Despliegue de una red MPLS L2VPN con equipamiento real

Raúl Naranjo Caballero
Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

José Manuel Castillo Pedrosa

Enero 2023

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	Despliegue de una red MPLS L2VPN con equipamiento real
Nombre del autor:	Raúl Naranjo Caballero
Nombre del consultor:	José Manuel Castillo Pedrosa
Fecha de entrega (mm/aaaa):	01/2023
Área del Trabajo Final:	Administración de redes y sistemas operativos
Titulación:	*Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación*

Resumen del Trabajo (máximo 250 palabras):

Las interconexiones de las distintas sucursales de las empresas están cobrando mayor relevancia dentro del sector de las telecomunicaciones, ya que, durante los últimos años, se han incrementado las compañías que cuentan con sedes ubicadas en diferentes localizaciones.

Esta situación supone para las empresas un gasto económico extra en infraestructura y equipamiento, que en ocasiones no están dispuestos a asumir. Ahora bien, la gran mayoría desean, a bajo coste, que sus conexiones sean fluidas y con baja latencia.

En este contexto, este Trabajo tiene como objetivo conseguir, mediante un escenario con equipamiento real, que una empresa pueda conectar sus equipos mediante circuitos de nivel 2 configurados sobre la red MPLS de un operador de servicios. Para ello, se han configurado varios circuitos EoMPLS (*Ethernet Over MPLS*) para que se pueda simular una conexión *Ethernet* directa entre sus equipos, siendo totalmente transparente la infraestructura del operador de servicios y consiguiendo un enlace de una capacidad determinada.

Para finalizar, se han incorporado varias funcionalidades para dar robustez a la red, de manera que se puedan ofrecer servicios que aporten una alta fiabilidad y disponibilidad para satisfacer las necesidades de los clientes o empresas.

Abstract (in English, 250 words or less):

Within the telecommunications sector, the interconnections of different company branches are becoming more important as companies with headquarters located in different locations have increased in recent years.

This situation means that companies are spending extra money on infrastructure and equipment, which they are sometimes unwilling to take on. However, most companies want their connections to be smooth and with low latency at a low cost.

In this context, the objective of this work is to achieve, by means of a scenario with real equipment, that a company can connect its equipment through level 2 circuits configured over the MPLS network of a service operator. To this end, several EoMPLS (Ethernet Over MPLS) circuits have been configured to simulate a direct Ethernet connection between its equipment, with the service operator's infrastructure being completely transparent and achieving a link of a given capacity.

Finally, several functionalities have been incorporated to give robustness to the network, so that services can be offered that provide high reliability and availability to meet the needs of customers or companies.

Palabras clave (entre 4 y 8):

MPLS, L2VPN, EPL, EVPL, Cisco, SFP, FRR, Traffic Engineering

Índice

Lista de figuras

Lista de tablas

Lista de configuraciones

1. Introducción

1.1 Contexto y justificación del Trabajo

En la actualidad, cada vez son más las empresas que cuentan con sedes ubicadas en diferentes localizaciones, lo que supone para ellas una mayor inversión en recursos económicos para garantizar una óptima interconexión entre las distintas sucursales.

En este escenario, nos podemos encontrar con empresas que, con el fin de reducir gastos, no quieran invertir en infraestructuras ni en equipamiento extra para conectar entre sí las distintas sedes. Pero que, a la vez, no desean renunciar a que sus conexiones sean fluidas y con baja latencia.

Una opción para solventar este problema es la de recurrir a operadores de servicios que ya disponen de un amplio despliegue de red y, a cambio de una cuota de alta y de un alquiler mensual, proporcionan a las empresas conectividad de ancho de banda entre sus sedes mediante circuitos de nivel 2.

Es importante destacar que el alquiler de un circuito a un tercero siempre resultará más económico que una inversión en infraestructura y equipamiento propios, teniendo en cuenta que en muchos casos será difícil de amortizar. Además, si una empresa desea cambiar de ubicación o cerrar una sede, le resultará más sencillo solicitar al operador una modificación del circuito o directamente tramitar la baja que acarrear con los gastos que supone trasladar todo el equipamiento e infraestructura.

En este contexto y con el fin de satisfacer la necesidad de las empresas, se justifica, pues el despliegue de una red MPLS L2VPN de un operador de servicios en la que se crearán circuitos de nivel 2 seguros y de baja latencia entre diferentes puntos para poder conectar los equipos de las distintas sedes.

Es importante tener en cuenta que cuanto más robusta sea la red de estos operadores mejor servicio ofrecerán. Por este motivo, es conveniente que se incorporen funcionalidades que permitan, por ejemplo, intentar reducir al máximo los tiempos de corte en incidencias, poder elegir siempre el mejor camino que toman los circuitos por la red, ofrecer servicios protegidos, etc. En definitiva, que la red aporte alta fiabilidad y disponibilidad para satisfacer las necesidades de los clientes.

1.2 Objetivos del Trabajo

Como se ha comentado en el apartado anterior, el objetivo principal de este Trabajo es poder ofrecer a un cliente de un operador de servicios (o a una empresa) la conexión de sus equipos de telecomunicaciones mediante circuitos de nivel 2 ofrecidos por la red MPLS de un operador de servicios.

De esta manera, el cliente simulará una conexión *ethernet* directa entre sus equipos, siendo totalmente transparente la infraestructura del operador.

Además, se establecen también los siguientes objetivos:

- Configurar y validar diferentes mecanismos de mejora que aporten robustez a la red:
    - *Traffic Engineering* para elegir el camino que los circuitos deben seguir sobre la red MPLS.

    - *Fast Reroute* para proporcionar una rápida recuperación del circuito si falla el camino asignado.

- Configurar un circuito EPL (*Ethernet Private Line*) en la red MPLS. Desde los equipos del cliente que estarán conectados en los extremos, se validará el correcto funcionamiento y la total transparencia de los protocolos de nivel 2 (CDP, STP, etc.).

- Configurar varios circuitos EVPL (*Ethernet Virtual Private Line*) sobre un mismo puerto de entrega de cliente y diferenciándolos con etiquetas VLAN. Posteriormente, se validará el correcto funcionamiento y se estudiará si los circuitos tienen transparencia de los protocolos de nivel 2.

- Configurar y validar circuitos protegidos con dos puertos de entrega, de manera que, si el puerto de entrega principal falla, el servicio pasaría a entregarse por el puerto de *backup* de forma automática.

- Configurar y validar la función *Dying Gasp* en el CPE ubicado en la sede del cliente, de manera que se pueda diferenciar si la caída del equipo es debida a un problema eléctrico o a un problema de la fibra que conecta el CPE con el PE.

- Configurar *policies* en los circuitos limitando el ancho de banda. Se validará mediante pruebas de tráfico (iPerf) que el funcionamiento es correcto.

Hay que destacar que el montaje de toda la red se realizará con equipamiento real.

1.3 Enfoque y método seguido

Como estrategia a seguir, este Trabajo se dividirá en diferentes bloques que se irán implementando en el orden indicado.

Bloque 1
En este primer bloque, se recopilará información para poder implementar desde cero una red MPLS con el fin de configurar servicios EoMPLS (*Ethernet Over MPLS*). En este punto será importante identificar todos los protocolos intervinientes, así como las funcionalidades que se pueden añadir a la red con tal de hacerla lo más robusta posible.

Además, se estudiará el hardware que finalmente se utilizará para el montaje de nuestro escenario real, analizando los pros y los contras de cada uno de ellos:

- Equipamiento PE (*Provider Edge Router*) que formará parte del anillo de la MPLS debe soportar la licencia *Advanced Metro IP Access* para poder configurar los servicios EoMPLS de nivel 2 y todas las mejoras que se introducirán en la red para darle robustez.
- Equipamiento CPE (*Customer Premises Equipment*) y de cliente preferiblemente del mismo proveedor que el resto de los equipos para evitar posibles incompatibilidades.
- Transceptores SFP (*Small Form-factor Pluggable Transceiver*) que se utilizarán para conectar los equipos entre sí a través de los latiguillos de fibra deben ser compatibles con el resto de equipamiento y con los cables (tipo y longitud) que se utilizarán.
- Latiguillos de cobre y de fibra compatibles a los diferentes transceptores SFP que se utilizarán.

Se priorizará la búsqueda de artículos, *datasheets*, foros de usuarios, etc. del proveedor de los equipos que se utilice (Cisco, Raisecom, etc), de manera que aporten una información más precisa a la hora de implementar todo lo que se verá en el resto de los bloques.

Bloque 2:
En este bloque, se hará uso de la información recopilada anteriormente para comenzar con la configuración y explicación paso a paso de la red MPLS.

En primer lugar, se evaluarán los protocolos y funcionalidades que se añadirán y descartarán en la red, ofreciendo una explicación detallada del motivo de la elección o descarte.

En segundo lugar, se comenzarán a incorporar mecanismos de mejora de la red MPLS y se configurará el primer circuito EPL (*Ethernet Private Line*). En este punto es importante analizar y evaluar el orden a seguir en la implementación de las configuraciones, ya que pueden existir dependencias que impidan el correcto funcionamiento.

Además, se realizarán simulaciones de fallo en algunos puntos de la red para poder verificar que todo lo configurado hasta ese momento funciona correctamente. En este punto se revisarán los datos obtenidos de las pruebas realizadas, con y sin los mecanismos de mejora, para realizar una comparativa que determine cómo y cuánto se mejora la red.

Bloque 3:
En este tercer bloque, se explicarán y se configurarán varios servicios EVPL (*Ethernet Virtual Private Line*) para posteriormente validar su correcto funcionamiento. También, se evidenciará la diferencia entre los circuitos EVPL y EPL, de manera de que queden bien reflejadas en el Trabajo las necesidades de usar un servicio u otro.

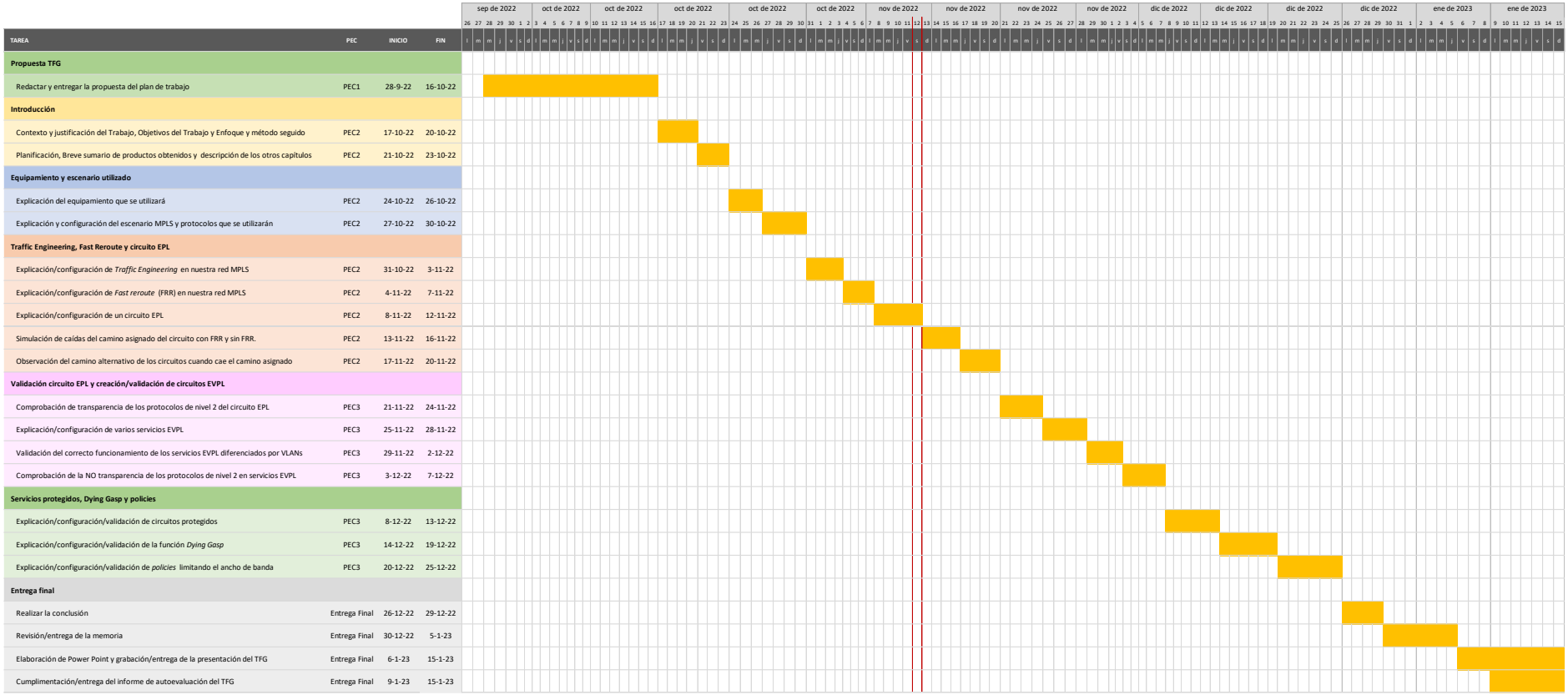
Para finalizar, se realizará una verificación de la transparencia de los protocolos de nivel 2 en los circuitos EPL y EVPL. Adicionalmente, se seleccionarán una serie de protocolos para validarlos directamente desde los equipos del cliente, que estarán conectados a ambos extremos.

Bloque 4
Este bloque está dedicado a otros aspectos de mejora y a remarcar algunas recomendaciones de fabricante que se pueden implementar en la red MPLS. Por lo tanto, se explicarán y se configurarán estas mejoras a través de una demostración en la que se valide de manera clara que funciona correctamente.

1.4 Planificación del Trabajo

Se establece el siguiente plan de Trabajo con una programación semanal de las diferentes tareas que conforman el TFG. Además, se incluyen los hitos parciales de cada una de las PECs:

Despliegue de una red MPLS L2VPN con equipamiento real



TAREA	PEC	INICIO	FIN
Propuesta TFG			
Redactar y entregar la propuesta del plan de trabajo	PEC1	28-9-22	16-10-22
Introducción			
Contexto y justificación del Trabajo, Objetivos del Trabajo y Enfoque y método seguido	PEC2	17-10-22	20-10-22
Planificación, Breve sumario de productos obtenidos y descripción de los otros capítulos	PEC2	21-10-22	23-10-22
Equipamiento y escenario utilizado			
Explicación del equipamiento que se utilizará	PEC2	24-10-22	26-10-22
Explicación y configuración del escenario MPLS y protocolos que se utilizarán	PEC2	27-10-22	30-10-22
Traffic Engineering, Fast Reroute y circuito EPL			
Explicación/configuración de *Traffic Engineering* en nuestra red MPLS	PEC2	31-10-22	3-11-22
Explicación/configuración de *Fast reroute* (FRR) en nuestra red MPLS	PEC2	4-11-22	7-11-22
Explicación/configuración de un circuito EPL	PEC2	8-11-22	12-11-22
Simulación de caídas del camino asignado del circuito con FRR y sin FRR.	PEC2	13-11-22	16-11-22
Observación del camino alternativo de los circuitos cuando cae el camino asignado	PEC2	17-11-22	20-11-22
Validación circuito EPL y creación/validación de circuitos EVPL			
Comprobación de transparencia de los protocolos de nivel 2 del circuito EPL	PEC3	21-11-22	24-11-22
Explicación/configuración de varios servicios EVPL	PEC3	25-11-22	28-11-22
Validación del correcto funcionamiento de los servicios EVPL diferenciados por VLANs	PEC3	29-11-22	2-12-22
Comprobación de la NO transparencia de los protocolos de nivel 2 en servicios EVPL	PEC3	3-12-22	7-12-22
Servicios protegidos, Dying Gasp y policies			
Explicación/configuración/validación de circuitos protegidos	PEC3	8-12-22	13-12-22
Explicación/configuración/validación de la función *Dying Gasp*	PEC3	14-12-22	19-12-22
Explicación/configuración/validación de *policies* limitando el ancho de banda	PEC3	20-12-22	25-12-22
Entrega final			
Realizar la conclusión	Entrega Final	26-12-22	29-12-22
Revisión/entrega de la memoria	Entrega Final	30-12-22	5-1-23
Elaboración de Power Point y grabación/entrega de la presentación del TFG	Entrega Final	6-1-23	15-1-23
Cumplimentación/entrega del informe de autoevaluación del TFG	Entrega Final	9-1-23	15-1-23

1.5 Breve sumario de productos obtenidos

A la finalización de este Trabajo se obtendrá la propuesta de arquitectura de una red MPLS L2VPN con servicios EoMPLS que permita conectar, mediante circuitos de nivel 2, los equipos de un cliente de un operador de servicios (todo ello testeado en equipamiento real).

Por otra parte, también se obtendrá la información necesaria para la configuración, paso a paso, de todos los equipos que forman la red. De manera que, si un usuario dispone del equipamiento adecuado podrá configurar el mismo escenario partiendo de cero.

Para finalizar, se adjuntará en los anexos del Trabajo la configuración extraída de todos los equipos de la red mediante el comando *"show running-config"*. Esto permitirá que cualquier usuario pueda realizar un copiado de esta configuración en otro equipo de las mismas características de manera rápida y sencilla. Además, se añadirá una lista de comandos básicos para verificar el correcto funcionamiento de los circuitos y de todas las funcionalidades incorporadas.

1.6 Breve descripción de los otros capítulos de la memoria

El Trabajo estará compuesto de los siguientes capítulos:

En el **capítulo 2** se detallará una explicación del *hardware* elegido y descartado para el Trabajo, que está compuesto por los equipos y su firmware, SFPs y latiguillos. Además, se explicará y se configurará el escenario MPLS, sobre equipamiento real, que será utilizado a lo largo de todo el Trabajo. En este capítulo también se especificarán los protocolos intervinientes en la red, tanto los seleccionados como los descartados.

En el **capítulo 3** se explicarán y se configurarán varios mecanismos de mejora de la red MPLS y el primer circuito EPL. El capítulo finalizará con la verificación del correcto funcionamiento, simulando fallos en algunos puntos de la red y validando que hay tráfico extremo a extremo en el circuito.

En el **capítulo 4** se explicarán y se configurarán varios circuitos EVPL, que posteriormente serán validados conforme funcionan correctamente. También se analizará si los circuitos EVPL y los EPL (vistos en el capítulo anterior) son transparentes en los protocolos de nivel 2 (CDP, STP, etc.).

En el **capítulo 5** se explicarán y se configurarán otras mejoras en la red MPLS, como por ejemplo *Policies, Dying Gasp,* etc. Para finalizar este apartado, se verificará que todas estas mejoras funcionan correctamente mediante comprobaciones específicas en los equipos.

2. Red MPLS L2VPN

En este capítulo se va a realizar una descripción de todo el material que se necesita para el montaje de la red MPLS. Además, se verificará qué *firmware* es necesario que incorporen los equipos y, si fuera necesario, se realizará un *upgrade* de la versión. Para finalizar, se explicará y se configurará paso a paso la arquitectura de la solución y los protocolos que se utilizarán.

2.1 Material

A continuación, se detallarán los equipos, SFPs y latiguillos necesarios para el despliegue de la red MPLS. También se revisará el *firmware* que incorporan los equipos.

2.1.1 Equipos

Primero de todo, hay que indicar que los equipos de una red MPLS L2VPN se clasifican según las funciones que desempeñan [1]:

- **PE** *(Provider Edge)* son los *routers* del proveedor que se conectan directamente a un equipo ubicado en la sede del cliente.

- **CPE** *(Customer Premises Equipment)* son los equipos que se ubican en la sede del cliente y tienen conexión directa con el PE. También se les puede llamar CE (*Customer Edge*).

- **P** *(Provider)* son los *routers* que forman parte de la red MPLS L2VPN y que no tienen conexión directa con los equipos de la sede del cliente (CPE).

En la red habrá equipos PE y CPE. No se contempla disponer de equipos P porque, aunque existan equipos sin ninguna conexión con los que están ubicados en la sede del cliente, el objetivo es que cualquiera de los PE pueda asumir este rol.

Por lo tanto, para el montaje de la red se necesita disponer de tres equipos PE que formarán una anilla MPLS y de un CPE, equipo donde terminarán los circuitos creados. Además, serán necesarios dos equipos más que se colocarán en los extremos de los circuitos para poder validar el correcto funcionamiento.

PE

Para formar el anillo MPLS se necesitan tres equipos PE., que es fundamental que cumplan las siguientes características:

- Que tengan un mínimo dos puertos de 10 Gbps para poder realizar las conexiones contra los otros PE.
- Que tengan un mínimo de 12 puertos de 1 Gbps para poder agregar y entregar circuitos de nivel 2.
- Deben soportar la licencia *Advanced Metro IP Access* para poder configurar los servicios EoMPLS de nivel 2 y todas las mejoras que

serán introducidas en la red para darle robustez (*Traffic Engineering, Fast reroute*, etc).

- Que los equipos no se encuentren en estado LDOS (*Last Date of Support*) [2]. Es decir, que no estén obsoletos por parte de proveedor, de manera que no se venden, no se mejoran, no se mantienen y no se les da soporte.

Para llevar a cabo este Trabajo, he conseguido que me presten tres modelos de equipos PE que pueden cumplir con todas estas características.

El primero de ellos se trata del modelo Cisco ME-3600X-24FS.

Figura 1 - Equipo Cisco ME-3600X-24FS [3]

Este equipo cuenta con dos puertos de 10 Gbps y 24 puertos de 1 Gbps e incorpora la licencia *Advanced Metro IP Access***.** No obstante, en la web de Cisco se indica que la fecha LDOS es del 31 de octubre de 2022 [4], esto hace que este equipo sea descartado, ya que si existiese algún problema durante la elaboración del Trabajo sería imposible escalarlo al fabricante.

Los dos restantes son de la misma serie, ASR-920. Se trata de dos equipos ASR-920-12CZ-A y un equipo ASR-920-24SZ-M. Ambos modelos contienen la licencia *Advanced Metro IP Access* y la fecha LDOS es del 30 de julio de 2025 [5]. La diferencia entre ambos modelos es que el ASR-920-12CZ-A contiene 12 puertos de 1 Gbps y 2 puertos de 10 Gbps, mientras que el ASR-920-24SZ-M contiene 24 puertos de 1 Gbps y 4 puertos de 10 Gbps. Por lo tanto, estos equipos cumplen todas las características que se buscaban.

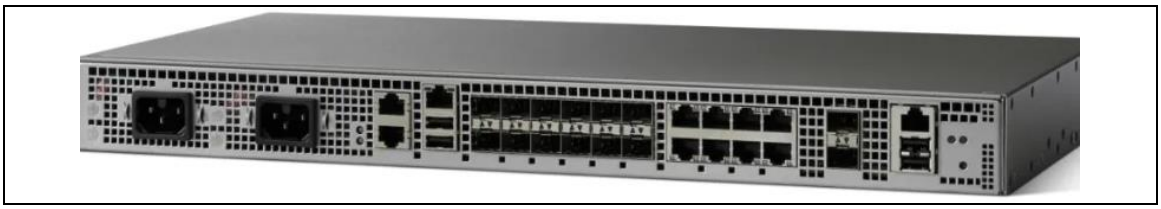


Figura 2 - Cisco ASR-920-12CZ-A [6]

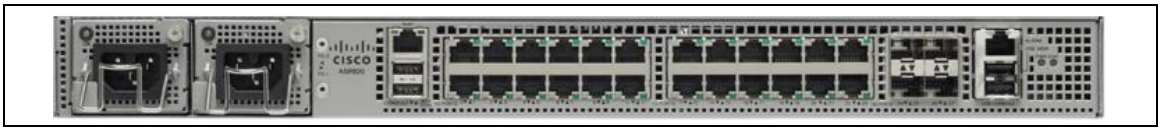


Figura 3 - Cisco ASR-920-24SZ-M [7]

Como se puede observar en la Figura 2 (ASR-920-12CZ-A), los ocho últimos puertos son tipo combo, lo que significa que pueden funcionar como RJ45

(cobre) o como fibra SFP (*Small Form-factor Pluggable Transceiver*) simplemente cambiando la configuración del puerto, como se indica en la Figura 4.

```
ASR-920-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ASR-920-1(config)#interface gigabitEthernet 0/0/4
ASR-920-1(config-if)#media-type ?
  100baseX     Legacy 100baseX command
  10baseT      Legacy 10baseT command
  auto-select  Use whichever connector is attached
  rj45         Use RJ45 connector
  sfp          Use SFP connector
```

Figura 4 - Figura 4 – Configuración media-type ASR-920-12CZ-A

CPE y Equipos de cliente

Como se ha señalado anteriormente, es necesario un equipo CPE que simule estar ubicado en la sede del cliente (empresa), que será desde dónde se entreguen todos los circuitos creados. Además, se necesitan también dos equipos que serán colocados en los extremos de los circuitos para poder validar su correcto funcionamiento. Estos equipos simularán ser los del cliente (empresa) y es importante que cumplan las siguientes características:

- Que dispongan de un mínimo de dos puertos de 1 Gbps tipo fibra SFP. Uno de estos puertos se utilizará para conectar el equipo CPE al equipo PE y el otro se utilizará en caso de que el cliente prefiera la entrega por fibra.
- Que tenga un mínimo de un puerto de 1 Gbps de cobre RJ45 en caso de que el cliente prefiera la entrega del circuito por cable de cobre.
- Deben de ser compatibles con los equipos PE.

En este caso también he podido conseguir que me presten dos modelos distintos de CPE. El primero se trata de un modelo Raisecom RAX711-L-4GC, con dos puertos de 1 Gbps de fibra SFP y cuatro puertos más de 1 Gbps tipo combo.

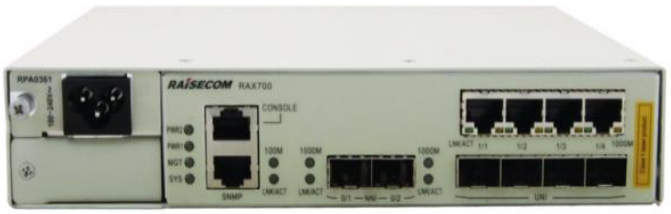


Figura 5 - Raisecom RAX711-L-4GC [8]

El segundo equipo se trata de un modelo Cisco ME-3400EG-2CS-A, con dos puertos de 1 Gbps de fibra SFP y dos puertos más 1 Gbps tipo combo.

Figura 6 - Cisco ME-3400EG-2CS-A [9]

Como los dos equipos cumplen con el mínimo de puertos que se buscaba, he elegido el modelo 3400EG-2CS-A porque, al igual que los PE, es un equipo Cisco y esto asegura que no habrá problemas de incompatibilidades. Además, dado que Cisco es un proveedor internacionalmente conocido, será mucho más fácil encontrar información del equipamiento que en el caso del otro proveedor, Raisecom. Así mismo, el hecho de que todos los equipos que se utilicen sean Cisco permitirá la configuración del protocolo de nivel 2 CDP (*Cisco Discovery Protocol*), que es propio de este proveedor.

Por lo tanto, los equipos que se utilizarán son los siguientes:

- 2 ASR-920-12CZ-A
- 1 ASR-920-24SZ-M
- 3 ME-3400EG-2CS-A

El siguiente paso será la revisión del *firmware* de los equipos, también conocido como IOS (*Internetwork Operating System*), para evaluarlo y actualizarlo en caso de que fuera necesario. Es un paso importante porque el fabricante presenta nuevas versiones que corrigen *bugs* detectados e incorporan nuevas funcionalidades.

Para revisar la IOS primero se debe acceder por consola a todos los equipos, siendo necesario para ello un cable de consola (Figura 7) y el programa PuTTY, que es un emulador de terminal gratuito que incorpora el SO Windows.

Figura 7 - Cable de consola - cable serie Rj45 a DB9 y RS232 a USB [10]

En este paso se conecta el cable del puerto de consola del equipo al puerto Ethernet del PC utilizado y se configura PuTTY con los parámetros de la Figura 8.

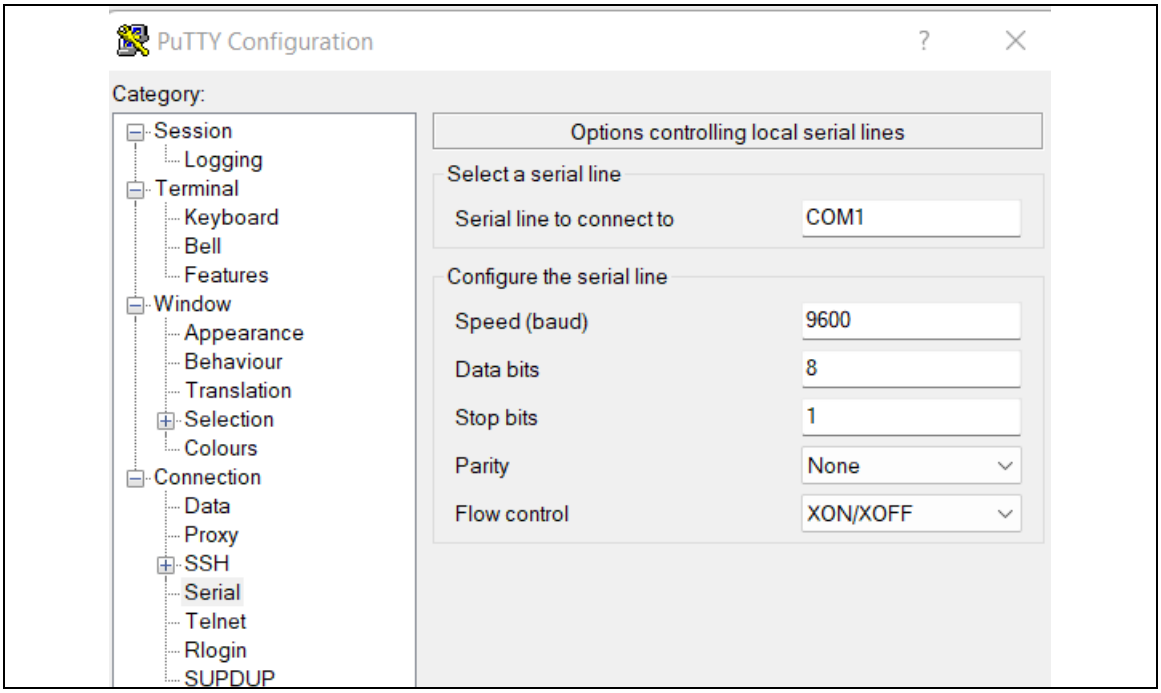


Figura 8 - Valores de configuración PuTTY [11]

Una vez dentro de los equipos, se puede ver la versión IOS que contienen los equipos mediante el comando "*show version*", como se muestra en las Figuras 9, 10 y 11.

```
ASR-920-1#show version
Cisco IOS XE Software, Version 16.09.03
Cisco IOS Software [Fuji], ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Version 16.9.3, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Wed 20-Mar-19 06:36 by mcpre
```

Figura 9 - Versión IOS de ambos ASR-920-12CZ-A

```
ASR-920-SZ-3#show version
Cisco IOS XE Software, Version 16.12.06
Cisco IOS Software [Gibraltar], ASR920 Software (PPC_LINUX_IOSD-UNIVERSALK9_NPE-M), Version 16.12.6, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Sat 04-Sep-21 20:12 by mcpre
```

Figura 10 - Versión IOS ASR-920-24SZ-M

```
ME-3400-17#show version
Cisco IOS Software, ME340x Software (ME340x-METROIPACCESSK9-M), Version 12.2(60)EZ10, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 02-Feb-17 00:59 by prod_rel_team
```

Figura 11 - Versión IOS de los tres ME-3400EG-2CS-A

Aquí se puede observar que los dos modelos ASR-920-12CZ-A tienen la versión 16.9.3, que corresponden a marzo de 2019 según la web de proveedor, de manera que se actualizarán a una versión más actual.

En la misma web se puede comprobar que la versión 16.12.7 es la última publicada, lo que hace que sea necesario actualizar los equipos a esa versión.

Por otra parte, el *firmware* del equipo ASR-920-24SZ-M no será necesario modificarlo, ya que contiene la versión 16.12.6, que pese a no ser la última, es bastante reciente y es un modelo de IOS de la misma serie (*train*) porque coinciden los 2 primeros dígitos 16.12.X [12].

En cuanto a los equipos ME-3400EG-2CS-A, se observa que tienen la versión 12.2(60)EZ10 y no se actualizarán pese a existir versiones más actuales, dado que estos equipos no formarán parte de la red MPLS y su configuración es más básica y sencilla.

En resumen, se deben actualizar los equipos ASR-920-12CZ-A de la versión 16.9.3 a la 16.12.7. Para ello, es necesario descargarse de la web de Cisco el fichero .bin (IOS) y el MD5 Checksum, que luego se detallará para que sirve.

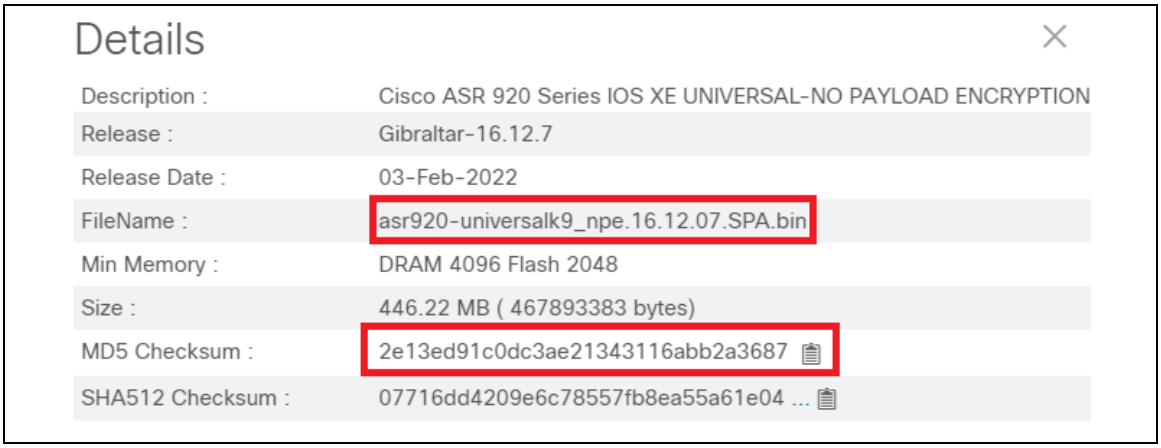


Figura 12 - Descarga IOS 16.12.7 y MD5 Checksum

Una vez descargado el fichero .bin, se guardará en un pincho USB y se deben seguir los siguientes pasos:

1. Introducir el USB en el puerto USB del equipo ASR-920-12CZ-A.

2. Copiar el fichero .bin del directorio usb0:/ a la bootflash:/.

```
ASR-920-1#copy usb0:asr920-universalk9_npe.16.12.07.SPA.bin bootflash:
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
467893383 bytes copied in 88.496 secs (5287170 bytes/sec)
```

Figura 13 - Copiar IOS de USB a bootflash

3. Validar la integridad del fichero .bin mediante la función de verificación de archivos MD5 y realizando la comprobación de que coincide con el código descargado anteriormente (Figura 12).

```
ASR-920-1#verify /md5 bootflash:asr920-universalk9_npe.16.12.07.SPA.bin
.....
.....
.....
.....
.....
verify /md5 (bootflash:asr920-universalk9_npe.16.12.07.SPA.bin) = 2e13ed91c0dc3ae21343116abb2a3687
```

Figura 14 - Verificar MD5 fichero .bin

4. Cargar la nueva IOS y verificar que está correctamente cargada mediante el comando "*show bootvar*". Posteriormente, se debe guardar la configuración y reiniciar el equipo.

```
ASR-920-1(config)#boot system bootflash:asr920-universalk9_npe.16.12.07.SPA.bin
ASR-920-1(config)#exit
ASR-920-1#show bootvar
BOOT variable = bootflash:asr920-universalk9_npe.16.12.07.SPA.bin,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102

ASR-920-1#wr
Building configuration...
[OK]
ASR-920-1#reload
Proceed with reload? [confirm]
```

Figura 15 - Cargar nueva IOS, verificar y reiniciar equipo

5. Una vez el equipo ha reiniciado, se verifica que ha actualizado a la nueva versión de IOS.

Hay que realizar el mismo procedimiento con el otro ASR-920-12CZ-A. De esta manera, todos los equipos dispondrán del *firmware* correcto y estarán preparados para empezar con la configuración de la red MPLS.

2.1.2 SFPs

Los transceptores SFP (*Small Form-factor Pluggable Transceiver*) son módulos que se insertan en los puertos SFP de los equipos y permiten la conexión entre dos dispositivos mediante cable de fibra óptica. Hay diferentes tipos de SFP, dependiendo de la capacidad del puerto (1G, 10G, etc.), de la distancia de la fibra óptica hasta el otro extremo, del tipo de fibra utilizado (monomodo o multimodo) o de si se dispone de una o dos fibras para la conexión entre los dos equipos [13].

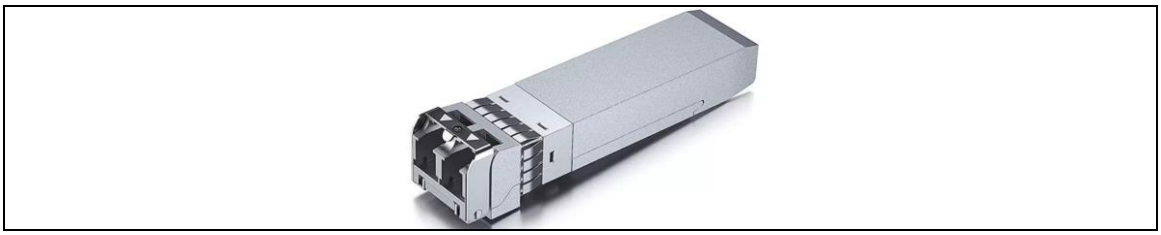


Figura 16 – SFP bifibra [13]

Para nuestro Trabajo se utilizarán los SFP que se indican en la Tabla 1.

SFP	Cantidad	Capacidad	NºFibras	Tipo fibra	Distancia
SFP-10G-SR	2	10 Gbps	2	multimodo	300m
SFP-10G-LR	2	10 Gbps	2	monomodo	10km
SFP-10G-ER	2	10 Gbps	2	monomodo	40km
GLC-SX-MMD	2	1 Gbps	2	multimodo	300m
GLC-BX-D	1	1 Gbps	1	monomodo	20km
GLC-BX-U	1	1 Gbps	1	monomodo	20km

Tabla 1 - SFPs utilizados en el Trabajo

Los cuatro primeros modelos de SFP que aparecen en la tabla anterior tienen dos conectores, uno de recepción de potencia y otro de transmisión, por lo que se necesitan de dos fibras para conectar con el equipo del otro extremo. No obstante, en los dos últimos modelos se realiza la transmisión y recepción de potencia por el mismo conector y solo se necesita una fibra para conectar con el equipo del otro extremo. Por lo tanto, es importante aclarar que un modelo de SFP mono fibra GLC-BX-D siempre se tienen que enfrentar con un modelo GLC-BX-U, ya que uno transmite a 1490nm y recibe a 1310nm, mientras que el otro lo hace a la inversa, transmite a 1310nm y recibe a 1490nm.

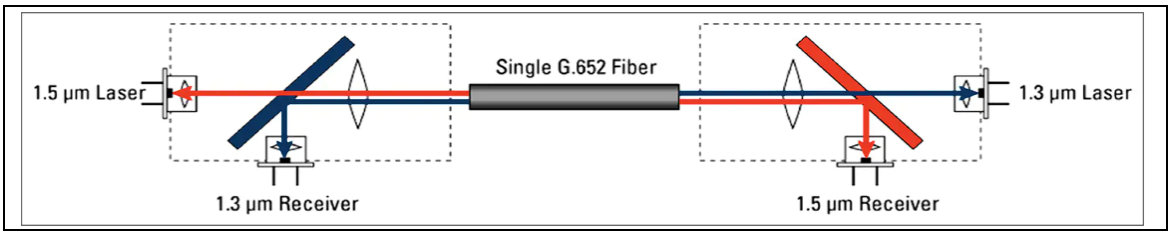


Figura 17 - Transmisión bidireccional de SFPs mono fibra [14]

Se ha creído conveniente la utilización de distintos modelos de SFP, ya que es lo más parecido a un escenario real.

2.1.3 Latiguillos

Para este Trabajo se utilizarán latiguillos de fibra y cobre:

- Latiguillos de fibra monomodo con conectores LC/PC
- Latiguillos de fibra multimodo con conectores LC/PC
- Cables de cobre RJ45 categoría 6

Es importante indicar que por compatibilidad de los SFP utilizados, todos los conectores de los latiguillos de fibra deben ser de tipo LC/PC (*Lucent Connector / Physical Contact*).

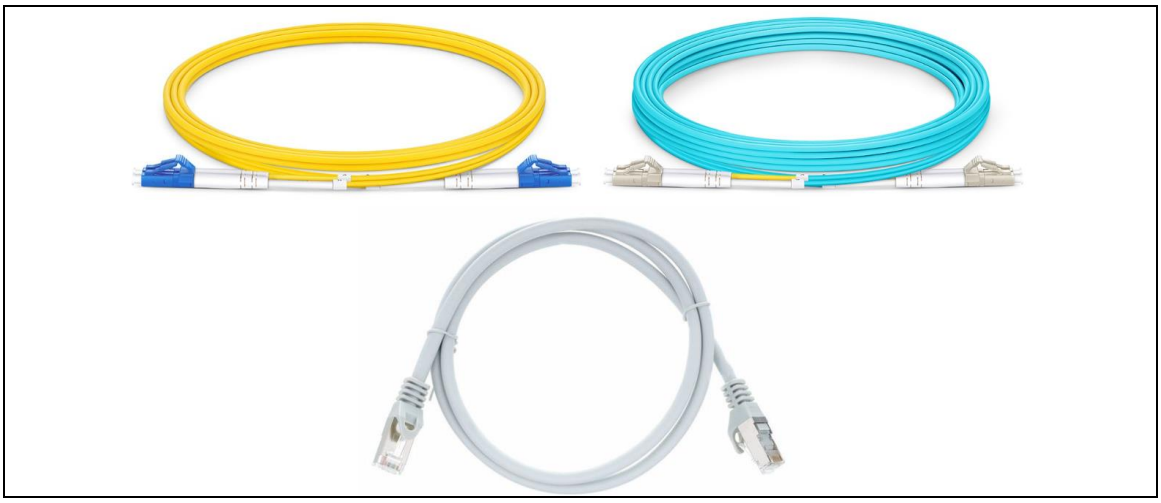


Figura 18 - Latiguillos monomodo, multimodo y de cobre [15][16]

2.2 Escenario MPLS

En este apartado se va a explicar la arquitectura MPLS que se va a utilizar en este Trabajo y los protocolos que intervendrán. También se configurarán todos los equipos paso a paso.

2.2.1 Explicación del escenario MPLS

Como se ha comentado en apartados anteriores, se va a desplegar una red MPLS L2VPN con servicios EoMPLS (*Ethernet Over MPLS*) para poder conectar, mediante circuitos de nivel 2, los equipos de un cliente/empresa.

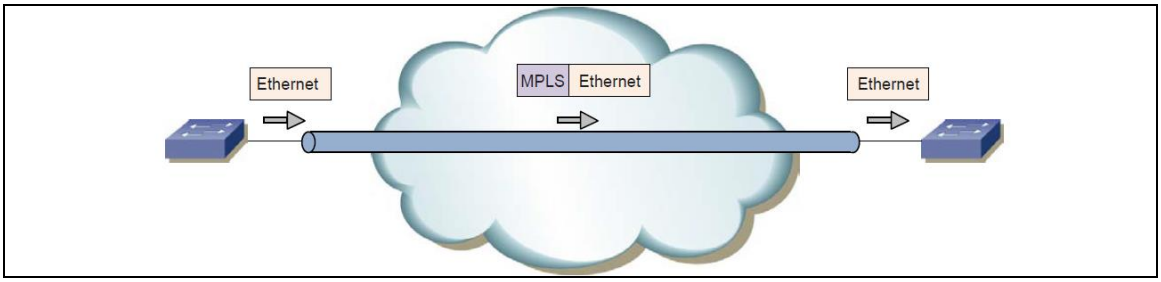


Figura 19 - EoMPLS

Con el mecanismo EoMPLS (Figura 19) se permite el transporte de las tramas *Ethernet* de nivel 2 sobre la red MPLS, de manera que se puedan conectar dos equipos del cliente ubicados en sedes diferentes [17].

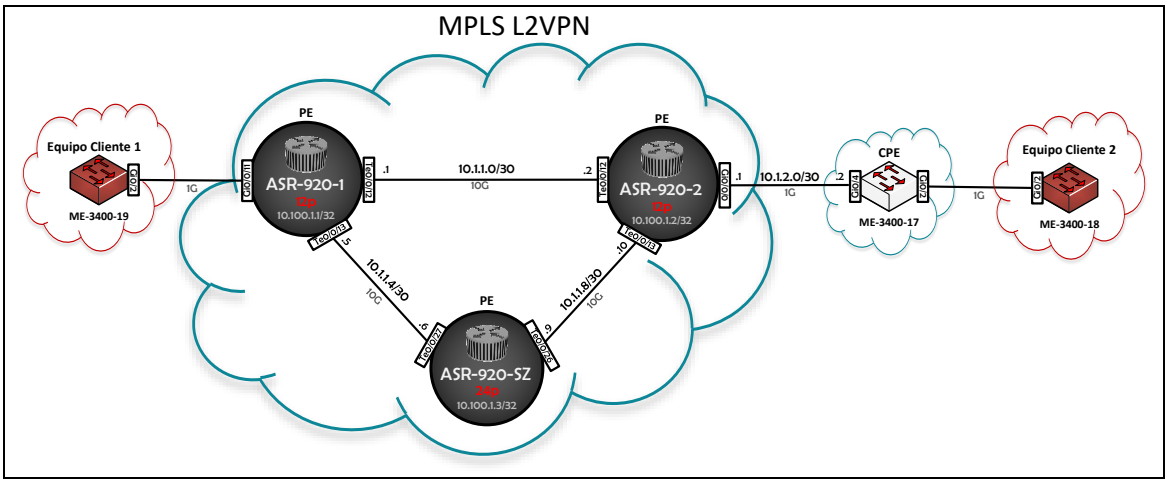


Figura 20 - Escenario MPLS

En la Figura 20 se puede observar el escenario que se va a utilizar en este Trabajo. Consta de tres equipos PE (ASR-920-1, ASR-920-2 y ASR-920-SZ) que formarán el anillo MPLS, todos ellos conectados mediante interfaces de 10 Gbps. También se dispone de un equipo CPE que estará conectado al PE ASR-920-2 mediante una interfaz de 1 Gbps al PE ASR-920-2. Este equipo CPE simulará estar en la sede de cliente.

Para finalizar, en los extremos están los dos equipos de cliente, uno de ellos conectado al CPE y el otro directamente al PE ASR-920-1, ambos conectados a puertos *Ethernet* de 1 Gbps. Desde estos equipos, que simularán ser los del cliente, se validará que los circuitos creados en la red MPLS funcionan correctamente.

La distribución de los equipos ha sido la siguiente:

Hostname	Equipo
ASR-920-1	ASR-920-12CZ-A
ASR-920-2	ASR-920-12CZ-A
ASR-920-SZ	ASR-920-24SZ-M
ME-3400-17	ME-3400EG-2CS-A
ME-3400-18	ME-3400EG-2CS-A
ME-3400-19	ME-3400EG-2CS-A

Tabla 2 - Relación modelos de equipo / *Hostname*

Además, como se puede apreciar en la Figura 20, se define una IP para cada uno de los equipos PE y redes distintas para las troncales (enlaces que unen a los PE), ya que será necesario para la configuración del protocolo de enrutamiento. Todas son redes distintas para que no haya problemas en la configuración.

Equipo	IP
ASR-920-1	10.100.1.1/32
ASR-920-2	10.100.1.2/32
ASR-920-SZ	10.100.1.3/32

Tabla 3 - Relación equipo / IP

Red	Equipo 1 / IP	Equipo 2 / IP
10.1.1.0/30	ASR-920-1 (10.1.1.1)	ASR-920-2 (10.1.1.2)
10.1.1.4/30	ASR-920-1 (10.1.1.5)	ASR-920-SZ (10.1.1.6)
10.1.1.8/30	ASR-920-SZ (10.1.1.9)	ASR-920-2 (10.1.1.10)

Tabla 4 - IPs conexiones entre equipos

Todas estas conexiones entre equipos se han realizado mediante SFP y latiguillos como se indica en la Figura 21.

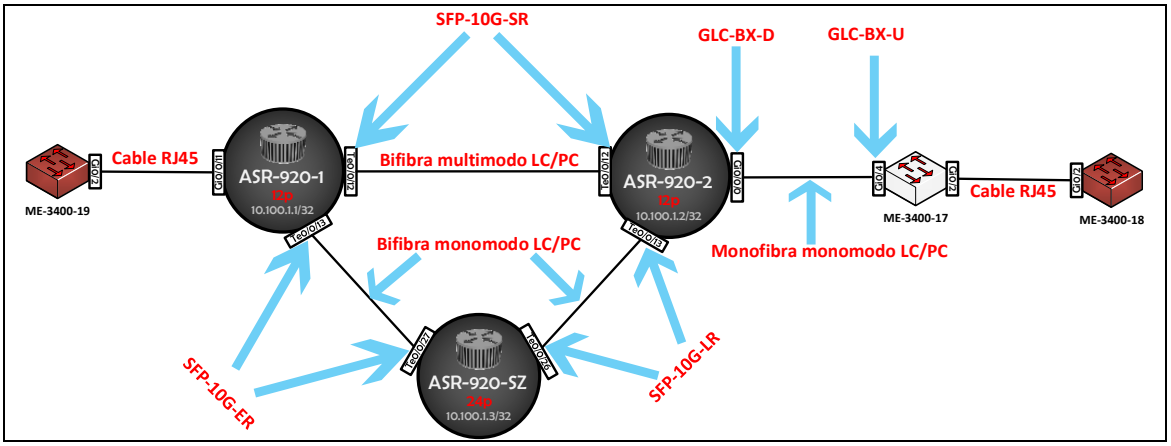


Figura 21 - Conexiones entre equipos

Se puede observar que no ha sido necesario insertar SFP en los enlaces con cable RJ45, ya que se han utilizado los puertos tipo combo y ya disponen de conector de entrada para este conector. También se puede apreciar en la Figura 21 que en enlace mono fibra entre el equipo ASR-920-2 y el ME-3400-

17 es necesario enfrentar distintos modelos de SFP como se ha comentado en el apartado anterior.

Hay que aclarar que los modelos de SFP GLC-SX-MMD se utilizarán más adelante, cuando se configuren los circuitos protegidos.

2.2.2 Protocolos que intervienen

En este apartado se elegirán los diferentes protocolos que serán configurados en la red MPLS, teniendo en cuenta que se deben de cubrir las siguientes necesidades:

- Protocolo para identificar de una manera fácil a los equipos vecinos.
- Protocolo de enrutamiento para que los equipos se comuniquen entre sí.
- Protocolo para la distribución de las etiquetas en la MPLS.

En primer lugar, se necesita un protocolo para poder identificar de una manera fácil a los equipos vecinos. En este punto existen dos protocolos que pueden servir: CDP (*Cisco Discovery Protocol*) y LLDP (*Link Layer Discovery Protocol*). Ambos son protocolos de detección de vecinos a nivel 2 y tienen como función la de anunciar información del dispositivo a los vecinos conectados directamente. No obstante, uno es propiedad de Cisco (CDP) y el otro *multivendor* (LLDP) [18]. Por lo tanto, como todos los equipos que se van a utilizar son Cisco es conveniente configurar el protocolo CDP.

En segundo lugar, se necesita un protocolo de enrutamiento para que los equipos se comuniquen entre sí. Es importante conocer que los protocolos de enrutamiento dinámico se dividen en dos grupos, IGP (*Interior Gateway Protocol*) y EGP (*Exterior Gateway Protocol*).

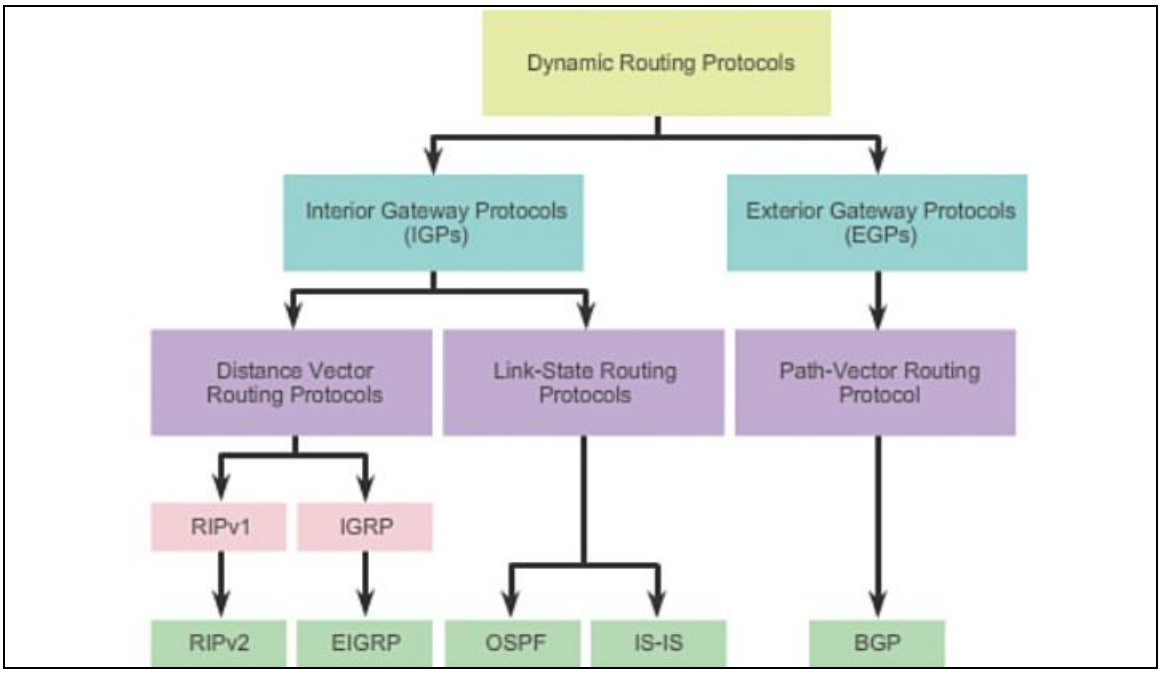


Figura 22 - Protocolos enrutamiento dinámico [19]

Para la configuración de la red, se necesita un protocolo de enrutamiento dentro de un solo sistema autónomo, ya que se trata de una red bajo el control de una misma entidad, por lo que debe ser tipo IGP. EGP se utiliza para interconectar diferentes sistemas autónomos/empresas.

Dentro del grupo IGP existen los protocolos de vector distancia y los de estado de enlace. Los de vector distancia son más fáciles de configurar y mantener, pero son más susceptibles a bucles por una convergencia lenta cuando se producen cambios. También consumen bastante ancho de banda porque envían la tabla de enrutamiento completa cuando hay cambios en la red en vez de enviar solamente una actualización de los cambios en concreto. Por otra parte, los protocolos de estado de enlace convergen más rápido y se envían actualizaciones específicas cuando hay cambios en la topología de la red. Como desventaja, se puede decir que estos protocolos consumen más memoria y CPU de los equipos y es más difícil de configurar [19].

Para el tipo de red que se va a desplegar, se suelen utilizar protocolos de enrutamiento de estado de enlace, ya que acostumbran a ser redes bastante grandes e interesa una rápida convergencia, de manera que los equipos no envíen la tabla de enrutamiento completa cuando hay cambios en la red, consumiendo así más ancho de banda. Por lo tanto, para esta red es más conveniente un protocolo de estado de enlace.

Dentro de los protocolos de estado de enlace está el protocolo OSPF (*Open Shortest Path First*) y IS-IS (*Intermediate System to intermediate System*). IS-IS suele utilizarse para redes de una escalabilidad de aproximadamente 500 equipos, mientras que OSPF alrededor de 100. Por lo tanto, se configurará OSPF ya que la escalabilidad que ofrece este protocolo es más que suficiente. Además, existe más documentación del protocolo OSPF porque suele ser más utilizado.

Por último, se necesita un protocolo para la distribución de las etiquetas en la MPLS. En este caso se utilizará LDP (*Label Distribution Protocol*), ya que se trata de un protocolo simple de señalización y actúa de manera rápida [20].

2.2.3 Configuración del escenario

En este apartado se van a configurar por pasos todos los protocolos que se han visto en el apartado anterior. Por el momento, solo se van a configurar los equipos PE.

CDP

Primero de todo hay que configurar el protocolo CDP mediante el comando "*cdp run*" en el modo de configuración global de los equipos. Posteriormente, se debe habilitar el protocolo en cada una de las interfaces troncales de nuestros equipos mediante el comando "*cdp enable*".

```
ASR-920-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ASR-920-1(config)#cdp run
ASR-920-1(config)#interface tenGigabitEthernet 0/0/12
```

```
ASR-920-1(config-if)#cdp enable
ASR-920-1(config)#interface tenGigabitEthernet 0/0/13
ASR-920-1(config-if)#cdp enable
```

Configuración 1 – CDP ASR-920-1

Se debe aplicar la misma configuración en cada uno de los equipos ASR-920 teniendo en cuenta que cambian las interfaces de 10 Gbps en el equipo de 24 puertos.

Una vez estén todos los equipos con CDP configurado, si se aplica el comando "*show cdp neighbors*" se pueden ver los equipos que hay directamente conectados. Este comando también proporciona información del puerto origen y el puerto del equipo destino de cada uno de los equipos detectados [21].

```
ASR-920-1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
ASR-920-2        Ten 0/0/12        160             R I   ASR-920-1 Ten 0/0/12
ASR-920-SZ       Ten 0/0/13        174             R I   ASR-920-2 Ten 0/0/27

Total cdp entries displayed : 2
ASR-920-1#
```

```
ASR-920-2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
ASR-920-1        Ten 0/0/12        177             R I   ASR-920-1 Ten 0/0/12
ASR-920-SZ       Ten 0/0/13        128             R I   ASR-920-2 Ten 0/0/26

Total cdp entries displayed : 2
ASR-920-2#
```

```
ASR-920-SZ#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
ASR-920-2        Ten 0/0/26        173             R I   ASR-920-1 Ten 0/0/13
ASR-920-1        Ten 0/0/27        174             R I   ASR-920-1 Ten 0/0/13

Total cdp entries displayed : 2
ASR-920-SZ#
```

Figura 23 - Comando "show cdp neighbors" equipos PE

INTERFACES

Las interfaces que conectan con otros equipos PE deben ser configuradas con la IP y la máscara correspondiente. A la interfaz del otro extremo se le debe asignar una IP de la misma red. Además, hay que añadir la MTU (*Maximum Transfer Unit*), que marcará el tamaño máximo de los paquetes de datos que cursarán los puertos.

```
ASR-920-1(config)#interface tenGigabitEthernet 0/0/12
ASR-920-1(config)#mtu 9216
ASR-920-1(config-if)#ip address 10.1.1.1 255.255.255.252

ASR-920-1(config)#interface tenGigabitEthernet 0/0/13
ASR-920-1(config)#mtu 9216
ASR-920-1(config-if)#ip address 10.1.1.5 255.255.255.252
```

Configuración 2 - IP/Máscara equipo ASR-920-1

El resto de los equipos PE se configuran con los mismos comandos, pero con la IP e interfaz que le corresponda.

OSPF

El siguiente paso es configurar el protocolo de enrutamiento OSPF mediante el comando "*router ospf X*", en el que la X especifica el *process-id* asignado al protocolo. Es importante conocer que OSPF funciona con identificativos distintos, aunque se aplicará el mismo (*router ospf 100*) para que la configuración sea más sencilla y visual. En el *router-id* se añadirá la IP del equipo, de manera que se podrán identificar fácilmente a los vecinos OSPF. Para finalizar, se debe hacer que corra OSPF por todas las interfaces de las troncales por la misma área 0.

```
ASR-920-1(config)#router ospf 100
ASR-920-1(config-router)#router-id 10.100.1.1

ASR-920-1(config)#interface tenGigabitEthernet 0/0/12
ASR-920-1(config-if)#ip ospf 100 area 0

ASR-920-1(config)#interface tenGigabitEthernet 0/0/13
ASR-920-1(config-if)#ip ospf 100 area 0
```

Configuración 3 - OSPF ASR-920-1

Se debe aplicar la misma configuración en cada uno de los equipos ASR-920, teniendo en cuenta que las interfaces de algunos equipos y los *router-id* pueden variar.

Una vez el protocolo OSPF esté configurado en todos los equipos PE, se ejecutará el comando "*show ip ospf neighbors*" para observar que funciona correctamente [22].

```
ASR-920-1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.100.3.1        1   FULL/DR         00:00:35    10.1.1.6        TenGigabitEthernet0/0/13
10.100.2.1        1   FULL/DR         00:00:39    10.1.1.2        TenGigabitEthernet0/0/12
ASR-920-1#
```

```
ASR-920-2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.100.3.1        1   FULL/BDR        00:00:33    10.1.1.9        TenGigabitEthernet0/0/13
10.100.1.1        1   FULL/BDR        00:00:39    10.1.1.1        TenGigabitEthernet0/0/12
ASR-920-2#
```

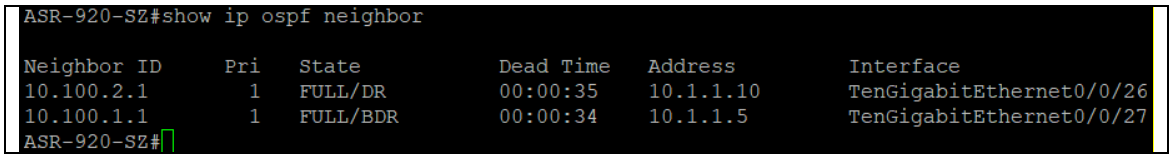


Figura 24 - Comando "show ip ospf neighbors" equipos PE

Se puede observar en la Figura 24 a los vecinos OSPF de los equipos y la interfaz por la que los detecta.

LDP

Para finalizar, se tiene que activar el protocolo LDP en los equipos mediante el comando "*mpls label protocol ldp*". Al igual que en la configuración del protocolo OSPF, el *router-id* será la IP del equipo. También hay que añadir de forma manual a los vecinos LDP de cada equipo [23].

```
ASR-920-1(config)#mpls label protocol ldp
ASR-920-1(config)#mpls tp
ASR-920-1(config-mpls-tp)#router-id 10.100.1.1
ASR-920-1(config)#mpls ldp router-id Loopback0 force
ASR-920-1(config)#mpls ldp neighbor 10.100.1.2 targeted
ASR-920-1(config)#mpls ldp neighbor 10.100.1.3 targeted
```

Configuración 4 - LDP ASR-920-1

El resto de los equipos PE se configuran con los mismos comandos, modificando en este caso la IP del *router-id* y a los vecinos LDP.

Para validar que el protocolo LDP funciona correctamente debemos esperar a que se haya creado algún circuito en la red MPLS.

3. Circuito EPL y mecanismos de mejora en la MPLS

En este capítulo se va a describir y a configurar algunos mecanismos de mejora de la red MPLS, como *Traffic Engineering* y *Fast reroute*. También se va a explicar en qué consisten los circuitos EPL y se va a configurar uno de ellos para acabar validándolo.

Para finalizar, se comprobará que todas las mejoras funcionan correctamente simulando caídas en la red y comparando los tiempos de recuperación del circuito sin las mejoras aplicadas. Además, se observará como la red es capaz de asignar un camino alternativo de forma automática.

3.1 *Traffic Engineering*

En este apartado se va a explicar en qué consiste *Traffic Engineering* y se configurará en los equipos de la red

3.1.1 ¿Qué es *Traffic Engineering*?

Traffic Engineering (TE) es una función que puede implementarse en las redes MPLS que consiste en diseñar las rutas que interesa utilizar para transportar los circuitos que existen en la red, de manera que el camino no sea elegido de forma automática por el protocolo de enrutamiento que tenga configurado los equipos.

Se debe tener en cuenta que los protocolos de enrutamiento siempre suelen utilizar el camino más corto, aunque existan múltiples rutas para llegar de un punto a otro. Esto implica que, si existen periodos de alto volumen de tráfico, puede dar lugar a la congestión de algunas rutas mientras que otras alternativas estarán infrautilizadas.

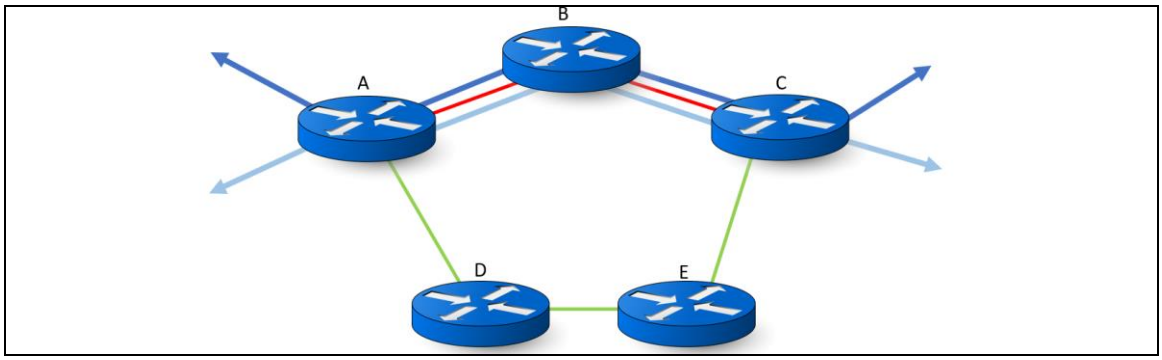


Figura 25 - Red sin *Traffic Engineering*

En la Figura 25 se puede observar un ejemplo de cómo el protocolo de enrutamiento crea un solo camino corto entre router A y router C, mientras el camino más largo (router D y E) está infrautilizado.

Con *Traffic Engineering*, en lugar de ampliar el ancho de banda para hacer frente a los aumentos de volumen de tráfico, se puede utilizar la capacidad ya existente de una forma más eficiente, eligiendo rutas explícitas de la red. Como

se puede observar en la Figura 26, gracias a TE, ahora se utiliza un camino distinto para cada uno de los circuitos [24].

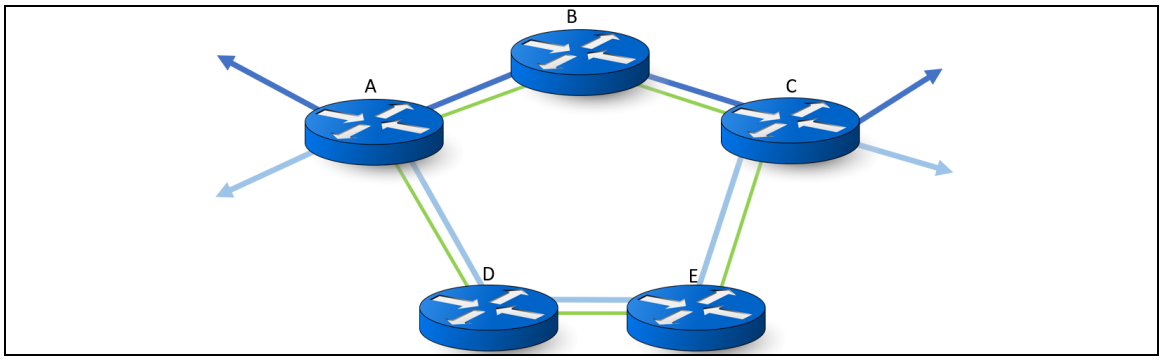


Figura 26 – Red con *Traffic Engineering*

3.1.2 Configuración *Traffic Engineering*

En la red MPLS interesa que los circuitos vayan del equipo ASR-920-1 al ASR-920-2, ya que el objetivo es que el circuito finalice en el CPE. Por lo tanto, como se muestra en la Figura 27, se aplicará *Traffic Engineering* para forzar que el tráfico pase por el equipo ASR-920-SZ.

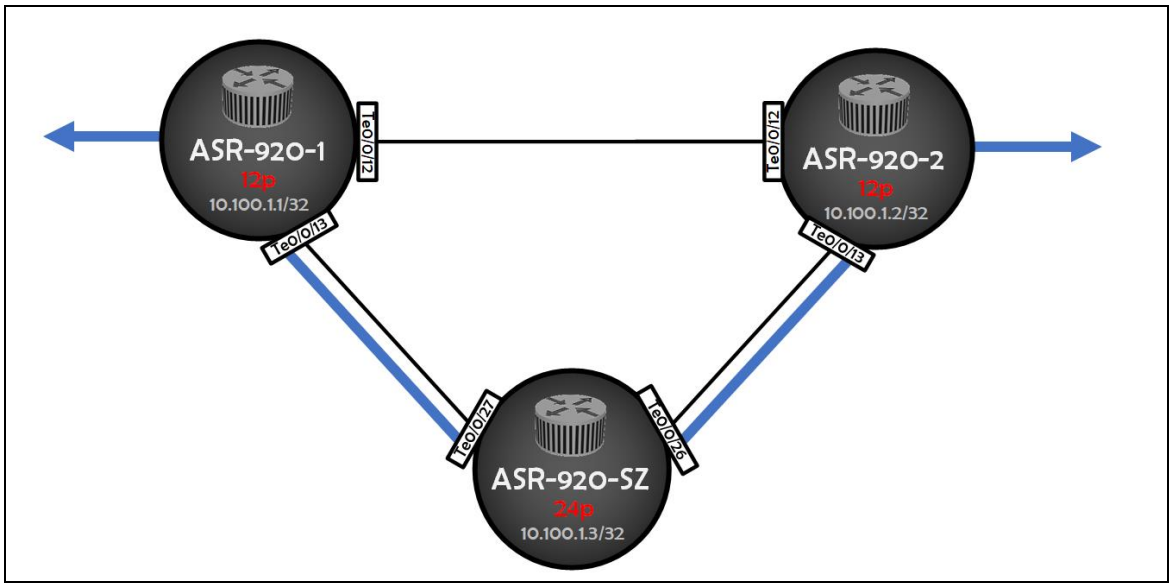


Figura 27 - Camino elegido por *Traffic Engineering*

Si hubiera un problema en la ruta elegida (también denominada ruta explícita), los circuitos se rencaminarán automáticamente utilizando la ruta directa entre el equipo ASR-920-1 y ASR-920-2.

Por lo tanto, para activar MPLS TE se comienza aplicando los siguientes comandos en el modo de configuración global de todos los equipos PE [25].

```
ASR-920-1(config)#mpls traffic-eng tunnels
ASR-920-1(config)#mpls traffic-eng signalling advertise explicit-null
ASR-920-1(config)#mpls traffic-eng signalling interpret explicit-null verbatim
```

Configuración 5 - TE en configuración global del equipo ASR-920-1

A continuación, se activa *Traffic Engineering* en el protocolo de enrutamiento OSPF (área 0) que se ha configurado en el capítulo anterior. No obstante, antes se debe configurar la interfaz "*Loopback 0*" y asignarle la IP del equipo, ya que con el comando "*mpls traffic-eng router-id Loopback0"* se especificará que el identificador sea la dirección IP asociada a esa interfaz. Además, se forzará a que el protocolo LDP seleccione la interfaz *Loopback0* como *router-id.*

```
ASR-920-1(config)#interface loopback 0
ASR-920-1(config-if)#ip address 10.100.2.1 255.255.255.255
ASR-920-1(config-if)#ip ospf 100 area 0

ASR-920-1(config)#mpls ldp router-id Loopback0 force
```

Configuración 6 - Creación Loopback0 en ASR-920-1

```
ASR-920-1(config)#router ospf 100
ASR-920-1(config-router)#mpls traffic-eng router-id Loopback0
ASR-920-1(config-router)#mpls traffic-eng area 0
```

Configuración 7 - Comandos TE OSPF ASR-920-1

Por último, se debe activar TE en las interfaces de los equipos PE que conectan con otros PE mediante el comando "*mpls traffic-eng tunnels"* [26].

```
ASR-920-1(config)#interface tenGigabitEthernet 0/0/12
ASR-920-1(config-if)#mpls traffic-eng tunnels

ASR-920-1(config)#interface tenGigabitEthernet 0/0/13
ASR-920-1(config-if)#mpls traffic-eng tunnels
```

El resto de los equipos PE se deben configurar de igual manera, con las IP e interfaces correspondientes.

En este punto, se puede comenzar a crear el túnel TE entre el equipo ASR-920-1 y ASR-920-2 pasando por ASR-920-SZ. Para ello son necesarios tres pasos:

- Configurar camino explícito (explicit-path).
- Configurar el túnel.
- Configurar el pseudowire-class.

EXPLICIT-PATH

El *explicit-path* indica la ruta que seguirán los circuitos. En los comandos se deben añadir los saltos necesarios hasta llegar al destino dentro del "*next-address"*. Es importante crear el *explicit-path* también en el equipo ASR-920-2, ya que se debe especificar la ruta igualmente en sentido contrario [27].

```
ASR-920-1(config)#ip explicit-path name Path-1-SZ-2 enable
ASR-920-1(config)#next-address 10.1.1.6
ASR-920-1(config)#next-address 10.1.1.10
```

Configuración 8 - Explicit-path ASR-920-1

```
ASR-920-2(config)#ip explicit-path name Path-2-SZ-1 enable
ASR-920-2(config)#next-address 10.1.1.9
ASR-920-2(config)#next-address 10.1.1.5
```

Configuración 9 - Explicit-path ASR-920-2

Como se puede apreciar, los *explicit-path* se nombran como "*Path-1-SZ-2*" y "*Path-2-SZ-1*" para que sean fácilmente identificables.

TÚNEL

Hay que crear una interfaz tipo túnel en cada uno de los equipos PE de los extremos.

```
ASR-920-1(config)#interface Tunnel1
ASR-920-1(config-if)#ip unnumbered Loopback0
ASR-920-1(config-if)#tunnel mode mpls traffic-eng
ASR-920-1(config-if)#tunnel destination 10.100.2.1
ASR-920-1(config-if)#tunnel mpls traffic-eng autoroute announce
ASR-920-1(config-if)#tunnel mpls traffic-eng priority 1 1
ASR-920-1(config-if)#tunnel mpls traffic-eng path-option 5 explicit name Path-1-SZ-2
ASR-920-1(config-if)#tunnel mpls traffic-eng path-option 10 dynamic
```

Configuración 10 - Túnel ASR-920-1

```
ASR-920-2(config)#interface Tunnel1
ASR-920-2(config-if)#ip unnumbered Loopback0
ASR-920-2(config-if)#tunnel mode mpls traffic-eng
ASR-920-2(config-if)#tunnel destination 10.100.1.1
ASR-920-2(config-if)#tunnel mpls traffic-eng autoroute announce
ASR-920-2(config-if)#tunnel mpls traffic-eng priority 1 1
ASR-920-2(config-if)#tunnel mpls traffic-eng path-option 5 explicit name Path-2-SZ-1
ASR-920-2(config-if)#tunnel mpls traffic-eng path-option 10 dynamic
```

Configuración 11 - Túnel ASR-920-2

A continuación, se explica la función de cada comando aplicado [28]:

- **"*ip unnumbered Loopback0*":** La interfaz de túnel no debe ser numerada porque se trata de un enlace unidireccional.
- **"*tunnel mode mpls traffic-eng*":** Se activa el modo MPLS TE.
- "*tunnel destination 10.100.X.1*" >> Se especifica la dirección IP del equipo destino del túnel.
- **"*tunnel mpls traffic-eng autoroute announce*":** Con este comando, OSPF utilizará ese túnel para calcular el camino más corto mejorado.
- **"*tunnel mpls traffic-eng priority 1 1*":** Con este comando se establece la prioridad de los túneles. Es importante indicar que en todos los túneles que se configuren en la red se aplicarán las mismas prioridades.
- **"*tunnel mpls traffic-eng path-option 5 explicit name Path-X*":** Aquí se asigna la ruta creada anteriormente como camino explícito, añadiendo el "5" como opción de camino para diferenciarlo de los otros tipos.

- **“*tunnel mpls traffic-eng path-option 10 dynamic*”:** Con este comando se indica que si fallase la ruta explícita se elegirá un camino dinámico según el ancho de banda de todos los saltos hasta llegar al destino. En este caso, se añade como opción “10” para diferenciarlo de los otros tipos.

PSEUDOWIRE-CLASS

Mediante el *pseudowire-class* se puede crear una plantilla de configuración para múltiples conexiones de pseudowire. En este punto es importante aclarar que un pseudowire, como se puede ver en la Figura 28, no es más que una conexión entre dos equipos PE para transportar tramas de nivel 2.

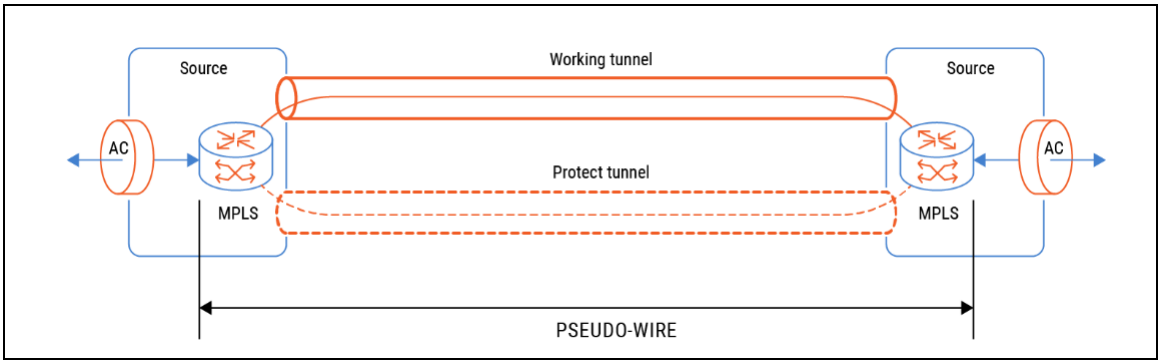


Figura 28 – Pseudowire [29]

Para configurar el *pseudowire-class*, primero hay que nombrar al *pseudowire-class* para que sea fácil de identificar. Luego, se indica el tipo de encapsulación “mpls” y se le asigna el túnel correspondiente mediante el comando *“preferred-path interface TunnelX”* [30]. Al igual que en los anteriores puntos, se debe configurar también en el equipo ASR-920-2.

```
ASR-920-1(config)#pseudowire-class 1-SZ-2
ASR-920-1(config-pw-class)#encapsulation mpls
ASR-920-1(config-pw-class)#preferred-path interface Tunnel1
```

Configuración 12 - pseudowire-class ASR-920-1

```
ASR-920-2(config)#pseudowire-class 2-SZ-1
ASR-920-2(config-pw-class)#encapsulation mpls
ASR-920-2(config-pw-class)#preferred-path interface Tunnel1
```

Configuración 13 - pseudowire-class ASR-920-2

Una vez se ha configurado el *explicit-path*, el túnel y el *pseudowire-class* se debe comprobar que la interfaz tipo túnel creada en los dos equipos PE levanta correctamente mediante el comando “*show interfaces description | i Tu1*”.

```
ASR-920-1#show interfaces description | i Tu1
Tu1                            up             up
ASR-920-1#
```

Figura 29 - Estado Tunnel1 ASR-920-1

```
ASR-920-2#show interfaces description | i Tu
Tu1                            up             up
ASR-920-2#
```

Figura 30 - Estado Tunnel1 ASR-920-2

Como se puede observar, la interfaz está levantada en ambos equipos.

3.2 *Fast reroute* (FFR)

En este apartado se va a explicar en qué consiste *Fast reroute* (FRR) y se configurará en los equipos de la red.

3.2.1 ¿Qué es FRR?

Fast reroute (FRR) es una funcionalidad muy útil en las redes MPLS en las que se aplica *Traffic Engineering*, debido a que realiza una protección de los enlaces troncales a través de un túnel previamente prestablecido, permitiendo un desvío temporal rápido cuando falla un enlace o nodo.

Si no se configura FRR, es importante destacar que los equipos tardarán más tiempo en restablecer los circuitos por una nueva ruta de backup

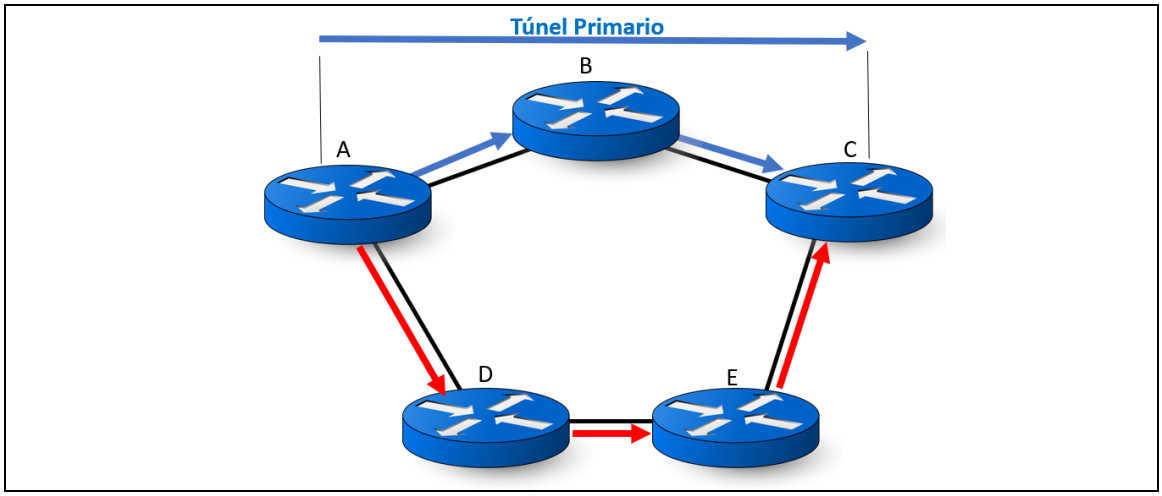


Figura 31 - Protección de enlace FRR

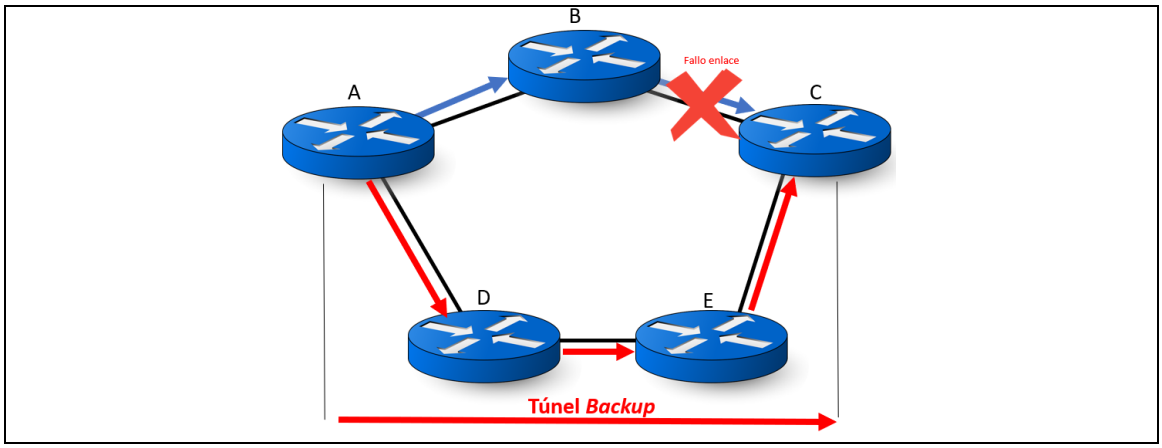


Figura 32 - Protección de enlace FRR en funcionamiento

En la Figura 31 se puede ver ilustrado el proceso de FRR mediante un túnel primario entre el equipo A y C, pasando por B. Por otra parte, existe un *backup* FRR entre los mismos equipos, pero ahora pasando por los equipos D y E. De esta manera, si hubiera un problema en cualquiera de los enlaces del túnel

primario, el equipo A detectaría que la ruta no está operativa y redirigiría inmediatamente el tráfico al túnel de *backup*.

Al igual que sucede con los túneles de TE, es importante destacar que los túneles FRR son también unidireccionales. Por lo tanto, debe haber uno en cada dirección.

En resumen, FRR proporciona una red con una alta fiabilidad, ya que ante una caída de la ruta principal el tiempo de conmutación de los circuitos es muy bajo, casi inapreciable para el cliente [31].

3.2.2 Configuración FRR

Antes de comenzar a configurar FRR, es importante recordar que en el apartado anterior se configuró un túnel TE en cada dirección, entre el equipo ASR-920-1 y ASR-920-2, pasando por ASR-920-SZ.

En el caso de los túneles FRR, se deben configurar tantos como enlaces troncales tenga el equipo que se quiere proteger. Por ejemplo, como se puede ver en la Figura 33, en el equipo ASR-920-1 hay que crear un túnel FRR hacía el ASR-920-2 pasando por ASR-920-SZ y otro hacía el ASR-920-SZ pasando por ASR-920-2.

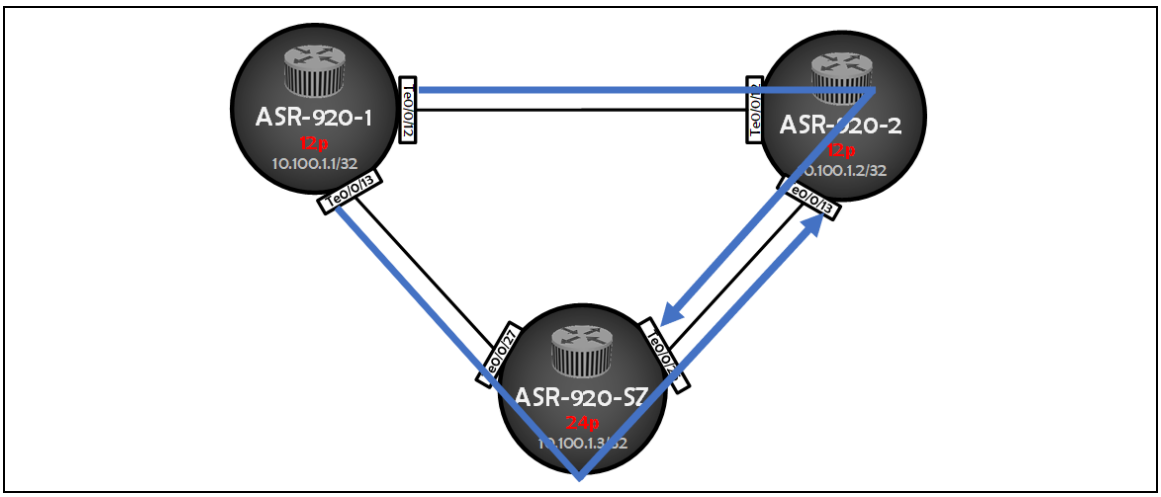


Figura 33 - Túneles FRR equipo ASR-920-1

En el resto de los equipos también hay que crear túneles FRR hacia los otros equipos (Figura 34 y 35), ya que se deben proteger todos los enlaces en ambos sentidos.

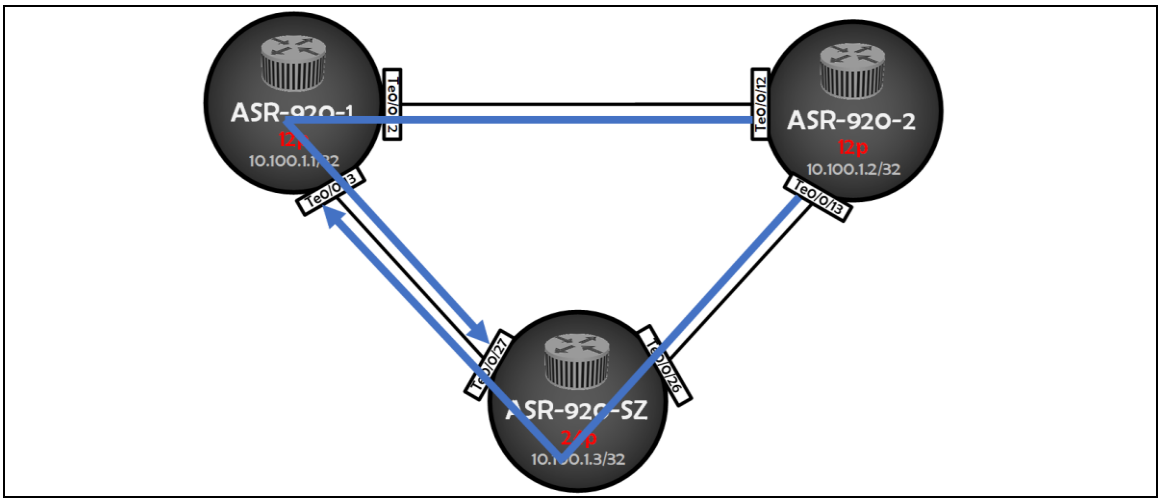


Figura 34 - Túneles FRR equipo ASR-920-2

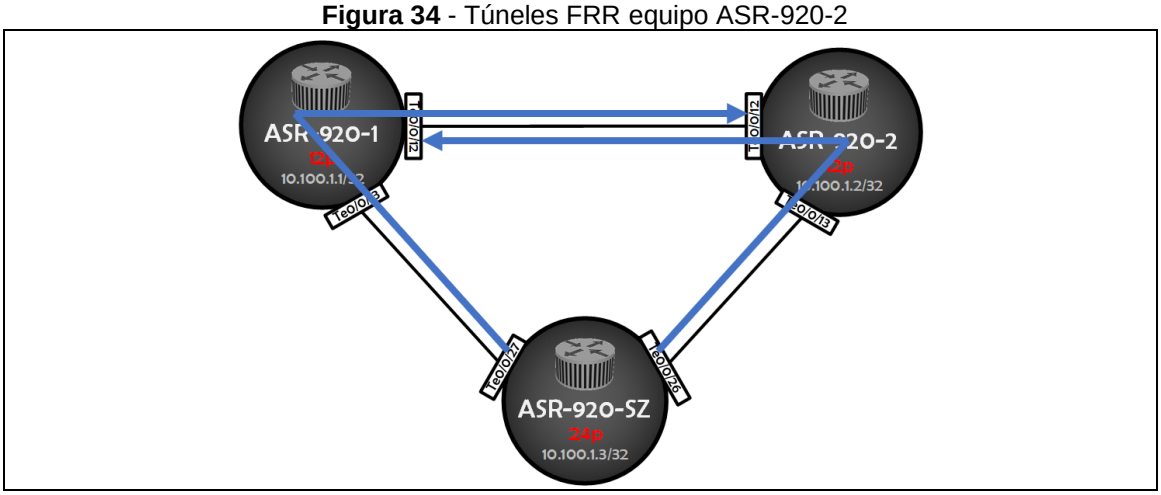


Figura 35 - Túneles FRR equipo ASR-920-SZ

Por lo tanto, para configurar los túneles FRR en los equipos se necesitan los siguientes cuatro pasos [31]:

- Configurar camino explícito (explicit-path).
- Configurar el túnel FRR.
- Aplicar el túnel FRR a la interfaz correspondiente.
- Permitir a los túneles TE que utilicen los túneles FRR en caso de fallo.

EXPLICIT-PATH

Como en el caso de los túneles TE, el *explicit-path* indicará la ruta que seguirán nuestros túneles FRR. Para la configuración es necesario añadir los saltos hasta llegar al equipo destino dentro del "*next-address"* [31].

```
ASR-920-1(config)#ip explicit-path name FRR-ASR-920-2 enable
ASR-920-1(config)#next-address 10.1.1.6
ASR-920-1(config)#next-address 10.1.1.10

ASR-920-1(config)#ip explicit-path name FRR-ASR-920-SZ enable
ASR-920-1(config)#next-address 10.1.1.2
ASR-920-1(config)#next-address 10.1.1.9
```

Configuración 14 – explicit-path FRR ASR-920-1

```
ASR-920-2(config)#ip explicit-path name FRR-ASR-920-1 enable
ASR-920-2(config)#next-address 10.1.1.9
ASR-920-2(config)#next-address 10.1.1.5

ASR-920-2(config)#ip explicit-path name FRR-ASR-920-SZ enable
ASR-920-2(config)#next-address 10.1.1.1
ASR-920-2(config)#next-address 10.1.1.6
```

Configuración 15 - explicit-path FRR ASR-920-2

```
ASR-920-SZ(config)#ip explicit-path name FRR-ASR-920-1 enable
ASR-920-SZ(config)#next-address 10.1.1.10
ASR-920-SZ(config)#next-address 10.1.1.1

ASR-920-SZ(config)#ip explicit-path name FRR-ASR-920-2 enable
ASR-920-SZ(config)#next-address 10.1.1.5
ASR-920-SZ(config)#next-address 10.1.1.2
```

Configuración 16 - explicit-path FRR ASR-920-SZ

Es importante nombrarlos de manera que sean fácil de indentificar. En este caso, se han nombrado como "*FRR-equipo_destino*".

TÚNEL

Hay que crear interfaces tipo túnel y añadirles la IP del equipo donde termina el túnel FRR. Además, se le debe asignar el *explicit-path* correspondiente [31].

```
ASR-920-1(config)#interface Tunnel10
ASR-920-1(config-if)#ip unnumbered Loopback0
ASR-920-1(config-if)#tunnel mode mpls traffic-eng
ASR-920-1(config-if)#tunnel destination 10.100.2.1
ASR-920-1(config-if)#tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-2

ASR-920-1(config)#interface Tunnel20
ASR-920-1(config-if)#ip unnumbered Loopback0
ASR-920-1(config-if)#tunnel mode mpls traffic-eng
ASR-920-1(config-if)#tunnel destination 10.100.3.1
ASR-920-1(config-if)#tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-SZ
```

Configuración 17 - Túneles FRR ASR-920-1

```
ASR-920-2(config)#interface Tunnel10
ASR-920-2(config-if)#ip unnumbered Loopback0
ASR-920-2(config-if)#tunnel mode mpls traffic-eng
ASR-920-2(config-if)#tunnel destination 10.100.1.1
ASR-920-2(config-if)#tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-1

ASR-920-2(config)#interface Tunnel20
ASR-920-2(config-if)#ip unnumbered Loopback0
ASR-920-2(config-if)#tunnel mode mpls traffic-eng
```

```
ASR-920-2(config-if)#tunnel destination 10.100.3.1
ASR-920-2(config-if)#tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-SZ
```

Configuración 18 - Túneles FRR ASR-920-2

```
ASR-920-SZ(config)#interface Tunnel30
ASR-920-SZ(config-if)#ip unnumbered Loopback0
ASR-920-SZ(config-if)#tunnel mode mpls traffic-eng
ASR-920-SZ(config-if)#tunnel destination 10.100.1.1
ASR-920-SZ(config-if)#tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-1

ASR-920-SZ(config)#interface Tunnel40
ASR-920-SZ(config-if)#ip unnumbered Loopback0
ASR-920-SZ(config-if)#tunnel mode mpls traffic-eng
ASR-920-SZ(config-if)#tunnel destination 10.100.2.1
ASR-920-SZ(config-if)#tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-2
```

Configuración 19 - Túneles FRR ASR-920-SZ

Es importante conocer que en el comando "*tunnel mpls traffic-eng path-option 1 explicit name FRR-nombre_equipo"* ahora se añade el "1" como opción de camino para diferenciarlo de los explicit-path (opción 5) y de los caminos dinámicos (opción 10).

FRR en interfaces

Se deben configurar las interfaces físicas del equipo para que utilicen el túnel FRR en el caso de que detecte un fallo en la interfaz. Es importante añadir el túnel correcto en la interfaz que debe aplicar [31].

```
ASR-920-1(config)#interface tenGigabitEthernet 0/0/12
ASR-920-1(config-if)#mpls traffic-eng backup-path Tunnel10

ASR-920-1(config)#interface tenGigabitEthernet 0/0/13
ASR-920-1(config-if)#mpls traffic-eng backup-path Tunnel20
```

Configuración 20 - FRR en interfaces equipo ASR-920-1

```
ASR-920-2(config)#interface tenGigabitEthernet 0/0/12
ASR-920-2(config-if)#mpls traffic-eng backup-path Tunnel10

ASR-920-2(config)#interface tenGigabitEthernet 0/0/13
ASR-920-2(config-if)#mpls traffic-eng backup-path Tunnel20
```

Configuración 21 - FRR en interfaces equipo ASR-920-2

```
ASR-920-SZ(config)#interface tenGigabitEthernet 0/0/27
ASR-920-SZ(config-if)#mpls traffic-eng backup-path Tunnel30

ASR-920-SZ(config)#interface tenGigabitEthernet 0/0/26
ASR-920-SZ(config-if)#mpls traffic-eng backup-path Tunnel40
```

Configuración 22 - FRR en interfaces equipo ASR-920-SZ

Túneles TE para FRR

Se debe permitir a los túneles TE que utilicen los túneles de FRR en el caso de que falle un enlace. Para esto, se aplica el comando "*tunnel mpls traffic-eng fast-reroute"* en todos los túneles de TE [31].

```
ASR-920-1(config)#interface Tunnel1
ASR-920-1(config-if)#tunnel mpls traffic-eng fast-reroute
```

Configuración 23 - Permiso FRR en túneles TE equipo ASR-920-1

```
ASR-920-2(config)#interface Tunnel1
ASR-920-2(config-if)#tunnel mpls traffic-eng fast-reroute
```

Configuración 24 - Permiso FRR en túneles TE equipo ASR-920-2

Una vez configurados los cuatro pasos, se puede comprobar que todas las interfaces tipo túnel FRR levantan correctamente mediante el comando *"show interfaces description | i Tu10|Tu20|Tu30|Tu40*".

```
ASR-920-1#show interfaces description | i Tu10|Tu20
Tu10                           up             up
Tu20                           up             up
ASR-920-1#
```

Figura 36 - Estado túneles FRR ASR-920-1

```
ASR-920-2#show interfaces description | i Tu10|Tu20
Tu10                           up             up
Tu20                           up             up
ASR-920-2#
```

Figura 37 - Estado túneles FRR ASR-920-2

```
ASR-920-SZ#show interfaces description | i Tu30|Tu40
Tu30                           up             up
Tu40                           up             up
ASR-920-SZ#
```

Figura 38 - Estado túneles FRR ASR-920-SZ

Como se puede observar, las interfaces están levantadas en todos los equipos.

3.3 Circuito EPL

En este apartado se va a explicar en qué consisten los circuitos EPL y se configurará uno en la red MPLS. Para finalizar, se validará que funciona correctamente.

3.3.1 ¿Qué es un circuito EPL?

Primero de todo, hay que indicar que un circuito EPL (*Ethernet Private Line*) es un servicio *Ethernet* definido en MEF (*Metro Ethernet Forum*), que es una asociación que se fundó en 2001 y que está compuesta por más de 200 organizaciones como fabricantes de equipos, proveedores de servicios de telecomunicaciones, etc. Su misión es la del desarrollo, evolución y promover un estándar de servicios e interfaces [32][33].

En segundo lugar, EPL se trata de un servicio que forma parte de la categoría de servicios *Ethernet E-Line*, ya que consiste en una conexión punto a punto entre dos nodos en la que el cliente se conecta a un puerto *Ethernet* del

dispositivo del proveedor para que le transporte el tráfico hacia otro punto de la red, donde también se conecta a otro puerto *Ethernet*. Dentro de la categoría de los servicios E-Line, existen también los servicios EVPL (*Ethernet Virtual Private Line*) que se verán en el siguiente capítulo.

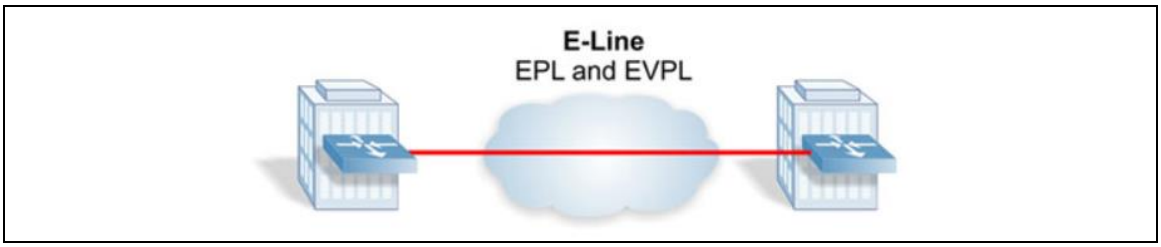


Figura 39 - Servicios E-Line (EPL y EVPL) [34]

Una vez visto esto, se puede decir que los servicios EPL proporcionan dos interfaces *Ethernet* dedicadas (una por extremo). Esto significa que por esas interfaces solo va a correr un único circuito y es ideal para los clientes que buscan obtener un alto grado de transparencia en los protocolos de nivel 2. Como contraprestación, EPL no permite la multiplexación de servicios, lo que significa que nunca se podrán agregar ni entregar más de un servicio por una misma interfaz *Ethernet* [35].

Figura 40 - Esquema servicio EPL [35]

En la Figura 40 se puede ver el esquema de un servicio EPL, donde la parte naranja sería la red del operador de servicios y la parte azul los equipos de cliente.

3.3.2 Configuración circuito EPL

Como se ha explicado en el apartado anterior, el circuito EPL tiene interfaces *Ethernet* dedicadas en las que solo puede existir un circuito. Por lo tanto, en la Figura 41 se puede ver el camino que recorrerá el circuito EPL que se va a configurar.

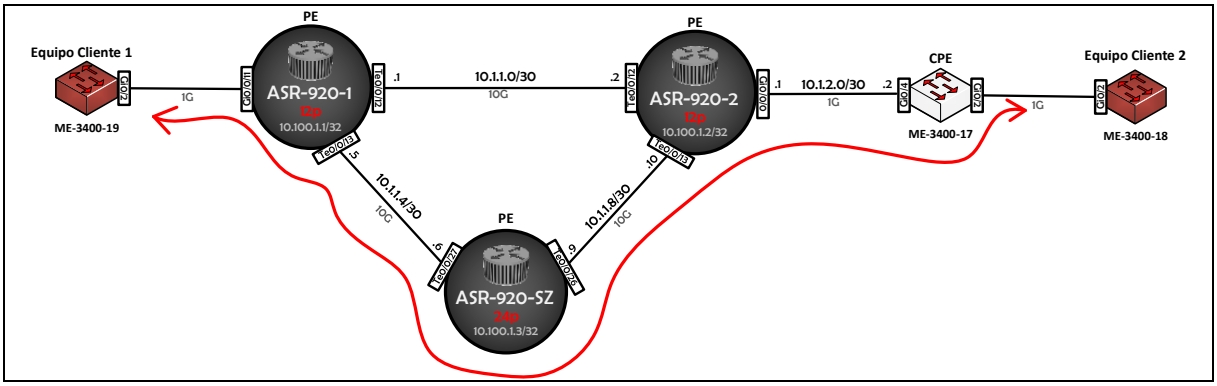


Figura 41 - Circuito EPL red MPLS

El circuito va a ir del puerto Gi0/0/11 del equipo PE ASR-920-1 al puerto Gi0/2 del equipo CPE ME-3400-17, de manera que en ambos extremos se conecten los equipos de cliente y poder validar que todo funciona correctamente.

Para crear el circuito EPL se deben configurar los siguientes puertos y equipos:

- Puerto Gi0/0/11 equipo PE ASR-920-1
- Puerto Gi0/0/0 equipo PE ASR-920-2
- Puertos Gi0/4 y Gi0/2 equipo CPE ME-3400-17

ASR-920-1
Primero se configura el puerto Gi0/0/11 del equipo ASR-920-1.

```
ASR-920-1(config)#interface GigabitEthernet0/0/11
ASR-920-1(config-if)#service instance 3001 ethernet
ASR-920-1(config-if-srv)#encapsulation default
ASR-920-1(config-if-srv)#l2protocol tunnel cdp stp vtp pagp lldp lacp udld
ASR-920-1(config-if-srv)#xconnect 10.100.2.1 1111111 encapsulation mpls pw-class 1-SZ-2
```

Configuración 25 - EPL Gi0/0/11 equipo ASR-920-1

A continuación, se explica la función de cada comando aplicado [36]:

- **"*interface GigabitEthernet0/0/11":*** Se accede a la interfaz Gi0/0/11 del equipo.
- **"*service instance 3001 ethernet*":** Se crea la instancia de servicio 3001 dentro de la interfaz Gi0/0/11. De esta manera se pueden separar los datos de un mismo puerto en diferentes interfaces lógicas (*Service Instance).* Es importante conocer que se puede asignar cualquier número del 1 al 4000.
- **"*encapsulation default":*** Con este comando se define como mapear una etiqueta que entra a una *Service Instance*. En este caso, como el circuito es EPL y solo se va a configurar un circuito por este puerto, se configura como "default". Como es lógico, el equipo solo va a permitir configurar una *Service Instance* por defecto por interfaz. Si se intentara configurar más de una aparecerá un mensaje de error.
- ***"l2protocol tunnel cdp stp vtp pagp lldp lacp udld":*** Con este comando se habilita el túnel de protocolos de nivel 2 para la *Service Instance*. Por lo tanto, los protocolos que aparecen son los que funcionarán a través de este circuito.
- **"*xconnect 10.100.2.1 1111111 encapsulation mpls pw-class 1-SZ-2":*** Aquí se vincula el circuito EPL a un VC *(Virtual Circuit)* pseudowire. Se debe añadir la IP del equipo destino, que en este caso es la del ASR-920-2. También hay que añadir el identificativo del VC, que deberá coincidir con el ID que se añada en el otro extremo (ASR-920-2). Por último, se debe de asignar la *pw-class* del túnel correspondiente, que en este caso es la "*1-SZ-2"* (configurada en el apartado de TE).

ASR-920-2
A continuación, se configura el puerto Gi0/0/0 del equipo ASR-920-2.

```
ASR-920-2(config)#interface GigabitEthernet0/0/0
ASR-920-2(config-if)#service instance 3001 ethernet
ASR-920-2(config-if-srv)#encapsulation dot1q 3001
ASR-920-2(config-if-srv)#rewrite ingress tag pop 1 symmetric
ASR-920-2(config-if-srv)#xconnect 10.100.1.1 1111111 encapsulation mpls pw-class 2-SZ-1
```

Configuración 26 - EPL Gi0/0/0 equipo ASR-920-2 SI 3001

A continuación, se explica la función de cada comando aplicado [36]:

- **"*interface GigabitEthernet0/0/0":*** Se accede a la interfaz Gi0/0/0 del equipo.
- **"*service instance 3001 ethernet*":** Se crea la instancia de servicio 3001 dentro de la interfaz Gi0/0/0.
- **"*encapsulation dot1q 3001":*** En este caso se define que se añadirá la etiqueta 3001 a la trama para diferenciar el tráfico del circuito que se va a enviar o recibir del CPE. Por lo tanto, si se recibe una trama con etiqueta VLAN 3001 por el puerto Gi0/0/0, entrará a la *Service Instance* 3001.
- ***"rewrite ingress tag pop 1 symmetric"*:** Este comando permite tratar la etiqueta antes de realizar el reenvío de la trama, eliminando el *tag* (VLAN 3001) cuando el tráfico entra a la interfaz o añadiendo el *tag* cuando el tráfico sale de la interfaz.
- **"*xconnect 10.100.1.1 1111111 encapsulation mpls pw-class 1-SZ-2":*** Mismo comando que se añadió en el puerto Gi0/0/11 del otro equipo, pero ahora añadiendo la IP del ASR-920-1 y el *pw-class* del túnel correspondiente. Como se puede ver, el ID del VC coincide con el del otro extremo.

Ahora se va a configurar otra *Service Instance* para poder gestionar el equipo CPE a través de esta interfaz Gi0/0/0.

```
ASR-920-2(config)#interface GigabitEthernet0/0/0
ASR-920-2(config-if)#service instance 3000 ethernet
ASR-920-2(config-if-srv)#encapsulation dot1q 3000
ASR-920-2(config-if-srv)#rewrite ingress tag pop 1 symmetric
ASR-920-2(config-if-srv)#bridge-domain 3000

ASR-920-2(config)#interface BDI 3000
ASR-920-2(config-if)#ip address 10.1.2.1 255.255.255.252
ASR-920-2(config-if)#no shutdown
```

Configuración 27 - Gestión Gi0/0/0 equipo ASR-920-2 SI 3000

En este caso se crea la *Service Instance* 3000, añadiendo la etiqueta 3000 a la trama para diferenciar el tráfico de gestión que se va a enviar o recibir del CPE.

La principal diferencia con la *Service Instance* creada anteriormente, es que ahora se asigna a un *bridge-domain*, que se trata de una interfaz lógica para permitir el tráfico bidireccional entre el de nivel 2 y el de nivel 3 [37]. Por lo

tanto, se debe crear una interfaz BDI (*Bridge Domain Interface*), asignarle una dirección IP y levantar la interfaz (*no shutdown*).

ME-3400-17

Por último, se deben configurar los puertos Gi0/4 y Gi0/2 del equipo CPE ME-3400-17. No obstante, primero hay que aplicar algunos comandos en el modo de configuración global del equipo para crear las VLANs de gestión y de tráfico del circuito.

```
ME-3400-17(config)#vlan 3000
ME-3400-17(config)#vlan 3001
```

Configuración 28 - Crear VLANs equipo ME-3400-17

También, es necesario crear una SVI (*Switched Virtual Interface*) para la VLAN 3000, de manera se le pueda asignar una dirección IP. Hay que indicar que una SVI es una interfaz virtual que se define en el equipo para asociar a una VLAN en concreto [38].

```
ME-3400-17(config)#interface vlan 3000
ME-3400-17(config-if)#ip address 10.1.2.2 255.255.255.252
```

Configuración 29 - Crear SVI VLAN 3000 equipo ME-3400-17

Ahora ya se puede configurar la interfaz Gi0/4 del equipo CPE ME-3400-17, que, como recordatorio, es la que va conectada directamente con el equipo PE ASR-920-2.

```
ME-3400-17(config)#interface GigabitEthernet0/4
ME-3400-17(config-if)#port-type nni
ME-3400-17(config-if)#switchport mode trunk
ME-3400-17(config-if)#switchport trunk allowed vlan 3000,3001
```

Configuración 30 - Gi0/4 equipo ME-3400-17

A continuación, se explica la función de cada comando aplicado [39]:

- **"*interface GigabitEthernet0/4":*** Se accede a la interfaz Gi0/4 del equipo.
- **"*port-type nni*":** Se asigna que el puerto sea del tipo NNI (*Network-to-Network interface*), ya que esta interfaz conectará dos o más redes. En este caso, el tráfico del circuito y el de gestión del equipo CPE.
- **"*switchport mode trunk*":** Se asigna que el puerto sea tipo trunk, de manera que permita pasar por ahí más de una VLAN.
- **"*switchport trunk allowed vlan 3000,3001*":** Se asigna al puerto la VLAN 3000 de gestión y la 3001 de tráfico.

Por último, se configura la interfaz Gi0/2, que es la interfaz que va conectada contra el equipo de cliente.

```
ME-3400-17(config)#interface GigabitEthernet0/2
ME-3400-17(config-if)#switchport access vlan 3001
ME-3400-17(config-if)#switchport mode dot1q-tunnel
```

```
ME-3400-17(config-if)#l2protocol-tunnel cdp
ME-3400-17(config-if)#l2protocol-tunnel lldp
ME-3400-17(config-if)#l2protocol-tunnel stp
ME-3400-17(config-if)#l2protocol-tunnel vtp
ME-3400-17(config-if)#l2protocol-tunnel point-to-point pagp
ME-3400-17(config-if)#l2protocol-tunnel point-to-point lacp
ME-3400-17(config-if)#l2protocol-tunnel point-to-point udld
```

Configuración 31 - Gi0/2 equipo ME-3400-17

A continuación, se explica la función de cada comando aplicado [40]:

- **"*interface GigabitEthernet0/2*":** Se accede a la interfaz Gi0/2 del equipo.
- **"*switchport access vlan 3001*":** El puerto será tipo *access*, ya que solamente se le asignará la VLAN de tráfico 3001.
- **"*switchport mode dot1q-tunnel*":** Este comando establece la interfaz como un puerto de túnel 802.1Q.
- **"*l2protocol-tunnel X*"** o **"*l2protocol-tunnel point-to-point X*":** Este comando configura el procesamiento de los protocolos de control de nivel 2. Se asigna uno a uno los protocolos que deben de funcionar a través de este circuito.

Una vez configurados todos los equipos, el circuito EPL en la red MPLS ya debería de funciona correctamente.

A través de la Figura 42 se va a revisar el procesamiento de las tramas del circuito desde que salen del equipo de cliente, pasan por la red MPLS y acaban llegando al otro equipo de cliente.

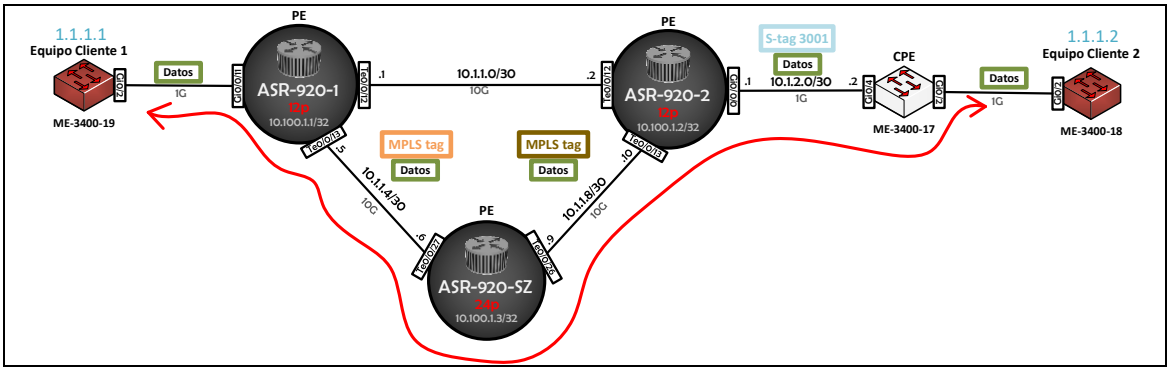


Figura 42 - Circuito EPL red MPLS especificando las tramas

Si se observa de izquierda a derecha, desde el equipo de Cliente 1 ME-3400-19 se puede ver como las tramas salen sin ningún tipo de etiqueta desde el equipo. Cuando llega al PE ASR-920-1, este le añade un *tag* MPLS justo antes de enviarlo por la red MPLS. Hay que indicar que este *tag* MPLS va variando según cambia de equipo PE, ya que cada uno le añade su *tag* correspondiente [41].

Una vez llega al equipo PE ASR-920-2, se elimina el *tag* MPLS y se añade el *S-tag* (etiqueta de servicio) 3001, de manera que cuando llegue al CPE ME-

3400-17 sepa diferenciar el tráfico de circuito con el de gestión. Por último, el CPE elimina el *S-tag* y entrega las tramas en el equipo de Cliente 2 ME-3400-18 tal y como las recibió en origen.

Si ahora se observa de derecha a izquierda, desde el equipo de Cliente 2 ME-3400-19, las tramas sin etiqueta salen de cliente y llegan al CPE ME-3400-17. Este añade el *S-tag* 3001 antes de enviar al PE. Cuando llega al equipo PE ASR-920-2, le añade el *tag* MPLS justo antes de enviarlo por la red MPLS y una vez llega al equipo PE ASR-920-1, se quita el *tag* MPLS correspondiente y se entrega la trama tal y como las recibió en origen.

Una vez visto cómo se comportan las tramas por toda la red, se va a comprobar que la configuración aplicada del circuito EPL funciona correctamente mediante las siguientes validaciones:

- Revisar que desde el equipo ASR-920-2 se llega a ping al CPE ME-3400-17.
- Revisar que hay ping entre los equipos de cliente ME-3400-19 y ME-3400-18.

Se valida que existe ping desde el equipo PE ASR-920-2 al CPE ME-3400-17.

```
ASR-920-2#ping 10.1.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
ASR-920-2#
```

Figura 43 - Ping de PE ASR-920-2 a CPE ME-3400-17

Posteriormente, para validar si existe ping entre los equipos de cliente ME-3400-19 y ME-3400-18, primero se deben configurar IPs del mismo rango en los equipos.

```
ME-3400-19(config)#vlan 1000

ME-3400-19(config)#interface vlan 1000
ME-3400-19(config-if)# ip address 1.1.1.1 255.255.255.0

ME-3400-19(config)#interface GigabitEthernet0/2
ME-3400-19(config-if)#switchport access vlan 1000
```

Configuración 32 - VLAN 1000 equipo cliente ME-3400-19

```
ME-3400-18(config)#vlan 1000

ME-3400-18(config)#interface vlan 1000
ME-3400-18(config-if)# ip address 1.1.1.2 255.255.255.0

ME-3400-18(config)#interface GigabitEthernet0/2
ME-3400-18(config-if)#switchport access vlan 1000
```

Configuración 33 - VLAN 1000 equipo cliente ME-3400-18

Como se puede ver, en ambos equipos se crean la VLAN 1000 y la SVI 1000 asignándole la IP que le corresponde. Seguidamente, se asigna la VLAN 1000 en modo *access* al puerto Gi0/2 de ambos equipos, ya que son los puertos que conectan contra los equipos del proveedor.

Con esto, se puede validar que hay ping entre los equipos y en ambos sentidos.

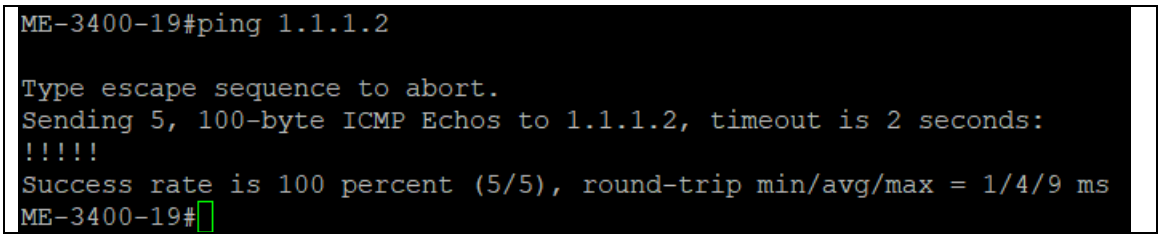


Figura 44 - Ping de equipo ME-3400-19 a ME-3400-18

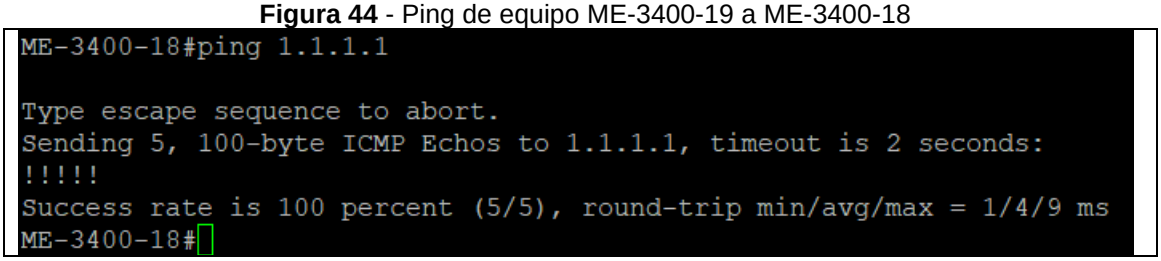


Figura 45 - Ping de equipo ME-3400-18 a ME-3400-17

3.4 Test *Traffic Engineering* y FRR

En este apartado, primero se va a validar que el *Traffic Engineering* configurado en apartados anteriores funciona correctamente. Hay que recordar que se configuró el túnel TE 1 en ambos sentidos para que el tráfico pasara por el equipo ASR-920-SZ. Por lo tanto, para realizar la validación se va a utilizar el comando "*show mpls traffic-eng tunnels tunnel 1"* [42] desde los equipos ASR-920-1 y ASR-920-2, que son los que tienen el túnel 1 TE configurado.

```
ASR-920-1#show mpls traffic-eng tunnels tunnel 1

Name: ASR-920-1_t1                        (Tunnel1) Destination: 10.100.2.1
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 5, type explicit Path-1-SZ-2 (Basis for Setup, path weight 2)
    path option 10, type dynamic

  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
    Hop Limit: disabled [ignore: Explicit Path Option with all Strict Hops]
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 0 [0] bw-based
    auto-bw: disabled
    Fast Reroute: enabled, Node Protection: No, Bandwidth Protection: No
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: explicit path option 5 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  Node Hop Count: 2

  InLabel  :  -
  OutLabel : TenGigabitEthernet0/0/13, 21
  Next Hop : 10.1.1.6
  FRR OutLabel : Tunnel20, 21
  RSVP Signalling Info:
       Src 10.100.1.1, Dst 10.100.2.1, Tun_Id 1, Tun_Instance 152
    RSVP Path Info:
      My Address: 10.1.1.5
      Explicit Route: 10.1.1.6 10.1.1.9 10.1.1.10 10.100.2.1
      Record   Route:   NONE
      Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:  10.100.3.1(21) 10.100.2.1(0)
      Fspec: ave rate=0 kbits, burst=0 bytes, peak rate=0 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 1 (TE)
    Explicit Route: 10.1.1.1 10.1.1.2 10.100.2.1
```

Figura 46 - Validación TE ASR-920-1 camino explícito

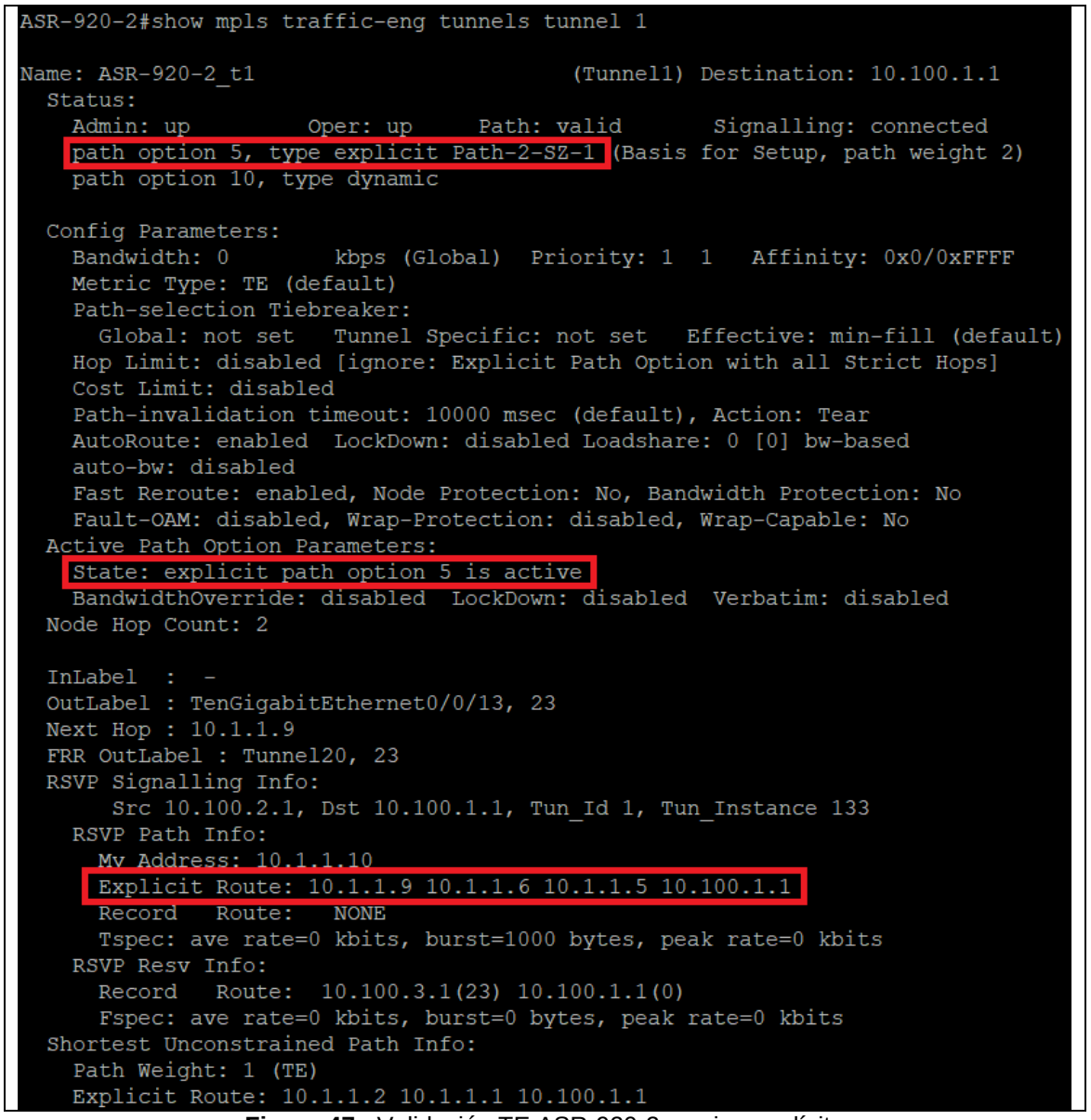


Figura 47 - Validación TE ASR-920-2 camino explícito

Como se puede apreciar en la Figura 46 y Figura 47, en ambos equipos el túnel TE está funcionando por la opción 5, que es el camino explícito que se configuró. Además, se puede apreciar que los saltos que sigue este camino hasta llegar al destino son correctos. Por lo tanto, se puede asegurar que *Traffic Engineering* está funcionando correctamente en ambos sentidos.

Ahora, como se puede ver en la Figura 48, se va a tirar la interfaz Te0/0/13 del equipo ASR-920-2 para provocar que ambos túneles TE cambien la ruta y recalculen automáticamente el camino dinámico (opción 10).

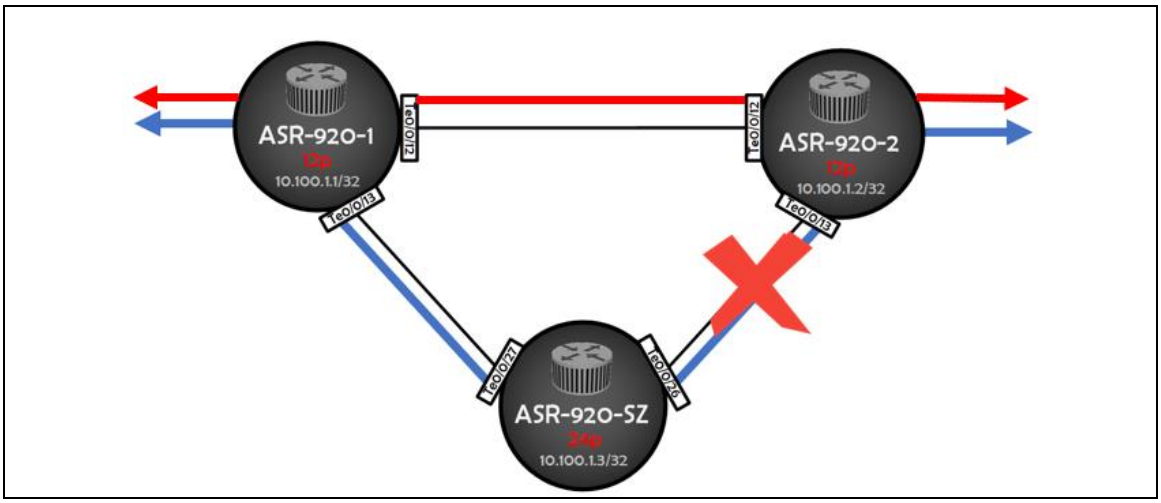


Figura 48 – Fallo enlace entre ASR-920-2 y ASR-920-SZ

Una vez tirada la interfaz, se va a volver a aplicar el comando "*show mpls traffic-eng tunnels tunnel 1"* desde los equipos ASR-920-1 y ASR-920-2.

```
ASR-920-1#show mpls traffic-eng tunnels tunnel 1

Name: ASR-920-1_t1                         (Tunnel1) Destination: 10.100.2.1
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, type dynamic (Basis for Setup, path weight 1)
    path option 5, type explicit Path-1-SZ-2

  Config Parameters:
    Bandwidth: 0        kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    Path-selection Tiebreaker:
      Global: not set   Tunnel Specific: not set   Effective: min-fill (default)
    Hop Limit: disabled
    Cost Limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear
    AutoRoute: enabled  LockDown: disabled Loadshare: 0 [0] bw-based
    auto-bw: disabled
    Fast Reroute: enabled, Node Protection: No, Bandwidth Protection: No
    Fault-OAM: disabled, Wrap-Protection: disabled, Wrap-Capable: No
  Active Path Option Parameters:
    State: dynamic path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  Node Hop Count: 1

  InLabel  :  -
  OutLabel : TenGigabitEthernet0/0/12, explicit-null
  Next Hop : 10.1.1.2
  RSVP Signalling Info:
       Src 10.100.1.1, Dst 10.100.2.1, Tun_Id 1, Tun_Instance 154
    RSVP Path Info:
      My Address: 10.1.1.1
      Explicit Route: 10.1.1.2 10.100.2.1
      Record   Route:   NONE
      Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:  10.100.2.1(0)
      Fspec: ave rate=0 kbits, burst=0 bytes, peak rate=0 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 1 (TE)
    Explicit Route: 10.1.1.1 10.1.1.2 10.100.2.1
```

Figura 49 - Validación TE ASR-920-1 camino dinámico

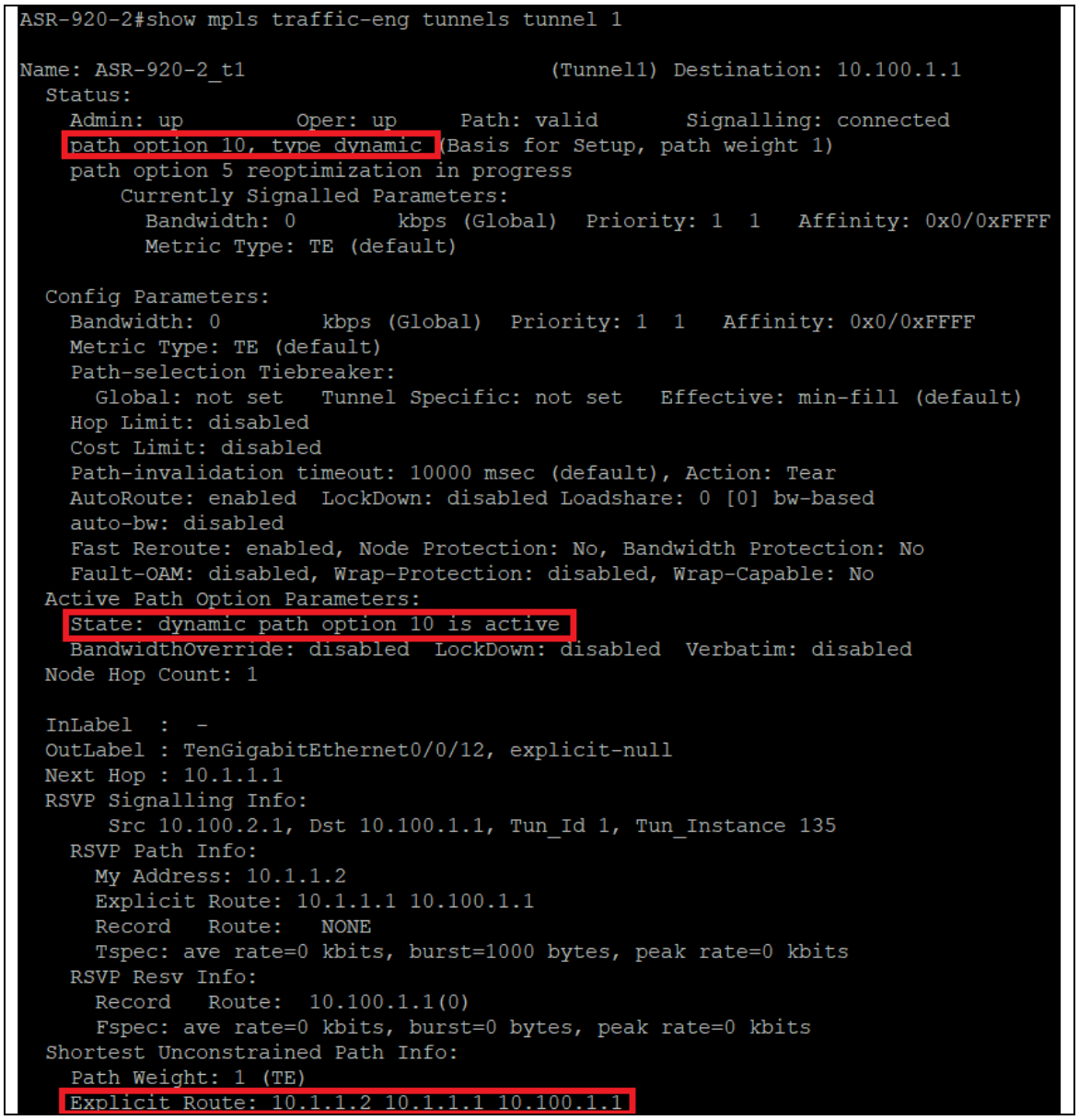


Figura 50 - Validación TE ASR-920-2 camino dinámico

Como se puede apreciar en la Figura 48 y Figura 49, en ambos equipos el túnel TE ahora está funcionando por la opción 10, que es el camino dinámico que ha calculado automáticamente. También se puede apreciar que los saltos que sigue este camino hasta llegar al destino han cambiado respecto lo visto anteriormente. Por lo tanto, se puede asegurar que la redundancia automática hacia el camino dinámico de TE ha funcionado correctamente.

Además, antes de tirar la interfaz se ha dejado lanzado un ping continuo de 1000 repeticiones (*ping 1.1.1.2 repeat 1000*) desde el equipo de Cliente 1 ME-3400-19 hacia el equipo de Cliente 2 ME-3400-18 para comprobar el tiempo del corte durante el cambio del camino explícito al camino dinámico. Hay que recordar que la red tiene configurado FRR, por lo que el tiempo de corte debería ser mínimo.

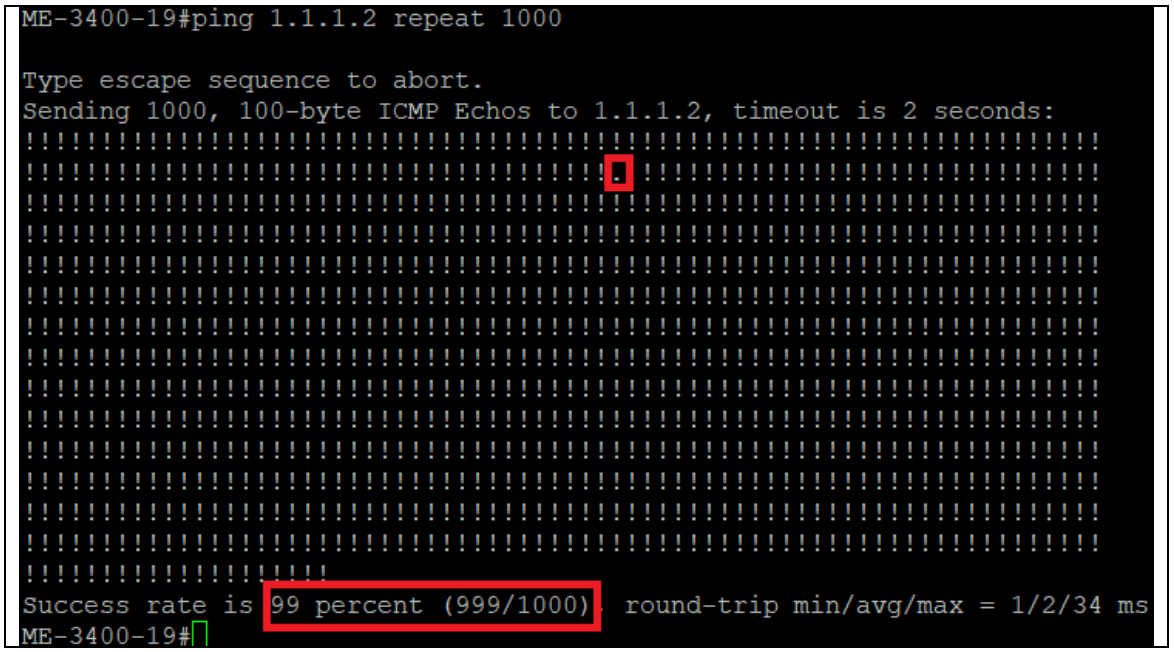


Figura 51 - Ping de equipo Cliente 1 a Cliente 2 con FRR configurado

Como se puede ver en la Figura 51, solamente se ha perdido un ping.

Para finalizar, se va a realizar la misma comprobación, pero desactivando FRR de todas las interfaces de los equipos PE.

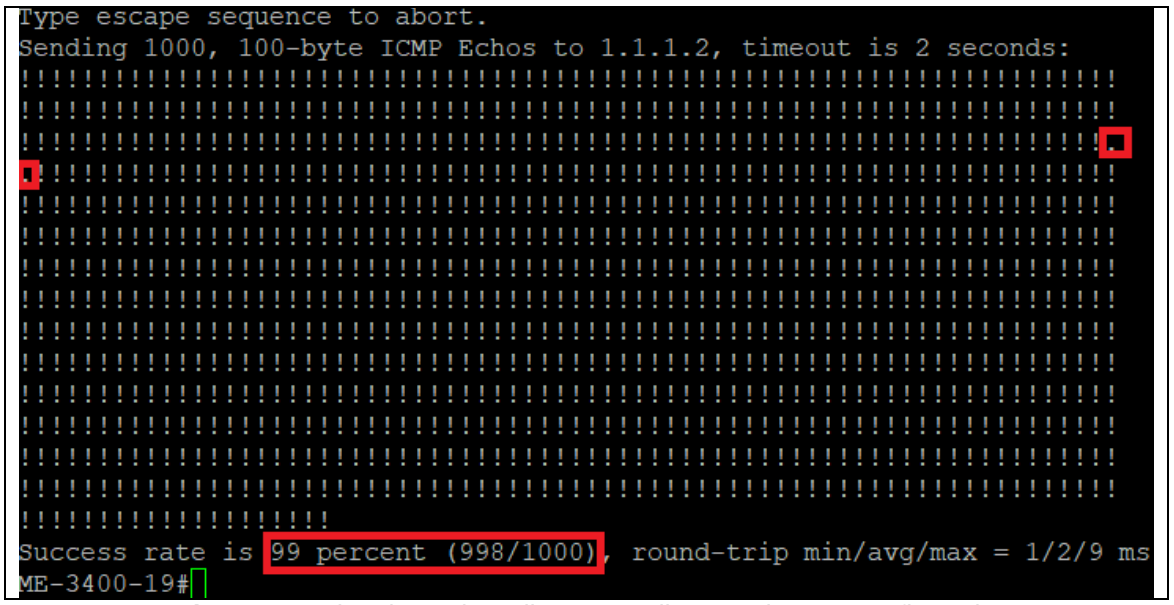


Figura 52 - Ping de equipo Cliente 1 a Cliente 2 sin FRR configurado

Como se puede ver en la Figura 52, ahora se han perdido dos pings, el doble que con FRR. Hay que indicar que en una red más grande y con más equipos esta diferencia sería aún mayor. No obstante, se puede validar que tanto TE como FRR funcionan correctamente.

4. Circuito EVPL vs EPL

En este capítulo se va a explicar en qué consisten los circuitos EVPL y se configurarán varios en la red para, posteriormente, validar si funcionan correctamente. También se va a revisar la transparencia de los protocolos de nivel 2 en los circuitos EPL (vistos en el capítulo anterior) y en los EVPL.

4.1 Transparencia de protocolos de nivel 2 en circuitos EPL

Para entender que son los protocolos de nivel 2, primero hay que explicar que, como describe el modelo OSI (*Internetwork Operating System*), los datos pasan por siete capas bien definidas durante una comunicación de un dispositivo a otro de una red [43].

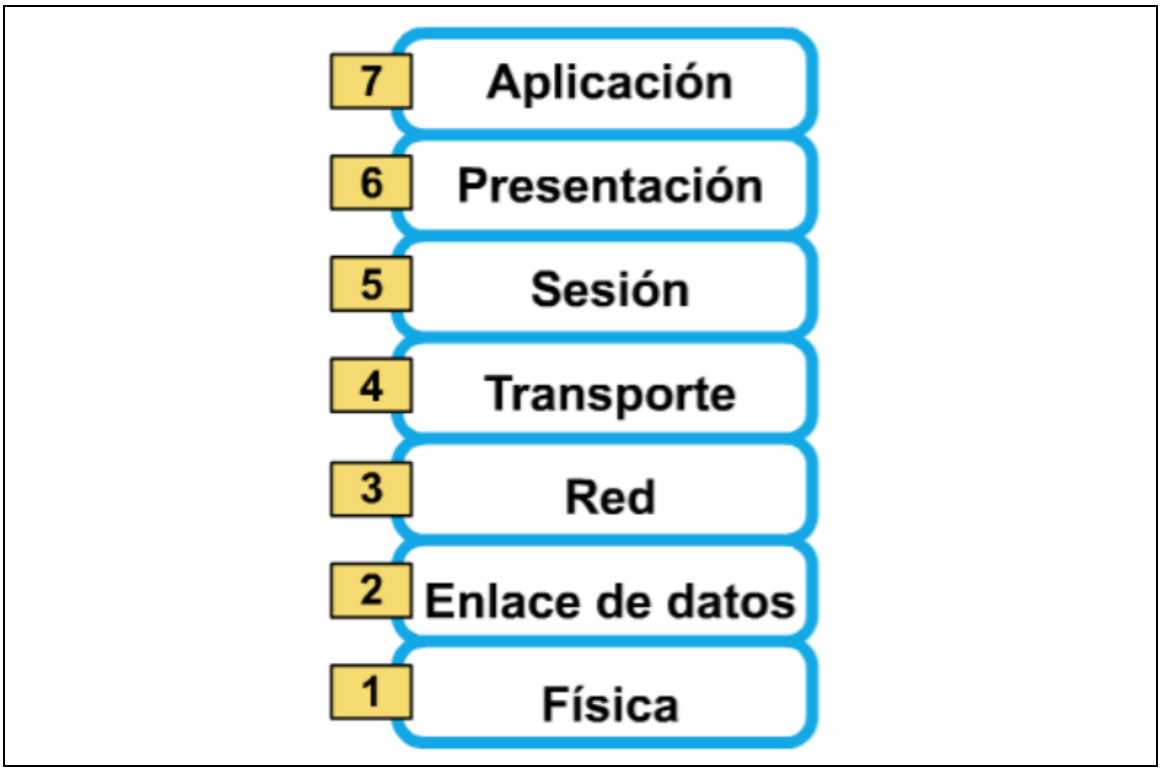


Figura 53 - Modelo OSI [44]

Como se puede ver en la Figura 53, la capa Física sería el nivel 1 del modelo OSI, la capa de Enlace de Datos el nivel 2, y así sucesivamente hasta llegar a la capa de Aplicación, que sería el nivel 7.

Por lo tanto, los protocolos de nivel 2 son aquellos que trabajan en la capa de Enlace de Datos del modelo OSI, que es la encargada de controlar la comunicación entre la capa Física y la capa de Red.

A continuación, se van a describir algunos ejemplos de protocolos de nivel 2 que actúan en la capa de Enlace de Datos [45][46]:

- **CDP** (*Cisco Discovery Protocol*): Ya descrito en apartados anteriores.
- **LLDP** (*Link Layer Discovery Protocol*): Ya descrito en apartados anteriores.

- **STP** (*Spanning Tree Protocol*): Es un protocolo que se encarga de deshabilitar enlaces redundantes en los equipos y así evitar bucles de nivel 2.
- **VTP** (*VLAN Trunking Protocol*): Es un protocolo propietario de Cisco que se encarga de propagar VLANs entre switches de una red para evitar repetir la misma configuración en todos los equipos.
- **LACP** (*Link Aggregation Control Protocol*): Es un protocolo que permite la agrupación de varios puertos físicos para formar un único canal lógico.
- **PAGP** (*Port Aggregation Protocol*): Este protocolo tiene la misma función que LACP, pero solo funciona con equipos Cisco.

Visto esto, es importante aclarar que, la transparencia en los protocolos de nivel 2 es el principal requisito de los circuitos EPL de la capa *Ethernet*. Esto significa que, cualquier trama enviada por el cliente, debe pasar por la red MPLS del operador de servicios como si de un cable físico de tratase.

Como se puede observar en la Figura 54, para validar que el circuito EPL creado es totalmente transparente con los protocolos de nivel 2, se va a configurar CDP y STP en los equipos de Cliente 1 (ME-3400-19) y Cliente 2 (ME-3400-18), para luego verificar que funcionan correctamente.

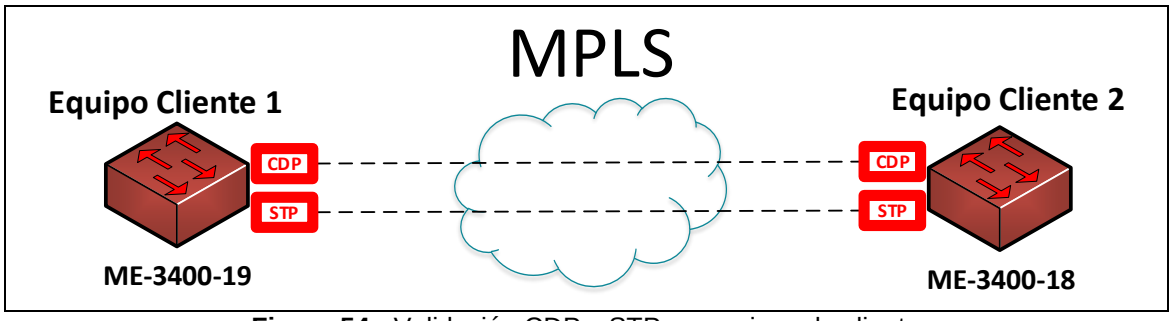


Figura 54 - Validación CDP y STP en equipos de cliente

Hay que recordar que al configurar el circuito sobre la red MPLS, se habilitó el comando *"l2protocol tunnel cdp stp vtp pagp lldp lacp udld"* para permitir que todos estos protocolos funcionasen a través del circuito.

CDP

Primero hay que habilitar el protocolo CDP en los equipos ME-3400-19 y ME-3400-18 mediante el comando "*cdp run*". Se debe aplicar en el modo de configuración global de los equipos.

```
ME-3400-19#configure terminal
ME-3400-19(config)#cdp run
```

Configuración 34 - Habilitar protocolo CDP ME-3400-19

```
ME-3400-18#configure terminal
ME-3400-18(config)#cdp run
```

Configuración 35 - Habilitar protocolo CDP ME-3400-18

En este caso no es necesario activar CDP también en las interfaces mediante el comando "*cdp enable*", ya que con el comando anterior queda ya habilitado en todos los puertos del equipo.

Por último, como se puede apreciar en las Figuras 55 y 56, se valida mediante el comando "*show cdp neighbors gigabitEthernet 0/2*" que los equipos se ven por CDP.

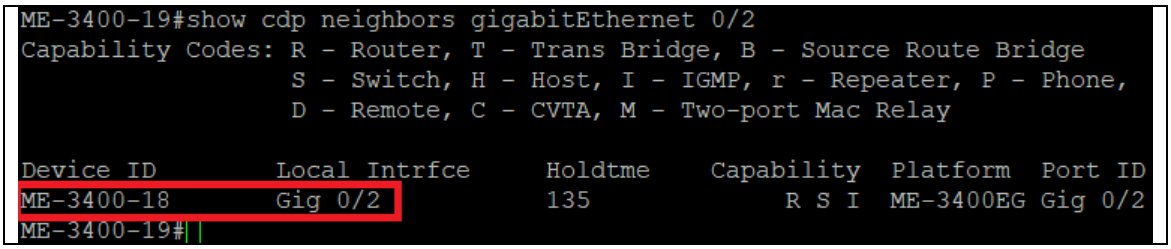


Figura 55 - Validación CDP equipo ME-3400-19

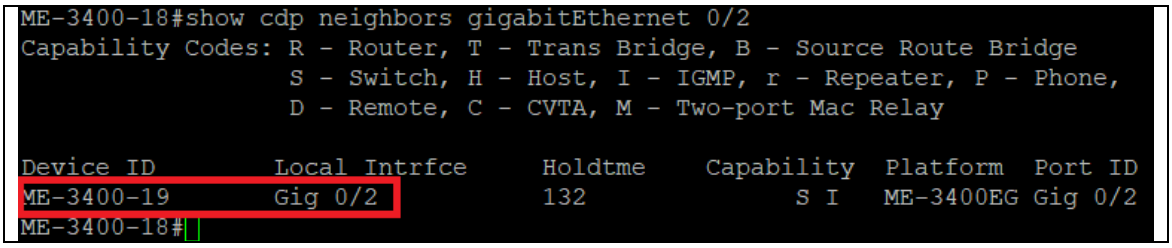


Figura 56 - Validación CDP equipo ME-3400-18

STP

Hay que habilitar el protocolo STP en los equipos ME-3400-19 y ME-3400-18 mediante el comando "*spanning-tree mode rapid-pvst*" [47]. Se debe aplicar en el modo de configuración global de los equipos.

```
ME-3400-19#configure terminal
ME-3400-19(config)#spanning-tree mode rapid-pvst
```

Configuración 36 - Habilitar protocolo STP ME-3400-19

```
ME-3400-18#configure terminal
ME-3400-18(config)#spanning-tree mode rapid-pvst
```

Configuración 37 - abilitar protocolo STP ME-3400-18

Se ha activado el modo *rapid-pvst* de STP, pero es necesario aclarar que para validar el correcto funcionamiento se puede configurar cualquier tipo de STP (CTP, MSTP, etc).

Por último, como se puede apreciar en las Figuras 57 y 58, se valida mediante el comando "*show spanning-tree*" que STP funciona correctamente en ambos equipos de cliente.

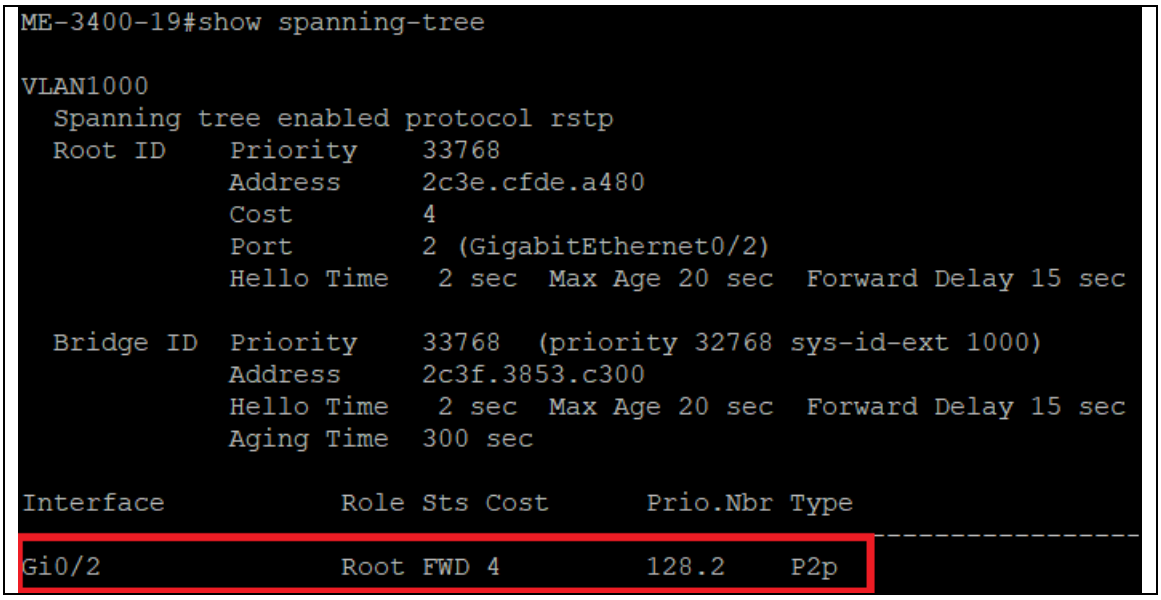


Figura 57 - Validación STP equipo ME-3400-19

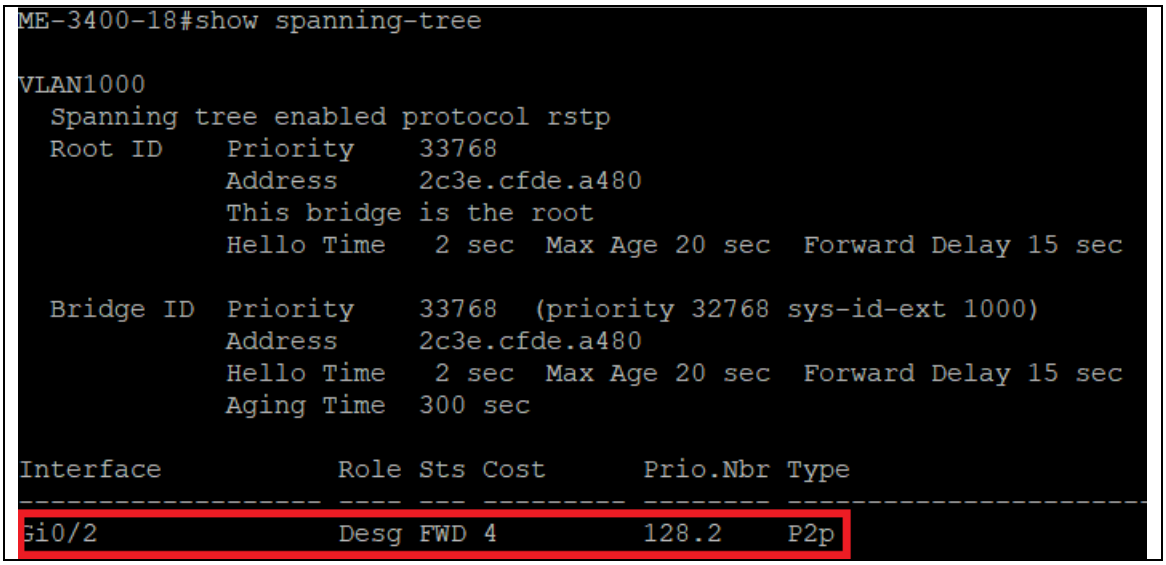


Figura 58 - Validación STP equipo ME-3400-18

En resumen, tras validar que los protocolos CDP y STP funcionan correctamente en los equipos Cliente 1 y Cliente 2, se puede confirmar que los protocolos de nivel 2 son transparentes en el circuito EPL creado en la red MPLS.

4.2 Circuito EVPL

En este apartado se va a explicar en qué consisten los circuitos EVPL y se configurarán varios sobre la red MPLS. Además, se validará que funcionan correctamente y se revisará si estos circuitos son transparentes en los protocolos de nivel 2.

4.2.1 ¿Qué es un circuito EVPL

Al igual que los circuitos EPL, los EVPL (*Ethernet Virtual Private Line*) también son servicios *Ethernet* definidos en MEF que forman parte de la categoría de los *E-Line*.

La diferencia frente a los circuitos EPL, es que en los EVPL se permite la configuración de más de un servicio sobre una misma interfaz, diferenciándolos con distintos etiquetados de VLAN. Por lo tanto, estos servicios soportan la multiplexación de servicios (punto a multipunto) y es idóneo para ahorrar interfaces de los equipos, ya que se permiten las agregaciones de varios servicios sobre un mismo puerto. Como contraprestación, se disminuye el grado de transparencia en los protocolos de nivel 2 [35].

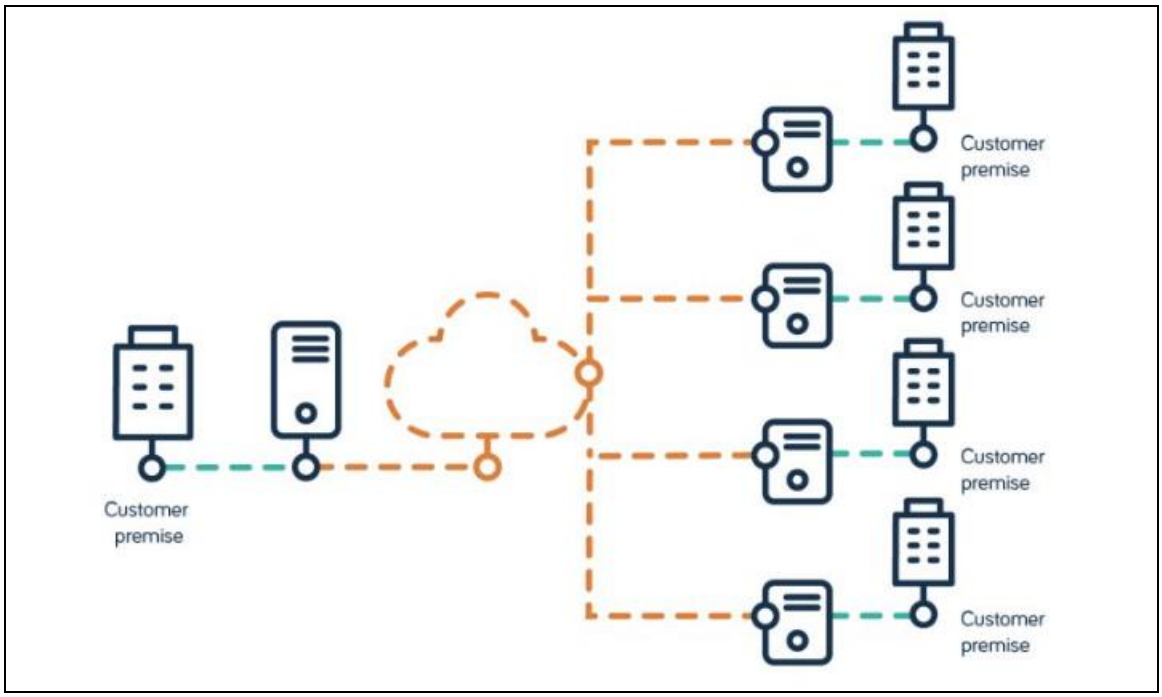


Figura 59 - Esquema servicio EVPL [35]

En la Figura 59 se puede ver el esquema de un servicio EVPL, donde la parte naranja sería la red del operador de servicios y la parte azul los equipos de cliente.

4.2.2 Configuración y validación de circuito EVPL

Como se ha explicado en el apartado anterior, los servicios EVPL permiten la opción de agregar más de un circuito sobre un mismo puerto *Ethernet*. Por lo tanto, en la Figura 60 se puede ver el camino de los dos circuitos que se van a configurar en la red MPLS.

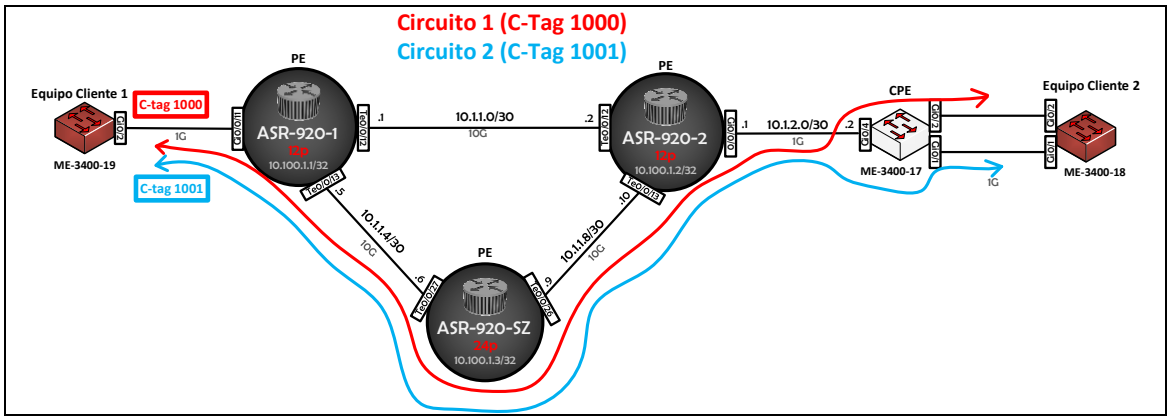


Figura 60 - Circuitos EVPL red MPLS

Uno de los circuitos (Circuito 1) va a ir del puerto Gi0/0/11 del equipo PE ASR-920-1 al puerto Gi0/2 del equipo CPE ME-3400-17 y el otro (Circuito 2), del puerto Gi0/0/11 del equipo PE ASR-920-1 al puerto Gi0/1 del equipo CPE ME-3400-17. Por lo tanto, ambos circuitos se agregarán en la interfaz Gi0/0/11 del equipo ASR-920-1, pero diferenciados por distinta VLAN:

- Circuito 1: VLAN 1000
- Circuito 2: VLAN 1001

Es importante aclarar que, para poder configurar el segundo circuito, se ha necesitado realizar una nueva conexión de cable RJ45 entre el puerto Gi0/1 del equipo CPE ME-3400-17 y el Gi0/1 del equipo ME-3400-18.

Una vez explicado el escenario de los dos circuitos y las nuevas conexiones realizadas, hay que indicar que en la configuración del Circuito 1 se va a aprovechar el circuito EPL creado en el anterior capítulo. Únicamente es necesario modificar la configuración del puerto Gi0/0/11 del equipo ASR-920-1, de manera que la entrega ahora sea etiquetada con la VLAN 1000 (*C-tag* 1000).

Circuito 1 EVPL
ASR-920-1
Para configurar el circuito 1 EVPL, hay que modificar el puerto Gi0/0/11 del equipo ASR-920-1 de una entrega por defecto (sin etiquetar) a una entrega etiquetada con la VLAN 1000.

Este cambio se realiza cambiando el comando "*encapsulation default*" por "*encapsulation dot1q 1000*", de manera que el equipo solo va a permitir el acceso en la *Service Instance* 3001 a las tramas que vengan marcadas con la VLAN 1000 [36].

```
ASR-920-1(config)#interface GigabitEthernet0/0/11
ASR-920-1(config-if)#service instance 3001 ethernet
ASR-920-1(config-if-srv)#encapsulation dot1q 1000
```

Configuración 38 - Circuito 1 EVPL Gi0/0/11 equipo ASR-920-1

Con este cambio realizado, el Circuito 1 EVPL ya estaría configurado.

Circuito 2 EVPL
Para crear el segundo circuito EVPL, se deben configurar los siguientes puertos y equipos:

- Puerto Gi0/0/11 equipo PE ASR-920-1 (VLAN 1001)
- Puerto Gi0/0/0 equipo PE ASR-920-2
- Puertos Gi0/4 y Gi0/1 equipo CPE ME-3400-17

ASR-920-1
Primero se configura el puerto Gi0/0/11 del equipo ASR-920-1 [36].

```
ASR-920-1(config)#interface GigabitEthernet0/0/11
```

```
ASR-920-1(config-if)#service instance 3002 ethernet
ASR-920-1(config-if-srv)#encapsulation dot1q 1001
ASR-920-1(config-if-srv)#l2protocol tunnel cdp stp vtp pagp lldp lacp udld
ASR-920-1(config-if-srv)#xconnect 10.100.2.1 1111112 encapsulation mpls pw-class 1-SZ-2
```

Configuración 39 - Circuito 2 EVPL Gi0/0/11 equipo ASR-920-1

Como se puede ver, se añade la nueva *Service Instance* 3002 con el comando "*encapsulation dot1q 1001*", de manera que solo actúe con las tramas que vengan marcadas con la VLAN 1001.

Además, como se está creando un nuevo circuito, es necesario vincularlo a un VC *(Virtual Circuit)* pseudowire distinto al del Circuito 1. En este caso se utilizará el VC 1111112.

ASR-920-2

A continuación, se configura el puerto Gi0/0/0 del equipo ASR-920-2 [36].

```
ASR-920-2(config)#interface GigabitEthernet0/0/0
ASR-920-2(config-if)#service instance 3002 ethernet
ASR-920-2(config-if-srv)#encapsulation dot1q 3002
ASR-920-2(config-if-srv)#rewrite ingress tag pop 1 symmetric
ASR-920-2(config-if-srv)#xconnect 10.100.1.1 1111112 encapsulation mpls pw-class 2-SZ-1
```

Configuración 40 – Circuito 2 EVPL Gi0/0/0 equipo ASR-920-2 SI 3002

En este caso es necesario crear la nueva *Service Instance* 3002 con el comando "*encapsulation dot1q 3002*", de manera que se añadirá la etiqueta 3002 a las tramas, para poder diferenciar el tráfico del circuito 2 al del resto. Es necesario también que el *xconnect* tenga el mismo ID del VC configurado en el otro extremo (1111112).

ME-3400-17

Por último, se deben configurar los puertos Gi0/4 y Gi0/2 del equipo CPE ME-3400-17. No obstante, primero hay que crear la nueva VLAN de tráfico del Circuito 2 en el modo de configuración global del equipo.

```
ME-3400-17(config)#vlan 3002
```

Configuración 41 - Crear VLAN Circuito 2 EVPL equipo ME-3400-17

Ahora ya se puede configurar la interfaz Gi0/4 del equipo CPE ME-3400-17, que va conectada directamente con el equipo PE ASR-920-2 [39].

```
ME-3400-17(config)#interface GigabitEthernet0/4
ME-3400-17(config-if)#switchport trunk allowed vlan add 3002
```

Configuración 42 - Gi0/4 equipo ME-3400-17 Circuito 2 EVPL

Es importante aclarar que, con el comando "*switchport trunk allowed vlan add 3002*", se está añadiendo la VLAN 3002 de tráfico del Circuito 2 al puerto *trunk* ya configurado en el capítulo anterior. Este puerto *trunk* ya tenía configurada la VLAN 3000 (gestión del equipo) y la VLAN 3001 (tráfico del Circuito 1) [48].

Por último, se configura la interfaz Gi0/1, que va conectada al equipo de Cliente 2 [40].

```
ME-3400-17(config)#interface GigabitEthernet0/1
ME-3400-17(config-if)#switchport access vlan 3002
ME-3400-17(config-if)#switchport mode dot1q-tunnel
ME-3400-17(config-if)#l2protocol-tunnel cdp
ME-3400-17(config-if)#l2protocol-tunnel lldp
ME-3400-17(config-if)#l2protocol-tunnel stp
ME-3400-17(config-if)#l2protocol-tunnel vtp
ME-3400-17(config-if)#l2protocol-tunnel point-to-point pagp
ME-3400-17(config-if)#l2protocol-tunnel point-to-point lacp
ME-3400-17(config-if)#l2protocol-tunnel point-to-point udld
```

Configuración 43 - Gi0/2 equipo ME-3400-17 Circuito 2 EVPL

En este caso, se configura la interfaz tipo *access,* ya que solamente se le asignará la VLAN de tráfico 3002 del Circuito 2 EVPL.

Una vez se ha aplicado la configuración correspondiente en todos los equipos de la red, ambos circuitos EVPL ya deberían de funcionar correctamente.

A través de la Figura 61, se va a revisar el procesamiento de las tramas del Circuito 1 EVPL, desde que salen del equipo de cliente, pasan por la red MPLS y acaban llegando al otro equipo de cliente.

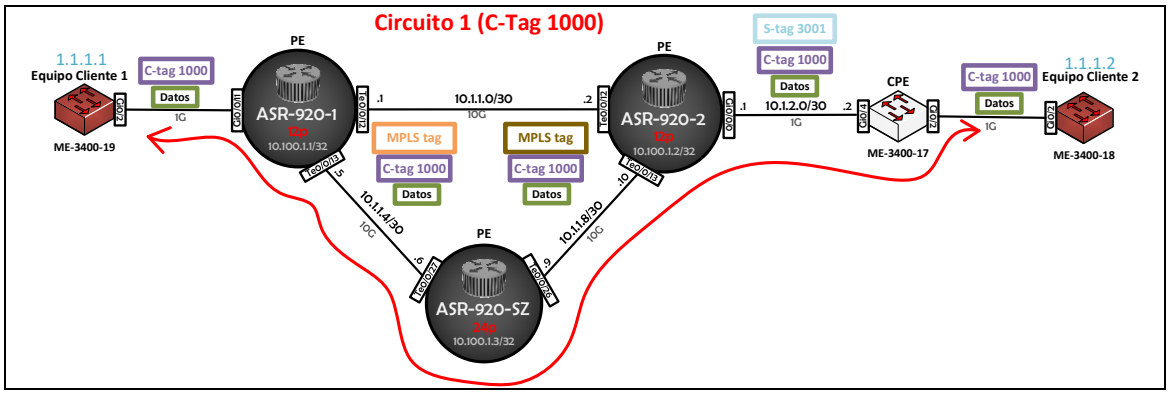


Figura 61 - Circuito 1 EVPL red MPLS especificando las tramas

Si se observa de izquierda a derecha, desde el equipo de Cliente 1 ME-3400-19 se puede ver como las tramas salen etiquetadas del equipo con *C-tag* (etiqueta de cliente) 1000. Cuando las tramas llegan al PE ASR-920-1, este les añade un *tag* MPLS justo antes de enviarlas por la red MPLS [41].

Una vez llega al equipo PE ASR-920-2, se elimina el *tag* MPLS y se añade el *S-tag* (etiqueta de servicio) 3001, de manera que cuando llegue al CPE ME-3400-17 sepa diferenciar el tráfico de este circuito con el de otros circuitos o el de gestión. Por último, el CPE elimina el *S-tag* y entrega las tramas en el equipo de Cliente 2 ME-3400-18 tal y como las recibió en origen, con *C-tag* 1000.

Observando nuevamente la Figura 61 se puede ver que cuando el tráfico va de derecha a izquierda tendría un proceso similar. Por otra parte, hay que aclarar que, como se puede ver en la Figura 62, en el Circuito 2 EVPL el proceso sería el mismo, pero con la modificación del *C-tag* (1001) y el *S-tag* (3002).

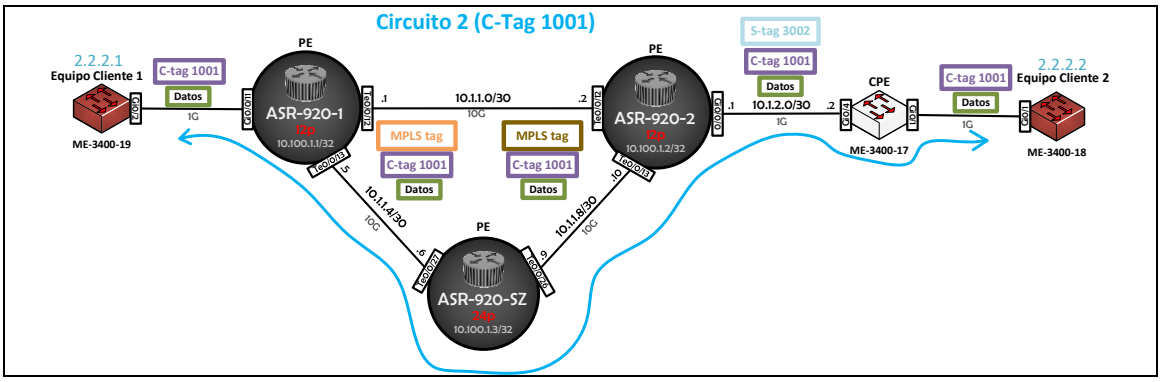


Figura 62 - Circuito 2 EVPL red MPLS especificando las tramas

Una vez visto cómo se comportan las tramas por toda la red, se va a validar que los dos circuitos EVPL funcionan correctamente. Para ello, se revisará si hay ping entre los equipos de cliente ME-3400-19 y ME-3400-18 en ambos circuitos y sentidos, configurando IPs del mismo rango en los equipos.

Para el Circuito 1, se va a modificar la VLAN 1000, ya configurada en la validación del circuito EPL del capítulo anterior. No obstante, se debe cambiar el tipo de interfaz de *access* a *trunk*, ya que ahora se configurarán dos VLANs por ese mismo puerto.

```
ME-3400-19(config)#interface GigabitEthernet0/2
ME-3400-19(config-if)#switchport mode trunk
ME-3400-19(config-if)#switchport trunk allowed vlan 1000
```

Configuración 44 - VLAN 1000 equipo cliente ME-3400-19 circuito 1 EVPL

```
ME-3400-18(config)#interface GigabitEthernet0/2
ME-3400-18(config-if)#switchport mode trunk
ME-3400-18(config-if)#switchport trunk allowed vlan 1000
```

Configuración 45 - VLAN 1000 equipo cliente ME-3400-18 circuito 1 EVPL

Para el Circuito 2, se crearán la VLAN 1001 y la SVI 1001 asignándole la IP que le corresponde. Seguidamente, se asigna la VLAN 1001 en modo *trunk* al puerto Gi0/2 del equipo ME-3400-19 y al puerto Gi0/1 del equipo ME-3400-18, ya que son los puertos que conectan contra los equipos del proveedor.

```
ME-3400-19(config)#vlan 1001

ME-3400-19(config)#interface vlan 1001
ME-3400-19(config-if)# ip address 2.2.2.1 255.255.255.0

ME-3400-19(config)#interface GigabitEthernet0/2
ME-3400-19(config-if)#switchport mode trunk
ME-3400-19(config-if)#switchport trunk allowed vlan add 1001
```

Configuración 46 - VLAN 1001 equipo cliente ME-3400-19 circuito 2 EVPL

```
ME-3400-18(config)#vlan 1001

ME-3400-18(config)#interface vlan 1001
ME-3400-18(config-if)# ip address 2.2.2.2 255.255.255.0

ME-3400-18(config)#interface GigabitEthernet0/1
ME-3400-18(config-if)#switchport mode trunk
ME-3400-18(config-if)#switchport trunk allowed vlan 1001
```

Configuración 47 - VLAN 1001 equipo cliente ME-3400-18 circuito 2 EVPL

En este momento ya se puede validar que hay ping entre los equipos, en ambos circuitos y sentidos.

```
ME-3400-19#ping 1.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
ME-3400-19#ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
ME-3400-19#
```

Figura 63 - Ping de equipo ME-3400-19 a ME-3400-18 circuitos EVPL

```
ME-3400-18#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
ME-3400-18#ping 1.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
ME-3400-18#
```

Figura 64 - Ping de equipo ME-3400-18 a ME-3400-17 circuitos EVPL

Por lo tanto, se valida que ambos circuitos EVPL funcionan correctamente.

4.2.3 Transparencia de protocolos de nivel 2 en circuitos EVPL

Para validar si los circuitos EVPL son transparentes en los protocolos de nivel 2, se va a configurar el protocolo CDP en los equipos de Cliente 1 (ME-3400-19) y Cliente 2 (ME-3400-18), para luego comprobar si funciona correctamente.

Hay que recordar que en apartados anteriores ya se configuró el protocolo CDP en estos equipos, por lo que se puede aplicar directamente el comando "*show cdp neighbors gigabitEthernet 0/2*" para comprobar si los equipos se ven por CDP.

```
ME-3400-19#show cdp neighbors gigabitEthernet 0/2
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
ME-3400-19#
```

Figura 65 - Validación CDP equipo ME-3400-19 servicios EVPL

```
ME-3400-18#show cdp neighbors gigabitEthernet 0/2
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
ME-3400-18#
```

Figura 66 - Validación CDP equipo ME-3400-18 servicios EVPL

Como se puede apreciar en las figuras anteriores, no aparecen vecinos por CDP en ninguno de los equipos. Por lo tanto, se puede confirmar que en los circuitos EVPL no funciona CDP (Figura 67) y, por lo tanto, estos circuitos no son transparentes en los protocolos de nivel 2.

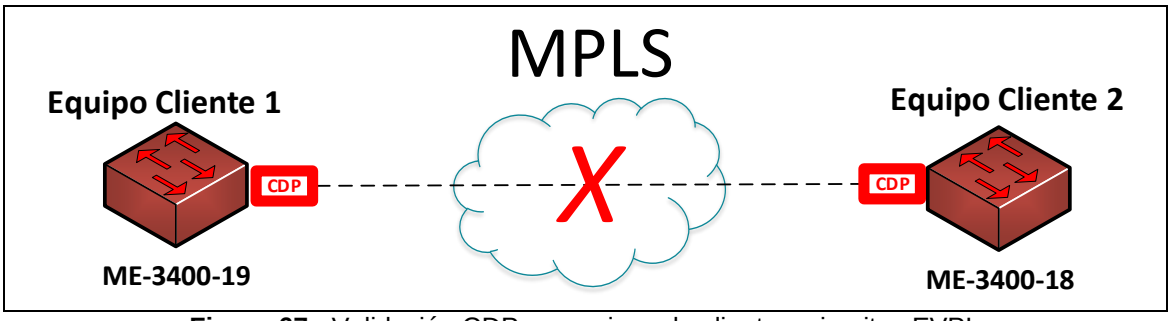


Figura 67 - Validación CDP en equipos de cliente y circuitos EVPL

Para entender el motivo de la no transparencia de los protocolos de nivel 2 en estos circuitos, es necesario conocer que los equipos siempre tienen configurada la VLAN nativa (VLAN 1 por defecto), que es utilizada para que algunos protocolos de nivel 2 se comuniquen con otros equipos. Esto quiere decir, que en el ejemplo anterior, CDP necesita de la VLAN 1 para poder funcionar correctamente [49].

Por este motivo, como algunos protocolos de nivel 2 necesitan de la VLAN 1 para comunicarse con otros equipos, implica que en el punto de agregación de varios circuitos EVPL no llegue a pasar las tramas etiquetadas con VLAN 1 y, por lo tanto, se pierda la transparencia de estos protocolos.

En la Figura 68 se puede ver esquemáticamente como CDP no llega al equipo de Cliente 1 porque la comunicación se pierde en el puerto de agregación de los dos servicios.

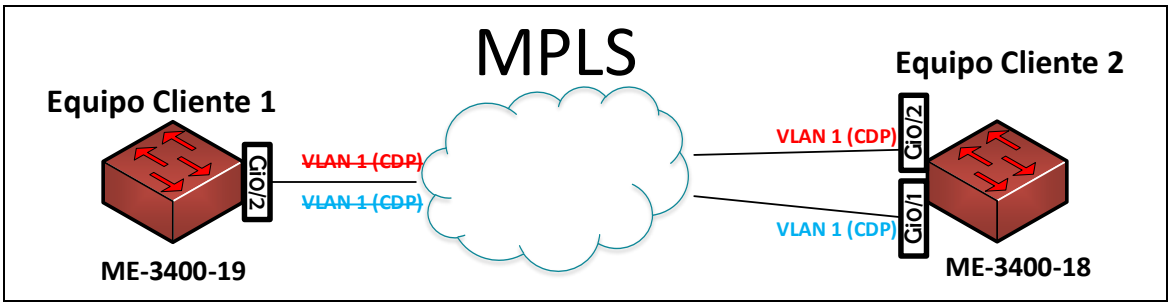


Figura 68 - VLAN 1 servicios EVPL

En resumen, los servicios punto a multipunto EVPL son idóneos para los clientes que buscan el ahorro de interfaces al permitir la agregación de más de un circuito sobre un mismo puerto. No obstante, si lo que se busca es un alto grado de transparencia en los protocolos de nivel 2, es mejor utilizar servicios punto a punto EPL.

5. Otras mejoras en la red MPLS

En este capítulo se va a describir y a configurar otros mecanismos de mejora de la red MPLS, como son los circuitos protegidos, *Dying Gasp* y la creación de *policies* para limitar el ancho de banda de los circuitos. Además, se comprobará que todas las mejoras aplicadas funcionan correctamente.

5.1 Circuitos protegidos

En este apartado se detallará la manera de dar redundancia a un circuito de la red MPLS mediante la configuración de circuitos protegidos con doble entrega. Para finalizar, se comprobará que la protección de los circuitos funciona correctamente.

5.1.1 ¿Cómo dar redundancia a un circuito en la red MPLS?

La red MPLS incluye la funcionalidad de redundancia de *pseudowire* L2VPN, que consiste en configurar un circuito con un punto de entrega de *backup*, de manera que permita que el servicio siga funcionando en el caso de que se detecte un fallo en algún punto del camino principal del circuito. Por lo tanto, esta función permite la recuperación de un circuito en el caso de que falle un PE (equipo o puerto) o el enlace entre un equipo CPE y PE [50].

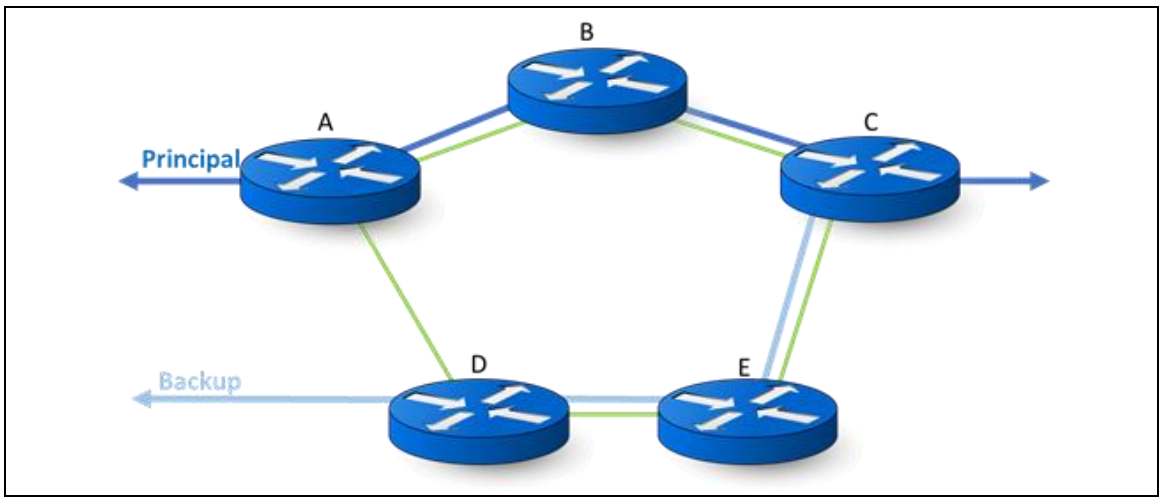


Figura 69 - Redundancia de *pseudowire* L2VPN

En la Figura 69 se puede ver un ejemplo de redundancia de *pseudowire* L2VPN, ya que existe un único circuito que dispone de un camino principal desde el equipo C al equipo A y un camino de *backup* desde el equipo C al equipo D. De esta manera, el circuito tiene un único puerto de agregación en el equipo C y dos puertos de entrega distintos, como principal en el equipo A y como *backup* en el equipo D.

Por lo tanto, si hubiera un fallo en alguno de los equipos o enlaces de la ruta principal, el circuito tomaría la ruta de *backup* y pasaría a entregarse desde el puerto asignado del equipo D sin afectar al servicio. No obstante, es importante aclarar que, si hubiera un problema en el equipo C, el circuito caería totalmente, ya que es el único punto coincidente de ambos caminos del circuito.

5.1.2 Configuración y validación de circuito protegido

En la Figura 70 se puede observar el circuito con redundancia de *pseudowire* L2VPN que se va a configurar.

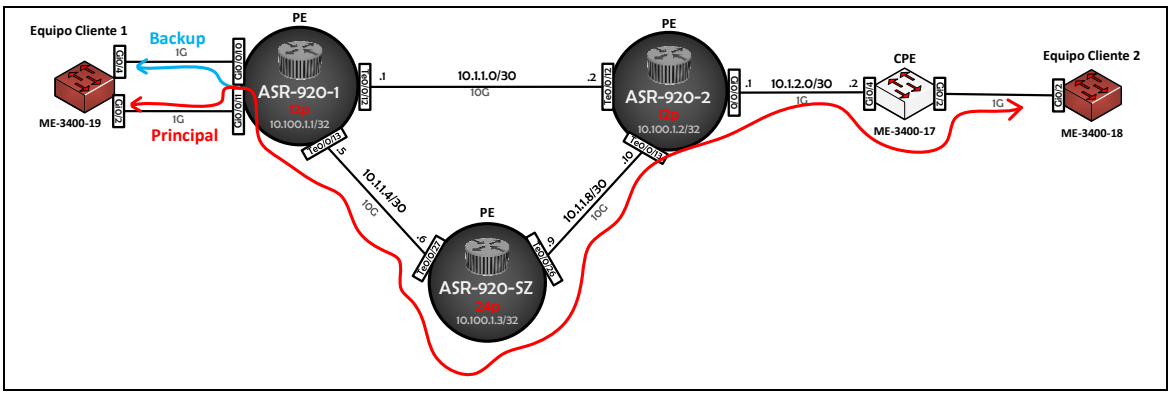


Figura 70 - Circuito protegido red MPLS

El circuito va a ir del puerto Gi0/2 del equipo CPE ME-3400-17 al puerto Gi0/0/11 del equipo PE ASR-920-1 como camino principal. Como camino de *backup* irá del puerto Gi0/2 del equipo CPE ME-3400-17 al puerto Gi0/0/10 del equipo PE ASR-920-1. De esta manera, si se produjera un fallo en el puerto Gi0/0/11 del equipo PE ASR-920-1, el circuito pasaría a entregarse de forma automática desde el puerto Gi0/0/10 del mismo equipo. Hay que añadir que en ambos extremos van conectados los equipos de cliente para poder validar que todo funciona correctamente.

Es importante aclarar que, para poder configurar el circuito con redundancia de *pseudowire* L2VPN, se ha necesitado realizar una nueva conexión entre el puerto Gi0/4 del equipo de Cliente 1 ME-3400-19 y el Gi0/0/10 del equipo PE ASR-920-1. Esta conexión se ha realizado mediante dos SFP GLC-SX-MMD y un latiguillo multimodo con conectores LC/PC.

Por lo tanto, para crear el circuito con redundancia de *pseudowire* L2VPN se van a realizar los siguientes pasos:

- Volver a configurar el Circuito 1 EVPL como EPL y eliminar el Circuito 2 EVPL del puerto Gi0/0/11 del equipo PE ASR-920-1
- Aplicar la configuración de "*backup peer"* al puerto Gi0/0/0 equipo PE ASR-920-2 y eliminar el Circuito 2 EVPL de ese mismo puerto.
- Configurar el puerto Gi0/0/10 del equipo PE ASR-920-1 como *backup* de entrega del circuito.

Gi0/0/11 del equipo PE ASR-920-1

Para pasar el Circuito 1 de EVPL a EPL, hay que modificar el puerto Gi0/0/11 del equipo ASR-920-1 de una entrega etiquetada por VLAN 1000 a una entrega sin etiquetar.

Este cambio se realiza modificando el comando "*encapsulation dot1q 1000"* por el comando "*encapsulation default*".

```
ASR-920-1(config)#interface GigabitEthernet0/0/11
ASR-920-1(config-if)#service instance 3001 ethernet
ASR-920-1(config-if-srv)#encapsulation default
```

Configuración 48 - Cambio a EPL Circuito 1 Gi0/0/11 equipo ASR-920-1

Además, se borra el Circuito 2 EVPL de esta interfaz.

```
ASR-920-1(config)#interface GigabitEthernet0/0/11
ASR-920-1(config-if)#no service instance 3002 ethernet
```

Configuración 49 - Borrado Circuito 2 EVPL Gi0/0/11 equipo ASR-920-1

Gi0/0/0 del equipo ASR-920-2

En primer lugar, se va a eliminar el circuito 2 EVPL de la interfaz Gi0/0/0 del equipo ASR-920-2

```
ASR-920-2(config)#interface GigabitEthernet0/0/0
ASR-920-2(config-if)#no service instance 3002 ethernet
```

Configuración 50 - Borrado Circuito 2 EVPL Gi0/0/0 equipo ASR-920-2

Para finalizar, hay que configurar en ese mismo puerto del equipo PE la redundancia de *pseudowire* L2VPN [50].

```
ASR-920-2(config)#interface GigabitEthernet0/0/0
ASR-920-2(config-if)#service instance 3001 ethernet
ASR-920-2(config-if-srv)#xconnect 10.100.1.1 1111111 encapsulation mpls pw-class 2-SZ-1
ASR-920-2(cfg-if-ether-vc-xconn)#backup peer 10.100.1.1 1111113 pw-class 2-SZ-1
```

Configuración 51 - Redundancia de pseudowire L2VPN Gi0/0/0 ASR-920-2

Como se puede observar, a diferencia de los circuitos configurados hasta ahora, en el *xconnect* se ha añadido un "*backup peer*" donde se especifica un VC *pseudowire* de respaldo, que solamente actuará en el caso de que falle el camino principal.

Gi0/0/10 del equipo PE ASR-920-1

Para finalizar, hay que configurar el puerto Gi0/0/10 del equipo PE ASR-920-1, que será un extremo del camino de *backup* y por donde se entregará el circuito en caso de que falle el camino principal [50].

```
ASR-920-1(config)#interface GigabitEthernet0/0/10
ASR-920-1(config-if)#service instance 3001 ethernet
ASR-920-1(config-if-srv)#encapsulation default
ASR-920-1(config-if-srv)#l2protocol tunnel cdp stp vtp pagp lldp lacp udld
ASR-920-1(config-if-srv)#xconnect 10.100.2.1 1111113 encapsulation mpls pw-class 1-SZ-2
```

Configuración 52 - Redundancia de pseudowire L2VPN Gi0/0/10 ASR-920-1

Como se puede observar, se configura igual que cualquier circuito EPL, pero en el *xconnect* hay que especificar el VC *pseudowire* configurado en el "*backup peer"* del equipo ASR-920-2 (1111113).

Una vez configurados todos los equipos, el circuito con redundancia de *pseudowire* L2VPN en la red MPLS ya debería de funcionar correctamente. Para comprobarlo, se realizarán las siguientes validaciones:

- Revisar que los *xconnects* están activos desde los equipos PE ASR-920-1 y ASR-920-2.
- Revisar que hay ping entre los equipos de cliente ME-3400-19 y ME-3400-18.
- Desactivar el puerto Gi0/0/11 del equipo PE ASR-920-1 para verificar que el circuito sigue funcionando por el puerto Gi0/0/10 de ese mismo equipo.

En primer lugar, se va a revisar el estado los *xconnects* desde los equipos PE ASR-920-1 y ASR-920-2. Para ello se va a utilizar el comando "*show xconnect all*" [50].

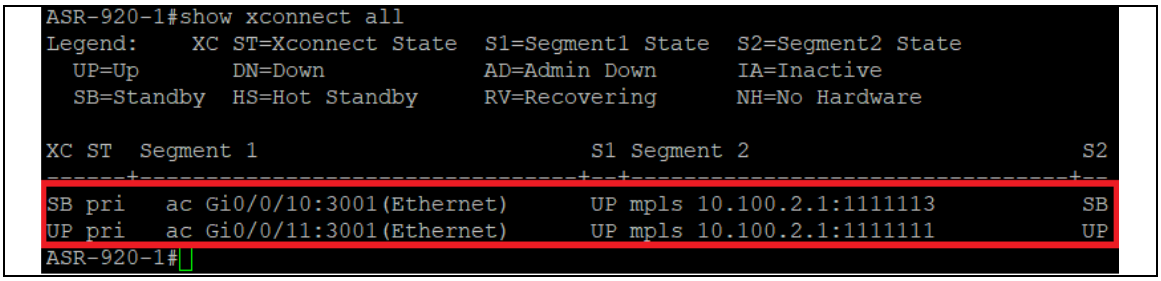


Figura 71 - Comando "show xconnect all" PE ASR-920-1 camino principal

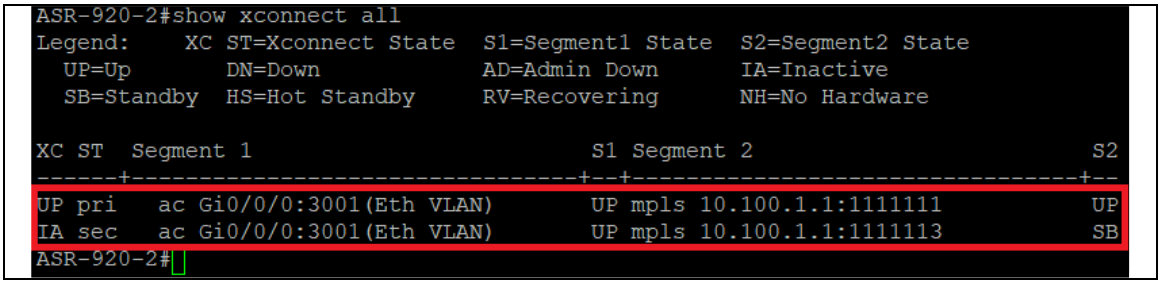


Figura 72 - Comando "show xconnect all" PE ASR-920-2 camino principal

Como se puede apreciar en las Figuras 71 y 72, el *pseudowire* VC con id 11111111 aparece en estado UP en ambos equipos, mientras que el VC con id 1111113 aparece en SB (*Standby*) en el equipo ASR-920-1 y en IA (*Inactive*) en el equipo ASR-920-2. Los estados observados son correctos cuando el circuito funciona por el camino principal. Más adelante veremos cómo cambian los estados en el momento que se produce un fallo en el camino principal y se activa el *backup*.

En segundo lugar, se va a revisar si hay ping entre los equipos de cliente ME-3400-19 y ME-3400-18 en ambos sentidos, configurando IPs del mismo rango en los equipos.

```
ME-3400-19(config)#interface gigabitEthernet 0/2
ME-3400-19(config-if)#no switchport trunk allowed vlan 1000,1001
ME-3400-19(config-if)#no switchport mode trunk
ME-3400-19(config-if)#switchport access vlan 1000
```

```
ME-3400-19(config)#interface gigabitEthernet 0/4
ME-3400-19(config-if)#switchport access vlan 1000
```

Configuración 53 - VLAN 1000 equipo cliente ME-3400-19 circuito protegido

```
ME-3400-18(config)#interface gigabitEthernet 0/2
ME-3400-18(config-if)#no switchport trunk allowed vlan 1000
ME-3400-18(config-if)#no switchport mode trunk
ME-3400-18(config-if)#switchport access vlan 1000
```

Configuración 54 - VLAN 1000 equipo cliente ME-3400-18 circuito protegido

Como se puede apreciar en ambas configuraciones, hay que volver a configurar los puertos Gi0/2 de ambos equipos en modo *access* con la VLAN 1000. Además, en el equipo ME-3400-19, que ahora tiene doble conexión contra el equipo PE ASR-920-1, también se debe pasar la VLAN 1000 por el puerto Gi0/4, de manera que cuando falle el camino principal (Gi0/2) el servicio siga funcionando por esta interfaz.

```
ME-3400-19#ping 1.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
ME-3400-19#
```

Figura 73 - Ping de equipo ME-3400-19 a ME-3400-18 circuito protegido

```
ME-3400-18#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
ME-3400-18#
```

Figura 74 - Ping de equipo ME-3400-18 a ME-3400-19 circuito protegido

Se valida en las Figuras 73 y 74 que el ping en ambos sentidos funciona correctamente.

Para finalizar, se va a dejar un ping continuo de 1000 repeticiones (*ping 1.1.1.2 repeat 1000*) desde el equipo de Cliente 1 ME-3400-19 hacia el equipo de Cliente 2 ME-3400-18, para posteriormente desactivar el puerto Gi0/0/11 del equipo PE ASR-920-1. De esta manera, se verificará que el circuito sigue funcionando por el puerto Gi0/0/10 de ese mismo equipo.

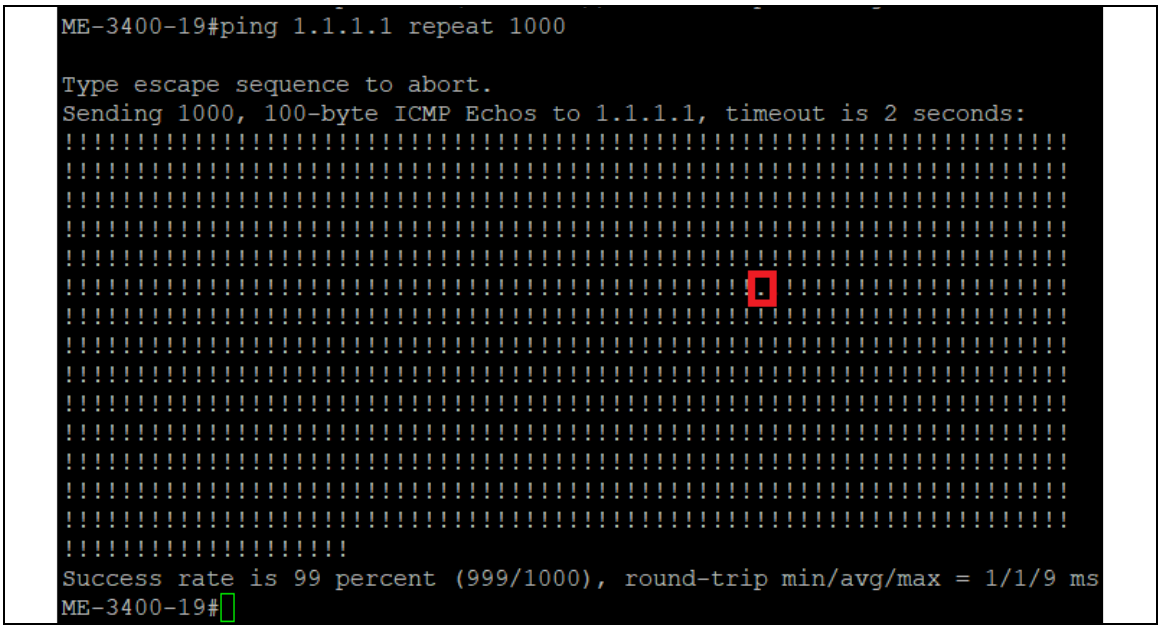


Figura 75 - Verificación circuito protegido equipo ME-3400-19

Como se puede observar en la Figura 75, únicamente se ha perdido un ping y el servicio ha seguido funcionando. Además, ahora que el circuito funciona por el camino de *backup*, se vuelven a revisar los *xconnects* desde los equipos PE ASR-920-1 y ASR-920-2 mediante el comando "*show xconnect all*" [50].

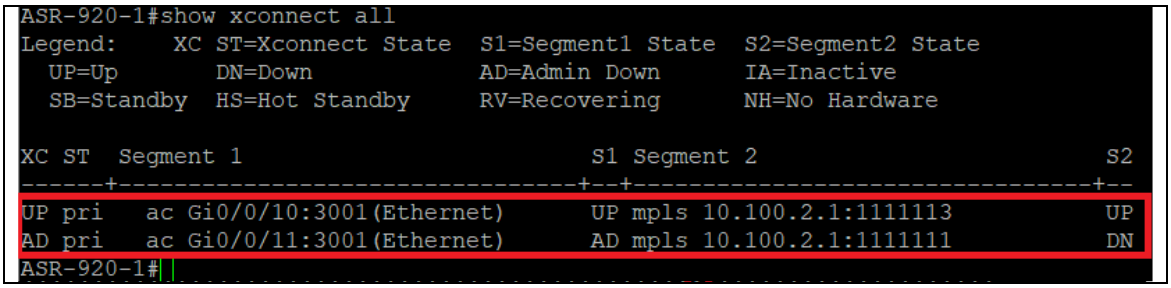


Figura 76 - Comando "show xconnect all" PE ASR-920-1 camino backup

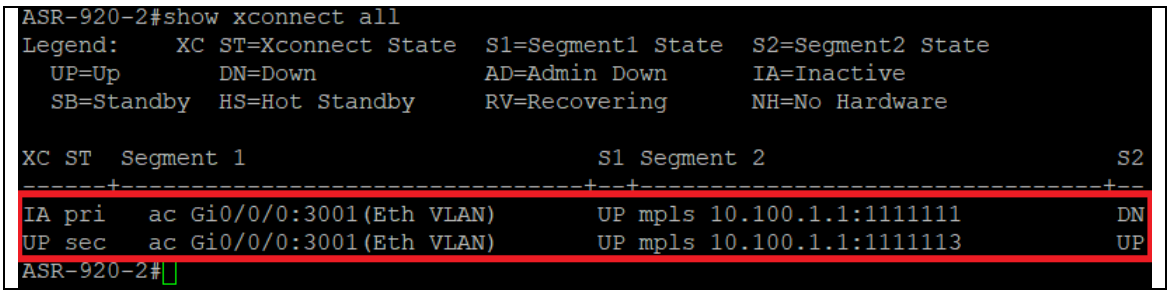


Figura 77 - Comando "show xconnect all" PE ASR-920-2 camino backup

En las Figuras 76 y 77 se puede apreciar como ahora aparecen en UP los pseudowires VC con id 1111113 (camino *backup*) en ambos equipos. Por lo que podemos validar que la configuración del circuito con redundancia de *pseudowire* L2VPN funciona correctamente.

5.2 *Dying Gasp*

En este apartado se va a configurar y a explicar la funcionalidad *Dying Gasp* para mejorar la detección de posibles incidencias en el equipo CPE. Para finalizar, se validará que funciona correctamente.

5.2.1 ¿Qué es el *Dying Gasp*?

El *Dying Gasp* es un mensaje que envían algunos dispositivos para avisar a sus equipos vecinos, o a un sistema de monitorización, de que se ha quedado sin energía eléctrica.

Esta funcionalidad es compatible con todo tipo de interfaces (*FastEthernet*, *GigabitEthernet,* etc.) y funciona gracias a que los equipos disponen de un condensador para realizar una reserva de alimentación temporal, de 10 a 20 milisegundos de duración, de manera que cuando el equipo se apague se pueda generar el mensaje *dying-gasp* [51].

Es importante incorporar esta funcionalidad en la red, ya que ofrece información instantánea de si un equipo ha caído por falta de alimentación eléctrica o porque se ha producido un corte en la fibra óptica que lo conecta. Por lo tanto, facilita mucho el *troubleshooting* (proceso de diagnóstico del origen de un problema) y la solución de una incidencia, puesto que desde el primer momento se conoce el origen del problema.

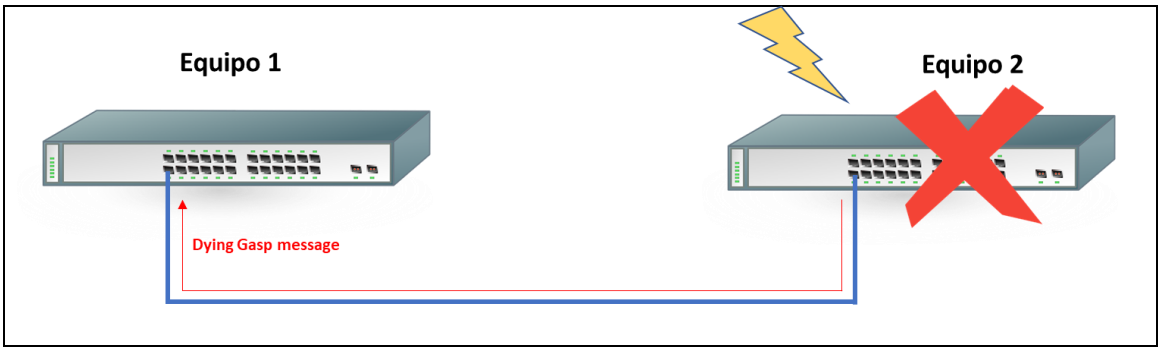


Figura 78 - *Dying Gasp* – Corte eléctrico

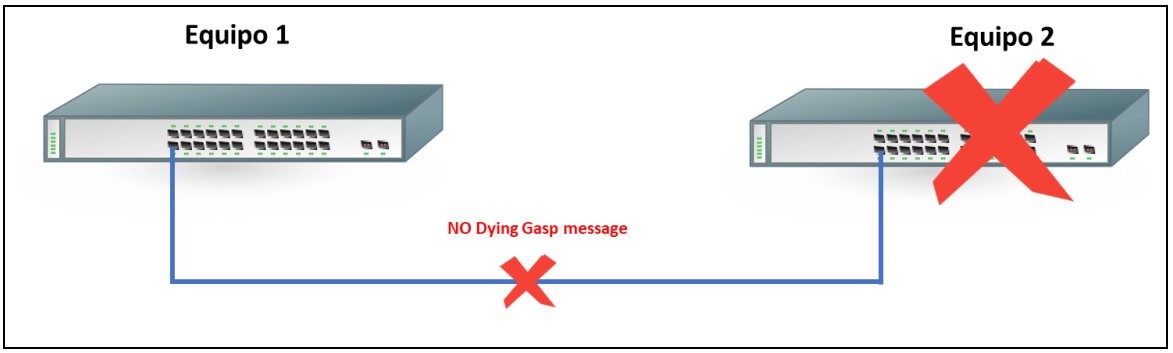


Figura 79 - *Dying Gasp* – Corte de fibra

En las figuras anteriores se puede ver el funcionamiento de forma gráfica. En la Figura 78, se puede observar que el Equipo 2 ha caído por falta de alimentación eléctrica, pero ha podido enviar un mensaje *dying-gasp* al Equipo 1 antes de caer. No obstante, en la Figura 79, el Equipo 2 cae por un corte de fibra entre ambos equipos, por lo que no ha enviado el mensaje *dying-gasp.*

Por lo tanto, si el técnico que monitoriza la red accede al Equipo 1, podrá saber el motivo de la caída del Equipo 2 y actuar en consecuencia.

5.2.2 Configuración y validación del *Dying Gasp*

Como se ha explicado en el apartado anterior, el *Dying Gasp* proporciona información instantánea de si un equipo ha caído por problemas eléctrico. Por lo tanto, como se puede ver en la Figura 80, se va a configurar en el equipo CPE ME-3400-17, que simula estar ubicado en la sede de cliente, y para que envíe el mensaje *dying-gasp* al equipo PE ASR-920-2 si tuviera algún problema eléctrico para facilitar el *troubleshooting* en el caso de una incidencia.

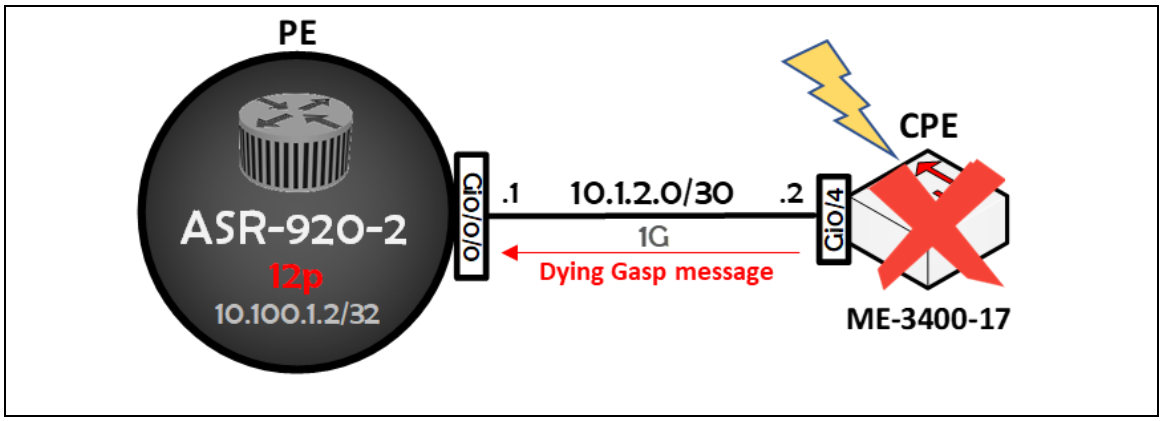


Figura 80 - *Dying Gasp* CPE ME-3400-17

Para que el *Dying Gasp* funcione se deben configurar los siguientes equipos:

- CPE ME-3400-17
- PE ASR-920-2

ME-3400-17

Hay que aplicar configuración en el modo de configuración global y en el puerto Gi0/4 del equipo [51].

```
ME-3400-17(config)#dying-gasp primary ethernet-oam secondary snmp-trap

ME-3400-17(config)#interface GigabitEthernet0/4
ME-3400-17(config-if)#ethernet oam
```

Configuración 55 - *Dying Gasp* equipo CPE ME-3400-17

El comando "*dying-gasp primary ethernet-oam secondary snmp-trap"* se aplica en el modo de configuración global del equipo para activar la notificación de *dying-gasp* a través de *ethernet-oam* (*Ethernet Operations, Administration, and Management*) como primario y *snmp-trap* (*Simple Network Management Protocol*) como secundario. Hay que aclarar que el comando obliga a añadir el método secundario, aunque en la práctica no se va a utilizar porque no se dispone de un equipo de monitorización que reciba los mensajes SNMP [51].

En este caso, los mensajes *dying-gasp* se enviarán por un *link* OAM configurado entre el equipo CPE ME-3400-17 y el PE ASR-920-2. Por lo tanto,

se aplica el comando "*ethernet oam*" dentro de la interfaz correspondiente para permitir la supervisión del enlace *Ethernet* [52].

ASR-920-2
También se debe configurar el equipo PE ASR-920-2 [51].

```
ASR-920-2(config)#interface GigabitEthernet0/0/0
ASR-920-2(config-if)#ethernet oam
ASR-920-2(config-if)#service instance 1 ethernet
ASR-920-2(config-if-srv)#encapsulation untagged
ASR-920-2(config-if-srv)#bridge-domain 1
```

Configuración 56 - *Dying Gasp* equipo PE ASR-920-2

Al igual que se ha hecho con el equipo CPE, se debe activar el *link* OAM aplicando el comando "*ethernet oam*" dentro de la interfaz Gi0/0/0. Además, en este caso se debe añadir la *Service Instance* 1 con los comandos "*encapsulation untagged*" y "*bridge-domain 1"* para que las tramas *Ethernet* sin etiquetar entren por esta interfaz (VLAN nativa) [53], ya que los mensajes *dying-gasp* sobre el *link* OAM necesitan de VLAN nativa para la comunicación.

Una vez se ha configurado *Dying Gasp* en los dos equipos se van a realizar las siguientes comprobaciones:

- Reiniciar el equipo CPE ME-3400-17 para verificar que el equipo PE ASR-920-2 recibe el mensaje *dying-gasp.*
- Tirar el enlace entre ambos equipos para verificar que el equipo PE ASR-920-2 ahora no recibe el mensaje *dying-gasp.*

Como se puede observar en la Figura 81, tras reiniciar el equipo CPE ME-3400-17, el equipo ASR-920-2 ha recibido varios mensajes *dying-gasp* conforme el CPE ha perdido alimentación eléctrica. Además, uno de ellos te detalla que el problema se ha debido a un reinicio del equipo remoto.

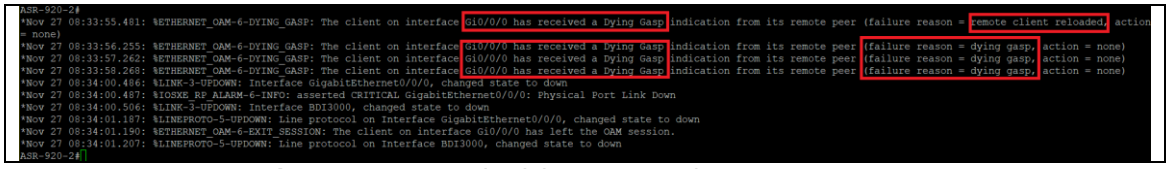


Figura 81 - Mensaje *dying-gasp* equipo PE ASR-920-2

En la Figura 82, tras tirar el enlace entre ambos equipos, se puede observar como el equipo ASR-920-2 no ha recibido ningún mensaje *dying-gasp*.

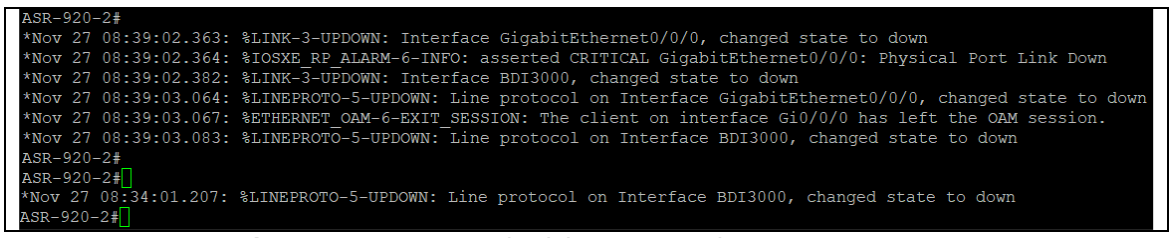


Figura 82 - NO mensaje *dying-gasp* equipo PE ASR-920-2

Por lo tanto, se puede afirmar que *Dying Gasp* funciona correctamente.

5.3 *Policies*

En este apartado se va a configurar y a explicar la funcionalidad de una *policy* para limitar el ancho de banda de un circuito. Para finalizar, se comprobará que funciona correctamente inyectando tráfico por un extremo del circuito.

5.3.1 ¿Cómo limitar el ancho de banda de los circuitos?

Es necesaria la limitación del ancho de banda de los circuitos configurados sobre una red MPLS, ya que no siempre los clientes van a precisar de circuitos con la capacidad máxima que ofrecen los puertos utilizados para interconectar con el proveedor de servicios (normalmente de 1 Gbps). Además, es una manera de disponer de un amplio catálogo de servicios, que puede variar de 1 Mbps hasta 1 Gbps.

Las limitaciones de ancho de banda de los circuitos se realizan mediante la aplicación de *policies* y es importante conocer los siguientes términos para entender cómo funcionan [54]:

- **CIR** (*Committed Information Rate*): Es el ancho de banda mínimo garantizado.
- **EIR** (*Excess Information Rate*): Especifica la cantidad de ancho de banda que se puede permitir sin garantizar. Debe ser un valor mayor o igual que el CIR.
- **PIR** (*Peak Information Rate*): Es el ancho de banda máximo permitido sin garantizar. Es la suma del CIR + EIR.

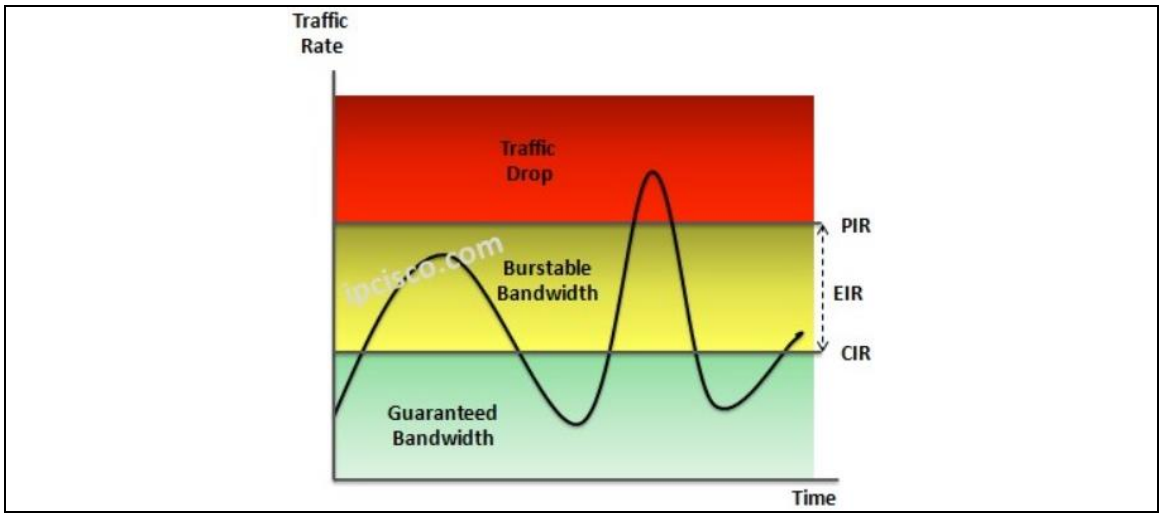


Figura 83 - CIR, PIR y EIR [54]

En la Figura 83 se puede ver que el tráfico por debajo del CIR está asegurado y el tráfico por encima del PIR es descartado. Por otra parte, entre el CIR y el PIR está el EIR, que es el tráfico no asegurado y que, permitirá o descartará el tráfico, dependiendo de la congestión de la red en un momento puntual.

5.3.2 Configuración y validación de una *policy*

En la Figura 84 se puede observar el escenario para este apartado, donde en los extremos de la red se han cambiado los dos equipos de cliente por dos PCs Linux Centos 7 con la aplicación iPerf3 instalada, que más adelante se detallará el caso de uso. Hay que destacar que el PC1 será el servidor iPerf3, ya que recibirá el tráfico que inyectará el PC2 (cliente iPerf3).

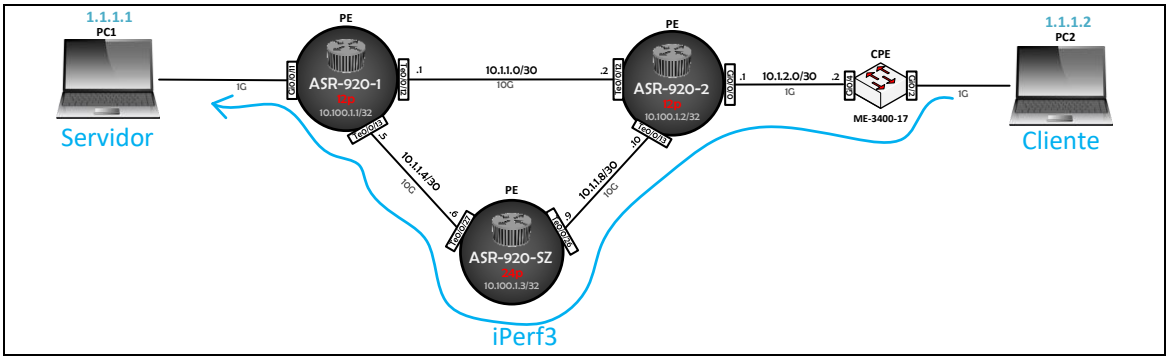


Figura 84 - *Policies* en red MPLS

Se van a configurar *policies* para limitar el tráfico a 100 Mbps, donde el CIR y el PIR tendrán el mismo valor. Por lo tanto, no se aplicará EIR y todo el tráfico permitido va a ser garantizado. Además, las *policies* se aplicarán en ambos extremos de la red en modo *input*, de manera que se limitará el tráfico de entrada a 100 Mbps en cada uno de estos puntos.

Por lo tanto, es necesario configurar los siguientes puertos/equipos:

- Puerto Gi0/0/11 del equipo PE ASR-920-1
- Puerto Gi0/2 del equipo CPE ME-3400-17

Puerto Gi0/0/11 del equipo PE ASR-920-1

Hay que configurar la interfaz Gi0/0/11 del equipo PE ASR-920-1.

```
ASR-920-1(config)#policy-map POLICY_100_Mbps
ASR-920-1(config-pmap)#class class-default
ASR-920-1(config-pmap-c)#police cir 100000000 pir 100000000 conform-action set-mpls-exp-imposition-transmit 1 exceed-action drop violate-action drop

ASR-920-1(config)#interface GigabitEthernet0/0/11
ASR-920-1(config-if)#service instance 3001 ethernet
ASR-920-1(config-if-srv)#service-policy input POLICY_100_Mbps
```

Configuración 57 - *Policy* puerto Gi0/0/11 equipo PE ASR-920-1

A continuación, se explica la función de los comandos aplicados [55]:

- **"*policy-map POLICY_100_Mbps*":** En modo de configuración global se crea una policy que se ha nombrado como "POLICY_100_Mbps" para que sea fácilmente identificada.

- **"*class class-default*":** Con este comando se especifica que la clase de la *policy* que se va a crear es la de por defecto. Con la aplicación de la clase por defecto se asegura que todo el tráfico va a ser clasificado.
- **"p*olice cir 100000000 pir 100000000 conform-action set-mpls-exp-imposition-transmit 1 exceed-action drop violate-action drop":*** Con este comando se establecen los umbrales para el tráfico del circuito (CIR=PIR=100 Mbps). Además, se marcan las tramas con el campo EXP=1 para identificar cual va a ser el tráfico asegurado. El tráfico superior a 100 Mbps quedará descartado.

Por último, se ha aplicado el comando "*service-policy input POLICY_100_*Mbps" dentro de la *Service Instance* de tráfico del circuito (SI 3001) y en modo *input,* para limitar solamente el tráfico de entrada a la red MPLS.

Puerto Gi0/2 del equipo CPE ME-3400-17

También hay que configurar el otro extremo, la interfaz Gi0/2 del equipo CPE ME-3400-17 [55].

```
ME-3400-17(config)#policy-map POLICY_100_Mbps
ME-3400-17(config-pmap)#class class-default
ME-3400-17(config-pmap-c)#police cir 100000000
ME-3400-17(config-pmap-c-police)#conform-action set-cos-transmit 1
ME-3400-17(config-pmap-c-police)#exceed-action drop

ME-3400-17(config)#interface GigabitEthernet0/2
ME-3400-17(config-if)#service-policy input POLICY_100_Mbps
```

Configuración 58 - *Policy* puerto Gi0/2 equipo CPE ME-3400-17

La configuración de este equipo es similar que la del PE ASR-920-1, pero con la diferencia de que solamente es necesario indicar el umbral CIR para el tráfico (CIR=100 Mbps). Además, en este equipo se marcan las tramas con el campo CoS=1 (*Classes of Service = 1*) para diferenciar que tráfico es el asegurado. Al igual que en el equipo PE, se aplica la *policy* en la interfaz en modo *input,* para limitar solamente el tráfico de entrada a la red MPLS.

Una vez se han configurado las *policies* en ambos extremos, se van a realizar las siguientes comprobaciones mediante un PC Linux Centos 7 conectado a cada extremo del circuito (revisar Figura 84):

- Confirmación de que hay ping extremo a extremo entre los PCs Linux.
- Inyectar 500 Mbps de tráfico (mediante *iPerf3*) de un PC a otro para confirmar que el tráfico queda limitado a 100 Mbps.
- Eliminar las *policies* y repetir la inyección de 500 Mbps de tráfico para confirmar que ahora no hay limitación de tráfico.

Para confirmar que hay ping extremo a extremo entre los PCs Linux, se configuran IPs de la misma red en ambos PCs para verificar que funciona correctamente en los dos sentidos.

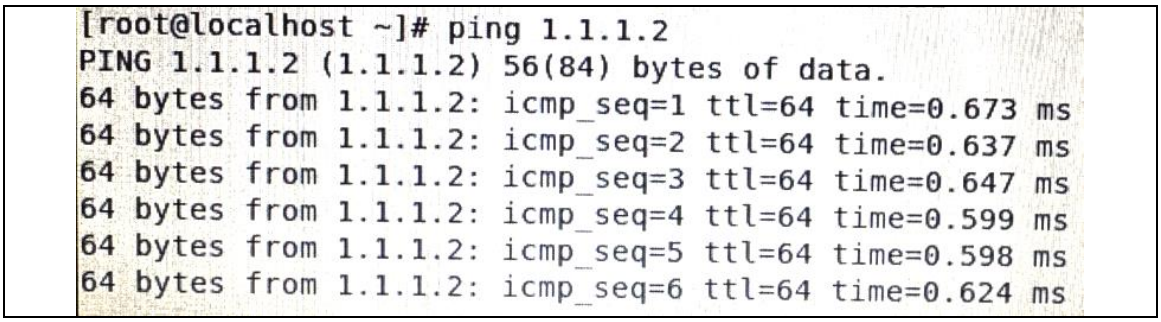


Figura 85 - *Ping* PC1 a PC2

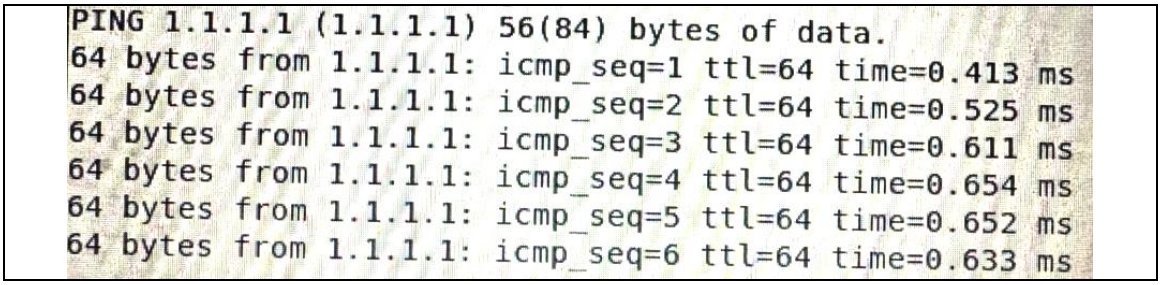


Figura 86 - Ping PC2 a PC1

Ahora se van a inyectar 500 Mbps de tráfico de un PC a otro mediante *iPerf3,* de manera que se podrá confirmar que el tráfico queda limitado a 100 Mbps. *iPerf3* es la versión 3 de una herramienta para OS *Linux* que permite medir activamente el ancho de banda de una red [56]. Se debe configurar un PC como cliente (PC2) para inyectar tráfico y el otro PC como servidor (PC1) para recibir el tráfico.

En la Figura 87 se puede observar el comando "*iperf3 -c 1.1.1.1 -b 500M -t 10000*" que se ha aplicado en el PC2.

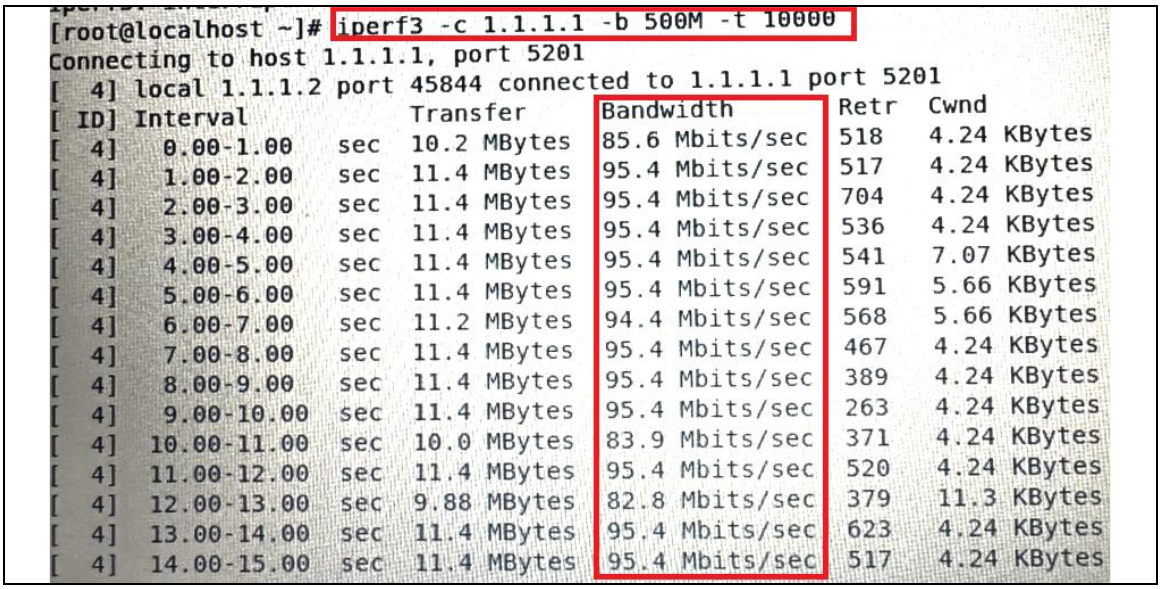


Figura 87 - Modo cliente iPerf3 PC2 con *policies*

A continuación explicamos los diferentes valores aplicados en el comando [57]:

- **-c**: Indica que el equipo va a ser cliente

- **1.1.1.1**: La IP destino del servidor (PC1) a la que va dirigido el tráfico
- **-b 500M**: Se indica que se inyectan 500 Mbps de tráfico
- **-t 10000**: Se indica que se enviarán 10000 repeticiones.

Por otra parte, en la Figura 88 se observa el comando "*iperf3 -s*" aplicado en el PC1. Se especifica que va a ser el equipo servidor mediante la opción "*-s*" [57].

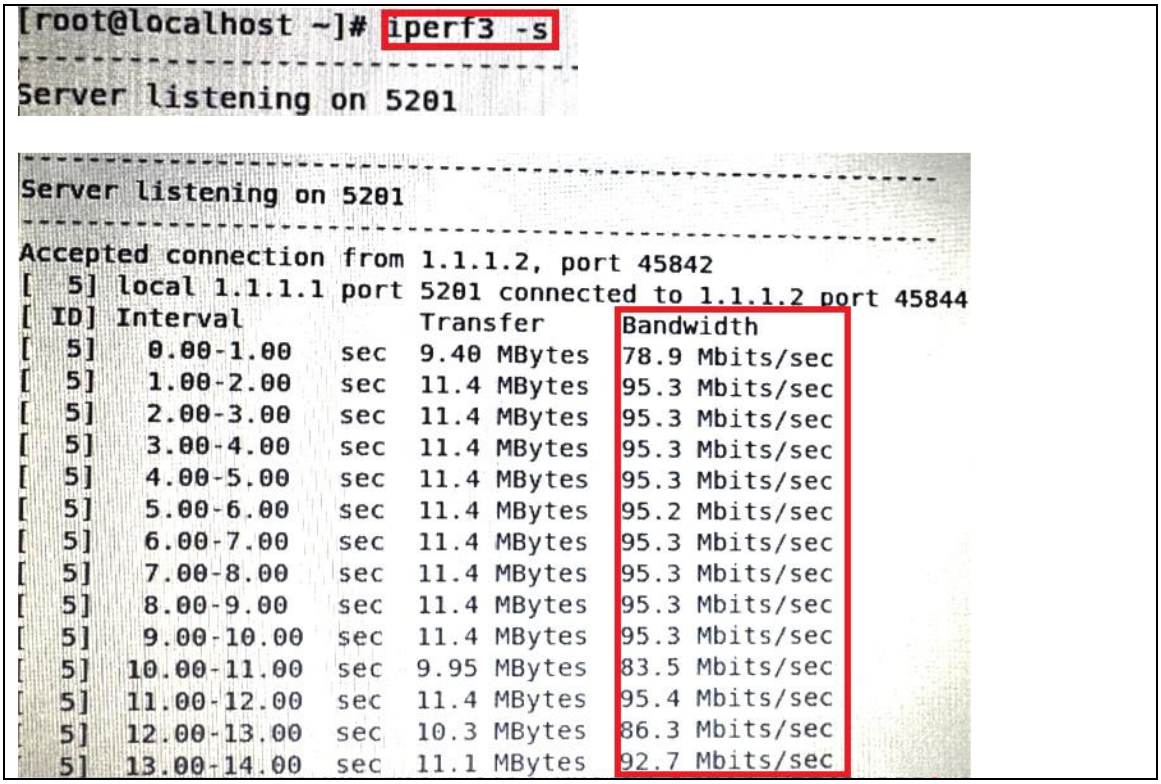


Figura 88 - Modo servidor iPerf3 PC1 con *policies*

Como se puede apreciar en las dos figuras anteriores, aunque inyectamos 500 Mbps desde el PC2 al PC1, en el *Bandwidth* solo se están cursando cerca de 100 Mbps.

Por último, se va a repetir la misma prueba eliminando las *policies* del equipo PE ASR-920-1 y el CPE ME-3400-17.

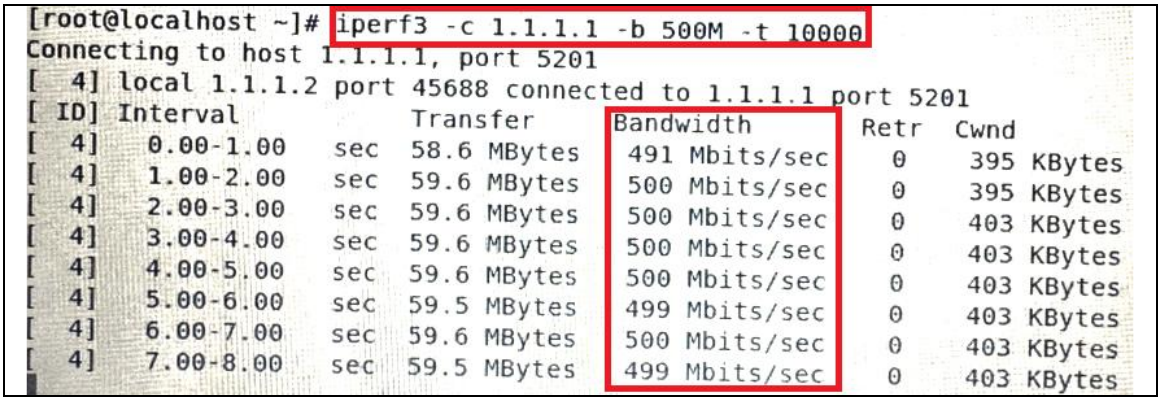


Figura 89 - Modo cliente iPerf3 PC2 sin *policies*

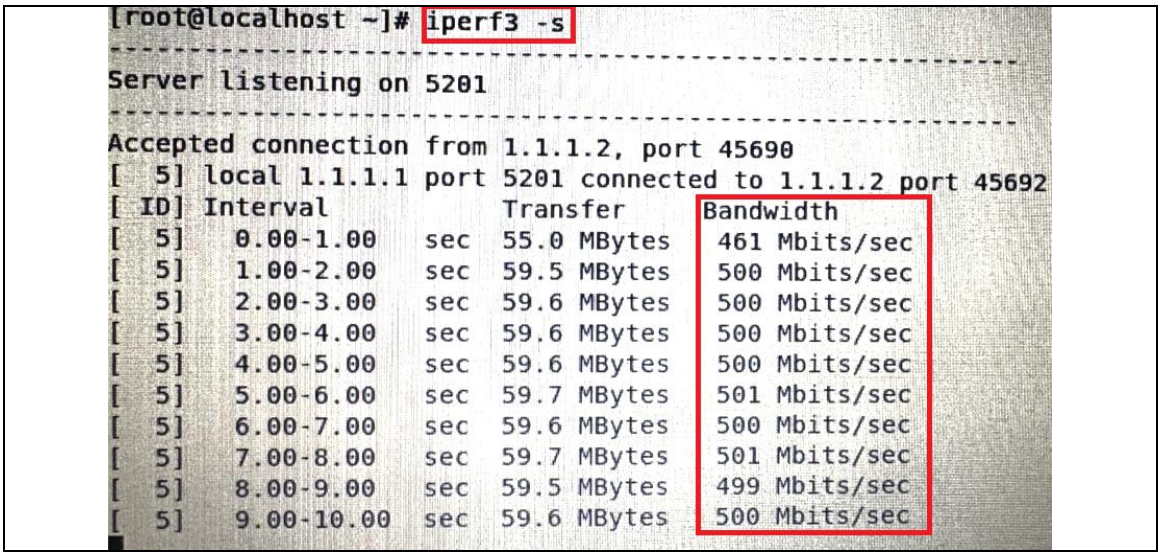


Figura 90 - Modo servidor iPerf3 PC1 sin *policies*

Como se puede apreciar ahora en las Figuras 89 y 90, en el *Bandwidth* se están cursando los 500 Mbps mediante *iPerf3*, por lo que se puede confirmar que las *policies* han funcionado correctamente.

A continuación, se adjuntan las capturas de tráfico extraídas de los equipos mediante el comando "*show interface gigabitEthernet X/X summary*" [58].

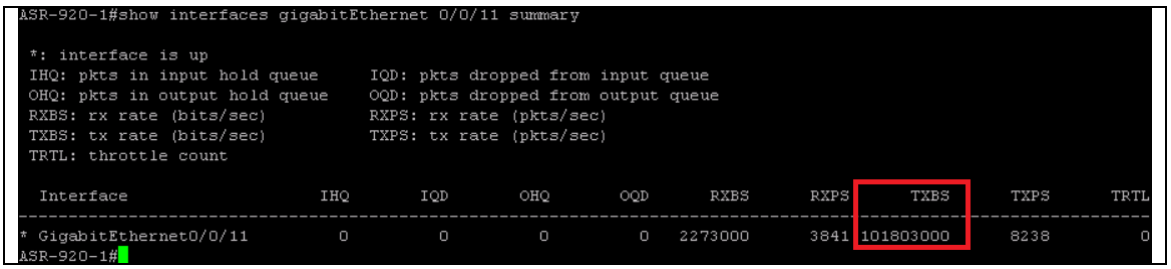


Figura 91 - Tráfico Gi0/0/11 equipo PE ASR-920-1 con *policy*

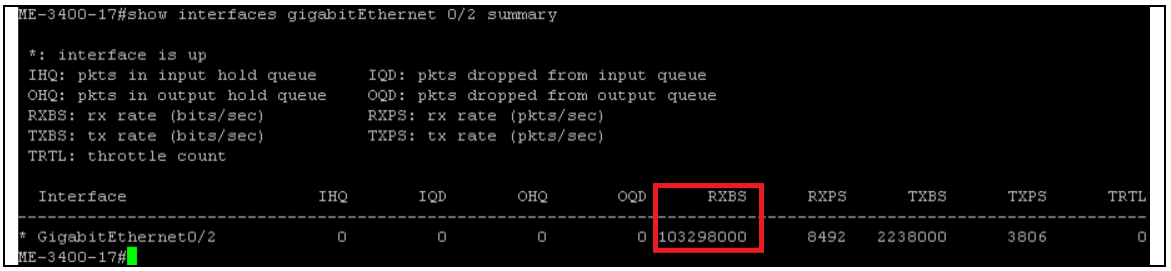


Figura 92 - Tráfico Gi0/2 equipo CPE ME-3400-17 con *policy*

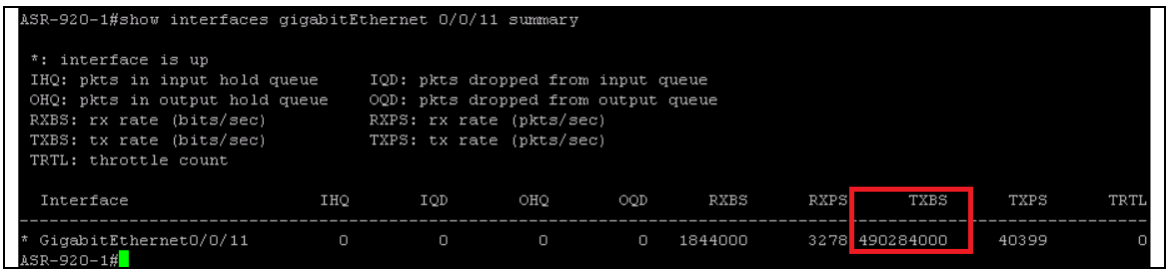


Figura 93 - Tráfico Gi0/0/11 equipo PE ASR-920-1 sin *policy*

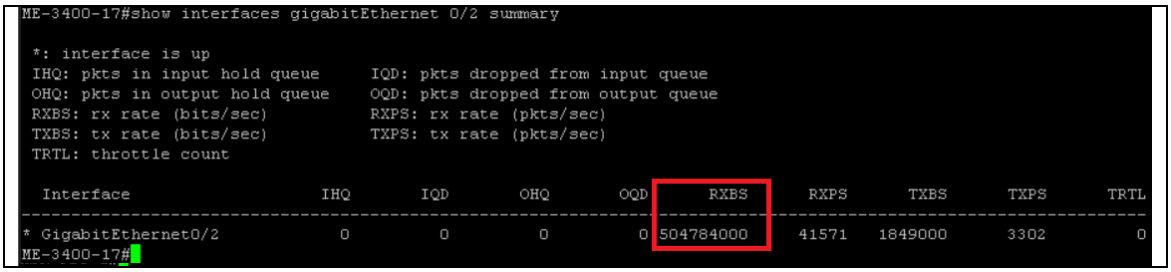


Figura 94 - Tráfico Gi0/2 equipo CPE ME-3400-17 sin *policy*

En las Figuras 91 y 92 se aprecian 100 Mbps de tráfico, como transmisión en el equipo PE ASR-920-1 (extremo servidor iPerf3) y como recepción en el equipo CPE ME-3400-17 (extremo cliente iPerf3). Comportamiento normal ya que estaban las *policies* aplicadas.

En cambio, en las Figuras 93 y 92 se aprecian los 500 Mbps de tráfico porque las *policies* ya se habían desconfigurado.

6. Conclusiones

En primer lugar, me gustaría destacar el cumplimiento del objetivo principal del Trabajo, que consistía en ofrecer a un cliente de un operador de servicios la posibilidad de poder conectar sus equipos de telecomunicaciones mediante circuitos de nivel 2 ofrecidos por la red MPLS de un operador de servicios. Además, se establecieron una serie de objetivos para poder llegar al fin principal, que a continuación vamos a valorar uno a uno:

- *Configurar y validar diferentes mecanismos de mejora que aporten robustez a la red.* Este objetivo se ha cumplido en su totalidad gracias a la implementación de *Traffic Engineering* y *Fast Reroute*. Quiero destacar que la dificultad principal ha sido la elección previa de los protocolos a incorporar en la red, ya que, sin la configuración de alguno de ellos, como OSPF o LDP, nada funcionaba.

- *Configurar y validar un circuito EPL.* Este objetivo también se ha cumplido, con la dificultad añadida de comprender el funcionamiento de las *Service Instance*, necesarias para separar los datos de una interfaz física en diferentes interfaces lógicas según el tipo de encapsulación que se aplique.

- *Configurar y validar varios circuitos EVPL*. Este objetivo se ha cumplido a pesar de la dificultad encontrada a la hora de poder realizar la validación de estos circuitos, ya que en ningún documento oficial del proveedor se especificaba la necesidad de configurar los puertos de los equipos de cliente en modo *trunk*.

- *Configurar y validar circuitos protegidos.* Este objetivo se ha logrado satisfactoriamente. La principal dificultad de este punto ha sido entender el funcionamiento de este tipo de circuitos y los casos de uso, ya que la configuración por sí misma no resulta compleja

- *Configurar y validar la función Dying Gasp.* Este objetivo se ha conseguido, aunque ha sido necesario dedicar más tiempo del que había previsto, debido al desconocimiento de la necesidad de configurar la *Service Instance 1* en la interfaz del equipo PE para que funcione correctamente.

- *Configurar y validar policies en los circuitos para limitar el ancho de banda*. Este último objetivo también se ha cumplido a pesar de la dificultad añadida de comprender el funcionamiento y la configuración de la herramienta iPerf3 para poder realizar la validación de la *policy* aplicada.

En segundo lugar, quiero comentar que la planificación establecida al inicio del Trabajo se ha seguido en su totalidad, pudiendo cumplir la mayoría de los diferentes hitos antes de la fecha prevista. Este logro ha sido gracias a, principalmente, haber hecho una planificación con suficiente margen de tiempo

para solventar cualquier posible error que surgiera y, por otro lado, haber realizado una gran inversión de tiempo y dedicación.

En cuanto a la metodología, considero que ha sido de gran ayuda para la realización del Trabajo, ya que me ha guiado hasta el cumplimiento de los diferentes objetivos. No obstante, quizás hubiera sido oportuno o de más ayuda si esta hubiera sido más detallada y concreta.

En tercer lugar, quiero destacar que gracias a la realización de este Trabajo he podido valorar la importancia que tiene la correcta elección del equipamiento a utilizar, ya que de no haber identificado correctamente todas las características de los equipos al inicio del Trabajo, este pudo haberse visto comprometido. Además, he podido ampliar mis conocimientos de todos los puntos tratados, la mayoría desconocidos antes de comenzar. Ha sido una gran satisfacción personal que, partiendo de unos documentos de fabricante y unos equipos, haya podido ser capaz de desplegar desde cero una red que podría ser utilizada por cualquier operador de servicios.

Por último, se plantean seguir las siguientes líneas futuras, que quedaron fuera del alcance de este Trabajo:

- Para hacer el escenario más real, disponer de rutas de fibra que conecten distintos emplazamientos para poder ubicar los equipos en diferentes localizaciones. Hay que recordad que en este Trabajo todos los equipos se encontraban en el mismo lugar y han sido conectados directamente mediante latiguillos de fibra y/o cobre.

- En este Trabajo solo se han configurado circuitos de la categoría E-Line (EPL y EVPL). Por lo tanto, se debería de ampliar el abanico y configurar también circuitos E-LAN (*multipoint-to-multipoint*) o E-TREE (*rooted multipoint*) [59].

- Añadir *policies* que trate el tráfico no asegurado, donde el valor del PIR sea mayor al del CIR, de manera que se pueda estudiar el distinto comportamiento distinto del tráfico asegurado y del tráfico no asegurado.

- Estudiar la posibilidad de añadir QoS (*Quality of Service*) para poder priorizar el tráfico según el tipo de circuito o del cliente al que pertenezca.

- Estudiar e implementar en la red MPLS tareas de automatización mediante la herramienta EEM (*Embedded Event Manager*) de Cisco [60].

7. Glosario

CDP *Cisco Discovery Protocol*
CIR *Committed Information Rate*
CoS *Classes of Service*
CPE / CE *Customer Premises Equipment / Customer Edge*
CPU *Central Processing Unit*
CTP *Common Spanning* Tree
EGP *Exterior Gateway Protocol*
EEM *Embedded Event Manager*
EIR *Excess Information Rate*
EoMPLS *Ethernet Over MPLS*
EPL *Ethernet Private Line*
EVPL *Ethernet Virtual Private Line*
IGP *Interior Gateway Protocol*
IOS *Internetwork Operating System*
IP *Internet Protocol*
IS-IS *Intermediate System to intermediate System*
L2VPN *Layer 2 Virtual Private Network*
LACP *Link Aggregation Control Protocol*
LAN *Local Area Network*
LC/PC *Lucent Connector / Physical Contact*
LDOS *Last Date of Support*
LDP *Label Distribution Protocol*
LLDP *Link Layer Discovery Protocol*
MD5 *Message-Digest Algorithm 5*
MEF *Metro Ethernet Forum*
MPLS *Multiprotocol Label Switching*
MSTP *Multiple Spanning Tree*
MTU *Maximum Transfer Unit*
NNI *Network-to-Network interface*
OAM *Operations, Administration, and Management*
OSI *Open Systems Interconnection*
OSPF *Open Shortest Path First*
P *Provider*
PAGP *Port Aggregation Protocol*
PE *Provider Edge*
SFP *Small Form-factor Pluggable Transceiver*
PIR *Peak Information Rate*
QoS *Quality of Service*
SNMP *Simple Network Management Protocol*
OS *Operating System*
STP *Spanning Tree Protocol*
SVI *Switched Virtual Interface*
TE *Traffic Engineering*
UNI *User-to-Network Interface*
VC *Virtual Circuit*
VLAN *Virtual Local Area Network*
VTP *VLAN Trunking Protocol*

8. Bibliografía

[1] *VPN and Connectivity Services* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: https://docs.oracle.com/cd/E35292_01/doc.72/e47715/con_vpn.htm#autoId0

[2] *End-of-Life Policy* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/products/eos-eol-policy.html

[3] *ME-3600X-24FS-M Switch Cisco Metro Ethernet 3600* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: https://sklep.comel-it.com/pl/products/me-3600x-24fs-m-switch-cisco-metro-ethernet-3600-1402.html

[4] *End-of-Sale and End-of-Life Announcement for the Cisco ME 3600X Series Ethernet Access Switches* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/switches/me-3600x-series-ethernet-access-switches/eos-eol-notice-c51-738038.html

[5] *End-of-Sale and End-of-Life Announcement for the Cisco ASR920* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/routers/asr-920-series-aggregation-services-router/eos-eol-notice-c51-743642.html

[6] *Routers de Servicios de Agregación Cisco ASR 920 Series* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: https://www.cisco.com/c/es_mx/support/routers/asr-920-series-aggregation-services-router/series.html

[7] *Cisco ASR 920 Series Aggregation Services Routers: High-Port-Density Models* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: https://www.andovercg.com/datasheets/cisco-asr-920-series-aggregation-services-router.pdf

[8] *RAX711-L | Multi-service Network Terminal* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: http://davantel.com/files/RC_Datasheet_RAX711-L--V4-.pdf

[9] *Cisco - ME-3400EG-2CS-A* [en línea] [fecha de consulta: 22 de octubre de 2022]. Disponible en: https://www.tonitrus.com/es/redes/cisco/switch/cisco-metro-ethernet-switch/10104286-003-cisco-me-3400eg-2cs-a-me3400e-2combo-2-sfp/

[10] *Cable de consola Cisco* [en línea] [fecha de consulta: 23 de octubre de 2022]. Disponible en: https://www.amazon.es/Cisco-Cable-Consola-Serie-Dispositivo/dp/B06Y51HSC5

[11] *Access the CLI via PuTTY using a Console Connection on 300 and 500 Series Managed Switches* [en línea] [fecha de consulta: 23 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb4984-access-the-cli-via-putty-using-a-console-connection-on-300-a.html

[12] *ASR 920-12CZ-A Router* [en línea] [fecha de consulta: 23 de octubre de 2022]. Disponible en: https://software.cisco.com/download/home/286288691/type/282046477/release/Gibraltar-16.12.6

[13] *Qué es un transceptor SFP y cómo elegir uno según tus necesidades* [en línea] [fecha de consulta: 23 de octubre de 2022]. Disponible en: https://www.redeszone.net/tutoriales/redes-cable/que-es-transceptor-sfp/

[14] *Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet* [en línea] [fecha de consulta: 23 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/datasheet-c78-366584.html

[15] *Cables de Conexión de Fibra Óptica* [en línea] [fecha de consulta: 23 de octubre de 2022]. Disponible en: https://www.fs.com/es/c/fiber-patch-cords-261

[16] *PureLink IQ-PC1001-010 Cat6A* [en línea] [fecha de consulta: 23 de octubre de 2022]. Disponible en: https://www.thomann.de/es/purelink_iq_pc1001_010_cat6a.htm?gclid=CjwKCAjwzNOaBhAcEiwAD7Tb6B3tPeTLXVZqE7kWhO1CmPyAIMOkVePJJVCSYYZFoQ9cvj-hlCQOVBoCj5kQAvD_BwE

[17] *EOMPLS PSEUDOWIRE SERVICE* [en línea] [fecha de consulta: 25 de octubre de 2022]. Disponible en: https://www.iptp.net/en_US/network/connectivity-services/eompls-pseudowire-service/

[18] *Protocolo de detección de capas de vínculos (LLDP)* [en línea] [fecha de consulta: 28 de octubre de 2022]. Disponible en: https://www.whatsupgold.com/es/network-discovery/protocolo-de-deteccion-de-capas-lldp

[19] *Cisco Networking Academy's Introduction to Routing Dynamically* [en línea] [fecha de consulta: 29 de octubre de 2022]. Disponible en: https://www.ciscopress.com/articles/article.asp?p=2180210&seqNum=7

[20] *MPLS Label Distribution Protocol (LDP)* [en línea] [fecha de consulta: 30 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/convert/mp_ldp_book/mp_ldp_overview.html

[21] *Configuración del protocolo de detección de Cisco en routers y switches Cisco que ejecutan IOS de Cisco* [en línea] [fecha de consulta: 28 de octubre de 2022]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/network-management/discovery-protocol-cdp/43485-cdponios43485.pdf

[22] *Configuring OSPF* [en línea] [fecha de consulta: 28 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html

[23] *MPLS Label Distribution Protocol* [en línea] [fecha de consulta: 28 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/15-s/mp-ldp-15-s-book/mp-ldp-overview.html

[24] *Traffic Engineering* [en línea] [fecha de consulta: 30 de octubre de 2022]. Disponible en: https://www.sciencedirect.com/topics/engineering/traffic-engineering

[25] *MPLS Traffic Engineering Commands on Cisco IOS XR Software* [en línea] [fecha de consulta: 30 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios_xr_sw/iosxr_r3-7/mpls/command/reference/gr37mpte.html

[26] *MPLS Traffic Engineering Interarea Tunnels* [en línea] [fecha de consulta: 30 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_setup/configuration/xe-3s/mp-te-path-setup-xe-3s-book/mp-te-interarea-tun.html

[27] *MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion* [en línea] [fecha de consulta: 30 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_protect/configuration/xe-3s/mp-te-path-protect-xe-3s-book/mp-te-expl-address.html

[28] *MPLS Traffic Engineering Tunnel Source* [en línea] [fecha de consulta: 30 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_te_path_setup/configuration/15-sy/mp-te-path-setup-15-sy-book/mp-te-tun-src.pdf

[29] *SERVICIO EOMPLS PSEUDOWIRE* [en línea] [fecha de consulta: 30 de octubre de 2022]. Disponible en: https://www.iptp.com/es_ES/network/connectivity-services/eompls-pseudowire-service/

[30] *Configuring Pseudowire* [en línea] [fecha de consulta: 30 de octubre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/scg/b_scg_for_asr901s/b_scg_for_asr901s_chapter_010100.pdf

[31] *MPLS Traffic Engineering Fast Reroute -- Link Protection* [en línea] [fecha de consulta: 31 de octubre de 2022]. Disponible en: https://www.cisco.com/en/US/docs/ios/12_0st/12_0st10/feature/guide/fastrout.html

[32] *Who is MEF?* [en línea] [fecha de consulta: 2 de noviembre de 2022]. Disponible en: https://www.mef.net/about-mef/

[33] *Metro Ethernet Forum (MEF)* [en línea] [fecha de consulta: 2 de noviembre de 2022]. Disponible en: https://opennetworking.org/about-onf/liaisons/mef/

[34] *Types of Carrier Ethernet 2.0 Services* [en línea] [fecha de consulta: 2 de noviembre de 2022]. Disponible en: https://www.omnitron-systems.com/carrier-ethernet-learning-center/carrier-ethernet-2-0-service-types

[35] *EPL Networks vs EVPL Networks* [en línea] [fecha de consulta: 2 de noviembre de 2022]. Disponible en: https://neosnetworks.com/products-services/ethernet/epl-vs-evpl/

[36] *Configuring Ethernet Virtual Connections on the Cisco ASR 903 Router* [en línea] [fecha de consulta: 5 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/wireless/asr_900/feature/guides/evc.html

[37] *Configuring Bridge Domain Interfaces* [en línea] [fecha de consulta: 5 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/bdi.html

[38] *Switch Virtual Interface* [en línea] [fecha de consulta: 5 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/L3_config/b_Cisco_APIC_Layer_3_Configuration_Guide/b_Cisco_APIC_Layer_3_Configuration_Guide_chapter_01010.pdf

[39] *Configuring VLAN Trunks* [en línea] [fecha de consulta: 5 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst_digital_building_series_switches/software/15-2_5_ex/configuration_guide/b_1525ex_consolidated_cdb_cg/b_1525ex_consolidated_cdb_cg_chapter_0110101.pdf

[40] *Configuring 802.1Q and Layer 2 Protocol Tunneling* [en línea] [fecha de consulta: 5 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/01xo/configuration/guide/tunnel.html

[41] *MPLS: Basic MPLS Configuration Guide, Cisco IOS Release x.x* [en línea] [fecha de consulta: 6 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios/mpls/configuration/guide/convert/mp_basic_book/mp_mpls_overview.html

[42] *Troubleshooting MPLS for Traffic Engineering* [en línea] [fecha de consulta: 6 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/dam/en/us/products/collateral/ios-nx-os-software/multiprotocol-label-switching-archive/prod_white_paper0900aecd803128b9.pdf

[43] *¿Qué es el modelo OSI?* [en línea] [fecha de consulta: 16 de noviembre de 2022]. Disponible en: https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/

[44] *Las 7 capas del modelo OSI* [en línea] [fecha de consulta: 16 de noviembre de 2022]. Disponible en: https://sites.google.com/site/tuxnots/materias-de-la-facu/gnu-linux/modeloosi

[45] *Cómo Comprender VLAN Trunk Protocol (VTP)* [en línea] [fecha de consulta: 16 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.pdf

[46] *What is the difference between LACP & PAGP?* [en línea] [fecha de consulta: 16 de noviembre de 2022]. Disponible en: https://www.cablesandkits.com/learning-center/lacp-vs-pagp

[47] *Configure STP Settings on a Switch through the CLI* [en línea] [fecha de consulta: 16 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5760-configure-stp-settings-on-a-switch-through-the-cli.html

[48] *How to define the VLANs allowed on a trunk link* [en línea] [fecha de consulta: 19 de noviembre de 2022]. Disponible en: https://community.cisco.com/t5/networking-knowledge-base/how-to-define-the-vlans-allowed-on-a-trunk-link/ta-p/3131083

[49] *Native VLAN – Default VLAN* [en línea] [fecha de consulta: 19 de noviembre de 2022]. Disponible en: https://todopacketracer.wordpress.com/2017/08/27/native-vlan-default-vlan/

[50] *L2VPN Pseudowire Redundancy* [en línea] [fecha de consulta: 24 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ha/configuration/xe-3s/wan-l2vpn-pw-red-xe.html

[51] *Configuring Dying Gasp* [en línea] [fecha de consulta: 26 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr2010/software/15_2_3_t/configuring_dying_gasp.html

[52] *Ethernet OAM* [en línea] [fecha de consulta: 27 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network/3-8/reference/guide/ethoam.html

[53] *Ethernet Virtual Connections Configuration* [en línea] [fecha de consulta: 27 de noviembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/ce/b_ce_xe-313s-asr920-book/b_ce_xe-313s-asr920-book_chapter_01.html

[54] *CIR and PIR* [en línea] [fecha de consulta: 02 de diciembre de 2022]. Disponible en: https://ipcisco.com/lesson/cir-and-pir/

[55] *Class-Based Policing* [en línea] [fecha de consulta: 03 de diciembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-xe-3s-book/qos-plcshp-class-plc.html

[56] *iPerf3 - Introduction* [en línea] [fecha de consulta: 03 de diciembre de 2022]. Disponible en: https://developer.cisco.com/docs/app-hosting/#!deploy-iperf3-performance-monitoring-application

[57] *iperf3: Mide la velocidad entre dos o más equipos en LAN, WiFi o Internet* [en línea] [fecha de consulta: 03 de diciembre de 2022]. Disponible en: https://www.redeszone.net/tutoriales/redes-cable/iperf3-medir-velocidad-lan-wifi-internet/

[58] *Ports and Interfaces Commands* [en línea] [fecha de consulta: 04 de diciembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/cmd-ref/me_cr_book/me_ports_and_interfaces_cli.pdf

[59] *SOLUCIONES CARRIER ETHERNET* [en línea] [fecha de consulta: 29 de diciembre de 2022]. Disponible en: http://davantel.com/files/carrier-ethernet.pdf

[60] EEM Scripts used to Troubleshoot [en línea] [fecha de consulta: 29 de diciembre de 2022]. Disponible en: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-embedded-event-manager-eem/116176-technote-eemscripts-00.html

9. Anexos

9.1 Configuración ASR-920-1

```
ASR-920-1#show running-config
Building configuration...

Current configuration : 5382 bytes
!
! Last configuration change at 03:12:46 UTC Sat Dec 3 2022
!
version 16.12
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform bfd-debug-trace 1
platform xconnect load-balance-hash-algo mac-ip-instanceid
platform tcam-parity-error enable
platform tcam-threshold alarm-frequency 1
platform shell
!
hostname ASR-920-1
!
boot-start-marker
boot system bootflash:asr920-universalk9_npe.16.12.07.SPA.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
login on-success log
!
!
```

```
!
!
!
!
!
mpls label protocol ldp
no mpls ip propagate-ttl forwarded
mpls ldp neighbor 10.100.2.1 targeted
mpls ldp neighbor 10.100.3.1 targeted
mpls traffic-eng tunnels
mpls traffic-eng signalling advertise explicit-null
mpls traffic-eng signalling interpret explicit-null verbatim
mpls tp
 router-id 10.100.1.1
multilink bundle-name authenticated
!
!
!
license udi pid ASR-920-12CZ-A sn FOC2536R4PJ
license accept end user agreement
license boot level advancedmetroipaccess
no license smart enable
memory free low-watermark processor 5127
file prompt quiet
!
!
spanning-tree extend system-id
sdm prefer default
diagnostic bootup level minimal
!
!
redundancy
!
!
!
!
!
transceiver type all
 monitoring
cdp run
!
!
!
policy-map POLICY_100_Mbps
 class class-default
  police cir 100000000 pir 100000000 conform-action set-mpls-exp-imposition-
transmit 1 exceed-action drop  violate-action drop
!
pseudowire-class 1-SZ-2
 encapsulation mpls
```

```
 preferred-path interface Tunnel1
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.100.1.1 255.255.255.255
 ip ospf 100 area 0
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.100.2.1
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 5 explicit name Path-1-SZ-2
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng fast-reroute
!
interface Tunnel10
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.100.2.1
 tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-2
!
interface Tunnel20
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.100.3.1
 tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-SZ
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
```

```
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/4
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/5
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/6
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/7
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/8
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/9
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/10
 no ip address
 media-type auto-select
 negotiation auto
 no keepalive
 service instance 3001 ethernet
  encapsulation default
  l2protocol tunnel cdp stp vtp pagp lldp lacp udld
  xconnect 10.100.2.1 1111113 encapsulation mpls pw-class 1-SZ-2
 !
!
interface GigabitEthernet0/0/11
 no ip address
 media-type auto-select
 negotiation auto
```

```
 no keepalive
 service instance 3001 ethernet
  encapsulation default
  l2protocol tunnel cdp stp vtp pagp lldp lacp udld
  service-policy input POLICY_100_Mbps
  xconnect 10.100.2.1 1111111 encapsulation mpls pw-class 1-SZ-2
 !
!
interface TenGigabitEthernet0/0/12
 description ASR-920-2 Te0/0/12
 mtu 9216
 ip address 10.1.1.1 255.255.255.252
 ip ospf 100 area 0
 cdp enable
 mpls traffic-eng tunnels
!
interface TenGigabitEthernet0/0/13
 description ASR-920-SZ-3 Te0/0/27
 mtu 9216
 ip address 10.1.1.5 255.255.255.252
 ip ospf 100 area 0
 cdp enable
 mpls traffic-eng tunnels
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
router ospf 100
 router-id 10.100.1.1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
!
ip explicit-path name Path-1-SZ-2 enable
 index 1 next-address 10.1.1.6
 index 2 next-address 10.1.1.10
!
ip explicit-path name FRR-ASR-920-2 enable
 index 1 next-address 10.1.1.6
 index 2 next-address 10.1.1.10
!
ip explicit-path name FRR-ASR-920-SZ enable
 index 1 next-address 10.1.1.2
```

```
 index 2 next-address 10.1.1.9
!
ip access-list standard LDP_PEERING
!
logging alarm informational
!
mpls ldp router-id Loopback0 force
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 61 0
 password 7 00071A150754
 login
 transport input telnet ssh
 transport output all
!

!

!
end
```

9.2 Configuración ASR-920-2

```
ASR-920-2#show running-config
Building configuration...

Current configuration : 5290 bytes
!
! Last configuration change at 08:16:42 UTC Sun Nov 27 2022
!
version 16.12
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform bfd-debug-trace 1
platform xconnect load-balance-hash-algo mac-ip-instanceid
platform tcam-parity-error enable
platform tcam-threshold alarm-frequency 1
platform shell
!
hostname ASR-920-2
!
```

```
boot-start-marker
boot system bootflash:asr920-universalk9_npe.16.12.07.SPA.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
!
!
mpls label protocol ldp
no mpls ip propagate-ttl forwarded
mpls ldp neighbor 10.100.1.1 targeted
mpls ldp neighbor 10.100.3.1 targeted
mpls traffic-eng tunnels
mpls traffic-eng signalling advertise explicit-null
mpls traffic-eng signalling interpret explicit-null verbatim
mpls tp
 router-id 10.100.2.1
multilink bundle-name authenticated
!
!
!
license udi pid ASR-920-12CZ-A sn FOC2536R4H8
license accept end user agreement
license boot level advancedmetroipaccess
no license smart enable
memory free low-watermark processor 5127
```

```
file prompt quiet
!
!
spanning-tree extend system-id
sdm prefer default
diagnostic bootup level minimal
!
!
redundancy
bridge-domain 1
!
!
!
!
!
transceiver type all
 monitoring
cdp run
!
!
pseudowire-class 2-SZ-1
 encapsulation mpls
 preferred-path interface Tunnel1
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.100.2.1 255.255.255.255
 ip ospf 100 area 0
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.100.1.1
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 5 explicit name Path-2-SZ-1
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng fast-reroute
!
interface Tunnel10
```

```
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.100.1.1
 tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-1
!
interface Tunnel20
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.100.3.1
 tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-SZ
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
 ethernet oam
 service instance 1 ethernet
  encapsulation untagged
  bridge-domain 1
 !
 service instance 3000 ethernet
  encapsulation dot1q 3000
  rewrite ingress tag pop 1 symmetric
  bridge-domain 3000
 !
 service instance 3001 ethernet
  encapsulation dot1q 3001
  rewrite ingress tag pop 1 symmetric
  xconnect 10.100.1.1 1111111 encapsulation mpls pw-class 2-SZ-1
   backup peer 10.100.1.1 1111113 pw-class 2-SZ-1
 !
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/4
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/5
 no ip address
```

```
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/6
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/7
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/8
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/9
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/10
 no ip address
 media-type auto-select
 negotiation auto
!
interface GigabitEthernet0/0/11
 no ip address
 media-type auto-select
 negotiation auto
!
interface TenGigabitEthernet0/0/12
 description ASR-920-1 Te0/0/12
 mtu 9216
 ip address 10.1.1.2 255.255.255.252
 ip ospf 100 area 0
 cdp enable
 mpls traffic-eng tunnels
!
interface TenGigabitEthernet0/0/13
 description ASR-920-SZ-3 Te0/0/26
 mtu 9216
 ip address 10.1.1.10 255.255.255.252
 ip ospf 100 area 0
 cdp enable
 mpls traffic-eng tunnels
!
interface GigabitEthernet0
```

```
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
interface BDI3000
 ip address 10.1.2.1 255.255.255.252
!
router ospf 100
 router-id 10.100.2.1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
!
ip explicit-path name Path-2-SZ-1 enable
 index 1 next-address 10.1.1.9
 index 2 next-address 10.1.1.5
!
ip explicit-path name FRR-ASR-920-1 enable
 index 1 next-address 10.1.1.9
 index 2 next-address 10.1.1.5
!
ip explicit-path name FRR-ASR-920-SZ enable
 index 1 next-address 10.1.1.1
 index 2 next-address 10.1.1.6
!
ip access-list standard LDP_PEERING
!
logging alarm informational
!
mpls ldp router-id Loopback0 force
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 61 0
 password 7 00071A150754
 login
 transport input telnet ssh
 transport output all
!
```

```
!

!
end
```

9.3 Configuración ASR-920-SZ

```
ASR-920-SZ#show running-config
Building configuration...

Current configuration : 13092 bytes
!
! Last configuration change at 10:29:25 DST Thu Nov 17 2022 by cisco
! NVRAM config last updated at 10:29:27 DST Thu Nov 17 2022 by cisco
!
version 16.12
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform bfd-debug-trace 1
platform xconnect load-balance-hash-algo mac-ip-instanceid
platform tcam-parity-error enable
platform tcam-threshold alarm-frequency 1
!
hostname ASR-920-SZ
!
boot-start-marker
boot system bootflash:asr920-universalk9_npe.16.12.06.SPA.bin
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no aaa new-model
!
!
!
!
!
!
!
!
```

```
!
!
login on-success log
!
!
!
!
!
!
!
mpls label protocol ldp
no mpls ip propagate-ttl forwarded
mpls ldp neighbor 10.100.1.1 targeted
mpls ldp neighbor 10.100.2.1 targeted
mpls traffic-eng tunnels
mpls traffic-eng signalling advertise explicit-null
mpls traffic-eng signalling interpret explicit-null verbatim
mpls tp
 router-id 10.100.3.1
multilink bundle-name authenticated
!
!
!
license udi pid ASR-920-24SZ-M sn CAT2230V1P4
license accept end user agreement
license boot level advancedmetroipaccess
no license smart enable
memory free low-watermark processor 5129
file prompt quiet
!
!
spanning-tree extend system-id
sdm prefer default
diagnostic bootup level minimal
!
!
redundancy
!
!
!
!
!
transceiver type all
 monitoring
cdp run
!
!
!
!
!
```

```
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.100.3.1 255.255.255.255
 ip ospf 100 area 0
!
interface Tunnel30
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.100.1.1
 tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-1
!
interface Tunnel40
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.100.2.1
 tunnel mpls traffic-eng path-option 1 explicit name FRR-ASR-920-2
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/5
 no ip address
 shutdown
 negotiation auto
```

```
!
interface GigabitEthernet0/0/6
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/7
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/8
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/9
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/10
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/11
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/12
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/13
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/14
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/15
 no ip address
 shutdown
 negotiation auto
```

```
!
interface GigabitEthernet0/0/16
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/17
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/18
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/19
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/20
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/21
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/22
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/23
 no ip address
 shutdown
 negotiation auto
!
interface TenGigabitEthernet0/0/24
 no ip address
!
interface TenGigabitEthernet0/0/25
 no ip address
!
interface TenGigabitEthernet0/0/26
 mtu 9216
 ip address 10.1.1.9 255.255.255.252
```

```
 ip ospf 100 area 0
 cdp enable
 mpls traffic-eng tunnels
!
interface TenGigabitEthernet0/0/27
 mtu 9216
 ip address 10.1.1.6 255.255.255.252
 ip ospf 100 area 0
 cdp enable
 mpls traffic-eng tunnels
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 negotiation auto
!
router ospf 100
 router-id 10.100.3.1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0
!
ip explicit-path name FRR-ASR-920-1 enable
 index 1 next-address 10.1.1.10
 index 2 next-address 10.1.1.1
!
ip explicit-path name FRR-ASR-920-2 enable
 index 1 next-address 10.1.1.5
 index 2 next-address 10.1.1.2
!
ip access-list standard LDP_PEERING
!
logging alarm informational
!
mpls ldp router-id Loopback0 force
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 61 0
```

```
 password 7 00071A150754
 login
 transport input telnet ssh
 transport output all
!

!

!
end
```

9.4 Configuración ME-3400-17

```
ME-3400-17#show running-config
Building configuration...

Current configuration : 4926 bytes
!
! Last configuration change at 12:12:37 DST Sat Dec 3 2022 by cisco
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ME-3400-17
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone DST 1 0
clock summer-time DST recurring last Sun Mar 2:00 last Sun Oct 2:00
system mtu routing 1500
ip routing
!
!
!
ip multicast-routing distributed
!
!
!
!
!
dying-gasp primary ethernet-oam secondary snmp-trap
!
```

```
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
vlan internal allocation policy ascending
!
vlan 3000-3002
!
!
policy-map POLICY_100_Mbps
 class class-default
    police cir 100000000
      conform-action set-cos-transmit 1
      exceed-action drop
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet0/1
 switchport access vlan 3002
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel lldp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
 l2protocol-tunnel point-to-point pagp
 l2protocol-tunnel point-to-point lacp
 l2protocol-tunnel point-to-point udld
!
interface GigabitEthernet0/2
 switchport access vlan 3001
 switchport mode dot1q-tunnel
 l2protocol-tunnel cdp
 l2protocol-tunnel lldp
 l2protocol-tunnel stp
 l2protocol-tunnel vtp
 l2protocol-tunnel point-to-point pagp
 l2protocol-tunnel point-to-point lacp
 l2protocol-tunnel point-to-point udld
 service-policy input POLICY_100_Mbps
!
interface GigabitEthernet0/3
 no ip address
 shutdown
!
interface GigabitEthernet0/4
 port-type nni
 switchport trunk allowed vlan 3000-3002
 switchport mode trunk
```

```
 shutdown
 ethernet oam
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan3000
 ip address 10.1.2.2 255.255.255.252
!
no ip http server
no ip http secure-server
!
!
ip sla enable reaction-alerts
logging esm config
!
line con 0
line vty 0 4
 session-timeout 60
 exec-timeout 0 0
 login local
line vty 5 15
 session-timeout 60
 exec-timeout 60 0
 login
!
end
```

9.5 Configuración ME-3400-18

```
ME-3400-18#show running-config
Building configuration...

Current configuration : 4276 bytes
!
! Last configuration change at 15:39:25 DST Thu Nov 24 2022 by cisco
! NVRAM config last updated at 20:40:21 DST Fri Nov 18 2022 by cisco
!
version 12.2
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ME-3400-18
!
```

```
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone DST 1 0
clock summer-time DST recurring last Sun Mar 2:00 last Sun Oct 2:00
system mtu routing 1500
ip routing
!
!
!
ip multicast-routing distributed
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
vlan internal allocation policy ascending
!
vlan 1000-1001
!
!
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet0/1
 port-type nni
 switchport trunk allowed vlan 1001
 switchport mode trunk
!
interface GigabitEthernet0/2
 port-type nni
 switchport access vlan 1000
!
interface GigabitEthernet0/3
 no ip address
 shutdown
!
interface GigabitEthernet0/4
 no ip address
 shutdown
!
```

```
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan1000
 ip address 1.1.1.2 255.255.255.0
!
interface Vlan1001
 ip address 2.2.2.2 255.255.255.0
!
no ip http server
no ip http secure-server
!
!
ip sla enable reaction-alerts
logging esm config
!
line con 0
line vty 0 4
 session-timeout 60
 exec-timeout 0 0
 login local
line vty 5 15
 session-timeout 60
 exec-timeout 60 0
 login
!
end
```

9.6 Configuración ME-3400-19

```
ME-3400-19#show running-config
Building configuration...

Current configuration : 4782 bytes
!
! Last configuration change at 19:30:46 UTC Thu Dec 8 2022 by cisco
! NVRAM config last updated at 19:54:52 UTC Fri Nov 18 2022 by cisco
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ME-3400-19
!
boot-start-marker
boot-end-marker
```

```
!
!
no aaa new-model
system mtu routing 1500
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
vlan internal allocation policy ascending
!
vlan 1000-1001
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface GigabitEthernet0/2
 port-type nni
 switchport access vlan 1000
!
interface GigabitEthernet0/3
 no ip address
 shutdown
!
interface GigabitEthernet0/4
 port-type nni
 switchport access vlan 1000
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan1000
 ip address 1.1.1.1 255.255.255.0
!
interface Vlan1001
 ip address 2.2.2.1 255.255.255.0
!
no ip http server
ip http secure-server
!
```

```
!
line con 0
line vty 0 4
 session-timeout 60
 exec-timeout 60 0
 login local
line vty 5 15
 session-timeout 60
 exec-timeout 60 0
 login
!
end
```