Universidad Nacional de La Matanza

Departamento de Ingeniería e Investigaciones Tecnológicas

"Redes de transporte de la nueva generación de Carrier - Ethernet"

Informe FINAL

Diciembre del 2015

Programa de Investigación: PROINCE

Código: C164
Director del Proyecto: Ing. Roca José Luis
Integrantes del Proyecto:
Ing. Biga Daniel Rodolfo (Codirector)
Ing. Dufour Fernando Javier
Ing. Serra Ariel Miguel
Ing. Peliza Carlos
Ing. Micieli Gustavo Ariel

Fecha de inicio: 01/01/14
Fecha de finalización: 31/12/15

Índice de contenidos

1. Otros proyectos con los que se relaciona 4
2. Resumen 4
3. Memoria descriptiva 5
3.1. Resumen ejecutivo de los resultados obtenidos 5
3.2. Desarrollo de la investigación. 6
3.2.1. Investigación Documental 6
3.2.1.1. Tecnologías base de Carrier Ethernet 6
3.2.1.1.1. VLAN (802.1q) 6
3.2.1.1.2. DOBLE TAG-SVLAN (802.1ad) – PROVIDER BRIDGE 7
3.2.1.1.3. MAC-IN-MAC (802.1ah) – PROVIDER BACKBONE BRIDGE 9
3.2.1.1.4. MPLS (MultiProtocol Label Switching) 11
3.2.1.1.4.1. Terminología 11
3.2.1.1.4.2. Funcionamiento MPLS 12
3.2.1.1.5. MPLS - TP 18
3.2.1.1.6. VPNs (Virtual Private Networks) 20
3.2.1.1.6.1. Clasificación de las VPNs 20
3.2.1.1.7. Provider Provisioned VPN (PPVPN) 22
3.2.1.1.7.1. Red MPLS que soporta VPN 24
3.2.1.1.7.2. L3 MPLS VPN 30
3.2.1.2. Metro Ethernet Fórum 33
3.2.1.2.1. CE 1.0 – Primera versión de Carrier Ethernet 33
3.2.1.2.1.1. Servicio E-Line 33
3.2.1.2.1.2. Servicio E-LAN 34
3.2.1.2.1.3. Servicio E-Tree 35
3.2.1.2.2. CE 2.0 – Next generation Carrier Ethernet 35
3.2.1.3. Análisis de la situación del mercado internacional 37
3.2.1.4. Contacto con personal relevante del mercado. 38
3.2.1.5. Equipamientos que satisfacen las funcionalidades de CE 2.0 (certificados). 39
3.2.2. Estudio de un caso de implementación real en Argentina 39
3.2.2.1. Descripción del Escenario 39
3.2.2.1.1. Introducción a las pruebas 41
3.2.2.1.2. INFORME DE PRUEBAS IOT (Inter Operability Test) Terminal Tellabs – Concentración y Distribución Huawei 41
3.2.2.1.3. INFORME DE PRUEBAS IOT (Inter Operability Test) Terminal Huawei – Concentración Tellabs 50
3.2.2.1.4. INFORME DE PRUEBAS IOT (Inter Operability Test) Terminal Alcatel-Lucent – Concentración y Distribución Huawei 54
3.2.3. Investigación de los potenciales servicios en Metro Ethernet 59
3.2.3.1. Estudio y descripción de servicios potenciales Metro-Ethernet de próxima generación en los próximos 3 años en Argentina 60
3.2.4. Mejores prácticas 64
3.3. Prospectiva a 3 años en Argentina 65
3.4. Conclusiones 65
3.5. Resultados obtenidos: 66
3.5.1. Resultados en cuanto a la producción de conocimiento: 66
3.5.2. Resultados en cuanto a la formación de recursos humanos: 66
3.5.3. Resultados en cuanto a la difusión de resultados: 66
3.5.4. Posibilidades de transferencia de resultados: 66
3.5.5. Resultados en cuanto a la transferencia de resultados a organismos externos a la U.N.L.a.M: 67

3.6. Bibliografía. 67
3.7. Producción Científica Tecnológica 67
Anexos 68
Anexo I: Datos de las entrevistas y contactos con profesionales involucrados en la temática. 69
A1.1 Actividad de las Empresas para con Metro Ethernet. 69
A1.2 Qué servicio transporta su red ME..... 69
A1.3 Barreras para la posibilidad de implementación actual de ME. 70
A1.4 Percepción sobre Proveedores de Tecnologías ME. 72
Anexo II: Detalle de siglas utilizadas..... 76
Anexo III: Protocolo de presentación del proyecto. 84
Anexo IV: Artículo presentado en el Congreso 2014..... 80
Anexo V: Artículo presentado en el Congreso 2015..... 93

1. Otros proyectos con los que se relaciona

El presente informe se apoya en algunos aspectos desarrollados en la Investigación que se detalla a continuación.

Programa de Investigación: ***CYTMA y PROINCE***
Institución en la que se realizó la investigación: ***UNLaM***
Unidad Académica: ***Departamento de Ingeniería e Investigaciones Tecnológicas***
Código de Identificación: ***ING0016/2007 y 55/C081***
Título del Proyecto: ***"Estudio de Estado del Arte en Transporte de Servicios de Voz y Video sobre IP y detección de Nichos de Desarrollo"***
Director del Proyecto: ***Director: Ing. Lupi***
Codirector: ***Ing. Daniel Biga***
Participante: ***Horacio Del Giorgio.***
Fecha de inicio: ***1/1/2010***
Fecha de finalización: ***31/1/2011***

2. Resumen

El mundo de las comunicaciones evoluciona rápidamente y quienes funcionan como motor de ese avance son los proveedores de tecnologías. Son ellos los que tienen todas las herramientas tecnológicas y de recursos humanos para impulsar el avance.

La metodología es a través de foros y Working Groups del IETF en donde los proveedores hacen participar sus especialistas de mayor nivel, reconocidos en el mercado internacional por su capacidad de abstracción y su visión global para ofrecer sus ideas y debatir sobre cuál es la mejor solución en cada caso.

De todo este trabajo surgen variadas soluciones tecnológicas que en muchos casos se superponen en la solución de un mismo problema. Ocurre también que algunas grandes ideas, pueden lograr convertirse en normativa de estandarización, sin embargo por la aparición de nuevas soluciones o el desinterés de algunos fabricantes no llegan a imponerse en el mercado.

Es por ello que en este documento hemos presentado las diversas soluciones tecnológicas disponibles para la implementación de redes Metro Ethernet de nueva generación, cuyos servicios están definidos por el MEF en la versión CE 2.0.

Sin embargo también hemos mencionado que el MEF es agnóstico respecto de las tecnologías, lo cual deja un amplio margen a los Carriers para elegir tecnologías y combinar arquitecturas para cumplir con los requerimientos de los nuevos servicios.

También hemos mencionado la existencia de un proceso de certificación para los servicios de los Carriers respecto de los Servicios ofrecidos, que aportan una garantía de calidad certificada por el MEF que es de suma importancia para las corporaciones a la hora de contratar servicios de comunicaciones.

Adicionalmente a lo expuesto, ocurre que sólo algunas combinaciones de las tecnologías expuestas permitirán a un Carrier ofrecer los servicios propuestos con la mejor relación costo beneficio. Esto se debe a que el tamaño de la red, del mercado, su crecimiento futuro y los servicios que el mercado solicita va a requerir son factores preponderantes a la hora de seleccionar las tecnologías y arquitecturas adecuadas.

Por lo expuesto se han relevado las opiniones de los principales especialistas del mercado Argentino, en sus comentario hemos obtenido sus percepciones respecto de las distintas tecnologías, proveedores de equipos, topologías y servicios que se pueden prestar.

Se debe tener en cuenta que la tecnología ME apunta la implementación de arquitecturas de redes y servicios convergentes, basados en las necesidades de los clientes, las necesidades de las empresas de fusionar sus redes, y la convergencia de las distintas tecnologías intervinientes.

Para la implementación de esta convergencia, existe un problema adicional a resolver, que es el de la necesidad de integrar estos servicios con las redes existentes, cuyo despliegue tecnológico es mono-servicio y no fueron pensadas para entornos de servicios convergentes. Por ello los equipamientos deberán inter-operar correctamente con los equipos existentes en un idioma (protocolos, interfaces, etc.), que éstos últimos comprendan.

Como ocurre históricamente en las comunicaciones, la responsabilidad de integrar las tecnologías existentes recaerá sobre las nuevas tecnologías y arquitecturas que se incorporan para cada servicio.

El objetivo principal de la investigación será determinar el grado de madurez de las redes ME existentes, los servicios que sobre estas se están prestando y su compatibilidad con las tecnologías tradicionales ya desplegadas, generando una recomendación de mejores prácticas de implementación o actualización según corresponda de acuerdo a el estado del arte actual.

La metodología utilizada es, la investigación documental, entrevistas a especialistas de distintos participantes (fabricantes, Carriers, etc.), análisis de Normas y el cumplimiento de las mismas por las principales tecnologías y prestadores de servicio.

Se buscarán las incompatibilidades y a partir de un debate interno se obtendrán las conclusiones respecto de las mejores prácticas que se contrastarán con pruebas realizadas por los Carriers y/o pruebas piloto.

Se generará un informe final en el que, entre otros aspectos, se detallarán las mejores prácticas para la implementación de estas redes y servicios.

El impacto que producirá la investigación será en el entorno académico, en las empresas de comunicaciones, y en las empresas de todo tipo que tendrán una guía para determinar qué servicios tendrán disponibles para mejorar sus servicios actuales de comunicaciones.

Palabras Clave: Ethernet, MPLS, MEF, CE 2.0, L2VPN, L3VPN

3. Memoria descriptiva

3.1. Resumen ejecutivo de los resultados obtenidos

A continuación describimos los principales resultados obtenidos hasta la fecha de entrega del presente informe.

- Se ha podido analizar las tecnologías de comunicaciones actualmente instaladas que formarán parte del proceso de integración de servicios multimedia.

- Se ha analizado detalladamente la base documental a partir de la cual se puede desarrollar la investigación.
- Se ha tenido acceso a la percepción de profesionales especialistas en comunicaciones involucrados en la tecnología ME (Metro Ethernet).
- Se ha analizado distintos aspectos de los proveedores de las tecnologías y su situación actual en el mercado.
- Se ha investigado su Arquitectura, Interfaces, Módulos y Protocolos que interactúan.
- Se ha estudiado un caso real en Argentina.

3.2. Desarrollo de la investigación.

3.2.1. Investigación Documental

Se ha realizado una profunda investigación documental que nos permitió contar con amplia información sobre la tecnología ME.

Esta información incluye material obtenido de la WEB, e información aportada por los profesionales del mercado involucrados con la tecnología de redes que hemos contactado.

Este material fue de suma importancia para determinar la complejidad del amplio espectro de tecnologías involucradas en ME como así también para determinar el gran desafío que la implementación de redes ME que cumplan con lo especificado por MEF CE 2.0 representa.

3.2.1.1. Tecnologías base de Carrier Ethernet

3.2.1.1.1. VLAN (802.1q)

Las VLAN (Virtual Local Área Network) son la base de las tecnologías Ethernet y por consecuencia Carrier Ethernet, las VLAN permiten separar los dominios de broadcast de nivel 2 (capa de enlace del modelo TCP/IP) incrementando el rendimiento de una red física. Una VLAN, nos brinda la posibilidad de que un administrador de red pueda crear grupos de dispositivos conectados de manera lógica, que actúan como una red independiente de otras con las cuales pueden compartir infraestructura. Para tener una trama etiquetada (802.1q), el procedimiento en el switch consiste en agregar 4 bytes luego de la dirección MAC origen de una trama Ethernet, debido a este agregado es necesario recalcular la secuencia de chequeo de trama (FCS).

Se muestra una gráfica de una trama de nivel 2 con 802.1q.

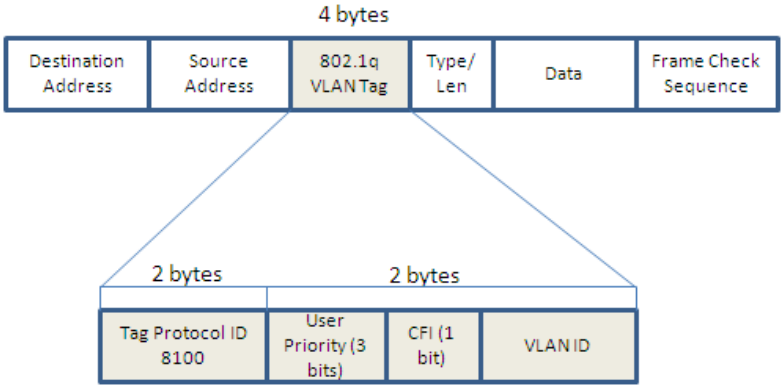


Figura 1: Encabezado 802.1q

Dentro de la etiqueta de VLAN, se descomponen los campos que se describen a continuación:

TPID (Tag Protocol IDentifier): Este campo indica que estamos en presencia de una trama etiquetada, se compone de los siguientes parámetros que se pueden apreciar en la gráfica. El valor en hexadecimal 8100 indica que estamos en presencia de una etiqueta 801.1q.

PCP (Priority Code Point o User Priority): Son 3 bits que se utilizan generalmente para priorizar un tipo de tráfico por sobre otro, en conjunto con otras políticas de red permite ofrecer una calidad de servicio en la red que permite a un operador dar múltiples servicios sobre la misma infraestructura. A estos bits se los conoce como “IEEE 802.1p”.

CFI (Canonical Format Indicator): Este bit se utiliza para indicar si en presencia de congestión esta trama puede ser descartada o no. También se lo conoce como DEI (Drop Eligible Indicator).

VID (Vlan IDentifier): Es el número identificador de la VLAN, son posibles 4096 numeraciones, aunque el número 0 no es posible utilizar.

Este protocolo permitió compartir una misma infraestructura para brindar múltiples servicios, pero rápidamente tuvo una limitante, que es la cantidad de VLANs que se pueden asignar (4094). Para solucionar este problema se desarrolló el estándar 802.1ad.

3.2.1.1.2. DOBLE TAG-SVLAN (802.1ad) – PROVIDER BRIDGE

802.1ad estandariza el uso de múltiples Tags de VLAN en los switches bridgeados, facilitando la implementación de los servicios de CE (Carrier Ethernet), por ejemplo, permite que el proveedor le ofrezca utilizar, VLANs del cliente y poder transportarlas dentro de la Red bridgeada del Carrier siendo completamente transparente para el cliente.

De similar procedimiento que el estándar 802.1q, el protocolo 802.1ad coloca una nueva etiqueta similar a la anterior pero con algunas diferencias que se comentan a continuación. El límite teórico de conexiones VLANs que se pueden configurar es de más de 16 millones de conexiones, ya que permite que las 4096 de la VLAN 802.1q combinarlas con las 4096 SVLAN 802.1ad.

Se puede ver en la gráfica a continuación donde se inserta la nueva etiqueta en la trama.

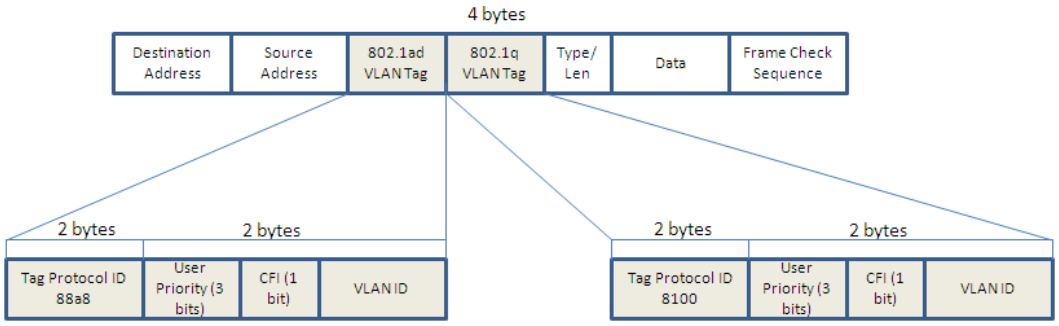


Figura 2: Doble TAG de VLAN (802.1ad)

En las SVLAN se utiliza el valor 88a8 hexadecimal en el TPID, para diferenciar la etiqueta de VLAN.

Con este protocolo no solo se aumenta la cantidad de VLANs que se pueden transportar en una red bridgeada sino que se puede transportar tráfico de nivel 2 de clientes (es la VLAN interna y se la conoce como Customer VLAN C-VLAN “801.1q”) dentro de una etiqueta de servicio propia del operador de la red (se la conoce como Service VLAN S-VLAN “802.1ad”).

Lo comentado puede verse mejor en el siguiente diagrama:

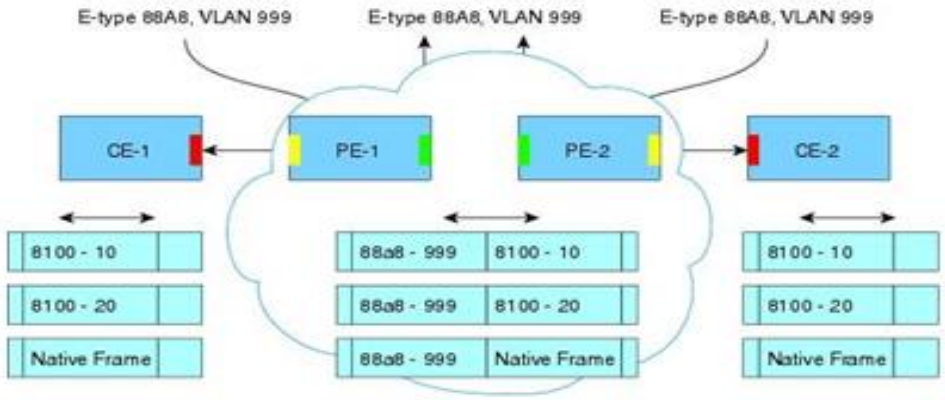


Figura 3: Ejemplo de arquitectura (802.1ad)

El cliente CE-1 tiene tráfico Ethernet sin etiquetar, etiquetado con la VLAN-10 y también tráfico con la VLAN-20. La red del proveedor utiliza el estándar 802.1ad para poder transportar en una red de nivel 2 los datos del cliente, en este ejemplo utiliza el número 999 como S-VLAN y mantiene las etiquetas de cliente que ahora serán las C-VLAN 10, C-VLAN 20 y tráfico sin etiqueta. En el equipo del cliente CE-2 se puede ver como el proveedor retira la etiqueta de servicio (S-VLAN) y entrega al equipo de forma transparente el tráfico a destino.

Al mismo tiempo que la demanda de servicios fue creciendo, los proveedores comenzaron a sufrir problemas de escalabilidad, el principal problema fue que la cantidad de MAC ADDRESS que los equipos tienen que contener en las tablas para conmutar las tramas crecía con la cantidad de clientes, esto impacta directamente en la capacidad de memoria de los equipos y el tiempo de procesamiento que los mismos deben tener para no aumentar la latencia de la red.

Existen dos soluciones de fondo para solucionar este problema, o se escala a nivel 3 del modelo TCP/IP (habitualmente utilizando la tecnología MPLS), es decir, utilizando

protocolos de la capa de IP, o se busca un mecanismo dentro de nivel 2 que solucione el problema de las MAC ADDRESS. A esto último apuntó el estándar 802.1ah que comentamos a continuación.

3.2.1.1.3. MAC-IN-MAC (802.1ah) – PROVIDER BACKBONE BRIDGE

El concepto consiste en definir un nuevo nivel de red bridgeada que tiene sus propios componentes y que son independientes de los del cliente, ofreciendo una completa separación entre los dominios de cliente con los dominios del proveedor, para lograr este resultado, se definió una nueva cabecera Ethernet. Es entonces que encontramos en esta arquitectura una nueva estructura de tramas con MAC ADDRESS independientes de las del cliente y otros elementos que detallaremos en la descripción del header.

En los accesos, todas las PB (802.1ad) de los clientes se mapean a una instancia PBB (802.1ah) de red, definida por el proveedor de servicios. Dicha PBB encapsulará el tráfico añadiendo sus propias direcciones MAC de origen y destino, de forma que el resto de equipos de la red sólo deben conocer las MACs de los nodos de red, dejando a los equipos de borde la responsabilidad de mantener las entradas de los clientes. Así, las MACs de los usuarios finales son transparentes para los nodos de red.

Los equipos en los extremos del PBB, llamados BEB (Backbone Edge Bridge), son los que soportan toda la carga del trabajo. Al ingreso de una trama al bridge de borde de la red 802.1ah, esta se la asocia con una instancia de servicio y la encapsula en una trama, de tal forma que se caracteriza por usar un nuevo juego de MACs que se denominan Backbone MACs.

En la parte de red, el proveedor añadirá una nueva cabecera Ethernet con direcciones MAC propias de los equipos de red, de forma que dentro del Core 802.1ah (BCB – Backbone Core Bridge) sólo se manejen las MACs de los nodos de red, dejando las direcciones de clientes en el borde de la red.

En el gráfico a continuación se resume lo expresado:

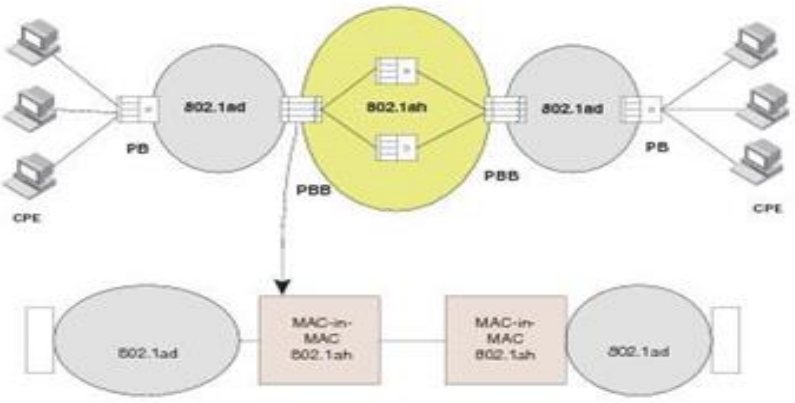


Figura 4: Ejemplo de arquitectura (802.1ah)

Apoyado en la gráfica siguiente comentaremos los campos que el estándar 802.1ah contiene:

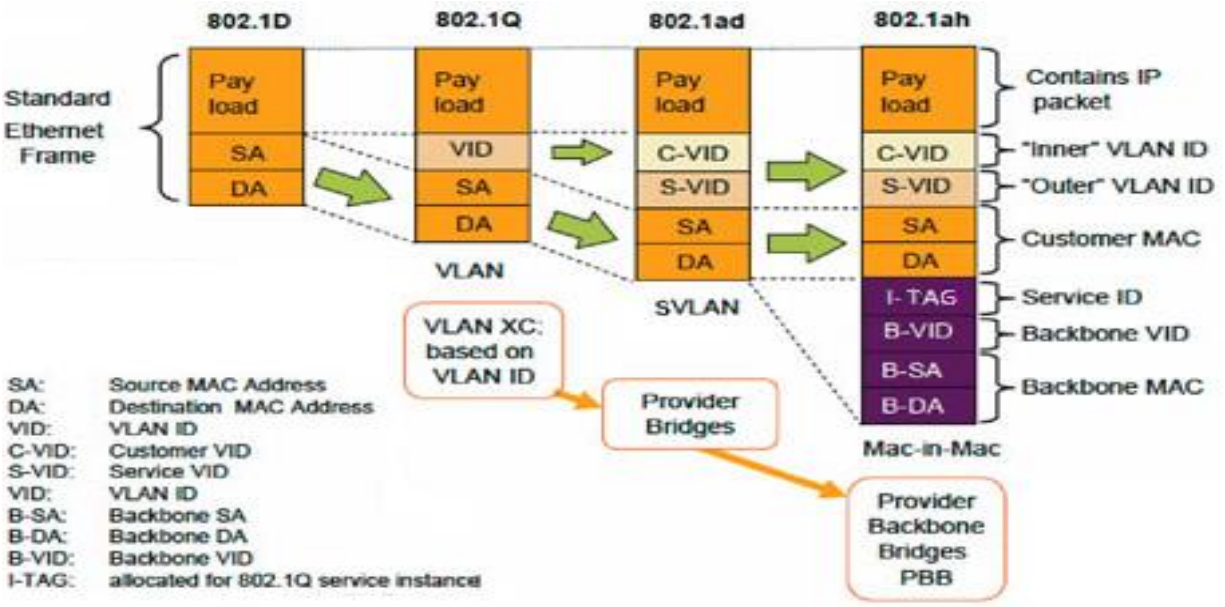


Figura 5: Tecnologías Carrier Ethernet

Como se puede observar, en la red del proveedor de servicios modifica la trama Ethernet incorporando 22 bytes en los campos que se detallan a continuación:

B-DA (Backbone Destination Address) 6 Bytes: Es la MAC de destino del nodo de la red del proveedor, es este caso la red no tiene visibilidad de las MAC del cliente.

B-SA (Backbone Source Address) 6 bytes: Es la MAC del equipo que origina la trama 802.1ah.

B-VID (Backbone Vlan ID) 4 bytes: Este campo es análogo al formato tradicional de VLAN, con el TPID (Ethertype) con el valor 88a8 en hexadecimal. El formato se completa con el PCP y CFI (DEI) y el VLAN ID.

I-TAG (Instance service TAG) 6 bytes: Contiene la instancia del servicio, el formato completo está compuesto por dos parámetros, un TPID (Ethertype) con valor 88e7 y el parámetro TCI (4 bytes) que podemos descomponer en sub-campos:

- PCP (3 bits)
- CFI (o DEI, 1 bit)
- Reservado (4 bits)
- I-SID (24 bits)

El sub-campo I-SID (Instance Service ID), contiene la instancia del servicio, con este valor se genera la EVC (Ethernet Virtual Circuit) y el estándar permite un total de más de 4 millones de EVCs.

Los campos detallados B-VID e I-TAG se pueden resumir en el siguiente gráfico:

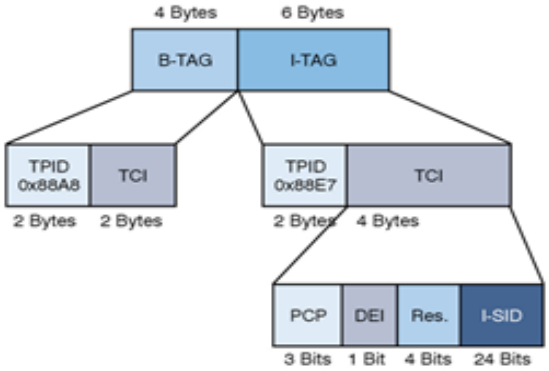


Figura 6: Encabezados B-TAG e I-TAG

3.2.1.1.4. MPLS (MultiProtocol Label Switching)

Es un mecanismo de transporte de datos estandarizado en la RFC 3031, es la integración entre las capas 2 y 3 del modelo OSI.

MPLS direcciona el flujo de datos a lo largo de toda la red, basándose en los requerimientos de dicho flujo y la reserva de recursos realizada por RSVP

La ruta más corta que cumpla con los requisitos de ancho de banda, medios y prioridades sobre otros flujos, será la que MPLS habrá de emplear para hacer viajar los datos.

MPLS se basa, primero en hacer el etiquetado de tramas con criterios de prioridad (QoS) y luego hacer la conmutación a nivel de etiquetas (lo que representa una mejora en la velocidad ya que realiza la conmutación a nivel de capa 2), sin la necesidad de hacer ruteo en capa 3. (Un concepto similar a los caminos y circuitos virtuales de ATM, pero utilizado en redes de paquetes).

Una red MPLS consiste en un conjunto de routers especiales llamados LABEL SWITCHING ROUTERS (LSR) que hacen el trabajo de conmutar y encaminar los datos, mirando etiquetas añadidas a cada paquete.

Cada etiqueta define un flujo de paquetes entre 2 puntos finales, por lo que cada etiqueta tiene sentido local y puede cambiar a lo largo del trayecto (al igual que lo hacían en ATM los V.C.I.)

3.2.1.1.4.1. Terminología

Dominio MPLS:

Conjunto de routers contiguos operando enrutamiento y reenvío MPLS y que pertenecen al mismo dominio de ruteo y administración MPLS.

LSR: Label Switching Router

Router que opera MPLS y es capaz de realizar la conmutación de paquetes etiquetados.

LER: Label Edge Router

Router MPLS que ingresa o egresa paquetes a la red MPLS basado en la dirección de flujo de tráfico, que puede ser o nó trafico MPLS y provenir desde otro dominio MPLS o nó.

LSP: Label Switched Path

Camino unidireccional que atraviesa un dominio MPLS.

FEC: Forward Equivalence Class

Conjunto de todos los paquetes que pertenecen al mismo LSP y reciben la misma política de reenvío.

LDP: Label Distribution Protocol

Protocolo utilizado para asignar y distribuir las etiquetas que deberán ser conocidas por los LSR para realizar su trabajo.

Label: Etiqueta

Identificador corto de longitud fija y significado local, que identifica un FEC. Un paquete puede tener una o varias etiquetas apiladas (Jerarquía).

3.2.1.1.4.2. Funcionamiento MPLS

Se ha mencionado que la forma de trabajo de MPLS consistía en armar rutas de acuerdo a políticas de etiquetado. Así, cuando un LER recibe un paquete, lo etiqueta, con la etiqueta que corresponde a un FEC adecuado. Esto hace que el "nuevo" paquete etiquetado, pueda viajar de manera unidireccional por un LSP.

Cuando el paquete etiquetado pase por un LSR intermedio, puede cambiar de etiqueta (pero no necesariamente de FEC) o recibir una nueva etiqueta que se apila a la anterior (tipo LIFO).

Cerca de llegar a destino, el LER de borde quita la etiqueta y el paquete se entrega a destino sin etiquetar.

El modo de funcionamiento de MPLS, debe analizarse desde dos procesos ligados pero diferentes.

1) El reenvío de paquetes/tramas.

2) La generación y distribución de etiquetas.

La generación de tablas de reenvió de etiquetas, se relaciona con la información de toda la red, que es algo propio de algoritmos de enrutamiento como OSPF o RIP.

Dado que un LSR es un router común al que se le agrega la funcionalidad de MPLS, lo que se hace es que para cada ruta IP en la red se crea un camino de etiquetas, en base a concatenar etiquetas de entrada con etiquetas de salida en cada tabla de los LSR

Sin embargo, queda por analizar la distribución de etiquetas para la conformación del LSP. Previamente estudiaremos el formato de la etiqueta MPLS.

A. Formato de la etiqueta MPLS

La etiqueta MPLS consiste en 4 campos que ocupan un total de 32 bits, dependiendo de la capa de enlace utilizada y que se colocan previos al encabezado IP (recordemos que MPLS busca conmutar antes que capa 3).

Gráficamente y de acuerdo a la capa de enlace:

Modo del Frame	Formato de la trama conformada

PPP	Encabezado PPP	Etiqueta	Encabezado capa 3
Frame Relay	Encabezado Frame Relay	Etiqueta	Encabezado capa 3
LAN	Encabezado MAC	Etiqueta	Encabezado capa 3

Figura 7: Etiqueta MPLS

En cambio, en modo celda o ATM:

Modo Celda	Formato de la celda conformada

ATM	GFC	Etiqueta (VPI + VCI)	PTI	CLP	HEC

Figura 8: Etiqueta MPLS en formato Celda o ATM

Otra forma gráfica de exponer la ubicación de las etiquetas es:

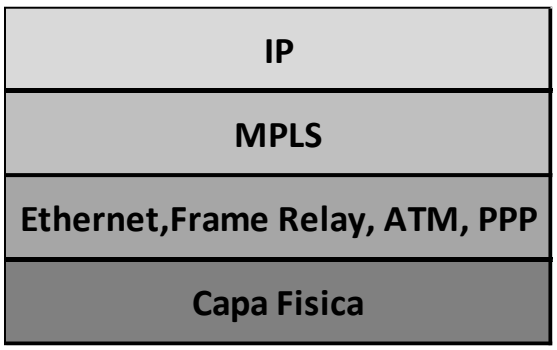


Figura 9: Ubicación de las etiquetas

El siguiente grafico nos muestra la ubicación y función de los grupos de bit que forman una etiqueta MPLS:

Valor de la etiqueta	Clase de servicio (EXP)	Stack o Pila	TTL (Time To Live)
(20 bits)	(3 bit)	(1 bit)	(8 bit)

Figura 10: Ubicación y función de los grupos de bit

Donde el campo EXP por experimental, se usa para identificar la clase de servicio y S de stack, se usa para “apilar” etiquetas de manera jerárquica, de manera que si este bit se halla en 1,dicha etiqueta es la última de la pila y si se halla en 0,esa etiqueta NO es la última de la pila.

Caso de Frame Relay y ATM:

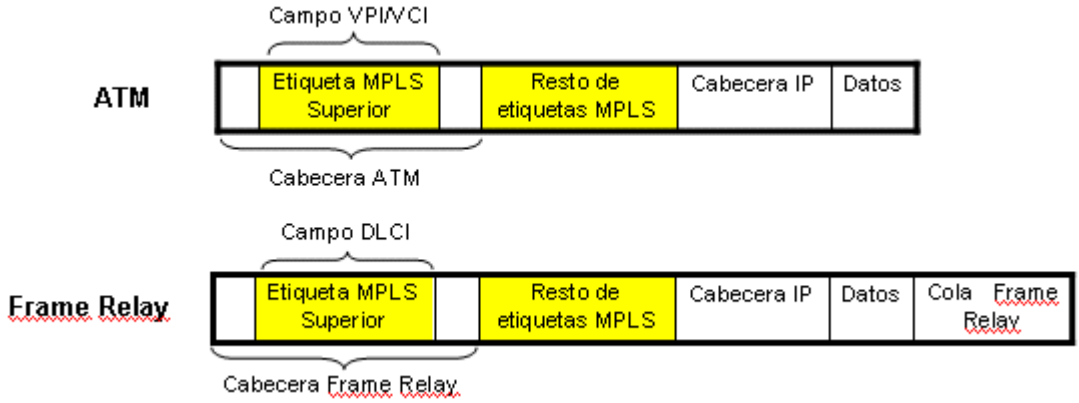


Figura 11: Ubicación de etiquetas y pila de etiquetas

Al igual que en la figura anterior se hace referencia a pila de etiquetas pues contempla el anidamiento de las mismas en escenarios multidominio, sin embargo en este caso la primer etiqueta es reemplazada por el DLCI en FR y el VPI/VCI de ATM según el caso.

B. Label Distribution Protocol

Es un Protocolo de Distribución es un conjunto de procesos por el cual un LSR informa a otro acerca de los vínculos Label/FEC. Dos LSRs que utilizan un protocolo de distribución de etiquetas para intercambiar la información de los vínculos Label/FEC son conocidos como “label distribution peers” con respecto a la información que entre ellos intercambian.

Si dos LSRs son label Distribution Peers, podemos hablar de que existe una “Label distribution Adjacency” entre ellos.

Recordemos que:

- La asignación de etiquetas se realiza salto a salto
- Pares LDP (LDP peers): Son dos LSR que usan una sesión LDP para intercambiar asignaciones de etiquetas y que pueden o no ser adyacentes.

El protocolo de distribución abarca cualquier negociación en el cual dos label distribution peers necesitan ocuparse de aprender del otro, las capacidades de MPLS.

La arquitectura de MPLS no solo puede utilizar un solo protocolo de distribución. De hecho existen varios protocolos de distribución estandarizados, como lo pueden ser MPLS-BGP, MPLS-RSVP-TUNNELS, MPLS-LDP o MPLS-CR-LDP

Particularmente hay dos protocolos muy usados, estos son LDP y RSVP (“Resource Reservation Protocol”).

LDP tiene las siguientes funciones principales:

Descubrimiento de vecinos LDP.

Si un LSR es un salto de su vecino(o sea está directamente conectado con su vecino). El LSR envía mensajes Hello de LDP como paquetes UDP al puerto 646 en modo Multicast. Un LSR vecino puede responder al mensaje Hello y con eso permite que los dos Routers establezcan a una sesión LDP. Esta detección básica se llama Discovery.

Establecimiento de la sesión TCP.

Resuelta la fase de descubrimiento de vecindad, el LSR que posea la numeración más alta, toma el rol de activo e inicia una sesión de TCP con su vecino (pasivo) que una vez aceptada deja la sesión TCP establecida. Para la sesión TCP también se utiliza el port 646.

Establecimiento y mantenimiento de la sesión LDP.

Establecida la sesión TCP se pasa al establecimiento de la sesión LDP a través del mensaje de Iniciación que envía el LDP activo, quien al recibir un Keep Alive como respuesta de su vecino deja la sesión LDP establecida.

El mantenimiento de la sesión LDP se realiza con el intercambio de mensajes Keep Alive periódicos.

Publicación, cambio y borrado de mappings de etiquetas.

Con la sesión LDP establecida comienza el intercambio y borrado de etiquetas a través de los mensajes específicos para ello.

Notificaciones de errores.

Frente a errores que se pueden producir en los mensajes existe una respuesta que consiste en un mensaje Notification que advierte sobre los mismos.

Mensajes LDP

Categoría	Tipo	Nombre
Notificación	0x001	Notification
Descubrimiento	0x100	Hello
Sesión o adyacencia	0x200	Initialization
	0x201	Keep Alive
	0x300	Address
	0x301	Address withdraw
Anuncio	0x400	Label mapping
	0x401	Label request
	0x402	Label withdraw
	0x403	Label release
	0x404	Label abort request

Figura 12: Mensajes utilizados en el protocolo LDP

Hay dos tipos de sesiones LDP:

1) Sesiones LDP directamente conectadas

Si un LSR es un salto de su vecino(o sea está directamente conectado con su vecino). El LSR envía mensajes Hello de LDP como paquetes UDP al puerto 646 en modo Multicast. Un LSR vecino puede responder al mensaje Hello y con eso permite que los dos Routers establezcan a una sesión LDP. Esta detección básica se llama Discovery, que debe continuarse con una sesión TCP en el puerto TCP 646, que se llama Negociation.

Para continuar al Discovery, se debe determinar que LSR tomará el rol de activo (lo hace el que posea la interfaz con mayor numeración)

El router que tiene el rol activo, establece una sesión de TCP o sea la conexión TCP LDP e inicia la negociación de los parámetros de sesión LDP.

Después de que se establezca la conexión TCP LDP, los LSR negocian los parámetros de sesión intercambiando mensajes Sync, LDP Init y Keepalive que son “LDP Session Messages” para establecer y mantener la sesión LDP entre 2 vecinos, incluyendo el método de distribución de etiqueta que se utilizará.

Dos métodos están disponibles:

- No solicitado rio abajo: Un LSR hace publicidad de las asignaciones de la escritura de la etiqueta a los pares sin que ellos se lo hayan pedido.

- Rio abajo a pedido: Un LSR hace publicidad de las asignaciones de la escritura de la etiqueta a un par solamente cuando, el par le pide ser notificado de ellas

Para ambos métodos se deben intercambiar Mensajes Address & Label Mapping que pertenecen al grupo “LDP Advertisement Messages”; con ellos cada router informa a su

vecino LDP la asignación de etiquetas a los distintos FEC (redes) que él tiene en su tabla RIB.

2) Las sesiones LDP nondirectly conectadas.

Cuando dos LSR no están directamente conectados, por ejemplo por la existencia de un router NO LSR en medio de los LSR.

Un LSR envía un mensaje Hello como paquete UDP unicast específicamente dirigido su LSR par. El LSR nondirectly conectado responde al mensaje Hello y ambos Routers comienzan a establecer a una sesión LDP. Esto se llama detección extendida.

Concepto de Downstrean y Upstream

Upstream: es la dirección hacia la fuente de origen de un paquete; el nodo de entrada en un dominio MPLS es el nodo ascendente más alejado posible.

Downstream: es la dirección hacia el destino de un paquete; el nodo de salida en un dominio MPLS es el nodo downstream más alejado posible. El nodo de salida también se lo conoce como el punto final del túnel.

Ordered e Independent Control

Ordered Control: Significa que un LSR no hace publicidad de una etiqueta para un FEC a menos que sea el LSR de salida para el FEC o hasta que haya recibido una etiqueta para el FEC de su par aguas abajo. De esta manera todo el LSP es establecido antes de MPLS comienza a trazar los datos en la LSP, evitando (temprana) de asignación de datos inapropiado que se produzcan en el primer LSR en el camino.

Independent Control: Control independiente significa que el LSR que envía la etiqueta lo hace en forma independiente de su vecino downstream (recordar que en el modo Ordered no puede asignar una etiqueta upstream antes de que le asigne una etiqueta su vecino downstream). En este caso el LSR no espera la asignación de una etiqueta por parte del LSR downstream antes de enviar una etiqueta a sus compañeros. El LSR anuncia una etiqueta a un vecino upstream antes de que haya recibido una etiqueta para la FEC desde el siguiente salto vecino downstream.

Métodos disponibles para la creación de LSPs:

1) Creación de LSPs con el método Independent control with Downstream Unsolicited:

Un LSR cuando detecta la aparición de una ruta nueva en la tabla de ruteo hace publicidad de las etiquetas asignadas por los pares sin que ellos se lo hayan solicitado.

2) Creación de LSPs con el método Ordered Control Downstream Stream on Demand (usado con el protocolo de señalización RSVP):

Un LSR hace publicidad de las asignaciones de la escritura de la etiqueta a un par solamente cuando, el par le pide ser notificado de ellas.

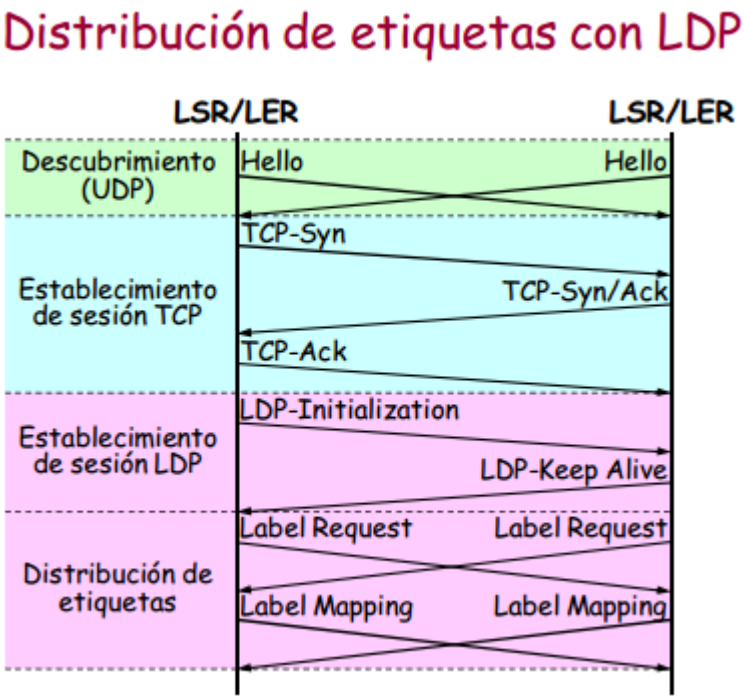


Figura 13: Secuencia de operación LDP en el modo Ordered Control Downstream Stream on Demand

Las caídas y recuperación instantánea de las interfaces, son catastróficos tanto para los IGP's como para las sesiones de LDP, debido a que cuando se cae una interfaz se cae también la sesión de LDP, cuando se levanta se tienen que reenviar todos las sesiones LDP establecidas.

Para protegernos de esto, LDP permite que la sesión de LDP no se caiga y se mantenga arriba aunque la interfaz se haya caído, se mantiene arriba gracias a una sesión de tipo targeted (vista más arriba) que se genera de forma automática entre los vecinos de LDP. Si la interfaz regresa entonces ya no se tiene que reiniciar la sesión de LDP, si en cambio la interfaz se queda abajo la sesión de LDP se quedará arriba de forma infinita a menos que se configure una duración en segundos o a menos que en ese tiempo haya otro camino hacia el vecino del LSP.

3.2.1.1.5. MPLS - TP

MPLS-TP o MPLS (Transport Profile) es un protocolo de transporte a comunicaciones por conmutación de paquetes del tipo conecction-oriented , que ha sido propiciado por el IETF. Está pensado como una tecnología de capa de red en las redes de transporte. Consiste en una evolución de la tecnología T-MPLS (desarrollado por ITU). En febrero de 2008, el ITU-T y el IETF se pusieron de acuerdo en trabajar en forma conjunta en el diseño de MPLS-TP.

Fue creado con el objetivo de lograr una versión de MPLS optimizada para redes de transporte.

Entre sus principales cualidades podemos encontrar que sus características fueron optimizadas para su aplicación en redes de transporte Carrier Class. Su forma de operación se asemeja más a la de las tradicionales de redes de transporte que a los modelos de Core IP. Es por ello que se parece más a redes de transporte basadas en circuitos. Evita los costos de desarrollo de nodos con necesidades de procesamiento para

soportar un sistema de control distribuido proveyendo configuración estática a través de un NMS (Network Management System)

Si bien el MPLS-TP está especificado a través de varias RFCs, sin embargo las más representativas son RFC 5654 y RFC 5921.

Su desarrollo se ha basado en los requerimientos proporcionados por los proveedores de servicios. Se trata de un protocolo de conmutación de paquetes orientado a la conexión. Uno de sus aspectos principales es la de eliminar características de MPLS que no son relevantes para las redes de transporte y la adición de los mecanismos que proporcionan soporte de la funcionalidad que estas redes necesitan.

Utiliza la misma filosofía de capas de redes que se utilizan en las tecnologías de redes de transporte existentes como SDH y OTN.

Como se ha dicho es una simplificación de MPLS, lo cual implica dejar de lado funciones del MPLS entre las cuales se encuentran: Penultimate Hop Popping que permite la remoción temprana de etiquetas, Equal Cost Multipath que permite el reparto de datagramas sobre distintos caminos de igual costo y Label Merge que consiste en el anidado de etiquetas. Sin embargo respeta el mecanismo de encaminamiento basado en etiquetas tradicional de MPLS. Una de las principales características es que no cuenta con los mecanismos de panel de control distribuido, descargando esa función en un NMS (Network Management System). El establecimiento de los LSPs. Se hace a través de un panel de control estandarizado usando GMPLS (Generalized MPLS) que consiste en un conjunto de RFCs que proveen un plano de control Carrier class. En caso de una caída temporaria del plano de control, ésta no afecta al plano de datos dado que ambos planos están separados. Si bien el MPLS-TP pierde características de MPLS, agrega capacidades deseadas por las redes de transporte entre las que se encuentran: Nuevas capacidades de OAM del plano de datos, utilizando un canal dedicado de señalización en banda llamado GAC o G-ac (Generic Associated Channel). Capacidades de protección nuevas que permite a los operadores lograr sub-50ms para protección del camino.

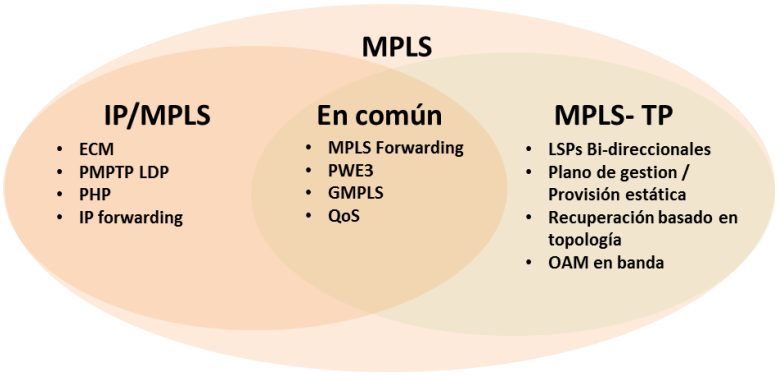


Figura 14: MPLS - TP

El ámbito de aplicación de MPLS-TP tiene su mayor aplicación en acceso y en agregación de servicios, en especial en agregación regional y metro en distintos tipos de tráfico (ATM, Frame Relay, y TDM). También tiene su ámbito de aplicación en backhaul móvil (para el transporte de trafico 3g y LTE), y para la comercialización directa de MPLS-TP en el mercado corporativo para aplicaciones que pueden sacar provecho de sus prestaciones.

Los Carriers cuentan ahora con una mezcla de opciones de tecnología para la próxima generación de redes de transporte de metro/regionales de acceso y agregación. La migración hacia las soluciones de transporte convergentes basados en paquetes, los

obligará a elegir entre las distintas alternativa, teniendo el MPLS-TP grandes chances de éxito por ser la filosofía de comunicación que los operadores conocen. Su arquitectura atrae la atención y el apoyo de operadores de redes muy grandes.

Tanto IP/MPLS como MPLS-TP tienen sus propias funciones que desempeñar en la red. MPLS-TP nos garantiza la escalabilidad, simplicidad y bajo costo. Por otro lado MPLS es una plataforma de transporte robusta y escalable para entornos de red de núcleo, y por lo tanto más caro que el MPLS-TP que es una tecnología de menor costo, con fuertes capacidades de transporte.

3.2.1.1.6. VPNs (Virtual Private Networks)

La característica principal de las VPN es que utilizan la infraestructura de las redes públicas o privadas compartidas para ofrecerle a un cliente las facilidades de una red privada. Esto permite a los usuarios beneficiarse de las prestaciones, seguridad y gestión de redes de alta performance a costos más accesibles.

Las VPNs se crean mediante el establecimiento de conexiones virtuales entre los equipos a comunicar.

Las redes de transmisión de datos X.25, Frame Relay y modo de transferencia asíncrono (ATM) con sus mecanismos de circuitos virtuales fueron las primeras que permitieron la implementación de redes virtuales independientes para cada cliente, soportadas sobre una misma red con nodos y enlaces físicos compartidos provistos y operados por las compañías de telecomunicaciones.

Existen distintos puntos de vista respecto de si estas tecnologías deben ser consideradas o no VPNs, a los efectos de entender la lógica la evolución de estas últimas las incluiremos como tales y las consideraremos VPNs de primera generación.

Sin embargo las primeras VPNs que fueron reconocidas como tales son las que se establecían sobre las redes IP, destacándose entre ellas las que armaban los clientes entre ordenadores y servidores de VPN en entornos corporativos conocidas como VPNs de acceso remoto. Este tipo de VPN permite que empleados puedan acceder a la intranet de su empresa desde su casa o mientras viaja fuera de la oficina

Otro tipo de VPNs son las punto-a-punto, que permiten unir las oficinas geográficamente dispersas de una empresa.

Las nuevas tecnologías permitieron implementar las VPNs basándolas en redes IP e IP / Multiprotocol Label Switching (MPLS), permitiendo bajar los costos, disponer de mayor ancho de banda. La línea de abonado digital (DSL) y las redes de fibra óptica son un ejemplo de esto.

A continuación detallaremos distintas formas de clasificar a las VPNs.

3.2.1.1.6.1. Clasificación de las VPNs

A. Evolución histórica de las VPNs

De acuerdo a la evolución histórica de las VPNs, podemos clasificarlas de la siguiente manera:

- 1ª Generación

Terminadas en el CE a base de circuitos virtuales ATM/Frame Relay sobre una red de conmutación de paquetes del proveedor

- 2ª Generación

Los proveedores ofrecen servicios para gestionar los routers del cliente usados en las terminaciones en el CE

- 3ª Generación

VPNs de nivel 3 terminadas en el PE y basadas en IP/MPLS

- 4ª Generación

VPNs de nivel 2 terminadas en el PE y basadas en IP/MPLS

B. Tipos de VPNs

Existen distintos aspectos que permiten caracterizar a las VPNs y una VPN puede contener varias estas características. En base a esta óptica se las puede clasificar por:

- Según el punto de terminación del túnel.
  - Basadas en el CE (overlay)
  - Basadas en el PE (peer-to-peer)
- Según el tráfico de cliente transportado
  - VPN de nivel 3
  - VPN de nivel 2
- Según el tipo de red del proveedor
  - IP, IP/MPLS, ATM, Frame Relay, SONET/SDH, red telefónica, etc.
- Según la tecnología (protocolos) utilizados para la implementación de túneles
  - Túneles IPSec, L2TP, PPTP, MPLS-LSP, ATM-VP/VC,
  - Frame Relay VC, SONET/SDH VT, PPP/Dial-up
- Número de redes conectadas
  - Punto a punto: 2 sedes
  - Multipunto: más de dos sedes
- Los niveles de seguridad proporcionados.
- Si ofrecen de sitio a sitio o conectividad de acceso remoto.

Para nuestro estudio la primera gran división a considerar es:

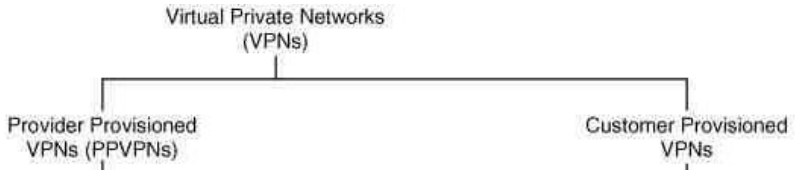


Figura 15: Tipos de VPNs

- Customer Provisioned VPN (CPVPN)

Son túneles que interconectan siempre terminales de clientes entre sí (basadas en el CE) que generalmente son simples túneles que interconectan equipos de clientes y en donde la red sólo transporta paquetes IP convencionales.

- Provider Provisioned VPN (PPVPN)

Son túneles que interconectan siempre equipos del Carrier y que permiten proveer los servicios definidos por el MEF. Este es el tipo de túneles en que se focaliza nuestro estudio.

3.2.1.1.7. Provider Provisioned VPN (PPVPN)

Las PPVPN son redes privadas virtuales en las que el proveedor es el responsable de crear y administrar los túneles para el tráfico privado entre los puntos de conexión de clientes.

En la actualidad las redes de los proveedores utilizan la tecnología MPLS que como sabemos, aprovecha el direccionamiento IP y el protocolo de ruteo OSPF, para el establecimiento de los virtual path.

Por este motivo los proveedores utilizan su infraestructura MPLS como medio de transporte para crear túneles entre los sitios privados. Creando de esta forma un nuevo tipo de servicio, y por ende un nuevo negocio utilizando su red de transporte existente.

Sobre la infraestructura de red MPLS de los Carriers se pueden implementar dos tipos de VPN, las L3VPN (4° generación de VPN) y las L2VPN (5° generación de VPN).

Sobre Las L2VPN nos explayaremos más adelante, pero a continuación haremos una breve mención sobre las L3VPN para que se entienda la diferencia entre ambas.

Las L3VPN también llamadas VPRNs (Virtual Private Routed Networks), permiten que la red sea vista como un super-router dado que para implementar las VPNs se tienen en cuenta las tablas de ruteo de nivel 3 de cada cliente.

El proveedor debe utilizar BGP (MP-BGP) como protocolo de ruteo dentro de la red del proveedor con el objeto de intercambiar la información de ruteo, lo que aumenta la complejidad del diseño y puesta en práctica de este tipo de redes.

Los clientes se conectan con el router del proveedor de servicio, con el que intercambia tablas de rutas, esta información de ruteo es colocada en tablas de ruteo específicas para cada cliente en el router del proveedor (y es transportada con MP-BGP dentro de la red).

Las L3 VPN se puede utilizar para implementar VPNs en redes corporativas, no utilizándose normalmente en redes de servicios públicos debido a su complejidad. Han o

están sido reemplazadas por las L2VPN que nos libera de la complejidad del manejo de la numeración IP a través de las tablas de ruteo.

De las dos opciones la tecnología L2VPN presenta grandes ventajas sobre la L3VPN dado que es vista por los clientes como un switch de nivel 2, evitando las serias consideraciones de plan de numeración IP que tienen las L3VPN. Es por ello que las L2 VPN es la tecnología utilizada para la implementación de los servicios Metro Ethernet CE2.0.

L2 MPLS VPN

Las L2 MPLS VPN permiten la implementación de dos tipos de servicios, VPWS (Virtual Private Wire Service) que implica la implementación de un Pseudo Wire que emula conexiones punto a punto y VPLS (Virtual Private Lane Service) que emula un gran LAN Switch permitiendo conexiones punto a punto y multipunto.

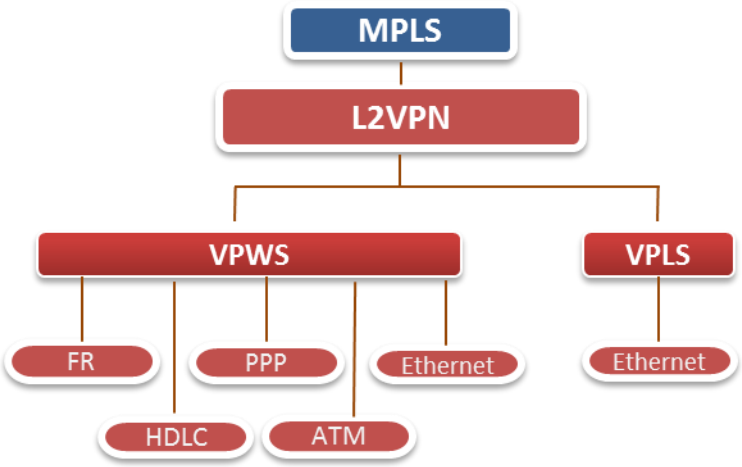


Figura 16: Modelos L2VPN

Utilizando L2VPNs se logra conectividad en capa 2 entre los sitios, tunelizando las diferentes tecnologías en caminos LSP. De esta forma, se logra transportar una trama L2 entre dos sitios remotos. Desde el punto de vista del cliente, la red del proveedor simula ser una conexión directa (cable) entre los sitios. Las L2VPN son de tipo punto a punto. Los equipos frontera del cliente (Router Customer Edge, CE) mapean el tráfico a un circuito específico (Ethernet, ATM, Frame Relay, etc.) y lo envían al proveedor (Router Provider Edge, PE). El proveedor encapsula dicho tráfico en un LSP, y lo envía hacia el Router PE remoto asociado a dicha conexión. Para obtener conectividad entre varios sitios de una L2VPN, se debe configurar un esquema full-mesh entre los Routers PE. Para este tipo de aplicaciones se puede considerar la utilización de VPLS.

Las tramas del cliente se transmiten utilizando un stack de dos etiquetas MPLS. La etiqueta externa identifica al LSP entre los Routers PE, y la interna identifica a la VPN (Circuito L2) que se está interconectando. Este esquema permite que múltiples VPNs utilicen el mismo LSP de transporte. Debido a que la conexión a través del proveedor se realiza en capa 2, el esquema de ruteo del cliente se implementa en los equipos CE y no involucra al proveedor.

Existen dos variantes de VPNs de capa 2. La diferencia entre las mismas radica en el protocolo de señalización y control que utilizan. Dicho protocolo se utiliza para establecer las sesiones entre Routers PE, y para negociar la etiqueta VPN a utilizar. Los esquemas son BGP L2VPN (Utiliza el protocolo BGP, draft-Kompella) y LDP L2VPN o LDP L2 Circuit (Utiliza el protocolo LDP, RFC 4447). Al utilizar el protocolo BGP se logra mayor escalabilidad y prestaciones como auto-descubrimiento de vecinos, pero el esquema se

hace más complejo. Al utilizar el protocolo LDP, se logra un ambiente más sencillo, pero se debe configurar explícitamente cada vecino y como consecuencia se pierde escalabilidad.

Usando estas tecnologías, el cliente puede tercerizar el transporte de circuitos manteniendo el control del ruteo, utilizando el protocolo de capa 3 que desee. Por otro lado, el proveedor puede utilizar la infraestructura IP/MPLS existente para brindar un nuevo servicio de valor agregado, y utilizar el mismo LSP de transporte para todos los servicios entre Routers PE.

3.2.1.1.7.1. Red MPLS que soporta VPN

Como se ha visto, las nuevas tecnologías de implementación de VPNs lo realizan sobre MPLS. Dado que estos routers agregan funciones para el armado de las VPNs, se los denomina con nuevos nombres. Lo que en una red MPLS se llama LER (Label Edge Router) pasa a llamarse PE y los LSR (Laber Switching Router) pasa a llamarse P.

A continuación mostramos la arquitectura de una red IP/MPLS que permite implementar VPNs.

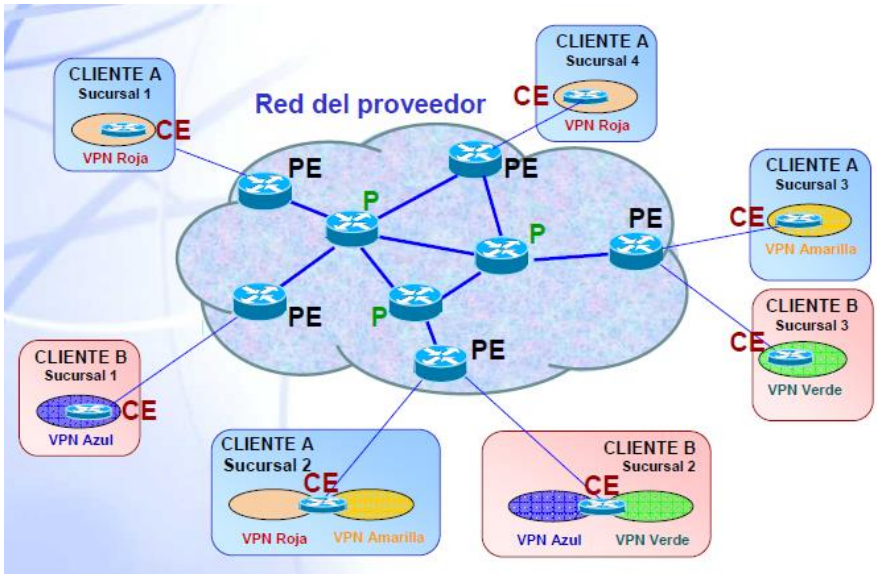


Figura 17: Arquitectura IP/MPLS VPN

Dispositivos de cliente (C)

Un dispositivo que está dentro de la red del cliente y no está conectado directamente a la red del proveedor de servicios. Dispositivos de C no son conscientes de la VPN.

CE (Customer Edge): Dispositivo borde de cliente Edge

Un dispositivo en el borde de la red del cliente que proporciona acceso a la PPVPN. Puede ser provisto y gestionado por el cliente o provisto y gestionado por el proveedor dela red, siendo de responsabilidad del proveedor o del cliente según el caso. Se conecta al PE a través del Attachment Circuit (AC). En el caso de VPLS, se asume que la interface entre PE y CE es Ethernet. En el caso de VPWS la interface puede ser FR, ATM, PPP, HDLC o Ethernet.

Attachment circuit (AC)

Es el circuito físico que une un CE a un PE. Un AC puede ser, por ejemplo, un DLCI de Frame Relay, un VPI / VCI de ATM, un puerto Ethernet, una VLAN, o un LSP MPLS. Uno o varios ACs pueden pertenecer a la misma VFI.

PE (Provider Edge): Dispositivo de borde de proveedor

Dispositivo de borde de proveedor: Un PE es un dispositivo o conjunto de dispositivos, en el borde de la red de los proveedores al que se conecta las redes de los clientes a través de dispositivos de CE. La unión del PE y el CE se realiza a través del AC y es el punto de entrada del cliente a la VPN. Los PEs son los elementos claves de las VPNs pues los túneles entre los distintos PE son los que conforman las VPNs. Es también el dispositivo donde residen las funciones las funciones necesarias para las decisiones de forwarding y switching (que siempre se realizan al ingreso de la red L2VPN)

P (Provider): Dispositivo de proveedor

Un dispositivo P opera dentro de la red del proveedor y no interactúa directamente con el punto final de cliente. Proporcionan enrutamiento de los túneles en la PPVPNs.

Pseudowire (PW):

(PWE3) es un mecanismo que emula el funcionamiento de interconexión de un servicio de telecomunicaciones (por ejemplo un circuito TDM, Frame relay o ATM) sobre una red de paquetes.

VC (virtual circuit):

Martini-based data encapsulation, tunnel label is used to reach remote PE, VC label is used to identify VFI. One or multiple VCs can belong to same VFI.

Hasta ahora hemos mencionado los components que tiene una L2 VPN, ahora nos concentraremos en los components propios de una VPLS.

Virtual Brige instance:

Reside dentro de un PE (puede tener distintos nombres según el proveedor), Un Virtual Bridge Instance pertenece a una sola VPLS El VB realiza las funciones standard de bridging de un Lanswitch. Al igual que un Lanswitch, se encarga del forwarding basado en la MAC addresses y VLAN tags.

VPLS Service ID (VPLS SID):

Es un término que utilizamos para identificar el conjunto de todos los VB que conformarían el VPLS para un cliente y que se ve como un súper bridge (a nivel de toda la red). Soporta el Multipoint briging entre todos los ACs y VCs. Es un dominio de broadcast como en todo switch está separado de los otros dominios de broadcast de las otras VPLS SID, Cada VPLS SID se comporta en el súper bridge como una VLAN se comporta en un Lanswitch.

. El Pseudo Wire (PW)

Pseudowire abreviado como PW) es un mecanismo para emular varios servicios de redes o de telecomunicaciones a través de redes de conmutación de paquetes que utilizan Ethernet, IP, o MPLS. Los servicios emulados pueden incluir servicios como Frame Relay, Ethernet, ATM, TDM o SDH. Tal como se define en el RFC 3985 [PWE3] Arquitectura") un pseudowire ofrece el mínimo de funcionalidad necesaria para emular una conexión física punto a punto con la calidad requerida por las características de cada servicio que emula.

Un PW consiste en un circuito emulado Punto a Punto, para lograr esto se requieren un par de LSP (MPLS) en direcciones opuestas. Dentro de cada LSP se ubican VC identificados por una PW label. La etiqueta del PW se mantiene extremo a extremo dentro de la red MPLS entre los dos PE

Para la conexión de los PE se pueden usar targeted LDP (para el caso que usemos señalización LDP).

Pseudowire Emulation Edge to Edge (PWE3), indica la forma en que se encapsula, transporta, controla, gestionan los servicios emulados sobre PSN sobre los PW.

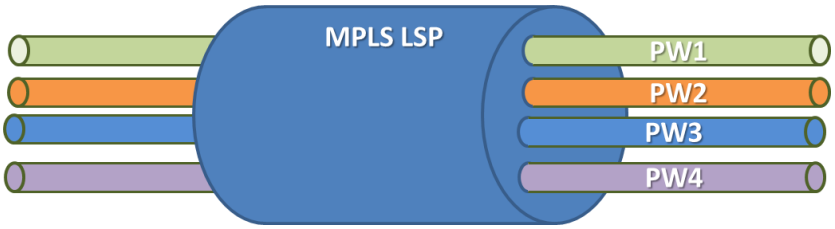


Figura 18: Pseudo Wire (PW)

Virtual Private LAN service (VPLS)

VPLS es un PPVPN de Capa 2 (L2VPN), que emula una LAN tradicional. VPLS permite que los segmentos remotos de LAN de un cliente se vean como una sola LAN, con una cobertura interurbana.

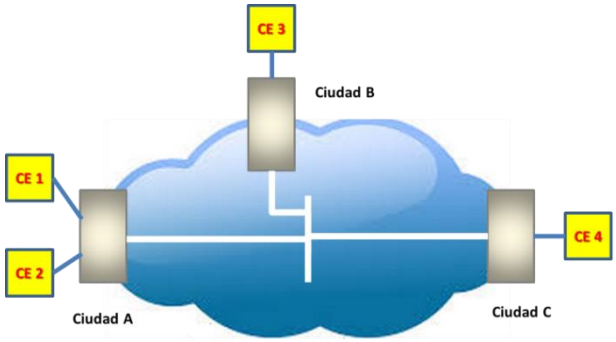


Figura 19: Modelos VPLS

En este caso el proveedor de red emula un gran Self Learnig Bridge (que podría ser visto como un súper bridge), que aprende las MAC origen, conmuta en función de la MAC destino y deja pasar las tramas broadcast / multicast / unknown.

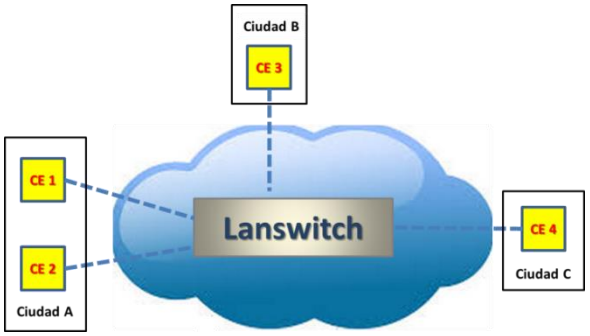


Figura 20: Modelos VPLS

VPLS también es conocido como TLS (transparent LAN Service) y como ELAN service.

VPLS se basa en VLLs tradicionales. Soporta comunicaciones multipoint-to-multipoint.

La inteligencia del servicio reside en los equipos PE, la red MPLS desconoce el contenido de los túneles que transportan y por lo tanto del servicio VPLS, para ella son túneles como los de cualquier otro cliente.

3.1.3.1. Arquitectura de la red VPLS

En una configuración simple todos los sitios de cliente que se conectan a los PEs de la red pertenecen a una sola instancia VPLS.

Los equipos de un cliente se conectan a uno de los Virtual Briges que cada PE tiene creados para él, y todos los VB creados para un cliente se conectan full mesh entre sí a través de Pseudo Wires.

Los PE tendrán configurados tantos Virtual Briges como clientes distintos tenga conectados, donde tiene asociada la interface y la VLAN (en caso de existir).

Es importante resaltar que existirán tantas redes de VBs independientes como servicios VPLS tenga implementados el proveedor. Por otro lado los PEs solo tendrán VB de un VPLS en los Pes que tenga a este cliente conectado.

El siguiente esquema nos permite visualizar lo explicado.

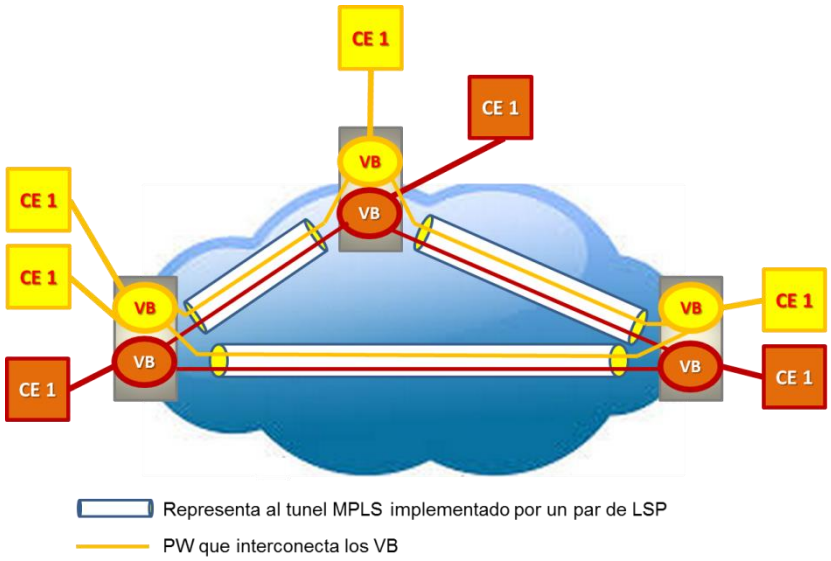


Figura 21: Modelos VPLS

3.1.3.2. Forma de operación de VPLS

Como dijimos los equipos a los que se conectan los clientes se son los PE, y en una red VPLS los PE deben estar interconectados full mesh.

Esta conexión se realiza a través de PWs, que utilizan un par de LSPs (recordar que los LSP en MPLS son unidireccionales, y los PWs son full dúplex).

Los Virtual Briges de cada VPLS se interconectan con PW solo asignados a ese servicio, en la Figura 21 se ve que los VB amarillos se interconectan con los PW amarillos, y los VB

rojos se interconectan con los PW rojos (se han utilizado colores para una mejor visualización).

3.1.3.3. Aprendizaje de las MAC y fordwarding

Cuando un VB de una VPLS recibe una trama del CE de un cliente, al igual que un Self Learning Bridge (no olvidemos que lo está emulando) aprende la MAC origen del CE lo almacena en la tabla de MAC del VB del VPLS del cliente (anotando en que puerta esa MAC se encuentra ubicada).

Luego analiza la MAC destino y pueden ocurrir dos cosas. La primera es que la MAC destino no se encuentre en la tabla de MAC del VB o que sea una dirección de broadcast, en este caso la trama recibida se envía a todos los VB asociados (a través de la malla de PW) que residen en los PE remotos. La segunda es que encuentre la MAC destino en el VB, en este caso sólo envía la trama al VB destino a través del PW que lo asocia.

Cuando los VB de este servicio VPLS ubicados en los PE remotos reciban las tramas, lo primero que harán es anotar en su tabla MAC la MAC origen (SA) de la trama (anotando como ubicación de la misma el PW por el que le llegó).

Respecto de la dirección destino en caso que sea una MAC unicast la entrega a la puerta correspondiente, y en caso que sea un broadcast se lo envía a todas las puertas de cliente que ese VB tenga.

Es importante mencionar que siempre que llegue una MAC destino unicast, la misma existirá en el VB destino, pues el hecho que llegue unicast implica que la MAC fue encontrada en el VB origen y por lo tanto aprendida por señalización (LDP o BGP).

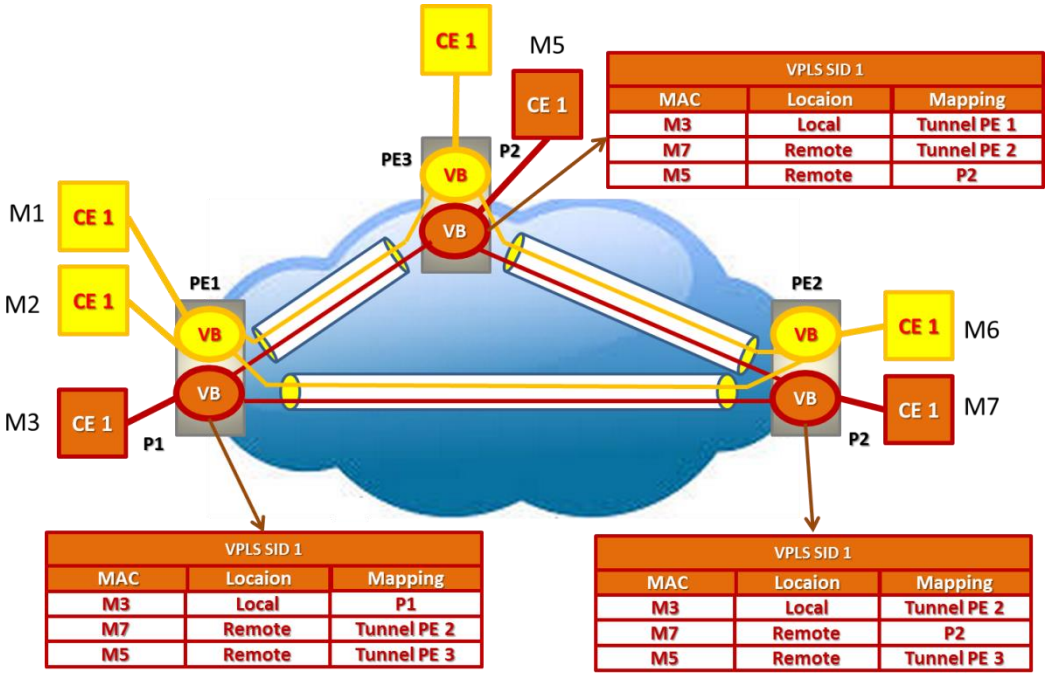


Figura 22: Modelos VPLS

3.1.3.4. Los loops en VPLS

Para evitar loops los VB implementan Split Horizon. No existe la posibilidad de la existencia de loops dentro de la red pues todos los VB están conectados full mesh.

El problema de los loops en las redes de LAN Switches es abordado por las normas STP, RST y MSP protocol.

Sin embargo puede ocurrir que el cliente (dado su topología externa a la red, requiera del uso de mecanismos para evitar loops (tal sería el caso de redes de clientes que se conectan a dos PE, pero que también tienen uniones externas entre sí).

Por ello VPLS tiene dos formas de funcionamiento a este respecto, que son:

VPLS Transparen Mode, que transporta los BPDUs generados por el cliente en forma transparente (solo le agrega las etiquetas de PW y VP para su transporte), haciéndoselo llegar a todos los AC (excepto por el que lo recibió) en donde haya Pes de este servicio VPLS.

VPLS Participation Mode, los VB también generan BPDUs dentro del core, el Bridge ID que se utiliza es la prioridad que le otorguemos al VB más MAC address que cada hardware PE tiene asignada de fábrica. El Port ID será el Virtual Channel port.

3.1.4. Virtual Pseudo Wire Service (VPWS)

En el caso de VPWS, el proveedor emula un circuito entre dos puntos de clientes, lo hace a través de un pseudo-wire a través de su red.

Esta tecnología ha sido desarrollada como una alternativa de mercado para los servicios de FR y ATM debido a que se presenta servicios similares. También es utilizada para inter-operar con estas tecnologías legacy. De esta forma el proveedor logra importantes ahorros dado que no requiere de redes específicas para cada servicio. También permite el transporte de los protocolos FR, ATM, HDLC y PPP, lo cual se muestra en la siguiente figura.

Figura 23: Modelo de transporte VPWS

Señalización y autodescubrimiento en L2 MPLS VPN

En las redes L2VPN, se deben atender dos problemas a saber:

Auto-Discovery: Consiste en lograr que los múltiples VB residentes en los PEs que pertenecen a las distintas VPLS, se encuentren entre ellos.

Señalización: Es la forma en que se establecen los túneles y que se distribuyen las etiquetas entre los PEs.

En L2 MPLS VPN, se pueden utilizar dos protocolos, ambas utilizan una cabecera MPLS estándar para encapsular datos.

Los protocolos que se utilizan, que pueden ser:

- Basado en BGP: Que realiza ambas funciones, Auto-Discovery y Señalización. RFC 4761.

- Basados en LDP: Que solo realiza la función de Señalización. RFC 4762.

Señalización en L2 MPLS VPN basada en BGP

Se basa en un borrador de la especificación escrito por Kireeti Kompella, de Juniper Networks.

Utiliza el Border Gateway Protocol (BGP) como el mecanismo para routers PE para comunicarse entre sí acerca de sus conexiones con los clientes.

Cada router se conecta a una nube central, usando BGP. Esto significa que cuando se agregan (por lo general a los nuevos routers) nuevos clientes, los routers existentes se comunicarán entre sí, a través de BGP, y añaden automáticamente los nuevos clientes con el servicio.

Señalización en L2 MPLS VPN basada en LDP

El segundo tipo se basa en un borrador de la especificación de Luca Martini de Cisco Systems. Este método también se conoce como un circuito de capa 2.

Utiliza el protocolo de distribución de etiquetas (LDP) para el establecimiento de la comunicación entre routers PE. En este caso, todos los routers de habla LDP intercambiarán FECs y establecerán LSP con cualquier otro enrutador de habla LDP en la red (o el otro router PE, en el caso de que LDP sea tunelizado en RSVP-TE), que difiere de la metodología basada en BGP.

El estilo basado en LDP de L2 VPN define nuevos TLV y parámetros para la LDP para ayudar en la señalización de las VPNs.

3.2.1.1.7.2. L3 MPLS VPN

L3 MPLS VPN es un servicio de red privada virtual Provider Provisioned que mantiene la arquitectura ya mencionada de equipamientos CE, Pe y P de las redes MPLS. A diferencia de la L2 MPLS VPN que se comporta como un gran bridge, en este caso la L3 MPLS VPN se comporta como un gran router.

Los routers PE y P del Carrier son interconectados en malla completa y topologías de redes jerárquicas. Los equipos de cliente que se conectan a la VPN son “routers” CE y están distribuidos geográficamente. Los CE se conectan a los routers PE del Carrier.

Los routers PE manejan también las rutas de usuarios en tablas llamadas VRF (VPN Routing and Forwarding), teniendo una VRF para cada VPN. Por el contrario los routers P no manejan las rutas de los usuarios.

Sin embargo los routers PE y P tienen asignadas direcciones públicas y tienen por lo tanto sus propias tablas de ruteo.

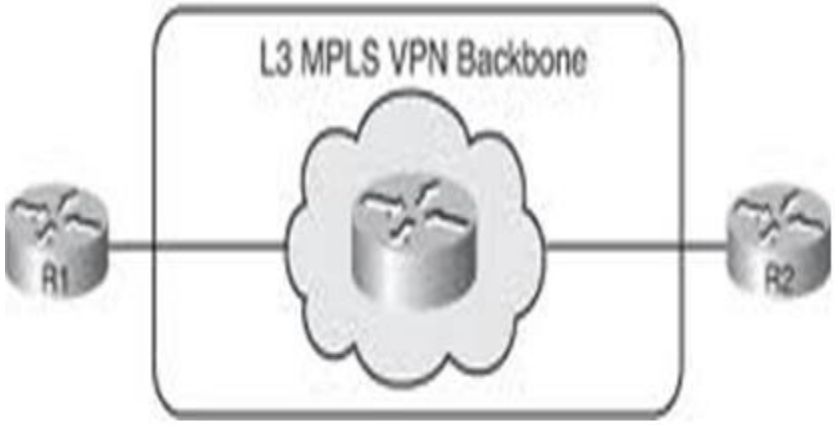


Figura 24: L3 MPLS VPN

PEs y Ps comparten un IGP (OSPF, ISIS, EIGRP) que los utilizan para actualizar sus tablas de ruteo con direcciones de red públicas

Todos los PE tienen interconexión directa vía túneles.

Los PEs usan MP-BGP para informar sobre sitios y VPNs conectadas, para lo cual arman sesiones MP-iBGP entre ellos.

Arquitectura básica de una L3VPN

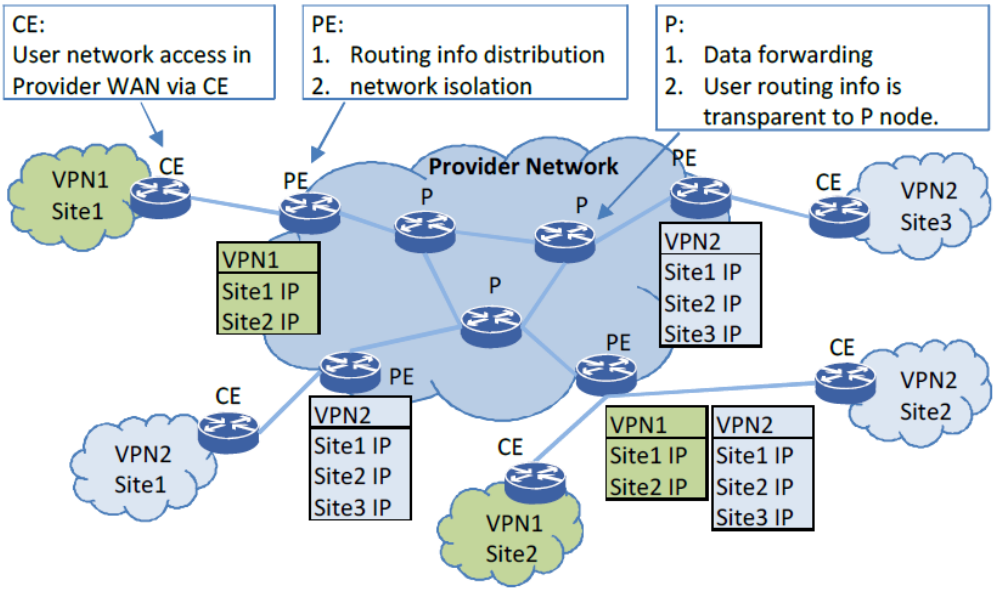


Figura 25: Arquitectura básica de una L3VPN

Túneles que interconectan los PEs involucrados en la red y que transportan instancias de VPN.

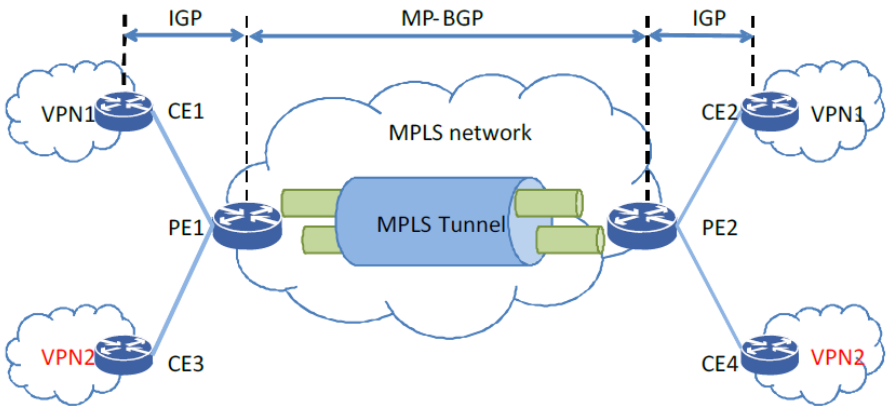


Figura 26: Túnel MPLS

Cada vez que llega un paquete IP al PE este busca la tabla VRF a la que corresponde, le inserta la etiqueta VPN label al paquete, encapsula todo en un túnel MPLS (un LSP) y lo envía en forma transparente a través de este al PE destino. Este último lo entregará al CE del sitio de cliente que corresponda según la VPN.

El formato de la trama del túnel es la siguiente:

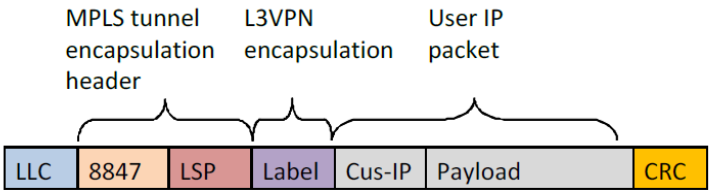


Figura 27: Formato de la trama del túnel MPLS

Donde el túnel MPLS se identifica por:

- 8847 que es el Ethertype que nos indica la presencia de MPLS
- LSP es la etiqueta de MPLS

El Label (L3 VPN encapsulation): nos indica la etiqueta que corresponde a cada VPN y que en sus extremos encontraremos las VRF de cada VPN.

Resumen de operación básica

1. Activación de VPNs (tantas VRFs por site como VPNs distintas)

2. CEs “enseñan” sus rutas a cada PE, que las ubica en la VRF correspondiente

3. PE incorpora información de cada VPN al proceso BGP

4. PE asigna una etiqueta diferente a cada VPN, e informa lo que conoce a otros PEs

5. PE receptor distribuye adecuadamente lo recibido de otro PE a cada CE, según corresponda a la VPN de destino

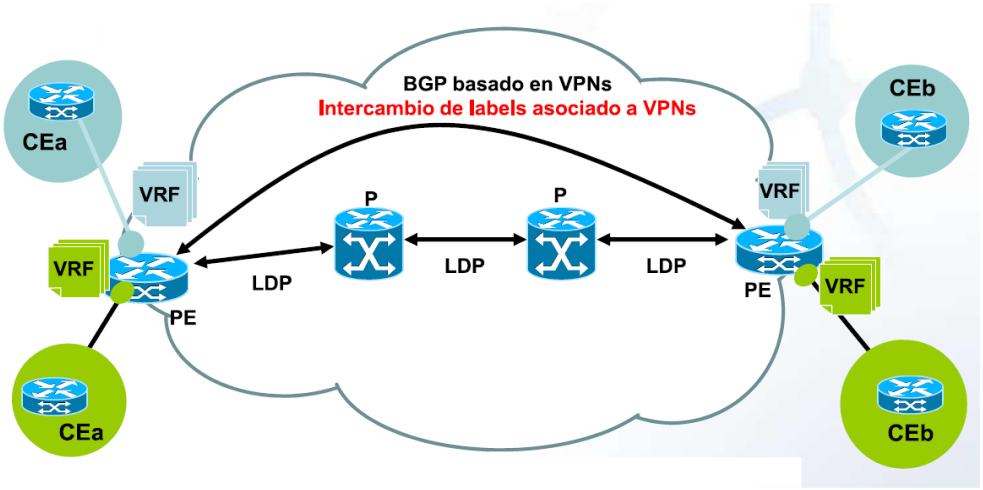


Figura 28: Operación básica

Debemos recordar que la red MPLS mantiene su señalización de etiquetas.

3.2.1.2. Metro Ethernet Fórum

El MEF es una alianza de la industria mundial que comprende más de 220 organizaciones, incluyendo proveedores de servicios de telecomunicaciones, fabricantes de equipos de redes y/o software, vendedores de semiconductores y organizaciones de prueba. Su función es definir todos los aspectos relacionados con los servicios Carrier Ethernet, la misión es acelerar la adopción mundial de redes y servicios Ethernet Carrier-class.

El Metro Ethernet Forum (MEF) ha definido los atributos de calidad de Carrier que distinguen a "Servicios de Carrier Ethernet" de los servicios Ethernet tradicionales basados en LAN. El MEF es agnóstico respecto de las tecnologías que implementan los servicios que comentaremos en este documento. Los proveedores adoptaron las tecnologías MPLS, MPLS-TP, PBB y PBB-TE para este tipo de prestaciones por tener las características y capacidades necesarias para prestar los servicios Carrier Ethernet, estas tecnologías las explicaremos en detalle.

3.2.1.2.1. CE 1.0 – Primera versión de Carrier Ethernet

En sus comienzos (2001) el MEF se focalizó en la necesidad de impulsar la tecnología Metro Ethernet, definiendo servicios y ordenando el caos que existía en la prestación de dichos servicios. A partir de allí se focalizó en los primeros servicios Carrier Ethernet, expandiendo estos a ámbitos nacionales e internacionales.

La primera versión definida por el MEF ofrece servicios Carrier Class estandarizados en la red de un proveedor, a esta se la conoce como CE1.0 (Carrier Ethernet1.0).

A continuación se comentan los servicios CE 1.0:

3.2.1.2.1.1. Servicio E-Line

El servicio E-Line consiste en un tipo de servicio Ethernet que se basa en un Ethernet Virtual Connection (EVC) punto-a-punto, para interconectar dos UNIs (User–Network Interfaces).

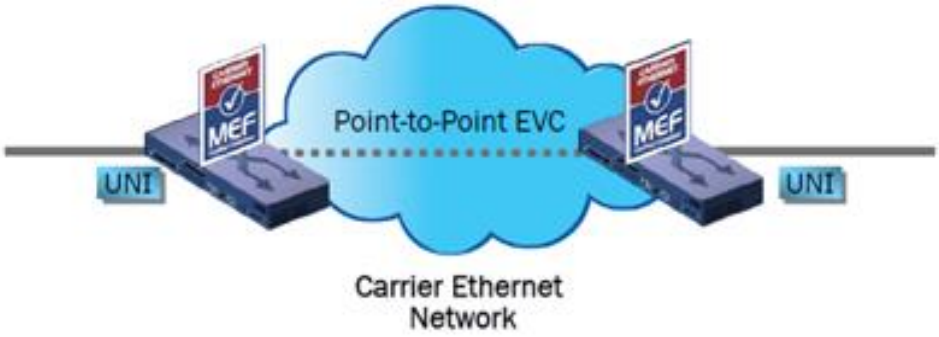


Figura 29: Servicio E-Line

Los Servicios E-Line que se pueden ofrecer son:

- Ethernet Private Lines
  - Una sola UNI en cada extremo de red.
  - Similar a un circuito TDM.
- Virtual Private Lines
  - Una UNI se usa para múltiples conexiones virtuales.
  - Similar a Frame Relay o ATM

3.2.1.2.1.2. Servicio E-LAN

El servicio E-LAN está basado en un EVC (Ethernet Virtual Connection) multipunto a multipunto.

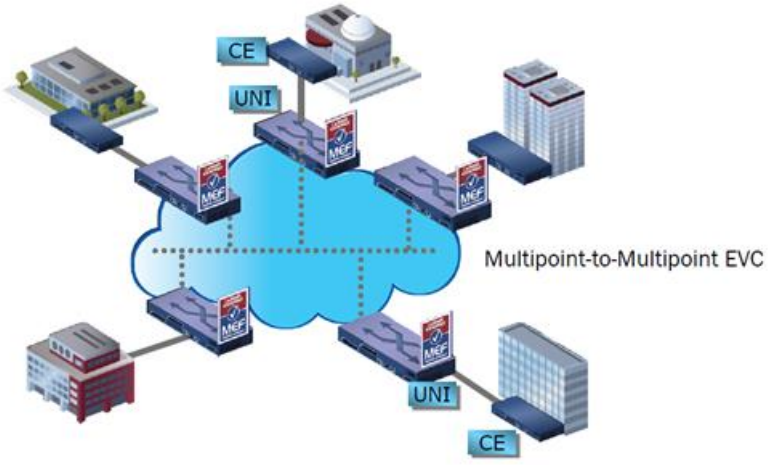


Figura 30: Servicio E-LAN

Los Servicios E-LAN que se pueden ofrecer son:

- Multipoint L2 VPNs Multipunto.

- Servicio de LAN transparente.

3.2.1.2.1.3. Servicio E-Tree

Es un tipo de servicio que está basado en EVCs multipunto que convergen en un nodo raíz.

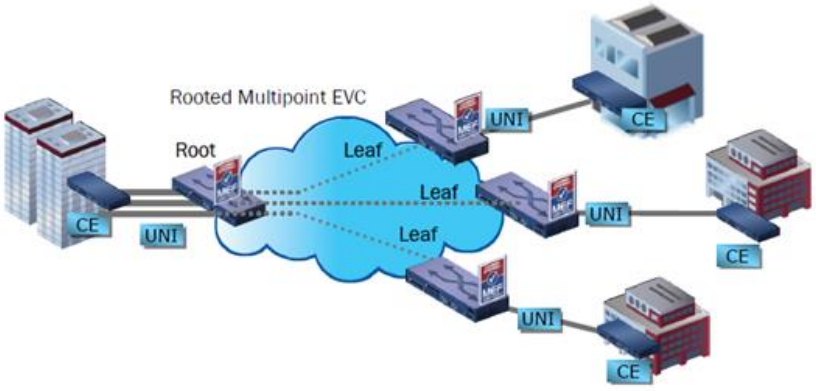


Figura 31: Servicio E-Tree

Servicios:

- Topología punto a multipunto.
- Provee separación de tráfico entre los terminales hoja del multipunto.
  - El nodo raíz se puede comunicar con cualquier hoja.
  - Las hojas solo se pueden comunicar con el nodo raíz.

Se puede resumir los tipos de servicios CE 1.0 en el siguiente gráfico:

MEF Service	Provides
E-Line	Point-to-point EVC
E-LAN	Multipoint-to-multipoint EVC
E-Tree	Rooted Multipoint EVC

Figura 32: Resumen Servicios CE 1.0

3.2.1.2.2. CE 2.0 – Next generation Carrier Ethernet

Mientras que CE 1.0 permitió la estandarización de redes y servicios Ethernet en el marco de una red de proveedor de servicios, Carrier Ethernet CE 2.0 (lanzado en 2012) innovó

con estándares de red para proveedores de servicios, que tiene tres características diferenciales: maneja Múltiple Clases de Servicio (Multi-CoS), e incorpora más funcionalidades de gestión e interconexión para expandir el alcance de los servicios.

Estas tres características se suman a la expansión de la cantidad de servicios soportados, que en CE 1.0 eran tres, ahora son ocho: dos por cada clase de servicio (E-Line, E-LAN, E-Tree y E-Access, las tres primeras ya estaban en CE 1.0), según están definidos por las especificaciones de MEF.

El servicio E-Access, permite a proveedores de servicios CE 2.0 minoristas ampliar su cobertura de manera más eficiente y económica mediante asociaciones con proveedores mayoristas.

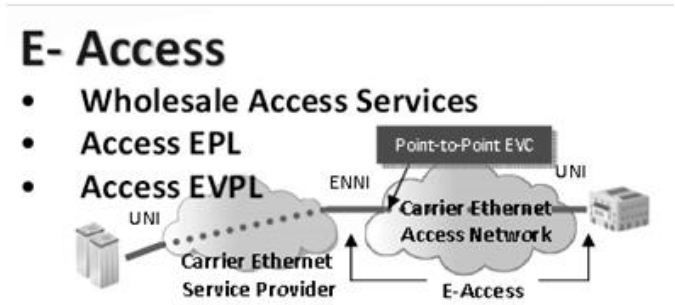


Figura 33: Resumen Servicios CE 2.0

“La aprobación de las especificaciones y los acuerdos de implementación de MEF en 2012 marcan el momento crítico en que esta nueva generación de redes y servicios pueden ser implementados y desplegados como nuevos estándares de la industria” literales palabra del presidente y fundador de MEF, Nan Chen.

Con respecto a las nuevas características de MEF CE 2.0, podemos detallar:

Multi-CoS

Las nuevas extensiones de Class of Service (clase de servicio), por primera vez, estandarizan los objetivos de desempeño a través de varias capas geográficas de desempeño y aplicaciones. Esto resulta en una calidad de servicios mejorada y optimiza la eficiencia, especialmente cuando se usan los cuatro servicios basados en VLAN de MEF.

Interconexión

Se refiere al intercambio estandarizado de tráfico Carrier Ethernet entre proveedores y para la provisión eventual en redes de acceso, usando los tipos de servicio E-Access recientemente aprobados, mientras que se preservan los atributos del servicio. En términos simples, esto permite que los proveedores diseñen múltiples redes interconectadas como una red única desde el punto de vista del usuario (lo cual habilita la concreción de un único Service Level Agreement, entre otras ventajas).

Gestión

CE 2.0 aporta nuevas funciones de gestión que estandarizan el manejo de fallas a niveles que no eran posibles en la versión anterior, para servicios provistos a través de múltiples redes.

A la fecha de creación de este documento, existen 21 proveedores de servicios certificados con 87 servicios definidos por el MEF CE 2.0 en 10 países. Además existen 31 proveedores de equipos de red con certificación CE 2.0 con más de 120 plataformas CE 2.0. La amplia disponibilidad y la creciente implantación de plataformas de redes CE 2.0 es un factor crucial del crecimiento en la certificación de servicios CE 2.0.

Durante el pasado año, el número de profesionales certificados por el MEF se ha triplicado hasta más de 1.700 en 224 organizaciones de 58 países. El 87 % de los profesionales certificados por el MEF trabaja para empresas miembros del MEF y el 62 % para proveedores de servicios.

3.2.1.3. Análisis de la situación del mercado internacional

Para conseguir el certificado CE 2.0, las empresas debe pasar una serie de pruebas rigurosas, 634 en total. En la actualidad, más de 197 empresas de servicios poseen la certificación CE 1.0 y las previsiones para la aprobación 2.0 son interesantes. La demanda de productos y servicios certificados es una fuerza impulsora, y para 2014 se espera un aumento significativo de certificaciones de proveedores de servicios, no solo de los mercados establecidos, sino también de las economías en desarrollo.

Existen 33 proveedores de servicios CE 2.0 con 91 servicios CE 2.0 en 14 países. Las certificaciones CE 2.0 para proveedores de servicios crecieron a una tasa dos veces mayor que las certificaciones CE 1.0 en un periodo de tiempo equivalente.

Current Statistics on Certified Services

Category	Certified Services	Service Providers	Countries
CE 1.0	197	73	27
CE 2.0	91	33	14

Figura 34: Estadísticas del mercado internacional

El listado completo de los certificados se puede encontrar en:

https://metroethernetforum.org/certification/services-certification-registry

A título de referencia ponemos algunos representativos.

Lo expuesto nos muestra las necesidad de las redes del mundo y especialmente en Argentina.

3.2.1.4. Contacto con personal relevante del mercado.

Con la finalidad de obtener información de referencia del Estado del Arte y de la situación actual desde el punto de vista de las implementaciones y percepciones de lo que se viene, se realizaron contactos con profesionales representativos del mercado con Know How sobre la tecnología ME.

La Metodología que se utilizó consistió en el armado de un Conjunto de Preguntas básicas comunes que le hicimos a todos los entrevistados, de manera de poder mesurar mejor las conclusiones sobre cada uno de los aspectos.

Por una cuestión de respeto profesional, y para hacer un tratamiento más personalizado, desestimamos la opción de una Encuesta.

A partir de los datos obtenidos se realizó un proceso de análisis y se volcó en gráficos, los cuales se detallan en el Anexo I.

A partir de esta información y luego de discusiones internas, el grupo pudo llegar a algunas conclusiones sobre distintos aspectos de la tecnología. Estas conclusiones se detallarán en cada punto del informe que corresponda. También servirá como apoyo para las siguientes etapas de la investigación.

Sin embargo como conclusión general, podemos decir que todos coincidieron en que MEF CE 2,0 es la especificación de servicios que permitirá elevar notablemente el estándar de calidad de las redes existentes. Esta mejora se percibirá en forma clara y directa sobre los servicios prestados.

A los efectos de facilitar su comprensión los modelos de capas se han incluido en el detalle de cada tecnología.

3.2.1.5. Equipamientos que satisfacen las funcionalidades de CE 2.0 (certificados)

CE 2.0 es una acreditación difícil de alcanzar. Los primeros veinte primeros proveedores de tecnologías certificados son: Accedian, Altera, BTI Systems, Ciena, Cisco, Cyan, FibroLAN, Huawei, Infinera, Juniper Networks, MRV, Omnitron, Overture, PT Inovacao, Pulsecom, RAD Data Communications, Telco Systems, Tellabs, Transition Networks y Transmode. (Datos al 30/12/2013).

3.2.2. Estudio de un caso de implementación real en Argentina

3.2.2.1. Descripción del Escenario

Se ha estudiado como caso real una red Metro Ethernet en Argentina, la infraestructura a detallar soporta servicios residenciales y corporativos, la empresa multinacional que estudiamos tienen además servicios de voz móviles, por lo que la red además de los servicios propios también brinda soporte de Backhaul de los servicios móviles, utilizando el siguiente esquema básico de su red Metro Ethernet.

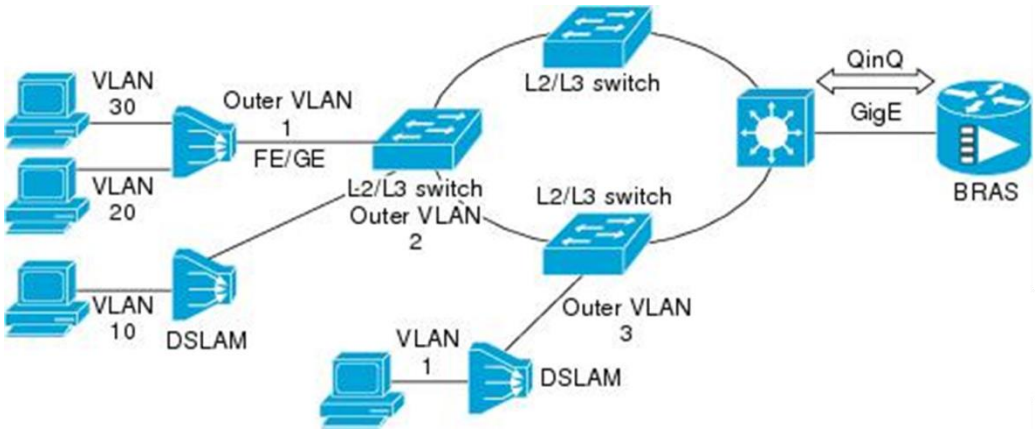


Figura 35: Esquema básico de red Metro Ethernet bajo estudio

La red de agregación Metro Ethernet que se observa en la gráfica anterior, representa la planificación de una red multi-servicio para agregar las diversas formas de acceso a través de DSLAM, OLT GPON y Switches Metro Ethernet de cliente (SWT) donde se transporta diversos servicios residenciales y corporativos sobre una misma infra-estructura de acceso.

La implementación de los criterios para dimensionamiento de red fue basada en los datos comerciales de crecimiento de los servicios con una previsión de 5 años.

De una forma general los puntos más relevantes en el modelo de red son:

- Separación de los dominios IGP y BGP entre la red Metro Ethernet y Core IP
- Separación física y lógica entre los servicios Internet y los servicios Corporativos
- Infra-estructura específica y dedicada para servicios críticos (voz y señalización)
- Transporte transparente a través de la red metro Ethernet del tráfico de Nodo B UMTS (Backhaul IP).

• Simplificación de la estructura lógica de la red Metro Ethernet con uso de VLL, eliminando funcionalidades de Full Routing BGP en los Switches de distribución y concentración.

La arquitectura de red permite también a través de su capilaridad soportar los servicios VPN ofertados en las redes legadas de datos (TDM / Frame Relay).

De esta forma, el servicio VPN IP basado en la red multi-servicio es un punto clave y traerá una importante reducción de CAPEX y OPEX en función de estas migraciones de redes legadas, proporcionando:

• Substitución de la VPN L2 – Frame-Relay / ATM / TDM;

• Substitución de la VPN L3 – X25

• Implementación de accesos Ethernet para interconexión con la red IP/MPLS, substituyendo los accesos legados en Frame-Relay, PPP y ATM

En síntesis, la arquitectura de red está compuesta por:

• Red Metro Ethernet transparente para la agregación de los servicios residenciales (xDSL, IPTV y VoIP), agregación de los servicios corporativos (IP dedicado, L2L y VPN IP) y transporte transparente del tráfico proveniente de las radio bases de las redes móviles a través de pseudowire

• Agregación BRAS independiente para el servicio Internet residencial

• Elementos PE Corporativos independientes para separación de los servicios corporativos de VPN IP, L2L Internet Corporativo y conexión con redes legadas Frame Relay y Determinística

• Backbone IP único para los servicios Internet y datos corporativos, entretanto, con dominio IGP totalmente separado de las otras redes a través de la segmentación de IGP del backbone en áreas de servicio (BRAS, PE y RC) y Core (RN y RI).

• Red de Voz para soportar tráfico de voz fija, voz móvil y señalización, con infra-estructura y plano de control dedicados, garantía de QoS y mecanismos de FRR (Fast re-routing) para la garantía de los tiempos de convergencia exigidos para el servicio de voz

• Estructura Headend del servicio IPTV, la cual está conectada solamente a los SWC de la red metro y a través de sistemas de transmisión SDH NG/DWDM para minimizar aspectos como el delay.

• Agregación Backhaul IP para soportar el tráfico proveniente de las BTS, así como de los servicios prestados por las operadoras móviles.

La infra-estructura de red de agregación Metro Ethernet se mantiene común para los servicios residenciales, corporativos y móviles donde cada cluster de la red Metro Ethernet está con su plano de control separado de los demás clusters Metro, del Core de la red IP y del plano de control de la Red de Voz.

La topología de Red Metro está basada en una estructura de anillos de distribución GE/10GE aplicados directamente sobre fibras ópticas con sistemas de transmisión DWDM, que interconectan los Switches de Distribución (SWD) a los Switches de Concentración (SWC). Los SWC pueden agrupar varios anillos de distribución, concentrando el tráfico en

clusters de la red Metro Ethernet perteneciente a un mismo dominio de ruteo IGP. A partir del elemento de concentración son conectados los agregadores BRAS (Broadband Remote Access Server), los PE de las VPNs Corporativas e Internet Corporativo, la Red de Voz, la Plataforma IPTV y el Core de la Red IP. El tráfico de las Radio Bases es encaminado hacia la infra-estructura de red de las operadoras móviles (BSC) y posteriormente la red de voz.

3.2.2.1.1. Introducción a las pruebas

En el apartado a continuación, comentaremos los resultados de pruebas que realizó una empresa multinacional de primera línea, de las cuales el grupo de investigación pudo tener acceso y participar en las conclusiones de las mismas.

Se realizó un set de pruebas entre proveedores (Tellabs, Alcatel-Lucent y Huawei) con equipos de las diferentes empresas ubicados en las tres ubicaciones de la red de Backhaul objetivo a estudiar.

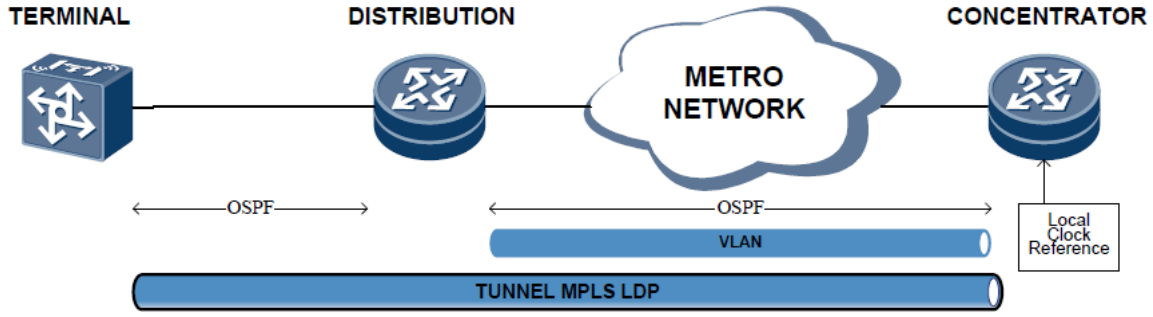


Figura 36: Topología de red objetivo a probar

3.2.2.1.2. INFORME DE PRUEBAS IOT (Inter Operability Test) Terminal Tellabs – Concentración y Distribución Huawei

El primer escenario de prueba consta de Equipos Huawei en la Concentración y Distribución de la red, NE40E-X8 y NE40E-X3, respectivamente. En tanto los terminales fueron empleados tres equipos de Tellabs, estos son: 8605, 8609 y 8611.

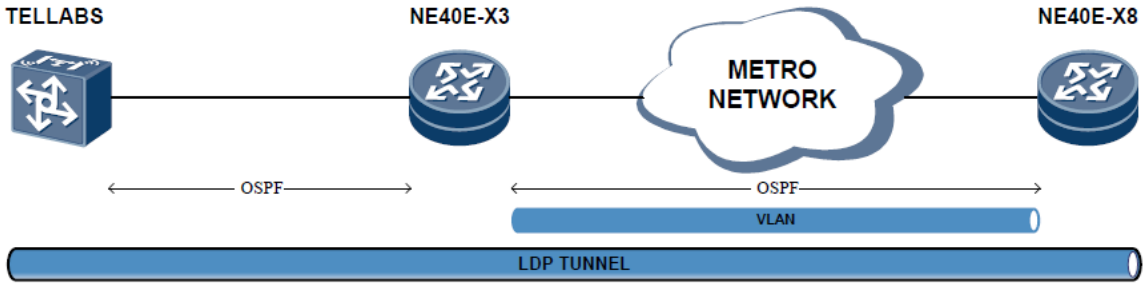


Figura 37: Primer escenario de prueba

NE40E-X3: configuración de MPLS, LDP y OSPF

#

```
mpls lsr-id 3.3.3.3
mpls
#
mpls l2vpn
#
mpls ldp
#
interface GigabitEthernet2/1/3
negotiation auto
undo shutdown
#
interface GigabitEthernet2/1/3.148
vlan-type dot1q 148
description link to NE-X8 (GE 8/0/4) for Tellabs_IOT
ip address 172.18.2.1 255.255.255.252
ospf network-type p2p
mpls
mpls ldp
#
interface LoopBack100
description for mpls lsr-id
ip address 3.3.3.3 255.255.255.255
#
ospf 1
area 0.0.0.0
network 172.18.2.0 0.0.0.3
network 3.3.3.3 0.0.0.0
network 172.18.1.0 0.0.0.3
network 172.18.1.4 0.0.0.3
network 172.18.1.112 0.0.0.3
```

NE40E-X3: configuración de interfaces hacia Terminales Tellabs

```
#
interface GigabitEthernet2/1/2
negotiation auto
description to_Tellabs__8605
undo shutdown
ip address 172.18.1.1 255.255.255.252
ospf network-type p2p
mpls
mpls ldp
#
interface GigabitEthernet2/1/6
negotiation auto
description to_Tellabs__8611 [2/5/0]
undo shutdown
ip address 172.18.1.113 255.255.255.252
ospf network-type p2p
mpls
mpls ldp
#
interface GigabitEthernet2/1/7
negotiation auto
description to_Tellabs__8609 [0/1]
undo shutdown
ip address 172.18.1.5 255.255.255.252
ospf network-type p2p
mpls
```

```
mpls ldp
```

NE40E-X8: configuración de MPLS, LDP y OSPF

```
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer tellabs__8605
remote-ip 6.6.6.5
mpls ldp remote-peer tellabs__8609
remote-ip 6.6.6.9
#
mpls ldp remote-peer tellabs__8611
remote-ip 6.6.6.11
#
interface GigabitEthernet8/0/4
negotiation auto
undo shutdown
#
interface GigabitEthernet8/0/4.148
vlan-type dot1q 148
description link to X3 (GE 2/1/3) for Tellabs_IOT
ip address 172.18.2.2 255.255.255.252
ospf network-type p2p
mpls
mpls ldp
#
interface LoopBack0
description for mpls lsr-id
ip address 2.2.2.2 255.255.255.255
#
ospf 1
area 0.0.0.0
network 172.18.2.0 0.0.0.3
network 2.2.2.2 0.0.0.0
```

NE40E-X8: configuración de Ethernet Pseudowire

```
#
interface GigabitEthernet3/0/6
negotiation auto
undo shutdown
#
interface GigabitEthernet3/0/6.140
vlan-type dot1q 140
description for PW-Ethernet Tellabs__8609
mpls l2vc 6.6.6.9 40
#
interface GigabitEthernet3/0/7
negotiation auto
undo shutdown
#
interface GigabitEthernet3/0/7.140
vlan-type dot1q 140
```

```
description for PW-Ethernet Tellabs__8609
mpls l2vc 6.6.6.9 41
```

Luego de las configuraciones los resultados en los equipos se puede ver a continuación.

LSP en el NE-X3:

```
[NE-X3]display mpls lsp
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
3.3.3.3/32          3/NULL        -/-
2.2.2.2/32          NULL/3        -/GE2/1/3.148
2.2.2.2/32          4180/3        -/GE2/1/3.148
6.6.6.5/32          NULL/1280     -/GE2/1/2
6.6.6.5/32          4103/1280     -/GE2/1/2
6.6.6.11/32         NULL/86400    -/GE2/1/6
6.6.6.11/32         4104/86400    -/GE2/1/6
6.6.6.9/32          NULL/1283     -/GE2/1/7
6.6.6.9/32          4105/1283     -/GE2/1/7
```

Figura 38: Resultado LSP en el NE-X3

LSP en el NE-X8:

```
[NE40Ex8]display mpls lsp
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
3.3.3.3/32          NULL/3        -/GE8/0/4.148
3.3.3.3/32          4171/3        -/GE8/0/4.148
6.6.6.5/32          NULL/4103     -/GE8/0/4.148
6.6.6.5/32          4172/4103     -/GE8/0/4.148
6.6.6.9/32          NULL/4105     -/GE8/0/4.148
6.6.6.9/32          4173/4105     -/GE8/0/4.148
6.6.6.11/32         NULL/4104     -/GE8/0/4.148
6.6.6.11/32         4174/4104     -/GE8/0/4.148
2.2.2.2/32          3/NULL        -/-
```

Figura 39: Resultado LSP en el NE-X8

LDP Peers en el NE-X3:

```
[NE-X3]display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0             2.2.2.2            GigabitEthernet2/1/3.148
 6.6.6.5:0             6.6.6.5            GigabitEthernet2/1/2
 6.6.6.9:0             6.6.6.9            GigabitEthernet2/1/7
 6.6.6.11:0            6.6.6.11           GigabitEthernet2/1/6
 ------------------------------------------------------------------------------
 TOTAL: 4 Peer(s) Found.
```

Figura 40: Resultado de LDP Peers en el NE-X3

LDP Peers en el NE-X8:

```
[NE40Ex8]display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress    DiscoverySource
 ------------------------------------------------------------------------------
 3.3.3.3:0             3.3.3.3             GigabitEthernet8/0/4.148
 6.6.6.5:0             6.6.6.5             Remote Peer : tellabs__8605
 6.6.6.9:0             6.6.6.9             Remote Peer : tellabs__8609
 6.6.6.11:0            6.6.6.11            Remote Peer : tellabs__8611
 ------------------------------------------------------------------------------
 TOTAL: 4 Peer(s) Found.
```

Figura 41: Resultado de LDP Peers en el NE-X8

Verificación del estado de los Pseudowire Ethernet:

Para las pruebas de los servicios Ethernet se configuraron dos Pseudowire Ethernet entre el equipo Terminal y el Concentrador cursando la misma VLAN. Por la disposición de los equipos de red en el laboratorio, el instrumento de medición fue conectado al concentrador y un loop físico se usó del lado del terminal con el fin de cerrar el circuito.

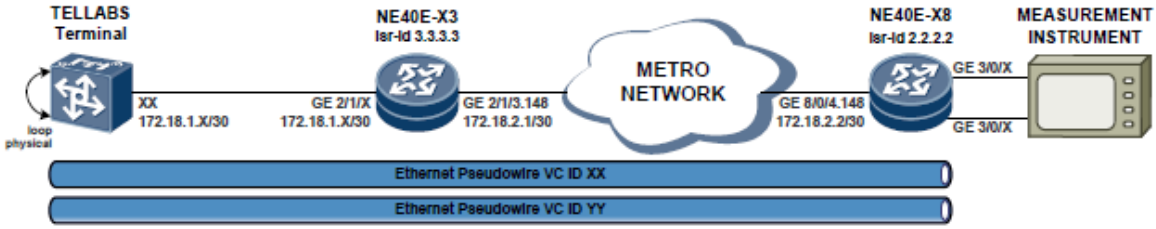


Figura 42: Prueba de verificación del estado de los Pseudowire Ethernet

Ethernet Pseudowire. Huawei X8 a Tellabs-8605:

```
[NE40Ex8]display mpls l2vc 150
Total LDP VC : 1 1 up 0 down
*client interface : GigabitEthernet3/0/6.150 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 150
VC type : VLAN
destination : 6.6.6.5
local VC label : 4107 remote VC label : 1285
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
```

```
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 0 days, 4 hours, 5 minutes, 2 seconds
up time : 0 days, 0 hours, 37 minutes, 45 seconds
last change time : 0 days, 0 hours, 37 minutes, 45 seconds
VC last up time : 2012/08/29 02:14:05
VC total up time : 0 days, 3 hours, 52 minutes, 50 seconds
CKey : 17
NKey : 14
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
Domain Name : --
[NE40Ex8]display mpls l2vc 151
Total LDP VC : 1 1 up 0 down
*client interface : GigabitEthernet3/0/8.150 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 151
VC type : VLAN
destination : 6.6.6.5
local VC label : 4111 remote VC label : 1282
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 0 days, 1 hours, 3 minutes, 25 seconds
up time : 0 days, 0 hours, 59 minutes, 29 seconds
last change time : 0 days, 0 hours, 59 minutes, 29 seconds
VC last up time : 2012/08/29 01:52:26
VC total up time : 0 days, 1 hours, 0 minutes, 23 seconds
CKey : 21
NKey : 14
```

```
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
Domain Name : --
```

Ethernet Pseudowire. Huawei X8 a Tellabs-8609

```
<NE40Ex8>display mpls l2vc 40
Total LDP VC : 1 1 up 0 down
*client interface : GigabitEthernet3/0/6.140 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 40
VC type : VLAN
destination : 6.6.6.9
local VC label : 4109 remote VC label : 1290
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 0 days, 22 hours, 59 minutes, 55 seconds
up time : 0 days, 0 hours, 35 minutes, 14 seconds
last change time : 0 days, 0 hours, 35 minutes, 14 seconds
VC last up time : 2012/09/12 12:54:09
VC total up time : 0 days, 1 hours, 56 minutes, 56 seconds
CKey : 26
NKey : 15
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
Domain Name : --
<NE40Ex8>display mpls l2vc 41
Total LDP VC : 1 1 up 0 down
*client interface : GigabitEthernet3/0/7.140 is up
Administrator PW : no
```

```
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 41
VC type : VLAN
destination : 6.6.6.9
local VC label : 4110 remote VC label : 1291
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 0 days, 22 hours, 59 minutes, 57 seconds
up time : 0 days, 0 hours, 35 minutes, 16 seconds
last change time : 0 days, 0 hours, 35 minutes, 16 seconds
VC last up time : 2012/09/12 12:54:09
VC total up time : 0 days, 1 hours, 52 minutes, 15 seconds
CKey : 27
NKey : 15
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
Domain Name : --
```

Ethernet Pseudowire. Huawei X8 a Tellabs-8611

```
<NE40Ex8>display mpls l2vc 45
Total LDP VC : 1 1 up 0 down
*client interface : GigabitEthernet3/0/14.130 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 45
VC type : VLAN
destination : 6.6.6.11
local VC label : 4113 remote VC label : 86415
control word : disable
forwarding entry : exist
```

```
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 0 days, 23 hours, 28 minutes, 8 seconds
up time : 0 days, 0 hours, 5 minutes, 12 seconds
last change time : 0 days, 0 hours, 5 minutes, 12 seconds
VC last up time : 2012/09/12 13:52:24
VC total up time : 0 days, 11 hours, 58 minutes, 3 seconds
CKey : 30
NKey : 17
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
Domain Name : --
<NE40Ex8>display mpls l2vc 46
Total LDP VC : 1 1 up 0 down
*client interface : GigabitEthernet3/0/15.130 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 46
VC type : VLAN
destination : 6.6.6.11
local VC label : 4114 remote VC label : 86417
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
```

```
load balance type : flow
Access-port : false
create time : 0 days, 23 hours, 28 minutes, 14 seconds
up time : 0 days, 0 hours, 5 minutes, 27 seconds
last change time : 0 days, 0 hours, 5 minutes, 27 seconds
VC last up time : 2012/09/12 13:52:15
VC total up time : 0 days, 11 hours, 58 minutes, 16 seconds
CKey : 31
NKey : 17
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
Domain Name : --
```

3.2.2.1.3. INFORME DE PRUEBAS IOT (Inter Operability Test) Terminal Huawei – Concentración Tellabs

En este escenario, se planteó utilizar como equipo concentrador un Tellabs 8630 y un equipo Terminal Huawei ATN910. El equipo Tellabs tiene la limitación de no poder proveer una fuente de reloj, por lo cual como fuente de reloj se emplea el equipo de Huawei X8.

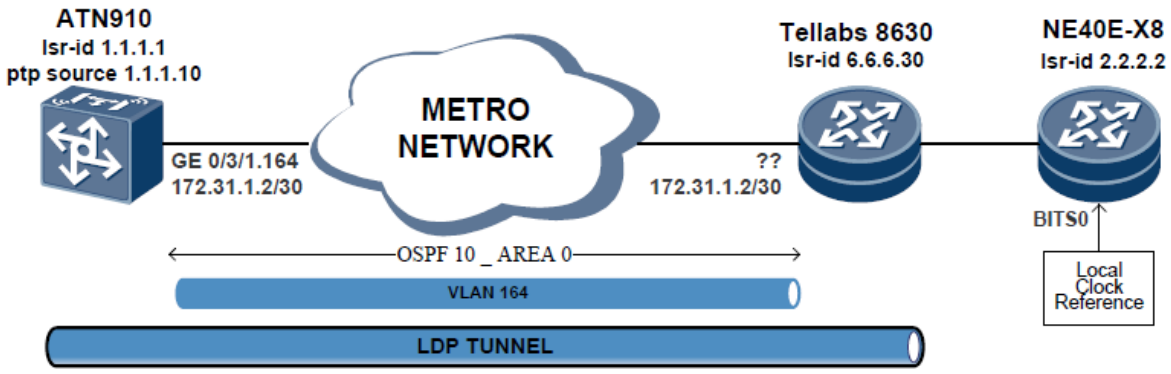


Figura 43: Escenario de prueba con equipo Tellabs 8630 como concentrador

ATN910: configuración de MPLS, LDP & OSPF

```
#
mpls lsr-id 1.1.1.1
mpls
lsp-trigger ip-prefix IOT_tellabs
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer tellabs_8630
remote-ip 6.6.6.30
#
interface Ethernet0/4/7
undo shutdown
description to_Tellabs__8630
```

```
ip address 172.31.1.2 255.255.255.252
ospf network-type p2p
mpls
mpls ldp
#
interface LoopBack0
description for mpls lsr-id
ip address 1.1.1.1 255.255.255.255
#
ospf 10
import-route direct
area 0.0.0.0
network 172.31.1.0 0.0.0.3
#
ip ip-prefix IOT_tellabs index 10 permit 1.1.1.1 32
ip ip-prefix IOT_tellabs index 20 permit 6.6.6.30 32
```

ATN910: configuración de Ethernet Pseudowire

```
#
interface Ethernet0/4/2
undo shutdown
#
interface Ethernet0/4/2.101
vlan-type dot1q 101
description for PW-Ethernet Tellabs__8630
mpls l2vc 6.6.6.30 91001
#
interface Ethernet0/4/3
undo shutdown
#
interface Ethernet0/4/3.101
vlan-type dot1q 101
description for PW-Ethernet Tellabs__8630
mpls l2vc 6.6.6.30 91002
```

Luego de las configuraciones los resultados en los equipos se puede ver a continuación.

Estado de LSP:

```
<ATN910>display mpls lsp
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
6.6.6.30/32         NULL/86400    -/Eth0/4/7
6.6.6.30/32         139/86400     -/Eth0/4/7
1.1.1.10/32         145/NULL      -/-
1.1.1.1/32          146/NULL      -/-
```

Figura 44: Estado de LSP

Estado de LDP Peers:

```
<ATN910>display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                 TransportAddress    DiscoverySource
 ------------------------------------------------------------------------------
 6.6.6.30:0             6.6.6.30            Ethernet0/4/7
 ------------------------------------------------------------------------------
 TOTAL: 1 Peer(s) Found.
```

Figura 45: Estado de LDP Peers

Verificación del estado de los Pseudowire Ethernet:

Ethernet Pseudowire. Huawei ATN910 a Tellabs-8630

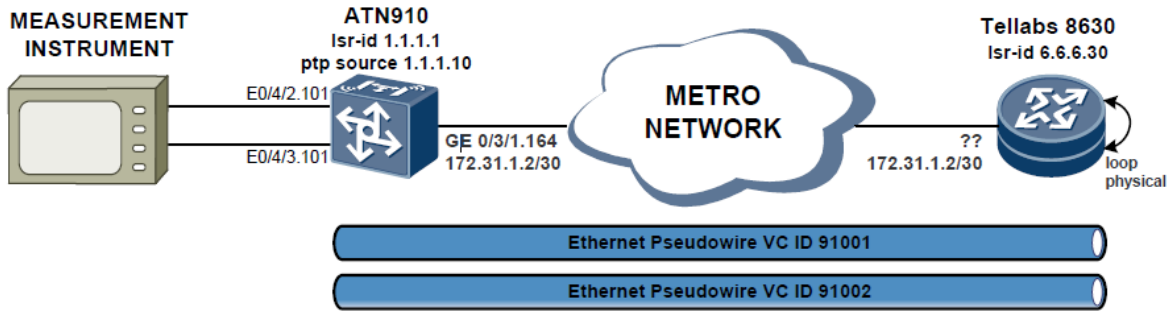


Figura 46: Verificación del estado de los Pseudowire Ethernet

```
[ATN910]display mpls l2vc 91001
Total LDP VC : 1 1 up 0 down
*client interface : Ethernet0/4/2.101 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 91001
VC type : VLAN
destination : 6.6.6.30
local VC label : 151 remote VC label : 86415
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
```

```
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 0 days, 0 hours, 20 minutes, 59 seconds
up time : 0 days, 0 hours, 20 minutes, 59 seconds
last change time : 0 days, 0 hours, 20 minutes, 59 seconds
VC last up time : 2012/09/20 13:56:44
VC total up time : 0 days, 0 hours, 20 minutes, 59 seconds
CKey : 4
NKey : 19
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
Domain Name : --
[ATN910]display mpls l2vc 91002
Total LDP VC : 1 1 up 0 down
*client interface : Ethernet0/4/3.101 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 91002
VC type : VLAN
destination : 6.6.6.30
local VC label : 152 remote VC label : 86416
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 0 days, 0 hours, 20 minutes, 42 seconds
up time : 0 days, 0 hours, 20 minutes, 42 seconds
last change time : 0 days, 0 hours, 20 minutes, 42 seconds
VC last up time : 2012/09/20 13:57:04
VC total up time : 0 days, 0 hours, 20 minutes, 42 seconds
CKey : 3
NKey : 19
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
```

```
Color : --
DomainId : --
Domain Name : --
```

3.2.2.1.4. INFORME DE PRUEBAS IOT (Inter Operability Test) Terminal Alcatel-Lucent – Concentración y Distribución Huawei

Las pruebas son realizadas con equipos Huawei NE40E-X8 y NE40E-X3 en la Concentración y Distribución, respectivamente, y como Terminal el equipo 7705 SAR-M de Alcatel-Lucent. La figura siguiente describe la topología lógica para esta prueba.

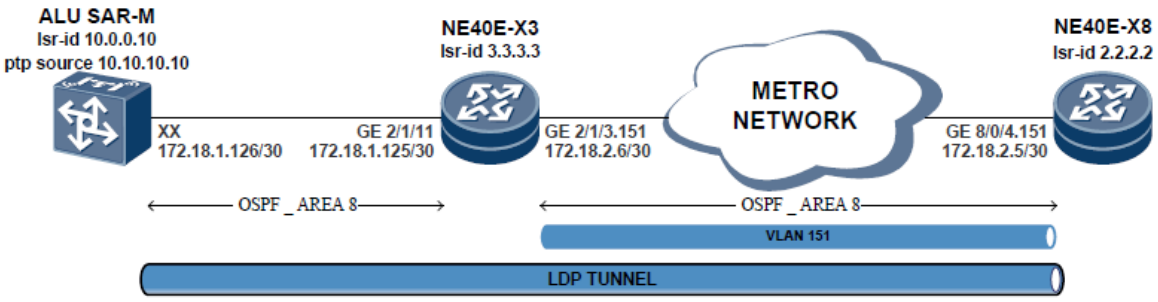


Figura 47: IOT con Terminal Alcatel-Lucent y Concentración y Distribución Huawei

NE40E-X3: configuración de MPLS, LDP & OSPF

```
#
mpls lsr-id 3.3.3.3
mpls
#
mpls l2vpn
#
mpls ldp
#
interface GigabitEthernet2/1/3
negotiation auto
undo shutdown
#
interface GigabitEthernet2/1/3.151
vlan-type dot1q 151
description link to NE-X8 (GE 8/0/4) for ALU_IOT
ip address 172.18.2.6 255.255.255.252
ospf network-type p2p
mpls
mpls ldp
#
interface LoopBack100
description for mpls lsr-id
ip address 3.3.3.3 255.255.255.255
ospf 3 router-id 3.3.3.3
import-route direct
area 0.0.0.8
network 172.18.1.124 0.0.0.3
network 172.18.2.4 0.0.0.3
```

NE40E-X3: configuración de interfaz a Terminal de Alcatel

```
interface GigabitEthernet2/1/11
negotiation auto
description to_ALU__SAR-M
undo shutdown
ip address 172.18.1.125 255.255.255.252
ospf network-type p2p
mpls
mpls ldp
```

NE40E-X8: configuración de MPLS, LDP & OSPF

```
#
mpls lsr-id 2.2.2.2
mpls
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer alu__sar-m
remote-ip 10.0.0.10
#
interface GigabitEthernet8/0/4
negotiation auto
undo shutdown
#
interface GigabitEthernet8/0/4.151
vlan-type dot1q 151
description link to X3 (GE 2/1/3) for ALU_IOT
ip address 172.18.2.5 255.255.255.252
ospf network-type p2p
mpls
mpls ldp
#
interface LoopBack0
description for mpls lsr-id
ip address 2.2.2.2 255.255.255.255
#
ospf 3
import-route direct
area 0.0.0.8
network 172.18.2.4 0.0.0.3
```

NE40E-X8: configuración de Ethernet Pseudowire

```
#
interface GigabitEthernet3/0/10
negotiation auto
description for PW-Ethernet ALU__SAR-M
undo shutdown
mpls l2vc 10.0.0.10 21
#
interface GigabitEthernet3/0/11
negotiation auto
description for PW-Ethernet ALU__SAR-M
undo shutdown
mpls l2vc 10.0.0.10 20
```

Estado de LSP:

```
<NE40Ex8> display mpls lsp
--------------------------------------------------------------------------------
                LSP Information: LDP LSP
--------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
3.3.3.3/32          NULL/3        -/GE8/0/4.148
3.3.3.3/32          4181/3        -/GE8/0/4.148
10.0.0.10/32        NULL/4182     -/GE8/0/4.151
10.0.0.10/32        4180/4182     -/GE8/0/4.151
2.2.2.2/32          3/NULL        -/-
```

Figura 48: Estado de LSP

```
<NE-X3>display mpls lsp
--------------------------------------------------------------------------------
                LSP Information: STATIC CRLSP
--------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
5.5.5.5/32          NULL/17       -/GE2/1/1
--------------------------------------------------------------------------------
                LSP Information: LDP LSP
--------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
3.3.3.3/32          3/NULL        -/-
2.2.2.2/32          NULL/3        -/GE2/1/3.148
2.2.2.2/32          4187/3        -/GE2/1/3.148
6.6.6.11/32         NULL/86400    -/GE2/1/6
6.6.6.11/32         4185/86400    -/GE2/1/6
10.0.0.10/32        NULL/131071   -/GE2/1/11
10.0.0.10/32        4182/131071   -/GE2/1/11
```

Figura 49: Estado de LSP

Estado de LDP Peers:

```
<NE40Ex8>display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 3.3.3.3:0             3.3.3.3            GigabitEthernet8/0/4.151
                                          GigabitEthernet8/0/4.148
 10.0.0.10:0           10.0.0.10          Remote Peer : alu__sar-8
 6.6.6.5:0             6.6.6.5            Remote Peer : tellabs__8605
 6.6.6.11:0            6.6.6.11           Remote Peer : tellabs__8611
 ------------------------------------------------------------------------------
 TOTAL: 4 Peer(s) Found.
```

Figura 50: Estado de LDP Peers

```
<NE-X3>display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID                TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0             2.2.2.2            GigabitEthernet2/1/3.151
                                          GigabitEthernet2/1/3.148
 10.0.0.10:0           10.0.0.10          GigabitEthernet2/1/11
 6.6.6.5:0             6.6.6.5            GigabitEthernet2/1/2
 6.6.6.11:0            6.6.6.11           GigabitEthernet2/1/6
 ------------------------------------------------------------------------------
 TOTAL: 4 Peer(s) Found.
```

Figura 51: Estado de LDP Peers

Verificación del estado de los Pseudowire Ethernet:

Ethernet Pseudowire. Huawei X8 to Alcatel SAR-M

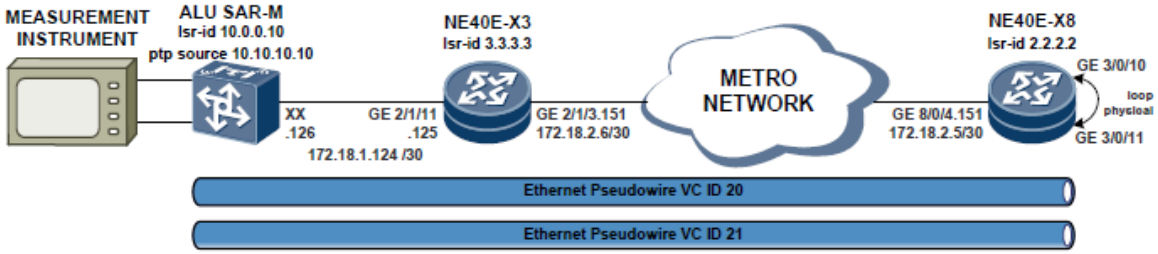


Figura 52: Ethernet Pseudowire. Huawei X8 to Alcatel SAR-M

```
[NE40Ex8]display mpls l2vc 20
Total LDP VC : 1 1 up 0 down
*client interface : GigabitEthernet3/0/11 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 20
VC type : Ethernet
destination : 10.0.0.10
local VC label : 4104 remote VC label : 131061
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 8 days, 2 hours, 2 minutes, 55 seconds
up time : 0 days, 0 hours, 2 minutes, 4 seconds
last change time : 0 days, 0 hours, 2 minutes, 4 seconds
VC last up time : 2012/09/19 16:30:19
VC total up time : 0 days, 2 hours, 1 minutes, 18 seconds
CKey : 20
NKey : 11
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
```

```
Domain Name : --
[NE40Ex8]display mpls l2vc 21
Total LDP VC : 1 1 up 0 down
*client interface : GigabitEthernet3/0/10 is up
Administrator PW : no
session state : up
AC status : up
VC state : up
Label state : 0
Token state : 0
VC ID : 21
VC type : Ethernet
destination : 10.0.0.10
local VC label : 4103 remote VC label : 131060
control word : disable
forwarding entry : exist
local group ID : 0
manual fault : not set
active state : active
OAM Protocol : --
OAM Status : --
OAM Fault Type : --
PW APS ID : 0
PW APS Status : --
TTL Value : 1
link state : up
local VC MTU : 1500 remote VC MTU : 1500
tunnel policy name : --
PW template name : --
primary or secondary : primary
load balance type : flow
Access-port : false
create time : 8 days, 2 hours, 2 minutes, 47 seconds
up time : 0 days, 0 hours, 1 minutes, 56 seconds
last change time : 0 days, 0 hours, 1 minutes, 56 seconds
VC last up time : 2012/09/19 16:30:19
VC total up time : 0 days, 2 hours, 2 minutes, 31 seconds
CKey : 19
NKey : 11
AdminPw interface : --
AdminPw link state : --
Diffserv Mode : uniform
Service Class : --
Color : --
DomainId : --
Domain Name : --
```

Prueba de gestión del equipo terminal de Huawei:

La prueba se realizó en el escenario con el equipo ATN910 como Terminal y el Tellabs 8630 como concentrador, la misma consiste en transmitir el tráfico de gestión del ATN por una interfaz de servicio a través del equipo Tellabs hacia el servidor U2000 (Gestor general de equipos Huawei).

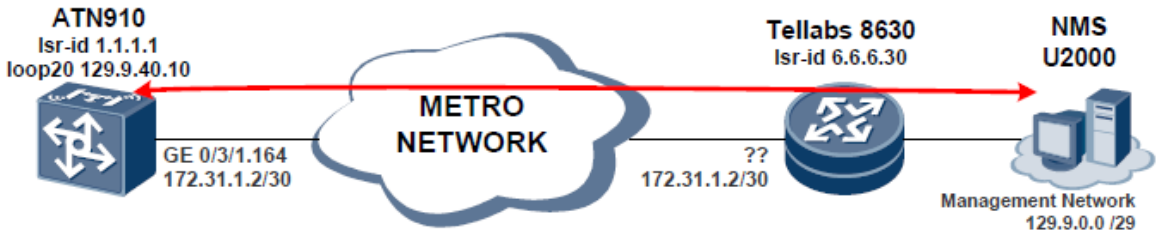


Figura 53: Prueba de gestión del equipo terminal de Huawei

A continuación se describen las configuraciones de snmp necesarias para hacer la transferencia de gestión y alarmas INBAND hacia el gestor. Los pasos consisten en crear una interfaz lógica, asociarla como la fuente de traps hacia el servidor y configurar la IP del servidor U2000 como el equipo que recibirá la información. Debe existir conectividad en capa 3 entre el ATN y el U2000. Para esta prueba se configuro una ruta default en el

ATN hacia la interfaz del equipo Tellabs, y en el U2000 una ruta estática apuntando hacia el mismo equipo.

```
#
interface LoopBack20
description for O&M test
ip address 129.9.40.10 255.255.255.255
#
ip route-static 0.0.0.0 255.255.255.255 GigabitEthernet0/3/1.164 172.31.1.1
#
snmp-agent
snmp-agent local-engineid 800007DB030819A626432C13
snmp-agent community read cipher %$%$o^St"5xr*$#m~X5d{YAFyne\%$%$
snmp-agent community write cipher %$%$GUZ{OG'4'"W:.zY@Qq>:yxof%$%$
snmp-agent sys-info version all
snmp-agent target-host trap address udp-domain 129.9.0.254 params securityname
public v2c private-netmanager
snmp-agent trap source LoopBack20
snmp-agent inform timeout 10
snmp-agent trap enable
```

Una vez que el ATN910 es gestionado por el U2000, éste recibirá alarmas ante cualquier eventualidad.

El resultado de las pruebas demostró que la interoperabilidad entre los operadores mencionados es posible.

3.2.3. Investigación de los potenciales servicios en Metro Ethernet

Una Red Metro Ethernet, es una arquitectura tecnológica destinada a suministrar servicios de conectividad de datos.

Estas redes denominadas "multi-servicio", soportan una amplia gama de servicios, aplicaciones, y cuentan con mecanismos donde se incluye soporte a tráfico "RTP" (tiempo real), para aplicaciones como Telefonía IP y Video IP, aun cuando este tipo de tráfico es especialmente sensible al retardo y al jitter (Fluctuación).

Las redes Metro Ethernet pueden utilizar líneas de cobre (MAN BUCLE), lo que garantiza la posibilidad de despliegue en cualquier punto del casco urbano, soportando el 100% de los servicios demandados.

Las redes Metro Ethernet suelen utilizar principalmente medios de transmisión guiados, como son el cobre (MAN BUCLE) y la fibra óptica, existiendo también soluciones de radio licenciada, los caudales proporcionados son de 10 Mbit/s, 20 Mbit/s, 34 Mbit/s, 100 Mbit/s, 1 Gbit/s y 10 Gbit/s.

Sin embargo, y de vital importancia para servicios que no están apalancados en cobre o fibra óptica, las redes Metro Ethernet, pueden brindar calidad de servicio y priorización de tráfico a servicios satelitales.

De esta forma, las dificultades de un acceso satelital, no sufren el agregado de dificultades de transito adicional en la red.

3.2.3.1. Estudio y descripción de servicios potenciales Metro-Ethernet de próxima generación en los próximos 3 años en Argentina

La potencialidad de nuevos servicios Metro Ethernet es ilimitada, dado que los servicios soportados actualmente son una enorme cantidad.

Sin embargo de un análisis detallado del cuadro posterior surge que las redes móviles presentan un campo de acción disponible y virtualmente inexplorado en lo referido a video móvil. Se debe mencionar la complejidad de dicho campo.

Application	Consumer	Business	Mobile
VoIP Data	☑	☑	☑
Interactive Video (Video Conferencing)	☑	☑	☐
VoIP and Video Signaling	☑	☑	☑
Web Browsing	☑	☑	☑
IPTV Data Plane	☑	☑	?
IPTV Control Plane	☑	☑	?
Streaming Media	☑	☑	☑
Interactive Gaming	☑		☑
Best Effort	☑	☑	☑
Circuit Emulation		☑	☑
Grid Computing		☑	
Telepresence		☑	
Remote Surgery (Video)		☑	
Remote Surgery (Control)		☑	
Telehealth (Hi-res image file transfer)		☑	
Email	☑	☑	☑
Broadcast Engineering (Pro Video over IP)		☑	
CCTV	☑	☑	☑
Financial/Trading		☑	
Database		☑	
Real Time Fax over IP	☑	☑	
Store and Forward Fax over IP	☑	☑	
SANs (Synchronous Replication)		☑	
SANs (Asynchronous Replication)		☑	
Wide Area File Services		☑	
Network Attached Storage	☑	☑	
Text Terminals (telnet, ssh)		☑	
Graphics Terminals (Thin Clients)		☑	
Point of Sale Transactions		☑	
E-Commerce (Secure transactions)	☑	☑	☑
Mobile Backhaul System Requirements			☑

Figura 54: Campo de acción disponible para las Redes Móviles

1) **CRM Negocios:**

El servicio de CRM permite organizar la información de un negocio, clientes y presupuestos generados de manera adecuada a los requerimientos oficiales y/o gubernamentales.

Organiza los datos de la actividad comercial para convertirla en información que permita gestionar un negocio.

Con CRM Negocios vas a poder analizar información como ¿Cuáles son los clientes que generan más ingresos?, ¿Cuantas cotizaciones envié este mes?, ¿Qué % de cotizaciones se cerraron este mes?

Además de enviar reportes detallados, de acuerdo a los formularios oficiales requeridos por organismos de control.

Facilita la interacción del cliente y la organización incorporando nuevos medios de conexión más eficiente como ser telefonía móvil.

2) **Comunicaciones Unificadas:**

Las Comunicaciones Unificadas son una solución de comunicación corporativa soportada sobre una red privada virtual IP y la red de nueva generación (NGN: Next Generation Network). Proporciona un servicio de centralita IP en red con las mismas características y funcionalidades que las plataformas usuales de telefonía, permitiendo una completa integración de tecnologías de móvil y otras TI.

Además, no requiere de otros servicios de voz ya que integra acceso a fijo y móvil.

Figura 55: Comunicaciones Unificadas
Figura 56: Comunicaciones Unificadas

Figura 57: Funcionalidades

3) BGAN (Broadband Global Area Network):

La modalidad de BGAN Terrestre-transportable, es un servicio muy útil para aquellos profesionales que necesitan un sistema de comunicación portátil, inmediato y económico en lugares remotos, con cobertura global y velocidad de conexión garantizada.

El servicio BGAN está basado en un producto mayorista, que permite ofrecer a sus usuarios finales las siguientes funcionalidades principales en un entorno tanto de movilidad como de portabilidad:

IP background: acceso a Internet y a VPNs de hasta 492Kbps.

Voz: de forma simultánea al IP background.

RDSI: un canal B de 64 o 56 Kbps.

IP streaming: canales asignados bajo demanda a velocidad garantizada de 32, 64, 128, 176, 256 o 384 Kbps bidireccionales.

SMS: con cualquier operador de móviles del mundo.

Buzón de voz, redirección de llamadas, restricción de llamadas, etc.

Canal de 3,1 KHz para fax grupo 3, módems, o equipos de encriptación.

El servicio BGAN le permite al cliente disponer de una conexión de datos de banda ancha en cualquier momento y en cualquier lugar de forma autónoma, sin necesidad de requerir una instalación compleja. Es sencillo de usar y el despliegue es muy rápido, dos requisitos imprescindibles en situaciones de emergencia. Además del acceso a Internet, se permite también acceso a redes privadas virtuales (VPNs) sobre la infraestructura de red terrestre (red MPLS).

Figura 58: Ejemplo de BGAN

4) Gestión Imágenes Médicas (G.I.M):

Por medio del servicio dedicado de Gestión de Imágenes Médicas (GIM), el cliente (Casa central y su red de Centros Médicos) contará con la aplicación instalada en servidores de uso exclusivo alojados en el Data Center, donde dispondrá de una base de datos para registrar su operatoria con alto nivel de seguridad y confiabilidad de la información.

Para la conexión de los sanatorios con el Data Center se utilizarán enlaces de banda ancha de 100 Mbps de fibra óptica, que soportarán el tráfico de los contenidos que serán almacenados y las consultas de las imágenes médicas digitales desde todos los centros médicos del Cliente.

El servicio GIM es operado y gestionado en forma centralizada desde el Data Center de la compañía proveedora, donde cuenta con seguridad tanto lógica como física y servicio de soporte para el reporte de cualquier inconveniente, el cual será atendido por el Centro de Atención Técnica del proveedor del servicio G.I.M, las 24 horas del día, los 365 días del año.

El Data Center del proveedor estará certificado por las normas ISO-IEC 27001 de seguridad de la información. Además, el servicio GIM cumple con todos los criterios de seguridad de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA su sigla en inglés), donde se recomienda la seguridad y confidencialidad de la información médica.

5) Telemergencia y Videosupervisión:

Una solución para negocios y comercios con CUIT que posean sucursales, lugares de acceso restringido o área que requieran un control las 24 hs. Se requiere de una línea de telefonía básica.

Una o varias Cámaras IP que te brindan la tranquilidad de ver lo que sucede en el lugar a vigilar independientemente de donde se encuentren ubicados los clientes.

Posibilidad de almacenar 24 horas de grabación.

Figura 59: Ejemplo de Telemergencia y Videosupervisión

6) Telecontrol Silo bolsa

Brinda información real y exacta de las variables climáticas, velocidad y dirección del viento, otorgando beneficios para la cosecha y fumigación.

7) GPS Vehículos

Localización y telemetría aplicada a flotas de camiones, taxis, ambulancias y vehículos en general

3.2.4. Mejores prácticas

Respecto de las mejores prácticas para la implementación de servicios SE ME ha llegado a las siguientes conclusiones.

A - Se debe dividir la red en tres áreas que se dividen en:

- Acceso
- Distribución
- Core

Las redes de acceso se podrán realizarse con tecnologías xDSL, APON o GPON.

Las redes de distribución se podrán implementar con:

- 802.1ad
- 802.1ah
- MPLS-TP

MPLS-TP es a nuestro criterio lo más adecuada, pues entendemos que es la tecnología más gestionable para los Carriers.

En el caso de las redes Core se deberán implementar con tecnología L2 MPLS VPN, y a través de los servicios VPWS y VPLS.

Respecto de la señalización, resulta muy conveniente la utilización del protocolo MP-BGP4, debido a tener la facilidad de auto-disconvery que el LDP no tiene.

Por otro lado la gran ventaja adicional de BGP es la escalabilidad.

3.3. Prospectiva a 3 años en Argentina

Las redes existentes en Argentina están dando servicios VPN en forma muy heterodoxas, que si bien prestan servicios no lo hacen de acuerdo a las mejores prácticas en la actualidad. Esto se debe a un grado de desactualización tecnológica existente.

Esta tecnología se está utilizando también en el despliegue de la red LTE (4G). La red LTE se encuentra en etapa de despliegue y en los próximos 3 años se espera una cobertura de gran parte del territorio nacional donde la tecnología descripta en este trabajo es la gran protagonista de este despliegue.

De lo expuesto se prevé para los próximos 3 años una renovación tecnológica orientada a las L2VPN.

Sin embargo la aparición de los servicios sufrirá la inercia lógica de la nuevas implementaciones y que están asociadas a la compra de equipos, puesta en operación, que las áreas de márquetin desarrollen más productos y que las áreas comerciales las hagan llegar a los clientes.

Se espera entonces que en el primer Carrier que lance los servicios, lo haga con el servicio VPWS en su configuración E-Tree para el mercado corporativo. Esto podrá ocurrir para clientes pioneros a fines de 2016 o principio del 2017.

Lamentablemente el servicio VPLS entendemos que demorará un poco más dado el cambio cultural que representa para los Carriers y para las áreas técnicas de los clientes corporativos. Es de esperar que los primeros clientes de este servicio aparezcan a fines del 2017 o principios del 2018.

Respecto de la Certificación ME CE2.0, no se avizora que la realice ningún Carrier en los próximos 3 años.

3.4. Conclusiones.

Se han cumplido plenamente las actividades comprometidas en la investigación y que se encuentran detalladas en el protocolo de presentación que se anexa al presente informe.

Conclusiones luego de realizado la investigación:

- Se ve claramente que las especificaciones MEF CE 2.0 son un norte para los proveedores de tecnología y proveedores de servicio.
- Existe un camino por recorrer para que esta tecnología alcance su madurez en la Argentina.

- La interoperabilidad entre la mayor parte de los proveedores está madura y se avizora como una fortaleza en la implementación de estas redes.
- En el mercado internacional las migraciones a CE 2.0 certificadas se está incrementando en forma acelerada.
- En Argentina las redes L2VPN están desplazando rápidamente a la tecnología legada.
- El mayor o menor avance de las tecnologías CE 2.0 en el mundo está asociado al mayor o menor desarrollo económico de los países.
- Las tecnologías líderes siguen manteniendo su liderazgo en ME CE 2.0.

3.5. Resultados obtenidos:

3.5.1. Resultados en cuanto a la producción de conocimiento:

Se ha investigado la temática con una profundidad que permitió la obtención de un alto nivel de conocimiento, especialmente teniendo en cuenta que la mayoría de ellas no se han implementado aún en redes de Carrier grade. Esto les está dando a los egresados (que reciben el conocimiento en los cursos de grado) grandes oportunidades laborales.

3.5.2. Resultados en cuanto a la formación de recursos humanos:

Frente a una tecnología en fase de desarrollo y con la dificultad que esto implica en la obtención de información, el grupo de investigación ha trabajado en forma eficiente y con gran avidez por la obtención de información.

Se ha trabajado en equipo y en forma proactiva, logrando obtener resultados destacados en el cumplimiento de nuestros objetivos.

En el último año de investigación se incorporo un nuevo integrante recientemente egresado con excelente resultado.

El grupo de estudiantes y profesores del Departamento de Ingeniería e Investigaciones Tecnológicas involucrados en el proyecto, resultarán directamente beneficiados con estos desarrollos en el aspecto académico y curricular.

3.5.3. Resultados en cuanto a la difusión de resultados:

Luego de la evaluación favorable de este informe, se lo difundirá entre especialistas de la temática de las principales empresas de comunicaciones de Argentina, entre los que se encuentran los profesionales que participaron en las encuestas, lo que les permitirá tener una visión global del tema.

El informe final una vez evaluado será ofrecido a la biblioteca de la UNLaM como material de consulta.

3.5.4. Posibilidades de transferencia de resultados:

Se dictó una clase sobre la temática de la investigación a los alumnos de la Materia “Redes de Computadoras” (Código 0377) de la carrera de Ingeniería en Electrónica de la UNLaM.

El desarrollo de Know How permitirá la provisión de servicio de asesoramiento a empresas por parte de la UNLaM.

El mercado podrá obtener información de potenciales servicios que podrán ofrecer los Carriers. Esto permitirá a las empresas que consumen servicios de comunicaciones determinar el grado de integración de sus redes y los servicios que cada empresa necesita.

El presente informe podrá servir como base para implementación de servicios en Carriers.

3.5.5. Resultados en cuanto a la transferencia de resultados a organismos externos a la U.N.L.a.M:

Se dictó una clase sobre la temática de la investigación a los alumnos de la Materia "Sistemas de Comunicaciones II a y b" de la carrera de Ingeniería en Electrónica de la UTN-FRBA.

3.6. Bibliografía.

Dada lo novedoso del tema que se trata nos hemos tenido que apoyar directamente en las normas.

[1] Metro Ethernet Forum: http://metroethernetforum.org/InformationCenter

[2] MPLS IETF Working Group: http://www.ietf.org/dyn/wg/charter/mpls-charter.html

[3] MPLS-TP IETF Working Group: http://www.ietf.org/dyn/wg/charter/mpls-charter.html

[4] PBB: IEEE 802.1ah – Provider Backbone Bridging

http://www.ieee802.org/1/pages/802.1ah.html

[5] PBB-TE: IEEE 802.1Qay – Provider Backbone Bridge Traffic

Engineering: http://www.ieee802.org/1/pages/802.1ay.html

[6] Ivan Pepelnjak et al, 2014, "MPLS and VPN Architectures", Volume II, Primera edición – Editorial: Cisco Press, San Jose California,USA. ISBN-13: 978-1587144325, ISBN-10: 1587144328

[7] Biga, Daniel et al, 2010, Proyecto de investigación "Estudio de Estado del Arte en Transporte de Servicios de Voz y Video sobre IP y detección de Nichos de Desarrollo". Códigos de Identificación: ING0016/2007 y 55/C081. Institución en la que se realizó la investigación: UNLaM. Director: Ing. Lupi, Codirector: Daniel Biga. Participante: Horacio Del Giorgio.

3.7. Producción Científica Tecnológica

a) Congresos Internacionales, Nacionales, Simposios, Jornadas, otros

Se presentó un paper que fue aceptado y presentado en el "Tercer Congreso Argentino de la Interacción-Persona Computador@, Telecomunicaciones, Informática e Información Científica", IPCTIIC 2014, Córdoba (Huerta Grande), Argentina: Diciembre 1 y 2 del 2014.

Se presentó un paper que fue aceptado y presentado en el “Cuarto Congreso Argentino de la Interacción-Persona Computador@, Telecomunicaciones, Informática e Información Científica”, IPCTIIC 2015, Córdoba (Huerta Grande), Argentina: Noviembre 16 y 17 del 2015.

b) Participación en libros

Se presentó un artículo para publicar en un libro, al día de la fecha de la presentación del informe final de la investigación aún no se ha publicado el mismo.

Anexos

Anexo I: Datos de las entrevistas y contactos con profesionales involucrados en la temática.

Anexo II: Detalle de siglas utilizadas.

Anexo III: Artículo presentado en el Congreso 2014.

Anexo IV: Artículo presentado en el Congreso 2015.

Anexo V: Protocolo de presentación del proyecto.

Anexo I: Datos de las entrevistas y contactos con profesionales involucrados en la temática.

A1.1 Actividad de las Empresas para con Metro Ethernet.

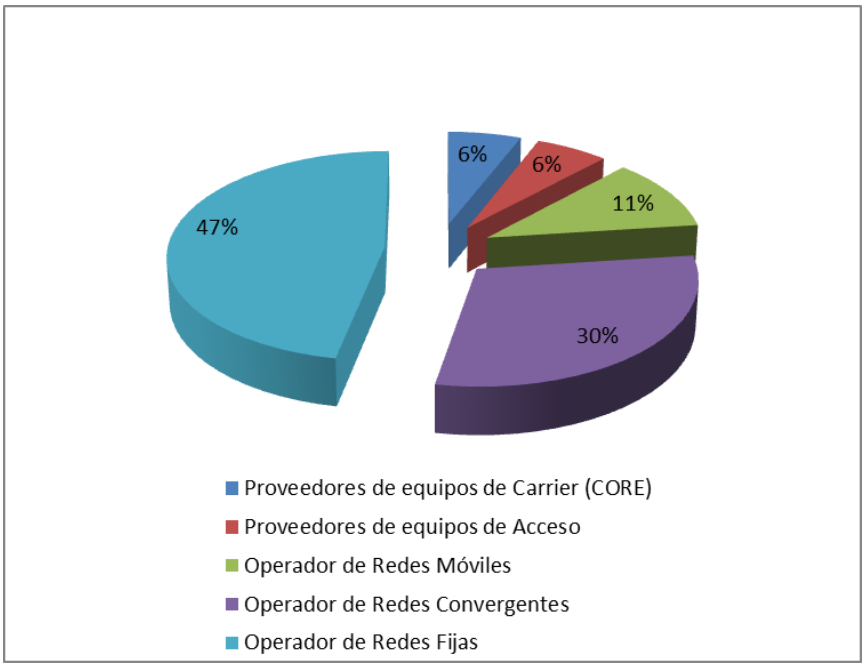


Figura 60: Utilización de Metro Ethernet en las empresas

El gráfico anterior nos indica que Metro Ethernet se encuentra en Operadores de Redes Fijas y Convergentes y en menor medida en Operadores de Redes Móviles, lo cual demuestra lo pertinente de nuestra investigación.

A1.2 Qué servicio transporta su red ME

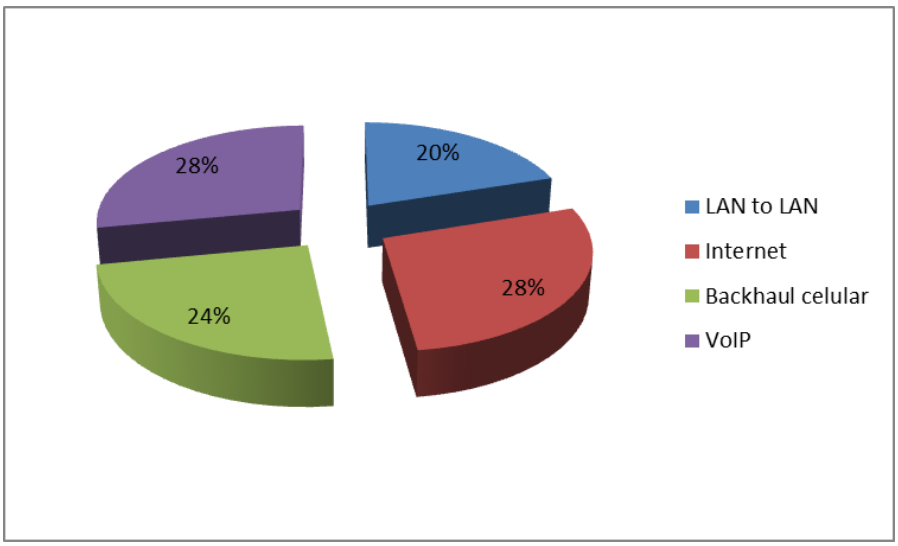


Figura 61: Servicios transportados por redes Metro Ethernet

Como se puede observar en el gráfico anterior, los mayores porcentajes se los llevan los servicios de “LAN To LAN” y servicios de “Internet”.

Un mercado que aprovecha los servicios ME está justamente en los Operadores Fijos y Móviles quienes poseen redes en constante crecimiento y mejora.

En especial, los servicios de “LAN To LAN”, orientados a interconectar segmentos de red de sus clientes.

A1.3 Barreras para la posibilidad de implementación actual de ME.

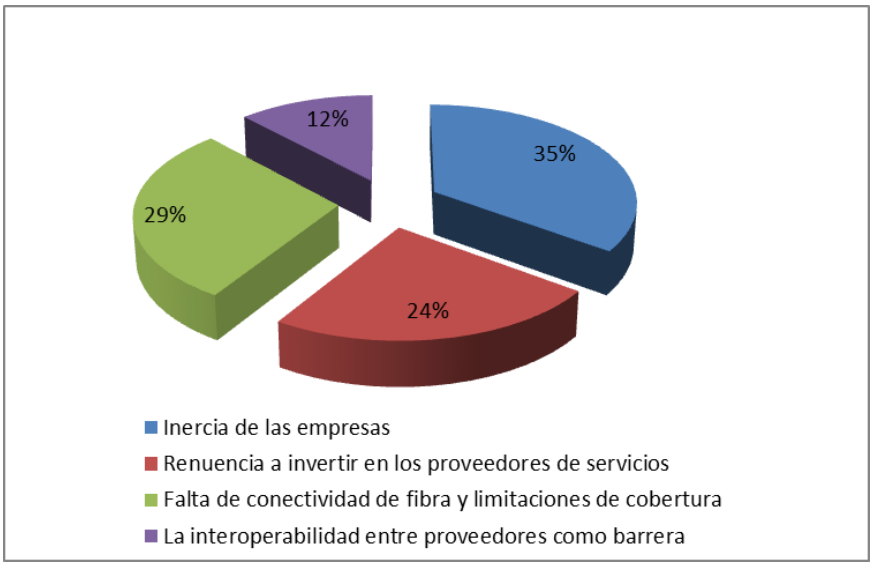


Figura 62: Barreras para implementar Metro Ethernet

Este gráfico nos muestra que existe algún tipo de dificultad para implementar ME.

Quizás, deba realizarse un análisis conjunto de las respuestas de esta pregunta con las respuestas a preguntas relacionadas a la necesidad de certificar ME que a continuación se detallan.

- ¿Cuál es la situación actual de su empresa respecto de la certificación de servicios MEF?

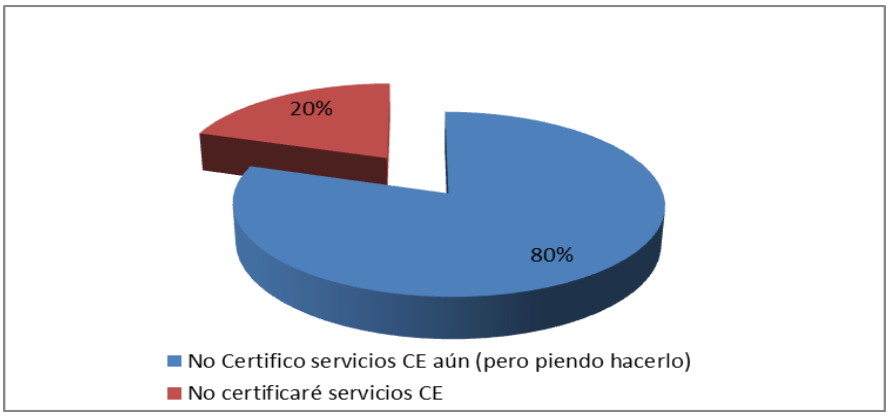


Figura 63: Certificación en las empresas

- ¿Cuál es la situación actual de su empresa respecto de la certificación de servicios MEF CE 2.0 en sus equipos?

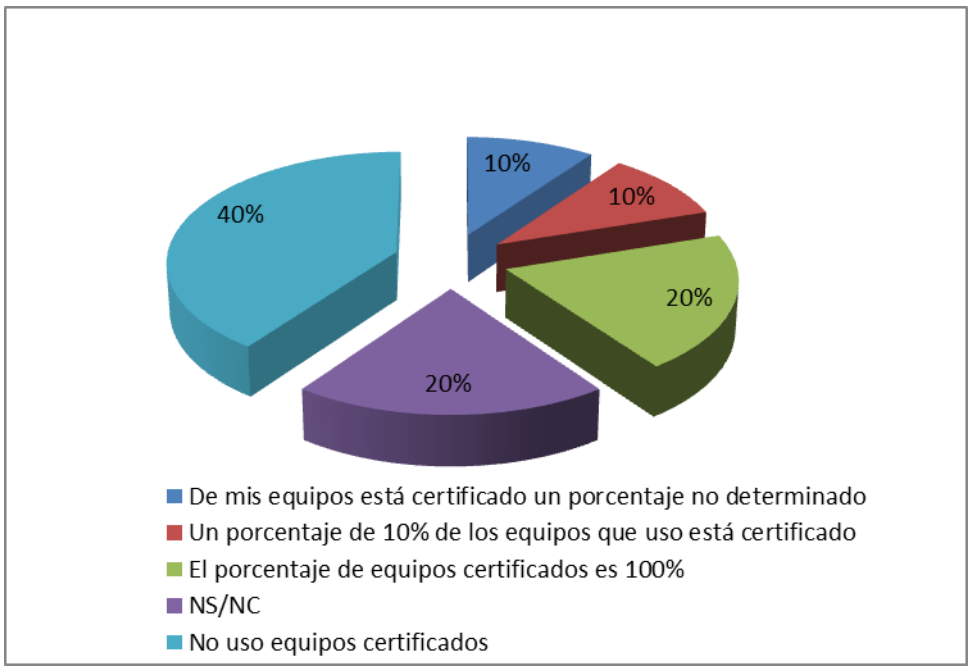


Figura 64: Certificaciones de equipos

- ¿Tiene previsto certificar MEF en la red o parte de ella?

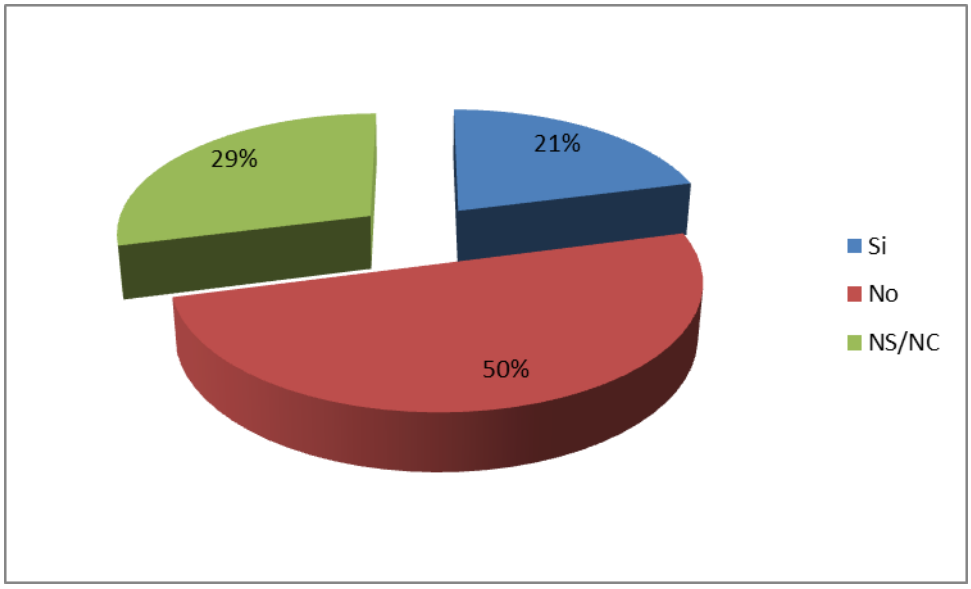


Figura 65: Intensión de las empresas de certificar

- ¿Cuál cree que será la situación a mediano plazo (3 a 5 años) de su empresa respecto de MEF CE2.0?

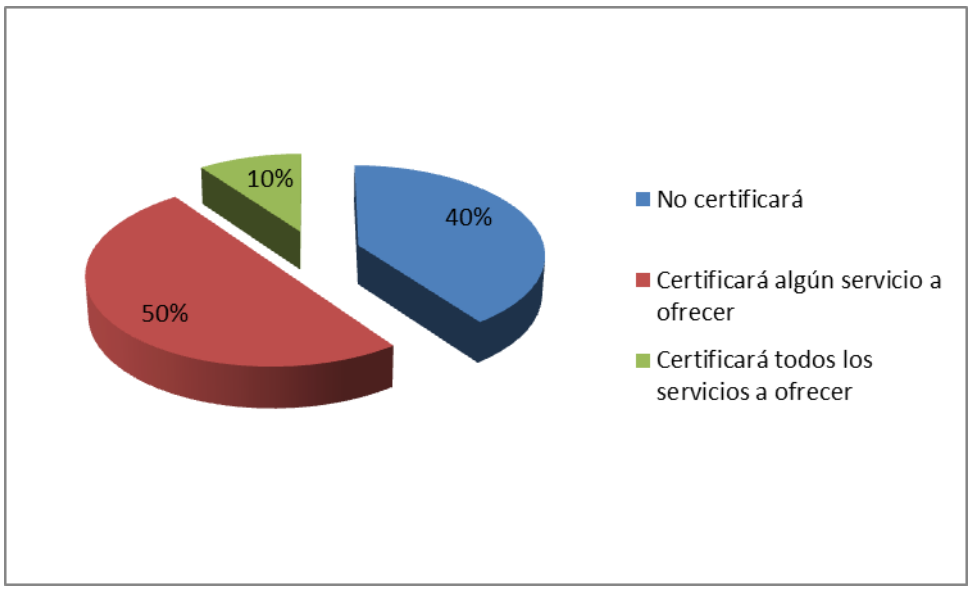


Figura 66: Percepción de los encuestados respecto a la certificación

El análisis conjunto de las respuestas a las 4 preguntas anteriores, permite interpretar que ME CE 2.0 no es visto como un diferencial de servicio, sino más bien como una solución a un problema, que no ha llegado todavía en varias redes.

Una primera línea de tendencia queda establecida cuando 60% de los encuestados afirman que a inercia de las empresas es una barrera al despliegue de servicios ME.

No se avanza en la adopción de ME CE 2.0 debido a que las empresas presentan baja adhesión a nuevas inversiones que no estén apalancadas en un negocio.

Un elevado porcentaje de encuestados cree que certificará en el futuro alguno de servicios que brinde y en parte de la red, cuando dicha certificación forme parte de un negocio.

Es elevado el porcentaje de empresas que no va a certificar en toda la red y ello es coherente con las respuestas sobre el uso de equipos certificados.

La segunda línea de tendencia puede describirse como de limitaciones técnicas, con un 40% de respuestas referidas a dificultades en la conectividad por fibra óptica.

En este caso, puede inferirse que, luego de un despliegue de fibra óptica, que requiere elevada inversión, la oferta de servicios ME certificados, actuará como diferencial, potenciando el despliegue de ME CE 2.0.

Las estimaciones a mediano plazo, de 3 a 5 años parecen reafirmar lo antes expuesto.

A1.4 Percepción sobre Proveedores de Tecnologías ME.

A los entrevistados se les solicitó que califiquen a los principales proveedores de tecnologías ME.

El siguiente gráfico muestra una percepción integral sobre estos proveedores. En el mismo se consideraron integralmente la calidad y cantidad de calificaciones que se realizaron.

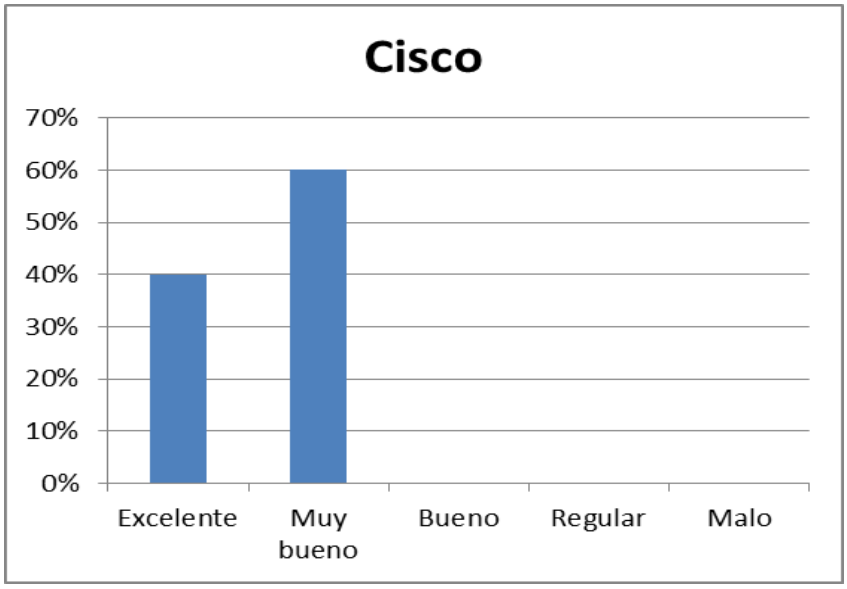


Figura 67: Percepción sobre equipos CISCO

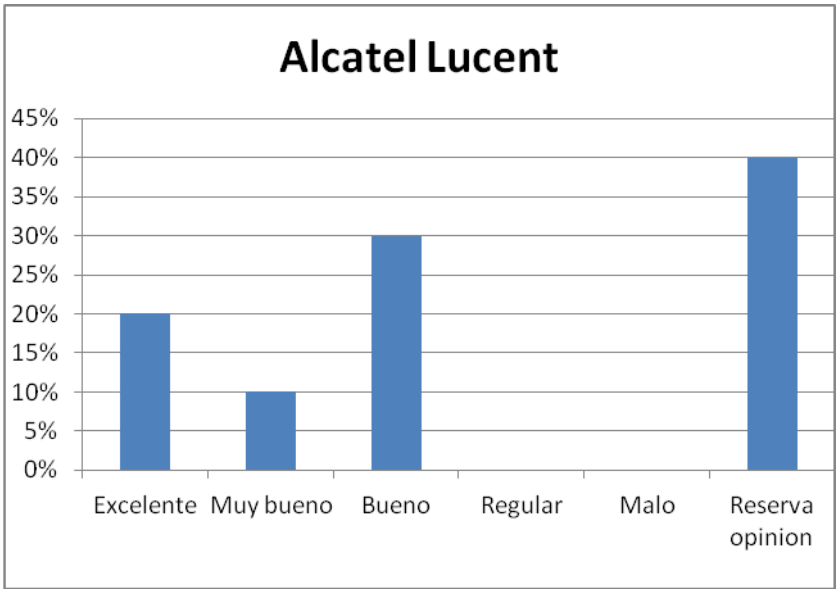


Figura 68: Percepción sobre equipos ALCATEL - LUCENT

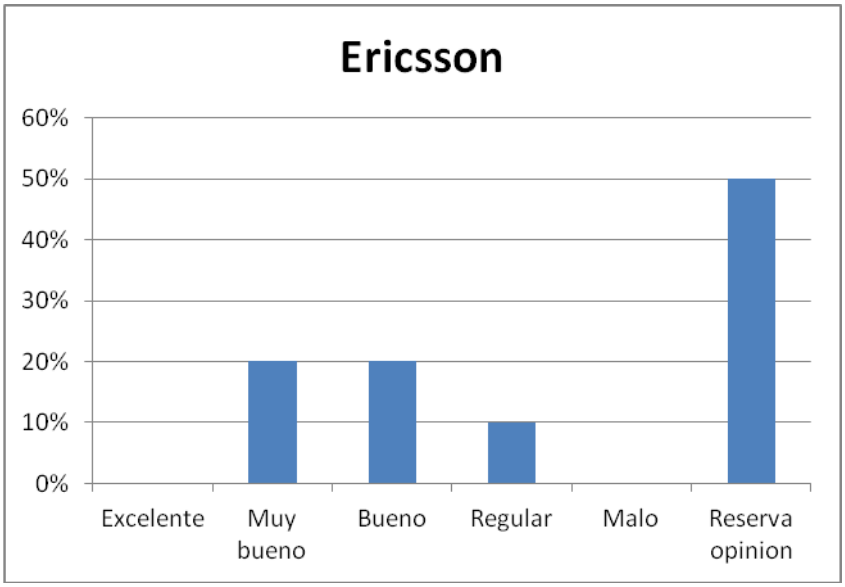


Figura 69: Percepción sobre equipos Ericsson

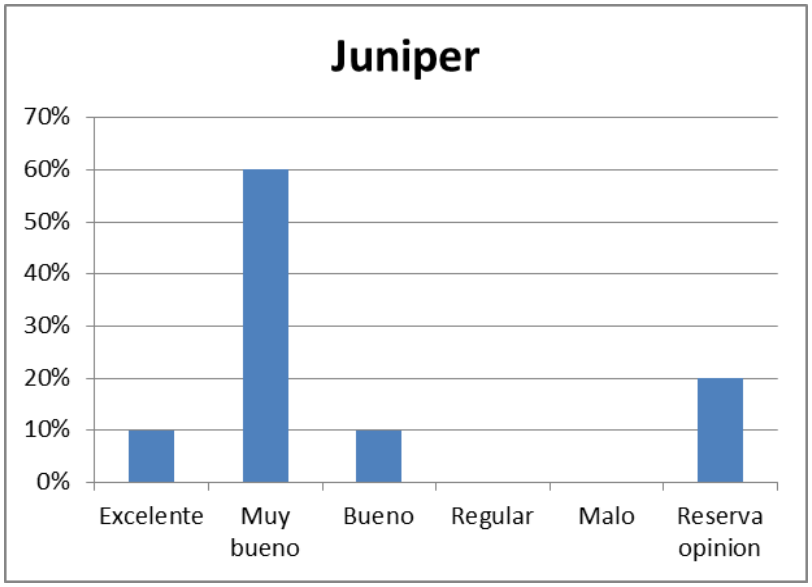


Figura 70: Percepción sobre equipos JUNIPER

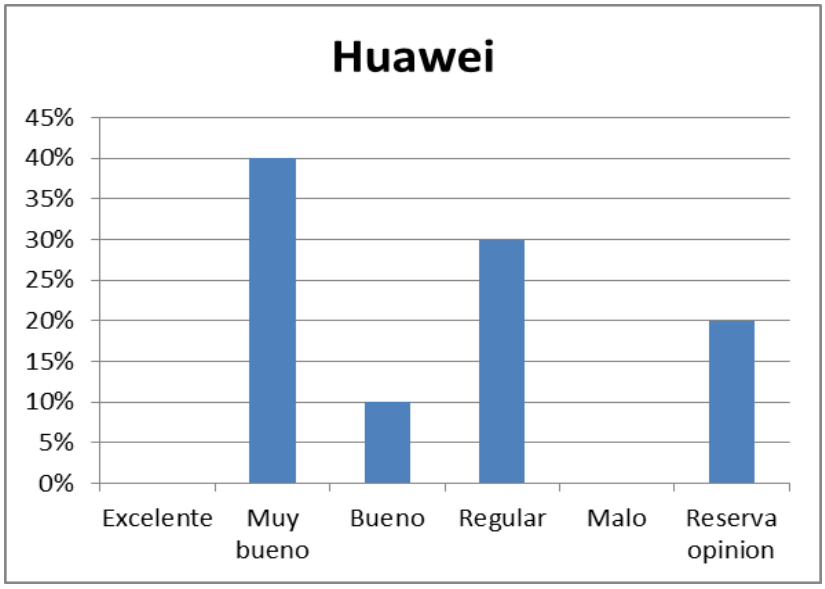


Figura 71: Percepción sobre equipos HUAWEI

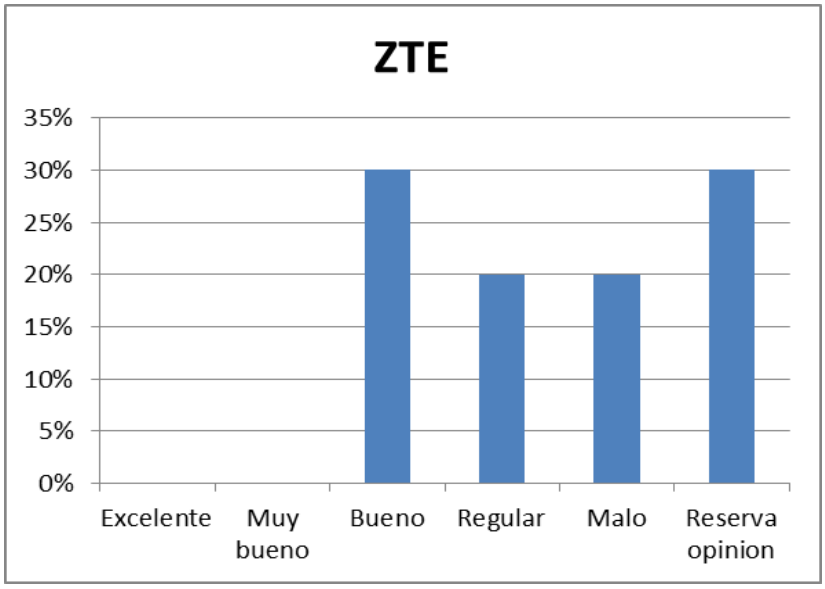


Figura 72: Percepción sobre equipos ZTE

Como se puede observar, Cisco es el mejor calificado en la opinión de los especialistas para proveer ME CE 2.0

Un hecho para mencionar es que la reserva de opinión se puede deber a las relaciones comerciales entre proveedores de equipos y sus consumidores.

Anexo II: Detalle de siglas utilizadas

802.1 ad: Norma del IEEE que especifica el funcionamiento de las redes PB.

802.1 ah: Norma del IEEE que especifica el funcionamiento de las redes PBB.

802.1Q: Norma del IEEE que especifica el tratamiento para el funcionamiento de redes virtuales.

ATM : Asynchronous Transfer Mode

BCB : Backbone Core Bridge in 802.1ah

B-DA : Backbone Destination Address

BEB : Backbone Edge Bridge in 802.1ah

BGP : Border Gateway Protocol

B-SA : Backbone Source Address

B-VID : Backbone VLAN ID

CE 1.0 : Carrier Ethernet 1.0 es una certificación otorgada por el MEF.

CE 2.0 : Carrier Ethernet 2.0 es una certificación otorgada por el MEF.

CFI : Canonical Format Indicator

CPVPN: Customer Provisioned VPN (CPVPN)

CSMA : Carrier Sense Multiple Access

CVLAN: Customer VLAN

DEI : Drop Eligible Indicator.

DLCI : Data Link Connection Identifier

DSL : Digital Subscriber Line

EIGRP : Enhanced Interior Gateway Routing Protocol

E-LAN : Servicio E-LAN definido por MEF utilizado para crear VPN L2 multipunto y un servicio de LAN transparente; constituye los cimientos de las redes IPTV y de multidifusión.

E-Line : Servicio E-Line definido por MEF utilizado para crear líneas privadas Ethernet, líneas privadas virtuales y acceso Ethernet a Internet.

E-Tree : Servicios de árbol privado Ethernet (EP-Tree) definido por MEF y árbol privado virtual Ethernet (EVP-Tree). Proporcionan la separación del tráfico entre usuarios,

permitiendo que el tráfico de una “hoja” llegue a una de varias “raíces”, pero que nunca se transmita a otras “hojas”.

EVC : Circuito virtual Ethernet definido por MEF.

EXP : Experimental bits in MPLS label

FCS : Frame Check Sequence

FEC : Forwarding equivalent Class

FR : Frame Relay

GAC o G-ac: Generic Associated Channel.

GMPLS: Generalized MPLS

HDLC : High level Data Link Control

IETF : Internet Engineering Task Force

IGP : Interior Gateway Protocol

IP - : Internet Protocol

I-SID : Instace Service ID

ISIS : Intermediate System-to-Intermediate System Protocol

I-TAG : Instance TAG

ITU : International Telecommunication Union

ITU-T : International Telecommunication Union Telecommunication Standardization Sector

L2VPN: Layer 2 Virtual Private Network

L3VPN: Layer 3 Virtual Private Network

LAN : Local Area Network

LDP : Label Distribution Protocol

LER : Label Edge Router

LIFO : Last Imput First Ouput

LLC : Logical Link Control

LSP : Label Switching Path

LSR : Label Switching Router

LTE : Long-Term Evolution, conocida como 4G LTE

MAC : Media Access Control

ME : Metro Ethernet

MEF : Metro Ethernet Forum

MPLS : Multi Protocol Label Switching

MPLS - BGP: MPLLS con señalización BGP

MPLS - LDP: MPLLS con señalización LDP

MPLS-RSVP-TUNNELS: Tunel MPLS con RSVP

NMS : Network Management System

OAM : Operation And Maintenance

OSI : Open system interconnection

OSPF : Open Shortest Path First

OTN : Optical Transport Network

P : Provider Router

PB : Provider Bridge

PBB : Provider Backbone Bridge

PBBTE: Provider Backbone Bridge traffic Engineering

PE : Provider Edge Router

PPP : Point to Point Protocol

PPTP : Point to Point Transport Protocol

PPVPN: Provider Provisioned VPN

QoS : Quality of Service

RFC : Request For Comments

RIB : Routing Information Base

RIP : Routing Information Protocol

RSVP : Resource Reservation Protocol

SDH : Synchronous Digital Hierarchy

SONET: Synchronous Optical Network

SVLAN: Service VLAN

TCP/IP: Transport Control Protocol / Internet Protocol

TDM : Time Division Multiplexing

TLV : Time Length Value

T-MPLS: Transport MPLS

TPID : Tag Protocol IDentifier

TTL : Time To Live

UDP : User Datagram Protocol

UNI : User Network Identifier

VC : Virtual Channel

VCI : Virtual Channel Identifier

VID : VLAN ID

VLAN : Virtual Local Area Network

VLAN-ID: VLAN ID

VLL : Virtual Leased Line

VPI : Virtual Path Identifier

VPLS : Virtual Private LAN Service

VPN´s : Virtual Private Networks

VPWS : Virtual Private Wire Service

VRF : Virtual Route Forwarding

X.25 : Recomendación ITU

Anexo III: Artículo presentado en el Congreso 2014.

Tecnologías Carrier-Ethernet

Daniel Biga, Fernando Dufour, Ariel Serra, Carlos Peliza

Universidad Nacional de La Matanza, Florencio Varela 1903 (B1754JEC) -- San Justo, Buenos Aires, Argentina
infoingenieria@unlam.edu.ar

Abstract

Ethernet es una tecnología originalmente diseñada para el intercambio sencillo de datos a través de red de área local (LAN) en los campus o empresas, sin embargo su éxito ha hecho que las necesidades de sus prestaciones se amplíen a áreas mucho mayores como lo son las redes MAN y WAN. La tecnología Carrier-Ethernet presenta un conjunto de protocolos estándares para poder brindar servicios Ethernet a clientes dentro de una infraestructura de gran porte, ofreciendo escalabilidad, transparencia de la información y calidad de servicio. Nuestra investigación se focaliza en el estado del arte de las tecnologías involucradas, la interoperabilidad de las mismas y el criterio para poder proporcionar los servicios Ethernet que el mercado solicita en la actualidad. Hemos analizado la opinión de los especialistas que trabajan en estas tecnologías y realizamos una prospectiva de lo que consideramos que ocurrirá en los próximos 3 años y nuestra visión de lo que en la actualidad son las mejores prácticas para su implementación.

Key words: **Carrier Ethernet, 802.1q, 802.1ad, 802.1ah, PBB y PBB-TE**

1. Introducción

En este trabajo se describe cómo funcionan los protocolos basados en tecnologías Ethernet para poder dar servicio a clientes (residenciales o empresas) que requieren interconectar sus sitios de forma transparente o un determinado servicio en redes de gran tamaño (Metro Ethernet). Para poder comprender cronológicamente como ha crecido la demanda y las nuevas necesidades de escalabilidad y calidad de servicio, presentaremos la evolución de los protocolos hasta el protocolo más actual estandarizado. Mostraremos como la evolución siempre contempla los escenarios legados de las redes para mantener los servicios existentes coexistiendo con los nuevos desafíos que presenta el mercado de las telecomunicaciones.

Comentaremos los resultados más significativos de las opiniones obtenidas en reuniones realizadas con especialistas del mercado involucrados en el desarrollo de estas tecnologías. En dichas reuniones, se trataron los temas relevantes asociados a Servicios Carrier-Ethernet y Redes de Telecomunicaciones. La información obtenida la hemos reflejado en diversas Tablas.

2. Metro Ethernet Forum

El MEF es una alianza de la industria mundial que comprende más de 220 organizaciones, incluyendo proveedores de servicios de telecomunicaciones, fabricantes de equipos de redes y/o software, vendedores de semiconductores y organizaciones de prueba. Su función es definir todos los aspectos relacionados con los servicios Carrier Ethernet, la misión es acelerar la adopción mundial de redes y servicios Ethernet Carrier-class.

El Metro Ethernet Forum (MEF) ha definido los atributos de calidad de Carrier que distinguen a "Servicios de Carrier Ethernet" de los servicios Ethernet tradicionales basados en LAN. El MEF es agnóstico respecto de las tecnologías que implementan los servicios que comentaremos en este documento. Los proveedores adoptaron las tecnologías MPLS, MPLS-TP, PBB y PBB-TE para este tipo de prestaciones por tener las características y capacidades necesarias para prestar los servicios Carrier Ethernet, estas tecnologías las explicaremos en detalle.

2.1. CE 1.0 – Primera versión de Carrier Ethernet

En sus comienzos (2001) el MEF se focalizó en la necesidad de impulsar la tecnología Metro Ethernet, definiendo servicios y ordenando el caos que existía en la prestación de dichos servicios. A partir de allí se focalizó en los primeros servicios Carrier Ethernet, expandiendo estos a ámbitos nacionales e internacionales.

La primera versión definida por el MEF ofrece servicios Carrier Class estandarizados en la red de un proveedor, a esta se la conoce como CE1.0 (Carrier Ethernet1.0).

A continuación se comentan los servicios CE 1.0:

2.1.1. Servicio E-Line

El servicio E-Line consiste en un tipo de servicio Ethernet que se basa en un *Ethernet Virtual Connection* (EVC) punto-a-punto, para interconectar dos UNIs (User–Network Interfaces)

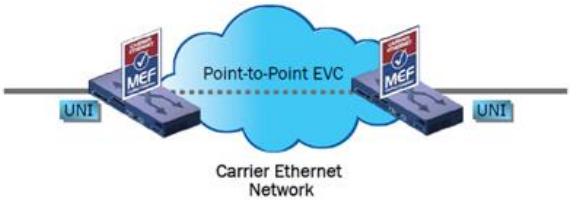


Fig. 1. Servicio E-Line

Los Servicios E-Line que se pueden ofrecer son:

- Ethernet Private Lines
  - Una sola UNI en cada extremo de red.
  - Similar a un circuito TDM.
- Virtual Private Lines
  - Una UNI se usa para múltiples conexiones virtuales.
  - Similar a Frame Relay o ATM

2.1.2. Servicio E-LAN

El servicio E-LAN está basado en un EVC (Ethernet Virtual Connection) multipunto a multipunto.

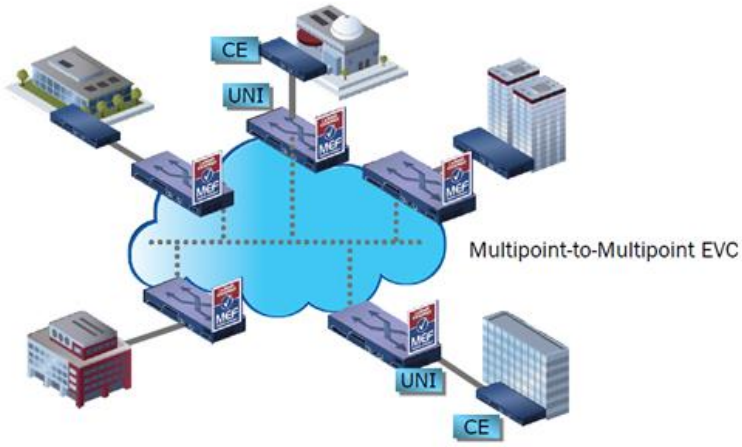


Fig. 2. Servicio E-LAN

Los Servicios E-LAN que se pueden ofrecer son:

- Multipoint L2 VPNs Multipunto.
- Servicio de LAN transparente.

2.1.3. Servicio E-Tree

Es un tipo de servicio que está basado en EVCs multipunto que convergen en un nodo raíz.

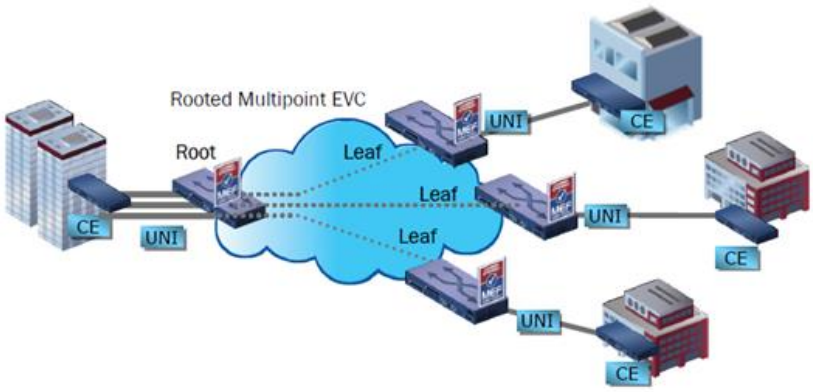


Fig. 3. Servicio E-Tree

Servicios:

- Topología punto a multipunto.

- Provee separación de tráfico entre los terminales hoja del multipunto.
    - El nodo raíz se puede comunicar con cualquier hoja.
    - Las hojas solo se pueden comunicar con el nodo raíz.

Se puede resumir los tipos de servicios CE 1.0 en el siguiente gráfico:

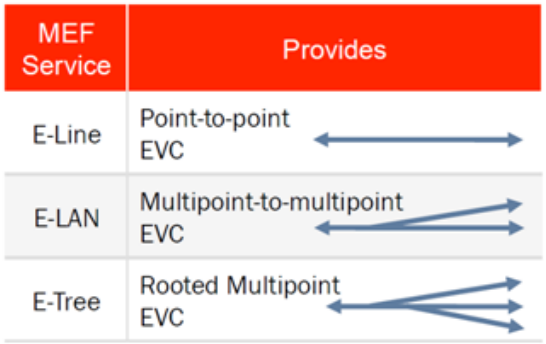


Fig. 4. Resumen Servicios CE 1.0

2.2. CE 2.0 – Next generation Carrier Ethernet

Mientras que CE 1.0 permitió la estandarización de redes y servicios Ethernet en el marco de una red de proveedor de servicios, Carrier Ethernet CE 2.0 (lanzado en 2012) innovó con estándares de red para proveedores de servicios, que tiene tres características diferenciales: maneja Multiple Classes of Service (Multi-CoS), e incorpora más funcionalidades de gestión e interconexión para expandir el alcance de los servicios.

Estas tres características se suman a la expansión de la cantidad de servicios soportados, que en CE 1.0 eran tres, ahora son ocho: dos por cada clase de servicio (E-Line, E-LAN, E-Tree y E-Access, las tres primeras ya estaban en CE 1.0), según están definidos por las especificaciones de MEF.

El servicio E-Access, permite a proveedores de servicios CE 2.0 minoristas ampliar su cobertura de manera más eficiente y económica mediante asociaciones con proveedores mayoristas.

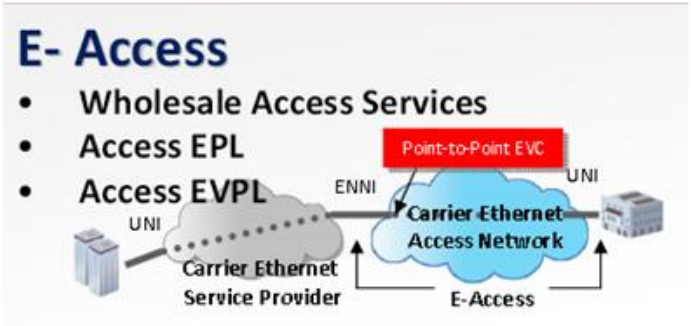


Fig. 4. Resumen Servicios CE 1.0

Con respecto a las nuevas características de MEF CE 2.0, podemos detallar:

Multi-CoS

Las nuevas extensiones de Class of Service (clase de servicio), por primera vez, estandarizan los objetivos de desempeño a través de varias capas geográficas de desempeño y aplicaciones. Esto resulta en una calidad de servicios mejorada y optimiza la eficiencia, especialmente cuando se usan los cuatro servicios basados en VLAN de MEF.

Interconexión

Se refiere al intercambio estandarizado de tráfico Carrier Ethernet entre proveedores y para la provisión eventual en redes de acceso, usando los tipos de servicio E-Access recientemente aprobados, mientras que se preservan los atributos del servicio. En términos simples, esto permite que los proveedores diseñen múltiples redes interconectadas como una red única desde el punto de vista del usuario (lo cual habilita la concreción de un único Service Level Agreement, entre otras ventajas).

Gestión

CE 2.0 aporta nuevas funciones de gestión que estandarizan el manejo de fallas a niveles que no eran posibles en la versión anterior, para servicios provistos a través de múltiples redes.

A la fecha de creación de este paper, existen 21 proveedores de servicios certificados con 87 servicios definidos por el MEF CE 2.0 en 10 países. Además existen 31 proveedores de equipos de red con certificación CE 2.0 con más de 120 plataformas CE 2.0. La amplia disponibilidad y la creciente implantación de plataformas de redes CE 2.0 es un factor crucial del crecimiento en la certificación de servicios CE 2.0.

Durante el pasado año, el número de profesionales certificados por el MEF se ha triplicado hasta más de 1.700 en 224 organizaciones de 58 países. El 87 % de los profesionales certificados por el MEF trabaja para empresas miembros del MEF y el 62 % para proveedores de servicios.[i]

3. Tecnologías Carrier Ethernet

3.1. VLAN (802.1q)

Las VLAN (Virtual Local Area Network) son la base de las tecnologías Ethernet y por consecuencia Carrier Ethernet, las VLAN permiten separar los dominios de broadcast de nivel 2 (capa de enlace del modelo TCP/IP) incrementando el rendimiento de una red física. Una VLAN, nos brinda la posibilidad de que un administrador de red pueda crear grupos de dispositivos conectados de manera lógica, que actúan como una red independiente de otras con las cuales pueden compartir infraestructura. Para tener una trama etiquetada (802.1q), el procedimiento en el switch consiste en agregar 4 bytes luego de la dirección MAC origen de una trama Ethernet, debido a este agregado es necesario recalcular la secuencia de chequeo de trama (FCS).

Se muestra una gráfica de una trama de nivel 2 con 802.1q.

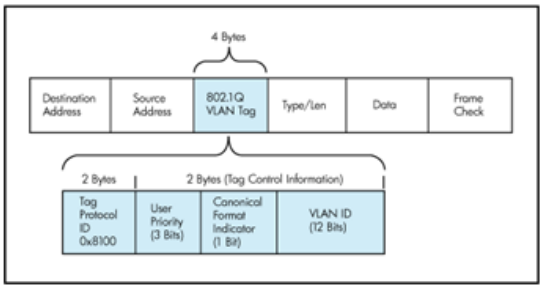


Fig. 5. Encabezado 802.1q

Dentro de la etiqueta de VLAN, se descomponen los campos que se describen a continuación:

TPID (Tag Protocol IDentifier): Este campo indica que estamos en presencia de una trama etiquetada, se compone de los siguientes parámetros que se pueden apreciar en la gráfica. El valor en hexadecimal 8100 indica que estamos en presencia de una etiqueta 801.1q.

PCP (Priority Code Point): Son 3 bits que se utilizan generalmene para priorizar un tipo de tráfico por sobre otro, en conjunto con otras políticas de red permite ofrecer una calidad de servicio en la red que permite a un operador dar múltiples servicios sobre la misma infraestructura. A estos bits se los conoce como “IEEE 802.1p”.

CFI (Canonical Format Indicator): Este bit se utiliza para indicar si en presencia de congestión esta trama puede ser descartada o no. También se lo conoce como DEI (Drop Eligible Indicator).

VID (Vlan IDentifier): Es el número identificatorio de la VLAN, son posibles 4096 numeraciones, aunque el número 0 no es posible utilizar.

Este protocolo permitió compartir una misma infraestructura para brindar múltiples servicios, pero rápidamente tuvo una limitante, que es la cantidad de VLANs que se pueden asignar (4094). Para solucionar este problema se desarrolló el estándar 802.1ad.

3.2. DOBLE TAG-SVLAN (802.1ad) – PROVIDER BRIDGE

802.1ad estandariza el uso de multiples Tags de VLAN en los switches bridgeados, facilitando la implementación de los servicios de CE (Carrier Ethernet), por ejemplo, permite que el proveedor le ofrezca utilizar, VLANs del cliente y poder transportarlas dentro de la Red bridgeada del Carrier siendo completamente transparente para el cliente.

De similar procedimiento que el estándar 802.1q, el protocolo 802.1ad coloca una nueva etiqueta similar a la anterior pero con algunas diferencias que se comentan a continuación. El límite teórico de conexiones VLANs que se pueden configurar es de más de 16 millones de conexiones, ya que permite que las 4096 de la VLAN 802.1q combinarlas con las 4096 SVLAN 802.1ad.

Se puede ver en la gráfica a continuación donde se inserta la nueva etiqueta en la trama.

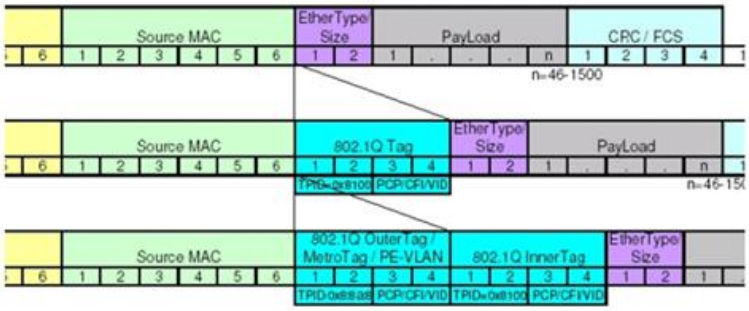


Fig. 6. Doble TAG de VLAN (802.1ad)

En las SVLAN se utiliza el valor 88a8 hexadecimal en el TPID, para diferenciar la etiqueta de VLAN.

Con este protocolo no solo se aumenta la cantidad de VLANs que se pueden transportar en una red bridgeada sino que se puede transportar tráfico de nivel 2 de clientes (es la VLAN interna y se la conoce como Customer VLAN C-VLAN “801.1q”) dentro de una etiqueta de servicio propia del operador de la red (se la conoce como Service VLAN S-VLAN “802.1ad”).

Lo comentado puede verse mejor en el siguiente diagrama:

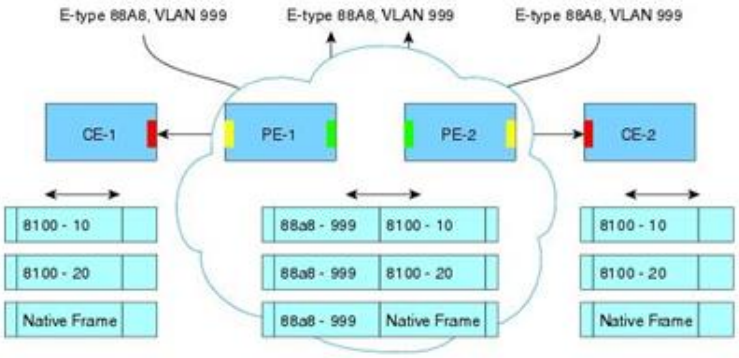


Fig. 7. Ejemplo de arquitectura (802.1ad)

El cliente CE-1 tiene tráfico Ethernet sin etiquetar, etiquetado con la VLAN-10 y también tráfico con la VLAN-20. La red del proveedor utiliza el estándar 802.1ad para poder transportar en una red de nivel 2 los datos del cliente, en este ejemplo utiliza el número 999 como S-VLAN y mantiene las etiquetas de cliente que ahora serán las C-VLAN 10, C-VLAN 20 y tráfico sin etiqueta. En el equipo del cliente CE-2 se puede ver como el proveedor retira la etiqueta de servicio (S-VLAN) y entrega al equipo de forma transparente el tráfico a destino.

Al mismo tiempo que la demanda de servicios fue creciendo, los proveedores comenzaron a sufrir problemas de escalabilidad, el principal problema fue que la cantidad de MAC ADDRESS que los equipos tienen que contener en las tablas para conmutar las tramas crecía con la cantidad de clientes, esto impacta directamente en la capacidad de memoria de los equipos y el tiempo de procesamiento que los mismos deben tener para no aumentar la latencia de la red.

Existen dos soluciones de fondo para solucionar este problema, o se escala a nivel 3 del modelo TCP/IP (habitualmente utilizando la tecnología MPLS), es decir, utilizando

protocolos de la capa de IP, o se busca un mecanismo dentro de nivel 2 que solucione el problema de las MAC ADDRESS. A esto último apuntó el estándar 802.1ah que comentamos a continuación.

3.3. MAC-IN-MAC (802.1ah) – PROVIDER BACKBONE BRIDGE

El concepto consiste en definir un nuevo nivel de red bridgeada que tiene sus propios componentes y que son independientes de los del cliente, ofreciendo una completa separación entre los dominios de cliente con los dominios del proveedor, para lograr este resultado, se definió una nueva cabecera Ethernet. Es entonces que encontramos en esta arquitectura una nueva estructura de tramas con MAC ADDRESS independientes de las del cliente y otros elementos que detallaremos en la descripción del header.

En los accesos, todas las PB (802.1ad) de los clientes se mapean a una instancia PBB (802.1ah) de red, definida por el proveedor de servicios. Dicha PBB encapsulará el tráfico añadiendo sus propias direcciones MAC de origen y destino, de forma que el resto de equipos de la red sólo deben conocer las MACs de los nodos de red, dejando a los equipos de borde la responsabilidad de mantener las entradas de los clientes. Así, las MACs de los usuarios finales son transparentes para los nodos de red.

Los equipos en los extremos del PBB, llamados BEB (Backbone Edge Bridge), son los que soportan toda la carga del trabajo. Al ingreso de una trama al bridge de borde de la red 802.1ah, esta se la asocia con una instancia de servicio y la encapsula en una trama, de tal forma que se caracteriza por usar un nuevo juego de MACs que se denominan Backbone MACs.

En la parte de red, el proveedor añadirá una nueva cabecera Ethernet con direcciones MAC propias de los equipos de red, de forma que dentro del Core 802.1ah (BCB – Backbone Core Bridge) sólo se manejen las MACs de los nodos de red, dejando las direcciones de clientes en el borde de la red.

En el gráfico a continuación se resume lo expresado:

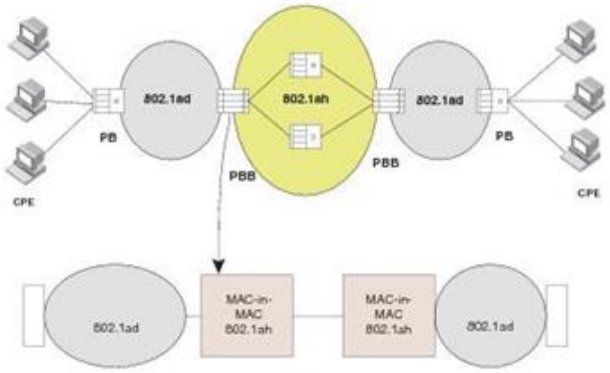


Fig. 8. Ejemplo de arquitectura (802.1ah)

Apoyado en la gráfica siguiente comentaremos los campos que el estándar 802.1ah contiene:

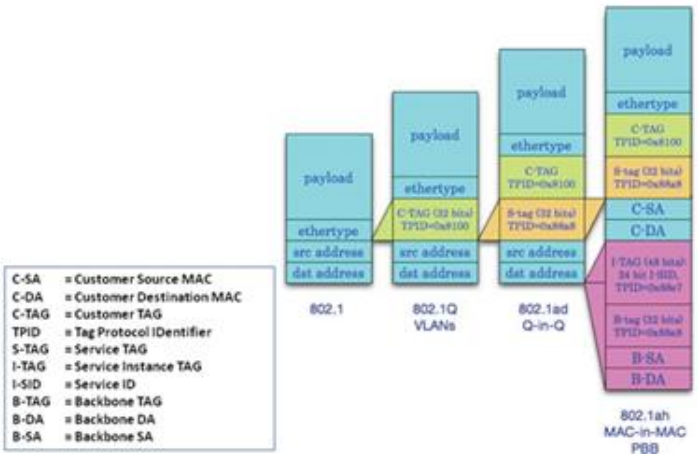


Fig. 9. Tecnologías Carrier Ethernet

Como se puede observar, en la red del proveedor de servicios modifica la trama Ethernet incorporando 22 bytes en los campos que se detallan a continuación:

B-DA (Backbone Destination Address) 6 Bytes: Es la MAC de destino del nodo de la red del proveedor, es este caso la red no tiene visibilidad de las MAC del cliente.

B-SA (Backbone Source Address) 6 bytes: Es la MAC del equipo que origina la trama 802.1ah.

B-TAG (Backbone vlan TAG) 4 bytes: Este campo es análogo al formato tradicional de VLAN, con el TPID (Ethertype) con el valor 88a8 en hexadecimal. El formato se completa con el PCP y CFI (DEI) y el VLAN ID.

I-TAG (Instance service TAG) 6 bytes: Contiene la instancia del servicio, el formato completo está compuesto por dos parámetros, un TPID (Ethertype) con valor 88e7 y el parámetro TCI (4 bytes) que podemos descomponer en sub-campos:

- PCP (3 bits)
- CFI (o DEI, 1 bit)
- Reservado (4 bits)
- I-SID (24 bits)

El sub-campo I-SID (Instance Service ID), contiene la instancia del servicio, con este valor se genera la EVC (Ethernet Virtual Circuit) y el estándar permite un total de más de 4 millones de EVCs.

Los campos detallados B-TAG e I-TAG se pueden resumir en el siguiente gráfico:

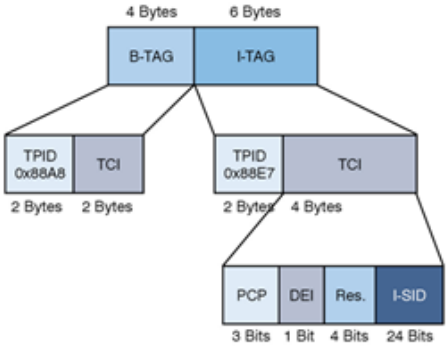


Fig. 10. Encabezados B-TAG e I-TAG

4. Conclusiones

El enfoque PBB limita el alcance de la información del cliente, dirigiéndose MAC y la topología, a los bordes de la red del proveedor de servicio. El núcleo sigue centrado en las funciones básicas y dejando de lado el conocimiento de la red del cliente. Sin embargo, PBB se enfrenta a serios desafíos en la red del proveedor. Uno de ellos es que PBB carece de ingeniería de tráfico y capacidad de recuperación de nivel de operador. Por otra parte, la dependencia de PBB en el protocolo Spanning Tree múltiple (MST) o el protocolo Rapid Spanning Tree (RSTP) para evitar bucle es un serio inconveniente ya que podría tardar unos segundos en converger ante una falla en la red. Las redes de transporte a gran escala han eliminado STP (Spanning Tree Protocol) a fin de ampliar y lograr mejores tiempos de recuperación. Para sortear las limitaciones de STP, el IEEE ha desarrollado una tecnología de detección de la topología alternativa llamada Shortest Path Bridging (SPB o IEEE 802.1aq) para las redes de PB y PBB.

Esta tecnología proporciona redes lógicas en una infraestructura Ethernet nativa, usando un protocolo “link state” para anunciar tanto la topología como la pertenencia a una red lógica. Los paquetes son encapsulados MAC-in-MAC 802.1ah o marcados 802.1Q/802.1ad en el extremo de la red y transportados solamente a otro miembro de la red lógica. El trafico unicast, multicast y broadcast está soportado y todo se encamina por el camino más corto. El plano de control está basado en “Intermediate System to Intermediate System (IS-IS)”, con un pequeño número de extensiones añadidas definidas en el RFC 6329. El protocolo 802.1aq es de reciente estandarización, su análisis no está contemplado dentro del presente artículo.

5. Estado del arte

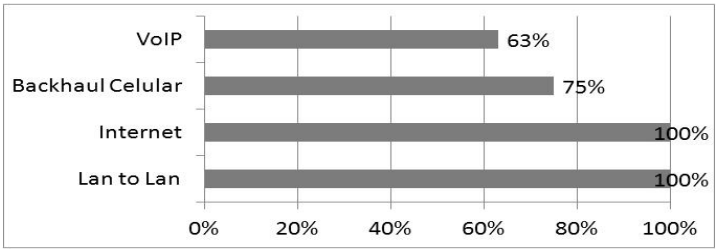
El presente trabajo refleja el estado del arte de las tecnologías metrohethernet de próxima generación en la Argentina.

Para ello hemos tenido reuniones con especialistas de las empresas de telecomunicaciones líderes y de empresas proveedoras de equipos quienes nos aportan su visión actual y futura sobre estas tecnologías.

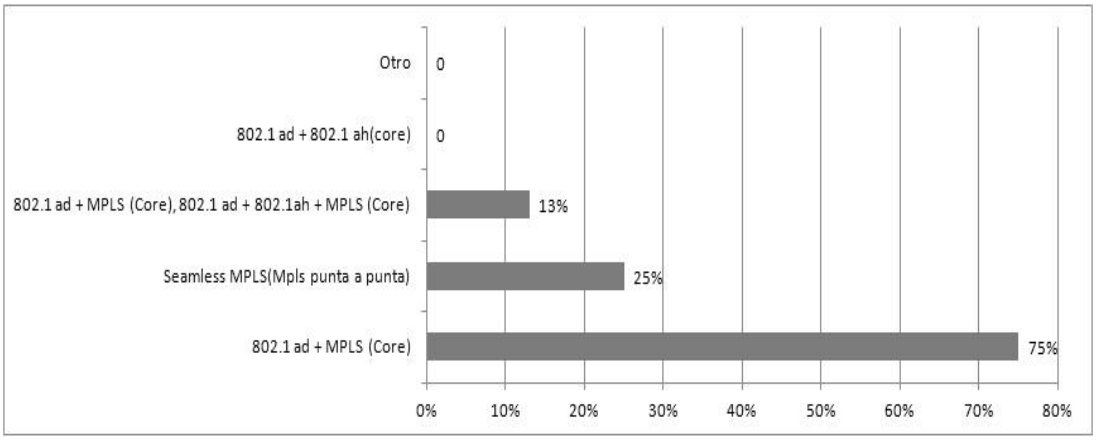
El relevamiento de las opiniones de especialistas y profesionales de comunicaciones nos permitieron determinar las nuevas tendencias sobre la evolución de la tecnología.

En los siguientes gráficos mostramos una parte relevante de los resultados de la investigación:

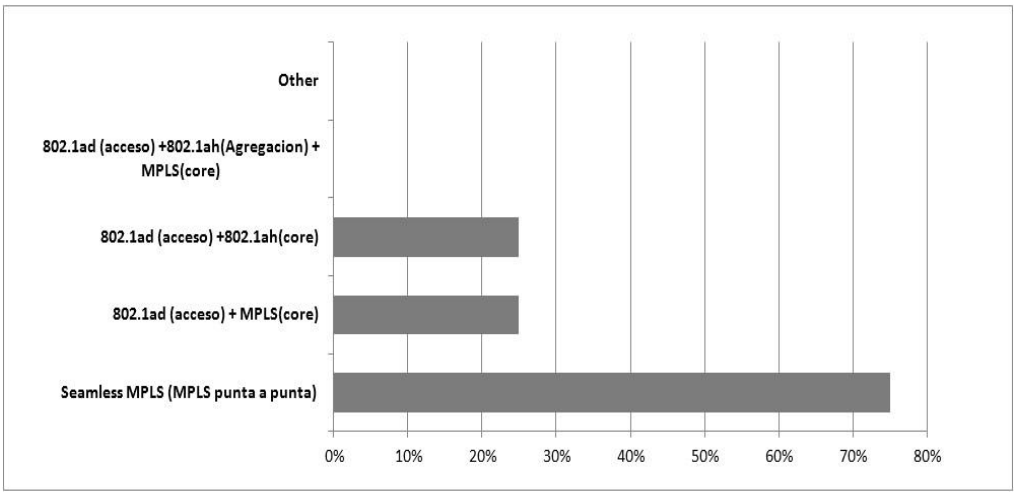
Respecto de los servicios que se transportan en las redes Metroethernet actuales, hemos obtenido los siguientes resultados:



Respecto de las soluciones tecnológicas que están siendo usadas en la actualidad, hemos obtenido los siguientes resultados:



Respecto de la forma en que se escalará la red para satisfacer el crecimiento del mercado, se han obtenido las siguientes respuestas:



6. Futuras líneas de investigación

La solución adecuada para cada problemática es dependiente de la dimensión de la red que hay que diseñar como así también de las prestaciones que pretendemos de ella. Por ello y dada la gran variedad de combinaciones tecnológicas posibles para dar solución en particular y la cantidad de casos posibles existentes en el mercado, hemos puesto nuestro foco en las necesidades y dimensiones del mercado Argentino.

Con esta información desarrollaremos una futura línea de investigación en la que nos focalizaremos en la determinación de las mejores prácticas y prospectiva para los próximos 3 años en el mercado Argentino.

7. Referencias

Michael Beck (2005). *Ethernet in the First Mile: The IEEE 802.3ah EFM Standard (Communications Engineering)*. McGraw-Hill Professional, ISBN-13: 978-0071455060 ISBN-10: 007145506X. First edition.

Sam Halabi (2003). *Metro Ethernet*. Cisco Press. Indianapolis.ISBN: 1-58705-096-X.

Monique Monrrow and Azhar Sayeed. (2006). *MPLS and Next-Generation Network*. Cisco Press. Indianapolis. ISBN: 1-58720-120-8.

J. Guichard and I. Pepelnjak (2000). *MPLS and VPN Architectures*, Cisco Press. Indianapolis. ISBN: 1-58705-002-1.

Bruce S. Davie,Paul Doolan,Yakov Rekhter (May 1998). *Switching in IP Networks: IP Switching, Tag Switching, and Related Technologies*. ISBN-13: 978-1558605053 ISBN-10: 1558605053. First edition

Wei Luo,Carlos Pignataro,Dmitry Bokotey,Anthony Chan (February 2005) *Layer 2 VPN Architectures*. Cisco Press. Indianapolis. ISBN: 1-58705-168-0.

Bruce S. and Davie, Yakov Rekhter (June 2, 2000) *MPLS: Technology and Applications*. ISBN-13: 978-1558606562. ISBN-10: 1558606564. First Edition.

8. Definiciones

E-LAN - Servicio E-LAN definido por MEF utilizado para crear VPN L2 multipunto y un servicio de LAN transparente; constituye los cimientos de las redes IPTV y de multidifusión.

E-Line - Servicio E-Line definido por MEF utilizado para crear líneas privadas Ethernet, líneas privadas virtuales y acceso Ethernet a Internet.

E-Tree - Servicios de árbol privado Ethernet (EP-Tree) definido por MEF y árbol privado virtual Ethernet (EVP-Tree). Proporcionan la separación del tráfico entre usuarios, permitiendo que el tráfico de una “hoja” llegue a una de varias “raíces”, pero que nunca se transmita a otras “hojas”.

EVC - Circuito virtual Ethernet definido por MEF.

802.1Q - SPB combina una ruta de datos Ethernet (IEEE 802.1Q o puentes de red troncal de proveedor (PBB) IEEE 802.1ah) con un protocolo de control de estado de enlace IS-IS entre los puentes con rutas más cortas (enlaces NNI).

Certificado de referencia


Tercer Congreso Argentino de la Interacción-Persona Computadora, Telecomunicaciones, Informática e Información Científica (IPCTIIC)

Third Argentine Conference on Human-Computer Interaction, Telecommunications, Informatics and Scientific Information (HCITISI)

Certificate

PAPER PRESENTATION

IPCTIIC 2014 :: HCITISI 2014

Huerta Grande – Córdoba, Argentina

November 13 – 14, 2014

Tecnologías Carrier-Ethernet

Fernando Javier Dufour

Universidad Nacional de La Matanza

Buenos Aires, Argentina

AInCI

ALAIPO

Anexo IV: Artículo presentado en el Congreso 2015

VPNs (Virtual Private Networks)

Daniel Biga, Fernando Dufour, Ariel Serra, Carlos Peliza

Universidad Nacional de La Matanza, Florencio Varela 1903 (B1754JEC) -- San Justo, Buenos Aires, Argentina
infoingenieria@unlam.edu.ar

Abstract

La característica principal de las VPN (Virtual Private Network) es utilizar la infraestructura de las redes públicas y privadas compartidas para ofrecerle a un cliente las facilidades de una red privada. Esto permite a los usuarios beneficiarse de las prestaciones, la seguridad y la gestión de redes de alta performance a costos más accesibles. Las nuevas tecnologías permitieron implementar las VPNs basándolas en redes IP e IP/MPLS (MultiProtocol Label Switching), permitiendo minimizar inversiones y disponer de mayor velocidad de transmisión.

En nuestro trabajo hemos realizado una investigación sobre el estado del arte actual de esta tecnología, focalizándonos en sus principios y alternativas de funcionamiento, también hemos expuesto un ejemplo de un caso de implementación actual en Argentina que nos permite ver la importancia de esta tecnología para las comunicaciones actuales.

Key words: **MPLS, VPN, Servicios, Pseudowire**

9. Introducción

Las redes de transmisión de datos X.25, Frame Relay y modo de transferencia asíncrono (ATM) con sus mecanismos de circuitos virtuales fueron las primeras que permitieron la implementación de redes virtuales independientes para cada cliente, soportadas sobre una misma red con nodos y enlaces físicos compartidos provistos y operados por las compañías de telecomunicaciones.

Existen distintos puntos de vista respecto de si estas tecnologías deben ser consideradas o no VPNs, a los efectos de entender la lógica la evolución de estas últimas las incluiremos como tales y las consideraremos VPNs de primera generación.

Sin embargo las primeras VPNs que fueron reconocidas como tales son las que se establecían sobre las redes IP, destacándose entre ellas las que armaban los clientes entre ordenadores y servidores de VPN en entornos corporativos conocidas como VPNs de acceso remoto. Este tipo de VPN permite que empleados puedan acceder a la intranet de su empresa desde su casa o mientras viaja fuera de la oficina

Otro tipo de VPNs son las punto-a-punto, que permiten unir las oficinas geográficamente dispersas de una empresa.

En las VPN el proveedor proporciona la conectividad entre los sitios del cliente, y permite que sólo los dispositivos que pertenezcan a la misma VPN tengan visibilidad entre ellos. Ningún dispositivo no autorizado pueda acceder a la VPN.

A continuación detallaremos distintas formas de clasificar a las VPNs.

De acuerdo a la evolución histórica de las VPNs, podemos clasificarlas de la siguiente manera:

1ª Generación →Terminadas en el CE y basadas en líneas dedicadas que se alquilaban al proveedor.

2ª Generación →Terminadas en el CE a base de circuitos virtuales ATM/Frame Relay sobre una red de conmutación de paquetes del proveedor.

3ª Generación → Los proveedores ofrecen servicios para gestionar los routers del cliente usados en las terminaciones en el CE.

4ª Generación → VPNs de nivel 3 terminadas en el PE y basadas en IP/MPLS.

5ª Generación → VPNs de nivel 2 terminadas en el PE y basadas en IP/MPLS.

Existen distintos aspectos que permiten caracterizar a las VPNs y una VPN puede contener varias de estas características. En base a esta óptica se las puede clasificar por:

- Según el punto de terminación del túnel.
- Basadas en el CE (overlay)
- Basadas en el PE (peer-to-peer)

Según el tráfico de cliente transportado

- VPN de nivel 3
- VPN de nivel 2

Según el tipo de red del proveedor

IP, IP/MPLS, ATM, Frame Relay, SONET/SDH, red telefónica, etc.

Según la tecnología (protocolos) utilizados para la implementación de túneles

Túneles IPsec, L2TP, PPTP, MPLS-LSP, ATM-VP/VC, Frame Relay, SONET/SDH VT, PPP/Dial-up

Según el Número de redes conectadas

- Punto a punto: 2 sedes
- Multipunto: más de dos sedes

Para nuestro estudio la primera gran división a considerar es:

Customer Provisioned VPN (CPVPN)

Son túneles que interconectan siempre terminales de clientes entre sí (basadas en el CE) que generalmente son simples túneles que interconectan equipos de clientes y en donde la red sólo transporta paquetes IP convencionales.

Provider Provisioned VPN (PPVPN)

Son túneles que interconectan siempre equipos del Carrier y que permiten proveer los servicios definidos por el MEF.

Este es el tipo de túneles en que se focaliza nuestro estudio.

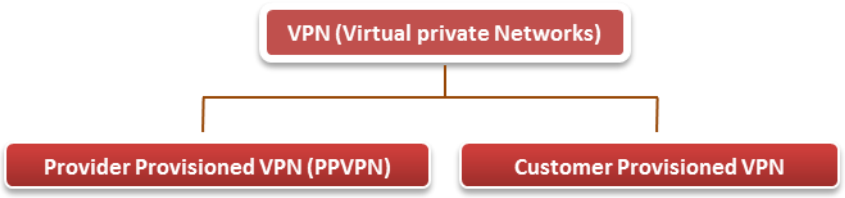


Fig. 2. Primera clasificación de las VPNs

Nos focalizaremos en las PPVPN que es al grupo al que pertenecen las L2VPN.

Provider Provisioned VPN (PPVPN)

Las PPVPN son redes privadas virtuales en las que el proveedor es el responsable de crear y administrar los túneles para el tráfico privado entre los puntos de conexión de clientes.

En la actualidad las redes de los proveedores utilizan la tecnología MPLS que como sabemos, aprovecha el direccionamiento IP y el protocolo de ruteo OSPF, para el establecimiento de los caminos virtuales (Virtual Path).

Por este motivo los proveedores utilizan su infraestructura MPLS como medio de transporte para crear túneles entre los sitios privados. Creando de esta forma un nuevo tipo de servicio, y por ende un nuevo negocio utilizando su red de transporte existente.

Sobre la infraestructura de red MPLS de los Carriers se pueden implementar dos tipos de VPN, las L3VPN (4° generación de VPN) y las L2VPN (5° generación de VPN).

Sobre Las L2VPN nos explayaremos más adelante, pero a continuación haremos una breve mención sobre las L3VPN para que se entienda la diferencia entre ambas.

Las L3VPN también llamadas VPRNs (Virtual Private Routed Networks), permiten que la red sea vista como un súper-router dado que para implementar las VPNs se tienen en cuenta las tablas de ruteo de nivel 3 de cada cliente.

El cliente debe utilizar BGP (MP-BGP) como protocolo de ruteo dentro de la red del proveedor con el objeto de intercambiar la información de ruteo, lo que aumenta la complejidad del diseño y complica la puesta en práctica de este tipo de redes.

Los clientes se conectan con el router del proveedor de servicio, con el que intercambian tablas de rutas, esta información de ruteo es colocada en tablas de ruteo específicas para cada cliente en el router del proveedor (y es transportada con MP-BGP dentro de la red).

Las L3 VPN se puede utilizar para implementar VPNs en redes corporativas, no utilizándose normalmente en redes de servicios públicos debido a su complejidad. En las

redes de servicio público, se ha focalizado en las L2VPN situación que los libera de la complejidad del manejo de la numeración IP a través de las tablas de ruteo.

De las dos opciones la tecnología L2VPN presenta grandes ventajas sobre la L3VPN dado que es vista por los clientes como un switch de nivel 2, evitando las serias consideraciones de plan de numeración IP que tienen las L3VPN. Es por ello que las L2 VPN es la tecnología utilizada para la implementación de los servicios Metro Ethernet CE2.0.

10. L2 MPLS VPN

Las L2 MPLS VPN permiten la implementación de dos modelos de servicio, VPWS (Virtual Private Wire Service) que implica la implementación de un Pseudo Wire que emula conexiones punto a punto y VPLS (Virtual Private Lan Service) que emula un gran LAN Switch permitiendo conexiones punto a punto y multipunto.

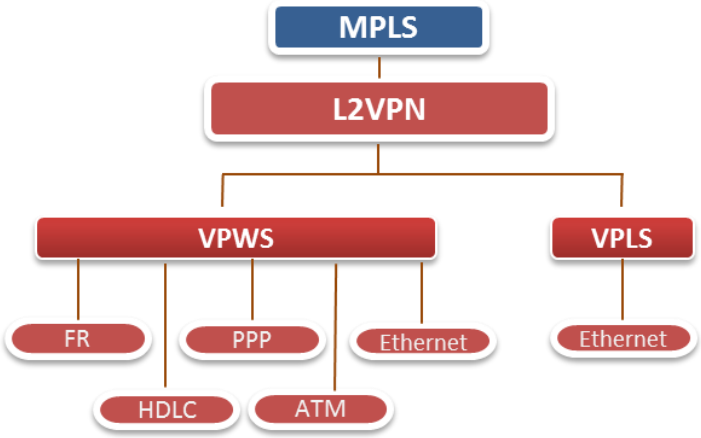


Fig. 2. Modelos L2VPN

Utilizando L2VPNs se logra conectividad en capa 2 entre los sitios, tunelizando las diferentes tecnologías en caminos LSP. De esta forma, se logra transportar una trama L2 entre dos sitios remotos. Desde el punto de vista del cliente, la red del proveedor simula ser una conexión directa (cable) entre los sitios. Las L2VPN son de tipo punto a punto. Los equipos frontera del cliente (Router Customer Edge, CE) mapean el tráfico a un circuito específico (Ethernet, ATM, Frame Relay, etc.) y lo envían al proveedor (Router Provider Edge, PE). El proveedor encapsula dicho tráfico en un LSP, y lo envía hacia el Router PE remoto asociado a dicha conexión. Para obtener conectividad entre varios sitios de una L2VPN, se debe configurar un esquema full-mesh entre los Routers PE. Para este tipo de aplicaciones se puede considerar la utilización de VPLS.

Las tramas del cliente se transmiten utilizando un stack de dos etiquetas MPLS. La etiqueta externa identifica al LSP entre los Routers PE, y la interna identifica a la VPN (Circuito L2) que se está interconectando. Este esquema permite que múltiples VPNs utilicen el mismo LSP de transporte. Debido a que la conexión a través del proveedor se realiza en capa 2, el esquema de ruteo del cliente se implementa en los equipos CE y no involucra al proveedor.

Existen dos variantes de VPNs de capa 2. La diferencia entre las mismas radica en el protocolo de señalización y control que utilizan. Dicho protocolo se utiliza para establecer

las sesiones entre Routers PE, y para negociar la etiqueta VPN a utilizar. Los esquemas son BGP L2VPN (Utiliza el protocolo BGP, draft-Kompella) y LDP L2VPN o LDP L2 Circuit (Utiliza el protocolo LDP, RFC 4447). Al utilizar el protocolo BGP se logra mayor escalabilidad y prestaciones como auto-descubrimiento de vecinos, pero el esquema se hace más complejo. Al utilizar el protocolo LDP, se logra un ambiente más sencillo, pero se debe configurar explícitamente cada vecino y como consecuencia se pierde escalabilidad.

Usando estas tecnologías, el cliente puede tercerizar el transporte de circuitos manteniendo el control del ruteo, utilizando el protocolo de capa 3 que desee. Por otro lado, el proveedor puede utilizar la infraestructura IP/MPLS existente para brindar un nuevo servicio de valor agregado, y utilizar el mismo LSP de transporte para todos los servicios entre Routers PE.

11. Componentes de una red VPLS

Como se ha visto, las nuevas tecnologías de implementación de VPNs trabajan sobre MPLS y a consecuencia de ello, los routers MPLS agregan funciones para el armado de las VPNs, y se los denomina con nuevos nombres. Lo que en una red MPLS se llama LER (Label Edge Router) pasa a llamarse PE y los LSR (Label Switching Router) pasan a llamarse P.

Las empresas públicas que participan en una VPN basada en VPLS se presentan como un LAN Switch de tamaño nacional, independiente para cada cliente que toma servicios sobre sus puertas.

En VPLS, no se pueden producir bucles de información, conocidos como LOOPS: Los PE están conectados en forma full mesh por lo que una trama recibida por un PE (entrante) se envía a otro PE (saliente por una conexión virtual directa. El uso de una configuración full mesh junto con el Split Horizon garantiza un dominio de broadcast, libre de bucles.

A continuación mostramos la arquitectura de una red IP/MPLS que permite implementar VPNs.

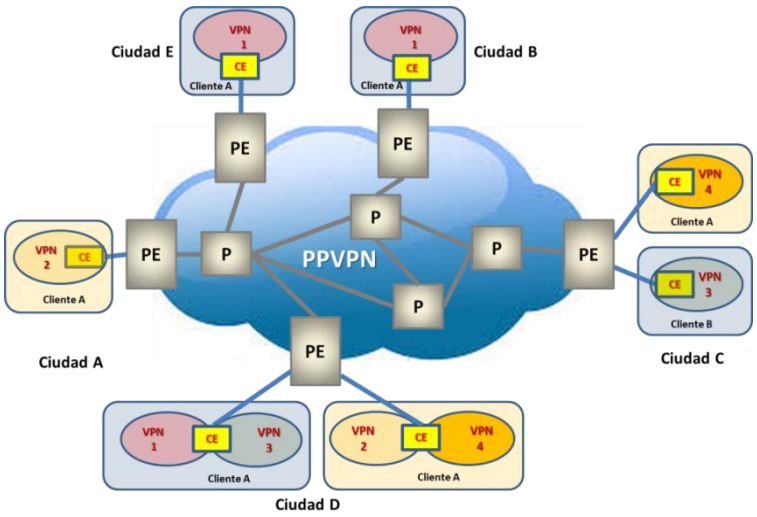


Fig. 3. Arquitectura de L2VPN

Dispositivos de cliente (C): Un dispositivo que está dentro de la red del cliente y no está conectado directamente a la red del proveedor de servicios. Dispositivos de C no son conscientes de la VPN.

CE (Customer Edge): Dispositivo borde de cliente Edge: Un dispositivo en el borde de la red del cliente que proporciona acceso a la PPVPN. Puede ser provisto y gestionado por el cliente o provisto y gestionado por el proveedor dela red, siendo de responsabilidad del proveedor o del cliente según el caso. Se conecta al PE a través del Attachment Circuit (AC). En el caso de VPLS, se asume que la interface entre PE y CE es Ethernet. En el caso de VPWS la interface puede ser FR, ATM, PPP, HDLC ó Ethernet.

PE (Provider Edge): Dispositivo de borde de proveedor: Un PE es un dispositivo o conjunto de dispositivos, en el borde de la red de los proveedores al que se conecta las redes de los clientes a través de dispositivos de CE. La unión del PE y el CE se realiza a través del AC y es el punto de entrada del cliente a la VPN. Los PEs son los elementos claves de las VPNs pues los túneles entre los distintos PE son los que conforman las VPNs. Es también el dispositivo donde residen las funciones las funciones necesarias para las decisiones de forwarding y switching (que siempre se realizan al ingreso de la red L2VPN)

Attachment Circuit (AC): Es el circuito físico que une un CE a un PE. Un AC puede ser, por ejemplo, un DLCI de Frame Relay, un VPI / VCI de ATM, un puerto Ethernet, una VLAN, o un LSP MPLS. Uno o varios ACs pueden pertenecer a la misma VFI.

P (Provider): Es un dispositivo de proveedor que opera dentro de la red del proveedor y no interactúa directamente con el punto final de cliente. Proporcionan enrutamiento de los túneles en la PPVPNs.

Pseudowire (PW): (PWE3) es un mecanismo que emula el funcionamiento de interconexión de un servicio (por ejemplo un circuito TDM, Frame relay o ATM) sobre una red de paquetes.

Hasta ahora hemos mencionado los componentes que tiene una L2 VPN, ahora nos concentraremos en los components propios de una VPLS.

Virtual Bridge instance: Reside dentro de un PE (puede tener distintos nombres según el proveedor), Un Virtual Bridge Instance pertenece a una sola VPLS El VB realiza las funciones standard de bridging de un Lanswitch. Al igual que un Lanswitch, se encarga del forwarding basaado en la MAC addresses y VLAN tags.

VPLS Service ID (VPLS SID): Es un término que utilizamos para identificar el conjunto de todos los VB que conformarían el VPLS para un cliente y que se ve como un súper bridge (a nivel de toda la red). Soporta el Multipoint briging entre todos los ACs y VCs. Es un dominio de broadcast como en todo switch está separado de los otros dominios de broadcast de las otras VPLS SID, Cada VPLS SID se comporta en el súper bridge como una VLAN se comporta en un Lanswitch.

12. El Pseudo Wire (PW)

Pseudowire (PW) es un mecanismo para emular varios servicios de redes o de telecomunicaciones a través de redes de conmutación de paquetes que utilizan Ethernet, IP, o MPLS. Los servicios emulados pueden incluir servicios como Frame Relay, Ethernet, ATM, TDM o SDH. Tal como se define en el RFC 3985, un Pseudowire ofrece el mínimo de

funcionalidad necesaria para emular una conexión física punto a punto con la calidad requerida por las características de cada servicio que emula.

Un PW consiste en un circuito emulado Punto a Punto, para lograr esto, se requieren un par de LSP (MPLS) en direcciones opuestas. Dentro de cada LSP se ubican VC identificados por una etiqueta del PW (PW label). La etiqueta del PW se mantiene extremo a extremo dentro de la red MPLS entre los dos PE.

Para la conexión de los PE se pueden usar targeted LDP (para el caso que usemos señalización LDP).

Pseudowire Emulation Edge to Edge (PWE3), específica la forma en que se encapsula, transporta, controla y gestionan los servicios emulados sobre los PW.

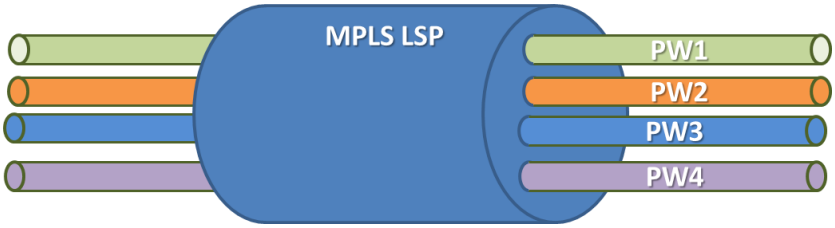


Fig. 4. Pseudo Wire

13. Virtual Private LAN service (VPLS)

VPLS es un PPVPN de Capa 2 (L2VPN), que emula una LAN tradicional. VPLS permite que los segmentos remotos de LAN de un cliente se vean como una sola LAN, con una cobertura interurbana.

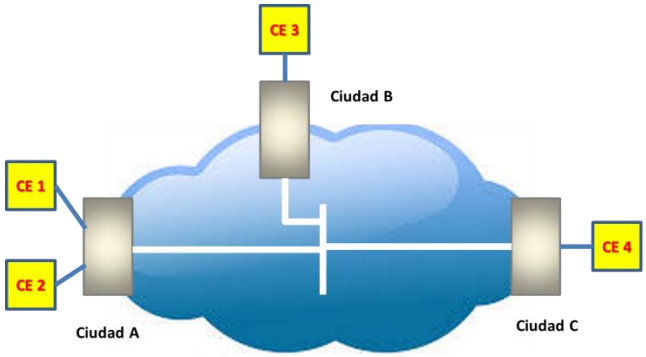


Fig. 5. Modelo 1 VPLS

En el siguiente caso el proveedor de red emula un gran Self Learnig Bridge (que podría ser visto como un Súper Bridge), que aprende las MAC origen, conmuta en función de la MAC destino y deja pasar las tramas broadcast / multicast / unknown.

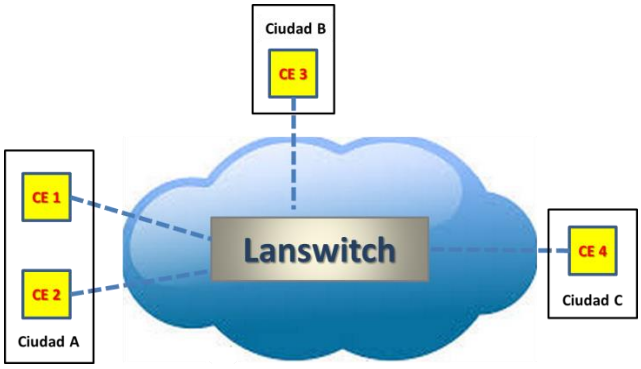


Fig. 6. Modelo 2 VPLS

Las VPLS también son conocidas como TLS (Transparent LAN Service) y como ELAN service.

VPLS se basa en VLLs tradicionales. Soporta comunicaciones multipunto a multipunto.

La inteligencia del servicio reside en los equipos PE, la red MPLS desconoce el contenido de los túneles que transporta y por lo tanto, para ella son túneles como los de cualquier otro cliente.

14. Arquitectura de la red VPLS

En una configuración simple todos los sitios de cliente que se conectan a los PEs de la red pertenecen a una sola instancia VPLS.

Los equipos de un cliente se conectan a uno de los Virtual Bridges (VB) que cada PE tiene creados para él, y todos los VB creados para un cliente se conectan Full Mesh entre sí a través de Pseudo Wires.

Los PE tendrán configurados tantos VB como clientes distintos tenga conectados.

Los clientes se conectan a una VB a partir de una interface o una VLAN (en caso de existir).

Es importante resaltar que existirán tantas redes de VBs independientes como servicios VPLS tenga implementados el proveedor. Por otro lado los PEs solo tendrán VB de un VPLS en los Pes que tenga a este cliente conectado.

El siguiente esquema nos permite visualizar lo explicado.

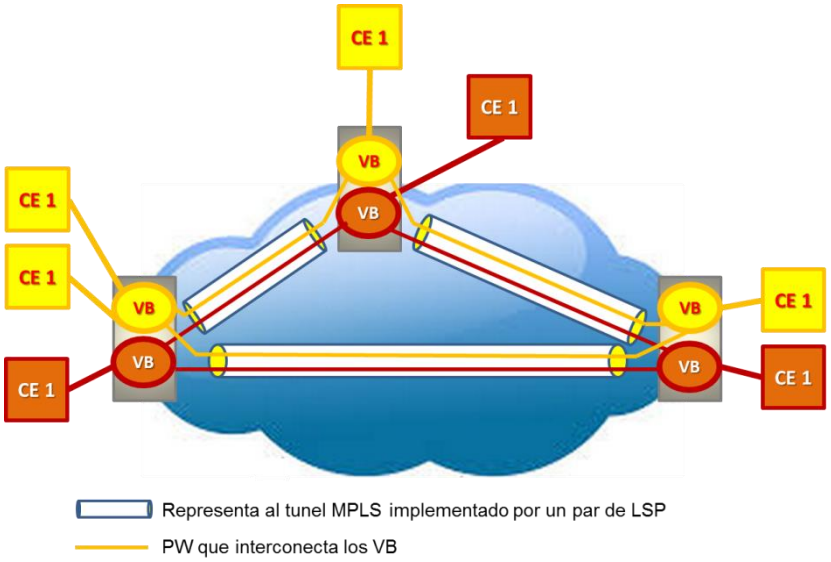


Fig. 7. Modelo 3 VPLS

15. Forma de operación de VPLS

Como dijimos los equipos a los que se conectan los clientes se son los PE, y en una red VPLS los PE deben estar interconectados Full Mesh.

Esta conexión se realiza a través de PWs, que utilizan un par de LSPs (recordar que los LSP en MPLS son unidireccionales, y los PWs son full dúplex).

Los Virtual Bridges de cada VPLS service se interconectan con con PW solo asignados a ese servicio, en la Fig, 6 se ve que los VB amarillos se interconectan con los PW amarillos, y los VB rojos se interconectan con los PW rojos (se han utilizado colores para una mejor visualización).

15.1. Aprendizaje de las MAC y fordwarding

Cuando un VB de una VPLS recibe una trama del CE de un cliente, al igual que un Self Learning Bridge (no olvidemos que lo está emulando) aprende la MAC origen del CE, lo almacena en la tabla de MAC del VB del VPLS del cliente (anotando en que puerta esa MAC se encuentra ubicada)

Luego analiza la MAC destino y pueden ocurrir dos cosas. La primera es que la MAC destino no se encuentre en la tabla de MAC del VB o que sea una dirección de broadcast, en este caso la trama recibida se envía a todos los VB asociados (a través de la malla de PW) que residen en los PE remotos. La segunda es que encuentre la MAC destino en el VB, en este caso sólo envía la trama al VB destino a través del PW que lo asocia.

Cuando los VB de este servicio VPLS ubicados en los PE remotos reciban las tramas, lo primero que harán es anotar en su tabla MAC, la MAC origen (SA) de la trama (anotando como ubicación de la misma el PW por el que le llegó).

Respecto de la dirección destino en caso que sea una MAC unicast la entrega a la puerta correspondiente, y en caso que sea un broadcast se lo envía a todas las puertas de cliente que ese VB tenga.

Es importante mencionar que siempre que llegue una MAC destino unicast, la misma existirá en el VB destino, pues el hecho que llegue unicast implica que la MAC fue encontrada en el VB origen y por lo tanto aprendida por señalización (LDP o BGP).

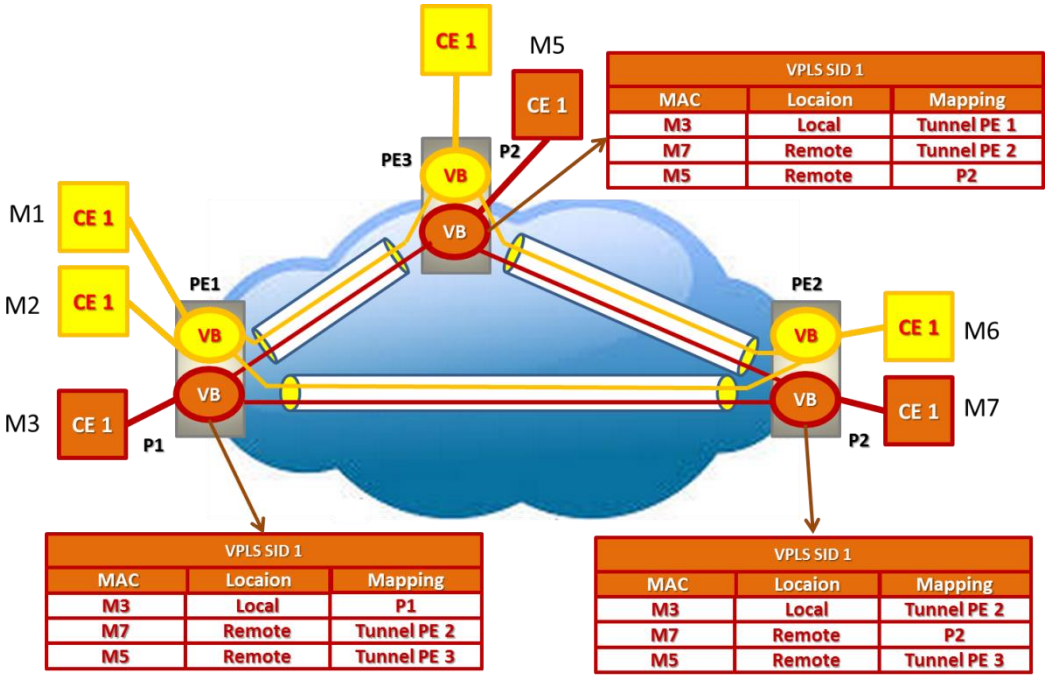


Fig. 8. Aprendizaje en VPLS

15.2. Los bucles en VPLS

Para evitar bucle o loops, los VB implementan Split Horizon. No existe la posibilidad de la existencia de loops dentro de la red pues todos los VB están conectados full mesh.

El problema de los loops en las redes de LAN Switches es abordado por las normas STP, RST y MSP protocol.

Sin embargo puede ocurrir que el cliente (dado su topología externa a la red, requiera del uso de mecanismos para evitar loops (tal sería el caso de redes de clientes que se conectan a dos PE, pero que también tienen uniones externas entre sí).

Por ello VPLS tiene dos formas dee funcionamiento a este respecto, que son:

VPLS Transparen Mode, que transporta los BPDUs generados por el cliente en forma transparente (solo le agrega las etiquetas de PW y VP para su transporte), hacinédoselo llegar a todos los AC (excepto por el que lo recibió) en donde haya Pes de este servicio VPLS.

VPLS Participation Mode, los VB también generan BPDUs dentro del core, el Bridge ID que se utiliza utiliza es la prioridad que le otorguemos al VB más MAC address que cada hardware PE tiene asignada de fábrica. El Port ID será el Virtual Channel port.

16. Virtual Pseudo Wire Service (VPWS)

En el caso de VPWS, el proveedor emula un circuito entre dos puntos de clientes, lo hace a través de un Pseudowire que atraviesa su red.

Esta tecnología ha sido desarrollada como una alternativa de mercado para los servicios de FR y ATM debido a que se presenta servicios similares. También es utilizada para inter-operar con estas tecnologías legacy. De esta forma el proveedor logra importantes ahorros dado que no requiere de redes específicas para cada servicio. También permite el transporte de los protocolos FR, ATM, HDLC y PPP, lo cual se muestra en la siguiente figura.

Fig. 9. Modelo de transporte en VPWS

17. Señalización y autodescubrimiento en L2 MPLS VPN

En las redes L2VPN, se deben atender dos problemas a saber:

Auto-Discovery: Consiste en lograr que los múltiples VB residentes en los PEs que pertenecen a las distintas VPLS, se encuentren entre ellos.

Señalización: Es la forma en que se establecen los túneles y que se distribuyen las etiquetas entre los PEs.

En L2 MPLS VPN, se pueden utilizar dos protocolos, ambas utilizan una cabecera MPLS estándar para encapsular datos.

Los protocolos que se utilizan, que pueden ser:

Basado en BGP: Que realiza ambas funciones, Auto-Discovery y Señalización.

Basados en LDP: Que solo realiza la función de Señalización.

En la siguiente tabla vemos las RFCs que tratan el tema:

VPLS Implementation Model	Discovery	Signaling
RFC 4761 (BGP-based VPLS)	BGP	BGP
RFC 4762 (LDP-based VPLS)	None	LDP

Fig. 10. RFCs VPLS

18. Señalización en L2 MPLS VPN basada en BGP

Se basa en un borrador de la especificación escrito por Kireeti Kompella, de Juniper Networks.

Utiliza el Border Gateway Protocol (BGP) como el mecanismo para routers PE para comunicarse entre sí acerca de sus conexiones con los clientes.

Cada router se conecta a una nube central, usando BGP. Esto significa que cuando se agregan (por lo general a los nuevos routers) nuevos clientes, los routers existentes se comunicarán entre sí, a través de BGP, y añadirán automáticamente los nuevos clientes con el servicio.

19. Señalización en L2 MPLS VPN basada en LDP

El segundo tipo se basa en un borrador de la especificación de Luca Martini de Cisco Systems. Este método también se conoce como un circuito de capa 2.

Utiliza el protocolo de distribución de etiquetas (LDP) para el establecimiento de la comunicación entre routers PE. En este caso, todos los routers de habla LDP, intercambiarán FECs y establecerán LSP con cualquier otro enrutador de habla LDP en la red (o el otro router PE, en el caso de que LDP sea tunelizado en RSVP-TE), que difiere de la metodología basada en BGP.

El estilo basado en LDP de L2 VPN define nuevos TLV y parámetros para la LDP para ayudar en la señalización de las VPNs.

20. Ejemplo de caso real

Uno de los más desafiantes proyectos en redes de datos, de la actualidad nacional es proveer de una solución eficiente para el acceso a los nodos de radio de telefonía celular.

La adopción de los sistemas de tercera generación (3G) de telefonía móvil incluyen las operaciones de oferta de datos. La proporción de volumen de tráfico de datos y de voz cambia completamente respecto al escenario de la generación anterior (2G).

En especial para la red de acceso, denominado Backhaul, donde se cursa todo tráfico de datos y de voz desde los nodos de radio (BTS/NODO B) hasta sus controladores (BSC/RNC).

El Backhaul hasta hace muy poco tiempo estaba basado solo en PDH/SDH lo cual es un escenario pensado únicamente para el tráfico de voz pero no lo es para tráfico de datos, en estas condiciones el Backhaul se puede volver en el cuello de botella para el crecimiento de oferta de BAM (Banda Ancha Móvil), necesitando altas inversiones en estructuras TDM no evolutivas y de mayores costes. Es por ello que se está realizando la transformación del Backhaul hacia una estructura Ethernet que soporte cursar tanto el tráfico de voz como el de datos, manteniendo los requerimientos de disponibilidad y seguridad en la entrega de estos tráficos característicos de operaciones móviles.

Esta evolución del Backhaul basada en una red de paquetes se alinea con la estrategia de evolución de red móvil hacia una estructura "all-over IP" (3GPP) desde la tercera generación.

Las operadoras están aprovechando la capilaridad de su red Metroethernet existente y buscan generar una solución más eficiente usando MPLS.

El modelo de Red del punto de vista lógico se basa en la utilización de PWE3 sobre MPLS (caso particular de VPN MPLS Capa 2) para el transporte del tráfico móvil a través de una red de paquetes.

La figura siguiente ilustra el modelo de red planificado, desde el punto de vista lógico, para los casos donde haya red Metro Ethernet y el acceso esté basado en puertos Ethernet:

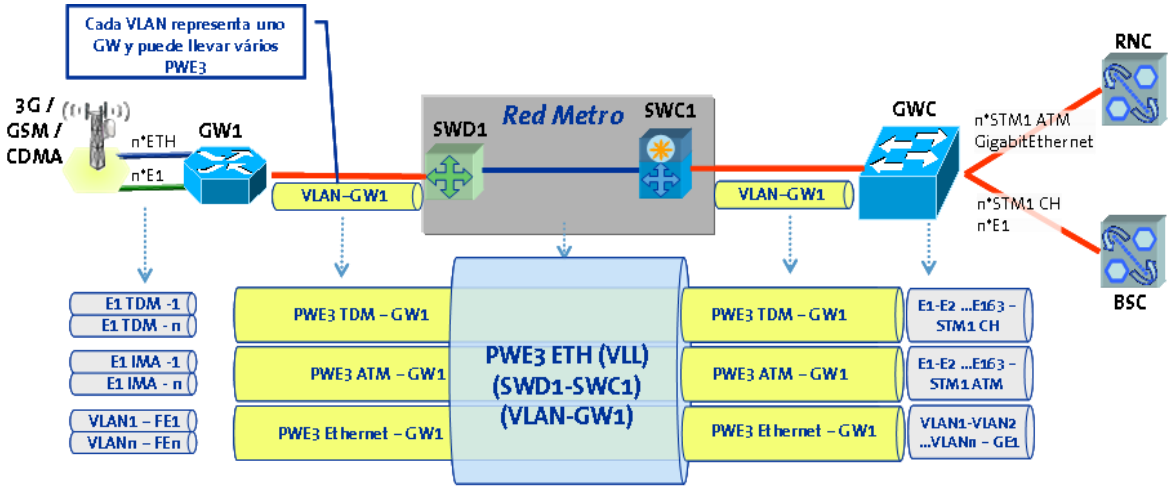


Fig. 11. Modelo de red

Conforme podemos observar en la figura, que los PWE3 son establecidos entre el GW de acceso (GWT o GWD) y el GWC sobre MPLS a través del uso de LDP. Los gateways son capaces de establecer PWE3 TDM (CESoPSN), PWE3 ATM y PWE3 ETH, los 3 tipos de tráficos actualmente encontrados en una red móvil.

Los GWT establecen los PWE3 correspondientes al tipo de tráfico recibido y una VLAN transporta el tráfico hasta el GWD donde es establecida una VLL que lo transporta hasta el GWC donde la VLL y los PWE3 son desmontados y el tráfico es entregado a las controladoras (BSC /RNC). La adopción de tal modelo (con desarrollo de VLLs entre los GWD y GWC) ya contempla un posible desarrollo de otros servicios, por eso son adoptadas las VLL para separación del tráfico de otros servicios.

En la implementación real, las exigencias de un rápido despliegue del Backhaul con costos bajos hicieron que muchas operadoras se volcaran a la compra de equipos chinos para GWT, GWD y GWC, dentro de los cuales, es un proveedor destacado Huawei.

A continuación se muestra el esquema general que se utiliza actualmente en el AMBA (Área Múltiple Buenos Aires) por una importante operadora y los principios de funcionamiento:

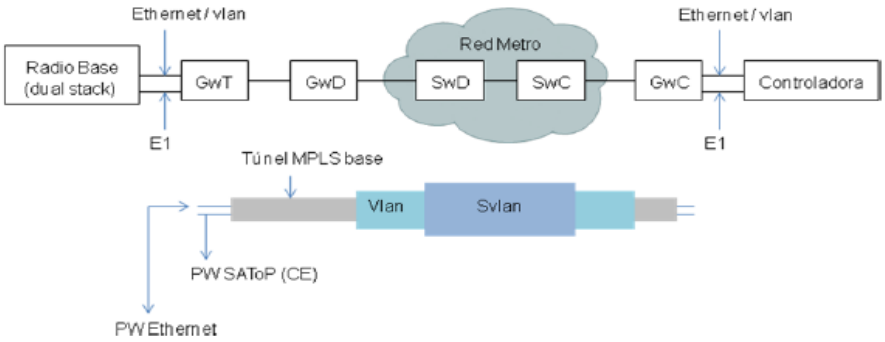


Fig. 12. Esquema general

Entre el GwT (modelo PTN 910, de Huawei) y el GwC (NE 40E de Huawei) se levanta un túnel (estático) base MPLS.

El túnel MPLS que se levanta entre los extremos es un túnel estático, es decir no se utiliza ningún protocolo de distribución de etiquetas (LDP) ya que estas se configuran a mano en los extremos. La falta de manejo de LDP se debe a una limitación técnica de los GwT estas limitaciones son propias de soluciones de compromiso para bajas costos.

En el túnel se transportan los PWs, un PW Ethernet y un PW SAToP (Structure-Agnostic TDM over Packet) producto de la emulación de circuitos realizada para transportar la trama E1 a través de la red Metro (se levanta un PW SAToP por cada E1).

En el GwD (PTN 950/ NE 40E X3, ambos de Huawei) el túnel se encapsula en una VLAN. En el SwD, en la red Metro, se agrega un segundo tag (sVLAN), con el que se transporta el tráfico hasta el SwC, equipo donde se retira dicho sVLAN.

En el GwC, se retira la VLAN, se termina el túnel base y los PWs son convertidos en las respectivas tramas Ethernet y E1 que luego son entregadas a la frontera con la red móvil.

Los proveedores ya están ofreciendo equipos económicos con capacidad de armar túneles de manera dinámica con la utilización de LDP, con estos equipos se espera mejorar la confiabilidad de la red de Backhaul.

21. Conclusiones

Las redes L2 MPLS VPN es la tecnología que están ofreciendo en la actualidad los Carriers de todo el mundo en la actualidad para servicios internos y redes corporativas. El motivo es que es el reemplazo natural de los servicios legados provisto a través de la infraestructura MPLS, también permite el transporte de estos servicios y la interconexión con estas redes residuales.

Adicionalmente con el servicio VPLS pueden ofrecer servicio de conmutación de nivel 2 a múltiples clientes y a nivel nacional como si fuese un Lanswitch de alcance nacional, donde cada servicio VPLS se comporta como una VLAN, separando entornos de broadcast. En este escenario la red del proveedor se independiza de la numeración IP del cliente dado que conmuta a nivel 2.

22. Futuras líneas de investigación

La solución adecuada para cada problemática es dependiente de la dimensión de la red que hay que diseñar como así también de las prestaciones que pretendemos de ella. Por ello y dada la gran variedad de combinaciones tecnológicas posibles para dar solución en particular y la cantidad de casos existentes en el mercado, hemos puesto nuestro foco en las necesidades y dimensiones del mercado Argentino.

Con esta información desarrollaremos una futura línea de investigación en la que nos focalizaremos en la determinación de las mejores prácticas y prospectivas para los próximos 3 años en el mercado Argentino.

23. Referencias

https://datatracker.ietf.org/wg/l2vpn/charter/l2vpn-charter.html
https://datatracker.ietf.org/wg/pwe3/charter/

Sam Halabi (2003). *Metro Ethernet*. Cisco Press. Indianapolis.ISBN: 1-58705-096-X.

J. Guichard and I. Pepelnjak (2000). *MPLS and VPN Architectures*, Cisco Press. Indianapolis. ISBN: 1-58705-002-1.

Bruce S. Davie, Paul Doolan,Yakov Rekhter (May 1998). *Switching in IP Networks: IP Switching, Tag Switching, and Related Technologies*. ISBN-13: 978-1558605053 ISBN-10: 1558605053. First edition

Wei Luo, Carlos Pignataro,Dmitry Bokotey,Anthony Chan (February 2005) *Layer 2 VPN Architectures*. Cisco Press. Indianapolis. ISBN: 1-58705-168-0.

Bruce S. and Davie, Yakov Rekhter (June 2, 2000) *MPLS: Technology and Applications*. ISBN-13: 978-1558606562. ISBN-10: 1558606564. First Edition.

24. Definiciones

E-LAN - Servicio E-LAN definido por MEF utilizado para crear VPN L2 multipunto y un servicio de LAN transparente; constituye los cimientos de las redes IPTV y de multidifusión.

E-Line - Servicio E-Line definido por MEF utilizado para crear líneas privadas Ethernet, líneas privadas virtuales y acceso Ethernet a Internet.

E-Tree - Servicios de árbol privado Ethernet (EP-Tree) definido por MEF y árbol privado virtual Ethernet (EVP-Tree). Proporcionan la separación del tráfico entre usuarios,

permitiendo que el tráfico de una “hoja” llegue a una de varias “raíces”, pero que nunca se transmita a otras “hojas”.

EVC - Circuito virtual Ethernet definido por MEF.

Certificado de referencia


Cuarto Congreso Argentino de la Interacción-Persona Computadora, Telecomunicaciones, Informática e Información Científica (IPCTIIC)

Fourth Argentine Conference on Human-Computer Interaction, Telecommunications, Informatics and Scientific Information (HCITISI)

Certificate

PAPER PRESENTACION

IPCTIIC 2015 :: HCITISI 2015
Huerta Grande – Córdoba, Argentina
November 16 – 17, 2015

Virtual Private Networks

Fernando Javier Dufour
DNI 27.178.618

Universidad Nacional de La Matanza
Buenos Aires, Argentina

ALAIPO & AInCI

[i] Entrevista con Diario TI en septiembre de 2013, Kevin Vachon, Director General de Operaciones del MEF (http://webcache.googleusercontent.com/search?q=cache:wM-ALHBVR9kJ:diarioti.com/los-servicios-los-equipos-de-red-y-los-programas-de-certificacion-profesional-del-mef-ganan-popularidad-en-todo-el-mundo/76153+&cd=1&hl=es-419&ct=clnk&gl=ar&client=firefox-a)

Anexo V: Protocolo de presentación del proyecto.

DATOS DEL DIRECTOR/A DEL PROYECTO

A.1. Apellido y Nombres:
Roca José Luis

A.2. Datos personales:
Tipo y número de Documento de Identidad: 7961016
Domicilio: Esteban Bonorino 837, CABA
Localidad: Capital Federal
Código Postal: 1406
Provincia: Buenos Aires
Teléfonos: 4634-1600
Correo electrónico: jlroca@conae.gov.ar

A.3.Datos Curriculares
Título/s de grado: Ingeniero Electrónico FIUBA
Título/s de postgrado: Doctor en Ingeniería FIUBA
A.4. Antigüedad en la U.N.L.a.M.: 18 años
A.5. Cargo docente en la U.N.L.a.M.: Profesor Asociado con función de Titular
A.6. Dedicación docente en la U.N.L.a.M.: Tiempo Parcial
A.7. Número de Legajo en la U.N.L.a.M.: 1794
A.8. Código de las asignatura/s en la/s que se desempeña: 794
A.9. Unidades Académicas en las que se desempeña en la U.N.L.a.M.: Departamento de Ingeniería e Investigaciones Tecnológicas
A.10. Antecedentes científicos del Director: Periodo 2009 -2013

Investigación 1:

Institución en la que se realizó la investigación. UNLaM

Responsabilidad asumida: Codirector

Título del Proyecto: DESARROLLO DE MODELOS DE FALLAS DE SISTEMAS ELECTRONICOS UTILIZANDO REDES BAYESIANAS

Código: C100 (años: 2009-2010)

Breve síntesis del Proyecto:

La construcción de modelos físico-matemáticos para la caracterización de fallas en productos electrónicos y su simulación son herramientas importantes en el diseño del mismo desde sus fases iniciales, en las cuales se contempla el mapeo de los requerimientos del mercado o clientes en las especificaciones del producto a través de la función de despliegue de la calidad QFD (Quality Function Deployment). Actualmente, la práctica corriente es utilizar aproximaciones basadas en ecuaciones representativas del comportamiento, respecto a las fallas, de la electrónica asociada al producto, ya sea hardware como software. Los modelos basados en este tipo de enfoque pueden requerir demasiados recursos en tiempo y dinero para la construcción de modelos que representen fidedignamente el comportamiento del producto respecto a las fallas en el ambiente real. El objetivo fundamental de este trabajo de investigación fue explorar otras metodologías de generación de modelos de modo de simular exactamente el comportamiento del producto respecto a las fallas en su ambiente de trabajo rápidamente y a un costo inferior.

El propósito del trabajo de investigación fue la utilización de las BBN (Belief Bayesian Nets) como herramienta de modelización de fallas tanto de hardware como de software de un producto electrónico.

Investigación 2:

Institución en la que se realizó la investigación. UNLaM

Responsabilidad asumida: Director

Título del Proyecto: Certificación de la Confiabilidad de Sistemas que utilizan COTS mediante BBN

Código de Identificación: C122 (años 2011-2012)

Breve síntesis del Proyecto

Estudio y análisis de las diversas técnicas utilizadas para el análisis de la confiabilidad de sistemas basados en componentes de software comerciales denominados comúnmente COTS (Commercial- off-the-shelf). Modelizar el sistema vía una red de probabilidad Bayesiana (BBN) utilizando el conocimiento a priori de los componentes intervinientes juntamente con los registros históricos del comportamiento de dichos componentes del lado proveedor. Luego mediante la utilización de los datos recolectados durante el proceso de

certificación realizar la actualización correspondiente de la BBN propuesta como modelo. Finalmente es posible obtener la confiabilidad del sistema bajo análisis.

Investigación 3:

-Institución en la que se realizó la investigación: Universidad Nacional de La Matanza

-Responsabilidad asumida: Director.

-Título del Proyecto: Determinación de las mejores prácticas para la implementación de la arquitectura de redes y servicios convergentes.

-Código de Identificación: PROINCE C127 (años 2012-2013)

-Breve síntesis del Proyecto: El IMS es un paraguas que apunta a integrar todas las tecnologías de información y comunicaciones, para que se puedan implementar servicios que hagan uso pleno e integrado de los servicios de comunicaciones.

Para entender la magnitud de la problemática, debemos hacer una descripción de las tecnologías de comunicación existentes, teniendo en cuenta que, a pesar de que unas son más modernas que otras, todas ellas forman parte de la planta existente y en funcionamiento en la actualidad. Analizamos las tecnologías de comunicaciones actualmente instaladas que formarán parte del proceso de integración de servicios multimedia, hemos tenido acceso a la percepción de profesionales especialistas en comunicaciones e involucrados en la tecnología IMS (IP Multimedia Subsystem) sobre distintos aspectos de misma. Analizamos distintos aspectos de los proveedores de las tecnologías y su situación actual en el mercado, investigando la arquitectura e Interfaces entre Módulos y Protocolos que interactúan. Estudiamos un caso real en Argentina.

DATOS DE LOS INTEGRANTES

Nómina de los integrantes del equipo:

B. Biga Daniel Rodolfo. Codirector
C. Dufour Fernando Javier
D. Serra Ariel Miguel
E. Carlos Peliza
F. Micieli Gustavo Ariel

B.1. Apellido y Nombres:
Biga Daniel Rodolfo (codirector)

B.2. Datos personales:
Tipo y número de Documento de Identidad: DNI 10.939.452
Domicilio: Pje. El hornero 665
Localidad: Capital Federal

Código Postal: 1408
Provincia: Buenos Aires
Teléfonos: 4642 - 9969
Correo electrónico: dbiga@ing.unlam.edu.ar

B.3.Datos Curriculares
Título/s de grado: Ingeniero en Electrónica
Título/s de postgrado: Postgrado ENTel 1981
B.4. Antigüedad en la U.N.L.a.M.: 16 años
B.5. Cargo docente en la U.N.L.a.M.: Profesor Asociado Ordinario
B.6. Dedicación docente en la U.N.L.a.M.: Exclusiva
B.7. Número de Legajo en la U.N.L.a.M.: 1840
B.8. Código de las asignatura/s en la/s que se desempeña: 0377 y 0644
B.9. Unidades Académicas en las que se desempeña en la U.N.L.a.M.: Ingeniería Electrónica e Ingeniería en Sistemas.
B.10. Antecedentes científicos del Integrante:

Investigación 1:

-Institución en la que se realizó la investigación: UNLaM

-Responsabilidad asumida: Integrante.

-Título del Proyecto: "Contribución a un ejercicio Nacional de Prospectiva Tecnológica, Tecnologías de la información".

-Código de Identificación: Código Incentivos C046 (años: 2002-2004)

-Breve síntesis del Proyecto: El proyecto consistió en el estudio del estado del arte de las tecnologías de transporte de datos y video. Realizándose una prospectiva de la evolución de dichas tecnologías.

Investigación 2:

-Institución en la que se realizó la investigación: UNLaM

-Responsabilidad asumida: Codirector.

-Título del Proyecto: Estudio del estado del arte en transporte de servicios de voz y videos sobre IP y detección de nichos de desarrollo.

-Código de Identificación: Código Incentivos C081 (años: 2007-2009)

-Breve síntesis del Proyecto: El proyecto consistió en el estudio del estado del arte de las tecnologías de transporte de voz y videos sobre IP, el nicho de desarrollo sobre el que se trabajó fue el transporte de servicios en redes para achicamiento de la brecha digital para comunidades. Sobre este tema se produjo un informe sobre las mejores prácticas para la implementación en este tipo de redes.

Investigación 3:

-Institución en la que se realizó la investigación: Universidad Nacional de La Matanza

-Responsabilidad asumida: Codirector.

-Título del Proyecto: Optimizaciones de Soluciones de Calidad de Servicio en Escenarios Multiprotocolo.

-Código de Identificación: ING002/2009 (años: 2009 a 2011)

-Breve síntesis del Proyecto: Se trató de una Proyecto en el cual se realizó el estudio de los diferentes esquemas y protocolos utilizados en escenarios de Calidad de Servicio, se analizaron casos reales de implementaciones en Carriers, se estudiaron los diferentes indicadores utilizados en mediciones de Calidad de Servicio y se realizó un estudio de Investigación de Mercado sobre las diferentes tecnologías utilizadas para la medición (sondas).

Investigación 4:

-Institución en la que se realizó la investigación: Universidad Nacional de La Matanza

-Responsabilidad asumida: Codirector.

-Título del Proyecto: Determinación de las mejores prácticas para la implementación de la arquitectura de redes y servicios convergentes.

-Código de Identificación: PROINCE C127 (años: 2012-2013)

-Breve síntesis del Proyecto: El IMS es un paraguas que apunta a integrar todas las tecnologías de información y comunicaciones, para que se puedan implementar servicios que hagan uso pleno e integrado de los servicios de comunicaciones.

Para entender la magnitud de la problemática, debemos hacer una descripción de las tecnologías de comunicación existentes, teniendo en cuenta que, a pesar de que unas son más modernas que otras, todas ellas forman parte de la planta existente y en funcionamiento en la actualidad. Analizamos las tecnologías de comunicaciones actualmente instaladas que formarán parte del proceso de integración de servicios multimedia, hemos tenido acceso a la percepción de profesionales especialistas en comunicaciones e involucrados en la tecnología IMS (IP Multimedia Subsystem) sobre distintos aspectos de la misma. Analizamos distintos aspectos de los proveedores de las tecnologías y su situación actual en el mercado, investigando la arquitectura e Interfaces entre Módulos y Protocolos que interactúan. Estudiamos un caso real en Argentina.

C.1. Apellido y Nombre:
Dufour Fernando Javier

C.2. Datos personales:
Tipo y número de Documento de Identidad: 27.178.618
Domicilio: República de Chile 356 – Departamento 2
Localidad: Villa Luzuriaga
Código Postal: 1754
Provincia: Buenos Aires
Teléfonos: 4650 - 9203 / 15-6530-3998
Correo electrónico: fdufourf@hotmail.com

C.3. Datos Curriculares
Título/s de grado: Ingeniero Electrónico
Título/s de postgrado: Diplomatura en Telecomunicaciones Multimedia.
C.4. Antigüedad en la U.N.L.a.M.: 4 años y 4 meses

C.5. Cargo docente en la U.N.L.a.M: Ayudante de primera
C.6. Dedicación docente en la U.N.L.a.M: Parcial
C.7. Número de Legajo en la U.N.L.a.M.: 2329
C.8. Código de las asignatura/s en la/s que se desempeña: 377
C.9. Unidades Académicas en las que se desempeña en la U.N.L.a.M.: Departamento de Ingeniería e Investigaciones Tecnológicas
C.10. Antecedentes científicos del Integrante:

Investigación 1:

-Institución en la que se realizó la investigación: Universidad Nacional de La Matanza

-Responsabilidad asumida: Investigador.

-Título del Proyecto: Optimizaciones de Soluciones de Calidad de Servicio en Escenarios Multiprotocolo.

-Código de Identificación: ING002/2009 (años: 2009 a 2011)

-Breve síntesis del Proyecto: Se trató de una Proyecto en el cual se realizó un estudio de los diferentes esquemas y protocolos utilizados en escenarios de Calidad de Servicio, se analizaron casos reales de implementaciones en Carriers, se realizó un estudio de los diferentes indicadores utilizados en mediciones de Calidad de Servicio y se realizó un estudio de Investigación de Mercado sobre las diferentes tecnologías utilizadas para la medición (sondas).

Investigación 2:

-Institución en la que se realizó la investigación: Universidad Nacional de La Matanza

-Responsabilidad asumida: Investigador.

-Título del Proyecto: Determinación de las mejores prácticas para la implementación de la arquitectura de redes y servicios convergentes.

-Código de Identificación: PROINCE C127 (años 2012-2013)

-Breve síntesis del Proyecto: El IMS es un paraguas que apunta a integrar todas las tecnologías de información y comunicaciones, para que se puedan implementar servicios que hagan uso pleno e integrado de los servicios de comunicaciones.

Para entender la magnitud de la problemática, debemos hacer una descripción de las tecnologías de comunicación existentes, teniendo en cuenta que, a pesar de que unas son más modernas que otras, todas ellas forman parte de la planta existente y en funcionamiento en la actualidad. Analizamos las tecnologías de comunicaciones actualmente instaladas que formarán parte del proceso de integración de servicios multimedia, hemos tenido acceso a la percepción de profesionales especialistas en comunicaciones e involucrados en la tecnología IMS (IP Multimedia Subsystem) sobre distintos aspectos de la misma. Analizamos distintos aspectos de los proveedores de las

tecnologías y su situación actual en el mercado, investigando la arquitectura e Interfaces entre Módulos y Protocolos que interactúan. Estudiamos un caso real en Argentina.

D.1. Apellido y Nombre:
Serra Ariel Miguel

D.2. Datos personales:
Tipo y número de Documento de Identidad: DNI 25.574.127
Domicilio: Alvear 1430
Localidad: Ramos Mejía
Código Postal: 1704
Provincia: Buenos Aires
Teléfonos: 4658-0273 / 15-6748-6832
Correo electrónico: arielmiguel.serra@gmail.com

D.3. Datos Curriculares
Título/s de grado: Ingeniero en Electrónica
Título/s de postgrado:---
D.4. Antigüedad en la U.N.L.a.M. :6 años y 4 meses
D.5. Cargo docente en la U.N.L.a.M.: Ayudante de primera
D.6. Dedicación docente en la U.N.L.a.M.: Parcial
D.7. Número de Legajo en la U.N.L.a.M.: 2146
D.8. Código de las asignatura/s en la/s que se desempeña: 794
D.9. Unidades Académicas en las que se desempeña en la U.N.L.a.M.: Departamento de Ingeniería e Investigaciones Tecnológicas
D.10. Antecedentes científicos del Integrante:

Investigación 1:

Institución en la que se realizó la investigación. UNLaM

Responsabilidad asumida: Investigador.

Título del Proyecto: Certificación de la Confiabilidad de Sistemas que utilizan COTS mediante BBN

Código de Identificación: C122 (años 2011-2012)

Breve síntesis del Proyecto

Estudio y análisis de las diversas técnicas utilizadas para el análisis de la confiabilidad de sistemas basados en componentes de software comerciales denominados comúnmente COTS (Commercial- off-the-shelf). Modelizar el sistema vía una red de probabilidad Bayesiana (BBN) utilizando el conocimiento a priori de los componentes intervinientes juntamente con los registros históricos del comportamiento de dichos componentes del lado proveedor. Luego mediante la utilización de los datos recolectados durante el proceso de certificación realizar la actualización correspondiente de la BBN propuesta como modelo. Finalmente es posible obtener la confiabilidad del sistema bajo análisis

Investigación 2:

-Institución en la que se realizó la investigación: Universidad Nacional de La Matanza

-Responsabilidad asumida: Investigador.

-Título del Proyecto: Optimizaciones de Soluciones de Calidad de Servicio en Escenarios Multiprotocolo.

-Código de Identificación: ING002/2009 (años: 2009 a 2011)

-Breve síntesis del Proyecto:

Se trató de un Proyecto en el cual se realizó un estudio de los diferentes esquemas y protocolos utilizados en escenarios de Calidad de Servicio, se analizaron casos reales de implementaciones en Carriers, se realizó un estudio de los diferentes indicadores utilizados en mediciones de Calidad de Servicio y se realizó una Investigación de Mercado sobre las diferentes tecnologías utilizadas para la medición (sondas).

Investigación 3:

-Institución en la que se realizó la investigación: Universidad Nacional de La Matanza

-Responsabilidad asumida: Investigador.

-Título del Proyecto: Determinación de las mejores prácticas para la implementación de la arquitectura de redes y servicios convergentes.

-Código de Identificación: PROINCE C127 (años 2012-2013)

-Breve síntesis del Proyecto: El IMS es un paraguas que apunta a integrar todas las tecnologías de información y comunicaciones, para que se puedan implementar servicios que hagan uso pleno e integrado de los servicios de comunicaciones.

Para entender la magnitud de la problemática, debemos hacer una descripción de las tecnologías de comunicación existentes, teniendo en cuenta que, a pesar de que unas son más modernas que otras, todas ellas forman parte de la planta existente y en funcionamiento en la actualidad. Analizamos las tecnologías de comunicaciones actualmente instaladas que formarán parte del proceso de integración de servicios multimedia, hemos tenido acceso a la percepción de profesionales especialistas en comunicaciones e involucrados en la tecnología IMS (IP Multimedia Subsystem) sobre distintos aspectos de la misma. Analizamos distintos aspectos de los proveedores de las tecnologías y su situación actual en el mercado, investigando la arquitectura e Interfaces entre Módulos y Protocolos que interactúan. Estudiamos un caso real en Argentina.

E.1. Apellido y Nombre:
Peliza Carlos Horacio

E.2. Datos personales:
Tipo y número de Documento de Identidad: DNI 20.593.370

Domicilio: Tte Pablo Ricchieri 4451 -Fte
Localidad: Ciudadela
Código Postal: 1702
Provincia: Buenos Aires
Teléfonos: 4657 - 6324 / 15-6700-9927
Correo electrónico: pelizac@yahoo.com.ar

E.3. Datos Curriculares
Título/s de grado: Ingeniero Electrónico
Título/s de postgrado:
E.4. Antigüedad en la U.N.L.a.M.: 9 años
E.5. Cargo docente en la U.N.L.a.M.: Ayudante de primera
E.6. Dedicación docente en la U.N.L.a.M.: Parcial
E.7. Número de Legajo en la U.N.L.a.M.: 2074
E.8. Código de las asignatura/s en la/s que se desempeña: 0619/0937/1119
E.9. Unidades Académicas en las que se desempeña en la U.N.L.a.M.: Departamento de Ingeniería e Investigaciones Tecnológicas
E.10. Antecedentes científicos del Integrante:

F.1. Apellido y Nombre:
Micieli Gustavo Ariel

F.2. Datos personales:
Tipo y número de Documento de Identidad: DNI 29.250.350
Domicilio: José León Suarez 1468 - Departamento 2
Localidad: CABA
Código Postal: 1408
Provincia: Buenos Aires
Teléfonos: 2068 - 1524 / 15-6972-9798
Correo electrónico: gmicieli@gmail.com

F.3. Datos Curriculares
Título/s de grado: Ingeniero Electrónico
Título/s de postgrado:
F.4. Antigüedad en la U.N.L.a.M.: 2 años
F.5. Cargo docente en la U.N.L.a.M.: Ayudante de primera
F.6. Dedicación docente en la U.N.L.a.M.: Simple
F.7. Número de Legajo en la U.N.L.a.M.: 4313
F.8. Código de las asignatura/s en la/s que se desempeña: 377
F.9. Unidades Académicas en las que se desempeña en la U.N.L.a.M.: Departamento de Ingeniería e Investigaciones Tecnológicas
F.10. Antecedentes científicos del Integrante:

IDENTIFICACIÓN DEL PROYECTO

1. Programa de investigación: PROINCE: X CyTMA2:…
2. Código: C164
3. Título del Proyecto: “Redes de Transporte de la nueva generación de Carrier-Ethernet”
4. Apellido y Nombre del Director: Roca José Luis
5. Fechas

Fecha de Iniciación del Proyecto: 01/01/2014
Fecha de Finalización del Proyecto: 31/12/2015

6. Unidad Académica donde se presenta el protocolo: DIIT
7. Otras dependencias de la U.N.L.a.M. que intervienen en el Proyecto:Ninguna
8. Otras instituciones externas a la U.N.L.a.M. intervinientes:Ninguna

PLAN DE INVESTIGACIÓN

Resumen del Proyecto:

El mundo de las comunicaciones avanza hacia la próxima generación de redes Carrier Ethernet, basados en las necesidades de los Carriers de superar las limitaciones de las redes bridgeadas con tecnología 802.1ad.

Para la implementación de esta nueva generación de tecnologías, existe el problema adicional a resolver de la necesidad de integrar a estos servicios las redes existentes.

La responsabilidad de integrar las tecnologías existentes recaerá sobre las nuevas tecnologías y arquitecturas que se incorporarán para estos servicios.

Estos equipamientos deberán inter-operar correctamente con los equipos existentes en un idioma (protocolos, interfaces, etc.), que estos últimos comprendan.

Frente a semejante desafío, la complejidad de las interacciones que se deben desarrollar, plantea dificultades de implementación.

Lo mencionado nos permite prever que existen distintas alternativas, y soluciones posibles, que utilizarán en los distintos ámbitos de aplicación.

El objetivo principal de la investigación será determinar el grado de madurez de la nueva generación de la tecnología Metro Ethernet y los servicios que se pueden prestar basados en la compatibilidad con los estándares y las tecnologías ya desplegadas; generando una recomendación de mejores prácticas de implementación para el estado del arte actual. Existen además objetivos complementarios que se lograran en el proceso de investigación.

La metodología a utilizar será, la investigación documental, entrevistas a especialistas de distintos participantes (fabricantes, Carriers, etc.), análisis de Normas y el cumplimiento de las mismas por las principales tecnologías.

Se buscarán las incompatibilidades y a partir de un debate interno se sacarán las conclusiones respecto de las mejores prácticas que se contrastarán con pruebas hechas por los Carriers y/o pruebas piloto.

Se generará un informe final en el que entre otros aspectos se detallaran las mejores prácticas para la implementación de estas redes y servicios.

El impacto que producirá la investigación será en el entorno académico, en las empresas de comunicaciones, y en las empresas de todo tipo que tendrán una guía para determinar qué servicios tendrán disponibles mejorar sus servicios actuales de comunicaciones.

Características de la investigación:

8.1: Tipo de investigación:

Básica: No aplica.

Aplicada:

La investigación será aplicada, dado que obtendremos conocimientos respecto de esta nueva tecnología, y tendrá como objetivo practico específico principal una recomendación de las mejores prácticas para la implementación de redes Metro-Ethernet de próxima generación.

Desarrollo Experimental: No aplica.

8.2 Definición de área y disciplina de conocimiento:

Área de conocimiento: Ing. de Com. Electrónica y Control

Código de Área de conocimiento: Código Área: 18.

Disciplina de conocimiento:

Disciplina: Comunicaciones.

Código Disciplina de conocimiento:

Código Disciplina: 1803.

8.3 Definición de campo de Aplicación:

Campo de Aplicación: Ordenamiento Territorial.

Código Campo de Aplicación: Código 0651

9. Antecedentes:

PROINCE código: C127, Titulo: Determinación de las mejores prácticas para la implementación de la arquitectura de redes y servicios convergentes.

10. Objetivos:

Objetivo principal

Esclarecer el grado de madurez de la tecnología y determinar las mejores prácticas para la implementación de las redes, como así también la gama de servicios que se pueden

prestar basados en la compatibilidad con los estándares y las tecnologías ya desplegadas; generando una recomendación de mejores prácticas de implementación para el estado del arte actual.

Objetivos complementarios

- Reconocer las tecnologías que existen en el mercado disponibles en la próxima generación de Metro-Ethernet.
- Determinar cuáles de ellas y cuando utilizarán los Carriers en la Argentina y de qué modo.
- Detectar los problemas de interoperabilidad entre proveedores.
- Determinar los servicios potenciales de valor agregado que se pueden brindar con esta tecnología.
- Determinar las limitaciones y potencialidades que los potenciales servicios tendrán.

11. Hipótesis:

Frente a la variedad de tecnologías asociadas a las Metro-Ethernet de nueva generación, sus estados de desarrollo, su compatibilidad con los estándares y las características de las redes existentes, estamos observando la falta de una recomendación sobre las mejores prácticas que garanticen la prestación y las calidades de servicio que el mercado requiere y requerirá aún más en los próximos años.

12. Estado actual del conocimiento:

Las redes Metro-Ethernet son el camino para la prestación de servicios de banda ancha y para resolver el transporte de tráfico de todo tipo por parte de los grandes Carriers.

Sin embargo éstas presentan limitaciones, entre las que podemos destacar como más importante la limitación de 4096 Vlans que se pueden implementar con los C-Tags.

En base a esto se han desarrollado nuevas normas para la solución de esta problemática cuyo despliegue es bastante limitado.

A título de ejemplo en Argentina no se han desplegado estas nuevas tecnologías aún.

Toda esta problemática se ve agravada por las técnicas de mapeos de servicios, como así también la forma de explotar e implementar las distintas alternativas de asignación de calidad de servicio.

El despliegue de estas redes se encuentra en un estado de desarrollo y despliegue primario, existiendo normativas que aún no están depuradas o de depuración reciente.

13. Presentación de la problemática a investigar:

La problemática a investigar es la interacción entre las distintas tecnologías nuevas y existentes que tienen que interactuar, para la provisión de servicios. Estas tecnologías apuntan a lograr el escalamiento de las redes para lo cual existen distintas alternativas de solución.

De toda esta problemática surgirán distintas soluciones de implementación que llevarán asociadas cada una de ellas, ventajas y limitaciones, que condicionaran los servicios que se presten.

El objeto de investigación es determinar dentro del universo de soluciones posibles de arquitecturas de redes, cuáles son las mejores prácticas para su implementación que impliquen la menor cantidad de limitaciones, de acuerdo al estado del arte.

El campo específico de la investigación consiste en trabajar sobre los aspectos de interoperabilidad y capacidades de los elementos de red de distintos proveedores determinando su compatibilidad de funcionamiento frente a los estándares, concentrándonos en el comportamiento frente a los servicios de este nuevo escenario tecnológico.

El modelo teórico conceptual se estructura a partir del conocimiento de incompatibilidades históricas que presentan las tecnologías en sus estados iniciales de desarrollo con las necesidades de buen funcionamiento de los servicios.

Esto requiere un análisis de dichas incompatibilidades de acuerdo al estado del arte, con el objeto que los proveedores de tecnologías trabajen sobre las mismas y que los Carriers de comunicaciones tengan claro cuáles son las limitaciones a la hora de implementar sus servicios.

La validez de los resultados se obtendrá a través de la verificación de la compatibilidad de las tecnologías para los servicios convergentes y la búsqueda de pruebas exitosas que convaliden nuestras conclusiones. Para lo cual una vez obtenido el resultado se lo contrastará con pruebas de laboratorio o pruebas piloto en Carriers independientes que se buscarán en el mercado.

14. Metodología:

La metodología a utilizar será:

- Se hará una investigación documental del estado actual de la tecnología.
- Se realizarán entrevistas con:
    - Especialistas del mercado
    - Especialistas de los fabricantes de tecnologías
    - Especialistas de laboratorios de prueba
- Se analizarán las normas existentes asociadas a la problemática y el cumplimiento de las mismas por las distintas tecnologías.
- En base a esa investigación determinaremos cuales son las incompatibilidades y tecnologías que pueden aparecer en el mercado argentino, esto se realizará:
    - A través de entrevistas con especialistas de comunicaciones del mercado
    - A través de pruebas (protocolos de pruebas)

- Se hará un proceso de debate interno sobre las conclusiones individuales.
- Se buscarán los consensos y se determinará si hay aspectos en que las conclusiones divergen, y en tal caso trabajaremos en forma conjunta repitiendo las partes de la metodología focalizándonos sobre esos aspectos.
- Verificación de resultados obtenidos con resultados de pruebas de algún Carrier o con alguna prueba piloto exitosa.
- Se redactará un informe final con las conclusiones de la investigación.

15. Resultados esperados:

15.1. Resultados en cuanto a la producción de conocimiento:

Obtener Know How sobre el estado de arte real sobre la tecnología y sus posibilidades de implementación.

Determinar una prospectiva de este tipo de redes en los próximos 3 años.

Prever aplicaciones y servicios que aparecerán en el mercado.

Obtener información sobre las tecnologías que se utilizarán en la Argentina.

Lograr reconocer las implementaciones más convenientes (mejores prácticas) que podrán ser utilizadas por los operadores.

15.2. Resultados en cuanto a la formación de recursos humanos:

El grupo de estudiantes y profesores del Departamento de Ingeniería e Investigaciones Tecnológicas involucrados en el proyecto, resultarán directamente beneficiados con estos desarrollos en el aspecto académico y curricular.

Estos conocimientos se volcarán en el dictado de clases de las cátedras afines.

15.3. Resultados en cuanto a la difusión de resultados:

Los temas desarrollados en sus distintas profundidades podrán ser integrados en materias de grado, postgrado y tesis.

El informe final será ofrecido a la biblioteca de la UNLaM como material de consulta.

Se darán charlas en ámbitos de grado y/o postgrado en ámbitos Universitarios.

16. Transferencia de resultados:

16.1. Resultados en cuanto a transferencia hacia las actividades de docencia y extensión:

El desarrollo de Know How permitirá la provisión de servicio de asesoramiento a empresas por parte de la UNLaM.

El mercado podrá obtener información de potenciales servicios que podrán ofrecer los Carriers. Esto permitirá a las empresas que consumen servicios de comunicaciones determinar el grado de integración de sus redes y los servicios que cada empresa necesita.

El presente informe podrá servir como base para implementación de servicios en Carriers.

Institución / organismo	Resultados a transferir
Carriers de Comunicaciones.	Informe de mejores prácticas – Parte de tecnologías y Servicios. Prospectiva de despliegue de redes.
Empresas que requieran servicios.	Informe de servicios que pueden disponer.
Universidades.	Know How que aporta la investigación.

16.2. Resultados en cuanto a la transferencia de resultados a organismos externos a la U.N.L.a.M.:

Se entregará a los especialistas del mercado local un informe de la investigación para que puedan aprovecharlo en sus futuras implementaciones.

Se solicitará una evaluación del informe por parte de expertos en el tema.

17. Vinculación del proyecto con otros grupos de investigación del país y del extranjero:

La presente investigación por tener aspectos que aún están en estudio y por tratarse de tecnologías que aún no se han desplegado masivamente, requiere la interacción con expertos de empresas proveedoras de tecnologías y de servicios.

18. Bibliografía:

Metro Ethernet Forum: http://metroethernetforum.org/InformationCenter

• MPLS IETF Working Group: http://www.ietf.org/dyn/wg/charter/mpls-charter.html

• MPLS-TP IETF Working Group: http://www.ietf.org/dyn/wg/charter/mpls-charter.html

• PBB: IEEE 802.1ah – Provider Backbone Bridging http://www.ieee802.org/1/pages/802.1ah.html

• PBB-TE: IEEE 802.1Qay – Provider Backbone Bridge Traffic

Engineering: http://www.ieee802.org/1/pages/802.1ay.html

19. Programación de actividades (GANTT):

19.1. Programación de tareas del 1er Año

1 - Investigación documental. (5 meses)

1.1 Estudio pormenorizado del tema y análisis de la situación del mercado internacional en cuanto a Proveedores de Servicios y Proveedores de tecnologías.

1.2 Contacto con personal relevante del mercado para realizar entrevistas que permitan informarnos sobre el estado de la tecnología en el mercado Argentino.

1.3 Relevamiento de información de la Web respecto de la situación de las tecnologías en cuestión.

2 - Estudio de las capas de la arquitectura de las redes (5 meses).
2.1 Estudio de las capas de las redes.

2.2 Equipamientos que satisfacen las funcionalidades lógicas

2.3 Protocolos que interaccionan dentro de la arquitectura

3 - Estudio de un caso real o despliegue avanzado (2 meses)
3.1 Estudio de un caso de implementación real o despliegue avanzado.

4 – Desarrollo de un informe del primer año de investigación (1 mes)

19.2. Programación de tareas del 2do Año

5 – Interoperabilidad entre proveedores. (4 meses)
5.1 Análisis de interoperabilidad entre proveedores que tengan presencia en Argentina.

5.2 Verificación del funcionamiento de los protocolos en un escenario multi-vendedor.

6 – Investigación de los servicios Metro-Ethernet de próxima generación (3 meses).
6.1 Informe de los potenciales servicios en Metro-Ethernet de próxima generación.

6.2 Estudio y descripción de servicios potenciales Metro-Ethernet de próxima generación en los próximos 3 años en Argentina.

7 – Evidenciar las limitaciones de las redes (2 meses)
7.1 Informe sobre las limitaciones de los equipamientos Metro-Ethernet de próxima generación en la actualidad.

8 – Informe final de la investigación realizada (3 meses)

Actividades / Responsables 1er Año	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Estudio pormenorizado del tema y análisis de la situación del mercado internacional	X	X										

Contacto con personal relevante del mercado para realizar entrevistas que permitan informarnos sobre el estado de la tecnología en el mercado Argentino		X	X	X								
Relevamiento de información de la Web respecto de la situación de las tecnologías en cuestión.				X	X							
Estudio de las capas de las redes 802.1.						X	X					
Equipamientos que satisfacen las funcionalidades lógicas								X	X			
Protocolos que interaccionan dentro de la arquitectura									X	X		
Estudio de un caso de implementación real o despliegue avanzado										X	X	
Desarrollo de un informe del primer año de investigación												X
Actividades / Responsables 2do Año	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Análisis de interoperabilidad entre proveedores que tengan presencia en Argentina	X	X										
Verificación del funcionamiento de los protocolos en un escenario multi-vendedor			X	X								
Informe de los potenciales servicios en Metro-Ethernet de próxima generación					X	X						
Estudio y descripción de servicios potenciales Metro-Ethernet de próxima generación en los próximos 3 años en Argentina						X	X					
Informe sobre las limitaciones de los equipamientos Metro-Ethernet de próxima generación en la actualidad								X	X			
Informe final de la investigación realizada										X	X	X

20. Cantidad de horas destinadas a la investigación:

Apellido y Nombre del Director/a:
Roca José Luis
Nº de horas semanales: 10

Apellido y Nombre de Investigador/a:
Biga Daniel Rodolfo
Nº de horas semanales: 20

Apellido y Nombre de Investigador/a:
Dufour Fernando Javier
Nº de horas semanales: 10

Apellido y Nombre de Investigador/a:
Serra Ariel Miguel
Nº de horas semanales: 10

Apellido y Nombre de Investigador/a:
Peliza Carlos Horacio
Nº de horas semanales: 10

21. Presupuesto solicitado:

Se detallarán espacios, infraestructura y servicios disponibles en la Unidad Académicai, así como los elementos necesarios a adquirir en cuanto a equipamiento, insumos, bibliografía, y otros, requeridos para la ejecución del proyecto acompañado en cada caso con un precio testigo con identificación de fuente de procedencia de cotización de cada ítem presupuestadoi.

PRESUPUESTO DEL PROYECTO SOLICITADO AL PROGRAMA PROINCE			
	(a)	(b)	
Rubro:	**Precio testigo por unidad en ($)**	**Cantidad de unidades**	**Subtotal de rubro en ($)***
1. Insumos:			
1.1 (detallar)			
1.2 (etc.)			
2. Equipamiento:			
2.1 (detallar)			
2.2 (etc.)			
3. Servicios Técnicos Especializados:			
3.1 (detallar)			
3.2 (etc.)			
		Subtotal (3)	
4. Viáticos:[i]			
4.1 (detallar)			
4.2 (etc.)			
		Subtotal (4)	
5. Bibliografía:[i]			
5.1 Libro de Shortest Path Bridging	700	1	700
5.2 (etc.)			
		Total**	700

*Producto de los datos incluidos en columnas (a) y (b)
*Sumatoria de los valores obtenidos en (1)-(2)-(3)-(4)-(5)

22. Detalle del presupuesto por rubro:

22.1. Insumos:
1.1 Descripción (200 Palabras):
1.1Justificación (200 Palabras):
1.1 Precio testigo por unidad:
1.1 Fuente de procedencia de precio testigo:

22.2. Equipamiento:
2.1 Descripción (200 Palabras):
2.2 Justificación (200 Palabras):
2.3 Precio testigo por unidad:
2.4 Fuente de procedencia de precio testigo:

22.3. Servicios Técnicos Especializados:
3.1 Descripción (200 Palabras):
3.2 Justificación (200 Palabras):
3.3 Precio testigo por unidad:
3.4 Fuente de procedencia de precio testigo:

22.4. Viáticos:
4.1 Descripción (200 Palabras):
4.2 Justificación (200 Palabras):
4.3 Precio testigo por unidad:
4.4 Fuente de procedencia de precio testigo:

A los efectos de no hacer estimaciones erróneas, los gastos para congresos y/o publicaciones serán pagados por los miembros del grupo de investigación.

22.5. Bibliografía:
22.5.1 Descripción (200 Palabras):

Libro Networks and Services: Carrier Ethernet, PBT, MPLS-TP, and VPLS (Information and Communication Technology Series)

Datos del libro:
Fecha: Octubre de 2012
ISBN-10: 0470391197
ISBN-13: 978-0470391198
Edition: 1

22.5.2 Justificación (200 Palabras):

Solicitamos contar con un libro que describe arquitecturas Carrier Ethernet, limitaciones y evolución tecnológica, orientada a nuestro objetivo del presente protocolo.

22.5.3 Precio testigo por unidad:

El precio que estimamos entre el costo del libro y el envío a Argentina es de $ 700 (pesos), debido a que el costo está en moneda dólar estadounidense, a lo que tenemos que adicionar el transporte y el 20%.

22.5.4 Fuente de procedencia de precio testigo:

La fuente de consulta fue el sitio www.Amazon.com

http://www.amazon.com/Networks-Services-Information-Communication-Technology/dp/0470391197/ref=sr_1_7?s=books&ie=UTF8&qid=1379030526&sr=1-7&keywords=provider+backbone+bridge

23. Explicitar la factibilidad del plan de trabajo propuesto con los recursos disponibles, en caso de no recibir financiamiento[i]

La implementación del plan de trabajo se realizará a partir de normativas que se pueden obtener de la web y especificaciones técnicas de equipamientos que proveen los fabricantes. Estas se podrán complementar con algunas pruebas de laboratorio.

El plan de trabajo puede realizarse sin financiamiento debido a que las normas son de libre acceso y se pueden obtener la desde internet.

24. Pautas de presentación del Protocolo y material Anexo

24.1 La presentación del protocolo y material Anexo se realizará ante la Secretaría de Ciencia y Tecnología de la Unidad Académica en donde corresponda acreditar el proyecto de investigación, debiéndose preparar 3 ejemplares impresos de idéntico tenor conteniendo en el siguiente orden:

a) Carátula en la que conste: Unidad Académica donde se presenta el protocolo y Anexos, Nombre del Programa (PROINCE/CyTMA2), Título del Proyecto y Apellido y Nombre/s del Director, lugar y fecha de presentación.

b) Protocolo de presentación del proyecto (el presente documento).

c) Curriculum Vitaei del Director e Integrantes del equipo de investigación en el orden en el que han sido presentados en el protocolo. En el caso de alumnos que participan del proyecto, el Director en reemplazo del Curriculum Vitae, deberá incluir el formularioi de Propuesta de alumnos para integrar Equipos de Investigación acompañado del Certificado de materias aprobadas expedido por la Universidad.

d) Anexo con documentación relacionada con las fuentes de procedencia de precios testigo en el presupuesto (complementaria a lo ya informado en el protocolo)

24.2 Los ejemplares impresos se presentarán en papel tamaño A4 impreso en una sola cara (dos ejemplares anillados y uno presentado en carpeta con perforación central y tapa transparente acompañado de 2 CD incluyendo todos los archivos que conforman la presentación impresa). Presentar todos los ejemplares en un sobre dirigido al Secretario de Ciencia y Tecnología de la Unidad Académica donde se presente, identificado con la siguiente información: Unidad Académica, Nombre del Programa, Título del Proyecto y Apellido y Nombre/s del Director, lugar y fecha de presentación.

25. La información que consta en este protocolo de presentación de proyecto tiene el carácter de declaración jurada. Autorizo su verificación cuando la Universidad Nacional de La Matanza a través de sus órganos correspondientes lo considere pertinente.

.....	.....
Lugar y Fecha	Firma del Director del Proyecto
	.....
	Aclaración de firma del Director del Proyecto
	.....
	N° de DNI del Director del Proyecto