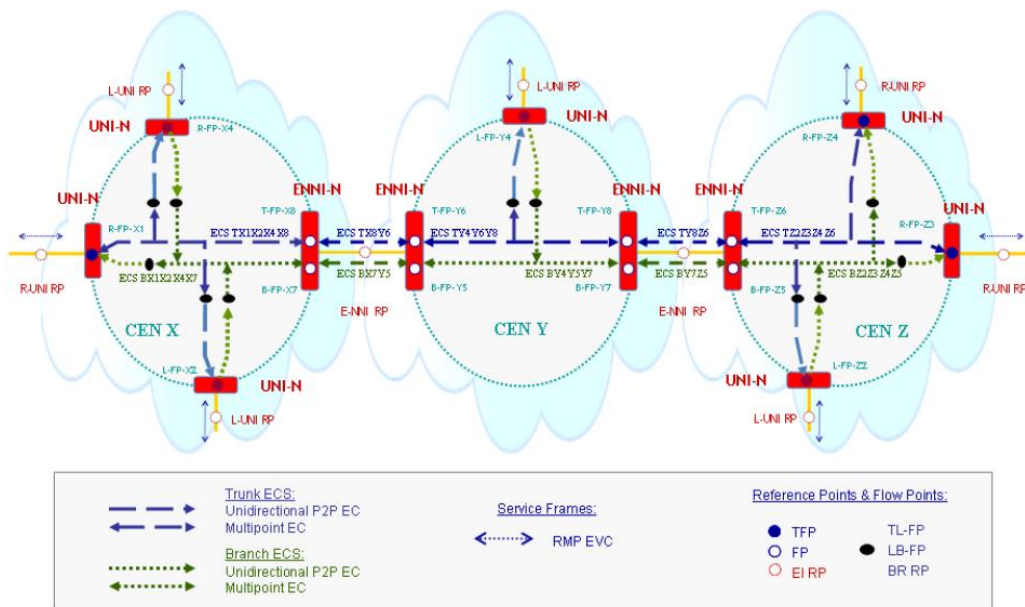


Figura 2. 14: Ejemplo Servicios EVP-Tree

Fuente: (MEF, MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer, 2014)

E-Access

Se define como E-Access a la interconexión entre proveedores de servicios que se utiliza para alcanzar a localidades de los clientes, a las cuales un único proveedor no puede alcanzar con su infraestructura. Esta interconexión se utiliza para que un proveedor pueda alcanzar a un “operador” (la tercera entidad incluida en CE 2.0). Las interfaces entre el proveedor y el operador se las denominan Interfaces de Red a Red Externas (ENNI). Se puede proveer una arquitectura basada en puerto o en VLAN, en la figura 2.15 se ejemplifica un E-Access. (Mizrahi & Safrai, 2015)

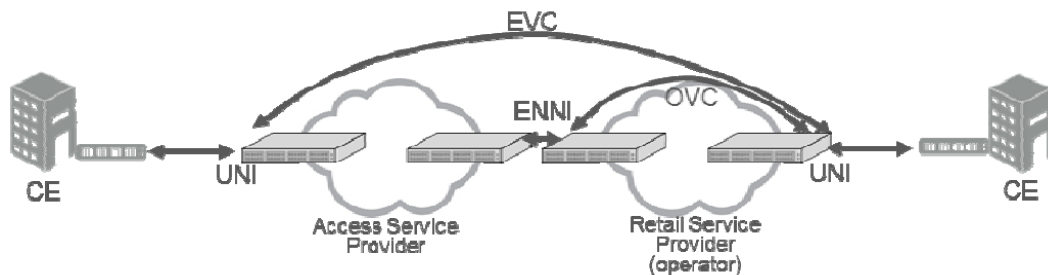


Figura 2. 15: Servicio E-Access: Interconexión entre proveedor y operador

Fuente: (Mizrahi & Safrai, 2015)

Un servicio E-Access permite al proveedor configurar un servicio EVC entre dos sitios del cliente, teniendo a uno de los dos sitios fuera del alcance de la red del proveedor. El EVC creado podrá alcanzar al sitio que se encuentra fuera de la red del proveedor a través de un OVC (Operator Virtual Connection).

Las consideraciones a tomar en cuenta, de una manera global, son los diferentes formatos que manejan las interfaces ENNI a diferencia de las interfaces UNI, ya que incrementa el tamaño de la trama en 4 bytes, con el fin de permitir aplicar diferentes políticas para la diferenciación y el tratamiento del tráfico que atraviesa la interface ENNI, así como la inclusión de la etiqueta para la VLAN de Proveedor de Servicio (S-VLAN). (MEF, CE 2.0 Ethernet Access Services, 2013).

Capítulo 3: Simulación de red con servicios CE2.0.

En el Capítulo 3 se muestra al lector todos los requerimientos y pasos a seguir para la implementación de la simulación en base a un estudio de ingeniería a detalle, utilizando de una manera organizada y escalable los recursos necesarios que permitan el análisis de la situación actual de la red de un Proveedor de Servicio, y la implementación de servicios CE 2.0 como propuesta de solución a la problemática planteada.

3.1. Introducción.

En este trabajo de titulación se propone la simulación de una red típica de un proveedor de servicio, en la que actualmente se estén brindando servicios a clientes finales a través del uso de métodos convencionales en el medio (L3VPN), en los cuales se intercambia direccionamiento, políticas y atributos entre la red del cliente y la del proveedor. Una vez propuesta la red en la cual se va a desarrollar el análisis sobre la implementación de servicios CE2.0, se analizará paso a paso la configuración que se requiere implementar en la red, con el fin de migrar los servicios desde el método tradicional hacia el propuesto con el uso de los esquemas EP-Line y EVP-Line, proponiendo así diferentes esquemas como casos de uso para la solución del problema planteado. Finalmente se realizará un análisis de los resultados obtenidos con la simulación en los diferentes casos de estudio, para dar un resultado en base a las pruebas propuestas respecto a la implementación de servicios “Carrier Ethernet” EP-Line y EVP-Line del estándar MEF sobre la red de transporte MPLS de un Proveedor de Servicios local para la conectividad en capa 2 de clientes finales.

En el capítulo previo se expusieron las características y funcionalidades que se plantean con los servicios CE2.0, teniendo como principal enfoque promover el uso de Ethernet como estándar de conectividad, extendiendo el dominio de redes LAN hacia un esquema WAN, y preparando las redes de los proveedores de servicio para la nueva era de la redes en las que se las ofrece como un servicio (NaaS). De la misma manera se pretende mostrar a los diferentes clientes el

cambio en el esquema de conectividad ante el servicio contratado hacia el proveedor de servicios, junto con las ventajas a nivel de independencia y versatilidad a la hora de tener un mejor control sobre las decisiones y cambios que pueden tomar sobre su propia red interna.

Distintos proveedores de equipos a nivel mundial incluyen en sus ofertas las funcionalidades para configurar servicios EP-Line y EVP-Line. Para cada uno de los casos las configuraciones pueden ser distintas, ya que esto depende de la marca del equipo en el que se requiera configurar los servicios, pero que en cuanto a la funcionalidad todos cumplen con el estándar planteado ante MEF. Dichos proveedores de equipos pasan por procesos de certificación para poder cumplir con el principio de funcionamiento de acuerdo a lo estipulado en los diferentes informes técnicos dentro del Metro Ethernet Forum.

La metodología utilizada en el presente capítulo será experimental, ya que se partirá desde cero en la simulación y se irán definiendo paso a paso los diferentes componentes que serán tomados en cuenta para armar el escenario de pruebas (simulación). Partiendo desde la definición del software y los equipos (imágenes) que se utilizará para este fin se definirá paso a paso, mediante una planificación adecuada en función a una topología propuesta, la implementación de una red típica de un Proveedor de Servicios sobre la cual se indicarán las configuraciones y la metodología propuesta para la migración hacia los servicios EP-Line y EVP-Line.

3.2. Software GNS3.

GNS3 es un software que permite construir, diseñar y poner a prueba un escenario de red en un ambiente controlado a través de una simulación, lo que permite trabajar bajo un entorno libre de riesgos ya que facilita implementar las configuraciones deseadas sin poner en peligro una red que se encuentre en operación. Según los lineamientos planteados en los objetivos del presente trabajo, GNS3 permite cumplir con los mismos ya que permitirá implementar la

topología propuesta junto con las configuraciones para la operación de una red típica de un Proveedor de Servicios.

En su portal web, GNS3 permite el acceso a una comunidad considerada de las más amplias para profesionales de redes, en las que se puede encontrar documentación respecto a diferentes temas relacionados a redes. Figura 3.1. Dentro de las principales características a resaltar para el uso del software se tiene:

- Permite la simulación en tiempo real de redes con el fin de probarlas previo a su despliegue sin la necesidad de contar con el hardware (equipamiento) físico.
- Soporta más de 20 diferentes Proveedores de Equipos bajo su entorno de simulación, lo que permite probar diferente hardware en función a las necesidades del diseño planteado.
- Permite la simulación de entornos de red con diferentes configuraciones para realizar pruebas de concepto o troubleshooting.
- Posee la funcionalidad de conectar la red simulada en el software GNS3 a una red operativa real, permitiendo la posibilidad de expandir el entorno de prueba una vez que ya se hayan superado las pruebas preliminares en la simulación.
- Topologías y laboratorios personalizados que permiten la capacitación en diferentes temas dentro del entorno de redes con el fin de proporcionar un ambiente académico idóneo para profesionales de redes.



Figura 3. 1: Logo de Software GNS3

Fuente: (GNS3, 2017)

Los requerimientos mínimos de instalación del software en un computador se especifican en la siguiente tabla 3-1:

Tabla 3-1. Requerimientos mínimos GNS3

Requerimientos Mínimos	
Sistema Operativo	Windows 7 (64 bit) o posterior, Mavericks (10.9) o posterior, Cualquier distribución de Linux - Debian/Ubuntu son soportadas
Procesador	2 o más núcleos lógicos - AMD-V / RVI Series o Intel VT-X / EPT - con extensiones de virtualización habilitadas en la BIOS.
Memoria	4 GB RAM
Almacenamiento	1 GB available space (Windows Installation is < 200MB)
Notas Adicionales	Se requiere almacenamiento adicional par alas imágenes de los equipos.

Fuente: (GNS3, 2017)

Debido a que los recursos de simulación están en función de la topología a implementar, número y capacidad de los equipos simulados, se recomiendan los requerimientos de la tabla 3-2 para la instalación de GNS3 en un computador: (GNS3, 2017)

Tabla 3-2. Requerimientos recomendados GNS3

Requerimientos Recomendados	
Sistema Operativo	Windows 7 (64 bit) o posterior, Mavericks (10.9) o posterior, Cualquier distribución de Linux - Debian/Ubuntu son soportadas
Procesador	4 o más núcleos lógicos - AMD-V / RVI Series o Intel VT-X / EPT - con extensiones de virtualización habilitadas en la BIOS.
Memoria	8 GB RAM
Almacenamiento	SSD - 35 GB de espacio disponible
Notas Adicionales	RAM hasta 16 GB y procesador i7 o equivalente para uso óptimo.

Fuente: (GNS3, 2017)

Dentro de la documentación disponible para el usuario de GNS3 a través de su portal, se encuentran las diferentes versiones del software y sus “release notes”, la academia de GNS3 en la cual se encuentra una variedad de cursos y eventos con sus respectivos costos o en ciertos casos pueden llegar a ser gratuitos, temarios

acerca de la información del software, videos, soporte, links de descarga y guías rápidas de inicio/instalación en los diferentes sistemas operativos soportados. En la figura 3.2 se muestra las opciones en la documentación del portal web.

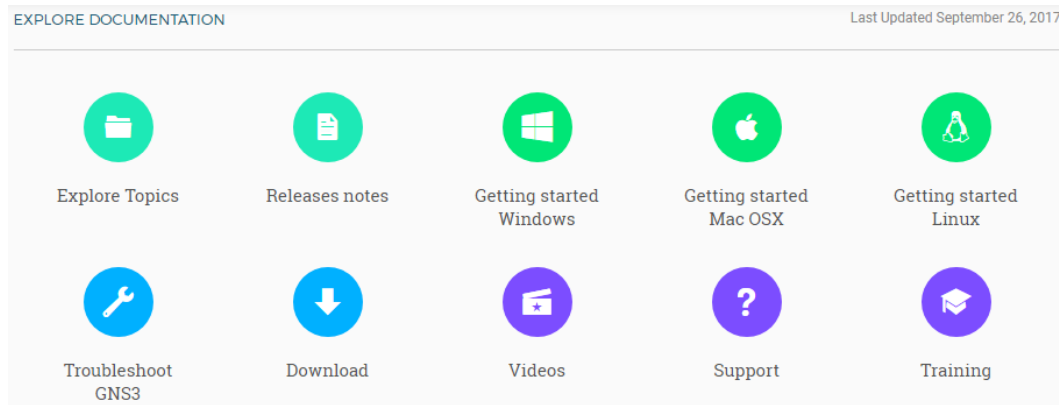


Figura 3. 2: Logo de Software GNS3

Fuente: (GNS3, 2017)

3.3. Equipamiento a utilizar.

Debido a que se trabajará en un ambiente de simulación controlado, se tiene que definir el equipamiento a utilizarse para poder plantear la topología a implementar de la red del Proveedor de Servicios. Los equipos a definirse cuentan con ciertas características debido a que utilizarán recursos de procesamiento y memoria RAM (Random Access Memory) en el computador donde se ejecutará la simulación.

Al plantear una red de un Proveedor de Servicios se debe tomar en cuenta que se utilizarán equipos de distintas características en base a la función que desempeñarán en la topología propuesta. Dentro de la documentación que facilita el portal del simulador GNS3 se puede elegir entre diferentes dispositivos enrutadores para integrar la red como se indica en la tabla 3-3 (GNS3, 2017).

Tabla 3-3. Routers soportados en GNS3

ROUTERS			
A10 vThunder	Cisco 3620	Cisco IOU L3	KEMP Free VLM
Alcatel 7750	Cisco 3640	NetScaler VPX	LEDE
Big Cloud Fabric	Cisco 3660	CloudRouter	Loadbalancer.org Enterprise VA
BIRD	Cisco 3725	Dell FTOS	MikroTik CHR
vRouter	Cisco 3745	F5 BIG-IP LTM VE	OpenWrt
vTM DE	Cisco 7200	FortiADC	OpenWrt Realview
BSDRP	Cisco CSR1000v	HPE VSR1001	VyOS
Cisco 1700	Cisco IOSv	Internet	ZeroShell
Cisco 2600	Cisco IOS XRv	Juniper vMX vCP	
Cisco 2691	Cisco IOS XRv 9000	Juniper vMX vFP	

Fuente: (GNS3, 2017)

Como equipo robusto para la red a implementar, se ha definido utilizar la imagen del equipo Cisco 7200 ya que la misma es una de las más estables probadas en entornos de emulación en GNS3 y representa un equipo de altas prestaciones para operar en el CORE de la red. Debido a que este equipamiento soporta la versión del IOS 15.X también se utilizará para la configuración de los servicios EP-LINE y EVP-LINE en la capa de AGREGACIÓN para la conexión de los clientes finales. Las características técnicas que requiere esta imagen para su simulación se indican en la tabla 3-4:

Tabla 3-4. Requerimientos de simulación CISCO7200

Cisco 7200 SERIES
IOS 15 (Mainline)
Este router recibió la actualización a la nueva versión IOS 15.X
La última liberada hasta la fecha es:
Nombre de Archivo: c7200-adventerprisek9-mz.152-4.M7.bin
RAM Mínima: 512MB
IOS 12.4.25g (Mainline)
MD5: 3 ^a 78cb61831b3ef1530f7402f5986556
Nombre de Archivo: c7200-a3jk9s-mz.124-25g.bin
RAM Mínima: 256MB
IOS 12.4.24T5 (Technology train)
No se trata de la última versión pero es fácil encontrar
MD5: 3c4148f62acf56602ce3b371ebae60c9
Nombre de Archivo: c7200-adventerprisek9-mz.124-24.T5
RAM Mínima: 256MB

Fuente: (GNS3, 2017)

Debido a las limitantes de memoria RAM y procesamiento al momento de simular una alta cantidad de equipamiento en la red, se opta que para la capa de ACCESO de los servicios a simular se utilizará un equipo Cisco 2691, el cual presenta los requerimientos en la tabla 3-5. (GNS3, 2017)

Tabla 3-5. Requerimientos de simulación CISCO2691

Cisco 2691	
IOS 12.4.25d (Mainline)	
Nombre de Archivo: c2691-adventerprisek9-mz.124-25d.bin	
MD5: a8e1f5821d87456595488d6221ce42e5	
RAM Mínima: 192MB	
IOS 12.4.15T14 (Technology train)	
Nombre de Archivo: c2691-adventerprisek9-mz.124-15.T14.bin	
MD5: 91388104d7276ad09204e36d2dfcf52d	
RAM Mínima: 256MB	

Fuente: (GNS3, 2017)

Las imágenes que fueron utilizadas dentro del simulador para el presente trabajo se detallan en la figura 3.3, figura 3.4 y figura 3.5. Una vez definido el equipamiento a utilizar y tomando en cuenta los recursos de procesamiento y hardware se procederá a proponer la topología a implementar para la red típica de un Proveedor de Servicios sobre la cual se implementarán los servicios tradicionales brindados a los clientes, y posteriormente los servicios CE2.0.

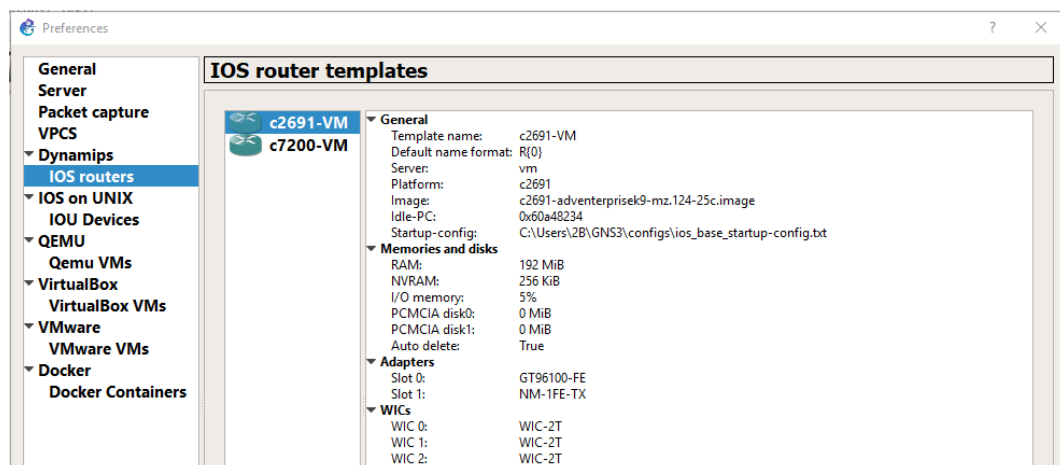


Figura 3. 3: Imagen de equipo C2691 para simulación.

Fuente: Autor

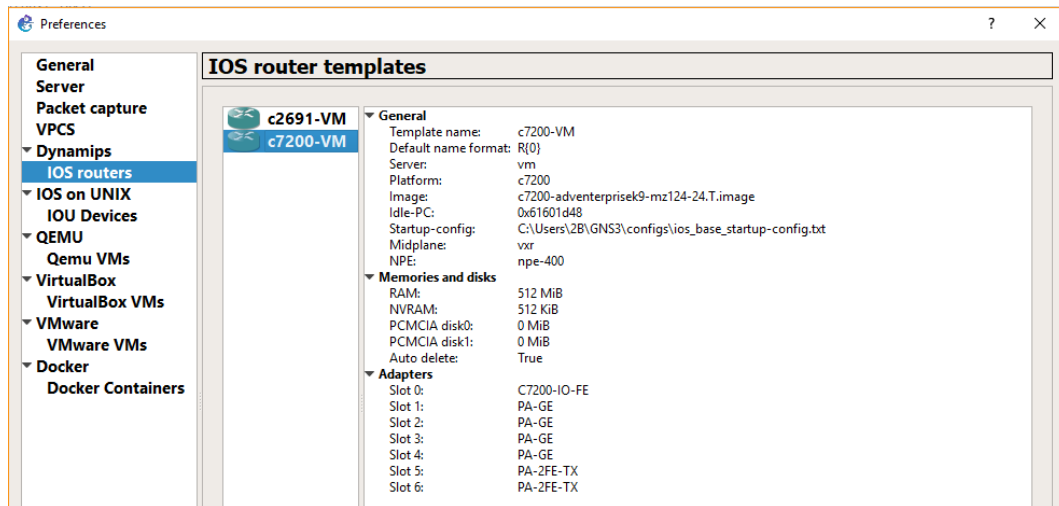


Figura 3. 4: Imagen de equipo C7200 para simulación.

Fuente: Autor

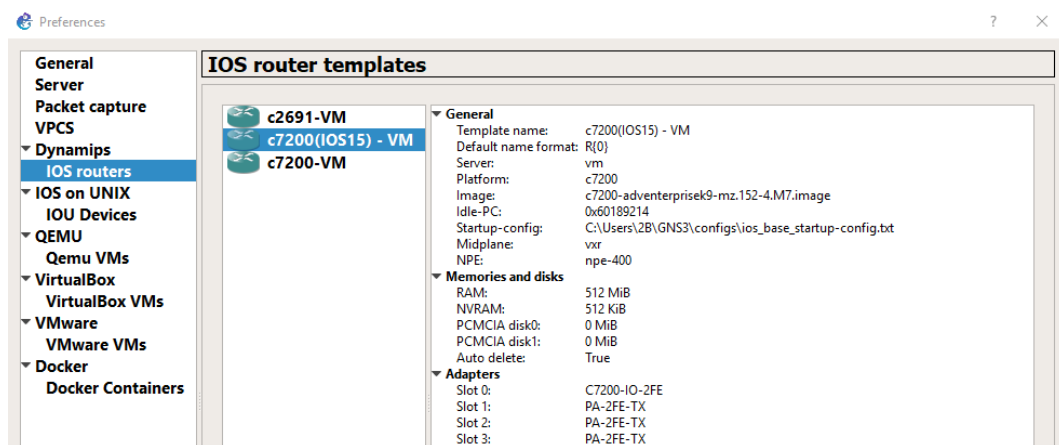


Figura 3. 5: Imagen de equipo C7200 IOS15.X para simulación.

Fuente: Autor

3.4. Diseño de la red del Proveedor de Servicios.

Para el desarrollo de la simulación sobre la cual se va a trabajar es importante tener una planificación adecuada en el despliegue de la misma. La planificación de los diferentes parámetros, configuraciones, topología y requerimientos, permite tener un dimensionamiento real sobre los recursos que se va a necesitar y de los resultados próximos a conseguir.

Dentro de un ambiente de red de un Proveedor de Servicios es de vital importancia tener una planificación que permita la escalabilidad de los parámetros y configuraciones iniciales con los que nace la red para no tener que en el futuro

replantear todo un nuevo esquema. De manera adicional la planificación sirve de base documentada para disponer de la información de manera global y generalizada, así como ciertas configuraciones puntuales y definiciones tomadas para el despliegue de la misma.

La planificación del despliegue por lo general se la denomina la Ingeniería del proyecto dentro de un ambiente laboral en un Proveedor de Servicios. Es importante que se implemente de manera previa las ingenierías a utilizarse sobre la red con el fin de mantener un orden, una planificación y un registro de toda la red. Las ingenierías se pueden desarrollar de manera independiente en base a las diferentes funcionalidades que se tendrán sobre la red, permitiendo de esa manera agregar/descartar ciertos diseños o definiciones conforme se necesiten.

Para la prestación de los servicios finales hacia los clientes es importante llevar un registro de la ingeniería que lleva cada cliente con el fin de tener documentada, en el caso de que se requiera algún cambio o, como es el caso presentado en este trabajo, la migración del mismo a una nueva ingeniería.

Ya que las ingenierías/planificaciones de la red se las puede ejecutar de una manera modular conforme a los requerimientos que se necesiten implementar, en los siguientes sub-temas se presentarán las diferentes ingenierías para la simulación de la red típica de un Proveedor de Servicios.

3.4.1. Planificación de la topología de red

Como primer paso es importante definir la topología que se va a implementar en la red con el fin de definir el rol que tendrán los equipos, la escalabilidad de la red, la redundancia, el flujo que debe tomar el tráfico, la ubicación de cada equipo (en función al número de localidades que abarcará la red), la segmentación de capas para la red, etc.

Para la red a simular se va a implementar una red que tenga su capa de CORE, AGREGACIÓN y ACCESO como se indica en la figura 3.6 a continuación:

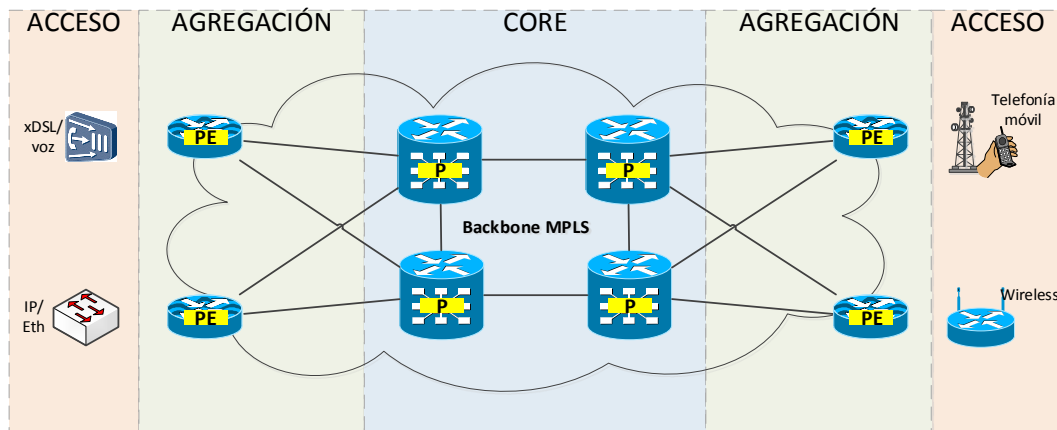


Figura 3. 6: Topología de red a Simular

Fuente: Autor

En el apartado 3.3 se definieron los equipos a utilizar en el presente trabajo, por lo que las imágenes de los equipos CISCO 7200 servirán para la capa de CORE como equipos P (Provider), los cuales tendrán la funcionalidad de un equipo de conmutación de etiquetas de altas prestaciones (LSR - Label Switch Router) y de manera adicional servirán como Reflectores de Rutas (RR - Route Reflector).

Para la capa de agregación se utilizará los equipos CISCO 7200 con la versión de software IOS 15.X, en los cuales se configurarán los servicios para los clientes a simular. Debido a que se va a centrar en los servicios CE2.0 la capa de acceso será Ethernet por lo que los equipos de los clientes finales se pueden simular utilizando la imagen de los equipos CISCO 2691.

La definición de la ingeniería para la topología a utilizarse da como resultado el uso de 8 equipos para la red del Proveedor de Servicios. Con base a los 8 equipos a utilizarse se planteará la asignación de los recursos que cada uno utilizará para su despliegue.

3.4.2. Planificación de los recursos para los equipos de red

Debido a que se utilizarán 8 equipos para simular la red del Proveedor de Servicios, se debe realizar la planificación de los recursos que estos equipos

utilizarán dentro de la red con el fin de tener documentado el despliegue inicial de la red sobre la cual se va a trabajar.

3.4.2.1. Definición del Nombre del Equipo (Hostname)

En una red real de un Proveedor de Servicios en la que su área de cobertura abarque una zona total o parcial del territorio de un país se tienen más de 8 equipos por lo que es importante asignarles una nomenclatura clara que permita identificar de una manera rápida al operador de red la zona a la que pertenece el equipo. Para la simulación a utilizarse se define que los 8 equipos a los que se hace referencia se encontrarán ubicados en 8 sitios diferentes uno del otro, simulando así 8 localidades que cubrirá la red a ser desplegada.

En la figura 3.5 se pudo observar la definición de la topología lógica que se está implementando, en la que es notoria la disposición que se tiene para la capa de CORE, AGREGACIÓN y ACCESO, pero en una implementación física puede ser que las localidades donde se implementan los equipos no se encuentren dispuestas geográficamente en ese orden, lo que imposibilita realizar la distinción de la funcionalidad y de la capa a la que pertenece un equipo. Es necesario asignar un distintivo dentro de la nomenclatura de cada equipo que pueda aclarar la funcionalidad que va a desempeñar sobre la red y la capa a la que pertenece.

En diversos entornos y según la disposición de los recursos que se planifiquen en el despliegue de una red de proveedores de servicio, es posible tener más de un equipo en la misma central/sitio que se encuentre ejecutando las mismas funcionalidades a uno ya existente. Este tipo de consideraciones se tiene cuando el crecimiento a nivel de flujo de tráfico, interfaces utilizadas y el diseño de la expansión de la red determinan la instalación o bajo un concepto de ingeniería que maneje el personal encargado del diseño de la red. Para poder diferenciar los equipos que se encuentran geográficamente en la misma central/sitio del Proveedor de Servicios, y que se encuentran desempeñando las mismas funciones, se coloca un identificador numérico en su nomenclatura para así identificar cada uno de los equipos que se encuentren bajo estas consideraciones.

Teniendo en cuenta las consideraciones indicadas se puede definir un patrón para la nomenclatura de los equipos que formarán la red, y que permita el crecimiento a futuro en caso de necesitar una expansión planificada. Si bien bajo los objetivos enmarcados en este trabajo no se tiene planificada una expansión, es importante resaltar estas consideraciones ya que forman parte del criterio para el diseño de una red de un Proveedor de Servicios.

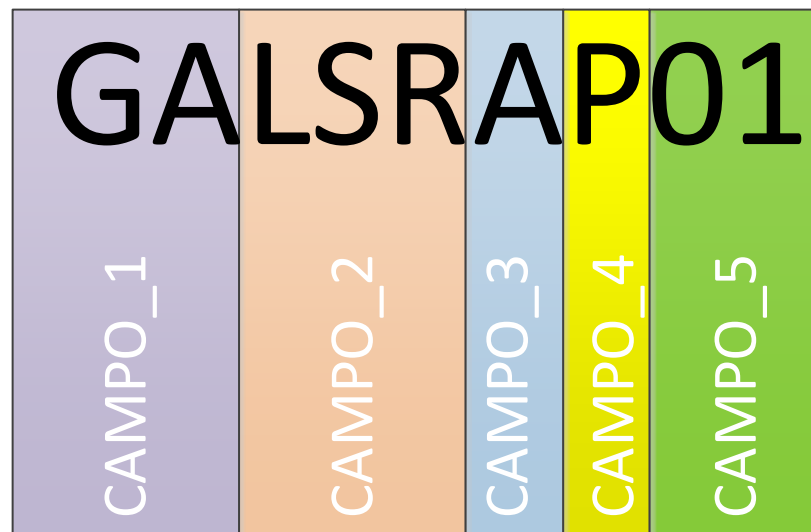


Figura 3. 7: Patrón de Nomenclatura para equipos de Red

Fuente: Autor

En la figura 3.7 se define un patrón que cuenta con 5 campos para definir las diferentes centrales/sitios a los que pertenecerán los equipos de la red a simular, así como la funcionalidad que desempeñan, la red a la que pertenecen y un número para especificar la cantidad de equipos en la misma central que realizan las mismas funciones.

- Campo_1: Indica la red a la que pertenece el equipo. Se define la nomenclatura “GA” para los 8 equipos ya que pertenecen al mismo entorno de red simulado y se encontrarán bajo un mismo ambiente. Las letras hacen un acrónimo para el nombre del autor de este trabajo (Geovanny Avendaño).

- Campo_2: Indica la funcionalidad que va a tener un equipo dentro de la red del Proveedor de Servicio, distinguiendo equipos que operan como LSR de los que operan como LER (Label Edge Router). La definición de las funcionalidades las dicta quien diseña la red.
- Campo_3: Indica el sitio/localidad a la que pertenece el equipo. Para el caso de la simulación se tiene 8 diferentes localidades para los 8 equipos que conforman la red. Las localidades se definen por las primeras 8 letras del alfabeto.
- Campo_4: Indica si un equipo se encuentra en el CORE de la red (P - Provider) o sirve de AGREGACIÓN/ACCESO (PE – Provider Edge).
- Campo_5: Identificador numérico para distinguir equipos de la misma central/sitio que desempeñan funciones iguales. El contador puede ir desde 01 – 99 para un posible crecimiento de la red.

Los diferentes campos pueden ser definidos de maneras distintas según sea el criterio de quien diseña la red y de los requerimientos que se tengan, pudiendo ser utilizados para indicar una provincia, ciudad, nombre del sitio, nombre de la central, etc. O incluso puede variar el número de campos que se asigne para la nomenclatura de los equipos que conforman la red de un Proveedor de Servicios. Los campos indicados se definen para la simulación a implementarse en el presente trabajo como se indica en la tabla 3-6 a continuación:

Tabla 3-6. Recursos de equipamiento asignado por Sitio

Sitio	Código	Num	Tipo	Nombre del equipo
ROUTERS (CORE)				
SP_A	P	01	LSR	GALSRAP01
SP_B	P	01	LSR	GALSRBP02
SP_C	P	01	LSR	GALSRCP03
SP_D	P	01	LSR	GALSRDP04
ROUTERS (AGREGACIÓN-DISTRIBUCIÓN)				
SP_E	E	01	LER	GALEREE01
SP_F	E	01	LER	GALERFE02
SP_G	E	01	LER	GALERGE03
SP_H	E	01	LER	GALERHE04

Fuente: Autor

3.4.2.2. Definición del Direccionamiento de Sistema del Equipo

Es importante que cada equipo de la red contenga su direccionamiento administrativo (direccionamiento de sistema) en una interface que siempre se encuentre activa y que no se vea afectada por problemas físicos de la red (caídas de enlaces, daño en puertos, daños en tarjetas, etc.) ya que será quien permita identificar y acceder al equipo para poder configurarlo, diagnosticarlo y monitorearlo. Este direccionamiento se lo configura por lo general en una interface Loopback en cada equipo ya que permite tenerla siempre en modo activo administrativamente y no pasará a un estado inhibido salvo que todo el equipo falle.

El direccionamiento que se le asigna a cada equipo debe estar bien definido en el diseño inicial ya que éste debe ser único a lo largo de toda la red con el fin de evitar conflictos entre los equipos, y entre los protocolos que suelen utilizar este direccionamiento para su operación como el IGP (Interior Gateway Protocol), EGP (Exterior Gateway Protocol), etc. Para la definición del direccionamiento de sistema de los equipos de la simulación, se asigna el segmento de red 10.50.0.0/16 al cual se le aplicará un proceso de subnetting con el fin de utilizar todo ese segmento para los equipos actuales y futuros cuando aplique el caso. En la tabla 3-7 se indica el direccionamiento asignado a cada equipo que será utilizado en la simulación. Este direccionamiento se lo configura a cada equipo en la interface Loopback 10.

Tabla 3-7. Direccionamiento de sistema asignado

Sitio	Nombre del equipo	Loopback IP 10 (/32)
ROUTERS (CORE)		
SP_A	GALSRAP01	10.50.1.100
SP_B	GALSRBP02	10.50.2.100
SP_C	GALSRCP03	10.50.3.100
SP_D	GALSRDP04	10.50.4.100
ROUTERS (AGREGACIÓN-DISTRIBUCIÓN)		
SP_E	GALEREE01	10.50.10.100
SP_F	GALERFE02	10.50.20.100
SP_G	GALERGE03	10.60.30.100
SP_H	GALERHE04	10.60.40.100

Fuente: Autor

3.4.2.3. Definición de enlaces de red

En base a la figura 3.6 en la que se plantea la topología a implementar en la simulación y a los equipos a ser utilizados dentro del entorno del software GNS3 se procederá a definir los enlaces que brindarán la conexión deseada entre los equipos con el fin de conseguir la red propuesta sobre la que se implementarán los servicios para los clientes finales.

Para la definición de los enlaces se debe tomar en cuenta los recursos a nivel de interfaces físicas que se cuenta en los equipos con el fin de planificar el despliegue de cada uno de los enlaces. Para los enlaces a nivel de la capa de CORE se utilizará las interfaces GigabitEthernet de los equipos CISCO 7200 mientras que para las interfaces que conectan los sitios de AGREGACIÓN hacia el CORE serán a nivel de interfaces FastEthernet. Cabe indicar que al no ser una red que curse un tráfico real no se requiere mayor capacidad en los enlaces descritos.

En la figura 3.8 se presenta el diagrama de conexión planteado en la simulación dentro del software GNS3 junto con la capa a la que pertenece cada equipo y las interfaces utilizadas para la conexión de cada enlace.

Los recursos que se asignan para los enlaces de red pertenecientes al dominio de CORE se detallan en la tabla 3-8:

Tabla 3-8. Interfaces asignadas enlaces CORE

SITIO Origen	Nombre de equipo Origen	Interface Origen	SITIO Destino	Nombre de equipo Destino	Interface Destino
SP_A	GALSRAP01	Gi1/0	SP_B	GALSRBP02	Gi1/0
SP_A	GALSRAP01	Gi2/0	SP_C	GALSRCP03	Gi2/0
SP_D	GALSRDP04	Gi2/0	SP_B	GALSRBP02	Gi2/0
SP_D	GALSRDP04	Gi1/0	SP_C	GALSRCP03	Gi1/0

Fuente: Autor

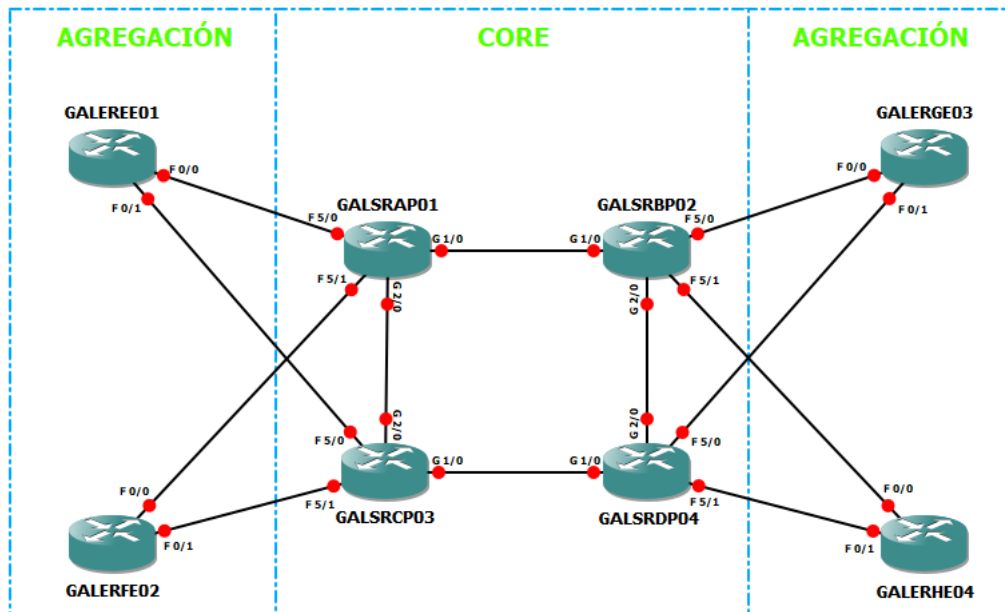


Figura 3. 8: Diagrama de conexión de equipos de red

Fuente: Autor

De igual forma los recursos que se asignan para los enlaces de red pertenecientes al dominio de AGREGACIÓN se detallan en la tabla 3-9:

Tabla 3-9. Interfaces asignadas enlaces AGREGACIÓN

SITIO Origen	Nombre de equipo Origen	Interface Origen	SITIO Destino	Nombre de equipo Destino	Interface Destino
SP_A	GALSRAP01	Fa5/0	SP_E	GALEREE01	Fa0/0
SP_A	GALSRAP01	Fa5/1	SP_F	GALERFE02	Fa0/0
SP_B	GALSGBP02	Fa5/0	SP_G	GALERGE03	Fa0/0
SP_B	GALSGBP02	Fa5/1	SP_H	GALERHE04	Fa0/0
SP_C	GALSRCP03	Fa5/0	SP_E	GALEREE01	Fa0/1
SP_C	GALSRCP03	Fa5/1	SP_F	GALERFE02	Fa0/1
SP_D	GALSBDP04	Fa5/0	SP_G	GALERGE03	Fa0/1
SP_D	GALSBDP04	Fa5/1	SP_H	GALERHE04	Fa0/1

Fuente: Autor

Una vez definidas las interfaces a utilizar para cada uno de los enlaces según el planteamiento de la topología de red, es importante asignarles una descripción con el fin de mantener un orden y de facilitar la operatividad y mantenimiento de la red. Se recomienda que la descripción que se le asigna a cada uno de los enlaces

tenga la información necesaria para que el ingeniero que se encuentra operando la red pueda identificar de manera rápida los recursos que involucran al enlace en mención. En las tablas 3-10 y 3-11 se indica el cuadro de descripciones para cada uno de las interfaces y enlaces en la capa de CORE.

Tabla 3-10. Descripción de interfaces origen para enlaces CORE

Nombre de equipo Origen	Descripción del enlace Equipo Origen	Interface Origen
GALSRAP01	###LINK_TO_GALSRBP02_Gi1/0_1G###	Gi1/0
GALSRAP01	###LINK_TO_GALSRCP03_Gi2/0_1G###	Gi2/0
GALSRDP04	###LINK_TO_GALSRBP02_Gi2/0_1G###	Gi2/0
GALSRDP04	###LINK_TO_GALSRCP03_Gi1/0_1G###	Gi1/0

Fuente: Autor

Tabla 3-11. Descripción de interfaces destino para enlaces CORE

Nombre de equipo Destino	Descripción del enlace Equipo Destino	Interface Destino
GALSRBP02	###LINK_TO_GALSRAP01_Gi1/0_1G###	Gi1/0
GALSRCP03	###LINK_TO_GALSRAP01_Gi2/0_1G###	Gi2/0
GALSRBP02	###LINK_TO_GALSRDP04_Gi2/0_1G###	Gi2/0
GALSRCP03	###LINK_TO_GALSRDP04_Gi1/0_1G###	Gi1/0

Fuente: Autor

Las descripciones de origen y destino de los enlaces a nivel de la capa de AGREGACIÓN se indican en las tablas 3-12 y 3-13.

Tabla 3-12. Descripción de interfaces origen para enlaces AGREGACIÓN

Nombre de equipo Origen	Descripción del enlace Equipo Origen	Interface Origen
GALSRAP01	###LINK_TO_GALEREE01_Fa0/0_100M###	Fa5/0
GALSRAP01	###LINK_TO_GALERFE02_Fa0/0_100M###	Fa5/1
GALSRBP02	###LINK_TO_GALERGE03_Fa0/0_100M###	Fa5/0
GALSRBP02	###LINK_TO_GALERHE04_Fa0/0_100M###	Fa5/1
GALSRCP03	###LINK_TO_GALEREE01_Fa0/1_100M###	Fa5/0
GALSRCP03	###LINK_TO_GALERFE02_Fa0/1_100M###	Fa5/1
GALSRDP04	###LINK_TO_GALERGE03_Fa0/1_100M###	Fa5/0
GALSRDP04	###LINK_TO_GALERHE04_Fa0/1_100M###	Fa5/1

Fuente: Autor

Tabla 3-13. Descripción de interfaces destino para enlaces AGREGACIÓN

Nombre de equipo Destino	Descripción del enlace Equipo Destino	Interface Destino
GALEREE01	###LINK_TO_GALSRAP01_Fa5/0_100M###	Fa0/0
GALERFE02	###LINK_TO_GALSRAP01_Fa5/1_100M###	Fa0/0
GALERGE03	###LINK_TO_GALSRBP02_Fa5/0_100M###	Fa0/0
GALERHE04	###LINK_TO_GALSRBP02_Fa5/1_100M###	Fa0/0
GALEREE01	###LINK_TO_GALSRCP03_Fa5/0_100M###	Fa0/1
GALERFE02	###LINK_TO_GALSRCP03_Fa5/1_100M###	Fa0/1
GALERGE03	###LINK_TO_GALSRDP04_Fa5/0_100M###	Fa0/1
GALERHE04	###LINK_TO_GALSRDP04_Fa5/1_100M###	Fa0/1

Fuente: Autor

Por último para habilitar un enlace de red se necesita asignar el direccionamiento necesario para tener conectividad entre los equipos a través de todas las interfaces ya definidas. Para el direccionamiento de los enlaces de red entre equipos de CORE ha sido asignado el segmento 10.10.0.0/16 y para los enlaces a nivel de la capa de AGREGACIÓN el segmento 10.20.0.0/16. Es importante que en el diseño se especifique los segmentos asignados a cada capa con el fin de evitar duplicidades y garantizar la escalabilidad de la red en función del número de equipos. El direccionamiento asignado para los enlaces de CORE se indican en la tabla 3-14 a continuación.

Tabla 3-14. Direccionamiento asignado para enlaces CORE

Nombre de equipo Origen	Dirección IP de enlace Origen	Interface Origen	Nombre de equipo Destino	Dirección IP de enlace Destino	Interface Destino
GALSRAP01	10.10.0.1	Gi1/0	GALSRBP02	10.10.0.2	Gi1/0
GALSRAP01	10.10.0.5	Gi2/0	GALSRCP03	10.10.0.6	Gi2/0
GALSRDP04	10.10.0.9	Gi2/0	GALSRBP02	10.10.0.10	Gi2/0
GALSRDP04	10.10.0.13	Gi1/0	GALSRCP03	10.10.0.14	Gi1/0

Fuente: Autor

Para los enlaces de la capa de AGREGACIÓN se asigna el direccionamiento de la tabla 3-15:

Tabla 3-15. Direccionamiento asignado para enlaces AGREGACIÓN

Nombre de equipo Origen	Dirección IP de enlace Origen	Interface Origen	Nombre de equipo Destino	Dirección IP de enlace Destino	Interface Destino
GALSRAP01	10.20.0.1	Fa5/0	GALEREE01	10.20.0.2	Fa0/0
GALSRAP01	10.20.0.5	Fa5/1	GALERFE02	10.20.0.6	Fa0/0
GALSRBP02	10.20.0.9	Fa5/0	GALERGE03	10.20.0.10	Fa0/0
GALSRBP02	10.20.0.13	Fa5/1	GALERHE04	10.20.0.14	Fa0/0
GALSRCP03	10.20.0.17	Fa5/0	GALEREE01	10.20.0.18	Fa0/1
GALSRCP03	10.20.0.21	Fa5/1	GALERFE02	10.20.0.22	Fa0/1
GALSRDP04	10.20.0.25	Fa5/0	GALERGE03	10.20.0.26	Fa0/1
GALSRDP04	10.20.0.29	Fa5/1	GALERHE04	10.20.0.30	Fa0/1

Fuente: Autor

La planificación de los recursos a ser utilizados para la simulación en un ambiente controlado en el software GNS3 permite partir con la configuración inicial que tendrá la red. Una vez que se ha asignado los recursos hasta este punto, y con la respectiva configuración en los equipos, permite tener conectividad en cada uno de los sitios de la red del Proveedor de Servicios planteada para a futuro realizar la planificación de las ingenierías de cada protocolo y servicio a implementar. Las configuraciones iniciales de cada equipo se detallan en las tablas 3-16, 3-17, 3-18 y 3-19 a continuación.

Tabla 3-16. Plantilla de configuración inicial GALSRAP01 y GALSRBP02

CONFIGURACION INICIAL GALSRAP01	CONFIGURACION INICIAL GALSRBP02
hostname GALSRAP01	hostname GALSRBP02
!	!
interface Loopback10	interface Loopback10
description	description
###LOOPBACK_SYSTEM_IP_GALSRAP01###	###LOOPBACK_SYSTEM_IP_GALSRBP02###
ip address 10.50.1.100 255.255.255.255	ip address 10.50.2.100 255.255.255.255
!	!
interface GigabitEthernet1/0	interface GigabitEthernet1/0
description	description
###LINK_TO_GALSRBP02_Gi1/0_1G###	###LINK_TO_GALSRAP01_Gi1/0_1G###
mtu 2000	mtu 2000
ip address 10.10.0.1 255.255.255.252	ip address 10.10.0.2 255.255.255.252
negotiation auto	negotiation auto
no shutdown	no shutdown
!	!
interface GigabitEthernet2/0	interface GigabitEthernet2/0

<pre> description ###LINK_TO_GALSRCP03_Gi2/0_1G### mtu 2000 ip address 10.10.0.5 255.255.255.252 negotiation auto no shutdown ! interface FastEthernet5/0 description ###LINK_TO_GALEREE01_Fa0/0_100M### ip address 10.20.0.1 255.255.255.252 duplex auto speed auto no shutdow ! interface FastEthernet5/1 description ###LINK_TO_GALERFE02_Fa0/0_100M### ip address 10.20.0.5 255.255.255.252 duplex auto speed auto no shutdow ! end </pre>	<pre> description ###LINK_TO_GALSRDP04_Gi2/0_1G### ip address 10.10.0.10 255.255.255.252 negotiation auto no shutdown ! interface FastEthernet5/0 description ###LINK_TO_GALERGE03_Fa0/0_100M### ip address 10.20.0.9 255.255.255.252 duplex auto speed auto no shutdow ! interface FastEthernet5/1 description ###LINK_TO_GALERHE04_Fa0/0_100M### mtu 2000 ip address 10.20.0.13 255.255.255.252 duplex auto speed auto no shutdow ! End </pre>
--	--

Fuente: Autor

Tabla 3-17. Plantilla de configuración inicial GALSRCP03 y GALSRDP04

CONFIGURACION INICIAL GALSRCP03	CONFIGURACION INICIAL GALSRDP04
<pre> hostname GALSRCP03 ! interface Loopback10 description ###LOOPBACK_SYSTEM_IP_GALSRCP03### ip address 10.50.3.100 255.255.255.255 ! interface GigabitEthernet1/0 description ###LINK_TO_GALSRDP04_Gi1/0_1G### mtu 2000 ip address 10.10.0.14 255.255.255.252 negotiation auto no shutdown ! interface GigabitEthernet2/0 </pre>	<pre> hostname GALSRDP04 ! interface Loopback10 description ###LOOPBACK_SYSTEM_IP_GALSRDP04### ip address 10.50.4.100 255.255.255.255 ! interface GigabitEthernet1/0 description ###LINK_TO_GALSRCP03_Gi1/0_1G### mtu 2000 ip address 10.10.0.13 255.255.255.252 negotiation auto no shutdown ! interface GigabitEthernet2/0 </pre>

<pre> description ###LINK_TO_GALSRAP01_Gi2/0_1G### mtu 2000 ip address 10.10.0.6 255.255.255.252 negotiation auto no shutdown ! interface FastEthernet5/0 description ###LINK_TO_GALEREE01_Fa0/1_100M### ip address 10.20.0.17 255.255.255.252 duplex auto speed auto no shutdow ! interface FastEthernet5/1 description ###LINK_TO_GALERFE02_Fa0/1_100M### ip address 10.20.0.21 255.255.255.252 duplex auto speed auto no shutdow ! end </pre>	<pre> description ###LINK_TO_GALSRBP02_Gi2/0_1G### mtu 2000 ip address 10.10.0.9 255.255.255.252 negotiation auto no shutdown ! interface FastEthernet5/0 description ###LINK_TO_GALERGE03_Fa0/1_100M### ip address 10.20.0.25 255.255.255.252 duplex auto speed auto no shutdow ! interface FastEthernet5/1 description ###LINK_TO_GALERHE04_Fa0/1_100M### ip address 10.20.0.29 255.255.255.252 duplex auto speed auto no shutdow ! end </pre>
--	--

Fuente: Autor

Tabla 3-18. Plantilla de configuración inicial GALEREE01 y GALERFE02

CONFIGURACION INICIAL GALEREE01	CONFIGURACION INICIAL GALERFE02
<pre> hostname GALEREE01 ! interface Loopback10 description ###LOOPBACK_SYSTEM_IP_GALEREE01### ip address 10.50.10.100 255.255.255.255 ! interface FastEthernet0/0 description ###LINK_TO_GALSRAP01_Fa5/0_100M### ip address 10.20.0.2 255.255.255.252 duplex auto speed auto no shutdow ! interface FastEthernet0/1 description ###LINK_TO_GALSRCP03_Fa5/0_100M### </pre>	<pre> hostname GALERFE02 ! interface Loopback10 description ###LOOPBACK_SYSTEM_IP_GALERFE02### ip address 10.50.20.100 255.255.255.255 ! interface FastEthernet0/0 description ###LINK_TO_GALSRAP01_Fa5/1_100M### ip address 10.20.0.6 255.255.255.252 duplex auto speed auto no shutdow ! interface FastEthernet0/1 description ###LINK_TO_GALSRCP03_Fa5/1_100M### </pre>

<pre> ip address 10.20.0.18 255.255.255.252 duplex auto speed auto no shutdow ! end </pre>	<pre> ip address 10.20.0.22 255.255.255.252 duplex auto speed auto no shutdow ! end </pre>
--	--

Fuente: Autor

Tabla 3-19. Plantilla de configuración inicial GALERGE03 y GALERHE04

CONFIGURACION INICIAL GALERGE03	CONFIGURACION INICIAL GALERHE04
<pre> hostname GALERGE03 ! interface Loopback10 description ###LOOPBACK_SYSTEM_IP_GALERGE03### ip address 10.50.30.100 255.255.255.255 ! interface FastEthernet0/0 description ###LINK_TO_GALSRBP02_Fa5/0_100M### ip address 10.20.0.10 255.255.255.252 duplex auto speed auto no shutdow ! interface FastEthernet0/1 description ###LINK_TO_GALSRDP04_Fa5/0_100M### ip address 10.20.0.26 255.255.255.252 duplex auto speed auto no shutdow ! end </pre>	<pre> hostname GALERHE04 ! interface Loopback10 description ###LOOPBACK_SYSTEM_IP_GALERHE04### ip address 10.50.40.100 255.255.255.255 ! interface FastEthernet0/0 description ###LINK_TO_GALSRBP02_Fa5/1_100M### ip address 10.20.0.14 255.255.255.252 duplex auto speed auto no shutdow ! interface FastEthernet0/1 description ###LINK_TO_GALSRDP04_Fa5/1_100M### ip address 10.20.0.30 255.255.255.252 duplex auto speed auto no shutdow ! end </pre>

Fuente: Autor

3.4.3. Planificación del protocolo IGP para la red

Con el fin de obtener conectividad entre todas las direcciones IP de las interfaces físicas y lógicas en la red planteada es necesaria la utilización de un protocolo de enrutamiento dinámico. Para el caso de la red a implementar se ha elegido a ISIS (Intermediate System to Intermediate System) el cual permite el descubrimiento de las direcciones de red que participan en el protocolo de una manera dinámica

construyendo una base topológica completa de la red, la misma que se almacena en cada uno de los dispositivos que participan en el protocolo y sirve de herramienta para el despliegue de futuras funcionalidades como por ejemplo ingeniería de tráfico.

Los recursos que se asignan para poder implementar el protocolo de enrutamiento en cada uno de los nodos se define en la tabla 3-20.

Tabla 3-20. Recursos asignados para ISIS

Nombre del equipo	Network Entity Title (NET) AREA 49.0001	Tipo	Tipo de Métrica	Interfaces
GALSRAP0 1	49.0001.0100.5 000.1100.00	is-type level-2- only	metric-style wide	Loopback 10 (passive- interface) Gi1/0 Gi2/0 Fa5/0 Fa5/1
GALSRBP0 2	49.0001.0100.5 000.2100.00	is-type level-2- only	metric-style wide	Loopback 10 (passive- interface) Gi1/0 Gi2/0 Fa5/0 Fa5/1
GALSRCP0 3	49.0001.0100.5 000.3100.00	is-type level-2- only	metric-style wide	Loopback 10 (passive- interface) Gi1/0 Gi2/0 Fa5/0 Fa5/1
GALSRDP0 4	49.0001.0100.5 000.4100.00	is-type level-2- only	metric-style wide	Loopback 10 (passive- interface) Gi1/0 Gi2/0 Fa5/0 Fa5/1
GALEREE0 1	49.0001.0100.5 001.0100.00	is-type level-2- only	metric-style wide	Loopback 10 (passive- interface) Fa0/0 Fa0/1
GALERFE0 2	49.0001.0100.5 002.0100.00	is-type level-2- only	metric-style wide	Loopback 10 (passive- interface) Fa0/0 Fa0/1
GALERGE0 3	49.0001.0100.5 003.0100.00	is-type level-2- only	metric-style wide	Loopback 10 (passive- interface) Fa0/0

				Fa0/1
GALERHE0 4	49.0001.0100.5 004.0100.00	is-type level-2- only	metric-style wide	Loopback 10 (passive- interface) Fa0/0 Fa0/1

Fuente: Autor

Dentro de los parámetros asignados para cada equipo se tiene la dirección NET (Network Entity Title) la misma que sirve como un identificador único del equipo dentro de la red a desplegar, el mismo que no tiene ninguna relación con alguna dirección IP, pero que para tener un despliegue ordenado se ha embebido la dirección del sistema de cada equipo en la dirección NET para configurar ISIS.

Se definen todos los enlaces como ISIS de nivel 2 con el fin de obtener una sola red de backbone para el proveedor de servicios, la cual permite que todos los equipos puedan conocer el direccionamiento de todas las interfaces configuradas en la red propuesta. Este tipo de criterios pueden diferir en función del diseño que se desee implementar, del número de equipamiento y de las características de los mismos. El tipo de métrica a utilizar se la configura como “amplia” ya que la misma da una mayor apertura al momento de configurar cada enlace para tomar la decisión del flujo que tomará el tráfico por la red del Proveedor de Servicios. Finalmente se define las interfaces que participarán en el protocolo de enrutamiento, las mismas que podrán ser alcanzables en todo el dominio de red.

Se ejemplificará las configuraciones en la tabla 3-21 para uno de los equipos ya que para el resto se mantienen los mismos comandos y lo que difiere son los parámetros de la NET según lo indicado en la Tabla 3-20 y las interfaces en las que el protocolo se habilita.

Tabla 3-21. Plantilla de configuración inicial ISIS

CONFIGURACION ISIS GALSRAP01
<pre>router isis 1 net 49.0001.0100.5000.1100.00 is-type level-2-only metric-style wide</pre>

```

passive-interface Loopback10
!
interface Loopback10
ip router isis 1
!
interface GigabitEthernet1/0
ip router isis 1
isis circuit-type level-2-only
isis network point-to-point
!

```

Fuente: Autor

Para comprobar que efectivamente se encuentra habilitado el protocolo en las interfaces solicitadas, se prueba con el siguiente comando:

```

GALSRAP01#sh ip route isis
10.0.0.0/8 is variably subnetted, 20 subnets, 2 masks
i L2 10.20.0.28/30 [115/30] via 10.10.0.6, GigabitEthernet2/0
      [115/30] via 10.10.0.2, GigabitEthernet1/0
i L2 10.20.0.24/30 [115/30] via 10.10.0.6, GigabitEthernet2/0
      [115/30] via 10.10.0.2, GigabitEthernet1/0
i L2 10.10.0.8/30 [115/20] via 10.10.0.2, GigabitEthernet1/0
i L2 10.20.0.20/30 [115/20] via 10.20.0.6, FastEthernet5/1
      [115/20] via 10.10.0.6, GigabitEthernet2/0
i L2 10.10.0.12/30 [115/20] via 10.10.0.6, GigabitEthernet2/0
i L2 10.20.0.16/30 [115/20] via 10.20.0.2, FastEthernet5/0
      [115/20] via 10.10.0.6, GigabitEthernet2/0
i L2 10.20.0.12/30 [115/20] via 10.10.0.2, GigabitEthernet1/0
i L2 10.20.0.8/30 [115/20] via 10.10.0.2, GigabitEthernet1/0
i L2 10.50.30.100/32 [115/30] via 10.10.0.2, GigabitEthernet1/0
i L2 10.50.20.100/32 [115/20] via 10.20.0.6, FastEthernet5/1
i L2 10.50.10.100/32 [115/20] via 10.20.0.2, FastEthernet5/0
i L2 10.50.4.100/32 [115/30] via 10.10.0.6, GigabitEthernet2/0
      [115/30] via 10.10.0.2, GigabitEthernet1/0
i L2 10.50.2.100/32 [115/20] via 10.10.0.2, GigabitEthernet1/0
i L2 10.50.3.100/32 [115/20] via 10.10.0.6, GigabitEthernet2/0
i L2 10.50.40.100/32 [115/30] via 10.10.0.2, GigabitEthernet1/0

```

Con lo expuesto se verifica que se aprenden todas las direcciones IP asignadas a las interfaces Loopback y a las interfaces físicas de cada equipo. Se verifica que todos los enlaces están habilitados en el nivel 2 del protocolo de enrutamiento ISIS.

3.4.4. Planificación de MPLS y RSVP-TE

Una vez que se encuentra configurado el protocolo de enrutamiento en capa 3 en los equipos de la red, es necesaria la implementación de MPLS y RSVP-TE (Resource Reservation Protocol - Traffic Engineering) con el fin de aprovechar las funcionalidades que brindan los protocolos para el transporte del tráfico sobre una red de un Proveedor de Servicios. El protocolo MPLS permite la asignación de etiquetas a cada uno de los flujos de tráfico que cursan por la red, permitiendo así que los equipos no necesariamente analicen el encabezado IP sino únicamente el MPLS. Al analizar únicamente etiquetas en cada uno de los equipos de la red, permite aprovechar esta forma de transportar paquetes para añadir nuevas cabeceras, las mismas que facilitan la inclusión de protocolos como MP-BGP (Multi-Protocol Border Gateway Protocol) para la inclusión de L3VPN y L2VPN así como de etiquetas para túneles de ingeniería de tráfico como RSVP-TE.

La planificación para el despliegue de MPLS y RSVP-SE se muestra en la tabla 3-22. Todas las interfaces de los equipos que conforman la red del Proveedor de Servicios objeto de simulación tendrán configurados los protocolos ya que permite el transporte del tráfico de los diferentes servicios que cursan por la red.

Tabla 3-22. Recursos asignados para MPLS y RSVP-TE

SITIO	Nombre del Equipo	Interface MPLS	Interface RSVP TE	Porcentaje de reserva en RSVP TE
SP_A	GALSRAP01	Gi1/0 Gi2/0 Fa5/0 Fa5/1	Gi1/0 Gi2/0 Fa5/0 Fa5/1	80%
SP_B	GALSRBP02	Gi1/0 Gi2/0 Fa5/0 Fa5/1	Gi1/0 Gi2/0 Fa5/0 Fa5/1	80%
SP_C	GALSRCP03	Gi1/0 Gi2/0 Fa5/0 Fa5/1	Gi1/0 Gi2/0 Fa5/0 Fa5/1	80%

SP_D	GALSRDP04	Gi1/0 Gi2/0 Fa5/0 Fa5/1	Gi1/0 Gi2/0 Fa5/0 Fa5/1	80%
SP_E	GALEREE01	Fa0/0 Fa0/1	Fa0/0 Fa0/1	80%
SP_F	GALERFE02	Fa0/0 Fa0/1	Fa0/0 Fa0/1	80%
SP_G	GALERGE03	Fa0/0 Fa0/1	Fa0/0 Fa0/1	80%
SP_H	GALERHE04	Fa0/0 Fa0/1	Fa0/0 Fa0/1	80%

Fuente: Autor

En la tabla 3-23 se muestran las configuraciones para los equipos que pertenecen al dominio de CORE ejemplificado para un equipo.

Tabla 3-23. Plantilla de configuración MPLS y RSVP-TE equipos CORE

```

CONFIGURACION MPLS / RSVP EQUIPOS CORE
interface GigabitEthernet1/0
 mpls label protocol ldp
 mpls ip
 ip rsvp bandwidth 800 800
 !
interface GigabitEthernet2/0
 mpls label protocol ldp
 mpls ip
 ip rsvp bandwidth 800 800
 !
interface FastEthernet5/0
 mpls label protocol ldp
 mpls ip
 ip rsvp bandwidth 800 800
 !
interface FastEthernet5/1
 mpls label protocol ldp
 mpls ip
 ip rsvp bandwidth 800 800
 !

```

Fuente: Autor

Para los equipos de agregación se presentan las configuraciones en la tabla 3-24. De igual forma los parámetros son los mismos para cada uno de los equipos.

Tabla 3-24. Plantilla de configuración MPLS y RSVP-TE equipos AGREGACIÓN

```

CONFIGURACION MPLS / RSVP EQUIPOS AGREGACION
interface FastEthernet0/0
mpls label protocol ldp
mpls ip
ip rsvp bandwidth 800 800
!
interface FastEthernet0/1
mpls label protocol ldp
mpls ip
ip rsvp bandwidth 800 800
!

```

Fuente: Autor

Para comprobar el correcto funcionamiento de MPLS y RSVP-TE en las interfaces de los equipos de la red se verifica con los siguientes comandos ejecutados en uno de los equipos, este caso en GALEREE01:

```

GALEREE01#sh ip rsvp interface
interface  allocated  i/f max  flow max sub max
Fa0/0     0      800K  800K  0
Fa0/1     0      800K  800K  0

```

```

GALEREE01#sh mpls interfaces
Interface      IP      Tunnel Operational
FastEthernet0/0  Yes (ldp) No      Yes
FastEthernet0/1  Yes (ldp) No      Yes

```

Se verifica que se haya construido la tabla con la asignación de etiquetas para cada uno de los flujos de tráfico presentes en el equipo como se indica a continuación.

```

GALEREE01#sh mpls forwarding-table
Local  Outgoing Prefix          Bytes
tag    tag or VC      or Tunnel Id    tag      Outgoing Next Hop
tag    VC            10.10.0.0/30    0 Fa0/0  10.20.0.1
16 Pop tag

```

17	23	10.20.0.28/30	0 Fa0/1	10.20.0.17
18	Pop tag	10.10.0.4/30	0 Fa0/1	10.20.0.17
	Pop tag	10.10.0.4/30	0 Fa0/0	10.20.0.1
19	22	10.20.0.24/30	0 Fa0/1	10.20.0.17
20	17	10.10.0.8/30	0 Fa0/1	10.20.0.17
	16	10.10.0.8/30	0 Fa0/0	10.20.0.1
21	Pop tag	10.20.0.20/30	0 Fa0/1	10.20.0.17
22	Pop tag	10.10.0.12/30	0 Fa0/1	10.20.0.17
23	19	10.20.0.12/30	0 Fa0/0	10.20.0.1
24	18	10.20.0.8/30	0 Fa0/0	10.20.0.1
25	Pop tag	10.20.0.4/30	0 Fa0/0	10.20.0.1
26	29	10.50.30.100/32	0 Fa0/1	10.20.0.17
	29	10.50.30.100/32	0 Fa0/0	10.20.0.1
27	28	10.50.20.100/32	0 Fa0/1	10.20.0.17
	28	10.50.20.100/32	0 Fa0/0	10.20.0.1
28	26	10.50.4.100/32	0 Fa0/1	10.20.0.17
29	Pop tag	10.50.1.100/32	0 Fa0/0	10.20.0.1
30	24	10.50.2.100/32	0 Fa0/0	10.20.0.1
31	Pop tag	10.50.3.100/32	0 Fa0/1	10.20.0.17
32	30	10.50.40.100/32	0 Fa0/1	10.20.0.17
	30	10.50.40.100/32	0 Fa0/0	10.20.0.1

Al ejecutar los comandos de verificación en cada uno de los equipos de la red se constata que se encuentran operativas las configuraciones implementadas para las funcionalidades de MPLS y RSVP-TE.

3.4.5. Planificación para MP-BGP

Dentro de la red de proveedores de servicio se utiliza a BGP (Border Gateway Protocol) como protocolo para transportar servicios. Una configuración de MP-BGP se trata de una extensión del protocolo BGP tradicional, la misma que permite el uso de “Address-Family” en la que se puede implementar diferentes servicios de manera simultánea bajo una misma infraestructura de red del Proveedor de Servicios. Dentro de los servicios que se puede implementar bajo el esquema de MP-BGP están Multicast, IPv4, IPv6, VPLS (Virtual Private LAN Services), L3VPN.

Para el caso de uso dentro de una red de un Proveedor de Servicios se utiliza de manera amplia las L3VPN ya que permite diferenciar a los clientes y a los

servicios que éstos contratan. Como resumen se puede ejemplificar a cada L3VPN como una red virtual asignada a cada cliente para el intercambio/propagación/distribución de rutas para el transporte del tráfico. MP-BGP permite la asignación de atributos (RD - Route Distinguisher y RT - Route Target) con los cuales diferencian el servicio entregado a un cliente de otro. A continuación se presentan en la tabla 3-25 los recursos asignados para la planificación del despliegue de BGP en la red simulada.

Tabla 3-25. Recursos asignados para BGP

SITIO	Nombre del Equipo	IP de Sistema Equipo	Sistema Autónomo (AS)	BGP router-id
SP_A	GALSRAP01	10.50.1.100	65100	10.50.1.100
SP_B	GALSRBP02	10.50.2.100	65100	10.50.2.100
SP_C	GALSRCP03	10.50.3.100	65100	10.50.3.100
SP_D	GALSRDP04	10.50.4.100	65100	10.50.4.100
SP_E	GALEREE01	10.50.10.100	65100	10.50.10.100
SP_F	GALERFE02	10.50.20.100	65100	10.50.20.100
SP_G	GALERGE03	10.50.30.100	65100	10.60.30.100
SP_H	GALERHE04	10.50.40.100	65100	10.60.40.100

Fuente: Autor

Para la configuración de BGP se debe definir el número de AS (Autonomous System) el cual es un atributo que permite identificar todos los equipos que se encuentran bajo una misma unidad administrativa, es decir, todos los equipos que

se encuentran bajo un mismo dominio de una red de un Proveedor de Servicios tendrá asignado el mismo AS. Se ha asignado el número 65100 para el AS de la red a simular.

El identificador del equipo dentro de BGP se ha definido que sea la dirección del sistema que posee cada equipo con el fin de llevar un esquema homologado que permita una rápida asignación e identificación en el caso de que se presente algún problema en la red. El identificador de cada equipo para BGP debe ser único dentro del dominio en el que se trabaja (AS), por lo que al asignar la misma dirección del sistema que posee el equipo se asegura este requerimiento.

Con el fin de que funcione correctamente las L3VPN asignadas a cada uno de los servicios de los clientes dentro de la red, es necesario que dentro del dominio BGP existan sesiones habilitadas entre todos los equipos que conforman el Sistema Autónomo, es decir, se requiere un full-mesh de sesiones BGP internas para la propagación de rutas. Se utilizará el método de RR (Route Reflector) con el fin de que dos de los equipos de altas prestaciones que se encuentran en el CORE (GALSRAP01 y GALSRBP02) de la red, sean los responsables de habilitar las sesiones BGP internas con todos los equipos de la red y que repliquen las rutas para tener una total conectividad. Con estas consideraciones se asegura que en cada uno de los sitios de la red a implementar se podrá configurar la L3VPN asignada a un cliente y que tenga la conectividad con el resto de sitios en donde el cliente tenga presencia con su L3VPN asignada. Las configuraciones a aplicar a los equipos que operan como Reflectores de Rutas se indican en la tabla 3-26:

Tabla 3-26. Plantilla de configuración BGP equipos RR

CONFIGURACION BGP EQUIPOS RR
router bgp 65100 bgp router-id 10.50.1.100 no bgp default ipv4-unicast bgp log-neighbor-changes neighbor ibgp-peer-group peer-group neighbor ibgp-peer-group remote-as 65100 neighbor ibgp-peer-group update-source Loopback10 neighbor ibgp-peer-group description ###iBGP Clientes### neighbor 10.50.3.100 peer-group ibgp-peer-group

```

neighbor 10.50.4.100 peer-group ibgp-peer-group
neighbor 10.50.10.100 peer-group ibgp-peer-group
neighbor 10.50.20.100 peer-group ibgp-peer-group
neighbor 10.50.30.100 peer-group ibgp-peer-group
neighbor 10.50.40.100 peer-group ibgp-peer-group
neighbor ibgp-RR peer-group
neighbor ibgp-RR remote-as 65100
neighbor ibgp-RR update-source Loopback10
neighbor ibgp-RR description ###iBGP RouteReflector###
neighbor 10.50.2.100 peer-group ibgp-RR
!
address-family vpnv4
neighbor ibgp-peer-group send-community both
neighbor ibgp-peer-group route-reflector-client
neighbor ibgp-RR send-community both
neighbor 10.50.2.100 activate
neighbor 10.50.3.100 activate
neighbor 10.50.4.100 activate
neighbor 10.50.10.100 activate
neighbor 10.50.20.100 activate
neighbor 10.50.30.100 activate
neighbor 10.50.40.100 activate
exit-address-family
!

```

Fuente: Autor

Para el caso del segundo equipo RR se modifica únicamente el bgp router-id y la dirección del vecino para formar parte del grupo de RRs. Para el caso del resto de equipamiento de red se utiliza la siguiente configuración para BGP, teniendo en consideración que la configuración difiere únicamente en el bgp router-id ya que los vecinos se mantienen. Se indican las configuraciones en la tabla 3-27.

Tabla 3-27. Plantilla de configuración BGP para la red

CONFIGURACION BGP EQUIPOS DE RED
<pre> router bgp 65100 bgp router-id 10.50.3.100 no bgp default ipv4-unicast bgp log-neighbor-changes neighbor ibgp-peer-group peer-group neighbor ibgp-peer-group remote-as 65100 neighbor ibgp-peer-group update-source Loopback10 neighbor ibgp-peer-group description ###iBGP Clientes### </pre>

```

neighbor 10.50.1.100 peer-group ibgp-peer-group
neighbor 10.50.2.100 peer-group ibgp-peer-group
!
address-family vpnv4
neighbor ibgp-peer-group send-community both
neighbor 10.50.1.100 activate
neighbor 10.50.2.100 activate
exit-address-family
!

```

Fuente: Autor

Para verificar que las configuraciones de BGP para cada uno de los equipos Reflectores de Ruta hayan sido ejecutadas de manera correcta se procede con la verificación ejecutando el siguiente comando.

```

GALSRAP01#sh bgp all summary
For address family: VPNv4 Unicast
BGP router identifier 10.50.1.100, local AS number 65100
BGP table version is 10, main routing table version 10

```

Neighbor	V	AS	MsgR cvd	MsgSent	TblVer	In Q	Out t Q	Up/Down	State/Pfx Rcd
10.50.2.100	4	65100	11	13	10	0	0	0:06:16	0
10.50.3.100	4	65100	8	13	10	0	0	0:06:13	0
10.50.4.100	4	65100	8	13	10	0	0	0:06:16	0
10.50.10.100	4	65100	13	13	10	0	0	0:06:23	0
10.50.20.100	4	65100	7	13	10	0	0	0:06:16	0
10.50.30.100	4	65100	8	13	10	0	0	0:05:59	0
10.50.40.100	4	65100	7	13	10	0	0	0:06:15	0

Se observa que se mantienen las sesiones BGP habilitadas con los 7 equipos restantes de la red dentro del Sistema Autónomo definido (65100). En la última columna se indica un “0” el cual hace referencia a que no existen prefijos que actualmente se anuncien por la red del proveedor de servicios ya que no existen servicios aún configurados.

3.4.6. Planificación para Servicios del Cliente

La red simulada en un ambiente controlado se encuentra apta para la configuración de los servicios con el fin de brindar al cliente final la posibilidad

de solicitar el transporte de su tráfico a través del Proveedor de Servicios. Como planteamiento inicial se brindará una solución de ingeniería/diseño para el cliente en el cual se ofrezcan los diferentes servicios contratados con el uso de L3VPN, las mismas que operan como una “address-family” dentro de MP-BGP, ya que se trata de la manera convencional que se utiliza para brindar servicios.

Al momento de utilizar una L3VPN para el servicio del cliente final se requiere una interacción de las redes del Proveedor de Servicio con la red del cliente final. La interacción consiste básicamente en el intercambio de rutas del cliente para que éstas sean propagadas a través de toda la red del Proveedor de Servicio con el fin de brindar la conectividad entre los diferentes sitios que requiera el cliente. El intercambio de rutas se puede ejecutar de manera manual mediante la inserción de rutas estáticas, o mediante el uso de un protocolo de enrutamiento en el que participarían el equipo del cliente con el del Proveedor de Servicios en base a un acuerdo previo.

Los requerimientos al momento de plantear la ingeniería a detalle para la solución brindada al cliente varían en función a las necesidades planteadas por el usuario en base a la conectividad solicitada para el flujo del tráfico requerido. Para la simulación de los servicios sobre la red del Proveedor de Servicios se utilizarán dos casos de uso comunes en los cuales en el primer caso de uso el cliente solicita la asignación de todo el puerto para la conectividad a nivel de capa 3 con la red del Proveedor de Servicios, mientras que el segundo caso de uso el cliente solicita la asignación de varios servicios diferenciados a través del mismo puerto físico de la red del Proveedor de Servicios.

3.4.6.1. Servicio 1: Conectividad entre dos sitios mediante una L3VPN

Para el caso de estudio que se plantea, la conectividad a nivel de capa 3 entre las redes del cliente y la del Proveedor de Servicios, implica que se utilizará un único puerto físico para la asignación del servicio, el mismo que se configurará con un direccionamiento asignado, mediante el cual se levantarán los protocolos de

enrutamiento definidos para el intercambio de rutas entre los equipos del cliente y del Proveedor de Servicios.

Debido a que el tráfico que curse el cliente a través del servicio brindado debe mantenerse aislado del resto de tráfico que fluye por la red del Proveedor de Servicios, se asigna una L3VPN sobre la cual se transportarán los prefijos del cliente y se brindará la conectividad solicitada.

La ingeniería demanda la asignación ordenada de los recursos sobre la red del Proveedor, debido a que permite mantener un esquema escalable para cuando se empiecen a brindar más servicios de este tipo para otros clientes, manteniendo así la autonomía de sus conexiones. Para definir una L3VPN se asignan los parámetros de RD y RT, los cuales permiten hacer únicos los prefijos del cliente en toda la red del Proveedor de Servicios y definir la importación/exportación que se manejará en los distintos sitios de presencia en los cuales se deba brindar el servicio respectivamente.

Para el escenario planteado se define que los equipos que participarán en este modelo, por parte del Proveedor de Servicios serán el GALEREE01 y el GALERGE03, el servicio se brindará entre los sitios SP_E y SP_G por lo que la asignación de los recursos para los sitios definidos se precisa en la tabla 3-28:

Tabla 3-28. Recursos asignados para Servicio1 Cliente_A en equipos del Proveedor

	GALEREE01	GALERGE03
	vrf ClienteA	vrf ClienteA
RD	65100:100	65100:100
RT	65100:100	65100:100
red	192.168.100.0	172.16.100.0
mascara	255.255.255.252	255.255.255.252
IP SP	192.168.100.1	172.16.100.1
IP Cliente	192.168.100.2	172.16.100.2
Puerto SP	Fa1/0	Fa1/0

Fuente: Autor

Como equipo de acceso para el lado del cliente se utilizará un CISCO 2961, que cuenta con las características indicadas en la figura 3.3. Ya que este equipo cuenta con 3 interfaces, una se utilizará para la conexión WAN hacia el equipo del Proveedor de Servicios para conectividad mediante OSPF (Open Shortest Path First) y las otras dos para la conexión a redes internas del cliente. La asignación de los recursos para los equipos del cliente en cada sitio se indica en la tabla 3-29:

Tabla 3-29. Recursos asignados para Servicio1 Cliente_A en equipos del Cliente

	CLIENTE_A_2	CLIENTE_A_1
	Protocolo OSPF 100	Protocolo OSPF 100
Interfaces OSPF	Fa0/0 Fa0/1 Fa1/0	Fa0/0 Fa0/1 Fa1/0
Area OSPF	0	0
Red Fa0/0	192.168.101.0/24	172.16.101.0/24
Red Fa0/1	192.168.102.0/24	172.16.102.0/24
Red Fa1/0	192.168.100.0/30	172.16.100.0/30
Redistribución en OSPF	Conectadas Estáticas	Conectadas Estáticas

Fuente: Autor

Con los recursos asignados se plantea el diseño de la ingeniería que se va a aplicar para el servicio del cliente, misma que se indica en la figura 3.9:



Figura 3. 9: Ingeniería del cliente – Servicio 1

Fuente: Autor

Con las consideraciones planteadas en la ingeniería asignada al primer servicio para el cliente, y con los recursos asignados para proporcionar la conectividad a través de la red del Proveedor de Servicios, se procede a configurar los equipos

con los parámetros asignados. La configuración se la realiza en los equipos del cliente y del Proveedor de Servicios, con el fin de realizar la propagación de las rutas y permitir el flujo del tráfico del cliente desde el SP_E hacia el SP_G y viceversa.

Para el caso del Proveedor de servicios, se utiliza la configuración de la tabla 3-30 en las interfaces asignadas para el equipo GALEREE01, en el caso del equipo GALERGE03 se utiliza la misma configuración pero con el direccionamiento asignado en las interfaces según la ingeniería antes indicada:

Tabla 3-30. Configuración Servicio1 en red del Proveedor

CONFIGURACION SERVICIO 1 GALEREE01
<pre>ip vrf ClienteA rd 65100:100 route-target export 65100:100 route-target import 65100:100 ! interface FastEthernet1/0 description ###Interfaz ClienteA### ip vrf forwarding ClienteA ip address 192.168.100.1 255.255.255.252 ip ospf network point-to-point ip ospf cost 100 ip ospf mtu-ignore ip ospf 100 area 0 duplex auto speed auto no shutdown ! router bgp 65100 address-family ipv4 vrf ClienteA redistribute connected redistribute static redistribute ospf 100 vrf ClienteA metric 100 match external 1 external 2 no synchronization exit-address-family ! router ospf 100 vrf ClienteA log-adjacency-changes redistribute connected subnets redistribute bgp 65100 metric 100 subnets</pre>

```

network 192.168.100.0 0.0.0.3 area 0
!
ip route vrf ClienteA 192.168.101.0 255.255.255.0 FastEthernet1/0 192.168.100.2
ip route vrf ClienteA 192.168.102.0 255.255.255.0 FastEthernet1/0 192.168.100.2
!

```

Fuente: Autor

Del lado de los equipos del cliente la configuración que se requiere es básica, ya que únicamente se configurará el direccionamiento en las interfaces indicadas, mismas que participarán en el proceso de enrutamiento dinámico OSPF. No se requiere configuraciones adicionales para la conectividad entre las redes asignadas en las dos localidades SP_E y SP_G. Las configuraciones de la tabla 3-31 hacen referencia al equipo Cliente_A_1, el cual se encuentra en el sitio SP_G, para las configuraciones en el equipo Cliente_A_2 se replican los mismos pasos con el direccionamiento asignado para la localidad SP_E:

Tabla 3-31. Configuración Servicio 1 en equipos del Cliente

CONFIGURACION SERVICIO 1 CLIENTE_A_1
<pre> hostname CLIENTE_A_1 ! interface FastEthernet0/0 ip address 172.16.101.1 255.255.255.0 ip ospf 100 area 1 ip ospf network point-to-point ip ospf cost 100 ip ospf mtu-ignore no shutdown ! interface FastEthernet0/1 ip address 172.16.102.1 255.255.255.0 ip ospf 100 area 2 ip ospf network point-to-point ip ospf cost 100 ip ospf mtu-ignore no shutdown ! interface FastEthernet1/0 description ###Interfaz 1 SP### ip address 172.16.100.2 255.255.255.252 ip ospf network point-to-point ip ospf cost 100 </pre>

```

ip ospf mtu-ignore
ip ospf 100 area 0
duplex auto
speed auto
no shutdown
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
redistribute bgp 65100 metric 100 subnets
network 172.16.100.0 0.0.0.3 area 0
network 172.16.101.0 0.0.0.255 area 1
network 172.16.102.0 0.0.0.255 area 2
!

```

Fuente: Autor

Una vez aplicadas las configuraciones sobre el equipamiento asignado para brindar el servicio, se procede con la comprobación de la operatividad de los protocolos y de la conectividad de las redes del cliente entre los dos sitios. Como primer paso se verifica que se establezcan de manera satisfactoria las vecindades a nivel del protocolo OSPF entre el cliente y el Proveedor de Servicios.

Para el equipamiento del Proveedor de Servicios:

```
GALEREE01#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.102.1	0	FULL/ -	00:00:28	192.168.100.2	FastEthernet1/0

```
GALERGE03#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.102.1	0	FULL/ -	00:00:39	172.16.100.2	FastEthernet1/0

Para el equipamiento del cliente:

```
CLIENTE_A_2#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.100.1	0	FULL/ -	00:00:34	192.168.100.1	FastEthernet1/0

```
CLIENTE_A_1#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.100.1	0	FULL/ -	00:00:39	172.16.100.1	FastEthernet1/0

Se procede a verificar que en la tabla de enrutamiento del cliente se establezcan las rutas para alcanzar las redes de cada una de las localidades:

```
CLIENTE_A_1#sh ip route ospf
```

```
O E2 192.168.102.0/24 [110/100] via 172.16.100.1, 00:21:48, FastEthernet1/0
    192.168.100.0/30 is subnetted, 1 subnets
O IA  192.168.100.0 [110/200] via 172.16.100.1, 00:21:53, FastEthernet1/0
O E2 192.168.101.0/24 [110/100] via 172.16.100.1, 00:21:48, FastEthernet1/0
```

```
CLIENTE_A_2#sh ip route ospf
```

```
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O IA 172.16.100.0/30 [110/200] via 192.168.100.1, 00:21:36, FastEthernet1/0
O E2 172.16.101.0/24 [110/100] via 192.168.100.1, 00:21:36, FastEthernet1/0
O E2 172.16.102.0/24 [110/100] via 192.168.100.1, 00:21:36, FastEthernet1/0
```

En los equipos del Proveedor de Servicios se verifica la tabla de enrutamiento asignada al servicio, es decir, la tabla de enrutamiento de la vrf ClienteA:

```
GALEREE01#sh ip route vrf ClienteA
```

```
172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
B   172.16.100.0/30 [200/0] via 10.50.30.100, 00:33:56
B   172.16.101.0/24 [200/0] via 10.50.30.100, 00:33:56
B   172.16.102.0/24 [200/0] via 10.50.30.100, 00:33:56
S   192.168.102.0/24 [1/0] via 192.168.100.2, FastEthernet1/0
    192.168.100.0/30 is subnetted, 1 subnets
C   192.168.100.0 is directly connected, FastEthernet1/0
S   192.168.101.0/24 [1/0] via 192.168.100.2, FastEthernet1/0
```

```
GALERGE03#sh ip route vrf ClienteA
```

172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks

C 172.16.100.0/30 is directly connected, FastEthernet1/0

S 172.16.101.0/24 [1/0] via 172.16.100.2, FastEthernet1/0

S 172.16.102.0/24 [1/0] via 172.16.100.2, FastEthernet1/0

B 192.168.102.0/24 [200/0] via 10.50.10.100, 00:27:52

192.168.100.0/30 is subnetted, 1 subnets

B 192.168.100.0 [200/0] via 10.50.10.100, 00:27:52

B 192.168.101.0/24 [200/0] via 10.50.10.100, 00:27:52

En la red del Proveedor de Servicios es imperativo que se distribuyan las rutas del cliente utilizando BGP bajo el concepto del uso de una L3VPN, por lo que al verificar el número de prefijos que actualmente cursan la red, se confirma que ya no son cero como antes de la implementación del servicio:

GALSRAP01#sh bgp all summary

For address family: VPNv4 Unicast

BGP router identifier 10.50.1.100, local AS number 65100

BGP table version is 13, main routing table version 13

6 network entries using 936 bytes of memory

12 path entries using 816 bytes of memory

4/3 BGP path/bestpath attribute entries using 672 bytes of memory

2 BGP rinfo entries using 48 bytes of memory

3 BGP extended community entries using 104 bytes of memory

0 BGP route-map cache entries using 0 bytes of memory

0 BGP filter-list cache entries using 0 bytes of memory

Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory

BGP using 2608 total bytes of memory

BGP activity 6/0 prefixes, 18/6 paths, scan interval 15 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
State/PfxRcd								
10.50.2.100	4	65100	43	43	13	0	0 00:37:06	6
10.50.3.100	4	65100	57	63	13	0	0 00:42:10	0

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
10.50.4.100	4	65100	57	63	13	0	0	00:42:17 0
10.50.10.100	4	65100	59	61	13	0	0	00:42:18 3
10.50.20.100	4	65100	38	63	13	0	0	00:42:17 0
10.50.30.100	4	65100	58	61	13	0	0	00:42:02 3
10.50.40.100	4	65100	38	63	13	0	0	00:42:19 0

Como indica la salida expuesta, el propagar rutas de clientes por la red del Proveedor de Servicios conlleva la utilización de recursos en los equipos para los cuales se tiene configurados los servicios.

Para validar la operatividad de las configuraciones y de las comprobaciones de rutas antes mencionadas, se procede a realizar pruebas de ping entre las diferentes redes desde los equipos del cliente. De esta manera se valida la conectividad de las redes del cliente en las localidades SP_E y SP_G:

```
CLIENTE_A_1#ping 192.168.100.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/82/108 ms
```

```
CLIENTE_A_1#ping 192.168.101.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.101.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/89/96 ms
```

```
CLIENTE_A_1#ping 192.168.102.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.102.1, timeout is 2 seconds:
```


!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/86/136 ms

Finalmente se tiene el servicio operativo entre los puntos SP_E y SP_G, según el planteamiento de la ingeniería para el servicio del cliente.

3.4.6.2. Servicio 2: Conectividad entre dos sitios mediante varias L3VPN

A diferencia del Servicio 1, en el que la conectividad entre el equipamiento del cliente hacia la red del Proveedor de Servicios se la realizaba utilizando un puerto físico sobre el cual se pasaba un único servicio, en el Servicio 2 se pretende pasar varios servicios que contrate el cliente a través del mismo puerto físico, estos servicios pueden ser separados mediante el uso de VLAN y de sub-interfaces en cada uno de los equipos con el fin de simular diferentes conexiones virtuales mediante el uso de un mismo recurso físico a nivel de equipamiento.

En el escenario 2 planteado se define que los equipos que participarán del lado del Proveedor de Servicios serán el GALERFE02 y el GALERHE04, por lo que el servicio será brindado entre los sitios SP_F y SP_H de la topología planteada. A través del enlace físico que se habilitará entre el cliente y el Proveedor, se habilitarán 3 servicios que serán diferenciados a través de sub-interfaces y VLAN, para la propagación de las rutas entre los distintos sitios se utilizarán 3 L3VPN (una para cada servicio) del lado del Proveedor de Servicios y rutas estáticas del lado del equipamiento del cliente. Los recursos asignados se detallan en las tablas 3-32 y 3-33:

Tabla 3-32. Recursos asignados Servicio 2 para GALERFE02

	GALERFE02		
	vrf ClienteB_1	vrf ClienteB_2	vrf ClienteB_3
RD	65100:200	65100:300	65100:400
RT	65100:200	65100:300	65100:400
red	192.168.220.0	192.168.230.0	192.168.240.0
mascara	255.255.255.252	255.255.255.252	255.255.255.252
IP SP	192.168.220.1	192.168.230.1	192.168.240.1
IP Cliente	192.168.220.2	192.168.230.2	192.168.240.2
Puerto SP	Fa1/0.200	Fa1/0.300	Fa1/0.400

Fuente: Autor

Tabla 3-33. Recursos asignados Servicio 2 para GALERHE04

	GALERHE04		
	vrf ClienteB_1	vrf ClienteB_2	vrf ClienteB_3
RD	65100:200	65100:300	65100:400
RT	65100:200	65100:300	65100:400
red	172.16.220.0	172.16.230.0	172.16.240.0
mascara	255.255.255.252	255.255.255.252	255.255.255.252
IP SP	172.16.220.1	172.16.230.1	172.16.240.1
IP Cliente	172.16.220.2	172.16.230.2	172.16.240.2
Puerto SP	Fa1/0.200	Fa1/0.300	Fa1/0.400

Fuente: Autor

Como equipo de Acceso para el lado del cliente se utilizará un CISCO 2961 que cuenta con las características indicada en la figura 3.3. En la interface utilizada para la conexión hacia el Proveedor de Servicios se configurarán 3 sub-interfaces, cada una con su respectivo direccionamiento. La asignación de los recursos para los equipos del cliente en cada sitio se indica en la tabla 3-34:

Tabla 3-34. Recursos asignados Servicio 2 para equipos del Cliente

	CLIENTE_B_2	CLIENTE_B_1
	Rutas estáticas	Rutas estáticas
Inteface Servicio_B_1	Fa1/0.200	Fa1/0.200
Direccionamiento Servicio_B_1	192.168.220.0/30	172.16.220.0/30
Inteface Servicio_B_2	Fa1/0.300	Fa1/0.300
Direccionamiento Servicio_B_2	192.168.230.0/30	172.16.230.0/30
Inteface Servicio_B_3	Fa1/0.400	Fa1/0.400
Direccionamiento Servicio_B_3	192.168.240.0	172.16.240.0

Fuente: Autor

Con los recursos asignados se plantea el diseño de la ingeniería que se va a aplicar para el servicio del cliente, misma que se indica en la figura 3.10:

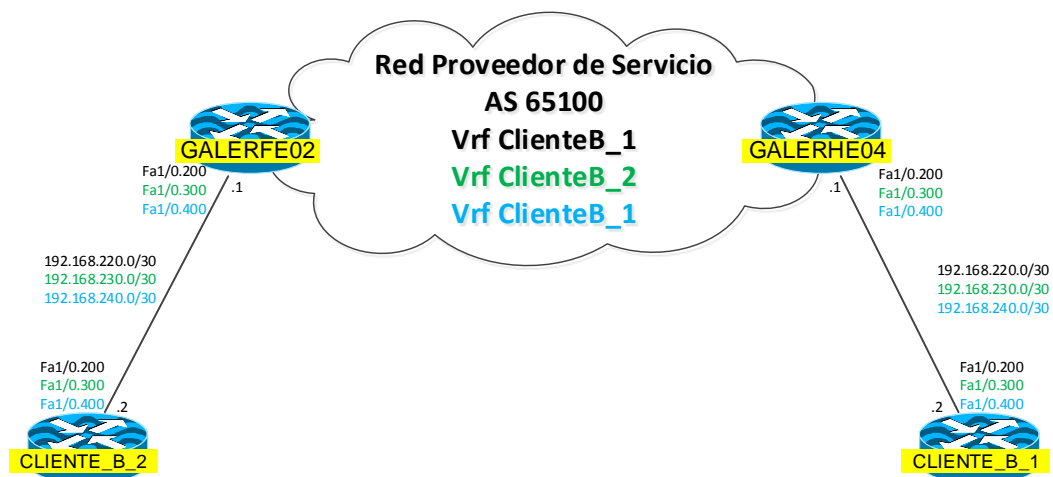


Figura 3. 10: Ingeniería del cliente – Servicio 2

Fuente: Autor

Con las consideraciones planteadas se procede a configurar los equipos con los parámetros asignados. La configuración se la realiza en los equipos del cliente y del Proveedor de Servicios.

Para el caso del Proveedor de servicios se utiliza la configuración de la tabla 3-35 en la interfaz asignada para el equipo GALERFE02, en el caso del equipo GALERHE04, se utiliza la misma configuración pero con el direccionamiento asignado en las interfaces según la ingeniería antes indicada:

Tabla 3-35. Configuración Servicio 2 en red del Proveedor

CONFIGURACION SERVICIO 2 GALERFE02
ip vrf ClienteB_1
rd 65100:200
route-target export 65100:200
route-target import 65100:200
!
ip vrf ClienteB_2
rd 65100:300
route-target export 65100:300
route-target import 65100:300
!
ip vrf ClienteB_3
rd 65100:400

```

route-target export 65100:400
route-target import 65100:400
!
interface FastEthernet1/0
description ###Interfaz ClienteB###
no ip address
duplex auto
speed auto
!
interface FastEthernet1/0.200
description ###Interfaz ClienteB_1###
encapsulation dot1Q 200
ip vrf forwarding ClienteB_1
ip address 192.168.220.1 255.255.255.252
!
interface FastEthernet1/0.300
description ###Interfaz ClienteB_2###
encapsulation dot1Q 300
ip vrf forwarding ClienteB_2
ip address 192.168.230.1 255.255.255.252
!
interface FastEthernet1/0.400
description ###Interfaz ClienteB_3###
encapsulation dot1Q 400
ip vrf forwarding ClienteB_3
ip address 192.168.240.1 255.255.255.252
!
router bgp 65100
address-family ipv4 vrf ClienteB_1
redistribute connected
redistribute static
exit-address-family
!
address-family ipv4 vrf ClienteB_2
redistribute connected
redistribute static
exit-address-family
!
address-family ipv4 vrf ClienteB_3
redistribute connected
redistribute static
exit-address-family
!

```

Fuente: Autor

En los equipos del cliente se configura de la misma manera las sub-interfaces con los recursos asignados. Se toma como ejemplo la configuración del equipo Cliente_B_2 indicada en la tabla 3-36. La configuración del equipo Cliente_B_1 es idéntica, tomando en cuenta que se cuenta con un direccionamiento diferente.

Tabla 3-36. Configuración Servicio 2 en red del Cliente

CONFIGURACION SERVICIO 2 CLIENTE_B_2
<pre> hostname CLIENTE_B_2 ! interface FastEthernet1/0 description ###Interfaz SP_H GALERFE02 Fa0/1### no ip address duplex auto speed auto ! interface FastEthernet1/0.200 description ###Interfaz ClienteB_1### encapsulation dot1Q 200 ip address 192.168.220.2 255.255.255.252 ! interface FastEthernet1/0.300 description ###Interfaz ClienteB_2### encapsulation dot1Q 300 ip address 192.168.230.2 255.255.255.252 ! interface FastEthernet1/0.400 description ###Interfaz ClienteB_3### encapsulation dot1Q 400 ip address 192.168.240.2 255.255.255.252 ! ip route 172.16.220.0 255.255.255.252 FastEthernet1/0.200 192.168.220.1 ip route 172.16.230.0 255.255.255.252 FastEthernet1/0.300 192.168.230.1 ip route 172.16.240.0 255.255.255.252 FastEthernet1/0.400 192.168.240.1 </pre>

Fuente: Autor

Una vez implementadas las configuraciones, se procede a verificar que los tres servicios se encuentren operativos y que se encuentren diferenciados a través de las diferentes sub-interfaces creadas. Se utiliza ARP (Address Resolution Protocol) para verificar la correspondencia entre el direccionamiento IP y las

direcciones MAC de las interfaces según los recursos asignados y las configuraciones aplicadas.

En el equipo CLIENTE_B_1 se tienen las siguientes salidas:

```
CLIENTE_B_1#sh ip arp fastEthernet 1/0.200
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.220.1	6	ca0f.0947.001c	ARPA	FastEthernet1/0.200
Internet	172.16.220.2	-	c009.0735.0010	ARPA	FastEthernet1/0.200

```
CLIENTE_B_1#sh ip arp fastEthernet 1/0.300
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.230.2	-	c009.0735.0010	ARPA	FastEthernet1/0.300
Internet	172.16.230.1	10	ca0f.0947.001c	ARPA	FastEthernet1/0.300

```
CLIENTE_B_1#sh ip arp fastEthernet 1/0.400
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	172.16.240.1	10	ca0f.0947.001c	ARPA	FastEthernet1/0.400
Internet	172.16.240.2	-	c009.0735.0010	ARPA	FastEthernet1/0.400

En el equipo Cliente_B_2 se tiene las siguientes salidas, confirmando la correcta configuración del direccionamiento asignado en los dos sitios del cliente:

```
CLIENTE_B_2#sh ip arp fastEthernet 1/0.200
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.220.1	15	ca0e.0938.001c	ARPA	FastEthernet1/0.200
Internet	192.168.220.2	-	c006.0731.0010	ARPA	FastEthernet1/0.200

```
CLIENTE_B_2#sh ip arp fastEthernet 1/0.300
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.230.2	-	c006.0731.0010	ARPA	FastEthernet1/0.300
Internet	192.168.230.1	19	ca0e.0938.001c	ARPA	FastEthernet1/0.300

```
CLIENTE_B_2#sh ip arp fastEthernet 1/0.400
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.240.1	19	ca0e.0938.001c	ARPA	FastEthernet1/0.400
Internet	192.168.240.2	-	c006.0731.0010	ARPA	FastEthernet1/0.400

Una vez verificada la correcta asignación del direccionamiento en las interfaces de cada servicio, se procede a verificar la conectividad extremo – extremo entre los sitios para cada uno de los servicios. Cabe indicar que al ser servicios diferenciados no se debe tener conectividad entre ellos:

Pruebas para servicio Cliente_B_1:

```
CLIENTE_B_1#ping 192.168.220.1 source Fa 1/0.200
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.220.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.220.2

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 68/105/128 ms

```
CLIENTE_B_1#ping 192.168.220.1 source Fa 1/0.300
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.220.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.230.2

.....

Success rate is 0 percent (0/5)

```
CLIENTE_B_1#ping 192.168.220.1 source Fa 1/0.400
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.220.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.240.2

.....

Success rate is 0 percent (0/5)

Pruebas para el servicio Cliente_B_2:

```
CLIENTE_B_1#ping 192.168.230.1 source Fa 1/0.300
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.230.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.230.2

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 120/126/148 ms

CLIENTE_B_1#ping 192.168.230.1 source Fa 1/0.200

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.230.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.220.2

.....

Success rate is 0 percent (0/5)

CLIENTE_B_1#ping 192.168.230.1 source Fa 1/0.400

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.230.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.240.2

.....

Success rate is 0 percent (0/5)

Pruebas para el servicio Cliente_B_3:

CLIENTE_B_1#ping 192.168.240.1 source Fa 1/0.400

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.240.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.240.2

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 88/153/384 ms

CLIENTE_B_1#ping 192.168.240.1 source Fa 1/0.200

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.240.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.220.2

.....

Success rate is **0 percent** (0/5)

CLIENTE_B_1#ping 192.168.240.1 source Fa 1/0.300

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.240.1, timeout is 2 seconds:

Packet sent with a source address of 172.16.230.2

.....

Success rate is **0 percent** (0/5)

Finalmente se tiene los tres servicios operativos entre los puntos SP_F y SP_H según el planteamiento de la ingeniería para el servicio del cliente.

Al tener todos los servicios operativos de los dos clientes en la red del Proveedor de Servicios, se puede verificar el número de prefijos que se empiezan a aprender y a distribuir a lo largo de la red como se muestra a continuación:

GALSRAP01#sh ip bgp all summary

For address family: VPNv4 Unicast

BGP router identifier 10.50.1.100, local AS number 65100

BGP table version is 13, main routing table version 13

12 network entries *using 1872 bytes of memory*

24 path entries *using 1632 bytes of memory*

7/6 BGP path/bestpath attribute entries using 1176 bytes of memory

4 BGP rinfo entries using 96 bytes of memory

6 BGP extended community entries using 176 bytes of memory

0 BGP route-map cache entries using 0 bytes of memory

0 BGP filter-list cache entries using 0 bytes of memory

Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory

BGP using 4984 total bytes of memory

BGP activity 12/0 prefixes, 24/0 paths, scan interval 15 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
State/PfxRcd								
10.50.2.100	4	65100	73	73	13	0	0	01:02:57 12
10.50.3.100	4	65100	64	73	13	0	0	01:02:50 0
10.50.4.100	4	65100	64	73	13	0	0	01:02:58 0
10.50.10.100	4	65100	45	73	13	0	0	01:02:23 3
Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
State/PfxRcd								
10.50.20.100	4	65100	45	73	13	0	0	01:02:30 3
10.50.30.100	4	65100	44	73	13	0	0	01:02:26 3
10.50.40.100	4	65100	73	73	13	0	0	01:02:10 3

Los prefijos que se distribuyen consumen recursos de procesamiento y de memoria en los equipos del Proveedor de Servicios. En el presente proyecto se pretende utilizar servicios CE2.0, en los cuales se extiende el dominio ETHERNET entre las localidades de los clientes con el fin de evitar el intercambio de rutas/enrutamiento hacia el cliente, evitando de esta manera el consumo de memoria en la red y proyectando los servicios que se ofrecen con el nuevo enfoque ETHERNET.

3.5. Planificación para migrar servicios utilizando servicios basados en CE2.0

Dentro de los objetivos del presente trabajo, está el crear un entorno de red simulado bajo un ambiente controlado para recrear una red típica de un Proveedor de Servicios, el cual ha sido cumplido en el numeral 3.4.6. Al realizar la implementación de los servicios para los clientes en los numerales 3.4.6.1 y 3.4.6.2, se evidencia un consumo de memoria y el intercambio de rutas que se experimenta al utilizar L3VPN para cumplir con este objetivo.

Se plantea el uso de servicios EP-Line y EVP-Line descritos en el numeral 2.3.1.2, con el fin de extender el dominio ETHERNET del cliente a través de la red del Proveedor de Servicios para evitar el intercambio de rutas y otorgar la

autonomía total al cliente sobre la administración de su red. Esto quiere decir que la red del Proveedor de Servicios actuará de manera transparente para el cliente simulando una conexión de extremo – extremo entre los sitios solicitados.

Se planteará la ingeniería/diseño para la migración de los dos clientes que actualmente se encuentran simulados en la red del Proveedor de Servicios mediante un esquema EP-Line para el caso del Servicio 1 y de un esquema EVP-Line para el caso del servicio 2.

3.5.1. Migración de Servicio 1 utilizando un esquema EP-Line

El planteamiento de la ingeniería que utiliza el Cliente A para la prestación de su servicio en la red del Proveedor de Servicios se detalla en la figura 3.9, definiendo los puertos físicos que se asignan junto con el direccionamiento y los recursos de la L3VPN utilizada del lado de la red del Proveedor. Bajo el esquema planteado se tiene un consumo de recursos a nivel de memoria y rutas en los equipos del Proveedor, debido a que se tienen que aprender los distintos direccionamientos que el cliente requiere transportar desde un sitio a otro.

Con el fin de evitar el intercambio de direccionamiento IP a través del uso de protocolos de enrutamiento entre el cliente y el Proveedor, y evitando el consumo de recursos del lado de la red del Proveedor, se plantea la extensión del dominio ETHERNET del cliente, utilizando un servicio bajo el esquema EP-Line en el cual la red del Proveedor de Servicios actúa como un cable ante los ojos del cliente.

Al brindar un servicio en capa 2 transparente para el cliente entre los dos sitios de interés, sobre los cuales se va a establecer el transporte del tráfico, se entrega la autonomía total de su red al cliente, ya que no se requiere un protocolo de enrutamiento para comunicarse con el Proveedor e intercambiar rutas hasta el sitio remoto. Este esquema implica que se cambie la ingeniería a detalle del cliente como se indica a continuación en la figura 3.11:

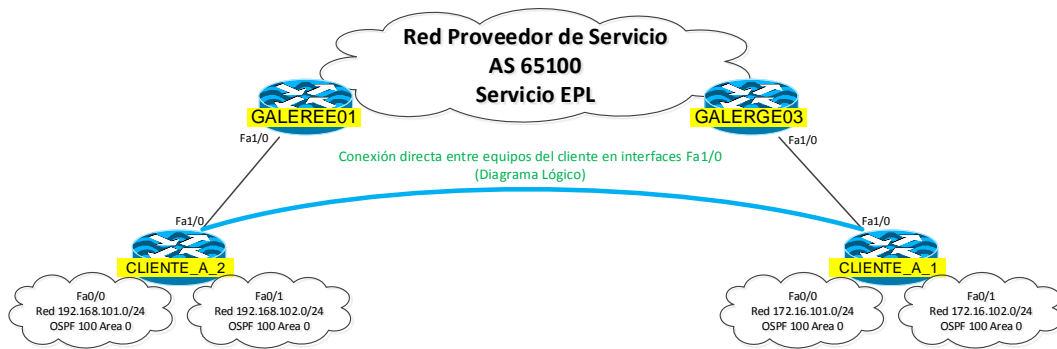


Figura 3. 11: Ingeniería del cliente – Servicio 1 utilizando EP-Line

Fuente: Autor

El diagrama de la ingeniería para el Servicio 1 utilizando el esquema EP-Line muestra que físicamente las conexiones hacia la red del Proveedor de Servicios se mantienen utilizando los enlaces CLIENTE_A_2(Fa1/0-Fa1/0)GALEREE01 y CLIENTE_A_1(Fa1/0-Fa1/0)GALERGE03, pero a un nivel lógico para el cliente se tiene una conexión directa entre CLIENTE_A_2(Fa1/0-Fa1/0)CLIENTE_A_1, pudiendo así hacer uso de este enlace entre los sitios SP_E y SP_G según conveniencia del cliente.

Para el caso puntual del Servicio 1 ofertado, se utilizará para habilitar el protocolo OSPF entre los dos equipos del cliente directamente, sin necesidad de aprender esas rutas en la red del Proveedor para proporcionar la conectividad solicitada. Para la asignación de recursos de las tablas 3-37 y 3-38 se tienen las siguientes variantes debido a que no se asignan direccionamientos en el Proveedor sino en el cliente únicamente:

Tabla 3-37. Recursos asignados para EP-Line Servicio1 en el Proveedor

	GALEREE01	GALERGE03
	Servicio 1	Servicio 1
Host Remoto EP-Line	GALERGE03	GALEREE01
IP sistema remoto	10.50.30.100	10.50.10.100
VC asignado	100	100
Puerto SP	Fa1/0	Fa1/0

Fuente: Autor

Tabla 3-38. Recursos asignados para EP-Line Servicio1 en el Cliente

	CLIENTE_A_2	CLIENTE_A_1
	Protocolo OSPF 100	Protocolo OSPF 100
Interfaces OSPF	Fa0/0 Fa0/1 Fa1/0	Fa0/0 Fa0/1 Fa1/0
Area OSPF	0	0
Red Fa0/0	192.168.101.0/24	172.16.101.0/24
Red Fa0/1	192.168.102.0/24	172.16.102.0/24
Red Fa1/0	192.168.100.0/30	192.168.100.0/30
Redistribución en OSPF	Conectadas Estáticas	Conectadas Estáticas

Fuente: Autor

Del lado de la red del Proveedor ya no se asignan recursos para la creación de una L3VPN y tampoco se asigna direccionamiento ya que no se encarga de aprender rutas, sino que se asigna para cada sitio el nodo remoto con el cual se levantará el servicio en capa 2 EP-Line. Para el caso del cliente se re-asigna el direccionamiento de la interface Fa1/0 del lado del equipo CLIENTE_A_1 ya que al ser la red del Proveedor transparente, mediante una conexión L2, se tiene una conexión directa entre sus dos equipos.

Para el proceso de migración de la ingeniería anterior a la propuesta para el cliente, se tiene que ocasionar una interrupción en el servicio debido a que se borrarán las configuraciones del servicio actual y se configurará con los nuevos recursos asignados. Del lado de la red del Proveedor se tiene las siguientes configuraciones para eliminar los servicios actuales:

```
GALERGE03(config)#no ip vrf ClienteA
% IPv4 addresses from all interfaces in VRF ClienteA have been removed
GALERGE03(config)#!
GALERGE03(config)#default interface FastEthernet1/0
```

*Oct 28 18:49:42.147: %OSPF-5-ADJCHG: Process 100, Nbr 172.16.102.1 on FastEthernet1/0 from FULL to DOWN, Neighbor Down: Interface down or detached

*Oct 28 18:49:42.223: %OSPF-6-PROC_REM_FROM_INT: OSPF process 100 removed from interface FastEthernet1/0

Interface FastEthernet1/0 set to default configuration

GALEREE01(config)#no ip vrf ClienteA

% IPv4 addresses from all interfaces in VRF ClienteA have been removed

GALEREE01(config)#!

GALEREE01(config)#default interface FastEthernet1/0

*Oct 28 18:49:37.835: %OSPF-5-ADJCHG: Process 100, Nbr 192.168.102.1 on FastEthernet1/0 from FULL to DOWN, Neighbor Down: Interface down or detached

*Oct 28 18:49:37.991: %OSPF-6-PROC_REM_FROM_INT: OSPF process 100 removed from interface FastEthernet1/0

Interface FastEthernet1/0 set to default configuration

Una vez eliminadas las configuraciones del servicio del lado del Proveedor, se procede con las configuraciones del lado del cliente. Según los recursos asignados se mantienen el mismo direccionamiento, exceptuando el asignado a la interface Fa1/0 del equipo CLIENTE_A_1 por lo que las configuraciones se indican a continuación:

```
CLIENTE_A_1(config)#int fa 1/0
```

```
CLIENTE_A_1(config-if)#ip address 192.168.100.1 255.255.255.252
```

```
CLIENTE_A_1(config-if)#end
```

Una vez actualizado el direccionamiento del lado del cliente, se procede con las configuraciones del servicio EPL en capa 2 con el fin de proporcionar la conectividad entre los equipos del cliente de los sitios SP_E y SP_G. Las configuraciones se indican a continuación:

```
GALEREE01#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
GALEREE01(config)#interface fastEthernet 1/0
```

```
GALEREE01(config-if)#xconnect 10.50.30.100 100 encapsulation mpls
```

```
GALEREE01(config-if-xconn)#end
```

```
GALERGE03#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
GALERGE03(config)#interface FastEthernet 1/0
```

```
GALERGE03(config-if)#xconnect 10.50.10.100 100 encapsulation mpls
```

```
GALERGE03(config-if-xconn)#end
```

Configurado el servicio, se procede con la verificación de la operatividad del mismo a través de los mensajes de la consola de cada equipo y con los comandos que se indican a continuación:

- Mensajes en la consola de equipos GALEREE01 y GALERGE03

```
GALEREE01#
```

```
*Oct 28 18:59:37.347: %SYS-5-CONFIG_I: Configured from console by console
```

```
GALEREE01#
```

```
*Oct 28 19:00:25.195: %LDP-5-NBRCHG: LDP Neighbor 10.50.30.100:0 (3) is  
UP
```

- Comando para verificar operatividad del servicio EPL creado:

```
GALEREE01#sh mpls l2transport vc
```

Local intf	Local circuit	Dest address	VC ID	Status
-----	-----	-----	-----	-----
Fa1/0	Ethernet	10.50.30.100	100	UP

Del lado del cliente se procede a verificar la conectividad a nivel de ARP, CDP (Cisco Discovery Protocol), ping y de OSPF:

•Pruebas de ARP:

```
CLIENTE_A_1#sh ip arp fastEthernet 1/0
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.100.1	-	c00a.09f9.0010	ARPA	FastEthernet1/0
Internet	192.168.100.2	2	c00b.0a09.0010	ARPA	FastEthernet1/0

•Pruebas de CDP:

```
CLIENTE_A_1#sh cdp neighbors fastEthernet 1/0
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
CLIENTE_A_2	Fas 1/0	130	R S I	2691	Fas 1/0
GALERGE03	Fas 1/0	174	R	7206VXR	Fas 1/0

•Pruebas de OSPF:

```
CLIENTE_A_1#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.102.1	0	FULL/ -	00:00:35	192.168.100.2	FastEthernet1/0

```
CLIENTE_A_1#sh ip route ospf
```

```
O 192.168.102.0/24 [110/200] via 192.168.100.2, 00:03:53, FastEthernet1/0  
O IA 192.168.101.0/24 [110/200] via 192.168.100.2, 00:03:53, FastEthernet1/0
```

```
CLIENTE_A_2#sh ip route ospf
```

```
172.16.0.0/24 is subnetted, 2 subnets  
O 172.16.101.0 [110/200] via 192.168.100.1, 00:04:23, FastEthernet1/0  
O 172.16.102.0 [110/200] via 192.168.100.1, 00:04:23, FastEthernet1/0
```

•Pruebas de ping entre las redes de los dos sitios del cliente:

```
CLIENTE_A_1#ping 192.168.100.2
```


Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 68/86/108 ms

CLIENTE_A_1#ping 192.168.101.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.101.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 84/92/108 ms

CLIENTE_A_1#ping 192.168.102.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.102.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 84/96/120 ms

Una vez ejecutadas todas las pruebas se puede verificar que el servicio ha sido migrado correctamente y se encuentra operativo entre los dos sitios del cliente mediante el uso de un EPL.

3.5.2. Migración de Servicio 2 utilizando un esquema EVP-Line

Para la migración del servicio 2, se plantea la utilización de un servicio bajo el esquema EVP-Line debido a que no se basa en un puerto, sino en diferentes VLAN que diferencian cada uno de los servicios en un único puerto físico. Al igual que en el servicio 1, en esta migración se pretende extender el dominio ETHERNET para cada una de las VLAN en las cuales se transporta los datos del cliente desde un sitio a otro.

El diagrama planteado para la migración del servicio, utilizando un esquema EVP-Line pretende utilizar un único puerto físico en la interconexión de la red del cliente con la red del Proveedor de Servicios, con el fin de configurar tres

diferentes servicios diferenciados por sub-interfaces y con la asignación de una VLAN para cada uno de ellos. La extensión del dominio ETHERNET del cliente le permitirá evitar el uso de direccionamiento estático, ya que tendrá las redes directamente conectadas en la interface de su equipo. A continuación se indica el diagrama de la ingeniería en la figura 3.12 para la migración del servicio 2:

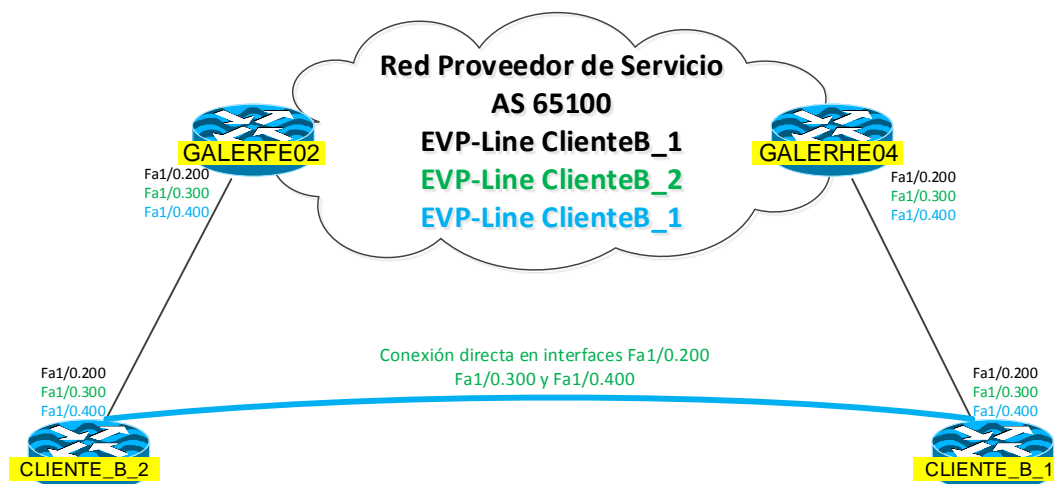


Figura 3. 12: Ingeniería del cliente – Servicio 2 utilizando EVP-Line

Fuente: Autor

Las conexiones físicas que se tienen entre los equipos del cliente y del Proveedor se mantienen, ya que se cambia únicamente a nivel de configuración lógica la migración del servicio. Ya que el Proveedor de servicios es transparente desde el punto de vista del cliente, la re-asignación de recursos se detalla en las tablas 3-39, 3-40 y 3-41:

Tabla 3-39. Recursos asignados para EVP-Line Servicio2 en GALERFE02

	GALERFE02		
	Servicio ClienteB_1	Servicio ClienteB_2	Servicio ClienteB_3
Nombre de equipo	GALERHE04	GALERHE04	GALERHE04
IP Sistema	10.50.40.100	10.50.40.100	10.50.40.100
VC	200	300	400
Puerto SP	Fa1/0.200	Fa1/0.300	Fa1/0.400

Fuente: Autor

Tabla 3-40. Recursos asignados para EVP-Line Servicio2 en GALERHE04

	GALERHE04		
	Servicio ClienteB_1	Servicio ClienteB_2	Servicio ClienteB_3
Nombre de equipo	GALERHE04	GALERHE04	GALERHE04
IP Sistema	10.50.40.100	10.50.40.100	10.50.40.100
VC	200	300	400
Puerto SP	Fa1/0.200	Fa1/0.300	Fa1/0.400

Fuente: Autor

Tabla 3-41. Recursos asignados para EVP-Line Servicio2 en el Cliente

	CLIENTE_B_2	CLIENTE_B_1
	Conexión directa	Conexión directa
Inteface Servicio_B_1	Fa1/0.200	Fa1/0.200
Direccionamiento Servicio_B_1	192.168.220.2/30	192.168.220.1/30
Inteface Servicio_B_2	Fa1/0.300	Fa1/0.300
Direccionamiento Servicio_B_2	192.168.230.2/30	192.168.230.1/30
Inteface Servicio_B_3	Fa1/0.400	Fa1/0.400
Direccionamiento Servicio_B_3	192.168.240.2/30	192.168.240.1/30

Fuente: Autor

La asignación de recursos del lado del Proveedor de Servicios se la realiza para cada uno de los servicios a migrar. Al ser servicios diferenciados se utiliza distintas conexiones y por lo tanto los recursos son diferentes. Para los equipos del cliente se actualiza el direccionamiento para las interfaces Fa1/0.200, Fa1/0.300 y Fa1/0.400 del equipo CLIENTE_B_1.

El proceso de migración implica la eliminación de los servicios L3VPN que actualmente utiliza el cliente, el cambio de direccionamiento de las interfaces en CLIENTE_B_1 según los recursos asignados y la creación de los servicios bajo el esquema EVP-Line. Esta migración implica una afectación en el servicio del cliente. Los comandos a ejecutarse se indican a continuación:

Eliminación de los servicios actuales:

```
GALERFE02(config)#no ip vrf ClienteB_1
% IPv4 addresses from all interfaces in VRF ClienteB_1 have been removed
GALERFE02(config)#no ip vrf ClienteB_2
% IPv4 addresses from all interfaces in VRF ClienteB_2 have been removed
GALERFE02(config)#no ip vrf ClienteB_3
% IPv4 addresses from all interfaces in VRF ClienteB_3 have been removed
GALERFE02(config)#default interface FastEthernet 1/0.200
Interface FastEthernet1/0.200 set to default configuration
GALERFE02(config)#default interface FastEthernet 1/0.300
Interface FastEthernet1/0.300 set to default configuration
GALERFE02(config)#default interface FastEthernet 1/0.400
Interface FastEthernet1/0.400 set to default configuration
```

```
GALERHE04(config)#no ip vrf ClienteB_1
% IPv4 addresses from all interfaces in VRF ClienteB_1 have been removed
GALERHE04(config)#no ip vrf ClienteB_2
% IPv4 addresses from all interfaces in VRF ClienteB_2 have been removed
GALERHE04(config)#no ip vrf ClienteB_3
% IPv4 addresses from all interfaces in VRF ClienteB_3 have been removed
GALERHE04(config)#default interface FastEthernet 1/0.200
Interface FastEthernet1/0.200 set to default configuration
GALERHE04(config)#default interface FastEthernet 1/0.300
Interface FastEthernet1/0.300 set to default configuration
GALERHE04(config)#default interface FastEthernet 1/0.400
Interface FastEthernet1/0.400 set to default configuration
```

Se configura el direccionamiento asignado en los equipos del cliente
CLIENTE_B_1:

```
CLIENTE_B_1(config)#interface FastEthernet 1/0.200
```

```

CLIENTE_B_1(config-subif)# ip address 192.168.220.1 255.255.255.252
CLIENTE_B_1(config-subif)#interface FastEthernet 1/0.300
CLIENTE_B_1(config-subif)# ip address 192.168.230.1 255.255.255.252
CLIENTE_B_1(config-subif)#interface FastEthernet 1/0.400
CLIENTE_B_1(config-subif)# ip address 192.168.240.1 255.255.255.252
CLIENTE_B_1(config-subif)#end

```

Una vez actualizado el direccionamiento del lado del cliente, se procede con las configuraciones del servicio bajo el esquema EVP-Line en capa 2, con el fin de proporcionar la conectividad entre los equipos del cliente de los sitios SP_F y SP_H. Las configuraciones se indican a continuación:

```

GALERFE02(config)#interface fastEthernet 1/0.200
GALERFE02(config-subif)# encapsulation dot1q 200
GALERFE02(config-subif)# xconnect 10.50.40.100 200 encapsulation mpls
GALERFE02(config-subif-xconn)# exit
GALERFE02(config-subif)#interface fastEthernet 1/0.300
GALERFE02(config-subif)# encapsulation dot1q 300
GALERFE02(config-subif)# xconnect 10.50.40.100 300 encapsulation mpls
GALERFE02(config-subif-xconn)# exit
GALERFE02(config-subif)#interface fastEthernet 1/0.400
GALERFE02(config-subif)# encapsulation dot1q 400
GALERFE02(config-subif)# xconnect 10.50.40.100 400 encapsulation mpls
GALERFE02(config-subif-xconn)# exit

```

```

GALERHE04(config)#interface fastEthernet 1/0.200
GALERHE04(config-subif)# encapsulation dot1q 200
GALERHE04(config-subif)# xconnect 10.50.20.100 200 encapsulation mpls
GALERHE04(config-subif-xconn)# exit
GALERHE04(config-subif)#interface fastEthernet 1/0.300
GALERHE04(config-subif)# encapsulation dot1q 300
GALERHE04(config-subif)# xconnect 10.50.20.100 300 encapsulation mpls
GALERHE04(config-subif-xconn)# exit

```

```
GALERHE04(config-subif)#interface fastEthernet 1/0.400
GALERHE04(config-subif)# encapsulation dot1q 400
GALERHE04(config-subif)# xconnect 10.50.20.100 400 encapsulation mpls
GALERHE04(config-subif-xconn)# exit
```

Configurado el servicio se procede con la verificación del mismo a través de los siguientes comandos:

```
GALERFE02#sh mpls l2transport vc
```

Local intf	Local circuit	Dest address	VC ID	Status
Fa1/0.200	Eth VLAN 200	10.50.40.100	200	UP
Fa1/0.300	Eth VLAN 300	10.50.40.100	300	UP
Fa1/0.400	Eth VLAN 400	10.50.40.100	400	UP

Del lado de los equipos del Proveedor de Servicio, se verifica que la configuración bajo el esquema EVP-Line se encuentra operando. Para verificar del lado del cliente se utiliza ARP y ping:

- Pruebas de ARP en el cliente:

```
CLIENTE_B_1#sh ip arp fastEthernet 1/0.200
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.220.1	-	c009.0735.0010	ARPA	FastEthernet1/0.200
Internet	192.168.220.2	0	c006.0731.0010	ARPA	FastEthernet1/0.200

```
CLIENTE_B_1#sh ip arp fastEthernet 1/0.300
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.230.2	0	c006.0731.0010	ARPA	FastEthernet1/0.300
Internet	192.168.230.1	-	c009.0735.0010	ARPA	FastEthernet1/0.300

```
CLIENTE_B_1#sh ip arp fastEthernet 1/0.400
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.240.1	-	c009.0735.0010	ARPA	FastEthernet1/0.400
Internet	192.168.240.2	0	c006.0731.0010	ARPA	FastEthernet1/0.400

- Pruebas de ping en el cliente para cada servicio:

```
CLIENTE_B_1#ping 192.168.220.2 source fastEthernet 1/0.200
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.220.2, timeout is 2 seconds:

Packet sent with a source address of 192.168.220.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 176/197/272 ms

```
CLIENTE_B_1#ping 192.168.230.2 source fastEthernet 1/0.300
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.230.2, timeout is 2 seconds:

Packet sent with a source address of 192.168.230.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 120/132/156 ms

```
CLIENTE_B_1#ping 192.168.240.2 source fastEthernet 1/0.400
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.240.2, timeout is 2 seconds:

Packet sent with a source address of 192.168.240.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 88/134/180 ms

Con las validaciones indicadas, se comprueba la migración exitosa del servicio 2 utilizando un esquema EVP-Line.

Concluido el proceso de migración del segundo servicio utilizando esquemas EP-Line y EVP-Line, se realiza la verificación de la cantidad de rutas que cursan actualmente la red del Proveedor de servicios:

```
GALSRAP01#sh ip bgp all summary
```

For address family: VPNv4 Unicast

BGP router identifier 10.50.1.100, local AS number 65100

BGP table version is 37, main routing table version 37

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.50.2.100	4	65100	180	181	37	0	0	02:43:44	0
10.50.3.100	4	65100	164	191	37	0	0	02:43:39	0
10.50.4.100	4	65100	164	190	37	0	0	02:43:35	0
10.50.10.100	4	65100	187	198	37	0	0	02:43:07	0
10.50.20.100	4	65100	137	192	37	0	0	02:43:22	0
10.50.30.100	4	65100	184	196	37	0	0	02:43:19	0
10.50.40.100	4	65100	136	196	37	0	0	02:42:56	0

La salida de la línea de comandos indica que no existen rutas que cursan actualmente en la red del Proveedor de Servicios, una vez que se han migrado a los clientes optimizando de esta manera los recursos de memoria y de procesamiento de todos los equipos en la red del Proveedor. Cabe indicar que actualmente por limitaciones al momento de la simulación, se recrearon un máximo de 8 equipos por parte del Proveedor y de 2 clientes conectados, pero en el día a día de un Proveedor de Servicios que tenga una cobertura a nivel nacional, se pueden fácilmente superar los 2000 equipos en su red y la cantidad de servicios que se transportan tiene un volumen mucho mayor al de esta simulación, teniendo así un mayor impacto en cuanto a rutas y memoria que se pueden optimizar.

Conclusiones

- Se exponen los conceptos más relevantes que se definen a través del MEF, para los diferentes tipos de servicios estandarizados ETHERNET, presentando una idea completa de sus características, usos y proyección a futuro de los mismos.
- Se realiza su caracterización a nivel teórico y se brinda una perspectiva a futuro de las ventajas de usar este tipo de servicios, ya que se integran de manera óptima con otras tecnologías como SDN, NaaS, NFV, LSO, etc.
- Se detalló un esquema para el diseño, planificación, asignación de recursos y puesta en funcionamiento de una red de un Proveedor de Servicios bajo un entorno simulado, enfatizando en la importancia del manejo y la asignación de recursos disponibles para garantizar un correcto despliegue y escalabilidad de la red. De igual manera se presenta la ingeniería a detalle de los servicios prestados hacia los clientes bajo el esquema de L3VPN en los cuales existe un intercambio de rutas Proveedor-Cliente y por ende un consumo de recursos que pueden ser optimizados.
- La solución presentada en el presente trabajo al implementar servicios CE2.0 para migrar los actuales servicios de los clientes, permite tener un esquema de conexión extremo-a-extremo manteniendo el objetivo del servicio y presentando los recursos y el plan de migración necesario para cada caso de uso expuesto.
- Se cumple con los objetivos específicos planteados en el presente trabajo, permitiendo de la misma manera cumplir el objetivo general, y se demuestra la hipótesis planteada al reducir los recursos de memoria y de rutas que se aprenden del lado de la red del Proveedor, y brindando la autonomía completa al Cliente sobre la administración de su red.

Recomendaciones

- El análisis para la implementación de este tipo de ingenierías para los clientes, mediante el uso de servicios CE2.0 en redes de Proveedores de Servicio con el fin de optimizar los recursos que actualmente poseen en la red.
- Realizar el análisis para casos de usos en los que se pueda aplicar el resto de servicios CE 2.0 (EP-LAN; EVP-LAN; EP-Tree; EVP-Tree; E-Access). El análisis depende de los factores/consideraciones para el flujo del tráfico que cursará por el servicio. Este tipo de análisis puede abarcar no solamente a servicios que se vendan a clientes finales, sino también para diferentes servicios de usuarios internos que cursen por la red del Proveedor.
- Existen varias tecnologías tales como SDN, NaaS, NFV, LSO, etc., que se integran con los servicios CE2.0 y trabajan de forma conjunta para brindar una nueva perspectiva en la prestación/administración de los servicios que cursan por la red de un Proveedor de Servicios. Se recomienda realizar un análisis de la manera en la que estas tecnologías se integran y de los casos de usos que se hayan implementado a nivel mundial.
- MEF exige la certificación de la red de un Proveedor de Servicios para poder garantizar la correcta interoperabilidad de los servicios CE2.0, por lo que se puede realizar un trabajo de investigación en donde se expongan los diferentes parámetros que se requiere para la certificación y las pruebas que se ejecutan sobre la red.

Referencias Bibliográficas

- C. S. (2014). *Cisco CPT Configuration Guide–CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01)*. San Jose, CA.
- C. S. (2015). *Carrier Ethernet Configuration Guide, Cisco IOS Release 15S*. San Jose, CA.
- Cisco Systems Inc. (2013). *Carrier Ethernet 2.0 Certification Understanding and Layer 2 Control Protocol Behaviour Across Cisco Carrier Ethernet Platforms*. San Jose, CA: Cisco Systems Inc.
- GNS3. (26 de Septiembre de 2017). Obtenido de <https://gns3.com/>
- Green, H., Monette, S., Olsson, J., Saltsidis, P., & Takács, A. (2007). *Carrier Ethernet: The native approach*. Ericsson.
- MEF. (2004). *Introduction to Circuit Emulation Services over Ethernet*. Metro Ethernet Forum.
- MEF. (2004). *MEF 11 User Network Interface (UNI) Requirements and Framework*. Metro Ethernet Forum.
- MEF. (2004). *MEF 4 Metro Ethernet Network Architecture Framework - Part 1: Generic Framework*. Metro Ethernet Forum.
- MEF. (2010). *Understanding Carrier Ethernet Throughput*. Metro Ethernet Forum.
- MEF. (2012). *MEF 33 Ethernet Access Services Definition*. Metro Ethernet Forum.
- MEF. (2013). *CE 2.0 Ethernet Access Services*. Metro Ethernet Forum.
- MEF. (2013). *MEF 10.3 Ethernet Services Attributes Phase 3*. Metro Ethernet Forum.
- MEF. (2014). *Carrier Ethernet and SDN Part 1 : An Industry Perspective*. Metro Ethernet Forum.
- MEF. (2014). *Carrier Ethernet and SDN Part 2: Practical Considerations*. Metro Ethernet Forum.
- MEF. (2014). *MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer*. Metro Ethernet Forum.
- MEF. (2014). *MEF 6.2 EVC Ethernet Services Definitions Phase 3*. Metro Ethernet Forum.
- MEF. (2016). *MEF 23.2 Carrier Ethernet Class of Service – Phase 3*. Metro Ethernet Forum.
- MEF. (2016). *MEF 26.2 External Network Network Interfaces (ENNI) and Operator Service Attributes*. Metro Ethernet Forum.
- MEF. (2016). *Understanding Carrier Ethernet Service Assurance Part 1*. Metro Ethernet Forum.
- MEF. (2016). *Understanding Carrier Ethernet Service Assurance Part 2*. Metro Ethernet Forum.
- MEF, & Santitoro, R. (2003). *Ethernet Access Services Definition*. Metro Ethernet Forum.
- MEF, ON.Lab, ONOS, OPEN-O, OpenDaylight(ODL), O. N., . . . T. F. (2016). *An Industry Initiative for Third Generation Network and Services*. Metro Ethernet Forum.

- Mizrahi, T., & Safrai, U. (2015). *Carrier Ethernet 2.0: A Chipmaker's Perspective*. MARVELL.
- Morency, I. (2012). *Carrier Ethernet 2.0 Services, Technical Foundation Document*. Iometrix.
- NTT. (2010). *The Evolution of Ethernet*. NTT Communications.
- Oña, G. (2016). *Diseño y comparación de redes de acceso MPLS y Metro Ethernet integradas a un backbone MPLS para un proveedor de servicios y realización de un prototipo base*. Quito.
- Salcedo, O., Pedraza, L. F., & Espinosa, M. (2012). *Evaluación de redes MPLS/VPN/BGP con rutas reflejadas*. Tecnura.
- Yerushalmi, I., & Mizrahi, T. (2011). *The OAM Jigsaw Puzzle*. MARVELL.

Glosario de Términos

APP (Application, Aplicación)

ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones)

AS (Autonomous System, Sistema Autónomo)

ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrona)

BGP (Border Gateway Protocol, Protocolo de Puerta de Enlace de Borde)

CCM (Connectivity Check Message, Mensaje de Verificación de Conectividad)

CDP (Cisco Discovery Protocol, Protocolo de Descubrimiento de Cisco)

CE (Client Edge, Borde del Cliente)

CE 2.0 (Carrier Ethernet 2.0, Carrier Ethernet 2.0)

CFM (Connectivity Fault Management, Gestión de Fallas de Conectividad)

CoS (Class of Service, Clase de Servicio)

EGP (Exterior Gateway Protocol, Protocolo de Puerta de Enlace Externa)

E-NNI (External Network-Network Interface, Interface Red-Red Externa)

EP (Ethernet Private, Ethernet Privado)

EPL (Ethernet Private Line, Línea Privada Ethernet)

ETH (Ethernet, Ethernet)

EVC (Ethernet Virtual Circuit, Circuito Virtual Ethernet)

EVP (Ethernet Virtual Private, Ethernet Privado Virtual)

EVPL (Ethernet Virtual Private Line, Línea Privada Virtual Ethernet)

Gbps (Giga bits per second, Giga bits por segundo)

IaaS (Infrastructure as a Service, Infraestructura como un Servicio)

IEEE (Institute of Electrical and Electronics Engineers, Instituto de Ingeniería Eléctrica y Electrónica)

IETF (Internet Engineering Task Force, Grupo de Trabajo de Ingeniería de Internet)

IGP (Interior Gateway Protocol, Protocolo de Puerta de Enlace Interna)

IP (Internet Protocol, Protocolo de Internet)

ISIS (Intermediate System to Intermediate System, Sistema Intermedio a Sistema Intermedio)

ITU (International Telecommunication Union, Unión Internacional de Telecomunicaciones)

L3VPN (Layer 3 Virtual Private Network, Red Privada Virtual de Capa 3)

LAN (Local Area Network, Red de Area Local)

LER (Label Edge Router, Router de Etiquetas de Borde)

LSO (Lifecycle Service Orchestration, Orquestación del Ciclo de Vida del Servicio)

LSP (Label Switched Path, Camino de Conmutación de Etiquetas)

LSR (Label Switch Router, Router de Conmutación de Etiquetas)

MA (Maintenance Association, Asociación de Mantenimiento)

MAC (Media Access Control, Control de Acceso al Medio)

MAN (Metropolitan Area Network, Red de Area Metropolitana)

Mbps (Mega bits per second, Mega bits por segundo)

MD (Maintenance Domain, Dominio de Mantenimiento)

MEF (Metro Ethernet Forum, Foro Metro Ethernet)

MEN (Metro Ethernet Network, Red Metro Ethernet)

MEP (Maintenance Endpoints, Puntos finales de Mantenimiento)

MIP (Maintenance Intermediate Points, Puntos Intermedios de Mantenimiento)

MP-BGP (Multi-Protocol Border Gateway Protocol, Protocolo de Puerta de Enlace de Borde - Multi Protocolo)

MPLS (Multi-Protocol Label Switching, Conmutación de Etiquetas Multi-Protocolo)

NaaS (Network as a Service, Red como un Servicio)

NET (Network Entity Title, Título de Entidad de Red)

NFV (Network Function Virtualization, Virtualización de Funciones de Red)

NI-NNI (Network-Interworking Network-Network Interface, Interface Red-Red Interoperación de Red)

OAM (Operations, administration and maintenance , Operación, Administración, Mantenimiento)

OSI (Open System Interconnection, Sistema Abierto de Interconexión)

OSPF (Open Shortest Path First, Primer Camino Más Corto)

OTN (Optical Transport Network, Red de Transporte Optica)

OVC (Operator Virtual Connection, Operador de Conexión Virtual)

P (Provider, Proveedor)

PC (Personal Computer, Computador Personal)

PDH (Plesiochronous Digital Hierarchy, Jerarquía Digital Plesiócrona)

PDU (Protocol Data Unit, Unidad de Protocolo de Datos)

PE (Provider Edge, Borde del Proveedor)

RAM (Random Access Memory, Memoria de Acceso Aleatorio)

RD (Route Distinguisher, Distinguidor de Ruta)

RR (Route Reflector, Reflector de Ruta)

RSVP-TE (Resource Reservation Protocol - Traffic Engineering, Protocolo de Reserva de Recursos - Ingeniería de Tráfico)

RT (Route Target, Objetivo de Ruta)

SDH (Synchronous Digital Hierarchy, Jerarquía Digital Síncrona)

SDN (Software Defined Network, Red Definida por Software)

SI-NNI (Service-Interworking Network-Network Interface, Interface Red-Red Interoperación de Servicio)

SLA (Service Level Agreement, Acuerdo de Nivel de Servicio)

SONET (Synchronous Optical Network, Red Óptica Síncrona)

TDM (Time Division Multiplexing, Multiplexación por División de Tiempo)

TRAN (Transport, Transporte)

UNI (User-Network Interface, Interfae Usuario-Red)

VLAN (Virtual Local Area Network, Red de Area Local Virtual)

VPLS (Virtual Private LAN Services, Servicio de LAN Privada Virtual)

VoIP (Voice over IP, Voz sobre IP)

VPN (Virtual Private Network, Red Privada Virtual)

WAN (Wide Area Network, Red de Area Amplia)

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Geovanny Marcelo Avendaño Castro**, con C.C: # **0105621148** autor/a del trabajo de titulación: **Implementación de servicios “Carrier Ethernet” EP-Line y EVP-Line del estándar MEF sobre la red de transporte MPLS de un Proveedor de Servicios local para la conectividad en capa 2 de clientes finales en un entorno simulado**, previo a la obtención del título de **Magister en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, a los 2 días del mes de febrero año 2018

f. _____

Nombre: Geovanny Marcelo Avendaño Castro

C.C: 0105621148

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Implementación de servicios “Carrier Ethernet” EP-Line y EVP-Line del estándar MEF sobre la red de transporte MPLS de un Proveedor de Servicios local para la conectividad en capa 2 de clientes finales en un entorno simulado		
AUTOR(ES)	Geovanny Marcelo Avendaño Castro		
REVISOR(ES)/TUTOR(ES)	MSc. Orlando Philco Asqui / MSc. Luis Cordova Rivadeneira / MSc. Manuel Romero Paz		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
CARRERA:	Maestría en Telecomunicaciones		
TÍTULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	Guayaquil, 2 de febrero de 2018	No. DE PÁGINAS:	120
ÁREAS TEMÁTICAS:	Protocolo IP, MPLS, Ethernet. Características de Servicios Carrier Ethernet y arquitectura de redes Metro Ethernet. Simulación e implementación de redes de Proveedores de Servicio IP/MPLS con Carrier Ethernet (E-Line)		
PALABRAS CLAVES/KEYWORDS:	IP, MPLS, VPN, Ethernet, Carrier Ethernet, MEF, SDN, NaaS, NFV, LSO		
RESUMEN/ABSTRACT:	<p>El trabajo de tesis a continuación consiste en simular una red de transporte IP/MPLS (Internet Protocol / Multi-Protocol Label Switching) bajo un ambiente controlado de un típico Proveedor de Servicios sobre la cual se va a configurar VPN (Virtual Private Network) de capa 3 como método actual de aprovisionamiento y servicios Carrier Ethernet (E-Line) como nueva tendencia de aprovisionamiento hacia el cliente final, con el objetivo de optimizar los recursos en la red del proveedor y brindar al cliente un servicio en base al nuevo paradigma que se maneja en las redes de comunicación a nivel mundial. Se presentará a manera de introducción un análisis de los servicios Carrier Ethernet así como el despliegue de redes Metro Ethernet para la provisión de estos servicios, indicando las ventajas de Ethernet sobre las tecnologías antecesoras, sus características, funcionalidades, estándares de configuración y estándares de interacción entre redes, siendo el Metro Ethernet Forum MEF el motor de la implementación de estos estándares con la visión a futuro al relacionar tecnologías como SDN (Software Defined Networks), NFV (Network Function Virtualization), LSO (Lifecycle Service Orchestration) que apuntan a brindar este tipo de servicios de red NaaS (Network-as-a-Service).</p>		
ADJUNTO PDF:	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
CONTACTO CON AUTOR/ES:	Teléfono: 0984047439	E-mail: gavendanoc91@gmail.com	
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE)::	Nombre: Manuel de Jesús Romero Paz		
	Teléfono: +593-4-2202935 /0994606932		
	E-mail: manuel.romero@cu.ucsg.edu.ec / mromeropaz@yahoo.com		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			

DIRECCIÓN URL (tesis en la web):	
---	--