ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS Y OPTIMIZACIÓN DEL SERVICIO VIRTUAL LAN PRIVADO (VPLS), QUE OFRECE LA CNT EP A SUS CLIENTES ISPs SOBRE SU RED MPLS, Y ESTUDIO DE ESCALABILIDAD USANDO TECNOLOGÍA HVPLS

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

HIDALGO JUMBO MARIUXI GISSELLE
giselh87@hotmail.com

MONTERO REVELO EVELYN PATRICIA
evitamontero24@hotmail.com

DIRECTOR: MSc. XAVIER ALEXANDER CALDERÓN HINOJOSA
xavier.calderon@epn.edu.ec

CO-DIRECTOR: Ing. CARLOS ÁNDRES ALMEIDA ARCOS
caaamh@gmail.com

Quito, Abril 2013

DECLARACIÓN

Nosotros, Mariuxi Gisselle Hidalgo Jumbo y Evelyn Patricia Montero Revelo, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Mariuxi G. Hidalgo J. Evelyn P. Montero R.

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Mariuxi Hidalgo y Evelyn Montero, bajo nuestra supervisión.

_____	_____
MSc. Xavier Calderón DIRECTOR DEL PROYECTO	Ing. Andrés Almeida CO-DIRECTOR DEL PROYECTO

AGRADECIMIENTO

Al Ingeniero Xavier Calderón por su valiosa guía y dedicada colaboración para el desarrollo y culminación del presente proyecto de titulación.

A todo el personal del Área O&M Plataforma IP/MPLS de la Corporación Nacional de Telecomunicaciones E.P., por las facilidades brindadas en el desarrollo del presente proyecto, de manera especial al Ingeniero Andrés Almeida por su destacable orientación y predisposición.

A los docentes de la prestigiosa ESCUELA POLITÉCNICA NACIONAL quienes me impartieron todos los conocimientos necesarios para poder culminar mi carrera universitaria.

A toda mi familia y amigos por su gran apoyo y por la confianza depositada en mí, de manera especial a Diana Oña por su apoyo y amistad.

A quienes conforman New Access por todo el apoyo y comprensión que me brindaron para culminar de manera exitosa el presente proyecto.

Gisselle Hidalgo

AGRADECIMIENTO

Al MSc. Xavier Calderón por su tiempo dedicación y apoyo incondicional durante el desarrollo de este proyecto.

A todos quienes conforman el Área O&M Plataforma IP/MPLS de la Corporación Nacional de Telecomunicaciones E.P., por su apoyo, auspicio y facilidades brindadas , de manera muy especial al Ing. Andrés Almeida por su colaboración y el tiempo dedicado a orientarnos de la mejor manera y cumplir con éxito los objetivos planteados.

A quienes conforman New Access por su comprensión y permisos brindados para que culmine con éxito este proyecto.

A la Escuela Politécnica Nacional por todos los conocimientos impartidos durante todos estos años de estudio.

A toda mi familia y amigos por su apoyo y ayuda incondicional, en especial a mi hermana Eliana Montero y a mi amiga Dianita Oña

Evelyn Montero

DEDICATORIA

A mis padres, Bolívar y Mélida por su inigualable sacrificio y esfuerzo diario, por ser las personas que con su apoyo me empujan día a día a ser mejor persona, gracias por su amor y por ayudarme a culminar mis estudios.

A mis hermanos por brindarme palabras de motivación y apoyo en los momentos más difíciles, de manera especial a mi hermana Jenny que a pesar de ya no estar con nosotros es y será mi fuente de inspiración.

¡Mi familia es el complemento de mi vida, este logro es para ustedes!

Gisselle Hidalgo

DEDICATORIA

A Dios por ser mi fuerza durante todo momento, a mis padres que con su sacrificio y amor incondicional han sido el pilar de mi vida y mi inspiración.

A mis hermanos que con sus palabras de aliento, comprensión y cariño hicieron que esta meta sea más fácil de cumplir, a Esteban quien siempre confió en mí desde principio a fin, y que con su apoyo motivó cada día más mis ganas de seguir adelante.

A toda mi familia que ha estado conmigo en los buenos y malos momentos por ser ese brazo extendido durante toda esta etapa universitaria, brindándome su apoyo y actitud positiva frente a cualquier adversidad.

Evelyn Montero

ÍNDICE

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ANEXOS

RESUMEN

Se presenta una descripción del Servicio LAN Privado Virtual (VPLS) que la Corporación Nacional de Telecomunicaciones provee a 16 ISPs clientes y la VPLS interna, se realiza un análisis de los factores que degradan el funcionamiento del servicio y se plantean alternativas de solución para la optimización y escalabilidad.

En el capítulo 1, se presentará una breve descripción de la red MPLS, redes privadas virtuales de capa 2 sobre redes MPLS (VPLS y HVPLS), además una descripción de los ataques a la seguridad de capa 2.

En el capítulo 2, se describe cómo se encuentra estructurado el servicio VPLS para los 16 ISPs y la VPLS interna, se describe además su funcionamiento operacional y administración del servicio.

En el capítulo 3, se realiza un análisis y monitoreo de tráfico de los 16 ISPs y la VPLS interna, se determinan los factores que causan la degradación del servicio, y se hace un análisis de los ataques a la seguridad de las VPLS en capa 2.

En el capítulo 4, se presenta un estudio y propuesta de escalabilidad del servicio VPLS mediante la tecnología HVPLS, su factibilidad y comparativa con VPLS y se describen las soluciones establecidas para cada ISP y la VPLS interna, así como las mejores prácticas consideradas para lograr la optimización del servicio

En el capítulo 5, se establecen las conclusiones y recomendaciones del proyecto.

Como anexos, se presentan las herramientas de monitoreo utilizadas en el análisis del servicio VPLS, las configuraciones del servicio VPLS y HVPLS, las capturas obtenidas del monitoreo VPLS con las herramientas utilizadas y características técnicas de los equipos utilizados por la CNT para ofrecer el servicio VPLS.

PRESENTACIÓN

El presente Proyecto de Titulación tiene como finalidad analizar las características y funcionamiento del Servicio LAN Privado Virtual (VPLS) que la Corporación Nacional de Telecomunicaciones provee a los diferentes ISPs clientes, y proponer alternativas de solución para las falencias encontradas.

El propósito del servicio VPLS, que actualmente está surgiendo en el país, es el de conectar múltiples sitios de una manera transparente en un único dominio de broadcast sobre su red MPLS de tal manera que todos los sitios de los clientes del ISP, se consideren en la misma LAN, sin tener en cuenta sus localizaciones. VPLS utiliza una interfaz Ethernet con el cliente, simplifica la frontera LAN/WAN y permite un aprovisionamiento rápido y flexible del servicio.

Actualmente la CNT E.P es el principal proveedor de servicios de telecomunicaciones en el país, ya que cuenta con el mayor número de clientes ISPs, clientes a los que les provee el servicio VPLS.

Se considera necesario el análisis del servicio VPLS para identificar las debilidades que puedan presentarse y que afecten el funcionamiento del mismo y la correcta prestación del servicio a los usuarios.

Además, VPLS al ser un servicio de capa 2 requiere del análisis de ataques a la seguridad; para identificar cuáles de ellos representan una amenaza para el servicio.

Este trabajo puede ser utilizado como guía para aquellas organizaciones que estén en proceso de implementación de este servicio o que a su vez deseen realizar análisis de un servicio de capa 2 ya implementado.

CAPÍTULO 1

FUNDAMENTOS TEÓRICOS

1.1 INTRODUCCIÓN [18]

Una carencia fundamental de la Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de usuario. La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como "*best-effort*[1] *(mejor esfuerzo)*".

Se necesita entonces introducir cambios tecnológicos fundamentales, que permitan ir más allá del nivel *best-effort* y puedan proporcionar una respuesta más determinística y menos aleatoria, es así que en los últimos años, diversos esfuerzos y actividades de conmutación de etiquetas multiprotocolo se han puesto en marcha, muchos de los cuales ya han afectado considerablemente las redes IP.

MPLS se ha introducido como la red de nuevas aplicaciones capaz de ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las necesarias garantías. Las principales motivaciones para su desarrollo han sido la ingeniería de tráfico[2], la diferenciación de clases de servicio, y las redes privadas virtuales[3] (VPN), servicio de interés para el presente proyecto de titulación en especial las levantadas en capa 2, servicio denominado Virtual Private LAN Service/Servicio LAN Privado Virtual (VPLS), las mismas que se establecen solo bajo este tipo de redes, por lo que es fundamental la introducción a esta arquitectura.

[1] Forma de prestar aquellos servicios para los que no existe garantía de recepción correcta de la información.
[2] Disciplina que procura la optimización del rendimiento de las redes operativas.
[3] Tecnología de red que permite una extensión de la red local sobre una red pública.

1.2 DEFINICIÓN DE MPLS [1], [2]

MPLS es una arquitectura especificada por la IETF[4] (Internet Engineering TaskForce/ Grupo Especial sobre Ingeniería de Internet), que trata sobre el encaminamiento, envío y conmutación[5] de los flujos de tráfico a través de la red mediante la asignación de etiquetas.

En el ruteo basado en IP[6] la desventaja se da porque cada router debe tomar decisiones de ruteo independiente, en base a la información IP de los paquetes, donde la cabecera IP de los paquetes es de gran tamaño.

MPLS mejora la conmutación de redes basadas exclusivamente en IP en donde el tamaño de la tabla de rutas[7] puede ser muy grande, sobre todo si la red no se administra óptimamente y donde la búsqueda de la interfaz de salida para el paquete puede introducir mucho retardo en la comunicación final.

Otra característica de MPLS es que sustituye la tabla de rutas basada en IP por una tabla de reenvío basada en etiquetas. Un equipo corriendo MPLS intercambia etiquetas con los vecinos, de forma que identifique el origen del tráfico y el destino en base a la etiqueta que encapsule el tráfico, de tal manera que la conmutación es extremadamente más rápida, ya que la búsqueda es precisa, sobre un valor de longitud determinado y entrada única en la tabla.

---

[4] Organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad etc.

[5] Intercambio de los Datos entre diferentes nodos para que la información llegue a su destino.

[6] Protocolo de Internet, primer protocolo definido y usado para la comunicación de datos a través de una red de información.

[7] Archivo de datos en la RAM de un Router que se usa para almacenar la información de rutas para redes remotas y redes conectadas directamente, contiene asociaciones entre la red y el siguiente salto.

1.2.1 COMPONENTES DE UNA RED MPLS [1], [2], [8], [9], [17]

En la figura 1.1 se representa el esquema de red MPLS con los componentes que la constituyen, los mismos que se detallan a continuación.

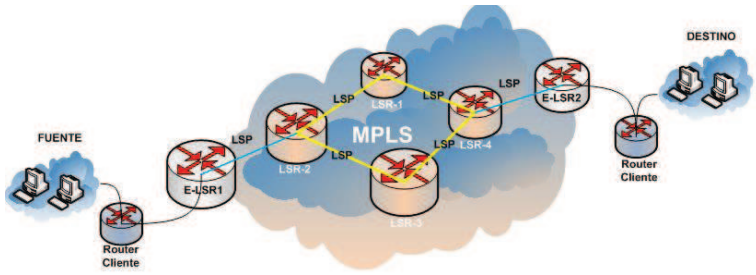


Figura 1. 1: Esquema de una red MPLS

1.2.1.1 LSR (*Label Switching Router/ Enrutador de conmutación de etiquetas*)

Llamado equipo P (*Provider Router/ Enrutador Proveedor*), es un router de gran velocidad ubicado en el núcleo de una red MPLS que se encarga de la conmutación de etiquetas dentro de la red. Cuando llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta y el interfaz de salida, reenvía el paquete por el camino predefinido hacia el siguiente ruteador, asignando la nueva etiqueta, tarea denominada *swap de etiquetas.*

1.2.1.2 E-LSR (*Edge-Label Switching Router/ Enrutador de borde de conmutación de etiquetas*)

Llamado equipo PE (*Provider Edge Router/ Enrutador de Borde hacia el Proveedor*), Constituye un LSR ubicado en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios.

El dispositivo E-LSR se encarga de unir diferentes subredes a la red MPLS, analiza y clasifica el paquete IP entrante, para asignarle una etiqueta de entrada tarea denominada *push de etiqueta* y de retirarla cuando el paquete sale de la red, tarea denominada *pop de etiqueta*.

1.2.1.3 LSP (*Label Switched Path/Camino Conmutado de Etiquetas*)

El LSP es como un túnel en el interior de la red MPLS, siendo una secuencia de nodos en la red. Un LSP se forma con la concatenación de varios LSRs, los mismos que sirven de "camino" para un paquete etiquetado; es decir es el camino lógico que un paquete MPLS toma a través de la red, hasta alcanzar el LSR de salida.

En la figura 1.2 se tiene un ejemplo del proceso de creación de un LSP. El flujo de datos está representando por las flechas de color azul, para lo cual el E-LSR de entrada inicia una cadena de mensajes de petición de etiquetas para crear el LSP (líneas de color verde), el E-LSR de salida responde con mensajes de asociación de etiquetas (línea del color amarillo) formando el LSP correspondiente. El LSP es unidireccional, lo que significa que para el tráfico de retorno es necesario utilizar un LSP diferente.

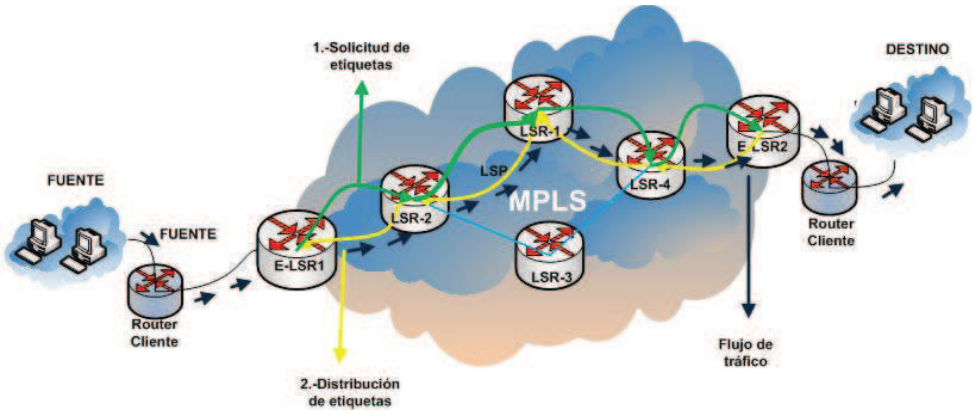


Figura 1. 2: Creación de LSP

1.2.1.4 FEC (*Forwarding Equivalence Class/Clase equivalente de envío*)

Es un conjunto de paquetes IP que tienen el mismo tratamiento y por lo tanto el mismo trayecto, los paquetes que pertenezcan a un mismo FEC tendrán el mismo LSP. Un FEC puede agrupar distintos flujos de tráfico que compartan los mismos requerimientos de transporte, la asignación a un FEC la realizan únicamente los dispositivos E-LSR que se encuentran en los extremos de la red MPLS, es decir cuando el paquete ingresa a la red MPLS.

1.2.1.5 Etiqueta

La etiqueta MPLS es un identificador de valor fijo y de significado local, empleado para asociar un determinado FEC. Al hablar de etiquetas MPLS se refiere a una percepción simplificada del encabezamiento IP, pero a diferencia de éste, las etiquetas no contienen una dirección IP sino más bien un valor numérico acordado entre dos nodos consecutivos para proporcionar una conexión a través de un LSP. Cada etiqueta contiene toda la información asociada al direccionamiento de un paquete hasta su destino final en la red MPLS.

La etiqueta es asignada de acuerdo a la dirección IP destino, tipo de servicio, o siguiendo algún otro criterio. La etiqueta MPLS es insertada a cada paquete entre la cabecera de capa 2 y la cabecera de capa 3.

1.2.1.5.1 Formato y ubicación de la etiqueta MPLS

La etiqueta MPLS se ubica entre la cabecera de nivel 2 y cabecera de nivel 3 y tiene una longitud de 32 bits, dividido en cuatro campos, detallados a continuación:

1. **Label (Etiqueta).-** Campo de 20 bits, corresponden a la etiqueta en sí.

2. **EXP (Experimental).-**Ahora llamado ToS (*Type of Service/Tipo de Servicio*), es un campo de 3 bits, usado para llevar valores de preferencia CoS (*Class of Service/Clase de Servicio)* que se asignan a un FEC.

3. **STACK o bit S.-**Campo de 1 bit, con valor igual a 0 indica si hay un grupo de etiquetas; si el bit está en 1 significa que sólo hay una etiqueta o es la última del grupo.

4. **TTL (TimeTo Live/ Tiempo de Vida).-**Campo de 8 bits, tiene la misma función que el TTL de la cabecera IP, por lo tanto cuando ingresa un paquete en la red MPLS el router de ingreso inicializa el TTL de la etiqueta al mismo valor que tiene en ese momento la cabecera IP. Durante el viaje del paquete por la red MPLS el campo TTL de la etiqueta disminuye en uno por cada salto, el de la cabecera IP no se modifica. A la salida, el router de egreso coloca en la cabecera IP el valor del TTL que tenía la etiqueta, menos uno. Si en algún momento el TTL vale 0 el paquete es descartado. Si hay etiquetas apiladas solo cambia el TTL de la etiqueta situada más arriba. Cuando se añade una etiqueta ésta hereda el valor TTL de la anterior en la pila, cuando se quita, pasa su valor (menos uno) a la que tenía debajo.

A continuación en la figura 1.3, se presenta el formato y ubicación de la etiqueta MPLS:

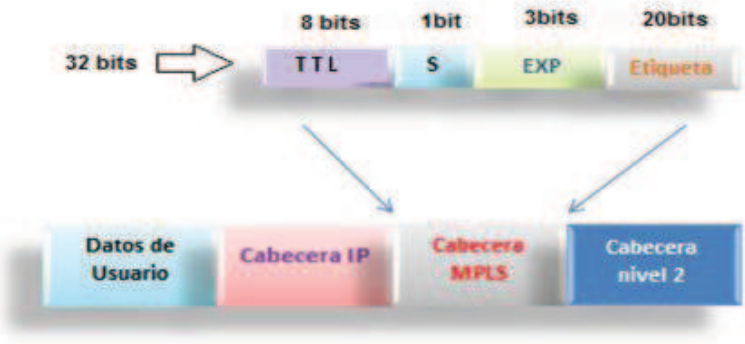


Figura 1. 3: Formato y ubicación de la Etiqueta MPLS

1.2.1.5.2 Stack de etiquetas

Un stack o pila de etiquetas es un conjunto ordenado de etiquetas, en donde cada etiqueta tiene una función específica. Si el Router E-LSR, adiciona más de una etiqueta sobre un paquete IP entonces ha generado una pila de etiquetas, en este caso el campo S indicará si una etiqueta constituye el tope inferior de la pila.

El campo S=1 indica que es la última etiqueta, cuando salga quedará vacía la pila, esto generalmente ocurre en el Router de salida. Cuando S=0 indica que por lo menos hay otra etiqueta antes en la pila, En la figura 1.4, se presenta un paquete que contiene tres etiquetas en donde la última etiqueta tiene el bis S en 1.

Figura 1. 4: Pila de tres etiquetas MPLS

1.2.2 LDP (*LABEL DISTRIBUTION PROTOCOL/ PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETAS*)

Luego de la asignación de etiquetas en un router, éstas son distribuidas entre LSRs directamente conectados, mediante el uso del protocolo LDP. Hay cuatro categorías de mensajes LDP:

- **Descubrimiento.-** Anuncian y mantienen una presencia LSR en la red.

- **Sesión.-** Son utilizados para establecer, mantener y remover sesiones entre LSRs

- **Anuncio.-** Se utilizan para crear, cambiar y borrar las asociaciones de etiqueta FEC.

- **Notificación:** se usan para indicar errores.

1.2.2.1.1 Establecimiento de una sesión LDP

1. Las sesiones LDP son iniciadas cuando un LSR envía mensajes *hello* sobre interfaces permitidas para el envío MPLS. Si otro LSR está conectado con esa interfaz (y la interfaz está habilitada para MPLS), el LSR directamente conectado intenta establecer una sesión con la fuente de los mensajes *hello*. El LSR con ID más alta es el LSR activo. El LSR activo intenta abrir una conexión TCP con el LSR pasivo (LSR con menor ID) sobre el puerto 646 de TCP (LDP usa el puerto 646 de TCP).

2. El LSR activo intercambia mensajes *Initialization* que permiten negociar parámetros de la sesión.

3. Si el LSR pasivo acepta los parámetros contesta con un mensaje *Initialization;* si los parámetros no son aceptables el LSR pasivo envía un mensaje de notificación de error.

4. El LSR pasivo envía un mensaje de *KeepAlive* al LSR activo después de enviar un mensaje de *Initialization*.

5. El LSR activo envía un KeepAlive al LSR pasivo y la sesión LDP tiene lugar. En este momento, las etiquetas FEC pueden ser intercambiadas entre los LSRs.

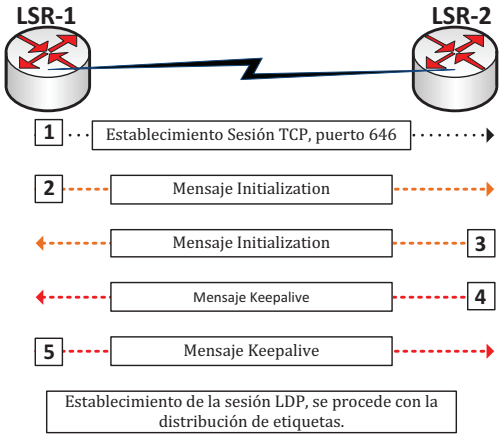


Figura 1. 5: Intercambio de mensajes LDP

1.2.3 ARQUITECTURA MPLS [2], [8], [13], [14]

La arquitectura MPLS contiene dos componentes principales, el plano de datos o componente de envío y el plano de control o componente de control. A continuación se detallan las tareas realizadas de cada componente.

1.2.3.1 Plano de control

Es el encargado de determinar la disponibilidad para acceder a una red de destino, para lo cual intercambia información de enrutamiento de capa tres, y además es el responsable de intercambiar etiquetas entre los routers vecinos, estas dos fuentes le permiten construir su tabla de envío, teniendo así la información de FECs y las direcciones de salto provistas por los protocolos de capa red.

El plano de control utiliza dos fuentes de información:

- **RIB** (*Routing Information Base/ Base de información de Enrutamiento*)

Esta tabla proporciona información sobre la red destino y los prefijos de subred que se utiliza para la asociación de etiquetas, aquí se encuentran todas las rutas aprendidas por cada uno de los nodos de la red MPLS.

- **LIB** *(Label Information Base/ Base de información de Etiquetas)*

En esta tabla se encuentran todas las etiquetas asignadas por el nodo MPLS local (etiquetas locales) y las asignaciones de dichas etiquetas a las etiquetas recibidas de los vecinos, es por esto que se requiere de un protocolo de distribución de etiquetas como LDP, para dar a conocer a otros routers que se ha realizado la asociación de etiquetas.

Cada LSR crea una asignación local y distribuye esta asignación a todos sus vecinos LDP, para los vecinos LDP estas asignaciones son consideradas como remotas y también las almacena junto con las asignaciones locales en su tabla LIB.

1.2.3.2 Plano de Datos

Este plano tiene como función conmutar los paquetes MPLS entrantes, basándose en las tablas de enrutamiento ofrecidas por el plano de control. El plano de datos utiliza dos fuentes de información:

- **FIB** *(Forwarding Information Base/ Base de Información de Envío)*

La FIB es una tabla que se utiliza para definir a qué interfaz se debe reenviar el paquete. En VPN de capa 3, la tabla FIB se llama VRF (Virtual Routing and Forwarding /Enrutamiento virtual y Reenvío) y almacenan las rutas de una determinada VPN, mientras que para VPN de capa 2, la tabla FIB se llama VFI (Virtual Forwarding Interfaces/ Interfaces Virtuales de Envío) y contienen direcciones MAC.

- **LFIB** *(Label Forwarding Information Base/Base de Información de reenvío de Etiquetas)*

Esta tabla es usada para la conmutación de etiquetas. La LFIB usa un subconjunto de etiquetas contenidas en la LIB para el envío del paquete y almacena solo las etiquetas que en ese momento el plano de datos está usando, contiene la información de etiquetas e interfaces entrantes y salientes, y la dirección del próximo salto.

Los nodos MPLS por lo tanto son responsables del reenvío de paquetes mediante el plano de datos, y construir y mantener las tablas de envío mediante el plano de control. A continuación en la figura 1.6 se presenta la arquitectura de un nodo MPLS.

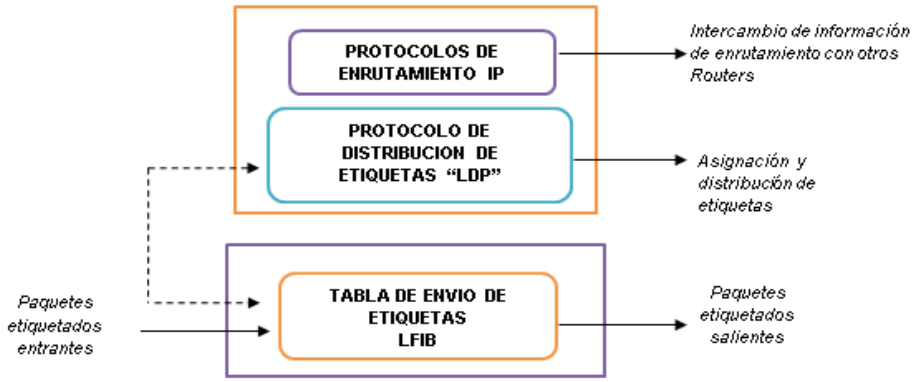


Figura 1. 6: Arquitectura básica de un Nodo MPLS

1.2.4 FUNCIONAMIENTO DE MPLS

El funcionamiento de MPLS es basado en la asignación e intercambio de etiquetas como se indica en la figura 1.7, en donde cada nodo asigna una etiqueta local para cada destino de la tabla de enrutamiento, en este caso la red de destino es la red X, y propagan las etiquetas en dirección contraria al flujo de datos, hacia los routers

directamente conectados (routers vecinos), empleando para ello el protocolo de distribución de etiquetas LDP.

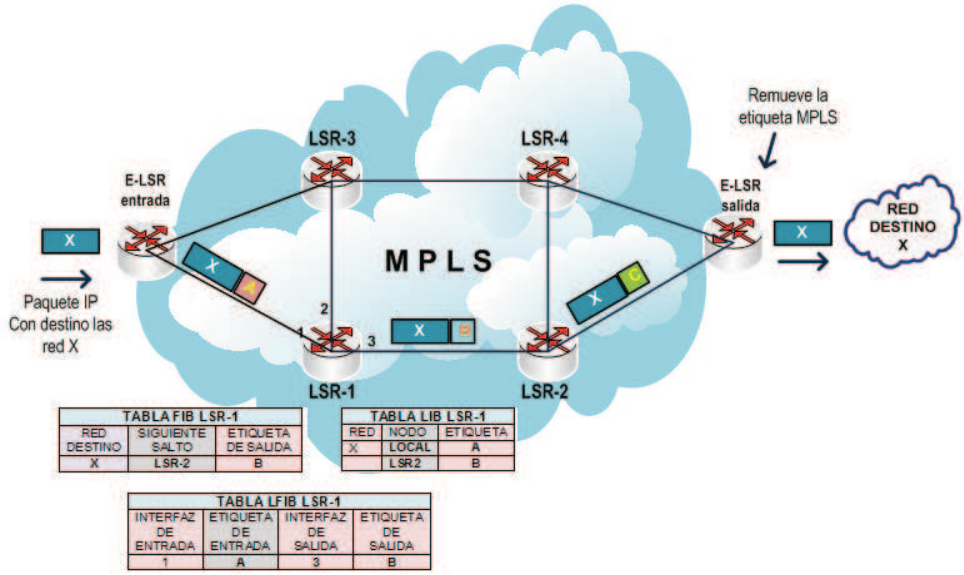


Figura 1. 7: Funcionamiento de MPLS

Una vez que el paquete IP entra a la red MPLS es clasificado y etiquetado por el enrutador de borde E-LSR. Los flujos de tráfico que comparten la misma ruta y el mismo tratamiento son asignados a un FEC con igual etiqueta, y por lo tanto tendrán el mismo trayecto pero no necesariamente el mismo destino.

Cada FEC tiene diferente QoS (*Quality Of Service/Calidad de Servicio),* esto es muy importante ya que permite tratar a los paquetes que van al mismo destino de igual manera, además permite utilizar todos los recursos de la red ya que no necesariamente se utiliza el camino más rápido si no el óptimo.

Una vez que una etiqueta MPLS ha sido insertada en un paquete, el E-LSR, se encarga de enviar dicho paquete al siguiente nodo, todos los nodos realizan una consulta en su tabla FIB para determinar el próximo salto y en su tabla LFIB para hacer un cambio de etiquetas, es decir una simple conmutación de etiquetas. El

paquete sigue la ruta LSP establecida por los LSR mediante el protocolo LDP, cada LSP es unidireccional, por lo que para el tráfico de regreso se deberá utilizar un LSP diferente.

En la nube MPLS, la cabecera de capa red del paquete no vuelve a ser analizada, y es conmutada simplemente por su etiqueta, si un LSR detecta que debe enviar un paquete a un E-LSR de salida, éste se encarga de remover la etiqueta MPLS y enrutar el paquete recibido según capa 3 del modelo OSI[8].

1.2.4.1 PHP (*Penultimate Hop Popping/Preparación del Penúltimo Salto*)

Esta funcionalidad del protocolo MPLS ahorra una etiqueta en el extremo final del túnel o LSP, evitando así una doble búsqueda en las tablas de reenvío del último LSR, la etiqueta debe ser extraída obligatoriamente en el penúltimo LSR para que sólo llegue tráfico encapsulado con la etiqueta del cliente.

1.2.4.2 MTU (*Maximum Transfer Unit/Unidad Máxima de Transferencia*)

MTU expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones. En el marco MPLS la etiqueta añade 4 bytes a cada paquete, por lo que es posible que se necesite aumentar el tamaño de MTU y así evitar que los paquetes sean fragmentados, también hay que considerar que en aplicaciones de MPLS tales como VPNs se añade más de una etiqueta, por lo tanto el tamaño del paquete aumenta con respecto al número de etiquetas que le sean asignadas.

El MTU se incrementa automáticamente en las interfaces WAN, pero se debe configurar manualmente en las interfaces LAN. El Cisco IOS tiene el comando ***mpls mtu*** *"tamaño máximo del paquete"* el mismo que es colocado en la interfaz deseada

[8]El modelo de interconexión de sistemas abiertos (OSI), es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

permitiendo especificar el tamaño del paquete etiquetado máximo que puede pasar por el enlace de datos.

1.3 REDES PRIVADAS VIRTUALES/VIRTUAL PRIVATE NETWORK (VPN) SOBRE MPLS

Dentro de las principales aplicaciones de una Red MPLS tenemos la implementación de redes privadas virtuales, las VPNs se construyen a base de conexiones realizadas sobre una infraestructura compartida, en el cual se pueden integrar aplicaciones multimedia de voz, datos y video de una manera aislada que provee seguridad, además incluye beneficios como calidad de servicio de extremo a extremo, protección de ancho de banda y recursos.

1.3.1 CLASIFICACIÓN DE VPNS SOBRE MPLS [10], [11], [19]

Las redes privadas virtuales sobre MPLS se pueden clasificar de acuerdo al servicio que se le ofrezca al cliente, el enfoque es de acuerdo a los requerimientos que se deseen. Éste proyecto está orientado hacia la implementación sobre capa de nivel de enlace de datos, así que la clasificación se realiza de acuerdo al nivel de la capa del modelo OSI en el que se implemente, ya sea redes privadas virtuales de capa 3 L3VPNs o de capa 2 L2VPNs, ver figura 1.8.

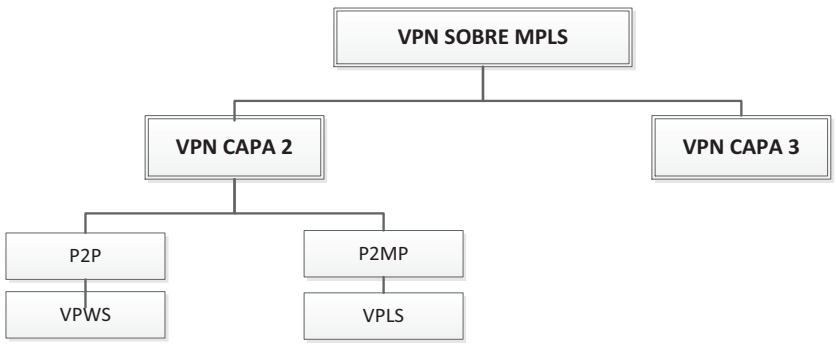


Figura 1. 8: Clasificación de VPNs sobre MPLS

Con lo dicho anteriormente los tipos de VPNs son:

- VPN Capa 3 sobre MPLS.
- VPN Capa 2 sobre MPLS.

1.3.1.1 VPN Capa 3 basadas en MPLS

Las VPNs IP basadas en MPLS, fueron introducidas hace algunos años, la característica principal de estas VPNs es su soporte de IP. Cada VPN tiene su propia tabla de envío y enrutamiento, creando enrutadores virtuales; así cualquier cliente o sitio que pertenezca a una VPN se le permite sólo el acceso a un grupo de rutas contenidas dentro de la tabla.

Cualquier enrutador PE en una red MPLS/VPN contiene un número de tablas de enrutamiento por VPN y una tabla de enrutamiento global que es usada para alcanzar los otros enrutadores en la red del proveedor, así como destinos alcanzables externos, como por ejemplo, el resto de Internet.

El concepto de enrutadores virtuales les permite a los clientes usar cualquier espacio de direcciones globales o privadas en cada VPN. La exclusividad de direcciones no es requerida entre VPNs, excepto cuando dos VPN que comparten el mismo espacio de direcciones privadas quieran comunicarse.

1.3.1.2 VPN Capa 2 basadas en MPLS

En los últimos años la VPN de Capa 2 basada en la tecnología MPLS ha emergido, estas redes tienen la naturaleza de ser multiprotocolo, es decir, pueden transportar tanto tráfico IP como tráfico no IP, gran parte de las especificaciones del IETF sobre como transportar el tráfico de Capa 2 a través de una red MPLS, están ya descritas.

Existen borradores y una especificación reciente, el borrador Martini del IETF (IETF Martini drafts), en este documento se describen los métodos de transporte del Protocolo de Unidad de Datos (PDUs), de protocolos de la capa 2, sobre una red MPLS.

Con respecto a las VPLS (Virtual Private LAN Services / Servicio Virtual LAN Privado), que es el servicio de interés en este proyecto, existen borradores en los Grupos de Trabajo del IETF, “draft Kompella” y “draft Lasserre-VKompella”, que son los borradores de los cuales se desarrolló la especificación reciente (año 2007) para VPLS, el RFC 4762, que especifica el Servicio Privado Virtual LAN con señalización LDP.

1.3.1.3 VPN punto a punto de capa 2

Dentro de este grupo se identifican las VPWS (Virtual Private Wire Service / Servicio Virtual Cable Privado) que es un circuito punto a punto que conecta dos equipos de cliente. Se establece una conexión lógica sobre una red de paquetes.

1.3.1.4 VPN multipunto de capa 2

Dentro de este grupo tenemos a las VPLS, servicio de red privado virtual LAN, también se las conoce como TLS (Servicio de LAN transparente) o servicio E-LAN (Ethernet LAN), así como las VPNs IP basadas en MPLS, VPLS es un servicio multipunto pero la diferencia es que éste puede transportar tráfico no-IP y por su naturaleza LAN se beneficia de las ventajas conocidas de Ethernet. Su objetivo es conectar múltiples sitios en un único dominio de broadcast sobre la red MPLS.

Este proyecto se centra a las soluciones que brinda VPLS, así que se describe de una forma detallada el servicio.

En la figura 1.9 se puede observar el esquema para la clasificación descrita anteriormente.

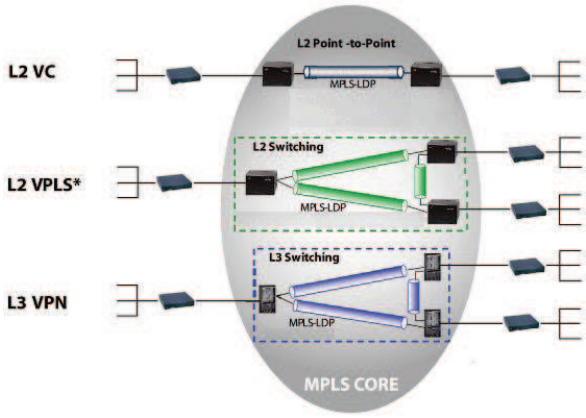


Figura 1. 9: VPNs Capa 2 y 3 sobre MPLS

1.4 SERVICIO VIRTUAL LAN PRIVADO/ VIRTUAL PRIVATE LAN SERVICE (VPLS) [3], [9], [10], [12]

Los servicios de transporte Ethernet de área amplia pueden brindarse a través de una red troncal MPLS para garantizar un servicio rápido y confiable, VPLS consiste en el uso de Ethernet para recrear una red de área amplia, sus siglas definen lo siguiente:

- “Virtual” implica una separación lógica del tráfico del cliente.
- “Privada” significa que existe un dominio de conmutación aislado.
- “LAN” se refiere a la Red de Área Local que consta de un solo dominio, por cliente.

- “Servicio” significa que el proveedor de servicio es quien asegura la prestación.

VPLS se construye sobre la pila de protocolos MPLS, es un servicio que crea Redes Privadas sobre estructuras basadas en Ethernet, y emula toda la funcionalidad de una red de área local completa independiente de su localidad geográfica, ver figura 1.10.

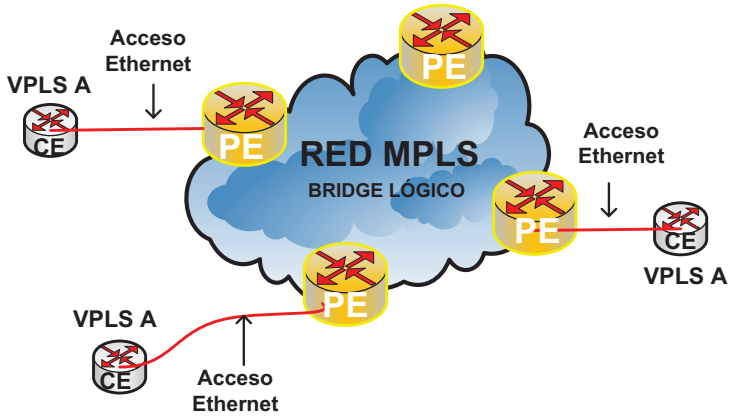


Figura 1. 10: Construcción de la red VPLS

VPLS permite entonces a múltiples clientes dispersos geográficamente conectarse entre sí a través de una red troncal, emulando un solo segmento LAN Ethernet para ese cliente.

Una red VPLS se comporta como un switch tradicional, separando dominios de colisión, consiguiendo ampliar un simple segmento Ethernet de red, en donde la red de Área Local va más allá de los clientes llegando hasta el proveedor de servicios donde se conecta a la red que emula el comportamiento de un switch.

El esquema VPLS se trata básicamente de VPNs de usuarios sobre una red IP/MPLS, al implementarse sobre esta red se consigue en cierto modo la capacidad de conectividad punto a multipunto y no solo punto a punto.

1.4.1 COMPONENTES DEL SERVICIO VPLS

Como se indica en la figura 1.11, una red VPLS está conformada por equipos PEs, equipos clientes CEs, Pseudowires y una instancia VPLS, cada uno se describe a continuación.

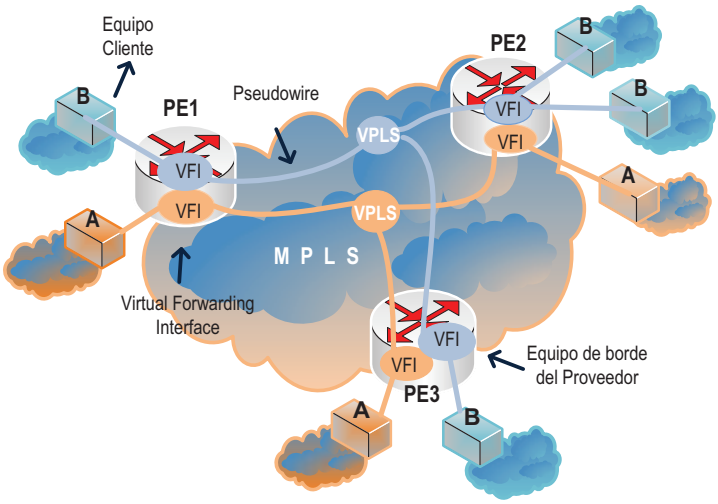


Figura 1. 11: Modelo de referencia VPLS

1.4.1.1 Equipo PE *(Provider Edge Router/ Enrutador de Borde hacia el Proveedor)*

Estos equipos se localizan en la frontera de la red MPLS, es en donde empieza y termina el servicio VPLS, al proporcionar al usuario la interfaz de acceso a la red, deben tener bien diferenciados el plano de datos y el plano de control dentro de los procesos de tráfico.

Para esto implementan dos pilas de protocolos de forma paralela debido a que por un lado el usuario pueda establecer comunicación con el equipo de acceso PE de forma que crea que la conexión es directamente con el equipo remoto que está físicamente conectado al otro lado de la red IP/MPLS.

A continuación en la figura 1.12 se indican las dos pilas de protocolos que el equipo PE maneja.

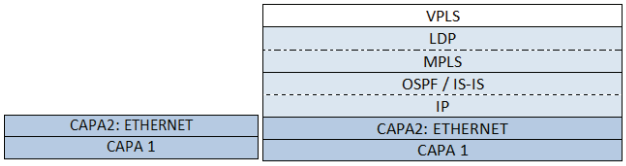


Figura 1. 12: Pila de protocolos de un equipo PE

Los routers PE deben soportar todas las prestaciones clásicas Ethernet, como aprendizaje MAC, replicación y envío de tramas. Además debe conocer las direcciones MAC del tráfico que llega a sus puertos de acceso y de red.

1.4.1.2 Equipo CE (*Customer Edge/ Enrutador de Borde hacia el Cliente)*

Es el punto final para completar la red que soporta VPLS, está situado en las instalaciones del cliente y conectado al Equipo PE; el circuito de conexión entre el CE y el PE es ethernet. El equipo CE puede ser un router o switch, la elección es dependiendo del proveedor y de las necesidades que requiera.

1.4.1.3 Pseudowire

La tecnología pseudowires está normalizada por el IETF, los pseudowires son conocidos históricamente como “túneles Martini”. Un pseudowire (PW) es un circuito virtual que está formado por un par de LSPs unidireccionales punto-a-punto de un solo salto, uno en cada dirección, a continuación en la figura 1.13 se presenta el modelo de un pseudowire.

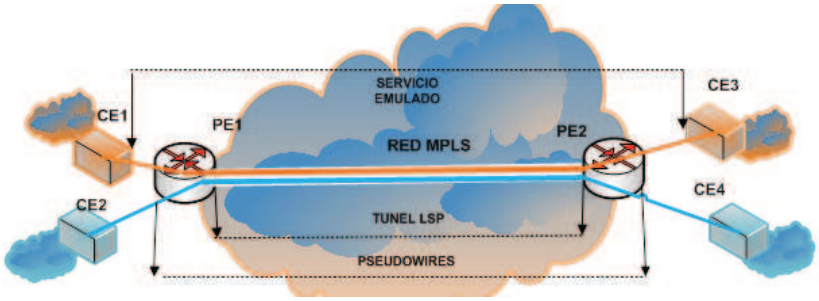


Figura 1. 13: Modelo de un Pseudowire

1.4.1.4 VFI *(Virtual Forwarding Interface/ Interfaz Virtual de Envío)*

Las VFI se crean en los equipos PEs, es aquí en donde se aplican todas las decisiones de reenvío de cada VPLS. La conexión entre los PEs relacionados en una misma instancia VPLS es realizada mediante Pseudowires.

Un router PE puede participar en más de un servicio VPLS para más de un cliente, por lo tanto un router PE puede tener más de una instancia VPLS. Aquí se crea la base de datos (FIB) para cada instancia la misma que es construida mediante el aprendizaje MAC sobre el tráfico Ethernet.

1.4.2 FUNCIONAMIENTO DE VPLS

El funcionamiento de VPLS está dado por la creación de una malla completa de túneles LSPs entre todos los PEs que participan en MPLS. Las VPLSs utilizan esta malla para crear su propia malla de túneles internos entre todos los PEs. Para la asociación de los PEs, el proveedor de servicio puede configurar el PE con las identidades de todos los otros PEs en la VPLS concreta.

Se forma entonces una instancia VPLS y es identificada por un VFI-ID (VPN-ID) de igual valor entre los PEs que participen en la VPLS; cada par de PEs realiza una

sesión LDP dirigida en la que se indica qué etiqueta VC usar para enviar paquetes hacia la VFI específica, creándose así los respectivos pseudowires o conexiones virtuales.

La etiqueta VC (Circuito Virtual) o PW (pseudowire) es la etiqueta interna recibida por el PE que determina el circuito virtual por el cual se va a transportar la trama así como la VLAN asociada hacia la interfaz del usuario CE. La asignación de esta etiqueta es debido a que la etiqueta obtenida después de realizar un push MPLS denominada etiqueta del túnel no le permite al equipo PE decidir qué hacer con el paquete que recibe, y es visible solamente hasta que el paquete llegue al PE correspondiente.

1.4.2.1 Plano de datos y control de una VPLS

En el servicio VPLS el plano de datos se encarga de colocar dos etiquetas MPLS en la trama Ethernet, la etiqueta externa que identifica el túnel al que pertenece la trama y la etiqueta interna VC que identifica el pseudowire hasta el circuito del cliente. Cada PE tiene una tabla de conmutación por instancia VPLS que relaciona MAC, VC y puertos específicos.

El Plano de Control es el encargado de la señalización del protocolo LDP, la sesión LDP señaliza cada VC o pseudowire entre un par de Routers PE permitiendo anunciar las etiquetas VC entre cada par de PEs.

1.4.2.2 Encapsulación y envío de la trama

El equipo CE primero encapsula el tráfico de capa 2 sobre Ethernet incluyendo la VLAN asociada a la VFI para luego ser enviadas al Router PE de borde, independientemente del protocolo de acceso usado entre el CE y el PE, Ethernet es siempre el protocolo usado en un sistema VPLS.

Para cada trama entrante, el PE de borde retira la cabecera de acceso junto con el preámbulo y posteriormente el PE selecciona el VC y el túnel LSP e inserta la etiqueta interior VC y la externa del túnel.

El LSR inmediato no es consiente del servicio VPLS, éste simplemente usa la etiqueta del túnel para conmutar los paquetes etiquetados a través de la red MPLS y hacia el PE de salida, realizando swapping de etiquetas en cada salto

Cuando el PE de salida recibe el paquete, éste retira la etiqueta externa e inspecciona la información de la etiqueta interna permitiendo al PE conjuntamente con la información de la FIB saber la instancia VPLS a la que la trama pertenece, puerto saliente o sub-interfaz para ser enviado al dispositivo CE.

El servicio VPLS permite conexiones punto-multipunto o multipunto a multipunto por replicación de tramas desde el PE de ingreso, utilizando el full mesh de pseudowires para la inundación de paquetes etiquetados hacia todos los PEs de la instancia VPLS. Tanto las tramas unicast o multicast con MAC de destino desconocida son tratadas de esta manera, en la figura 1.14 se presenta la encapsulación de la trama desde el equipo CE de origen hasta la dirección CE destino.

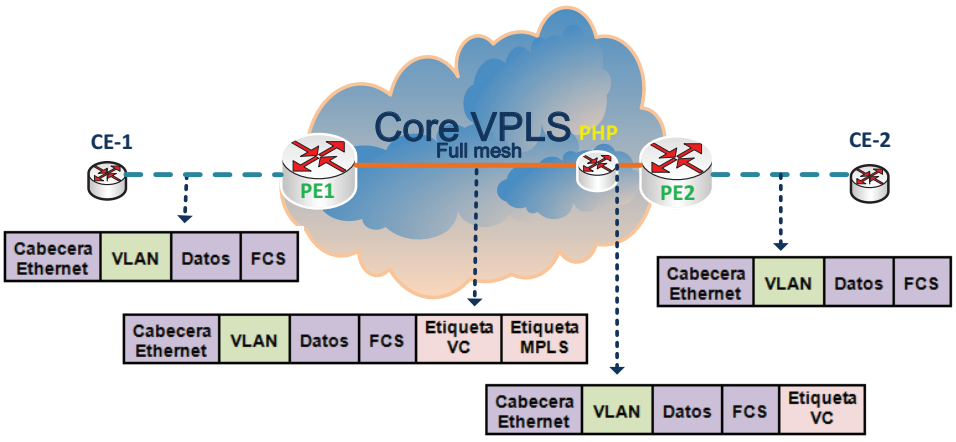


Figura 1. 14: Encapsulación de la trama en la VPLS

1.4.2.3 Aprendizaje MAC

Para cada VPLS el PE mantiene separada la tabla FIB que contiene todas las direcciones MAC y el identificador de las interfaces aprendida, y cualquier otra información necesaria para enviar el tráfico VPLS a las distintas direcciones. El PE aprende las direcciones MAC de origen mediante el tráfico enviado por otro PE en la VPLS.

Cuando un PE recibe una trama, se lleva a cabo la búsqueda de la dirección MAC destino, si existe una entrada para la dirección MAC destino en la tabla FIB, el PE utiliza esta información para fijar valores de etiqueta VC e identificar el puerto de salida correcto, si la FIB no contiene esta entrada, el PE replica la trama y la reenvía a cada PE de la VPLS usando las etiquetas VC que fueron señaladas por cada PE cuando se establecieron los pseudowires.

De manera similar si el PE reenvía la trama para ser enviada hacia el dispositivo CE y no existe una entrada en la tabla FIB, el PE reenvía la trama a cada dispositivo de acceso que pertenece al segmento LAN.

VPLS utiliza un mecanismo de envejecimiento de las direcciones de origen aprendidas por los PEs en donde se eliminan las MAC address que no se utiliza por un periodo de tiempo específico.

En la figura 1.15 se indica la transmisión de tramas con direcciones MAC conocidas y desconocidas, la respectiva replicación de las mismas y la FIB que un PE utiliza para tomar decisiones de reenvío.

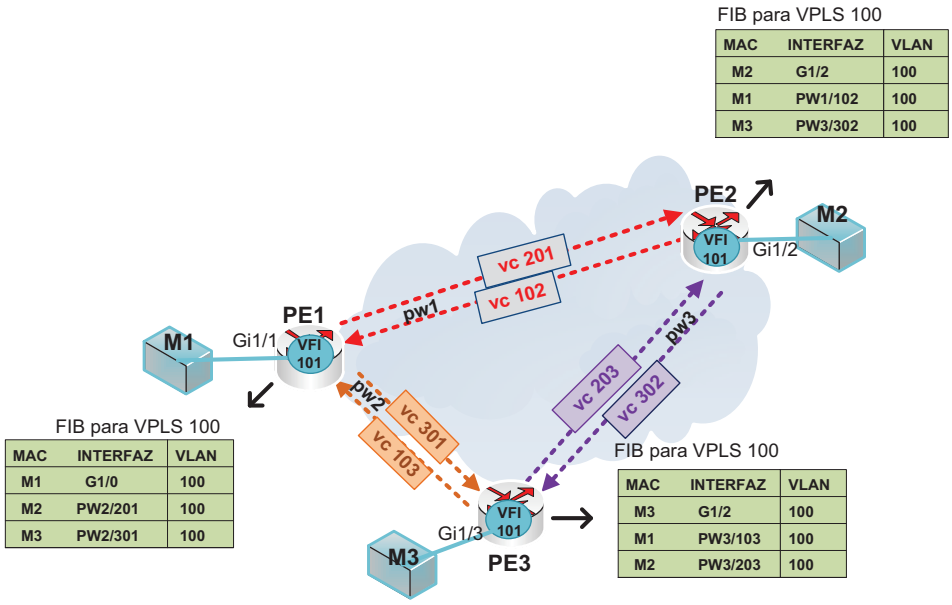


Figura 1. 15: Aprendizaje MAC en VPLS

1.4.2.4 VPLS libre de lazos

Los servicios VPLS son VPNs de nivel 2; éstas VPNs se conectan entre sí por medio de sesiones LDP entre PEs tunelizados sobre LSPs. Todos los enlaces de la misma región VPLS se definen como mesh, de forma que el tráfico que reciben los PEs, no se reenvía utilizando aquellos enlaces tipo mesh dentro de la VPLS.

De esta forma, el tráfico broadcast de un cliente, entra en la red por medio de un PE, al ser broadcast o al no haber cerrado el ciclo de aprendizaje de MACs reenvía la trama por toda la VPLS de dicho cliente, es decir lo reenvía por todas las interfaces del cliente que pudiera haber en ese PE y por todos los enlaces que conectan con el resto de PEs de la región.

Cuando la trama llega al PE remoto éste tampoco tiene una interfaz conocida para reenviarla puesto que la dirección MAC destino es broadcast, por lo tanto debería

reenviarla por todas las interfaces de clientes y por todos los enlaces de interconexión con los PEs remotos, pero éstos últimos son de tipo mesh por lo que la trama no vuelve a ser enviada a los PEs. Ésta aplicación es la denominada regla del *Horizonte Dividido* sobre el full-mesh de cada región, en donde se evita que a un mismo nodo le llegue la misma trama por dos caminos, referirse a la figura 1.16.

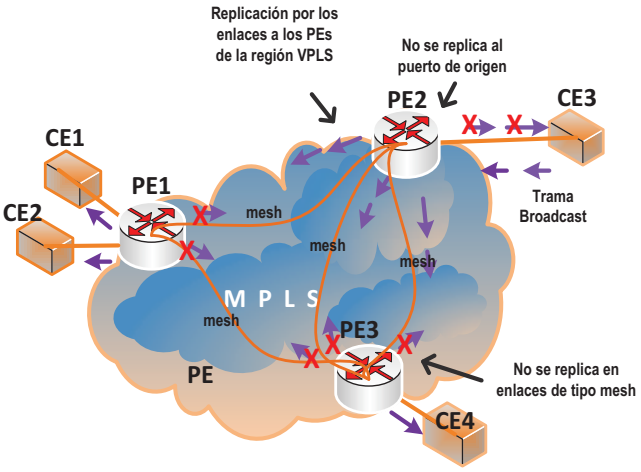


Figura 1. 16: Aplicación de la regla del Horizonte Dividido

1.4.3 MODELOS DE TOPOLOGÍAS BÁSICAS DE VPLS [12], [28]

La topología formada por los pseudowires desempeña un papel crítico en bucles de reenvío y contribuye a la escalabilidad y el rendimiento general.
La red VPLS puede tener las siguientes formas:

- Full Mesh
- Hub and Spoke
- Partial Mesh

1.4.3.1 Full Mesh VPLS/Mallado completo

La figura 1.17 muestra una topología totalmente mallada, es una forma básica del servicio VPLS. Cada Router PE está conectado directamente a todos los demás miembros PEs del servicio VPLS, en la malla de VPLS se requiere establecer n*(n-1)/2 pseudowires entre los miembros PEs, donde n representa el número de equipos PE participantes del servicio VPLS, debido a este tipo de mallado cada PE es consciente de todos los PEs que participan en el servicio VPLS.

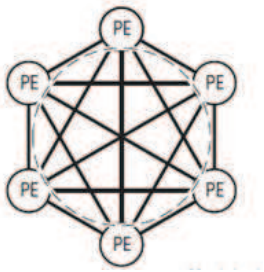


Figura 1. 17: Esquema Full Mesh VPLS

1.4.3.2 Hub and Spoke VPLS/Mallado en forma de Estrella

Para este tipo de conexión se utilizan los denominados spoke-pseudowires, definidos a continuación.

- Spoke-pseudowire.- Un Spoke-pseudowire no es un nuevo tipo de pseudowire, es en realidad una nueva forma para reenviar tráfico a nivel local para una VFI, permite intercambiar tráfico con otras entidades de transmisión (mallas pseudowires, Spoke-pseudowires, etc.).

La figura 1.18 representa una conexión de VPLS, en el cual los Routers PE centrales están conectados de una manera totalmente mallada de pseudowires y aseguran redundancia en el núcleo, en cambio los Routers PE de borde se conectan a los

Routers de núcleo mediante los spoke-pseudowires, con esto no se tiene una red totalmente mallada y se reduce el número de pseudowires requeridos para el servicio.

La red se divide en dos niveles: el núcleo de malla y el nivel spoke.

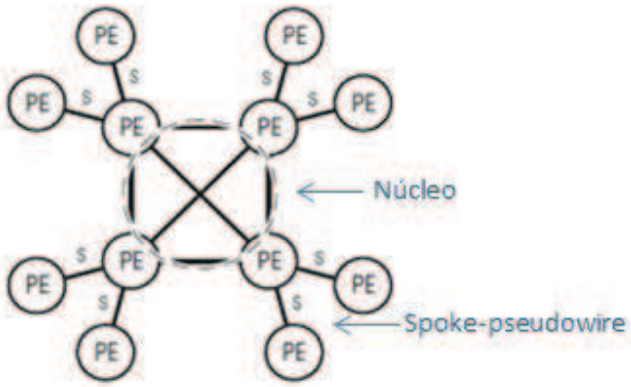


Figura 1. 18: Esquema Hub and Spoke VPLS

1.4.3.3 Partial Mesh

La figura 1.19 muestra una topología similar a la topología Hub and Spoke con la diferencia que de los equipos de PE de borde se conecta otro núcleo Full Mesh mediante dos spoke-pseudowires.

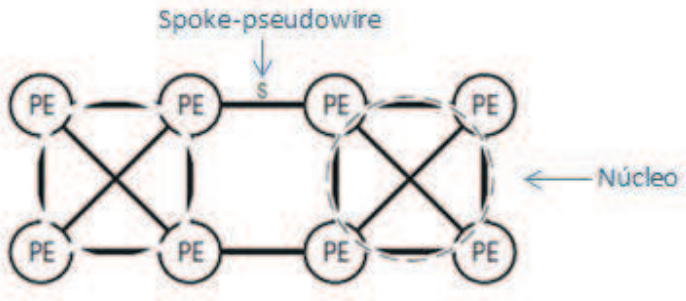


Figura 1. 19: Esquema Partial Mesh VPLS

El tráfico entre las mallas se transmite de una manera óptima a través de los spoke pseudowires; para prevenir lazos se activa solo un Spoke-pseudowire para el envío de tráfico.

Las figuras 1.18 y 1.19 reflejan el modelo jerárquico de VPLS en el cual se tiene dos niveles de pseudowires, de malla total y de spoke-pseudowires.

1.5 MODELO JERÁRQUICO VPLS/ HIERARCHICAL VPLS (HVPLS)[3], [12], [28]

Las redes basadas en la tecnología VPLS presentan escalabilidad limitada, el núcleo de la red se basa en una red IP/MPLS, por lo que necesitan un mallado completo de LSPs entre todos los PEs de la red. Esto claramente reduce el crecimiento debido a la complejidad que presenta el incremento en el tamaño del mallado total, como por la limitación en cuanto a los equipos a la hora de manejar control de tráfico de un gran número de LSPs.

La solución para el despliegue a gran escala con un gran número de PEs y la complejidad del mallado completo que presenta VPLS, es un servicio jerárquico denominado H-VPLS (Hierarchical VPLS), el cual se construye sobre las bases de la solución VPLS, ampliándola para poder proporcionar ventajas operacionales, reduciendo la señalización y la replicación.

Como su nombre lo indica esta arquitectura definirá niveles de jerarquía, que se pueden observar en la figura 1.20 En donde se define una región central o core, a la cual se conectarán las regiones de nivel inferior con uno o dos enlaces.

Al core VPLS se puede conectar un equipo que conecte directamente al cliente u otra región VPLS.

Esta separación jerárquica reduce considerablemente la necesidad de mallar la red completamente ya que sólo recae la obligatoriedad del full-mesh de LSPs sobre el core, y la funcionalidad es la misma detallada anteriormente para VPLS.

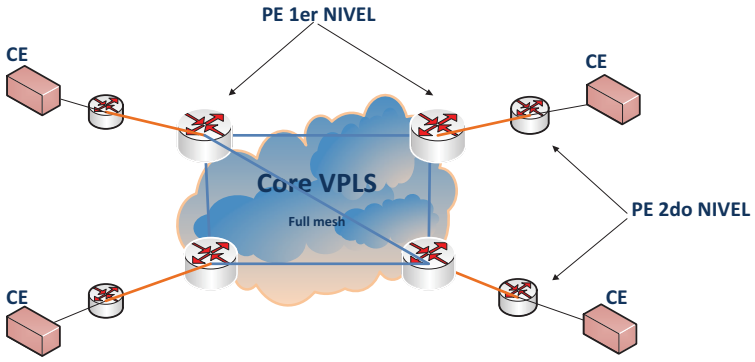


Figura 1. 20: Esquema H-VPLS

1.5.1 CONECTIVIDAD JERÁRQUICA

En el modelo jerárquico VPLS (H-VPLS), se puede identificar dos tipos de dispositivos físicos independientes, por lo tanto en la arquitectura hay dos tipos de dispositivos PE.

Los dispositivos a los que se refiere son U-PE y N-PE que se describen a continuación:

- ***User PE / PE DE USUARIO (U-PE):*** Es el dispositivo de nivel inferior que se conecta directamente al dispositivo cliente CE y tiene una conexión única al dispositivo correspondiente de la red Troncal MPLS.

- ***Network PE / PE DE RED (N-PE):*** Es el dispositivo de nivel superior, el cual está conectado en base a una malla completa VPLS con los otros dispositivos N-PE que participan en el servicio.

1.5.1.1 Operación del U-PE Y N-PES

Un U-PE no es más que un dispositivo que soporta las funciones de conmutación de capa 2, incluye las funciones de aprendizaje y replicación en todos los puertos, normalmente es dedicado para una empresa.

Un N-PE es un dispositivo que soporta todas las funciones de bridging del servicio VPLS y permite el enrutamiento y encapsulación MPLS, es decir éste soporta las capacidades de un N-PE de una VPLS.

En la figura 1.21 se observa la estructura para un modelo H-VLPS en el cual participan los clientes CEs, los dispositivos U-PEs y los N-PEs, dos sitios de los clientes se conectan a un U-PE a través de CE1 y CE2, el U-PE tiene una sola conexión al N-PE1, y los dispositivos N-PEs están conectados en base al VPLS básico de malla completa.

La jerarquía se obtiene al alcanzar un modelo de dos niveles en los que existen dos tipos de pseudowires unos los que conectan un N-PE a otro N-PE llamados simplemente pseudowires y los de acceso del U-PE al N-PE llamados spoke-pseudowires.

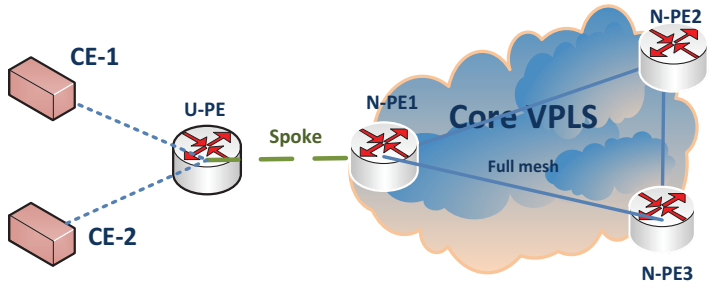


Figura 1. 21: Conectividad Jerárquica H-VPLS

Lo que se logra con este esquema es eliminar una malla completa de pseudowires entre los dispositivos participantes en la nube MPLS. El core VPLS, implementa la arquitectura y funcionalidad de VPLS completamente, desde el nivel físico hasta los peerings LDP entre PEs.

Para proporcionar conectividad con la región Core, se define la asociación tipo Spoke, todo el tráfico cuyo destino es otra región diferente a la región de Core será reenviado a través de la conexión spoke, ya que la regla de Horizonte Dividido no se aplica sobre dicho enlace, pues no es un tipo mesh.

1.5.2 FORMAS DE ACCESO EN H-VPLS

HVPLS se puede implementar de dos formas:

1) H-VPLS con dot1q tunneling en la capa de acceso.
2) H-VPLS con MPLS en la capa de acceso.

1.5.2.1 HVPLS con Red de Acceso MPLS (AToM)

Cualquier Transporte sobre MPLS (AToM)[9] transporta paquetes de nivel 2 en una conmutación por etiquetas multiprotocolo. AToM utiliza un protocolo de distribución de etiquetas dirigido (LDP) de sesión entre los routers de borde para la creación y mantenimiento de las conexiones. La etiqueta es una etiqueta de circuito virtual (VC) que determina la conexión en el punto final del túnel.

El tipo de capa 2 de datos que se transportan a través de la pseudowire, pueden ser tecnologías tales como Ethernet, Frame Relay o ATM.

[9] Any Transport over MPLS, solución para el transporte de tramas de Capa 2 sobre un backbone IP/MPLS

Para el caso de Ethernet, que es la base para este proyecto se le conoce con el nombre de EoMPLS.

Como se indica en la figura 1.22 el cliente envía su trama con su respectiva VLAN la cual llega al equipo U-PE el cual añade la etiqueta VC que es la misma para el núcleo MPLS y añade la etiqueta de túnel para el acceso entre el U-PE y el N-PE; el equipo N-PE conserva la etiqueta de VC y reemplaza la etiqueta de túnel entre U-PE y N-PE por la etiqueta de túnel entre equipos N-Pes; una vez que llega al extremo N-PE se realiza el proceso inverso.

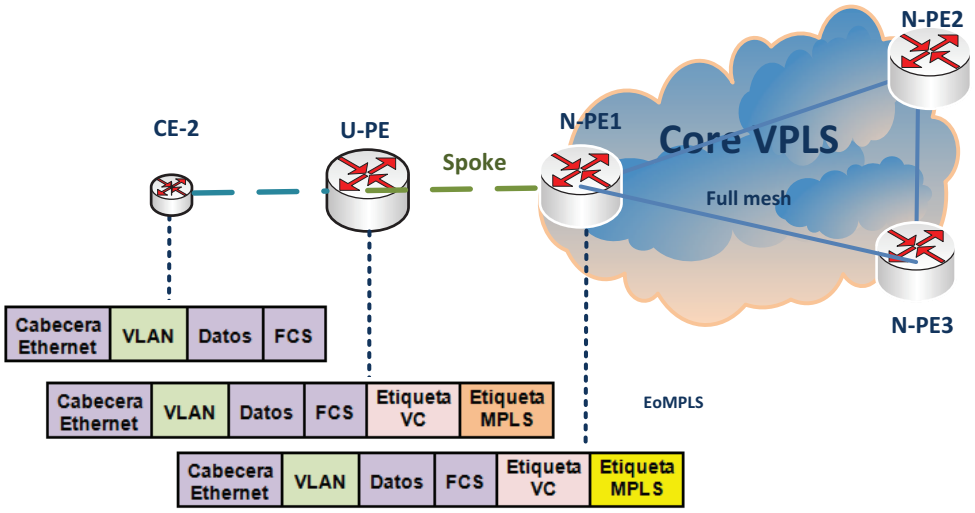


Figura 1. 22: Trama HVPLS con acceso EoMPLS

1.5.2.2 HVPLS con Red de Acceso Q-in-Q

Este modelo jerárquico tiene la misma topología y funcionalidad del modelo mencionado anteriormente con la diferencia que en el nivel inferior los U-PEs y los N-PEs se conectan a través de túneles Ethernet Q-in-Q.

Q-in-Q bajo el estándar IEEE 802.1ad consiste en la capacidad de un doble encapsulado 802.1Q, el propósito de la etiqueta VLAN externa es para enviar el

paquete desde el extremo del túnel de entrada al extremo del túnel de salida y oculta el interior de etiqueta VLAN de la red de transporte MPLS.

Como se indica en la figura 1.23 el cliente envía su trama con su respectiva VLAN la cual llega al equipo U-PE el cual añade una nueva etiqueta (doble etiquetado) que tiene sentido únicamente entre la conexión de U-PEs y N-PEs; el equipo N-PE retira la etiqueta colocada por el U-PE y añade la etiqueta de VC y la etiqueta de túnel; una vez que llega al extremo N-PE se realiza el proceso inverso.

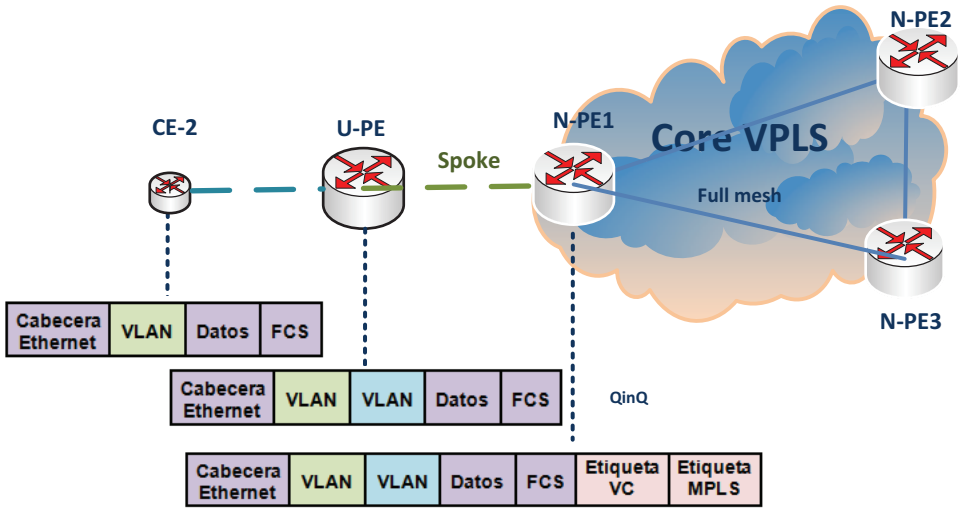


Figura 1. 23: Trama HVPLS con acceso QinQ

1.6 SEGURIDAD EN CAPA 2 [20], [21], [22]

Las VPNs sobre MPLS ofrecen el mismo nivel de seguridad que las VPNs tradicionales, se garantiza la seguridad de que ningún paquete saldrá o entrará de las rutas establecidas.

Las VPNs a pesar de que comparten los mismos medios físicos o lógicos no se invadirán, ya que como su nombre lo indica son redes privadas virtuales, por lo tanto mantendrán aislado el tráfico de los diferentes clientes y se garantiza que los

paquetes de los clientes recibidos en la frontera de la red del proveedor siempre serán enviados a la VPN correspondiente.

Las amenazas a las que está sometida la capa 2 del modelo OSI pueden ser diferentes tipos de ataques o por la saturación de tráfico en las interfaces de los equipos.

1.6.1 DESCRIPCIÓN DE LOS ATAQUES A LA SEGURIDAD DE CAPA DOS

Al tener como referencia al modelo OSI y como se puede observar en la figura 1.24, se debe tener en cuenta que la seguridad de las capas superiores depende de las capas inferiores, y se debe recalcar que los ataques en esta capa suelen producirse a nivel interno de la organización, ya sea por un empleado o visitante.

Por lo tanto es importante considerar la seguridad en la capa enlace de datos ya que aquí se unen los medios físicos y el software.

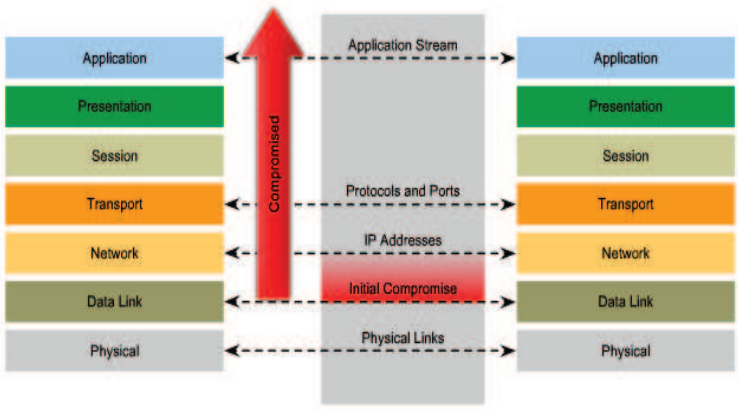


Figura 1. 24: Relación entre capas Modelo OSI

Los ataques maliciosos a la capa 2 son típicamente lanzados por un dispositivo conectado a la red en la LAN.

Éste puede ser un dispositivo ilegal físico puesto en la red o una intrusión externa que toma el control y lanza ataques desde un dispositivo confiable. En cualquier caso, la red visualiza todo el tráfico como originado desde un dispositivo conectado legítimo.

A continuación se describen los tipos de ataques que se tienen a nivel de capa 2:

- Ataques de capa MAC.
- Ataque VLAN.
- Ataques de falseo.
- Ataque de dispositivos Switch.

1.6.1.1 Ataque de capa MAC

En la tabla 1.1 se describe brevemente el ataque de capa MAC y el método para mitigarlo.

TIPO DE ATAQUE	DESCRIPCIÓN	MITIGACIÓN
ATAQUE DE CAPA MAC		
MAC ADDRESS FLOODING / INUNDACIÓN POR DIRECCIONES MAC	Múltiples tramas con direcciones inválidas desde un mismo origen inundan el switch y se agota el espacio de memoria disponible de almacenamiento de la tabla de direcciones (CAM), impidiendo las nuevas entradas de direcciones MAC válidas.	✓ Port Security (Seguridad a nivel de Puertos). ✓ MAC addresses VLAN Access maps (Listas para control de Acceso).

Tabla 1. 1: Descripción de Ataque de Capa MAC

1.6.1.1.1 Métodos de Seguridad

Para mitigar estos efectos se puede aplicar mecanismos de seguridad como son:

a. Port Security

Es un conjunto de medidas de seguridad a nivel de puertos, estas funciones dependen de la marca, modelo y versión de firmware del switch. Sirven para:

- Restringir el acceso a los puertos según la MAC.
- Restringir el número de MACs por puerto.
- Establecer la duración de las asociaciones MAC-Puerto.

Como se observa en la figura 1.25 un intruso no puede atacar un puerto seguro, ya que se restringe el acceso.

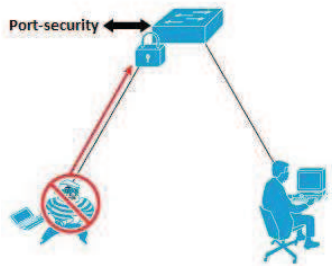


Figura 1. 25: Esquema Port Security

b. Mapas de acceso de Direcciones por VLAN o por puerto

Sirven para crear filtros o listas de acceso (ACL[10]). Con el uso de esta solución se consigue una mejor administración del tráfico global de la red. Las listas de acceso

[10] Una lista de control de acceso (ACL) es un conjunto de permisos asociados a un objeto.

constituyen una eficaz herramienta para el control de la red y añaden la flexibilidad necesaria para filtrar el flujo de paquetes que entra y sale de las diferentes interfaces del router.

1.6.1.2 Ataque VLAN

En la tabla 1.2 se describe brevemente el ataque VLAN y el método para mitigarlo.

TIPO DE ATAQUE	DESCRIPCIÓN	MITIGACIÓN
ATAQUE VLAN		
VLAN HOPPING / ASALTO DE VLAN	El atacante puede modificar el VLAN ID en paquetes encapsulados para trunking y de esta forma puede transmitir o recibir paquetes de otras VLANs.	✓ Asegurar que el puerto del enlace troncal no pertenezca a la VLAN Nativa de los usuarios. ✓ Deshabilitar los puertos no utilizados y colocarlos en una VLAN que no se utilice.
ATTACKS BETWEEN DEVICES ON A COMMON VLAN / ATAQUES ENTRE DISPOSITIVOS DE LA MISMA VLAN	Los dispositivos pueden necesitar protección entre sí, a pesar de que están en una VLAN común. Esto es necesario en los dispositivos que manejan múltiples clientes.	✓ Implementar VLANs Privadas(PVLAN)

Tabla 1. 2: Descripción de Ataque VLAN

1.6.1.2.1 Métodos de Seguridad

a) Refuerzo del enlace troncal y configuración de los puertos

Una forma de mitigar esta falencia es asegurar que el puerto del enlace troncal no pertenezca a la misma VLAN Nativa de los usuarios, deshabilitar los puertos no utilizados y colocarlos en una VLAN que no se utilice, no utilizar la VLAN 1 ya que ésta viene por defecto en todos los puertos.

b) PVLAN (Private VLAN)

Básicamente las PVLANs permiten aislar los puertos de switch dentro de un mismo dominio de broadcast, evitando que los dispositivos conectados en estos puertos se comuniquen entre sí aunque pertenezcan a la misma VLAN y subred.

Habitualmente, una VLAN forma un único dominio de broadcast donde todos los hosts conectados a ella pueden conectarse entre sí.

Por el contrario, una Private VLAN permite una segmentación en la capa 2 del modelo OSI, limitando el dominio de broadcast, de forma que es posible permitir conexiones de cada host con su Gateway, denegando la comunicación entre hosts, y obteniendo el resultado deseado, de modo que si un host se ve comprometido, el resto de equipos podría mantenerse a salvo, este esquema se puede ver en la figura 1.26.

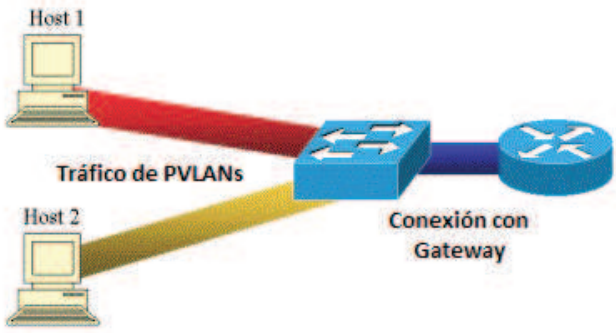


Figura 1. 26: Seguridad con PVLANs

1.6.1.3 Ataque de Suplantación

En la tabla 1.3 se describe brevemente el ataque de suplantación y el método para mitigarlo.

TIPO DE ATAQUE	DESCRIPCIÓN	MITIGACIÓN
ATAQUE DE SUPLANTACIÓN		
MAC SPOFFING / SUPLANTACIÓN MAC	El atacante remplaza su dirección MAC por otra de un host legítimo, el switch actualiza su tabla de direcciones y asigna dicha dirección a ese puerto. Las tramas de datos serán enviadas al intruso.	✓ Usar DHCP snooping. ✓ Port Security
STP SPOOFING / SUPLANTACIÓN STP	El atacante puede modificar su estación con un ID menor, con una prioridad más baja para que sea escogido como Root. Si el ataque tiene éxito todos los paquetes atravesarán a través de él.	✓ Definición de los dispositivos root primario y backup. ✓ Habilitar PortFast, Root Guard, y BDP Guard.
DHCP SPOOFING / SUPLANTACIÓN DHCP	Un dispositivo puede consumir las direcciones disponibles del servidor DHCP (Dynamic Host Configuration Protocol) por un periodo de tiempo, o a su vez puede establecerse como servidor DHCP en ataques de man-in-the-middle.	✓ Usar DHCP snooping.
ARP SPOOFING / SUPLANTACIÓN ARP	Ocurre cuando el atacante manda mensajes ARP de un host legítimo para anunciar que su MAC es la MAC del dispositivo que quiere suplantar, así este puede capturar todas las tramas que se intercambien, otro forma de ataque del hombre en la mitad.	✓ Usar Dynamic ARP Inspection (DAI). ✓ DHCP snooping. ✓ Port Security.

Tabla 1. 3: Descripción de Ataque de Suplantación

1.6.1.3.1 Métodos de seguridad

a) DHCP Snooping

Es una característica que establece qué puertos del switch pueden o no responder a consultas que realice el servidor DHCP, de esta manera se puede diferenciar dos tipos de puertos los seguros (trusted) y no seguros (untrusted). Como se ve en la

figura 1.27 solo el puerto marcado como trusted responde a consultas DHCP, ya que es el puerto asignado físicamente para conexión al servidor.

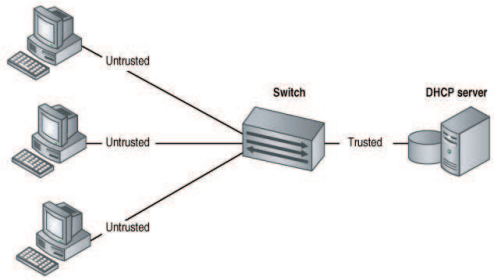


Figura 1. 27: DHCP Snooping

En el caso de los puertos seguros, estos puertos pueden ser origen de todos los mensajes DHCP, en cambio los no seguros únicamente pueden originar consultas DHCP y si se intenta enviar una respuesta DHCP el puerto automáticamente se cierra.

b) Correcta configuración de STP

Definición de los dispositivos root primario y backup, definición de los límites del dominio de STP, habilitar PortFast, habilitar Root Guard, y habilitar BDP Guard, ver esquema en la figura 1.28.

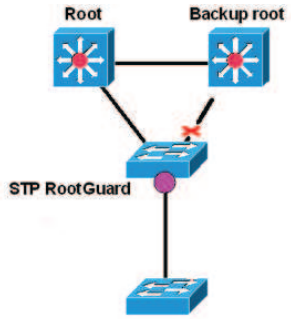


Figura 1. 28: Spannig tree

c) DAI (Dynamic ARP Inspection / Inspección de ARP dinámica)

Se aplica el concepto de puertos seguros e inseguros, cuando es seguro no realiza inspecciones, pero caso contrario es examinado en la tabla de asociaciones DHCP y si su dirección IP no corresponde con su MAC el paquete es descartado y el puerto es bloqueado, ver ejemplo en la figura 1.29.

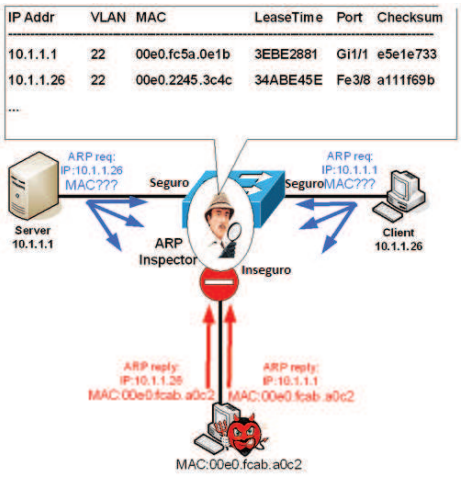


Figura 1. 29: Inspección de ARP dinámica

1.6.2 TORMENTA LAN

Se puede causar una tormenta LAN de muchas maneras como por ejemplo la creación de un tráfico excesivo, errores de aplicación en la pila de protocolos, errores en las configuraciones de la red o generación de ataques de Denegación de Servicio.

Los ataques del tipo DoS (Denial of Service) y los ataques DDoS (Distributed Denial of Service) como muestra la figura 1.30, son utilizados generalmente para hacer flood en un servidor y lograr que éste no pueda responder las solicitudes y no esté disponible para los usuarios legítimos de la red.

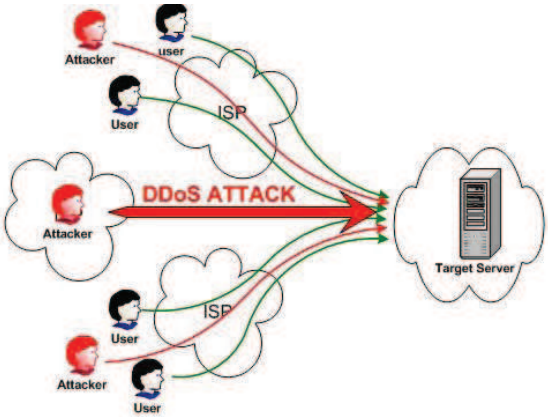


Figura 1. 30: Denegación de Servicio

Los ataques por Denegación de Servicio pueden producirse por desbordamientos de buffer, cuando se activa la ejecución de un código arbitrario en un programa al enviar un caudal de datos mayor que el que puede recibir, pudiendo llegar a sustituir datos de alguna aplicación existente. El DDoS realiza lo mismo que el DoS pero de manera distribuida debido a que el ataque proviene de diferentes puntos.

Todos estos problemas pueden provenir de un solo cliente o de algunos que pertenezcan a la organización saturando de esta manera a su entorno LAN.

1.6.2.1 Storm Control

Como contramedida para solucionar una tormenta LAN se puede utilizar Storm Control, el cual usa umbrales para bloquear y restaurar el reenvío de paquetes broadcast, unicast o multicast.

Usa un método basado en ancho de banda. Los umbrales se expresan como un porcentaje del total de ancho de banda que puede ser empleado para cada tipo de tráfico.

CAPÍTULO 2

CNT EP COMO PROVEEDOR DEL SERVICIO VPLS

2.1 INTRODUCCIÓN

La necesidad de ofrecer un servicio que permita una conexión con mayor eficacia para el transporte de datos sobre redes de área extendida a un costo razonable y en donde se debe proporcionar factibilidad, escalabilidad y alcance, ha sido la principal razón para que la Corporación Nacional de Telecomunicaciones CNT EP, considere usar el servicio VPLS, el cual proporciona las características de conexión anteriormente mencionadas, a fin de garantizar la satisfacción de sus clientes.

En este capítulo se presenta un estudio previo de la situación actual de la CNT EP como proveedor de servicio VPLS a sus clientes ISP. Se han escogido clientes puntuales, por características de cantidad de usuarios y tráfico, todos conectados a PEs en particular los cuales demandan mayor procesamiento. A esto se añade el estudio de la VPLS interna de la CNT EP denominada IP FIJA o Fast Boy, información necesarias para posteriores capítulos.

2.2 SITUACIÓN ACTUAL DEL SERVICIO VPLS EN EL ECUADOR [4]

2.2.1 SERVICIO VPLS EN LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP

La empresa ha adoptado este servicio gracias a las ventajas y altas prestaciones definidas y antes descritas, como solución para la interconexión de manera más rápida, eficiente y confiable en la mayor parte del territorio nacional.

En el portafolio de proyectos de plan de inversiones del año 2008, se completó la primera fase del proyecto de migración a la tecnología MPLS, por lo que en el mismo año se puso en marcha el servico VPLS a nivel de Pichincha, que incluyó diseño, configuración y puesta en funcionamiento. Ya para el año 2009 en la denominada fase dos, el servicio fue aplicado a nivel Nacional para completar y satisfacer la demanda en el resto del país.

Para el presente año se planifica la optimización del servicio en lo referente a monitoreo y mejoramiento de la funcionalidad del mismo, ya que el servicio ha ampliado su nivel de cobertura y de usuarios lo que implica un mayor reto para la CNT EP. El presente proyecto da soporte a los puntos anteriormente señalados.

2.2.2 OTRAS REDES VPLS PUESTAS EN MARCHA EN EL PAÍS POR EMPRESAS PRIVADAS

En el Ecuador, la empresa privada también ha optado por la implementación del servicio VPLS, como solución para brindar servicios de telecomunicaciones, incrementar su cobertura y estar a la vanguardia en la tecnología.

Estas empresas manejan su core con dicha tecnología y administran su infraestructura de voz y datos mediante el servicio VPLS tales como TV Cable, Setel, Global Crossing ahora denominado Level 3.

2.3 ADMINISTRACIÓN DEL SERVICIO VPLS

El servicio VPLS es administrado en cada región por el centro de operaciones de networking (NOC), con su principal sede en la ciudad de Quito.

Cada cliente ISP es identificado mediante un circuito virtual VC, que representa la VPLS, éste está asociado a una VLAN, el circuito de conexión entre el equipo del

cliente y el del proveedor es considerado de acuerdo a las necesidadades del cliente.

El monitoreo de cada VPLS está bajo la plataforma de MPLS y se lo realiza mediante comandos de networking admitidos en el IOS CISCO de cada equipo, comandos detallados en capítulos posteriores. Además se cuenta con monitoreo en tiempo real de tráfico de ciertas interfaces y VLAN de equipos pertenecientes a la red MPLS, mediante la herramienta CACTI, la misma que será detallada posteriormente.

2.4 INFRAESTRUCTURA DE LA RED VPLS EN PICHINCHA

Para el presente proyecto se analizará la funcionalidad del servicio en base a los clientes ISP que demandan la mayor cantidad de tráfico y por consiguiente requieren mayor monitoreo y administración del servicio, todos éstos ubicados en la provincia de Pichincha. A continuación en la tabla 2.1 se detallan los equipos PEs más importantes pertenecientes a la red VPLS de Pichincha.

#	NODO	NOMBRE	IP/GESTIÓN	MARCA	MODELO
1	MARISCAL	UIOMSCE01	172.168.0.10	CISCO	7613
2	QUITO CENTRO	UIOQCNE01	172.168.0.14	CISCO	7613
3	IÑAQUITO_1	UIOINQE01	172.168.0.18	CISCO	7613
4	VILLAFLORA	UIOVLFE01	172.168.0.20	CISCO	7613
5	ESTACIÓN TERRENA	UIOETTE01	172.168.0.26	CISCO	7609-S
6	VILLAFLORA	UIOVLFE01	172.168.0.28	CISCO	7609-S
7	GUAJALÓ	UIOGJLE01	172.168.0.30	CISCO	7609-S
8	PINTADO	UIOPTDE01	172.168.0.32	CISCO	7609-S
9	SANGOLQUÍ	UIOSGQE01	172.168.0.34	CISCO	7609-S

#	NODO	NOMBRE	IP/GESTIÓN	MARCA	MODELO
10	GUAMANÍ	UIOGMNE01	172.168.0.36	CISCO	7609-S
11	MONJAS	UIOMNJE01	172.168.0.38	CISCO	7609-S
12	CUMBAYÁ	UIOCBYE01	172.168.0.40	CISCO	7609-S
13	CARCELÉN	UIOCCLE01	172.168.0.42	CISCO	7609-S
14	CALDERÒN	UIOCLDE01	172.168.0.44	CISCO	7609-S
15	COTOCOLLAO	UIOCTCE01	172.168.0.46	CISCO	7609-S
16	LA LUZ	UIOLLZE01	172.168.0.48	CISCO	7609-S
17	CONDADO	UIOCNDE01	172.168.0.50	CISCO	7609-S
18	QUINCHE	UIOQCHE01	172.168.0.52	CISCO	7609-S
19	CAYAMBE	UIOCAYE01	172.168.0.54	CISCO	7609-S
20	MACHACHI	UIOMCHE01	172.168.0.56	CISCO	7609-S
21	LA FLORIDA	UIOLFLE01	172.168.0.60	CISCO	7606-S
22	MONTESERRÍN	UIOMSRE01	172.168.0.61	CISCO	7606-S
23	LAS CASAS	UIOLCSCE02	172.168.0.62	CISCO	7606-S
24	LAS CASAS	UIOLCSE01	172.168.0.64	CISCO	7606-S
25	CARONDELET	UIOCRDE01	172.168.0.63	CISCO	7606-S
26	LA PAZ	UIOLPZE01	172.168.0.65	CISCO	7606-S
27	ESCUELA ESPEJO	UIOEEPE01	172.168.0.67	CISCO	7606-S
28	COLLALOMA	UIOCLME01	172.168.0.69	CISCO	7606-S
29	LA BOTA	UIOLBTE01	172.168.0.70	CISCO	7607-S
30	TUMBACO	UIOTMBE01	172.168.0.72	CISCO	7606-S
31	SAN ISIDRO DEL INCA	UIOSNIE01	172.168.0.73	CISCO	7606-S
32	LOS NEVADOS	UIOLNVE01	172.168.0.74	CISCO	7606-S
33	CARAPUNGO	UIOCRPE01	172.168.0.79	CISCO	7060-S

#	NODO	NOMBRE	IP/GESTIÓN	MARCA	MODELO
34	QUITO CENTRO	UIOQCNE02	172.198.100.10	CISCO	7613-S
35	IÑAQUITO	UIOINQE02	172.198.100.11	CISCO	7613-S
36	MARISCAL	UIOMSCE02	172.198.100.12	CISCO	ME-6524
37	MARISCAL	UIOMSCE03	172.198.100.26	CISCO	ME-6524
38	LA CAROLINA	UIOLCLE02	172.198.100.19	CISCO	7060-S
39	MARISCAL	UIOMSCE04	172.198.100.210	CISCO	ME-6524

Tabla 2. 1: Equipos PE de la red MPLS de la CNT EP

2.4.1 INTERCONEXIÓN DE EQUIPOS PES EN LA PROVINCIA DE PICHINCHA/QUITO

El diagrama de topología de los equipos PE de la red MPLS de la CNT EP es presentado en la figura 2.1 en la cual se detalla además de los equipos PE, la interconexión con el core MPLS.

Se utiliza una nomeclatura la cual diferencia los diferentes tipos de routers, de core y distribución. De cada equipo se presenta su nombre y la interconexión a nivel de Core y distribución, cada uno con sus enlaces principales y redundantes. Cabe recalcar que los equipos que se presentan son los equipos PE de Pichincha/Quito que participan en el servicio VPLS.

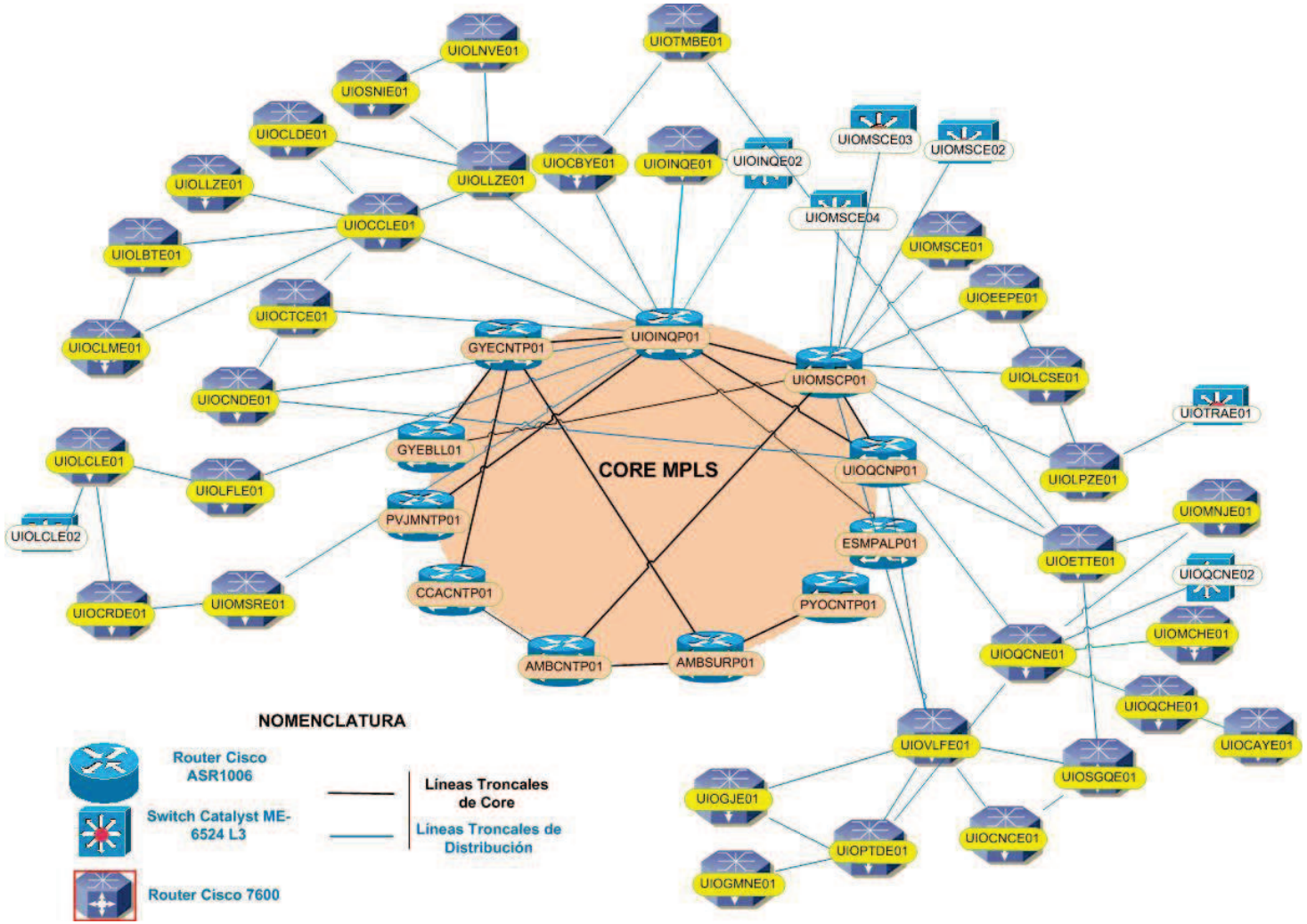


Figura 2. 1: Diagrama de interconexión PEs en Pichincha/Quito

2.5 CLIENTES ISP A ANALIZAR

Se ha considerado para este análisis los siguientes argumentos:

1. ISP clientes conectados a los equipos PE que manejan gran cantidad de tráfico.

2. ISP con un número considerable de clientes finales en la ciudad de Quito.

3. Criterio del personal que administra las VPLS que provee la CNT EP, por motivos de tener mayor historial de problemas reportados referentes al servicio por parte de los clientes.

Por lo mencionado anteriormente los ISPs a analizar son los ubicados en los equipos UIOINQE01 y UIOLCLE01 con sede en Quito. Se realizará el análisis de la VPLS interna de la CNT EP, la que es utilizada para el servicio de FAST-BOY a clientes finales residenciales, denominada IP FIJA.

A cada ISP, se lo nombrará con la nomenclatura ISP-X, donde X tomará el valor del 1 al 16.

En la tabla 2.2 se detalla los clientes ISPs a analizar, e IP FIJA, con la respectiva información que comprende: Nombre del ISP, Equipo PE de Interconexión, IP de gestión del equipo, Troncal de conexión y Circuito virtual asociado a la VPLS.

VPLS	NOMBRE	EQUIPO PE	IP/GESTION PE	TRONCAL	VC
ISP-1	ALIANZANET	UIOLCLE01	172.168.0.62	G5/2	313
ISP-2	BRAVCO	UIOINQE01	172.168.0.18	Gi 4/0/1	327
ISP-3	BRIGHCELL	UIOLCLE01	172.168.0.62	Fa2/4	328

VPLS	NOMBRE	EQUIPO PE	IP/GESTION PE	TRONCAL	VC
ISP-4	ENTREPRENEUR	UIONQE01	172.168.0.18	Gi 12/41	339
ISP-5	ESPOLTEL	UIOLCLE01	172.168.0.62	Gi5/2	322
ISP-6	GLOBAL CROSSING	UIOINQE01	172.168.0.18	Gi 13/39	343
ISP-7	MEGADATOS	UIOINQE01	172.168.0.18	Gi 12/2	303
ISP-8	MICROSISTEMAS	UIOINQE01	172.168.0.18	Gi13/32	345
ISP-9	MILLTEC	UIOLCLE01	172.168.0.62	Fa 2/32	352
ISP-10	NOVANET	UIOINQE01	172.168.0.18	Gi13/3	315
ISP-11	POWERFAST	UIOINQE01	172.168.0.18	Fa2/1	307
ISP-12	PUNTO NET	UIOINQE01	172.168.0.18	Gi 13/2	305
ISP-13	SOLUVIGOTEL	UIOLCLE01	172.168.0.62	Fa2/40	314
ISP-14	TAMBILLONET	UIOINQE01	172.168.0.18	Gi 4/0/1	312
ISP-15	TELYDATA	UIOINQE01	172.168.0.18	Gi 4/0/1	304
ISP-16	TELEFONICA	UIOINQE01	172.168.0.18	Gi 4/0/1	309
IP FIJA	FAST BOY	UIOINQE01	172.198.100.11	Gi 4/0/1	202

Tabla 2. 2: Descripción de Clientes ISPs a analizar

2.5.1 INTERCONEXIÓN DE ISPs

A continuación en la figura 2.2, se presenta la ubicación de los ISP a analizar en la red topológica MPLS de la CNT EP, se consideran únicamente los equipos en donde se conectan los ISP clientes y sus respectivos backup, así como de la IP FIJA. Como se puede observar la mayor concentración de ISPs se encuentran en los equipos UIOINQE01 Y UIOLCLE01, el resto de equipos PE están relacionados a brindar el servicio a estos ISPs.

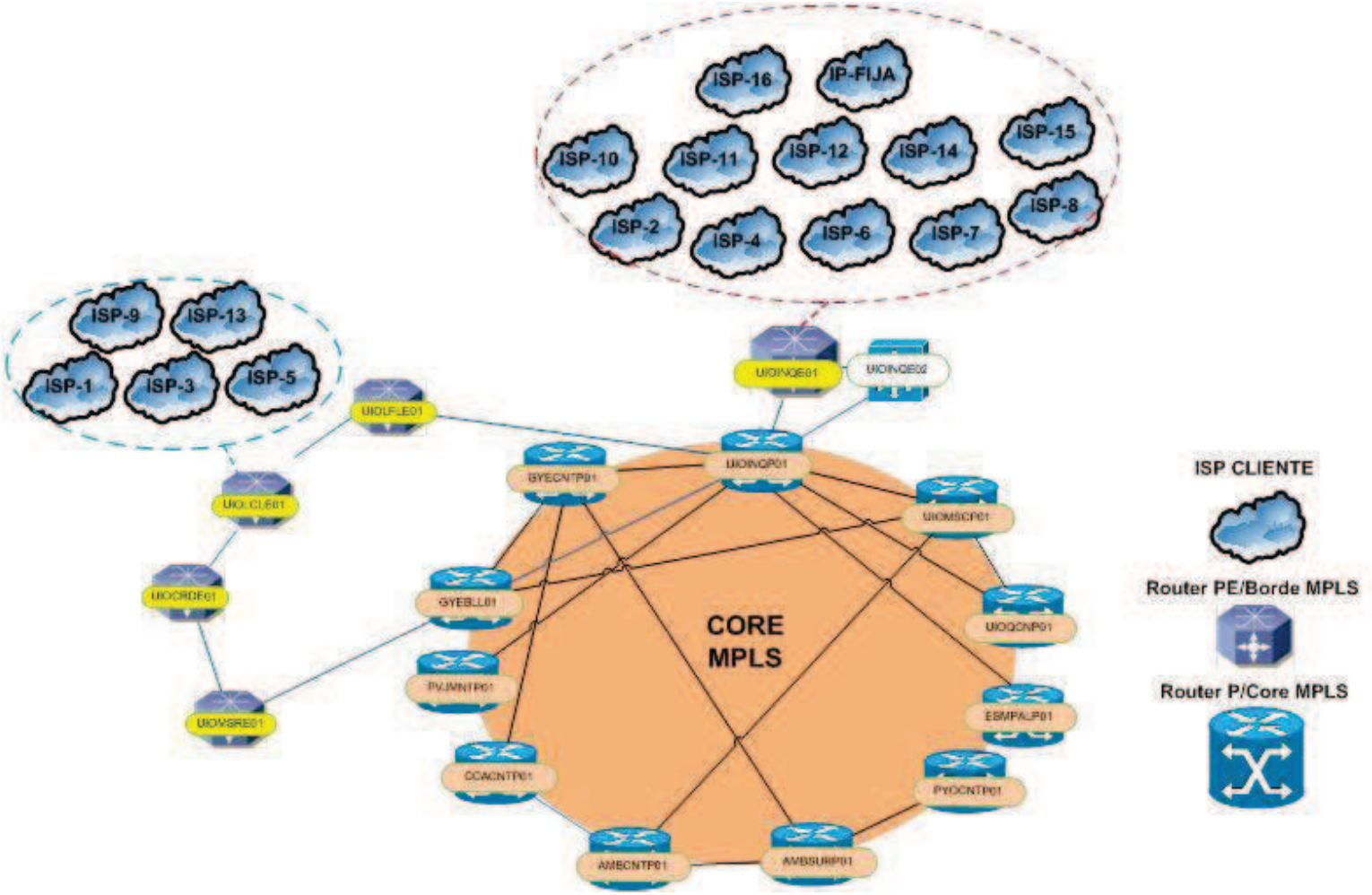


Figura 2. 2: Diagrama de interconexión de ISPs

2.5.2 SITUACIÓN ACTUAL DEL SERVICIO VPLS DE LOS ISPs A ANALIZAR

A continuación se detalla la representación lógica de los ISPs, como ejemplo se presenta la red VPLS el ISP 15, indicando los elementos que la comprenden; el circuito virtual desde el equipo PE troncal hacia sus respectivos PEs Remotos geográficamente distantes, denominados equipos de acceso, estos equipos permiten la inteconexión de distintas sedes del cliente. De cada equipo se presentan nombres, direcciones IPs e interfaces, los ISPs restantes se encuentran en el Anexo A.

2.5.2.1 Red VPLS ISP-15

El ISP-15 está directamente conectado al equipo **UIOINQE01** a través de la interfaz Gi4/0/1, el circuito virtual de conexión es el VC 304, todos los equipos de acceso tienen el mismo identificador VPN-ID 304. En la figura 2.3 se presenta el esquema de la Red VPLS de este ISP.

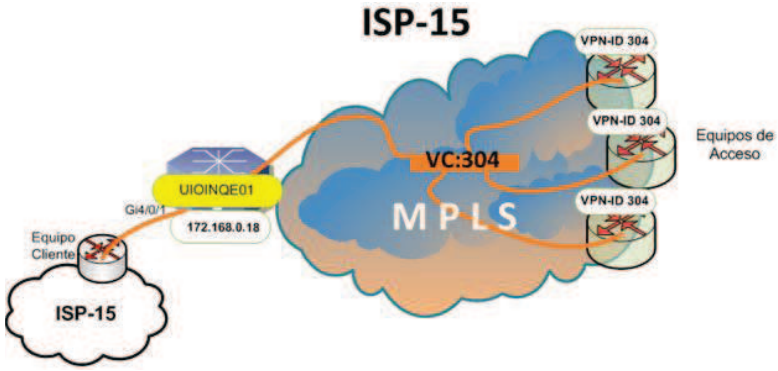


Figura 2. 3: Diagrama interconexión VPLS ISP-15

2.6 TIPOS DE CLIENTES ABONADOS [4], [23]

La oferta de servicios de voz y datos a clientes de la CNT EP es categorizada en dos grupos, los clientes masivos y los corporativos. Cada uno de ellos con diferentes

servicios de transporte siendo así que para los masivos se utiliza el mencionado servicio VPLS con una comunicación punto a multipunto, esquema utilizado también para los ISPs.

Mientras que para los corporativos se hace uso de las VRF (Virtual Routing and Forwarding) tecnología conocida como VPNs de enrutamiento y reenvío de sitios locales y remotos de los clientes, que permite tener múltiples tablas de rutas separadas, las cuales pueden coexistir en el mismo router y al mismo tiempo.

Al ser todas las tablas de rutas completamente independientes, las mismas direcciones IP que pueden solapar con otras existentes, evitan conflictos y pueden convivir sin problemas.

Es decir para cada cliente VPN se tiene un router PE dedicado, el cual transporta sus propias rutas y crea las tablas de enrutamiento, únicamente con las rutas anunciadas por sus clientes VPN conectados a ellos. Lo que permite un mayor control de los mismos ya que garantiza conexiones privadas a los servicios de sus intranets tales como:

- Multicast (Videoconferencias multipunto).
- Soporte de Telefonía mediante VPNs.
- Servicios Centralizados (web hosting).

2.6.1 RED DE TRANSPORTE DE VOZ Y DATOS

El esquema de la red para el transporte de voz y datos en los servicios masivos residenciales de la CNT EP se indica en la figura 2.4.

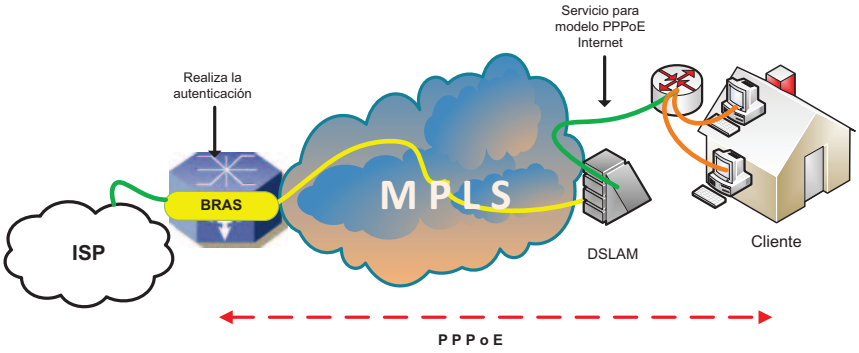


Figura 2. 4: Modelo de Internet PPPoE

Los clientes acceden al servicio a través de un módem, que actúa como conmutador entre el tráfico IP de la interfaz Ethernet y su interfaz WAN, el tráfico proveniente de cada uno es concentrado en un dispositivo denominado DSLAM[11] (*Digital Subscriber Line Access Multiplexer/ Multiplexor de línea de acceso digital del abonado*), encargado de procesar el flujo de datos de cada puerto mediante la tecnología ADSL[12] (*Asymmetric digital subscriber line/ Línea de abonado digital asimétrica)* y que posteriormente es multiplexado por el puerto de salida en donde obtiene el tráfico de todos los puertos, cada uno en distintas VLANs.

Este tráfico es enviado a la red MPLS para su transporte, y llega al router de borde que hace la función del BRAS (*Broadband Remote Access Server/ Servidor remoto de acceso de banda ancha*), dispositivo que finaliza las sesiones PPPoE[13] (*Point-to-Point Protocol Over Ethernet/ Protocolo Punto a Punto sobre Ethernet*) que se inician en los PCs del cliente, donde se realiza la autenticación pudiendo ser mediante RADIUS[14] (*Remote Authentication Dial-In User Server / Servicio de Autenticación Remota para Usuario Acceso Telefónico*) para acceder a la red del ISP.

[11] Multiplexor localizado en la central telefónica que proporciona a los abonados acceso a los servicios DSL sobre cable de par trenzado de cobre.
[12] Tecnología que utilizan técnicas de modulación y códigos de línea adecuados para permitir que sobre el par trenzado telefónico se transmitan datos a altas velocidades
[13] Protocolo de red para la encapsulación PPP sobre una capa de Ethernet, utilizada mayoritariamente para proveer conexión de banda ancha mediante servicios de cable módem y xDSL.
[14] Protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.

2.6.1.1 Protocolo de transporte

Mediante la combinación de Ethernet y el Protocolo punto a punto (*PPP*), PPPoE, se proporciona una manera eficaz de crear una conexión independiente para cada usuario a un servidor remoto.

Este protocolo es utilizado en clientes masivos de la CNT EP, como en clientes de ISPs a los que brinda el servicio VPLS, sin embargo existen clientes que hacen uso del protocolo IPoE (*IP over Ethernet/ IP sobre Ethernet)* que utiliza una tecnología de acceso de ADSL de forma más sencilla y eficiente.

La irrupción de este protocolo en el mercado es debido a la necesidad de convergencia de servicios en especial de la TV y el video, cuya naturaleza punto a multipunto necesitan de un nuevo mecanismo de control de la comunicación, necesariamente distinto al PPP.

2.6.1.2 Diferencias entre PPPoE e IPoE [23]

A continuación en la tabla 2.3, se detallan las diferencias entre los protocolos PPPoE e IPoE utilizados para transporte de datos, voz y video a través de una red de agregación en donde convergen estos servicios.

Características	PPPoE	IPoE
Autenticación y Autorización	Los flujos de autenticación se establecen, a través del BRAS, o RADIUS que es quien permite o deniega la comunicación con el usuario en cuestión.	El servidor de autorización podría ser un servidor RADIUS, o incluso el propio servidor DHCP (Protocolo de Configuración Dinámica de Host).
Control de Volumen	Al ser de naturaleza punto a punto, el control de la información se controla por un solo punto centralizado BRAS	Al ser de naturaleza multipunto a multipunto permite una arquitectura distribuida en la que no es necesario un único punto central de paso.

Características	PPPoE	IPoE
Identificación del Usuario.	Utiliza el estándar IEEE 802.1q y/o IEEE 802.1ad (QinQ), donde en cada mensaje enviado por el usuario, el dispositivo de acceso inserta la identificación de la red privada virtual VLAN al que pertenecen (una VLAN por usuario), de manera que cada trama Ethernet se "etiqueta" de acuerdo a esta VLAN.	También emplea estándares 802,1q y/o 802.1ad, para el etiquetado VLAN de las tramas Ethernet; sin embrago con el fin de permitir un mayor flexibilidad a la hora de definir las VLAN, las asigna a cada tipo de servicio en lugar de una por cada usuario para lo cual se utilizará un procedimiento del protocolo DHCP según el cual, el nodo de acceso inserta en el primer mensaje DHCP (el de solicitud de una de una dirección IP), la información del puerto físico que hace dicha petición, quedando el usuario así, identificado.
Seguridad en las comunicaciones	Habitualmente el BRAS establece mecanismos adicionales de seguridad, por ejemplo la creación de listas negras.	Los propios elementos que componen la red de agregación basada en Ethernet/MPLS son los que garantizan la seguridad en las comunicaciones

Tabla 2. 3: Diferencias entre PPPoE e IPoE

Tras este breve análisis, se comprueba que para un servicio punto a punto como se ofrece con el servicio de acceso a internet ambos modelos (PPPoE e IPoE), son capaces de ofrecer, las mismas capacidades con un comportamiento similar.

La principal ventaja del modelo IPoE para este tipo de servicios es la capacidad de implementar los mecanismos de control de tráfico de una manera distribuida, evitando el cuello de botella, que supone el elemento BRAS como elemento único de control, cuya falla llegaría a procesos críticos.

A continuación se detalla la evolución de los servicios de agregación:

- Escenario 1.- En este escenario se tiene el modelo de agregación para el servicio de internet con un único punto de control mediante el BRAS, utilizando el modelo PPPoE para el transporte de datos, ver figura 2.5.

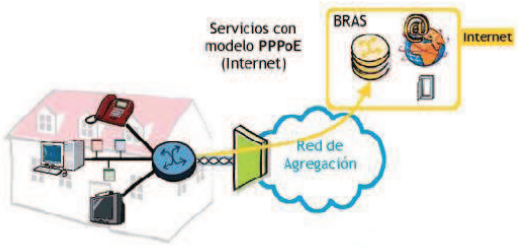


Figura 2. 5: AYER, modelo de agregación para el servicio Internet

- Escenario 2.- En este escenario se evidencia ya el uso en paralelo de PPPoE para lo que es internet e IPoE para servicios tales como IPTv y VoIP, figura 2.6.

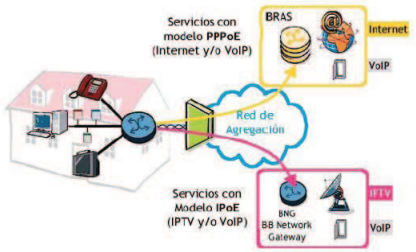


Figura 2. 6: HOY, diferente modelo de agregación para Internet y Video

- Escenario 3.- En este escenario se tiene lo que sería la evolución de los anteriores modelos teniendo un único modelo de agregación para la convergencia real de todos los servicios, ver figura 2.7.

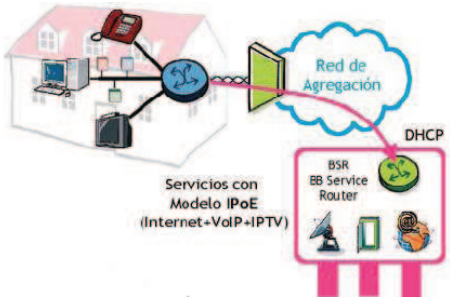


Figura 2. 7: EVOLUCIÓN, modelo de agregación única para todos los servicios

CAPÍTULO 3

DIAGNÓSTICO DEL SERVICIO VPLS

3.1 INTRODUCCIÓN

La detección de fallas y el monitoreo del desempeño de una red son actividades de gran importancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de la utilización de un esquema que permita mostrarnos el comportamiento mediante la recolección de tráfico.

El objetivo del diagnóstico de las redes de datos es identificar problemas, determinar su importancia, analizar sus causas, y adoptar medidas pertinentes en forma inmediata.

La necesidad de determinar el estado actual de desempeño del servicio VPLS que presta la CNT EP, y encontrar el motivo por el cual se ha reportado malestar por parte de sus clientes, es motivo principal para hacer uso de herramientas que permitan obtener estadísticas de tráfico, así como la implementación de medios que permitan obtener dichos datos de una manera sencilla pero segura.

En el presente capítulo se detallan las herramientas y los medios utilizados para el monitoreo de tráfico de las VPLS de interés para la generación de resultados iniciales, así como también se presenta un análisis de los ataques a la seguridad de las VPLS.

Concluido este capítulo y con los resultados obtenidos se podrá tener una visión clara del funcionamiento de las VPLS, y se podrá plantear soluciones para cumplir de una manera satisfactoria los objetivos de este proyecto.

3.2 PARÁMETROS DE ANÁLISIS DEL FUNCIONAMIENTO DEL SERVICIO VPLS [21], [22]

Para detectar los problemas del servicio VPLS que están afectando a los usuarios, se enfocará en el análisis de las conexiones y la detección de posibles problemas en la transmisión de paquetes. La pérdida de paquetes y/o conexión es uno de estos problemas por tal motivo se deben buscar las herramientas adecuadas para detectarlo.

En este caso no se pretende analizar lo que la red de cada ISP transmite, ya que el servicio que ofrece la CNT EP se encarga sólo de su transporte más no de manejar su contenido, así que no se profundizará en el contenido de los paquetes.

Partiendo del hecho de que se trata de un servicio que emula una Red LAN, se debe considerar los motivos por los que puede presentarse problemas de pérdidas de paquetes siendo éstos:

- Tormentas broadcast.
- Dimensionamiento de ancho de banda en la troncal.
- Problemas en el equipamiento de la red (equipos defectuosos).
- Problemas de conexión (problemas de cableado, problemas en conectores), etc.

Descartando los problemas físicos que pueden presentarse, se debe asegurar que la parte lógica de la red esté funcionando correctamente, de tal manera que se hace un enfoque de análisis a los 2 primeros puntos mencionados.

3.2.1 TORMENTAS BROADCAST

3.2.1.1 Descripción

Se procede hacer la estimación de la existencia de factores que pueden producir inundaciones de broadcast en la VPLS y ser causantes de degradar el servicio. La descripción de una tormenta broadcast se encuentra en el Capítulo 1, sección 1.6.2.

Aplicaciones de alto nivel y algunos protocolos utilizan paquetes broadcast, los protocolos más relevantes son:

- ***ARP (Address Resolution Protocol/ Protocolo de Resolución de Direcciones)***

Es un protocolo empleado por los hosts para conocer las direcciones MAC de equipos con determinada dirección IP. Esta información es almacenada en la caché interna de cada host dentro de una tabla ARP.

Esta tabla puede incluir entradas dinámicas (aquellas que se añaden y se borran automáticamente a lo largo del tiempo, con un tiempo de vida máximo), y entradas estáticas (que permanecen en la caché hasta que se reinicia el equipo).

- ***NetBIOS (Network Basic Input/Output System / Sistema Básico de entrada y salida de Red)***

Es un protocolo que funciona a nivel de capa de aplicación y es exclusivo de redes Windows. Se utiliza para asignar nombres y workgroups a las workstations y sirve fundamentalmente para compartir archivos e impresoras y para ver los recursos disponibles en redes Windows.

3.2.1.2 Afectación

El tráfico broadcast es necesario en el funcionamiento de los protocolos que operan una red, permite la comunicación de un terminal origen a todas las terminales de un mismo dominio, pero representa un problema cuando se presenta en forma excesiva.

La presencia de una tormenta de broadcast se considera un riesgo para la red por los siguientes motivos:

- Porque inunda la red utilizando ancho de banda innecesariamente.
- Porque consume recursos de los dispositivos que deben procesar este broadcast.
- Porque consume recursos de las terminales y servidores que reciben el broadcast y deben analizarlo.
- Porque genera inestabilidad de las tablas MAC Address.

En general una tormenta de broadcast causa deficiencia en el funcionamiento de la red, ya que utiliza una cantidad importante de ancho de banda que como consecuencia produce la pérdida de paquetes al caducar su TTL (tiempo de vida).

3.2.2 DIMENSIONAMIENTO DE ANCHO DE BANDA EN LA TRONCAL

3.2.2.1 Descripción

Un puerto en un equipo PE es utilizado para ser la troncal de varios clientes ISPs para proveer el servicio, como producto de esto la capacidad de ancho de banda del puerto se satura.

3.2.2.2 Afectación

- Se percibe lentitud en el servicio por parte de los usuarios.
- Afectación en el servicio a los clientes conectados en el puerto troncal.
- Descarte de paquetes al llegar a la capacidad máxima del puerto.

3.3 HERRAMIENTAS PARA EL DIAGNÓSTICO DE LAS VPLS [5], [15], [25]

Para monitorear las redes existen múltiples herramientas, muy simples y otras muy complejas, su utilización depende del grado de profundidad de análisis que se desee.

Para realizar un diagnóstico de la funcionalidad de las VPLSs, se eligió utilizar herramientas que permitan dar un estado general de las mismas, éstas son de fácil manejo como Wireshark, Cacti (herramienta ya utilizada en la CNT) y con ayuda de los comandos de gestión de IOS propios de los equipos.

Estas herramientas permiten obtener una visión completa y necesaria del estado de las VPLS, se consideran como herramientas suficientes para determinar las posibles fallas y poder plantear las mejorías al servicio.

Puede haber más métodos para detectar problemas en las VPLSs sin embargo lo que se desea en este proyecto es la detección rápida y de una manera general de aquellos factores que degraden el servicio.

La información sobre cada herramienta utilizada para el monitoreo del servicio VPLS, se describe en el Anexo B.

3.3.1 WIRESHARK

Para realizar el monitoreo de los paquetes de las VPLSs, se utilizó la herramienta Wireshark, ya que es de fácil instalación con GUI (Interfaz Gráfica de Usuario) y que proporciona el detalle de los paquetes capturados.

Esta herramienta ayudará a determinar si existe pérdida de paquetes por presencia de exceso de tráfico broadcast.

Se escogió Wireshark porque implementa una gama de filtros que facilitan la definición de criterios de búsqueda para los diferentes protocolos mediante una interfaz sencilla.

3.3.2 CACTI

Esta herramienta es utilizada actualmente por la administración de tráfico de CNT E.P., donde se monitorizan los equipos de la red y está administrado bajo la responsabilidad del Área O&M Plataforma IP/MPLS de CNT E.P.

Con Cacti se podrá esquematizar lógicamente el transporte del tráfico en el servicio VPLS de cada ISP. Como parte del análisis se realizaron los respectivos diagramas de cada ISP, para observar el comportamiento del tráfico por cada VPLS.

Con esta herramienta se puede administrar el tráfico de todos los equipos gestionados por el Área O&M Plataforma IP/MPLS de CNT E.P., son muchas las opciones avanzadas que presta este software para realizar análisis más profundos y complejos. Sin embargo para cumplir con el objetivo de monitoreo de las VPLS, no se requiere detallar todo el funcionamiento y opciones que éste presenta; pese a esto se debe explicar claramente como es la obtención de datos para poder realizar las respectivas gráficas de cada ISP.

3.3.3 COMANDOS IOS DE CISCO

La interfaz de comandos del IOS es el método más común para la configuración y administración del servicio VPLS. Mediante la ejecución de sentencias se puede obtener la información específica de acuerdo al requerimiento.

3.4 ANÁLISIS DE LA SITUACIÓN ACTUAL DEL SERVICIO VPLS

3.4.1 OBJETIVO

En esta sección se exponen las herramientas a utilizar para los parámetros de análisis identificados anteriormente, además se indican los criterios utilizados para el tratamiento de cada parámetro y el proceso realizado para obtener los resultados de cada herramienta.

3.4.2 IDENTIFICACIÓN DE LA HERRAMIENTA

De acuerdo a la descripción de las herramientas realizada en la sección 3.3 e identificado el parámetro de análisis, se establece la tabla 3.1, donde se identifican las herramientas seleccionadas que reflejan de mejor manera el resultado de cada parámetro.

Herramienta / Parámetro	Wireshark	Cacti	Comandos IOS Cisco
Tormentas Broadcast	% pérdida de paquetes e identificación de tráfico broadcast		% variación de MACs
Dimensionamiento de ancho de banda en la troncal		Saturación de puertos troncales y consumo VPLS	Identificar el puerto troncal de la VPLS

Tabla 3. 1: Herramienta de análisis VPLSs

3.4.3 CRITERIOS DEL TRATAMIENTO DEL ANÁLISIS

Es aconsejable desarrollar un enfoque adecuado para clasificar los parámetros a analizar de acuerdo a criterios. Estos criterios se establecen mediante el paradigma cualitativo basándose en escalas que permitan clasificar los resultados conjuntamente con una puntuación numérica para llegar a una estimación lo más exacta posible, no se aplicó la metodología cuantitativa ya que reclama cálculos matemáticos complejos.

3.4.3.1 Criterio de muestras

3.4.3.1.1 Porcentaje de pérdida de paquetes e identificación de broadcast

- **Criterio de porcentaje de pérdida de paquetes**

El criterio para establecer el porcentaje de pérdida de paquetes se obtiene con la herramienta Expert Info Composite de Wireshark, dentro de esta existen dos parámetros Error y Advertencia que se explican en más detalle en el Anexo B, la suma de ambos resultados (el total de Error y un porcentaje de Advertencias) dan el cálculo de pérdida de paquetes en valor porcentual.

Para obtener el porcentaje promedio de advertencias y que éste sea un dato conocido, se obtuvo el promedio de muestras de capturas de los ISPs y dentro de los paquetes de advertencias se observó los del grupo **TCP Previous Segment Lost,** los cuáles indican que durante el curso de transferencia de datos un paquete se ha perdido.

Como se observa en la figura 3.1 el total de Advertencias es de 114089 paquetes y el total correspondientes a TCP Previous Segment Lost es de 4336 donde se obtiene que el valor porcentual de los paquetes perdidos es 3,8 %.

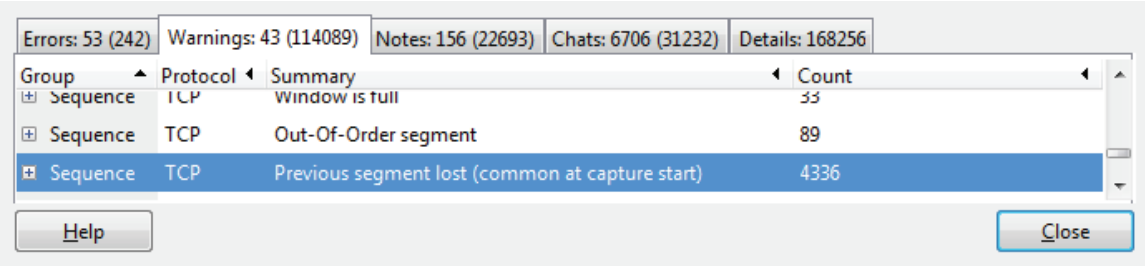


Figura 3. 1: Muestra 1, obtención porcentaje Advertencias

En una segunda muestra, figura 3.2: del total de Advertencias (3778) se obtiene que el valor porcentual de los paquetes perdidos es 5,45 %.

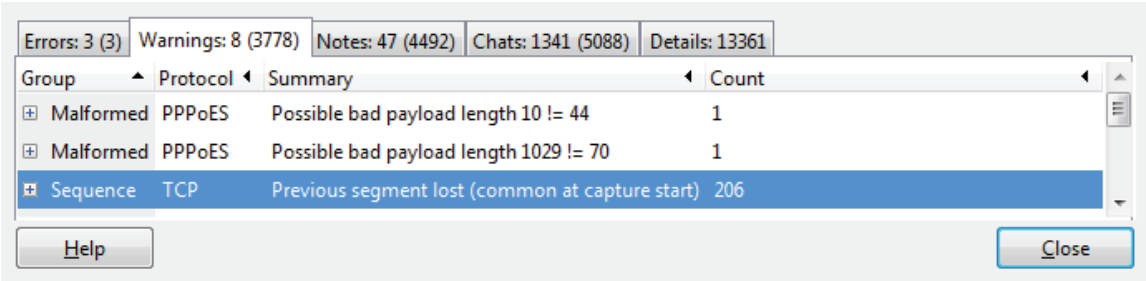


Figura 3. 2: Muestra 2, obtención porcentaje Advertencias

Al realizar el promedio de 5 muestras el resultado fue de 4,6%, que se lo aproximó al valor de 5% para tener un dato conocido como porcentaje de paquetes perdidos del total de advertencias.

Finalizando este criterio se tiene que el total de paquetes perdidos corresponde a la suma de Errores y el 5% de Advertencias.

$$\% \text{ Paquetes perdidos} = \left(\frac{Paquetes\ con\ Error + 5\%\ Paquetes\ con\ Advertencias}{Paquetes\ Totales}\right) * 100$$

Con el porcentaje de pérdida de paquetes se puede deducir si el análisis cumple o no con el valor aceptable que corresponde al porcentaje límite permitido de pérdida de paquetes especificados en los estándares SLA[15] de la CNT que se indica en la tabla 3.2.

Parámetro	Descripción	Valor en porcentaje	< 1%	> 1%
Pérdida de paquetes	Máximo de paquetes perdidos	1%	Aceptable	No Aceptable

Tabla 3. 2: Parámetro SLA de CNT: Pérdida de Paquetes

- **Criterio de identificación de tráfico broadcast**

El criterio para la identificación de tráfico broadcast se realizó con la herramienta IO Graphs la cual puede filtrar los paquetes de interés, y estimar la relación del tráfico total comparado con el tráfico de los protocolos que generan broadcast.

No es posible obtener un valor porcentual o cuantitativo con esta herramienta, sin embargo se puede obtener una ayuda utilizando el método visual que justifica la comparación de dos escenarios que evocan similitudes o diferencias para la descripción del problema, en base a esto se puede considerar si existe o no exceso de tráfico broadcast en relación al tráfico total.

En la tabla 3.3 se tiene una leyenda representada por colores y clasificada de acuerdo a la cantidad de paquetes filtrados por unidad de tiempo (Broadcast, ARP y NBNS) para más detalle de los protocolos referirse a la sección 3.2.1.

[15] Service Level Agreement (SLA)/ Acuerdo de nivel de servicio: Contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

	Parámetro
	Tráfico Total
	Broadcast
	ARP
	NBNS

Tabla 3. 3: Leyenda de tráfico, IO Graphs

3.4.3.1.2 Porcentaje de variación de MACs

El criterio para determinar el nivel de aceptación de la variación porcentual de MACs se realiza con el cálculo del coeficiente de variación estimado *(cve)*, el cual mide la magnitud de la variabilidad de la muestra, es decir, es el indicador del grado de aproximación con que se estiman las características del universo y está dado por:

$$\%\ cve = \frac{desviación\ estándar}{media} * 100$$

En donde la media y la desviación estándar se calculan de la siguiente manera:

N = Número total de la muestra

x = Dato de la muestra

- **Media**

$$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

- **Desviación Estandar**

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \overline{x})^2}$$

- **Interpretación del coeficiente de variación**

De acuerdo a datos obtenidos a partir de estudios estadísticos realizados para determinar los valores de aceptabilidad del Cve de muestras, se tiene la siguiente escala:

Cve Óptimo: (0–7) %
Cve Aceptable: (8-14) %
Cve Medianamente Aceptable: (15-19) %
Cve No Aceptable: (20-100) %

Sin embargo debido a la criticidad que representa tener variación de aprendizaje MAC en los equipos, se consideró un umbral de máxima variación de acuerdo a la comparación con los ISPs que presentaron pérdidas de paquetes dentro del SLA establecido, se encontró que el valor máximo de variación MAC fue de 9,9 % que se lo aproximó al 10%, lo que implica que un valor mayor a este se lo considera como No Aceptable.

La tabla 3.4 presenta la interpretación de variación MAC de acuerdo al criterio indicado.

VALORACIÓN		DESCRIPCIÓN
(0-10)%	ACEPTABLE	Variación de MACs tolerable.
(11-100)%	NO ACEPTABLE	Variación de MACs no tolerable.

Tabla 3. 4: Interpretación coeficiente de variación

3.4.3.1.3 Saturación de puertos troncales y consumo VPLS

El criterio para determinar si una troncal está saturada se basa en la observación de los gráficos de cada VPLS en Cacti, donde se utiliza una leyenda representada por colores y clasificada de acuerdo al porcentaje del tráfico total que circula por los enlaces en el instante de captura, considerando entre 0 y 100% la capacidad del puerto físico, ver tabla 3.5:

	Porcentaje	Utilización de AB
	0-1%	Nulo
	1-10%	Muy Bajo
	10-25%	Bajo
	25-40%	Medianamente Moderado
	40-55%	Moderado
	55-70%	Medianamente Alto
	70-85%	Alto
	85-100%	Saturado

Tabla 3. 5: Leyenda Cacti

Las VPLS donde se observe que la capacidad de su troncal está dentro del valor de 85 y 100% se considera saturada.

3.4.4 PROCEDIMIENTO DE ANÁLISIS

El proceso de monitoreo y de obtención de muestras para cada ISP se realizó en el periodo de una semana de lunes a viernes, entre las 10:00 y 16:00 (horarios de mayor ocupación del canal) y se estimó los resultados de acuerdo a los criterios de la sección 3.4.3.1.

Con el fin de evitar presentar información repetitiva puesto que todos los ISPs requieren el mismo proceso de análisis, se tomó como ejemplo a uno de los ISPs que presentó reportes de problemas por parte de los clientes, siendo éste el ISP 15 cuyas especificaciones generales se encuentran en el capítulo 2 sección 2.5. Al final se presenta un resumen de los resultados obtenidos de cada ISP cuyo resultado individual se encuentra en el Anexo D.

3.4.4.1 Análisis de tormentas Broadcast

De acuerdo a la tabla 3.1 para analizar este parámetro se hace uso de la herramienta Wireshark y comandos IOS de cisco.

3.4.4.1.1 Monitoreo con Wireshark [24]

A pesar de que normalmente se instala Wireshark en el propio equipo donde se quiere analizar el tráfico, se encuentran situaciones en las cuales no se puede tener acceso físico al equipo o no se puede instalar el software en el mismo, como es el caso de routers o switches. En este caso se puede utilizar alternativas en el uso de técnicas que permitan llevar a cabo una captura de tráfico sin necesidad de portar Wireshark en el equipo de interés.

En un esquema como es el de la red de VPLS, lo que se quiere analizar es el tráfico de las VPLS respectivas para lo cual se desea capturar paquetes de los equipos PE, la solución que se utilizó fue instalar Wireshark en una máquina para conectar al equipo PE perteneciente al servicio y poder capturar el tráfico, el esquema planteado es el que se observa en la figura 3.3.

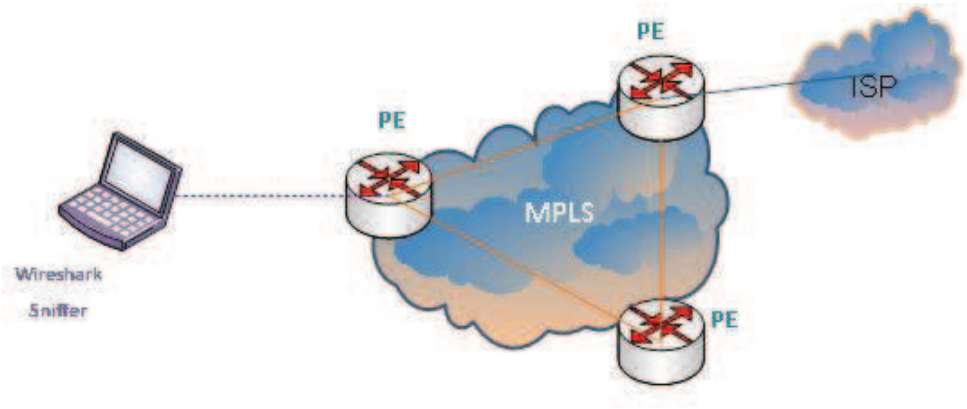


Figura 3. 3: Esquema monitoreo con Wireshark

- **Replicación de Tráfico de Puertos – Port-mirroring**

Para poder hacer uso de la herramienta Wireshark, una vez instalada, se debe buscar el medio para poder realizar las capturas de tráfico de cada VPLS para posteriormente analizarlas.

Los equipos PE que proveen el servicio VPLS a los ISPs se encuentran en diferentes lugares, por lo que no se puede tener acceso directo a cada uno de ellos para capturar el tráfico.

Por tal motivo se hace uso de un espejo *"Port-mirroring",* para que refleje el tráfico de las VPLS, dicho modo de trabajo, denominado modo SPAN en entornos Cisco, permite duplicar el tráfico que transcurre por un puerto del equipo que queremos analizar a otro puerto en el equipo al que se puede tener acceso físico, a este puerto se lo debe configurar como Port-mirroring y éste tiene que ser tan rápido como el puerto a monitorizar para evitar pérdida de tramas.

Para no generar mayor uso de recursos en equipos PE del servicio VPLS el espejo debe ser configurado en otro equipo donde se pueda realizar las pruebas, cabe aclarar que el tráfico reflejado no afecta el servicio ya que solo se lo realiza para tomar muestras en cortos intervalos de tiempo.

- **Equipo PE del laboratorio para monitoreo con Port Mirroring**

Para realizar el monitoreo de las VPLSs se utilizó un equipo para laboratorio, asignado por el Área O&M Plataforma IP/MPLS de CNT E.P, en el cual se configura el Port-mirroring, este equipo se convierte en un PE más, el cual está conectado lógicamente a los otros PEs pertenecientes al servicio VPLS y de fácil acceso al mismo.

En la tabla 3.6 se presenta la ubicación, nombre, dirección IP y modelo del equipo utilizado para el laboratorio.

UBICACIÓN	NOMBRE	IP	MODELO
MARISCAL	UIOLABE01	172.168.0.191	CISCO7600

Tabla 3. 6: Especificaciones Equipo PE de Laboratorio

- **Conexión a la red IP/MPLS del equipo UIOLABE01**

El equipo UIOLABE01 se encuentra ubicado físicamente en el cuarto de telecomunicaciones del Área O&M Plataforma IP/MPLS de CNT E.P y se conecta hacia el equipo UIOMSCE01 ubicado en el MUX de la zona Mariscal; de esta manera se puede acceder a los otros equipos PE que se conectan a los clientes ISPs de análisis.

En el equipo UIOLABE01 se configura Port-mirroring donde se reflejará el tráfico de todas las VPLS, se selecciona un puerto al que se le conecta la PC de monitoreo, donde está instalada la herramienta Wireshark y desde ahí se realiza las capturas de los paquetes para su posterior análisis.

En la figura 3.4 se presenta un diagrama general del esquema utilizado para el monitoreo de las VPLS con el uso de Wireshark y Port-Mirroring.

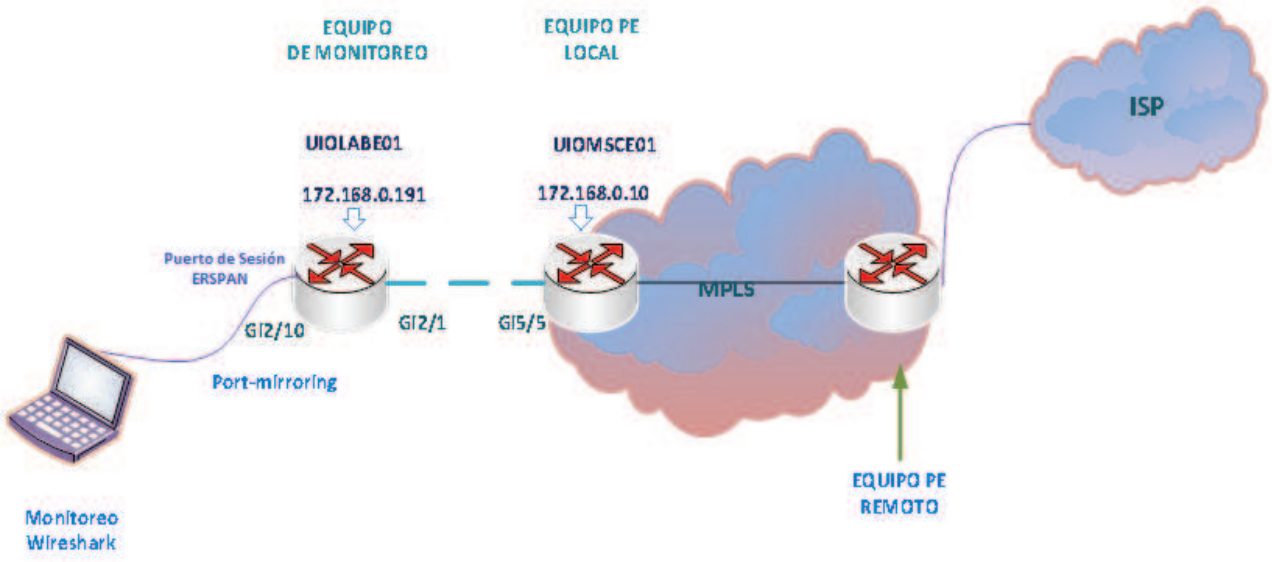


Figura 3. 4: Esquema monitoreo con Wireshark y Port Mirroring

- **Configuración Port-mirroring**

Lo primero que se debe hacer es la configuración del Port-mirroring en el equipo local de laboratorio UIOLABE01 y en el equipo PE remoto UIOINQE01 al cual se conecta al ISP 15.

En este ejemplo se muestra las respectivas configuraciones en los equipos PE correspondientes para el monitoreo del ISP-15. A continuación se presenta la configuración de origen y destino del Port-mirroring, para revisar en detalle éstas configuraciones referirse al Anexo B.

- ***Equipo remoto (Origen)***

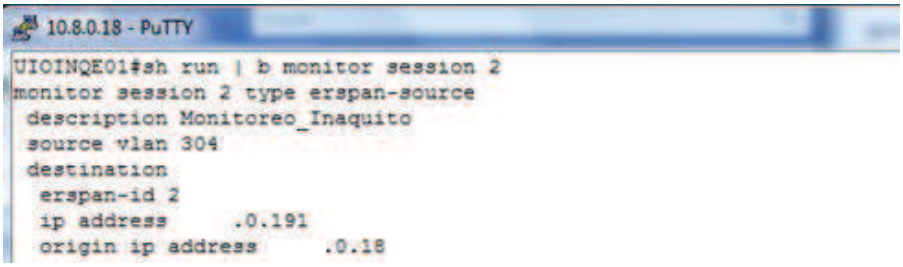


Figura 3. 5: Configuración, Port-mirroring Origen

- ***Equipo local de monitoreo (Destino)***

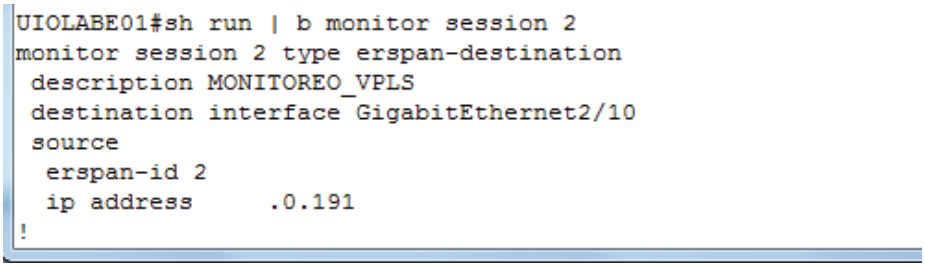


Figura 3. 6: Configuración, Port-mirroring Destino

Esta configuración se hace para cada VPLS, cambiando la configuración en el equipo remoto correspondiente a la VPLS que se desea analizar, en el caso del equipo local (Destino), donde se refleja el tráfico, la configuración se mantiene ya que ese equipo servirá para reflejar el tráfico de todas las VPLS a analizar.

- **Uso de Wireshark**

Con la correcta configuración del Port-mirroring, podemos empezar con la captura de los paquetes con Wireshark. Para este propósito se realizan 3 capturas, donde cada una se capturó en un tiempo estimado de 3 a 5 minutos, ya que en éste periodo de tiempo se pudo obtener muestras con suficiente cantidad de paquetes para poder establecer el porcentaje de pérdidas.

Desde el menú Capture, figura 3.7, se escoge la opción **Interfaces**, para ubicar la interfaz que esté capturando paquetes de la VPLS.

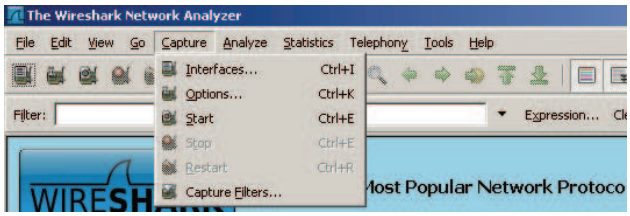


Figura 3. 7: Menú Capture – Wireshark

En la figura 3.8 se observa que en la interfaz eth0 es la que está conectada hacia el puerto Port-mirroring del equipo de laboratorio UIOLABE01, y se procede con el inicio de capturas.

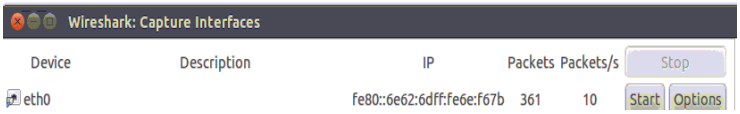


Figura 3. 8: Captura Interfaz– Wireshark

Con los paquetes capturados, se hace uso de las herramientas en Wireshark siendo estas:

- **Info Expert Composite**

Con esta herramienta se puede estimar un porcentaje de los paquetes que posiblemente ocasionan problemas, los principales errores y advertencias, entre éstos se reflejan la pérdida de paquetes.

- **IO Graps**

Mediante el uso de esta herramienta, se puede reflejar la cantidad del tráfico broadcast capturado en relación al tráfico total.

3.4.4.1.2 Datos obtenidos con Wireshark

- **Expert Composite *(Pérdida de Paquetes)***

En la figura 3.9, se presenta la primera captura del ISP-15, dentro del cuadro se despliegan las pestañas de los paquetes con errores (Errors) con un total de 284 paquetes y advertencias (Warnings) con un total de 21430 paquetes. El tamaño de la muestra tomada, es decir el número total de paquetes capturados es de 67022.

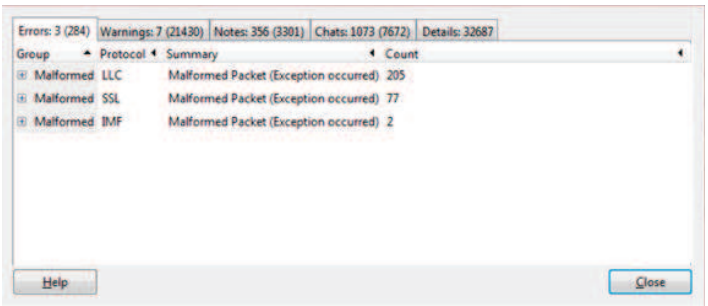


Figura 3. 9: Expert Composite ISP-15, Captura 1

En la figura 3.10 se presenta la segunda captura. El tamaño de la muestra tomada es de 58327.

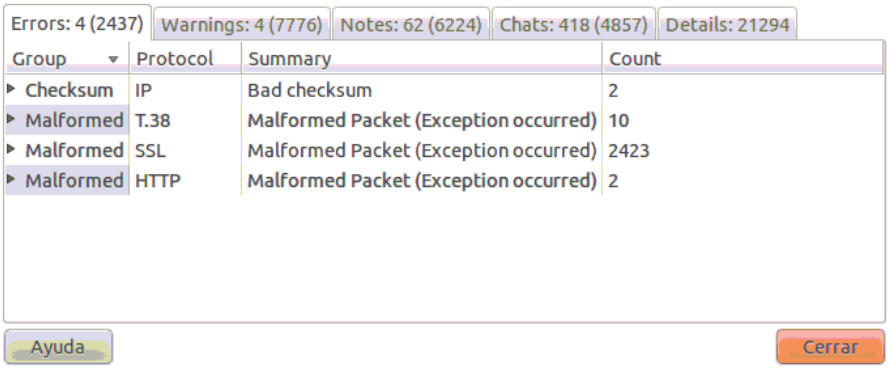


Figura 3. 10: Expert Composite ISP-15, Captura 2

En la figura 3.11, se muestra los resultados de la tercera captura. El tamaño de la muestra tomada es de 50118.

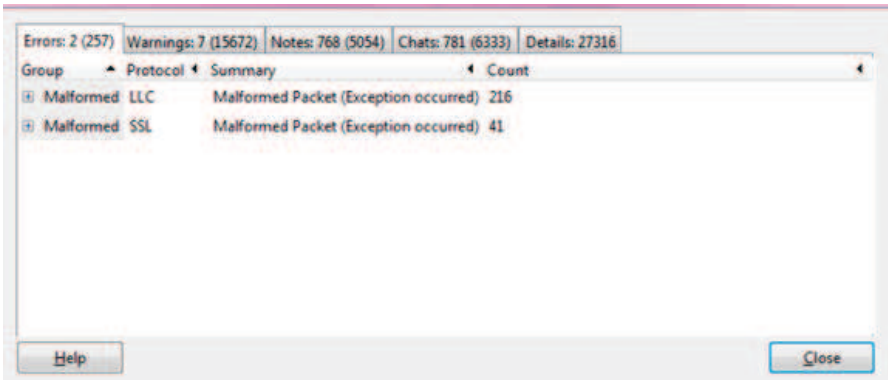


Figura 3. 11: Expert Composite ISP-15, Captura 3

Con los resultados obtenidos se realiza el cálculo del promedio de paquetes perdidos con la fórmula establecida en el criterio de la sección 3.4.3.1.1, que establece el siguiente cálculo:

$$\% \text{ Paquetes perdidos} = \left(\frac{Paquetes\ con\ Error + 5\%\ Paquetes\ con\ Advertencias}{Paquetes\ Totales}\right) * 100$$

A continuación se presenta la obtención de Porcentaje para la primera muestra, de la misma manera se procede para obtener los porcentajes de las dos muestras restantes.

- **Total de Paquetes: 67022**
- **Paquetes de Errores: 284**
- **Paquetes de Avisos: 21430**

$$\% \text{ Paquetes perdidos} = \left(\frac{Paquetes\ con\ Error + 5\%\ Paquetes\ con\ Advertencias}{Paquetes\ Totales}\right) * 100$$

$$\% \text{ Paquetes perdidos} = 2{,}00\%$$

En la tabla 3.7 se resumen los porcentajes y el promedio obtenido para el ISP-15.

	Captura 1	Captura 2	Captura 3	PROMEDIO	Criterio SLA
ISP 15	2,00 %	4,80%	2,07%	**2,96%**	**No Aceptable**

Tabla 3. 7: Promedio Errores y Warnings ISP-15

- ***IO Graphs (Tráfico Broadcast Vs Total)***

A continuación se presentan las capturas con la herramienta Expert composite del ISP 15.

En la figura 3.12 de la herramienta IO Graphs se presenta la captura de la primera muestra, donde se filtra los protocolos de broadcast.

Para una mejor visualización se escoge unidad de paquete por segundo en una escala automática (Cantidad de paquetes/segundo), que es la obtenida bajo los valores por defecto de IO Graphs.

Figura 3. 12: Captura IO Graphs ISP-15, Captura 1

En la figura 3.13, se presenta los resultados de la segunda muestra para el ISP-15.

Figura 3. 13: Captura IO Graphs ISP-15, Captura 2

En la figura 3.14, se muestra los resultados de la tercera captura para el ISP-15.

Figura 3. 14: Captura IO Graphs ISP-15, Captura 3

3.4.4.1.3 Monitoreo con Comandos IOS de Cisco

Para determinar la variación del aprendizaje MAC de las VPLS en el equipo PE se debe ejecutar el siguiente comando:

Router#show mac-address-table count vlan *vlan-id*

Este comando permite indicar las MAC aprendidas de cada vlan.

Se tomaron 4 muestras por cada ISP, cada una con 40 valores de la cantidad de MACs aprendidas en un periodo máximo de 5 minutos, ya que en ese periodo de tiempo el valor de MACs aprendidas no debe tener un porcentaje representativo de variación.

3.4.4.1.4 Datos obtenidos con Comandos IOS de Cisco

Se presenta el resultado de la ejecución del comando para la primera cantidad obtenida de la primera muestra.

```
UIOINQE01#show mac-address-table count vlan 304

MAC Entries for Vlan 304 :
Dynamic Address Count:                71
Static Address (User-defined) Count:  0
Total MAC Addresses In Use:           71
Total MAC Addresses Available:        98304
```

En la tabla 3.8 se presentan las 4 muestras tomadas para el ISP 15, cada una incluye las 40 variaciones en la cantidad de MACs aprendidas.

MUESTRAS	M ACs aprendidas ISP-15									
MUESTRA 1	71	94	130	99	146	130	99	149	149	151
	67	146	144	143	71	94	143	144	144	142
	141	140	139	137	135	136	137	138	134	133
	134	133	124	122	119	119	120	121	120	121
MUESTRA 2	113	123	99	126	128	129	92	125	122	110
	90	110	115	109	81	122	80	120	99	125
	113	123	99	126	128	129	92	125	122	110
	90	110	115	109	81	122	80	120	99	125
MUESTRA 3	99	88	87	98	101	56	45	23	44	55
	111	119	118	138	102	111	134	133	124	122
	99	88	87	98	101	56	45	23	44	55
	111	119	118	138	102	111	134	133	124	122
MUESTRA 4	110	88	120	138	122	121	134	90	125	122
	122	121	120	89	122	88	121	109	120	87
	110	115	120	110	122	121	120	90	125	122
	122	121	120	119	122	88	121	109	120	87

Tabla 3. 8: Muestras MAC ISP-15

Con los resultados obtenidos se realiza el cálculo del promedio de porcentaje de variación de MACs aprendidas con la fórmula establecida en el criterio de la sección 3.4.3.1.2, que establece el siguiente cálculo:

*% cve= (desviación estándar/media)*100*

A continuación se presenta la obtención de Porcentaje para la primera muestra, de la misma manera se procede para obtener los porcentajes de las tres muestras restantes.

Desviación estándar: 22,1

Media: 126,5

*% Cve= (desviación estándar/media)*100%*

Cve = 17,4 %

En la tabla 3.9 se resumen los porcentajes y el promedio obtenido para el ISP-15.

	Muestra 1	Muestra 2	Muestra 3	Muestra 4	PROMEDIO	Valoración
ISP 15	17,4 %	14%	35%	12,3%	**19,7%**	**No aceptable**

Tabla 3.9: Promedio Variación MAC ISP-15

3.4.4.1.5 VPLS inactivas

Para determinar las VPLS inactivas se ejecuta el comando de la sección 3.4.4.1.3. Con el uso del comando indicado en la sección 3.4.4.1.3 se identifica también si la VPLS se encuentra inactiva; las muestras donde el aprendizaje MAC es igual a cero indican que la misma no transporta tráfico.

3.4.4.1.6 Datos obtenidos de VPLSs inactivas

Se presenta el resultado de la ejecución del comando para el caso de una VPLS identificada como no activa, en este caso se toma como ejemplo el ISP 1.

```
UIOLCLE01#show mac-address-table count vlan 313

MAC Entries for Vlan 313:
Dynamic Address Count:                0
Static Address (User-defined) Count:  0
Total MAC Addresses In Use:           0
Total MAC Addresses Available:        65536
```

Las VPLSs que se identifican en estado inactivo no son tomadas en cuenta para el desarrollo de análisis, los resultados correspondientes de las capturas realizadas se indican en el Anexo C, y corresponden a los siguientes ISPs:

- ISP 1
- ISP 4
- ISP 5
- ISP 9
- ISP 14
- ISP 16

3.4.4.2 Análisis de saturación de puertos troncales, consumo VPLS e identificación del puerto troncal de la VPLS

3.4.4.2.1 Monitoreo con Cacti e IOS de Cisco

De acuerdo a la tabla 3.1 para analizar este parámetro se hace uso de los comandos IOS Cisco y de la herramienta Cacti.

Esta herramienta ya se encontraba implementada para monitoreo de la red IP/MPLS, de tal manera que se realizaron los diagramas de conexión de cada VPLS, para éste propósito se identificó el puerto troncal de la VPLS mediante los siguientes comandos:

- Para indicar los puertos por donde cruza la VLAN, posteriromente se puede obtener la descripcion de cada uno e identificar cual es la troncal del cliente.

Router#show vlan all-port

- De las interfaces obtenidas con el comando anterior se procede a identificar cuál de éstas corresponde a la troncal de la VPLS.

Router#show interface [interface] description

El diagrama realizado consta de 4 enlaces que representan la interconexión de la VPLS y son:

- *Enlace ISP - Equipo PE:* Éste enlace representa el tráfico de entrada hacia la troncal del ISP, este puerto troncal además de transportar el tráfico de este ISP, transporta tráfico de otros ISPs, de los cuales también es puerto troncal, cada puerto está representado con su máxima capacidad. La capacidad de los puertos es de 100 Mbps, con esto se puede saber si hay saturación en las troncales.

- *Enlace Equipo PE – ISP:* Éste enlace representa el tráfico de salida de la troncal del ISP.

- *Enlace Equipo PE – Equipos Acceso:* Éste enlace representa el tráfico de la VPLS, desde el Equipo PE hacia los equipos de acceso, para establecer el porcentaje de ocupación que está siendo utilizado por la VPLS, se asignó un valor promedio de ancho de banda de 50 Mbps que es la capacidad que normalmente se entrega a los ISPs, con esto se puede saber que VPLSs ocupan mayor AB[16].

- *Enlace Equipos Acceso – Equipo PE:* Es el enlace que representa el tráfico dentro de la VPLS, desde los equipos de acceso hacia el equipo PE.

[16] El ancho de banda (AB), se define como la cantidad de información que puede fluir a través de una red en un período dado.

3.4.4.2.2 Datos obtenidos con Cacti e IOS Cisco

Se presenta el resultado de la ejecución del comando para determinar la troncal del ISP 15.

```
UIOINQE01# show vlan all-port
VLAN    Name       Status    Ports
---- --------- -------- ------------------------------
304   isp-15-dsl   active Gi10/1, Gi12/10, Gi12/25, Gi12/35, Gi12/40,
                          Gi12/41, Gi12/42, Gi12/43, Gi4/0/1

UIOINQE01#show interface Gi4/0/1 description
Interface  Status  Protocol    Description
Gi 4/0/1     up       up     *** TRONCAL ISP-15***
```

En la figura 3.15 se observa el diagrama para el ISP 15.

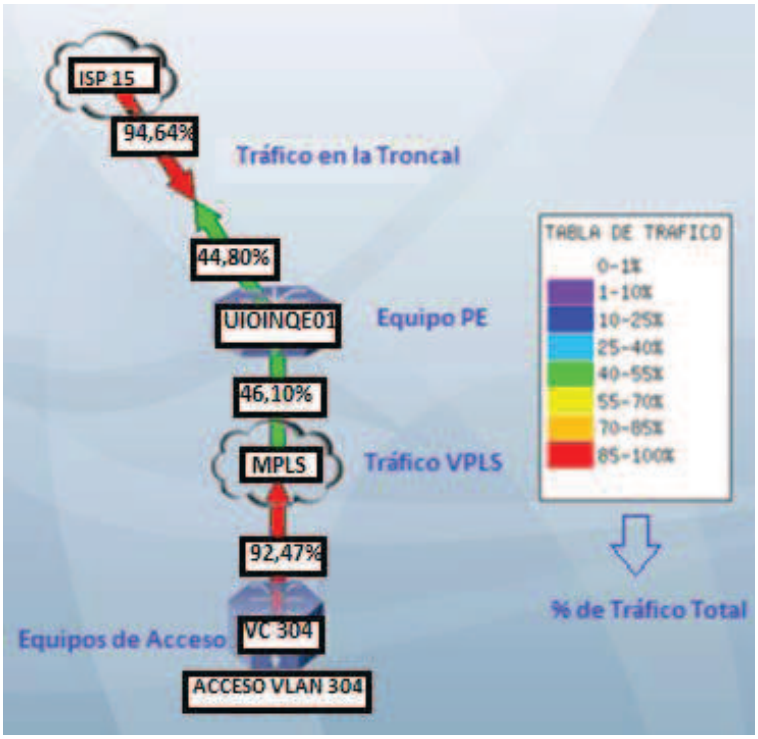


Figura 3. 15: Diagrama con Cacti ISP-15

En el diagrama se presentan dos tramos, el primero es la troncal al ISP y el segundo representa la VPLS.

Del primer tramo del diagrama interesa saber la cantidad de tráfico de la troncal del equipo PE para determinar si existe saturación.

Del segundo tramo del diagrama interesa saber la cantidad de tráfico que se transporta para determinar la cantidad de AB ocupado por los clientes de esta VPLS.

En la tabla 3.10 se presenta los resultados obtenidos con la respectiva clasificación de acuerdo al criterio descrito en la sección 3.4.3.1.3.

	Troncal	Criterio	VPLS	Criterio
ISP 15	94,64 %	Saturación	92,47 %	Saturación

Tabla 3. 10: Resultados Cacti ISP-15

3.5 RESULTADOS GENERALES DEL DIÁGNOSTICO DE LAS VPLS

Se presenta el resumen de los resultados obtenidos para cada parámetro de análisis con la respectiva herramienta utilizada.

3.5.1 RESULTADOS DE TORMENTAS BROADCAST

- **Datos obtenidos con Wireshark (Pérdida de paquetes)**

	Captura 1	Captura 2	Captura 3	PROMEDIO	Criterio SLA
ISP 2	1,30 %	1,30%	2,20%	**1,60%**	**No Aceptable**
ISP 3	0,61 %	0,78%	0,60%	**0,69%**	**Aceptable**

	Captura 1	Captura 2	Captura 3	PROMEDIO	Criterio SLA
ISP 6	1,24 %	1,17%	1,44%	**1,28%**	**No Aceptable**
ISP 7	0,54 %	0,73%	0,81%	**0,69%**	**Aceptable**
ISP 8	0,54 %	0,63%	0,30%	**0,49%**	**Aceptable**
ISP 10	0,69 %	0,45%	0,63%	**0,59%**	**Aceptable**
ISP 11	0,77 %	0,43%	0,66%	**0,62%**	**Aceptable**
ISP 12	1,3 %	0,98%	1,48%	**1,25%**	**No Aceptable**
ISP 13	0,18 %	0,27%	0,15%	**0,20%**	**Aceptable**
ISP 15	2,00 %	4,80%	2,07%	**2,96%**	**No Aceptable**
IP FIJA	1,90 %	1,91%	2%	**1,94%**	**No Aceptable**

Tabla 3. 11: Resultados Pérdida de Paquetes

De la tabla 3.11 se determina que los ISPs que presentan una pérdida de paquetes mayor al 1% con criterio No aceptable se incluirán en la optimización del servicio.

- **Datos obtenidos con Comandos IOS de Cisco (Variación MAC)**

	Muestra 1	Muestra 2	Muestra 3	Muestra 4	PROMEDIO	Valoración
ISP 2	28,9 %	13,9%	34,9%	12,3%	**22,5%**	**No aceptable**
ISP 3	5,3 %	7,6%	3,4%	4,1%	**5,1%**	**Aceptable**
ISP 6	22 %	18,8%	14,1%	32,5%	**21,8%**	**No aceptable**
ISP 7	2,9 %	2,4%	2,4%	2,3%	**8,6%**	**Aceptable**
ISP 8	8,6 %	10,1%	9,2%	11,8%	**9,9%**	**Aceptable**
ISP 10	7,5 %	8,9%	6,7%	5,9%	**7,3%**	**Aceptable**
ISP 11	2,3 %	4,7%	3,9%	3,8%	**3,8%**	**Aceptable**

	Muestra 1	Muestra 2	Muestra 3	Muestra 4	PROMEDIO	Valoración
ISP 12	18,3 %	21,3%	18,3%	19,1%	**19,3 %**	**No aceptable**
ISP 13	6,3 %	11,4%	6,3%	6,5%	**7,6%**	**Aceptable**
ISP 15	17,4 %	14%	34,9%	10,4%	**19,2%**	**No aceptable**
IP FIJA	24,7 %	29,7%	20,2%	31,4%	**26,5%**	**No aceptable**

Tabla 3. 12: Resultados Variación MAC

De la tabla 3.12 se determina que los ISPs que presentan una variación de MACs con criterio No aceptable se incluirán en la optimización del servicio.

3.5.2 RESULTADOS DE SATURACIÓN DE PUERTOS TRONCALES, CONSUMO VPLS E IDENTIFICACIÓN DEL PUERTO TRONCAL DE LA VPLS

	Troncal	Criterio	VPLS	Criterio
ISP 2	86,14 %	Saturación	79,06 %	Alto
ISP 3	54,25 %	Moderado	39,71 %	Medianamente Moderado
ISP 6	21,56 %	Bajo	92,50 %	Saturación
ISP 7	51,32 %	Moderado	42,65 %	Moderado
ISP 8	54,57 %	Moderado	40,22 %	Moderado
ISP 10	66,43 %	Medianamente Alto	35,87 %	Medianamente Moderado
ISP 11	57,85 %	Medianamente Alto	41,78 %	Moderado
ISP 12	63,34 %	Medianamente Alto	81,12 %	Alto
ISP 13	56,89 %	Medianamente Alto	57,19 %	Medianamente Alto
ISP 15	94,64 %	Saturación	92,47 %	Saturación
IP FIJA	75,13 %	Alto	89,09 %	Saturación

Tabla 3. 13: Resultados Saturación Puertos Troncales

De la tabla 3.13 se tiene que los ISP con un consumo alto o saturación en su puerto troncal, se encuentran en el equipo UIOINQE01 compartiendo la troncal Gi4/0/1 los cuales se considerarán para la optimización del servicio así como también los ISP que presentan alto consumo y saturación a nivel de la VPLS.

3.5.3 ISPs CONSIDERADOS PARA LA OPTIMIZACIÓN DEL SERVICIO VPLS

En la tabla 3.14, se presentan los ISPs considerados para la optimización del servicio en base a los resultados generales presentados, se selecciona de cada ISP el parámetro que será considerado en la optimización.

	Tormenta Broadcast		Líneas de comando innecesarias	Saturación	
	Pérdida de Paquetes	Variación MAC	Equipos DOWN	Troncal	VPLS
ISP 2	✓	✓	✓	✓	
ISP 3			✓		
ISP 6	✓	✓	✓		✓
ISP 7			✓		
ISP 8			✓		
ISP 10			✓		
ISP 11			✓		
ISP 12	✓	✓	✓		
ISP 13			✓		
ISP 15	✓	✓	✓	✓	✓
IP FIJA	✓	✓	✓	✓	✓

Tabla 3. 6: Resultado General de Problemas en los ISPs

3.6 ANÁLISIS DE LOS ATAQUES A LA SEGURIDAD DE LAS VPLS EN CAPA 2 [20], [21], [26], [27]

Como se revisó en el primer capítulo del presente proyecto de titulación acerca de los ataques a la seguridad en capa 2, el propósito de realizar un análisis a la

seguridad es identificar cuáles de ellos representan una amenaza que afecten la seguridad del servicio VPLS así como su nivel de riesgo y las medidas que se deberían tomar en cuenta para eliminar o reducir el impacto de los posibles ataques.

Para realizar un análisis de seguridad en VPLS se debe tener en cuenta que este servicio se transporta sobre una red IP/MPLS de tal manera que es necesario considerar las vulnerabilidades en la red IP/MPLS de la CNT EP. Al proteger toda la red se garantiza por parte del proveedor la correcta entrega del servicio de VPNs.

El análisis de riesgos ante los posibles ataques a la seguridad de las VPLS se realizará tomando como referencia los RFCs: RFC 2547 “BGP-MPLS VPNs” y RFC 2917 “A Core MPLS IP VPN Architecture”.

3.6.1 ALCANCE Y LÍMITES

La CNT EP provee el servicio VPLS a un gran número de ISPs los mismos que requieren que se garantice la seguridad en el servicio para el correcto funcionamiento del transporte de su información.

El presente análisis de ataques en capa 2 cubre los equipos que proveen el servicio VPLS en la provincia de Pichincha y su dependencia de la seguridad de la red IP/MPLS sobre la cual funciona.

3.6.2 EVALUACIÓN DE LA SEGURIDAD FRENTE A LOS ATAQUES DE CAPA 2

Para evaluar la seguridad del servicio se establecen criterios cualitativos que permiten estimar los ataques al servicio, el grado de afectación y la probabilidad de ocurrencia.

3.6.2.1 Estimación de ataques al servicio

Los criterios para estimar el tipo de ataque en capa 2 que afecte de manera directa a la seguridad de la VPLS se toman en base a los argumentos básicos especificados en el capítulo 1 sección 1.6.1.

Los ataques clasificados son orientados específicamente al funcionamiento del servicio VPN sobre la red IP/MPLS.

A continuación se describen los ataques que se consideran una amenaza para el servicio:

a) Ataque DoS entre VPNs

b) Ataque a equipos PE desde una VPN

c) Spoofing de etiquetas

d) Ataque dentro de la VPN

3.6.2.2 Estimación del nivel de afectación a la seguridad de la VPLS.

Los criterios para estimar el nivel de afectación se basan en el nivel de impacto al servicio VPLS.

La tabla 3.15 contiene la descripción del ataque y afectación al servicio desde el punto de vista de la pérdida o no del mismo.

PARÁMETROS / ATAQUE	DESCRIPCIÓN	AFECTACIÓN
Ataque DoS entre VPNs	Inundación de tráfico desde una VPN hacia otra para denegar el servicio a los usuarios legítimos de la red.	Pérdida parcial o total del servicio en la VPN atacada.
Ataque a equipos PE desde una VPN	Inundación de tráfico desde una VPN hacia él equipo PE.	Pérdida parcial o total del servicio en la VPN perteneciente al PE atacado.
Spoofing de etiquetas	Falsificación de etiquetas en la VPN para ingreso no autorizado.	No hay pérdida del servicio, existe perdida de confidencialidad de la información dentro de la VPN.
Ataque dentro de la VPN	Referido a tormentas LAN	Pérdida parcial o total del servicio.

Tabla 3. 15: Ataque vs. Afectación

3.6.2.3 Estimación de probabilidad de ataques a la VPLS.

En la tabla 3.16 se muestran criterios calificativos y la justificación correspondientes a la probabilidad de ocurrencia de ataques al servicio VPLS.

PARÁMETROS / ATAQUE	PROBABILIDAD	JUSTIFICACIÓN
Ataque DoS entre VPNs	MUY IMPROBABLE	Debido a la separación de tráfico no es posible realizar DoS desde una VPN hacia otra VPN. La única posibilidad de ataque DoS puede ser así misma.
Ataque a equipos PE desde una VPN	MEDIANAMENTE PROBABLE	Se puede atacar al PE ya que forman parte de la misma VPN.
	MUY IMPROBABLE	Debido al ocultamiento de los equipo P del core, no es posible atacar al PE si no se pertenece a la misma VPN.
Spoofing de etiquetas	ALTAMENTE PROBABLE	Si se tiene acceso al core MPLS esta puede ser exitosa.
	MUY IMPROBABLE	Equipos en Internet y los equipos CE no manejan etiquetas MPLS, simplemente direccionamiento IP, por lo que los equipos PE deben no permitir que ingresen etiquetas desde el exterior
Ataque dentro de la VPN	ALTAMENTE PROBABLE	Tormentas de difusión pueden ocurrir si existen demasiados usuarios en un único dominio de difusión

Tabla 3. 16: Ataques vs. Probabilidad

3.6.3 VALORACIÓN DE RIESGOS EN LA SEGURIDAD DE LA VPLS

El propósito de la valoración de riesgos es determinar los factores que permiten dar paso a los ataques ya descritos, exponiendo a la vulnerabilidad del servicio.

3.6.3.1 Identificación de riesgos

Se identifican dos posibilidades de riesgo al servicio VPLS siendo estos riesgos al core MPLS y riesgos dentro de la VPLS.

3.6.3.1.1 Riesgos a la red IP/MPLS

Basándose en la tabla 3.17 los ataques tienen éxito únicamente si son ejecutados por personas que tiene acceso a la red IP/MPLS, donde el personal identificado es el siguiente:

- Personal del Área O&M Plataformas IP/MPLS
- Personal de las diferentes áreas de la CNT EP que cuentan con accesos a la red IP/MPLS.
- Personal externo de soporte a la red IP/MPLS de la CNT EP.

3.6.3.1.2 Riesgos dentro de la VPLS

Dentro de la VPLS se transporta todo el tráfico desde el origen hasta el destino de los ISPs clientes llevando consigo problemas de nivel interno que generalmente son de tormentas de difusión debido a los siguientes factores:

- Muchos usuarios en un solo dominio.
- Medios de acceso físicos defectuosos.
- Ataques de capa 2 dentro de la VPLS por falta de políticas de seguridades por parte de los usuarios.

3.6.4 TRATAMIENTO DE RIESGOS EN LA SEGURIDAD DE LA VPLS EN LA CNT EP

Una vez identificados los riesgos a los que la VPLS se ve sometida se establecen medidas que se deberían tomar en cuenta para eliminar o reducir el impacto de los posibles ataques.

Los tratamientos se describen de acuerdo al riesgo identificado anteriormente.

3.6.4.1.1 Tratamiento al riesgo sobre la red IP/MPLS [16]

La red IP/MPLS de la CNT EP empezó manejando un sistema de control de acceso denominado CISCO ACCESS CONTROL SYSTEM ACS v3.2 con el cual completo la primera fase de la red IP/MPLS; según un análisis realizado recientemente en un proyecto de titulación denominado "ANÁLISIS DE RIESGOS DE LA RED IP/MPLS DE LA CORPORACIÓN NACIONAL DE TELECOMUNCACIONES, BASADO EN LA NORMA ISO/IEC 27005 Y PROPUESTA DE MEJORAMIENTO DEL CONTROL DE ACCESO A LA ADMINISTRACIÓN DE SUS DIPOSITIVOS" se detectó falencias en las políticas de control de acceso, administración de los dispositivos de la red IP/MPLS y falencias en el sistema de control de acceso Cisco ASC v3.2.

Al requerir mayor nivel de seguridad este análisis propuso un mejoramiento del control de acceso a la administración de los dispositivos de la red IP MPLS de la CNT EP; y la actualización del sistema de control de acceso a la versión más reciente para corregir las falencias y errores de funcionamiento encontrados en la primera fase.

Las normas y procedimientos para el acceso a la administración de los dispositivos de la red IP/MPLS de la CNT EP se resumen en la figura 3.16.

Figura 3. 16: Normas y Procedimientos de acceso Red IP/MPLS

3.6.4.1.2 Tratamiento al riesgo del equipo PE

Limitar el acceso a los dispositivos PEs dentro del alcance del control de la entidad operativa, para esto se puede realizar lo siguiente:

- ✓ Definir y aplicar las ACL para acceso remoto.
- ✓ Utilizar servidores AAA centralizados para controlar el acceso.
- ✓ Proteger el acceso a los puertos de consola y auxiliar.
- ✓ Uso de SSH para el acceso remoto.
- ✓ Limitar el acceso SNMP a servidores específicos a través de ACL.
- ✓ Facilitar el acceso de solo lectura y solo SNMP.
- ✓ Implementar DMZ usando IDS y firewalls para proteger las redes contra intrusiones.
- ✓ Usar MD5 para la LDP en el núcleo.
- ✓ Configuración de contraseñas de acceso al equipo.
- ✓ Habilitación de comandos para minimizar impacto de ataque a los equipos.
- ✓ Habilitación de traps.

3.6.4.1.3 Tratamiento al riesgo dentro de la VPLS

Las VPLS al ser un servicio de capa 2 se ven mayormente afectadas por el tráfico broadcast y están sujetas a múltiples ataques por parte de la red del cliente que cuanto mayor sea su tamaño mayor será la exposición y más complejo determinar en donde se origina el problema, por lo que el primer recurso para limitar el impacto negativo de esta situación es segmentar el tamaño de los dominios de broadcast.

Cuando se implementa switching de capa 2 el único recurso disponible para limitar la difusión de broadcast es la implementación de VLANs, ya que por definición los switches LAN no filtran el broadcast y lo inundan a toda la red, segmentar permite garantizar un mejora en la seguridad y proporciona una actividad de difusión controlada.

Debido a que la VPLS es el transporte del tráfico del cliente se debe recomendar al administrador de los ISPs que asegure su red utilizando políticas de seguridad en sus equipos internos para no conllevar problemas en el trasporte de tráfico en la VPLS, éstas pueden ser:

- ✓ Port Security (Seguridad a nivel de Puertos).
- ✓ MAC address VLAN Access maps (Listas para control de Acceso).
- ✓ Asegurar que el puerto del enlace troncal no pertenezca a la VLAN Nativa de los usuarios.
- ✓ Deshabilitar los puertos no utilizados y colocarlos en una VLAN que no se utilice.
- ✓ Implementar VLANs Privadas (PVLAN).
- ✓ Usar DHCP snooping.
- ✓ Habilitar PortFast, Root Guard, y BDP Guard.
- ✓ Usar Dynamic ARP Inspection (DAI).
- ✓ Configuración Storm Control.

CAPÍTULO 4

OPTIMIZACIÓN Y ESCALABILIDAD DEL SERVICIO [3], [4]

4.1 INTRODUCCIÓN

Del análisis desarrollado en el Capítulo 3 se encontraron diversos factores que afectan el servicio VPLS disminuyendo el desempeño del mismo.

En el presente capítulo se propone las alternativas de solución al servicio VPLS de cada ISP, en base a los parámetros de afectación ya identificados, donde se incluyen los resultados finales que reflejan el estado final de cada ISP.

En base a la situación actual del servicio de las VPLS se presentan las alternativas de escalabilidad incluyendo el modelo jerárquico HVPLS.

Como último punto se presenta un manual de mejores prácticas para el correcto funcionamiento del servicio VPLS incluyendo políticas de seguridad, ver Anexo H.

4.2 OPTIMIZACIÓN DEL SERVICIO VPLS EN LA CNT E.P.

Como parte de la optimización del servicio VPLS se presentan las alternativas de solución a los problemas identificados que afectan el correcto funcionamiento de las mismas así como la mejora al monitoreo.

4.2.1 SEGMENTACIÓN DE VLANS [6]

VPLS utiliza métodos de broadcast para la replicación de entrada y aprendizaje MAC esto limita la escalabilidad de la red (el hecho de agregar más puntos de acceso

conlleva a tener más carga de señalización de origen), por lo tanto la segmentación de VLANs introduce una solución al problema.

Este método hace uso de múltiples VFIs (Interfaz Virtual de Envío) en lugar de utilizar una sola VFI para la malla completa de pseudowires, por lo que la carga de replicación de origen se reduce de acuerdo al número de VFI creadas, además el utilizar múltiples VFI como se indica en la figura 4.1, permite mitigar el requisito de aprendizaje MAC y el dominio de broadcast es reducido ya que hay menos usuarios.

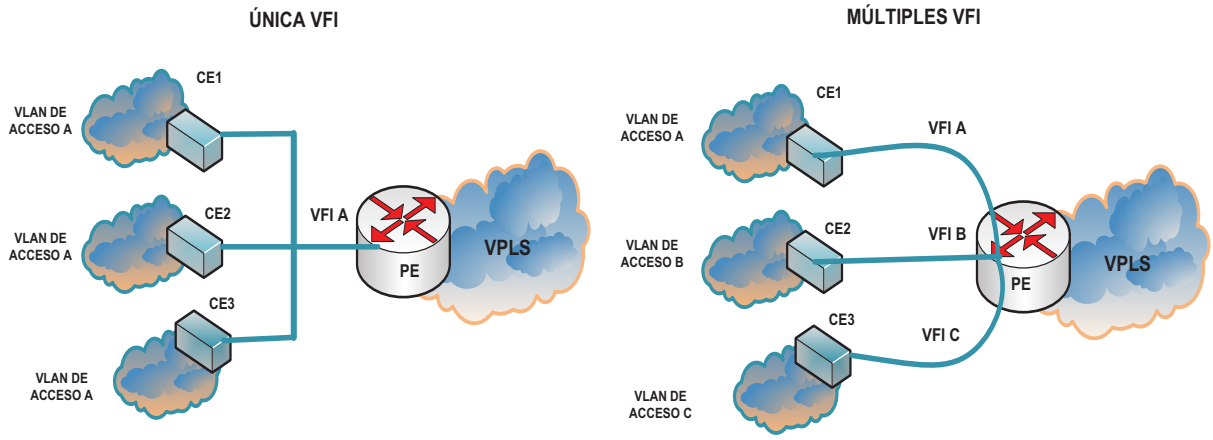


Figura 4. 1: Única VFI vs. Múltiples VFI

Los PEs remotos en una VPLS, pueden transportar transparentemente la etiqueta de VLAN original, dejando en el lado del cliente la responsabilidad de adecuar sus configuraciones para que la solución final sea consistente en cuanto a comunicación entre equipos pertenecientes a las mismas VLANs.

4.2.1.1 Criterio de segmentación de VLANs

Para la segmentación de VLANs se utiliza el criterio de cantidad de usuarios por VPLS de acuerdo a una estimación del aprendizaje MAC y si la cantidad de consumo de AB de la VPLS está saturada.

4.2.1.1.1 Criterio de segmentación por número de usuarios

En la tabla 4.1 se establece el criterio de segmentación de la VPLS donde consta el número de usuarios con una variación de +/- 50 como margen de error, y el número de VLANs a segmentar.

Número Usuarios	Segmentos	Rango (+/- 50)
150	1	1 – 200
300	2	250 – 350
450	3	400 -500
600	4	550 – 650

Tabla 4. 1: Segmentación por número de Usuarios

El número de usuarios para el primer segmento se establece mediante la comparación de los ISPs que en el análisis no presentaron problemas. Para éstos ISPs se determinó el máximo valor de MACs aprendidas simultáneamente al 100 %; éste valor corresponde al IPS 7 y es de 158 que se redondea a 150, la muestra se puede observar en el Anexo D.

4.2.1.1.2 Criterio de segmentación por Saturación de la VPLS

Si una VPLS consume el máximo de su capacidad asignada, CNT E.P. como proveedor del servicio debe implementar una solución a nivel lógico con la infraestructura existente; de tal modo que ISPs donde la VPLS esté saturada de acuerdo a los criterios de la tabla 3.5 del Capítulo 3, independientemente de su cantidad de usuarios deberá ser segmentada.

Otra solución sería el aumento de ancho de banda, sin embargo éste es un parámetro que implica una aceptación de tipo comercial debido a los términos de negociación entre proveedor y cliente ISPS.

4.2.1.1.3 Aplicación de los criterios a los ISPs a optimizar

Se considera que el 50% de los clientes se conectan simultáneamente en la VPLS, como criterio se toma el caso más crítico que es la conexión simultánea de todos los usuarios de la VPLS, es decir el 100% de los clientes conectados.

En la tabla 4.2 se presentan el valor máximo de las MACs aprendidas simultáneamente que se obtuvieron de las muestras realizadas para el proceso de análisis del Capítulo 3 sección 3.4.4.1.3, se añade el número de segmentos de acuerdo a los criterios de cantidad de usuarios por VPLS y cantidad de consumo de AB de la VPLS.

	Usuarios Simultáneos (50 %)	**Usuarios Simultáneos (100 %)**	**Consumo VPLS**	**Números Segmentos**
ISP 2	19	38	Alto	1
ISP 6	71	142	Saturación	2
ISP 12	253	506	Alto	3
ISP 15	151	302	Saturación	2
IP FIJA	297	594	Saturación	4

Tabla 4. 2: Segmentación de ISPs por número de Usuarios

Los usuarios para cada segmentos se pueden escoger de acuerdo al criterio del administrador del servicio, para la CNT P.E., se estableció de acuerdo a la ubicación geográfica; siendo estas Zona Norte, Sur, Valles y Provincias.

4.2.2 REGULACIÓN DE ANCHO DE BANDA EN LAS TRONCALES

En el análisis realizado en el Capítulo 3 sección 3.5.3, se pudo observar que un puerto que era troncal para algunos de los ISPs mostraba saturación.

Estos ISPs fueron ISPs 2, ISP 15 y la IP FIJA que utilizaban la interfaz t Gi 4/0/1 como troncal; de tal forma que se procedió a distribuir a cada ISP a diferentes troncales, excepto el ISP 2 el cuál no ingresó a la segmentación de VLANs y permaneció en la misma troncal.

Este procedimiento lo realizó el Área O&M Plataforma IP/MPLS de CNT E.P., ya que el personal tiene un conocimiento más profundo de las interfaces de los equipos de la red IP/MPLS; se migró el tráfico a los nuevos puertos troncales teniendo en cuenta que éstos no presenten saturación del mismo.

En la tabla 4.3 se presenta las nuevas troncales para los ISPs migrados.

ISP	NUEVA TRONCAL
ISP 2	Gi 4/0/1 (No Migrada)
ISP 15	Gi 10/1
ISP 15	Gi 12,5 – Gi 12/8

Tabla 4. 3: Asignación nueva troncal

4.2.3 MEJORAS EN EL MONITOREO DE LAS VPLSs Y ADMINISTRACIÓN DE LAS VPLSs.

Como parte de la optimización para mejorar el monitoreo de las VPLSs se optó por buscar un sistema que permita el constante monitoreo del tráfico de las VPLSs mediante la herramienta Wireshark especificada en el Capítulo 3 sección 3.3., donde se puede determinar pérdida de paquetes y visualización de tráfico broadcast con

respecto al tráfico total y además se plantea los comandos necesarios para realizar una correcta administración y revisión en la configuración de las VPLSs.

4.2.3.1 Servidor de Acceso Remoto [7], [29]

Para realizar el cometido se debe asegurar que el monitoreo se lo pueda realizar remotamente de una manera segura, para esto se instaló un servidor de acceso remoto en el sistema operativo Linux Ubuntu 9.04, en una máquina asignada por el Área O&M Plataforma IP/MPLS de CNT E.P, en donde está instalada la herramienta Wireshark para realizar el monitoreo.

Para el acceso remoto se a la herramienta Wireshark se basó en la aplicación cliente – servidor, en donde el cliente tiene control total del servidor utilizando la herramienta VNC, para mayor detalle de la herramienta y su implementación referirse al Anexo B.

Este servidor se encuentra conectado al equipo UIOLABE01 que refleja el tráfico de cada VPLS mediante el Port-mirroring, ya explicado en el Capítulo 3, sección 3.4.4.1.1.

Para proporcionar mayor seguridad y asegurar que solo personal autorizado pueda tener acceso a dicha información, el servidor estará dentro de la intranet de CNT EP, y únicamente accesible a través de la intranet de la CNT E.P.

En la figura 4.2, se presenta el esquema manejado para el monitoreo de VPLS mediante acceso remoto.

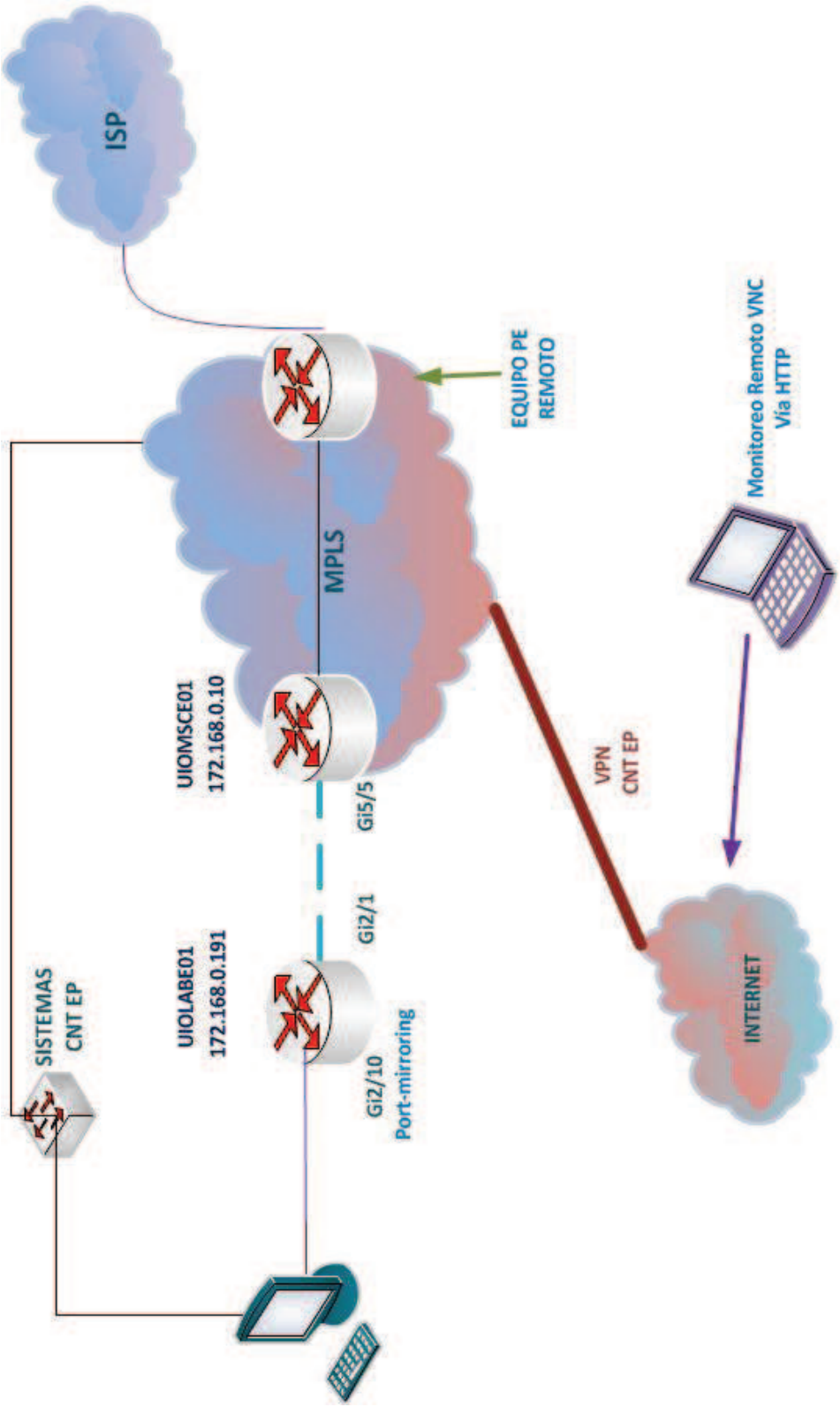


Figura 4. 2: Esquema del monitoreo VPLS - VNC

4.2.3.2 Comandos de Administración

A nivel de configuración se debe tener no una transparencia y organización de las líneas de comando de las cuales depende el servicio a entregar, para evitar que se presenten los siguientes puntos:

- Uso de recurso innecesarios a nivel de procesamiento de los equipos
- Información errada para el Administrador de red
- Diagnóstico en el servicio y cambios a realizar en la configuración requieren de mayor tiempo para el Administrador de red

Además se debe conocer los comandos que permiten obtener la información a detalle de cada parámetro del servicio. Se cita los principales comandos utilizados en el presente proyecto de titulación para la administración del servicio VPLS a través del propio IOS del equipo.

- Para indicar los puertos por donde cruza la VLAN. Se puede obtener la descripción de cada uno e identificar cuál es la troncal del cliente.

Router#show vlan all-port

- Para identificar los neighboors conectados vía pseudowire o spoke en la VPLS específica y si están activos o no. Su principal función es indicar si la conexión se encuentra configurada como VPLS o HVPLS (la S indica si está configurado como Horizonte dividido).

Router#show vfi “nombre-vpls”

- Para identificar el tipo de encapsulación del túnel y las propiedades del pseudowire usado para emular el circuito virtual de los neighboors conectados.

Router#show run | begin l2 vfi "nombre-vpls"

- Para indicar la tabla de MAC aprendida asociada a la VLAN. Se puede verificar si la VLAN está en uso cuando se tenga como resultado MACs aprendidas.

Router#show mac-address-table vlan vlan-id

- Para indicar las MACs aprendidas de cada VLAN. Se puede determinar si existe variación de MACs (variación representativa de MAC pueden representar tormentas de broadcast).

Router#show mac-address-table count vlan vlan-id

- Para verificar que la sesión dirigida LDP esté funcionando. Su salida indica los pseudowires creados para el transporte de tramas de capa 2 a través de la red troncal MPLS su principal función es identificar el estado del Pseudowire ya sea activo o desactivo. Si se omite el vc-id se despliega todos los VC creados en el equipo.

Router#show mpls l2 vc vc-id

- Para verificar por cada equipo de acceso el estado del VC, la interfaz de salida hacia el PE remoto, la etiqueta local y remota, el tamaño del MTU y la descripción de la interfaz troncal de la VPLS.

Router#show mpls l2 vc vc-id detail

4.3 ESTUDIO DE ESCALABILIDAD DEL SERVICIO

La tecnología VPLS ha logrado desplegar la prestación de servicios a través de una red basada en Ethernet de una manera fiable y flexible, sin embargo requiere de mejoras a niveles de operaciones sobre todo cuando se lleva esta tecnología a gran escala.

4.3.1 CRITERIOS PARA LA ESCALABILIDAD DEL SERVICIO

Escalabilidad para cualquier tipo de servicio o tecnología puede ser visto desde diferentes perspectivas y lograr el resultado requerido.

Para el caso puntual del servicio VPLS se considera como criterio de escalabilidad el crecimiento de la red a nivel topológico y de usuarios.

4.3.1.1 Crecimiento Topológico

Los proveedores de servicio constantemente se ven en la necesidad de implementar más servicios o aumentar su cobertura; CNT E.P. considerado como la empresa líder de Telecomunicaciones en el Ecuador no está exenta de este factor y puede incluir mayor cantidad de ISPs a su cartera de clientes, ante esta posibilidad se verá reflejado el crecimiento topológico.

4.3.1.2 Crecimiento de Usuarios

Cada ISPs cliente puede crecer a nivel corporativo representando un incremento de número de usuarios a su red.

4.3.2 COMPORTAMIENTO DEL SERVICIO VPLS DE ACUERDO A LOS CRITERIOS DE CRECIMIENTO [6]

En esta sección se analiza el comportamiento del servicio VPLS si se presentan los escenarios de crecimiento planteados en la sección 4.3.1.

4.3.2.1 Comportamiento ante un crecimiento topológico

Si es necesario incluir un equipo PE ya sea para agregar un nuevo sitio a una instancia VPLS o incluir una nueva, los equipos PEs tiene que actualizar todas las tablas de los PEs asociados a la misma, trayendo consigo una nueva replicación de paquetes, provocando una carga en el plano de datos y en el plano de control debido a la detección automática del nuevo punto, y la complejidad de mallado completo de LSP entre los PEs participantes, como se indica en la figura 4.3.

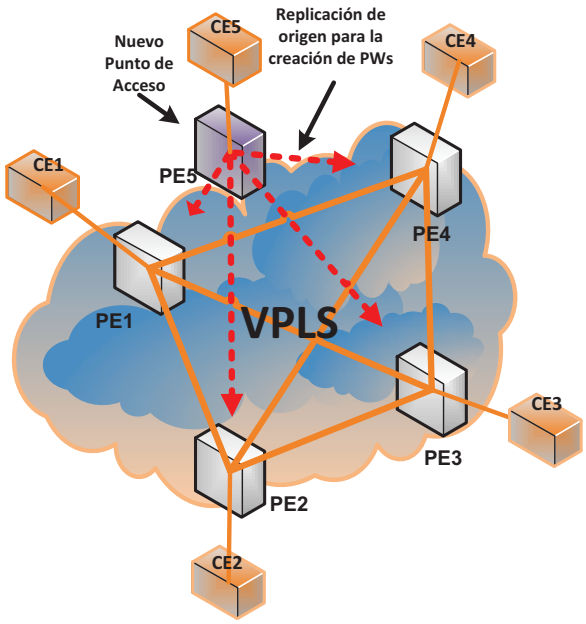


Figura 4. 2: Nuevo punto VPLS

4.3.2.2 Comportamiento ante un crecimiento de Usuarios

El crecimiento de usuarios las VPLS implica un mayor tamaño en sus dominios de difusión, la afectación en las VPLS se presentó en el Capítulo 3, sección 3.2.1.

El tener grandes cantidades de usuarios en un mismo PE implica que la replicación de paquetes se realice hacia todos ellos, creando una sobrecara de señalización en el equipo PE.

4.3.3 PLANTEAMIENTOS DE ESCALABILIDAD AL SERVICIO VPLS [3], [6], [12]

Se presenta las alternativas de solución ante un posible crecimiento a nivel topológico o de usuarios del servicio VPLS de la CNT E.P.

4.3.3.1 Escalabilidad ante crecimiento topológico

En esencia, HVPLS trata de solucionar el crecimiento topológico del servicio VPLS, creando nuevos puntos de replicación fuera del mallado VPLS, de tal manera que minimiza la cantidad de replicaciones de entrada necesarias para el transporte de tráfico broadcast sobre el mallado VPLS.

HVPLS utiliza un nodo como N-PE y el nodo extremo como U-PE; al ser la conexión de estos dos puntos de tipo spoke la regla del “horizonte dividido” no se aplica, de tal manera que el tráfico recibido de la región VPLS será reenviado únicamente al equipo U-PE, como lo indica la figura 4.4.

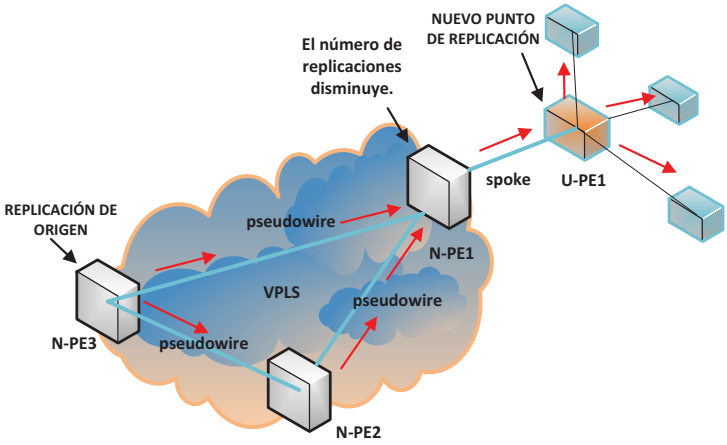


Figura 4. 3: Creación de nuevo punto de replicación

Si HVPLS añade un nuevo dispositivo U-PE éste requiere la configuración del router N-PE local al que se conecta, pero no requiere señalización alguna con otros routers N-PE o dispositivos U-PE, ya que el mallado original VPLS se mantiene como muestra en la figura 4.5.

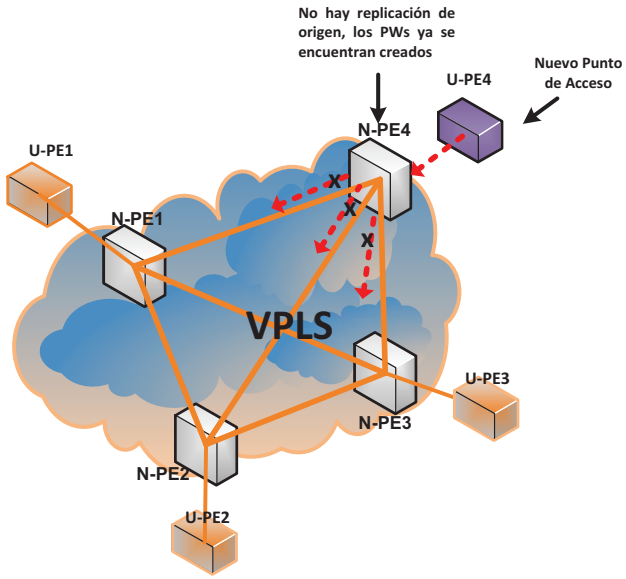


Figura 4. 4: Nuevo punto de acceso en HVPLS

4.3.3.2 Escalabilidad ante crecimiento de usuarios

Uno de los problemas detectados al realizar el análisis del funcionamiento de las VPLSs en la CNT E.P., se refiere a la cantidad de usuarios en una VPLS cuyo tráfico excesivo de broadcast puede afectar el funcionamiento de la misma, el detalle se expone en la sección 4.2.1.

La segmentación de VLANs dentro de una VPLS se planteó como solución al problema; frente a una escalabilidad ante el crecimiento de usuarios constituye la misma alternativa de solución.

4.4 RESULTADOS GENERALES DE LA OPTIMIZACIÓN Y ESCALABILIDAD DEL SERVICIO VPLS

Con los resultados obtenidos sobre el análisis de cada ISP, se determinó que los ISP: ISP2, ISP6, ISP12, ISP 15 y la IP FIJA son aquellos que requieren la solución a los problemas encontrados.

Se presentan los resultados obtenidos al aplicar los criterios de optimización del servicio a cada ISP y la propuesta de escalabilidad a 1 ISP. Se emplea el mismo proceso de análisis realizado para obtener los resultados iniciales tomando dos muestras con cada herramienta para cada ISP optimizado.

4.4.1 RESULTADOS DE LA OPTIMIZACIÓN DEL SERVICIO VPLS EN LA CNT E.P.

En esta sección se presentan los resultados obtenidos al realizar el monitoreo de las VPLS después de aplicar los criterios de optimización del servicio a cada ISP, los resultados individuales se presentan en el Anexo E.

En el caso del ISP 2 con respecto a la valoración de tormenta de broadcast, el muestreo MAC no reflejó una cantidad de usuarios mayor a lo establecido en la sección 4.2.1 para la segmentación de VLANs, sin embargo se observó una pérdida de paquetes y alto consumo de ancho de banda en la VPLS sin determinar su origen.

Cuando se realizó el proceso para obtener los resultados de los ISPs que entraron en el plan de optimización de acuerdo a los criterios establecidos en éste proyecto se evidenció que el ISP 2 presentó notables mejorías por lo que se concluye que el problema que se observó en el análisis inicial fue a nivel de red interna del cliente ISP.

4.4.1.1 Resultados de tormentas Broadcast después de la optimización

- **Datos obtenidos con Wireshark (Pérdida de paquetes)**

		Captura 1	Captura 2	PROMEDIO	Criterio SLA
ISP 2	327	0,83 %	0,73%	**0,78%**	**Aceptable**
ISP 6	2911	0,20%	0,28%	**0,24%**	**Aceptable**
	2912	0,76%	0,73%	**0,74%**	**Aceptable**
ISP 12	305	0,77%	0,87%	**0,82%**	**Aceptable**
	366	0,82%	0,58%	**0,70%**	**Aceptable**
	367	0,64%	0,75%	**0,70%**	**Aceptable**
ISP 15	304	0,86 %	0,92%	**0,89%**	**Aceptable**
	310	0,38%	0,64%	**0,51%**	**Aceptable**
IP FIJA	3370	0,79 %	0,82%	**0,80%**	**Aceptable**
	3372	0,67%	0,86%	**0,76%**	**Aceptable**
	3374	0,60%	0,42%	**0,51%**	**Aceptable**
	3376	0,73%	0.60%	**0,66%**	**Aceptable**

Tabla 4. 4: Resultados Pérdida de Paquetes - Optimización

De la tabla 4.4 se determina que las VLANs que conforman las VPLSs de los ISPs cumplen con el criterio aceptable para la pérdida de paquetes.

- **Datos obtenidos con Comandos IOS de Cisco (Variación MAC)**

	VLAN	Muestra 1	Muestra 2	PROMEDIO	Valoración
ISP 2	327	6 %	4,1%	**5,4%**	**Aceptable**
ISP 6	2911	4,6 %	4,4%	**4,5%**	**Aceptable**
	2912	5,9%	10,9%	**8,4%**	**Aceptable**
ISP 12	305	1,3 %	3,5%	**3,4%**	**Aceptable**
	366	0,3%	0,6%	**0,5%**	**Aceptable**
	367	1,5%	1,5%	**1,5%**	**Aceptable**
ISP 15	304	2,4 %	6,1%	**4,2%**	**Aceptable**
	310	4,3%	3,8%	**4,1%**	**Aceptable**
IP FIJA	3370	2,1%	1,3%	**1,7%**	**Aceptable**
	3372	0,4%	1,9%	**1,1%**	**Aceptable**
	3374	0%	0,44%	**0,2%**	**Aceptable**
	3376	0,8%	0,8%	**0,8%**	**Aceptable**

Tabla 4. 5: Resultados Variación de MAC – Optimización

De la tabla 4.5 se determina que los ISPs presentan una variación MAC de consideración Aceptable.

4.4.1.2 Resultados de saturación de puertos troncales, consumo VPLS después de la optimización.

ISP	VLAN	Troncal	Criterio	VPLS	Criterio
ISP 2	327	57,09%	Medianamente Alto	39,31%	Medianamente Moderado
ISP 6	2911	58,76%	Medianamente Alto	45,80%	Moderado
	2912			37,77%	Medianamente Moderado

ISP	VLAN	Troncal	Criterio	VPLS	Criterio
ISP 12	305	81,99%	Alto	29,93%	**Medianamente Moderado**
	366			20,97%	**Bajo**
	367			36,11%	**Medianamente Moderado**
ISP 15	304	65,89%	Medianamente Alto	34,18%	**Medianamente Moderado**
	310			22,51%	**Bajo**
IP FIJA	3372	59,17%	Medianamente Alto	61,56%	**Medianamente Alto**
	3370	63,15%	Medianamente Alto	61,30%	**Medianamente Alto**
	3374			46,51%	**Moderado**
	3376			32,35%	**Medianamente Moderado**

Tabla 4. 6: Resultados Saturación Puertos Troncales – Optimización

De la tabla 4.6 se observa que el consumo en la troncal y el consumo de la VPLS están dentro de los valores aceptables y no se observa saturación.

4.4.2 APLICACIÓN DE HVPLS COMO ESCALABILIDAD DEL SERVICIO VPLS

El criterio de escalabilidad utilizando HVPLS se lo consideraría cuando se presente un crecimiento de la red topológica del servicio VPLS. Al momento la topología e infraestructura de la red IP/MPLS de la CNT. E.P., cubre las necesidades de la cartera de sus clientes, de tal forma que no hubo la necesidad de añadir nuevos equipos a la topología e incrementar gastos.

Sin embargo para observar el comportamiento de HVPLS se utilizó un ISP como ejemplo para plantear la escalabilidad del servicio.

El ISP utilizado para éste propósito es el ISP 2 el cuál al realizar el análisis después de la optimización muestra un comportamiento aceptable en cuanto a funcionalidad de la VPLS.

El equipo PE local UIOINQE01 para este ISP está conectado físicamente al equipo UIOINQE02 el cual estaba disponible para la configuración de HVPLS y además cumple con las características requeridas.

La figura 4.7 presenta el esquema utilizado para HVPLS; se configuró un Spoke-pseudowire del equipo N-PE (UIOINQE01) al equipo que actuará como U-PE (UIOINQE02) colocando 1 nivel más de jerarquía de pseudowires, a continuación se presenta el esquema de solución con las respectivas configuraciones que muestran en cada equipos, las configuraciones de HVLS se encuentran el Anexo C.

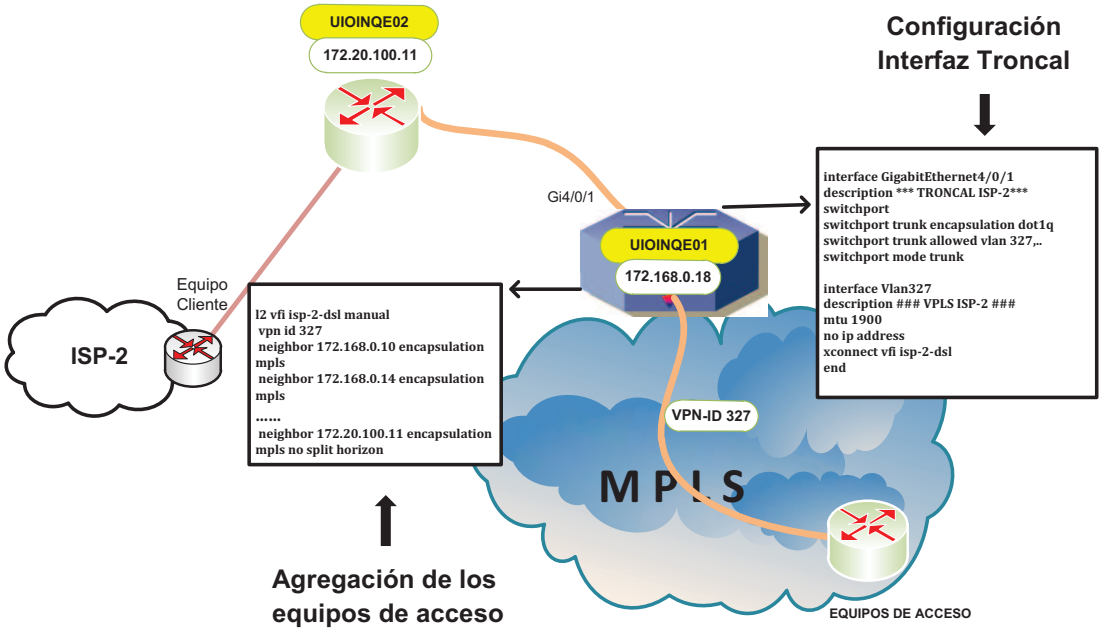


Tabla 4. 7: Configuración de HVPSL para el ISP-2

4.4.2.1.1 Costos referenciales de Hardware [17]

Para la implementación del modelo HVPLS se mantiene la red IP/MPLS debido a que la solución jerárquica no implica un cambio de infraestructura sino la extensión de la misma.

Una buena selección de los equipos se realiza de acuerdo a los requerimientos de la red del proveedor presentando varias alternativas, para establecer una comparación t escoger la mejor opción.

A partir del concepto presentado en el Capítulo 1, sección 1.5.1, donde se indican que los equipos que participan en el servicio HVPLS son el N-PE y el U-PE se plantea las características y costos referenciales de los mismos.

A pesar que en el mercado actual existen varios marcas que ofrecen equipos que soportan MPLS y VPNs capa 2; por confiabilidad y criterios de estabilidad en la capa de core y distribución de la red la mejor opción es utilizar equipos de la marca CISCO, es por eso que la CNT E.PE. , hace uso de esta marca.

La comparativa planteada se hace en base a la marca CISCO, con dos de los proveedores de equipos CISCO en Ecuador siendo estos TOTALTEK y ANDEAN TRADE.

- **Requerimientos del equipo N-PE**

Los principales requerimientos que deben cumplir los equipos que van a actual como N-PE son:

- ✓ Funcionalidad MPLS, con manejo de VPNs.
- ✓ Soporte de fibra óptica monomodo y multimodo.
- ✓ Soporte de protocolos en capa 2 como: VLAN Trunk Protocol (VTP), IEEE 802.1q.
- ✓ Soporte de protocolos en capa 3 como: OSPF, BGPv4.
- ✓ Soporte de protocolos de señalización como: RSVP,LDP.

- ✓ Manejo de puertos alta velocidad.
- ✓ Manejo de gran cantidad de direcciones MAC.

- **Requerimientos del equipo U-PE**

Los equipos U-PEs al no ser partícipes del core VPLS disminuyen las características requeridas para el equipo, sin embrago éstos deben soportar MPLS ya que son parte de la red.

Los principales requerimientos que deben cumplir los equipos que van a actual como U-PE son:

- ✓ Funcionalidad MPLS.
- ✓ Soporte de protocolos en capa 2 como: VLAN Trunk Protocol (VTP), IEEE 802.1q.
- ✓ Soporte de protocolos en capa 3 como: OSPF, BGPv4.
- ✓ Soporte de protocolos de señalización como: RSVP,LDP.
- ✓ Manejo de puertos alta velocidad.
- ✓ Manejo de gran cantidad de direcciones MAC.

- **Equipos que cumplen con las características requeridas N-PE**

La CNT E.PE., utiliza en la infraestructura para proveer el servicio VPLS equipos CISCO de la serie 7600, ya que cumplen con las características necesarias para el servicio.

Para seleccionar los equipos se presentan dos alternativas de equipos dentro de esta serie los cuales se diferencian en la capacidad de añadir servicios, siendo estos CISCO 7606-S y CISCO 7613-.S.

MARCA Y MODELO	CISCO 7606-S	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Requiere de 7 unidades de rack para su montaje.	
	Incorpora dos fuentes de alimentación AC o DC.	
	Dos tarjetas de procesamiento.	
	Rejillas de ventilación a los lados del chasis.	
	Cuenta con 6 slot.	
Características del sistema	Capacidad máxima de conmutación: 480 Gbps.	
	Potencia máxima a entrada AC 2700 W o DC 2700W.	
	Memoria RAM de 3 GB instalad, expansible a 6 GB.	
	Funciona con el sistema Operativo CISCO IOS.	
Protocolos	OSPF, RIP, BGPV4, IS-IS, IGM, PIM-SM, PIM-DM, MPLS.	
Descripción	Permite a los proveedores de servicios sobre redes IP/MPLS ofrecer una variedad de aplicaciones de voz, datos y video con gran rendimiento. Soporta Conmutación a nivel 3 y capa 2, asignación dirección dinámica IP, soporte de DHCP, limitación de tráfico, soporte ACL, VPNs, QoS.	
Entradas MAC	64.000	

Tabla 4. 7: Características técnicas, equipo CISCO 7606-S

MARCA Y MODELO	CISCO 7613	
Tipo de dispositivo	Base de expansión modular.	
Características del chasis	Requiere de 18 unidades de rack para su montaje.	
	Cuenta con 13 slot.	
	2 slot para porcesadores de router.	
	2 ventiladores.	
	2 fuentes de alimentación AC o DC.	
Características del sistema	Capacidad máxima de conmutación: 720 Gbps.	
	Potencia máxima a entrada AC 4000 W o DC 6000 W.	
	Funciona con el sistema Operativo CISCO IOS.	
Protocolos	LDP, IGMP, ATM, DHCP, Frame Relay, HDLC, ICMP, IP, PPP, PPPoA, PPPoE, IPSec.	
Descripción	Cisco que reúne las mejores cualidades de un Router convencional en el modelo 7613, ofrece configuraciones flexibles, arquitectura distribuida, reducción de costos y la protección de las inversiones.	
Entradas MAC	64.000	

Tabla 4. 8: Características técnicas, equipo CISCO 7613

- **Equipo que cumple con las características requeridas U-PE**

Se plantea como alternativa de uso, equipos de la marca CISCO serie ME 3600 ya que cumplen con las características necesarias para poder proveer el servicio.

MARCA Y MODELO	CISCO 3600	
Tipo de dispositivo	24 puertos SFP Gigabit Ethernet y dos 10 Gigabit Ethernet SFP puertos +	
Características del chasis	Cuenta con 1 slot	
Memoria RAM	DRAM: 1 GB Flash: 64 MB Búfer de paquetes: 44MB	
Interfaces	24 x 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x 10Base-T/100Base-TX/1000Base-T - RJ-45 - gestión 1 x consola - RJ-45 - gestión 2 x SFP+	
Protocolos	IP Routing (RIP, OSPF, EIGRP, IS-IS, BGP) y BFD Ethernet OAM (802.1ag, 802.3ah, E-LMI, 1731 PM)	
Descripción	Permite a los proveedores de servicios sobre redes IP/MPLS ofrecer una variedad de aplicaciones, Layer 2 Tunneling Protocol (L2PT) Servicios de LAN privada virtual (VPLS), VPLS jerárquico (H-VPLS)	
Entradas MAC	64.000	

Tabla 4. 9: Características técnicas, equipo CISCO 3600

- **Comparación de costos referenciales de los Equipo N-PE y U-PE**

Las proformas correspondientes de costos se encuentran en el Anexo G.

MODELO	TOTALTEK	ANDEAN TRADE
CISCO 7606-S	$ 37.734,31	$ 36.278,67
CISCO 7613-S	$ 44.558,91	$ 47.038,69
CISCO ME 3600	$ 7.180,32	$ 13.538,72
TOTAL	**$ 89.473,54**	**$ 96.856,08**

Tabla 4. 10: Comparativa costos referenciales

De acuerdo a los costos obtenidos de los dos proveedores de equipos expuestos en la tabla 4.10, se utiliza la proforma de TOTALTEK para hacer la selección de equipos.

- **Criterios para escoger los equipos**

En cuanto al equipo N-PE, el criterio para escoger éste equipo depende del costo y las características que ofrezcan, para una mejor prestación del servicio en un futuro; en base a esto se plantea lo siguiente:

La diferencia relevante entre los equipos Cisco 7613 y 7606 es el número de stots y la velocidad de conmutación en una relación aproximada de dos a uno, sin embargo esto no se ve reflejado a nivel de costos, por tal motivo se considera que la mejor opción es escoger el modelo Cisco 7613 ya que éste permitirá un mayor crecimiento de servicios con la única diferencia de costos igual a $ 6.824,60.

En cuanto al equipo U-PE el criterio para escoger éste equipo es que cumpla las característica requeridas planteadas, para el caso específico de la CNT se propone el equipo CISCO ME 3600, ya que extiende la velocidad de transporte a grandes capacidades en orden de los Gigabits/segundo en la capa de acceso para las aplicaciones de usuarios finales permitiendo dar servicios basados en VPN; simplificando la operación de la red.

- **Descripción final de costos**

Se realiza un cálculo del costo total referencial para los equipos a utilizarse en el caso de implementar la solución HVPLS, basándose en la adquisición de un equipo N-PE y un equipo U-PE, si se requeriría añadir más equipos el valor final sería de acuerdo al factor agregación.

Equipo	Cantidad	Precio Unitario
CISCO 7613-S	1	$ 37.734,31
CISCO ME- 3600	1	$ 7.180,32
Total	2	$44.914,63

Tabla 4. 11: Costo total entre Equipo N-PE y U-PE

La tabla 4.11 indica el costo total en la adquisición de un equipo N-PE y U-PE; se toma como fecha referencial el 11 de marzo del 2013.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Las soluciones establecidas y planteadas en este proyecto de titulación son el resultado del análisis obtenido de los clientes ISPs de la CNT E.P., por lo que los criterios de análisis pueden servir de ejemplo para realizar el diagnóstico de cualquier otra red y ser interpretados de acuerdo a los razonamientos propios del administrador de red para el planteamiento de soluciones.

- Se puede utilizar diferentes herramientas de monitoreo y diagnóstico para determinar problemas en una red de datos, sin embargo con el uso de Wireshark, Cacti y la ayuda de los comandos de administración propias del IOS de cisco, se pudo obtener de una manera general estado del servicio VPLS de la CNT y de esta manera se pudo determinar los problemas de las mismas.

- Ante un crecimiento topológico de la red del servicio VPLS, se concluye que el costo de agregar un equipo U-PE para HVPLS a diferencia de agregar un nuevo equipo PE en VPLS, es considerablemente más bajo ya que evita realizar un mallado de mayor tamaño reduciendo la señalización entre los equipos PEs, por lo que implica una buena solución a nivel de extender el dominio VPLS.

- Se concluye que la segmentación de VLANs disminuye la replicación de paquetes en los equipos PEs y además reduce o soluciona las posibilidades de tormentas de broadcast, ya que divide un único dominio en varios, también

se pueden identificar más fácilmente los problemas en dominios más reducidos.

- La seguridad del servicio VPLS depende directamente de que tan vulnerable sea el core IP/MPLS, ya que es un servicio transportado a través de él; al ser VPLS una VPN en capa 2 implica que es segura y que de manera externa es improbable que sea vulnerada, sin embargo está expuesta al riesgo que involucra una amenaza ejecutada desde el Core de la red. VPLS transporta todo el tráfico que envía el cliente, de tal forma que también puede llevar amenazas dentro de la propia VPLS si el administrador de red no aplica las correctas políticas de seguridad en su red interna.

- Al revisar las configuraciones de las VPLSs se concluye que la transparencia y claridad del servicio es un elemento que permite optimizar el servicio ya que anticipa un diagnóstico de problemas o cambios de parámetros con mayor rapidez.

- Se concluye que no todo problema reportado por el cliente implica mal funcionamiento del servicio que se le provee; ya que pueden ser problemas de causa interna; un administrador de red puede determinar esto mediante un previo análisis.

- Se concluye que VPLS y HVPLS tienen sus ventajas propias de acuerdo a las necesidades del cliente según sus requerimientos; HVPLS es la solución a VPLS si este llega a presentar un crecimiento topológico.

5.2 RECOMENDACIONES

- La solución establecida para un cliente que requiera el servicio VPLS debe ser analizada de acuerdo a los requerimientos y las necesidades que tenga, ya sea a nivel de una arquitectura full mesh con o sin segmentación, por ejemplo de acuerdo a la cantidad de usuarios.

- Es de mucha importancia tener un monitoreo constante con diferentes herramientas que ayuden a estimar de mejor manera el comportamiento del servicio para de esta forma poder actuar de manera inmediata ante la presencia de anomalías y mejorar el servicio brindado hacia los clientes.

- Se recomienda la utilización de las mejores prácticas planteadas como ayuda y guía a los usuarios que utilicen o puedan llegar a manejar el servicio VPLS, pues una administración o implementación del servicio basado en un correcto manejo es fundamental para obtener los resultados deseados.

- La infraestructura de cada proveedor depende de los servicios que ofrezca, por lo tanto no se tiene definido un valor máximo de MTU para cada servicio ya que cada equipo interno puede añadir cabeceras de diferentes tamaños de bytes, se ha definido teóricamente que el valor mínimo de MTU para las VPLSs es de 1530 bytes, de tal manera se recomienda utilizar un valor mayor a este para evitar problemas de fragmentación.

- Es recomendable realizar el estudio de las troncales de interconexión, esto para soportar un incremento de tráfico por la presencia de más usuarios a futuro, de esta manera se evitará tener varios clientes masivos en una misma troncal lo que podría implicar la saturación en su capacidad, además es primordial monitorizar las troncales de forma que se pueda ir ampliando caudales en función de las necesidades de tráfico.

- Se recomienda a nivel de administración deshabilitar servicios no utilizados mediante los comandos IOS de cada equipo y como por habilitación de traps generadas por eventos o cambios de configuración en los equipos.

- Entre las políticas de seguridad se recomienda, asegurar o restringir el acceso a los equipos PEs para evitar ataques a los mismos, para esto se puede utilizar ACLs, servidores de control de acceso, uso de firewalls y encriptación de la información.

- Se recomienda considerar criterios de crecimiento topológico y de usuarios, para tener una planificación a futuro de las alternativas de solución que se puedan dar a nivel de escalabilidad en el servicio.

REFERENCIAS BIBLIOGRÁFICAS Y ELECTRÓNICAS

LIBROS Y MANUALES

[1] VIVEK, Alwayn. “Advanced MPLS Desing and Implementation”. Cisco Press. Estados Unidos de América. Septiembre, 2001.

[2] ALMEIDA ARCOS, Carlos Andrés. “Arquitectura de Redes MPLS”. Academia de Certificaciones Internacionales en Redes y Tecnología de Información ACIERTE-EPN. Quito, Ecuador. Junio, 2011.

[3] WITTERS, Johan, SUNIL Khandekar, CLERCQ, Jeremy. “Tutorial Técnico VPLS”, Revista de Telecomunicaciones de Alcatel, 2004.

[4] Información proporcionada por el área O&M Plataforma IP/MPLS de la CNT EP.

[5] BORJA MERINO, Febrero. “Análisis de Tráfico con Wireshark”. INTECO-CERT”. 2011.

[6] ANÓNIMO. “Triple Play Service Scalability”. Huawei Technologies. 2007.

[7] BECERRO MARTÍNEZ, Antonio. “Guía Rápida de VNC, GNU”. Free Documentation License. 2005.

PROYECTOS DE TITULACIÓN

[8] CHÁVEZ PAREDES, Diego Lenin, MONTERO REVELO Silvana Fernanda. “Diseño para la migración de la red de SETEL hacia un carrier que utiliza tecnología MPLS, para proveer servicios de VoIP en todo el Distrito Metropolitano de Quito”. Marzo, 2008.

[9] BAEZ MARÍN, Jorge Gustavo, CEVALLOS QUINTANILLA, César Orlando, "Estudio y diseño de una red basada en tecnología MPLS para un carrier de datos". EPN. Noviembre, 2002.

[10] COSIOS CASTILLO, Eduardo Richard, SIMBAÑA LOACHAMÍN, Wilson Xavier. "Estudio y diseño de redes virtuales privadas (VPN) basadas en tecnología MPLS". EPN. Junio, 2004.

[11] SEGARRA ZAMBRANO, Ana Lucía. "Estudio de redes privadas virtuales basadas en la tecnología MPLS". ESPE, 2009.

[12] ORIHUELA SESMERO, Pablo. "Diseño de una Red VPLS Jerárquica". Universidad Carlos III, Madrid, España.

[13] ALBUJA OÑATE, Fernando René. "Diseño de una red inalámbrica aplicando tecnología WIMAX para los cantones de Cayambe, Pedro Moncayo y Otavalo para la Corporación Nacional de Telecomunicaciones CNT EP S.A.". EPN. Enero, 2010.

[14] HIDALGO LLUMIQUINGA, Luis Carlos, LAGUAPILLO MUÑOZ, David Alejandro. "Diseño e implementación de un laboratorio que permita emular y probar servicios IP y MPLS de la red de backbone CISCO de la Corporación Nacional de Telecomunicaciones CNT EP".EPN. Noviembre, 2011.

[15] CALVA POMA, Sandra Elizabeth. "Guía para el uso de herramientas propietarias y de libre difusión de la evaluación de Redes". EPN. Septiembre, 2010.

[16] FALCONÍ NORIEGA, Marco Fabricio, RODRÍGUEZ GARCÍA, Lucía Silveria. "Análisis de riesgos de la red IP/MPLS de la Corporación Nacional de Telecomunicaciones, basado en la norma ISO/IEC 27005 y propuesta de mejoramiento del control de acceso a la administración de sus dispositivos". EPN. Enero, 2012.

[17] JARAMILLO RODRÍGUEZ, María Soledad. “Diseño para la migración de una red de tecnología Metro Ethernet a la tecnología MPLS, para la empresa portadora de servicios de telecomunicaciones Puntonet S.A. para la ciudad de Quito”. EPN. Enero, 2011.

DIRECCIONES ELECTRÓNICAS

[18] CANALIS, María Sol. “MPLS (Multiprotocol Label Switching): Una Arquitectura de Backbone para la Internet del Siglo XXI”**.** Universidad Nacional del Nordeste. Corrientes, Argentina.
http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MPLS.PDF

[19] ANÓNIMO.“L2 VPN Any to Any Interworking”. MPLS Configuration on Cisco IOS Software.
http://mpls-configuration-on-cisci- iossoftware.org.ua/1587051990/ch11lev1sec3.html

[20] HERRERA JOANCOMARTI, Jordi**,** GARCIA ALFARO, Joaquín, PERRAMÓN TORNIL, Xavier. “Aspectos avanzados de seguridad en redes”. Barcelona, España. Julio, 2004.
http://www.sw-computacion.f2s.com/Linux/012.1-Aspectos_avanzados_en_seguridad_en_redes_modulos.pdf

[21] ANÓNIMO. “Seguridad en capa 2: VLANs Privadas”. Redes Cisco. NET
http://www.redescisco.net/v2/art/seguridad-en-capa-2-vlan-privadas

[22] ANÓNIMO. “Seguridad en Switch”.
http://es.scribd.com/doc/58116973/4/Describiendo-un-ataque-de-inundacion-MAC.

[23]CUSTODIO SALVADOR, Arturo. “Evolución del modelo de agregación en redes de Banda Ancha”. Arquitectura y soluciones de red en Alcatel-Lucent. España. Marzo, 2008.
http://www.coit.es/publicaciones/bit/bit167/tendenciascustodio.pdf

[24] ANÓNIMO. “SPAN, RSPAN, and ERSPAN”. Catalyst 6500 Release 12.2SX Software Configurations Guide. Cisco System.
http://www.cisco.com/en/US/docs/routers/asr9000/software/asr9k_r4.0/interfaces/configuration/guide/hc40span.pdf

[25] BERRY, Ian, ROMAN, Tony, ADAMS, Larry, CONNER, Jimmy, SCHECK, Reinhard, BRAUN, Andreas. “The Cacti Manual”. The Cacti Group. 2010.
http://www.cacti.net/downloads/docs/html/

[26] ANÓNIMO, “Bridging vs Routing en redes inalambricas PtmP”. Albentia System. Mayo, 2010.
http://www.albentia.com/Docs/WP/ALB-W-000007_BridgingvsRoutingA1.pdf

[27] REY, Enno. “MPLS and VPLS Security”.
http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Rey-up.pdf

[28] GAGLIANO, Roque. “Virtual Private LAN Service VPLS sobre un backbone MPLS”. IEE-Facultad de Ingeniería. 2003.
http://es.scribd.com/doc/95862870/Vitual-Private-Lan-Service-VPLS-Sobre-Un-Backbone-MPLS

[29] ANÓNIMO. “VNC”. Community Help Wiki. 2012.
https://help.ubuntu.com/community/VNC

ANEXOS

CONTENIDO ANEXOS

NOTA: Los Anexos se presentan en el cd adjunto.

ANEXO A

SITUACIÓN ACTUAL DEL SERVICIO VPLS DE LOS ISPs A ANALIZAR

A. 1 ESQUEMA LÓGICO DEL SERVICIO VPLS

Se detalla el esquema lógico de la red VPLS para cada ISP, donde se indica: equipo PE al que se conecta el cliente, troncal asignada en el equipo PE, equipos de acceso y circuito virtual.

A.1.1 ESQUEMA LÓGICO ISP-1

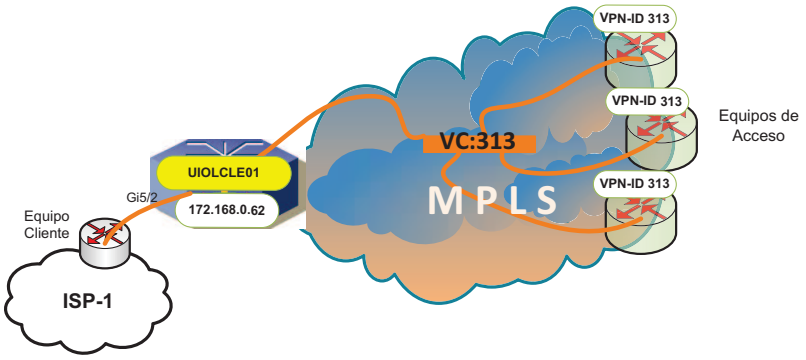


Figura A. 1: Diagrama interconexión VPLS ISP-1

A.1.2 ESQUEMA LÓGICO ISP-2

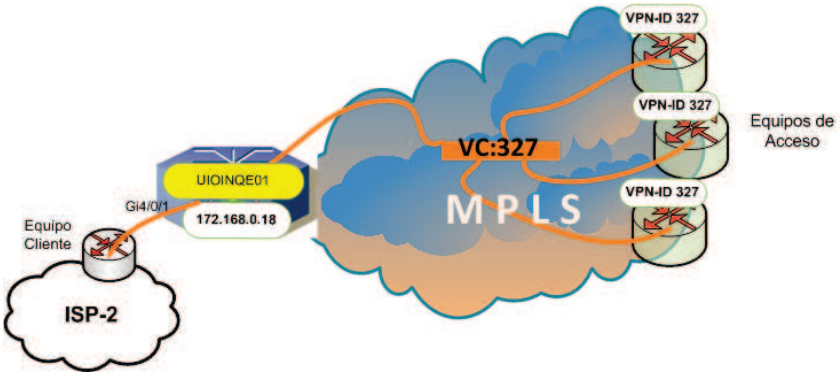


Figura A. 2: Diagrama interconexión VPLS ISP-2

A.1.3 ESQUEMA LÓGICO ISP-3

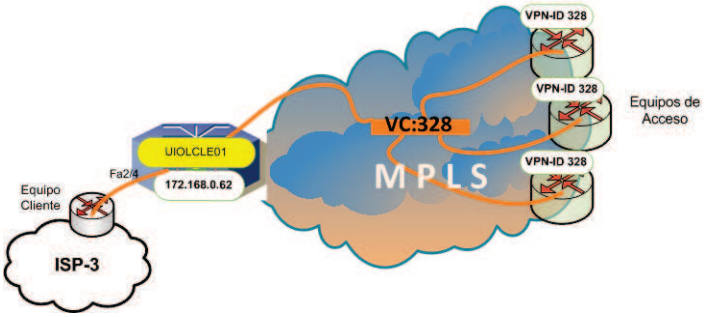


Figura A. 3: Diagrama interconexión VPLS ISP-3

A.1.4 ESQUEMA LÓGICO ISP-4

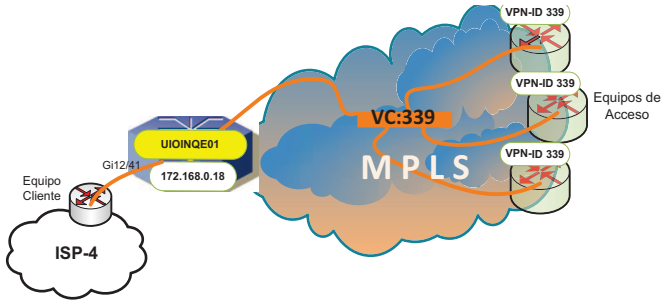


Figura A. 4: Diagrama interconexión VPLS ISP-4

A.1.5 ESQUEMA LÓGICO ISP-5

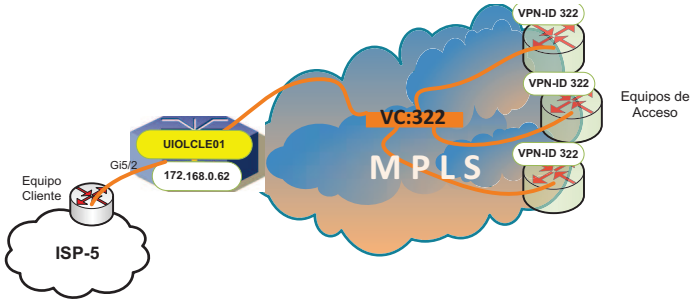


Figura A. 5: Diagrama interconexión VPLS ISP-5

A.1.6 ESQUEMA LÓGICO ISP-6

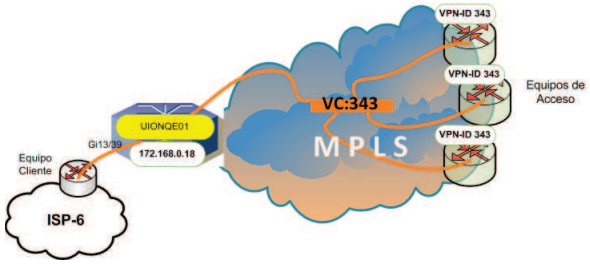


Figura A. 6: Diagrama interconexión VPLS ISP-6

A.1.7 ESQUEMA LÓGICO ISP-7

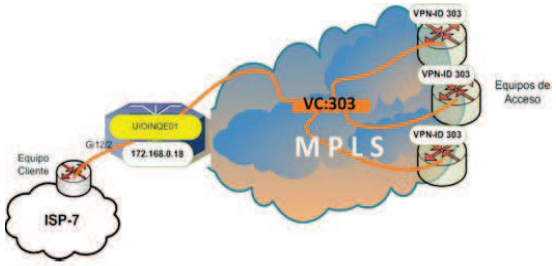


Figura A. 7: Diagrama interconexión VPLS ISP-7

A.1.8 ESQUEMA LÓGICO ISP-8

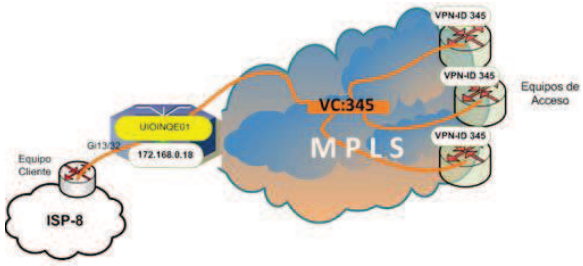


Figura A. 8: Diagrama interconexión VPLS ISP-8

A.1.9 ESQUEMA LÓGICO ISP-9

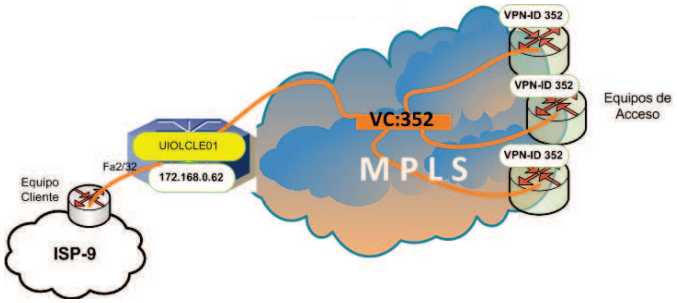


Figura A. 9: Diagrama interconexión VPLS ISP-9

A.1.10 ESQUEMA LÓGICO ISP-10

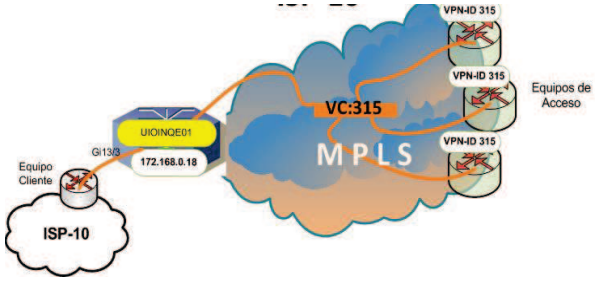


Figura A. 10: Diagrama interconexión VPLS ISP-10

A.1.11 ESQUEMA LÓGICO ISP-11

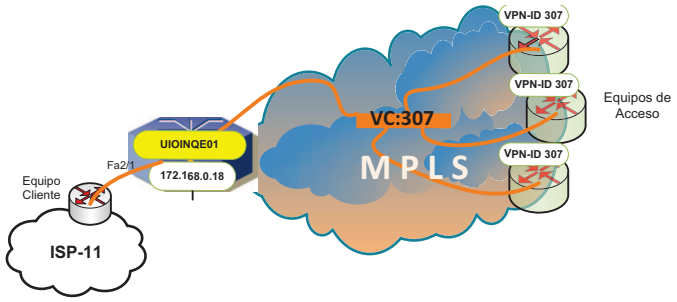


Figura A. 11: Diagrama interconexión VPLS ISP-11

A.1.12 ESQUEMA LÓGICO ISP-12

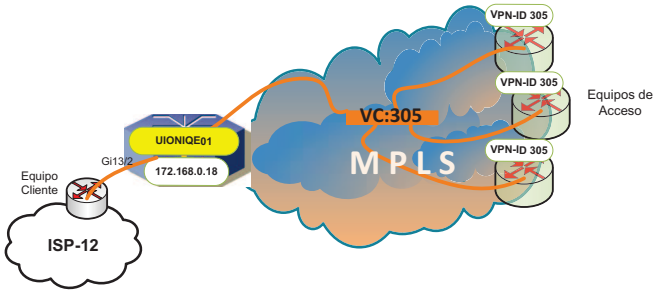


Figura A. 12: Diagrama interconexión VPLS ISP-12

A.1.13 ESQUEMA LÓGICO ISP-13

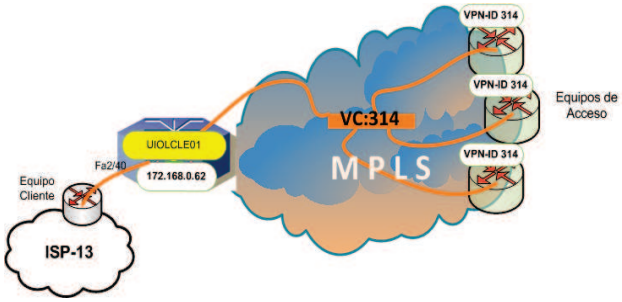


Figura A. 13: Diagrama interconexión VPLS ISP-13

A.1.14 ESQUEMA LÓGICO ISP-14

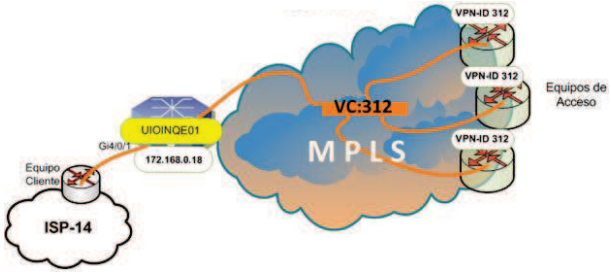


Figura A. 14: Diagrama interconexión VPLS ISP-14

A.1.15 ESQUEMA LÓGICO ISP-16

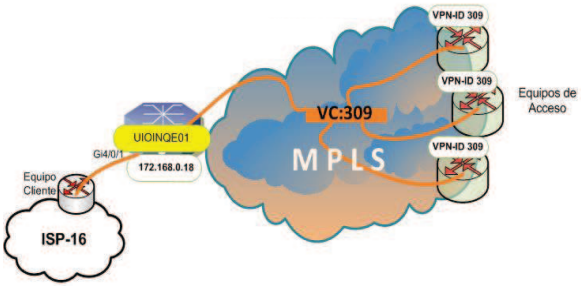


Figura A. 15: Diagrama interconexión VPLS ISP-16

A.1.16 ESQUEMA LÓGICO IP-FIJA

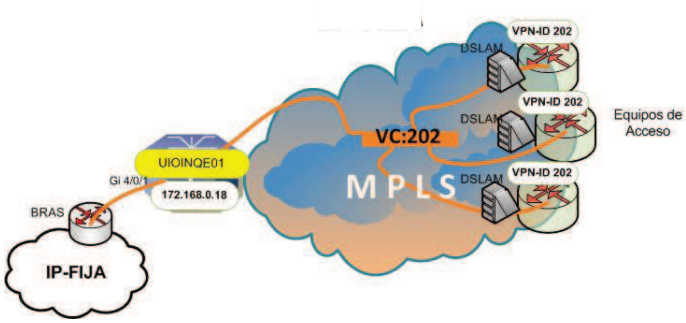


Figura A. 16: Diagrama VPLS IP FIJA

ANEXO B

HERRAMIENTAS DE MONITOREO UTILIZADAS EN EL ANÁLISIS DEL SERVICIO VPLS

B. 1 WIRESHARK

B.1.1 DESCRIPCIÓN GENERAL [1], [3], [5]

El *Sniffer*[17] Wireshark, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones.

Es muy utilizado como herramienta didáctica ya que permite ver todo el tráfico que pasa a través de una red, aplicar filtros para observar los paquetes de un protocolo concreto o examinar un archivo de captura previamente salvado en disco.

B.1.2 CARACTERÍSTICAS [3]

- Disponible para LINUX, WINDOWS y Mac OS.
- Captura los paquetes directamente desde una interfaz de red sea esta alámbrica o inalámbrica.
- Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.
- Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.
- Permite hacer un filtro que cumpla con un criterio previamente definido.
- Permite obtener estadísticas y gráficas mediante el uso de colores que identifican el filtro especificado.

B.1.3 INSTALACIÓN [4]

La instalación es sumamente sencilla, debido a que es un programa de licencia libre, este brinda todas las facilidades para su instalación y posterior uso y operación.

[17] Un Sniffer es un programa para monitorear y analizar el tráfico en una red.

El instalador y los archivos binarios de Wireshark pueden ser descargados en *http://www.wireshark.org/download.html.*

Wireshark soporta múltiples plataformas entre ellas UNIX, LINUX y Windows, su instalación se describe a continuación:

B.1.3.1 Instalación UNIX

Para iniciar la instalación se debe contar con las siguientes utilidades instaladas:

- GTK+, GIMP Tool Kit y Glib
- libpcap

Si es el caso de obtener los archivos fuentes, los siguientes pasos describen el proceso para descomprimir los archivos y generar el ejecutable:

Según la distribución de UNIX, se aplica el comando correspondiente para descomprimir el archivo obtenido.

- En versiones de UNIX con GNU tar

tar zxvf wireshark-1.0.0-tar.gz

- En caso contrario se deberá ejecutar los siguientes comandos

gzip –d wireshark-1.0.0-tar.gz
tar xvf wireshark-1.0.0-tar

Los pasos a seguir son los siguientes:

1. Cambiar al directorio raíz de Wireshark

cd <ruta_directorio_wireshark>

2. Configuración de los archivos fuentes con el objetivo de asegurar su buen funcionamiento en la versión de UNIX correspondiente.

./configure

3. Para generar el archivo ejecutable se debe aplicar el siguiente comando:

make

4. Finalmente para culminar la instalación de la aplicación se ejecuta el comando:

make install

Otros métodos aplicados según la distribución, Debian o sus derivados (Ubuntu, por ejemplo). La instalación es mucho más fácil con este comando:

sudo apt-get install wireshark

Además la mayoría de las distribuciones lo incluyen en sus repositorios, por lo que también es sencilla su instalación.

B.1.3.2 Instalación Windows

Una vez que se obtiene el instalador, y se corre el ejecutable para iniciar la instalación.

El instalador de Wireshark para Windows permite hacer la instalación de las librerías, plugins, servicios, etc. Después se sigue con la ayuda del asistente, escogiendo las opciones que se desee hasta que la instalación se hay realizado con éxito.

B.1.4 INTERFAZ DE USUARIO

En la figura B.1 se muestra la interfaz de usuario y las principales secciones del panel de Wireshark.

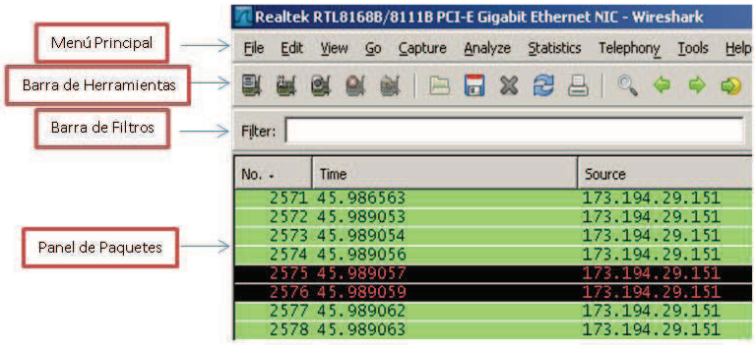


Figura B. 1: Interfaz de Usuario

La interfaz principal de Wireshark cuenta con varias secciones que se describen a continuación:

- Menú principal

  - ✓ **File,** manipulación de archivos.
  - ✓ **Edit,** funciones de los paquetes y configuración de interfaz de usuario.
  - ✓ **View,** configurar el despliegue de la pantalla capturada.
  - ✓ **Go,** desplazamiento entre los paquetes.
  - ✓ **Analyze,** manipulación de filtros, habilitación de protocolos.
  - ✓ **Stadistics,** estadísticas de captura.
  - ✓ **Help,** menú de ayuda.

- Barra de herramientas principal, permite el acceso rápido a las funciones más utilizadas.
- Barra de herramientas para filtros, donde se aplica el filtro que se desea aplicar a los paquetes que están siendo capturados.
- Panel De Paquetes Capturados, donde se despliega las lista de paquetes capturados.

En la figura B.2 se puede ver líneas de colores que corresponden a cada paquete capturado al seleccionar una de estas, ciertos detalles son desplegados en los paneles inferiores, que muestran características de la trama.

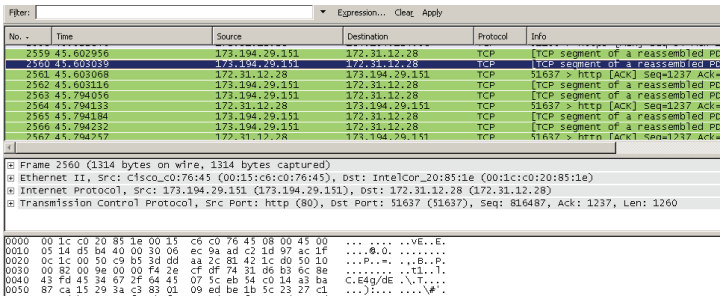


Figura B. 2: Panel de Paquetes capturados

Las columnas muestran datos del paquete capturado, Wireshark dispone de una gran cantidad de detalles que pueden agregarse en estas columnas desde el menú Edit->Preferences, por defecto se tiene:

- **No:** posición del paquete en la captura.
- **Time:** muestra el Timestamp del paquete.
- **Source:** dirección origen del paquete.
- **Destination:** dirección destino del paquete.
- **Protocol:** nombre del protocolo del paquete.
- **Info:** información adicional del contenido del paquete.

La ventana se divide en tres zonas: En la superior se muestra la lista de tramas/paquetes capturados, a razón de una línea por paquete. En la intermedia se muestra en detalle la estructura del paquete seleccionado en la primera, y en la inferior se muestra el contenido del paquete en hexadecimal.

Para analizar un paquete basta con pincharlo en la zona superior; entonces se puede seleccionar alguno de los campos que aparecen en la zona intermedia y desglosarlo en sus partes si las tiene. Al seleccionar algún campo de la zona intermedia automáticamente queda seleccionado en la inferior el contenido en hexadecimal correspondiente, con lo que es posible analizar el contenido con todo detalle.

B.1.5 ANÁLISIS DE TRÁFICO CON WIRESHARK [1], [3], [5]

Después de realizar una captura, el volumen de datos presentado puede llegar a ser interminable, entonces se puede hacer uso de las diferentes herramientas que Wireshark dispone para analizar los datos obtenidos, las más utilizadas y las que permiten cumplir el objetivo son:

B.1.5.1 IO GRAPHS

Se puede representar un gráfico de entrada/salida. El acceso a dicho gráfico, ver figura B.3, se consigue a través del menú Statistics/IO Graphs.

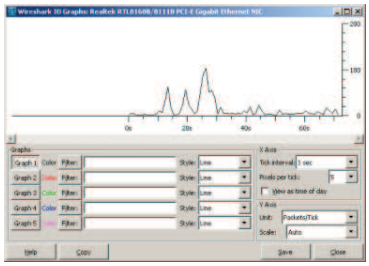


Figura B. 3: IO Graphs

Como podemos observar, las opciones de representación de los datos son muy variadas, ya que se nos permite el filtrado de los mismos de diferentes maneras.

Los parámetros seleccionados en IO Graphs, son de acuerdo a como se desea obtener la gráfica, estas opciones son:

- La opción de filter, permite especificar el protocolo que se desea graficar, cada uno de estos filtros es representado por diferentes colores.
- La opción style, permite establecer la forma de la línea que representa el tráfico, en este caso se representa con forma de línea, que es el valor por defecto.

La zona de edición tiene dos ejes:

- Eje X de tiempo: En este eje se puede ajustar el Tick Interval o intervalo de tiempo desde centésimas de segundo a 10 minutos. También hay una especie de Zoom, el Pixel per Ticks, ajustable de 1 a 10.

- Eje Y de paquetes capturados: En este eje se puede visualizar los datos por Paquetes, Bytes, Bits, o de forma avanzada realizando ciertas operaciones. Podemos también ajustar la escala del eje en Scale.

B.1.5.2 EXPERT INFO

La funcionalidad Expert Info es algo similar a un registro de anomalías que detecta automáticamente Wireshark en un fichero de captura. Cuando se tiene una captura con un número muy elevado de paquetes y no se pretende buscar una situación específica y se necesita agilizar el proceso de identificación de anomalías en la red, se puede hacer uso de la opción Expert Info, ver figura B.4, a la cual accedemos mediante el menú Analyze/Expert Info.

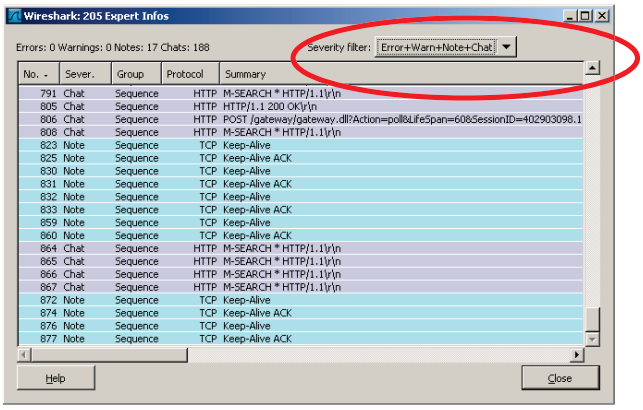


Figura B. 4: Expert Info

El cuadro desplegable de la parte superior derecha nos permite filtrar la salida de información (por defecto, se presentarán los errores, los avisos, las notificaciones y las negociaciones de protocolo), la cual es presentada en pantalla resaltada por diferentes colores.

Para una mejor visualización y organización por categoría en las opciones por defecto, se presentarán los errores, los avisos, las notificaciones y las negociaciones de protocolo, existe la opción Expert Info Composite, como se observa en la figura B.5, separa en listas cada opción.

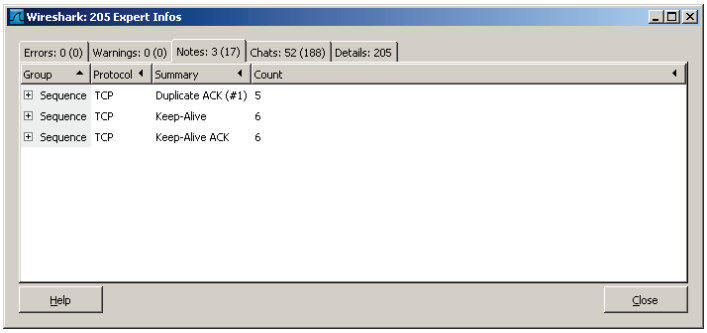


Figura B. 5: Expert Info Composite

La idea principal de esta herramienta es mostrar comportamientos inusuales o situaciones anómalas en la red, como retransmisiones o fragmentación. De esta forma, se pueden identificar más rápidamente problemas en la red.

Como se indica en la figura B.6, con esta opción se puede ver las entradas por cada categoría, estas entradas incluyen: grupo, protocolo, un resumen y la cantidad de paquetes pertenecientes a cada categoría.

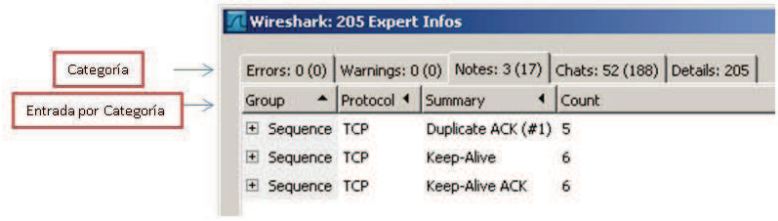


Figura B. 6: Entradas por Categoría Expert Info Composite

Los diferentes niveles de categoría de acuerdo a la severidad del evento usados son los siguientes:

- Error: Problemas graves como paquetes mal formados, pérdida de paquetes.
- Advertencia: Indica atención, problemas de conexión.
- Note: Reporte de errores usuales que no significan un problema serio.
- Chat: Información sobre conversaciones de protocolos.

Los tipos de grupos de falla más comunes dentro de las categorías que se puede encontrar son:

- Checksum: una suma de comprobación no es válida.
- Secuencia: secuencias de protocolo sospechosas como no continua o retransmisión.
- Código de Respuesta: problemas con códigos de respuesta de aplicaciones.

- Sin decodificar: división incompleta o los datos no se pueden decodificar por otros motivos.
- Ensamblado: problemas en el re ensamblaje.
- Mal formados: paquetes mal formados, errores graves, etc.

Todos estos errores, avisos, notificaciones e informaciones, nos proporciona el Expert Info Composite, como se puede ver se derivan de diversos factores y el objetivo no es analizar cada uno de ellos, solo servirán de referencia para saber en qué porcentaje existen paquetes con problemas en el análisis.

Como ya se indicó las categorías de acuerdo a su grado de severidad, se toma en cuenta en este análisis las que corresponden a Errores y Advertencias, ya que estas indican pérdida de paquetes.

Dentro de estos encontramos:

- Paquetes mal formados (Errores): son aquellos demasiado cortos para analizar el puerto, código ICMP su tipo y son ignorados (dropped) cuando dichos paquetes intentan llegar, por lo tanto representan pérdida de paquetes.

- Secuencia (Advertencias): son secuencias de protocolo no continuas o retransmisiones. Un Porcentaje de este tipo de paquetes representan pérdida de paquetes.

B. 2 PORT-MIRRORING [1], [10]

B.2.1 DESCRIPCIÓN GENERAL

Port-mirroring es una función que sirve para reflejar todo el tráfico de un puerto específico a otro puerto, ver figura B.7 generalmente se utiliza para atrapar todo el

tráfico de una red y poder analizarlo (con herramientas como whireshark por ejemplo).

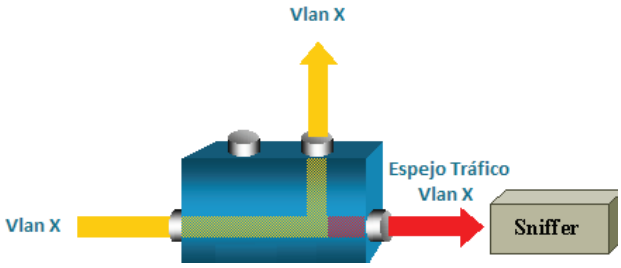


Figura B. 7: Port-mirroring

Esto es muy útil cuando necesitamos monitorizar el tráfico de red o detectar intrusiones en la red cuando no se puede tener un acceso físico directo. El uso de Port-mirroring no afecta a la conmutación del tráfico en las fuentes.

Dependiendo del fabricante tiene diferente terminología, en Cisco el Port-mirroring se llama Switched Port Analyzer (SPAN).

Para este proyecto se referirá a la configuración en equipos Cisco, porque la arquitectura manejada es marca Cisco.

B.2.2 TIPOS DE PORT MIRRORING EN CISCO

Se puede configurar diferentes tipos de SPAN dependiendo de los recursos que se utilice, SPAN locales, RSPAN o ERSPAN.

- Una sesión SPAN local es una asociación de puertos de origen y fuente de VLAN con uno o más destinos. Una sesión SPAN local se configura en un mismo equipo.

- RSPAN (Remote SPAN) soporta puertos de origen, fuente de VLAN, y destinos en equipos diferentes, lo que proporciona un control remoto de múltiples equipos en la red. RSPAN utiliza una VLAN de capa 2 para transportar el tráfico.

- ERSPAN (Encapsulated Remote SPAN) soporta lo mismo que el tipo RSPAN, con la diferencia que el tráfico se transporta mediante un túnel GRE[18] (Generic Routing Encapsulation / Encapsulación de enrutamiento genérica).

  En este proyecto por motivos de seguridad y ya que los datos van encapsulados, el monitoreo se realizará utilizando ERSPAN.

B.2.2.1 ERSPAN

Para la configuración, se asocia un conjunto de puertos de origen o VLAN con una dirección IP de destino, número de ID ERSPAN. Y para configurar una sesión de destino ERSPAN en otro switch, se asocia el destino con la dirección IP de origen, número de ID ERSPAN, se configuran por separado en diferentes equipos.

B.2.2.1.1 Configuración de sesiones ERSPAN Fuente

- Para configurar una sesión de fuente ERSPAN, realizar tarea de la tabla B.1:

PASOS	COMANDO	PROPÓSITO
Paso 1	`Router # configure terminal`	Entra en el modo de configuración global.
Paso 2	`Router(config)# monitor session source_session_number type Erspan-source`	Configura número de sesión y tipo de la fuente.
Paso 3	`Router(config-mon-erspan-src)# description session_description`	(Opcional) Describe la sesión fuente.
Paso 4	`Router(config-mon-erspan src)# source single_interface |interface_list |interface_range |mixed_interface_list |single_vlan | vlan_list |vlan_range |mixed_vlan_list} [rx | tx | both]}`	Asocia la fuente los puertos de origen, o VLANs, y selecciona la dirección del tráfico a controlar.
Paso 5	`Router(config-mon-erspan-src)# destination`	Entra a sesión destino al modo de configuración.

[18] Es un protocolo para el establecimiento de túneles a través de Internet, propietario de CISCO.

Paso 6	`Router(config-mon-erspan-src-dst)# ip address ip_address`	Dirección IP destino, a donde se va a enviar el tráfico.
Paso 7	`Router(config-mon-erspan-src-dst)# erspan-id ERSPAN_flow_id`	Configura el número de identificación de sesión.
Paso 8	`Router(config-mon-erspan-src-dst)# origin ip address ip_address`	Configura la dirección IP que se utiliza como el origen del tráfico ERSPAN.
Paso 9	`Router(config-mon-erspan-src)# no shutdown`	Activa la sesión fuente ERSPAN.
Paso 10	`Router(config-mon-erspan-src-dst)# end`	Sale del modo de configuración.

Tabla B. 1: Configuración de sesiones ERSPAN Fuente

B.2.2.1.1 Configuración de sesiones ERSPAN destino

- Para configurar una sesión de destino ERSPAN, realizar tarea de la tabla B.2:

PASOS	COMANDO	PROPÓSITO
Paso 1	`Router# configure terminal`	Entra en el modo de configuración global.
Paso 2	`Router(config)# monitor session destination_session_number type Erspan-destination`	Configura número de sesión y tipo de la fuente.
Paso 3	`Router(config-mon-erspan-dst)# description session_description`	(Opcional) Describe la sesión fuente.
Paso 4	`Router(config-mon-erspan-dst)# destination {single_interface | interface_list | interface_range | mixed_interface_list} [ingress [learning]]`	Específica donde se recibe el tráfico.
Paso 5	`Router(config-mon-erspan-dst)#source`	Entra a sesión origen al modo de configuración.
Paso 6	`Router(config-mon-erspan-dst-src)# ip address ip_address`	Configura dirección IP, donde se recibe el tráfico.
Paso 7	`Router(config-mon-erspan-dst-src)# erspan-id ERSPAN_flow_id`	Configura el número de identificación de sesión.
Paso 8	`Router(config-mon-erspan-dst)# no shutdown`	Activa la sesión de destino ERSPAN.
Paso 9	`Router(config-mon-erspan-dst-src)# end`	Sale del modo de configuración.

Tabla B. 2: Configuración de sesiones ERSPAN Destino

Como otra herramienta útil para monitorear tráfico, existe un potente software con el que se puede controlar en todo momento el estado de nuestra red, denominada Cacti. Este sistema de monitorización, contiene un recolector de datos excelente, un sistema avanzado de creación de plantillas y gráficos, y una completa interfaz de gestión de usuarios, lo que la hace atractiva para su manejo.

Esta herramienta es multiplataforma funciona tanto en Linux como en Windows, su instalación no es realmente compleja y provee seguridad de acceso, los usuarios registrados pueden ingresar mediante un Usuario y una contraseña.

B. 3 CACTI

B.3.1 DESCRIPCIÓN GENERAL

Cacti es una solución completa para la monitorización de redes mediante gráficos diseñada para aprovechar el poder de almacenamiento y la funcionalidad de graficar que poseen las RRDTool's[19].

Esta herramienta, desarrollada en PHP, provee plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios, además de tener una interfaz de usuario fácil de usar. La interfaz de usuario que se presenta es como se indica en la figura B.8.

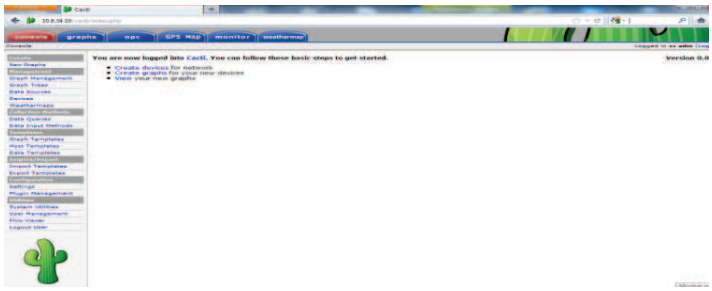


Figura B. 8: Interfaz de usuario de Cacti

[19]Round Robin Database tool (RRDTool). - Este sistema trata la Base de Datos como si fuera un círculo, sobrescribiendo los datos almacenados, una vez alcanzada la capacidad de la misma.

Para hacer uso de una RRDtool, lo que se necesita es un sensor para medir los datos y poder alimentar al RRDtool con esos datos. Entonces, la RRDtool crea una base de datos, almacena los datos en ella, recupera estos datos y se basa en ellos. La aplicación está construida en php[20], y utiliza MySql[21] para el almacenamiento de información sobre los gráficos y datos recogidos. El protocolo utilizado para la gestión con los distintos equipos es SNMP.

- **RRDTOOL**

Es el acrónimo de Round Robin Database tool, o sea que se trata de una herramienta que trabaja con una BD que maneja Planificación Round-robin. El principio de RRDtool es almacenar, recuperar y visualizar información, como se muestra en la figura B.9.

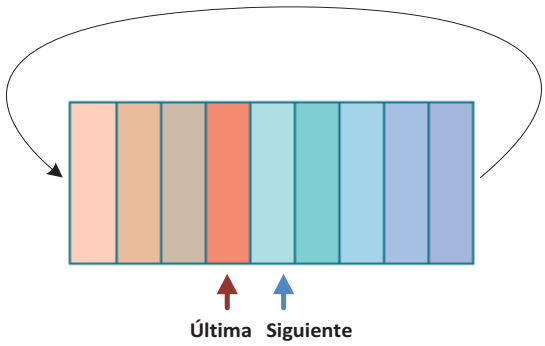


Figura B. 9: Principio de RRDTool

Esta técnica trabaja con una cantidad fija de datos y un puntero al elemento actual. El modo en que trabaja una base de datos utilizando Round Robin es el siguiente; se trata la Base de Datos como si fuera un círculo, sobrescribiendo los datos almacenados cuando se alcanza la capacidad de la de la misma.

[20] Hypertext Pre-processor.- lenguaje de programación interpretado.
[21] Lenguaje de Consulta Estructurado.- sistema de gestión de bases de datos relacional, multihilo y multiusuario

- **PHP**

PHP es un acrónimo recursivo que significa PHP Hypertext Pre-processor, es un lenguaje de programación interpretado, diseñado originalmente para la creación de páginas web dinámicas.

- **BASE DE DATOS**

Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

- **Protocolo SNMP**

SNMP (Simple Network Managment Protocol / Protocolo Simple de Administración de Red) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP.

B.3.2 INSTALACIÓN

Hay dos formas de instalar esta herramienta de graficado de red, monitoreo y gestión. La primera es descargando la fuente desde la página oficial del proyecto www.cacti.net, se debe compilar la aplicación y que la configuración corra por nuestra cuenta.

La segunda es utilizar el administrador de paquetes *apt* para descargar los paquetes pre-compilados desde los repositorios, se ejecuta en una terminal:

apt-get install cacti

Cacti requiere que el siguiente software esté en el sistema, antes de su instalación:

- RRDtool 1.0.49 o 1.2.x o superior
- MySQL 4.1.xo 5.x o superior
- PHP 4.3.6 o superior, mayor 5.x muy recomendable para funciones avanzadas
- Un servidor Web por ejemplo, Apache o IIS

Una vez que se tenga instalado eso se procede con la instalación de Cacti.

B.3.3 PRINCIPIO DE FUNCIONAMIENTO

Cacti se basa en el siguiente principio, en el orden que se indica en la figura B.10.

Figura B. 10: Principio de funcionamiento de Cacti

La primera tarea de Cacti es recuperar los datos. Para recuperar datos de hosts remotos, Cacti, principalmente utilizará el protocolo SNMP. Por lo tanto, todos los dispositivos capaces de utilizar SNMP serán elegibles para ser controlado por los Cacti.

Para la segunda tarea Cacti utiliza RRDtool, el cual almacena los datos de una manera muy compacta con el fin que no se expanda con el tiempo y ayudar a mantener los requisitos de almacenamiento.

Finalmente lo que se desea conseguir es la presentación de los datos, lo cual Cacti lo representa mediante gráficos, la función gráfica integrada es la característica más apreciada de RRDtool.

Esto resulta muy útil cuando se combina con un servidor web de uso común y es posible acceder a los gráficos desde cualquier navegador en cualquier Plataforma.

B.3.4 MANEJO DEL SISTEMA

B.3.4.1 Ingreso al sistema

Para poder comenzar a utilizar la aplicación, en el cuadro de ingreso que se despliega se debe ingresar el nombre de usuario (User Name) y una contraseña (Password) y luego presionar ENTER o hacer clic en Login como se muestra en la figura B.11.

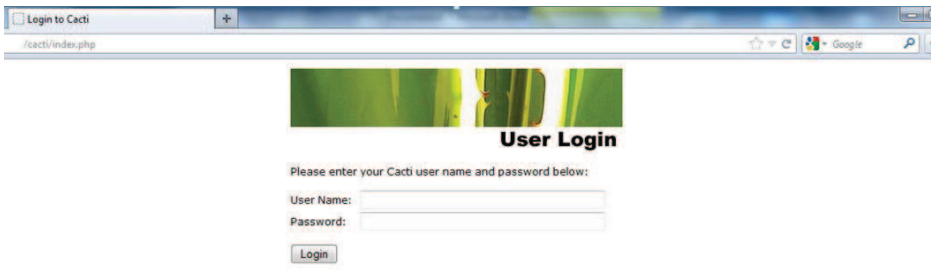


Figura B. 11: Login Cacti

B.3.4.2 Pantalla Inicial

Una vez ingresada el usuario y la contraseña registrada, la pantalla inicial es como se muestra en la figura B.12:

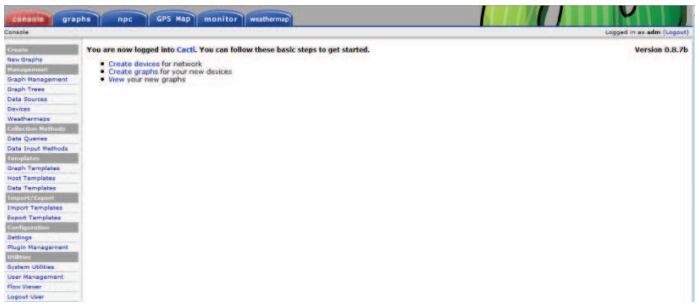


Figura B. 12: Pantalla de Inicio de CACTI.

B.3.4.3 Menús

Brevemente se describe cada menú:

- TAB CONSOLE

Esta opción muestra todos los servidores configurados en la aplicación. Aquí podremos agregar, configurar, modificar y borrar.

- TAB GRAPH

Se observa en la parte izquierda los directorios creados. Seleccionar previamente uno de los subdirectorios para apreciar las gráficas correspondientes.

- TAB NCP

Proporciona una pequeña interface hacia otro sistema de monitoreo denominado Nagios, cabe recalcar que cacti solamente permite la visualización de los equipos configurados en Nagios.

- TAB GPS MAP

Usa el GoogleMaps y nos permite identificar claramente en el mapa de Ecuador cada uno de los equipos y nodos situados a lo largo del país.

- TAB MONITOR

Muestran un esquema de cada host activado en Console como Monitor Host y sus respectivas estadísticas, además incluye una alarma para indicar algún tipo de incidencia. Se puede observar el estado del equipo, la dirección IP, y la disponibilidad, además visualizar las gráficas relacionadas con dicho equipo.

- TAB WEATHERMAP

Permite generar mapas de red donde se pueden añadir gráficos que Cacti tiene por defecto. Con esta opción se puede crear diagramas de red que nos permitan ver la cantidad de tráfico por las interfaces seleccionadas en el gráfico.

B.3.4.4 Adición de Dispositivos

1) El primer paso para la creación de gráficos para la red es la adición de un dispositivo:

   ✓ Presionamos el botón ADD desde la opción DEVICES, del menú console.

Dentro de esta opción ya se encuentran añadidos todos los equipos pertenecientes a la gestión del Área de MPLS, y por consiguiente los equipos del servicio VPLS.

Por tal motivo no es necesario añadir equipos en esta opción.

2) Para realizar las gráficas de las interfaces que nos interesan y que participan en el servicio, realizamos los siguientes pasos:

- ✓ Seleccionamos en el menú New Graphs
- ✓ En el menú desplegable de la parte superior escogemos el equipo donde se va a crear el gráfico.
- ✓ En la opción Graph Type se selecciona el tipo de gráfico, en la cual se sugiere escoger la opción SNMP- Interface Statistics donde aparecerán las interfaces del equipo seleccionado.
- ✓ Mediante un filtro se puede realizar la búsqueda de las interfaces del equipo seleccionado. El equipo mostrará todas sus interfaces.
- ✓ Se selecciona la interfaz a graficar, el tipo de gráfico (IN/OUT Bits) y se presiona créate, como indica la figura B.13.
- ✓ Si se creó correctamente en la parte superior aparecerá un mensaje de éxito.

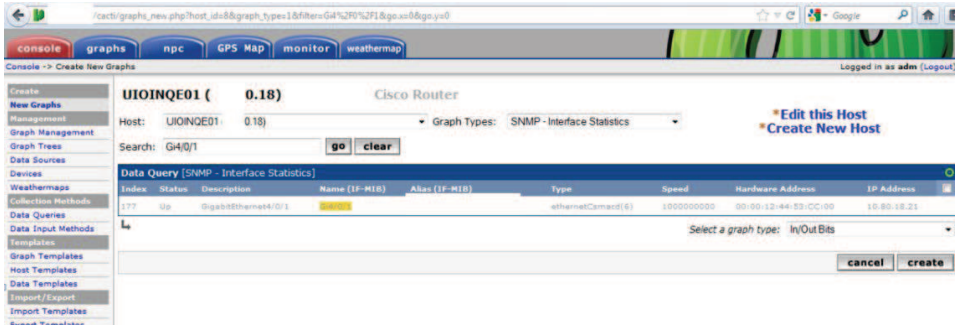


Figura B. 13: Adición de dispositivo

B.3.5 CREACIÓN DE DIAGRAMAS

Lo que nos interesa es un gráfico que muestre un esquema de cómo se encuentra la VPLS de cada ISP cliente, dentro de weathermaps se puede realizar mapas de red, donde se ubica las gráficas antes realizadas de las interfaces de cada equipo. Para crean un nuevo weathermap se siguen los pasos descritos a continuación en la figura B.14:

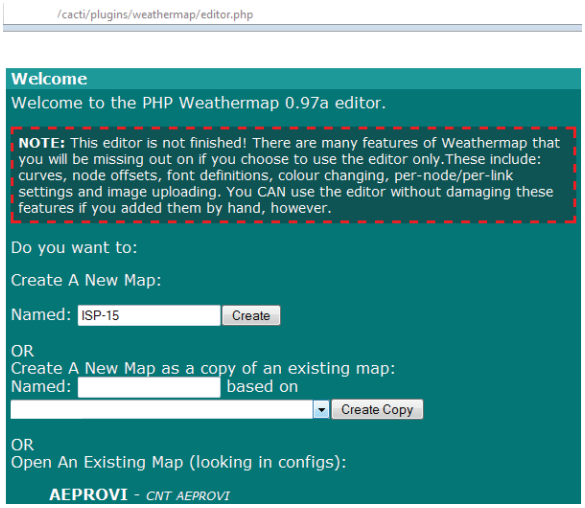


Figura B. 14: Creación de Weathermap

- En la opción de weathermap seleccionar editor
- Colocar el nombre del nuevo mapa que se desea crear

Si se quiere realizar un mapa en base a uno existente seleccionar Create A New Map as copy of an existing map.

En el caso de que se requiera modificar la configuración de un mapa ya existente seleccionar en la opción Open An Existing Map el nombre del mapa.

- En la figura B.15 se presenta las siguientes opciones que permiten administrar y realizar los mapas de las redes:

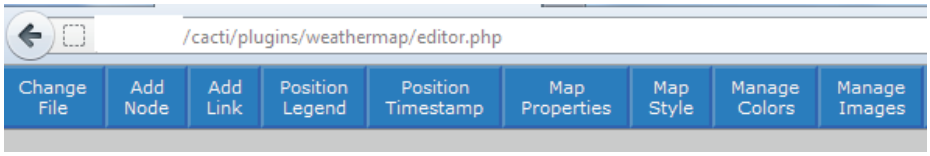


Figura B. 15: Menú para mapas de red

Change File: Regresa al menú Wathermap guardando los cambios realizados en el mapa.

Add node: Permite añadir un nodo y colocar los datos correspondientes además incluye la opción para escoger la imagen deseada en el mapa ya sea un router, switch, nube, etc. Ver figura B.16.

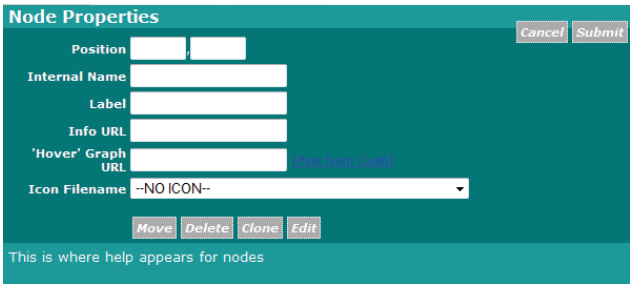


Figura B. 16: Propiedades nodo – CACTI

Add link: Permite añadir un enlace en un nodo y colocar la información necesaria de dicho enlace.

En la opción Pick from Cacti se puede buscar la interfaz graficada previamente relacionada con el equipo, para representar el enlace. Ver figura B.17.

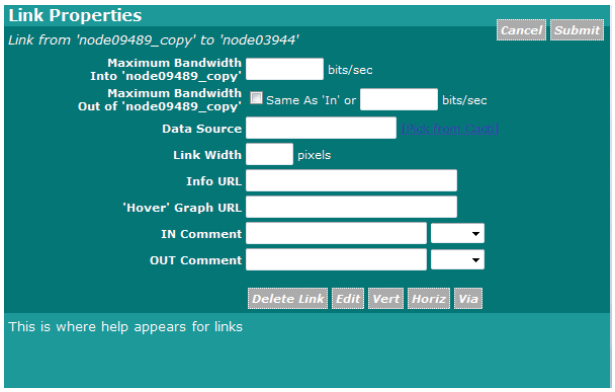


Figura B. 17: Propiedades enlace– CACTI

Las siguientes opciones no son relevantes para realizar el mapa de red y son:

- **Position Legend y Timestamp:** Seleccionando y posicionando muestra la posición del cursor.
- **Map properties:** Indica los datos configurados en el mapa, como el título del mapa y el fondo de pantalla.
- **Map style:** Permite establecer ciertos parámetros para dar un formato de presentación.
- **Manage Colors:** Esta opción no se encuentra habilitada todavía. Permite administrar los colores de cada uno de elementos insertados en el mapa.
- **Manage images:** Esta opción no se encuentra habilitada todavía. Permite administrar las imágenes insertadas en el mapa.

Después de haber utilizado las opciones correctamente el mapa se lo puede observar como muestra el ejemplo de la figura B.18.

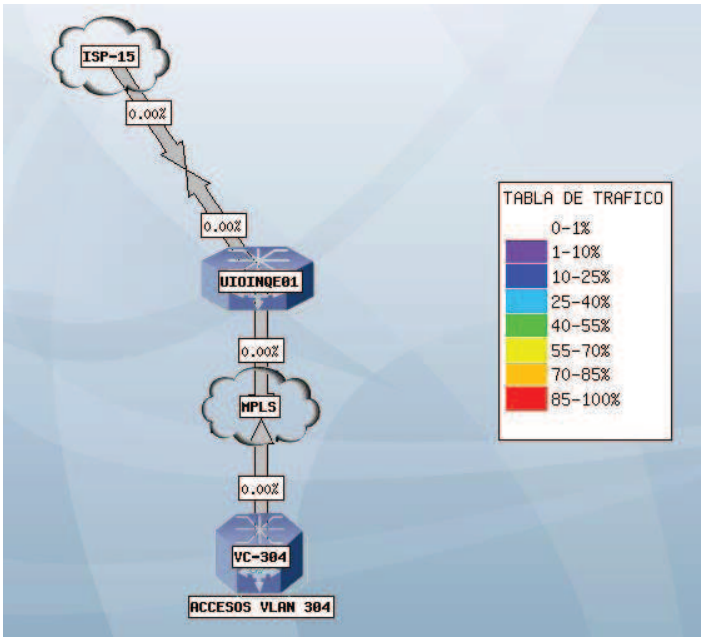


Figura B. 18: Diagrama– CACTI

B.3.6 VISUALIZACIÓN DEL MAPA

Después de haber creado el mapa presionamos en Change File, para salir y guardar, y nos lleva directamente al grupo de Wathermap, donde están los mapas realizados y que se pueden visualizar. A continuación se muestra gráficamente en pasos este procedimiento.

1) Para poder visualizar el mapa creado se debe presionar Add, para añadirlo a la lista.

Figura B. 19: Añadir el mapa a la lista de visualización

2) Se muestra los mapas que se pueden agregar, y se vuelve a presionar Add.

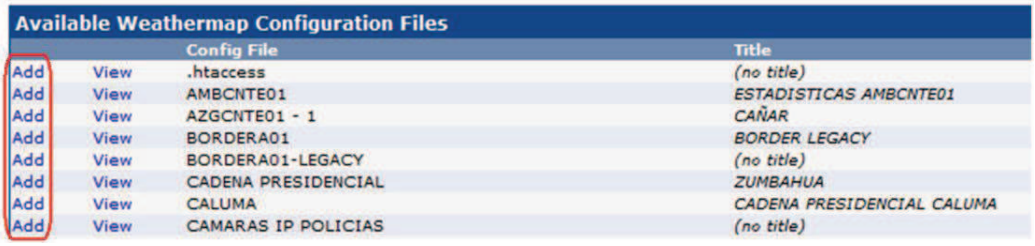


Figura B. 20: Lista de visualización

3) Una vez añadido, presenta las opciones para agregarlo a un grupo y para dar permisos para que sea visualizado solo para ciertos usuarios.

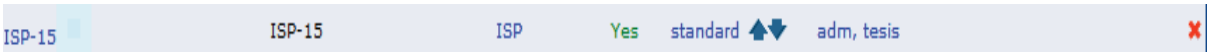


Figura B. 21: Agregar permisos de visualización

4) Para añadir a un grupo se debe seleccionar de la lista desplegable de Choose an existing Groups.

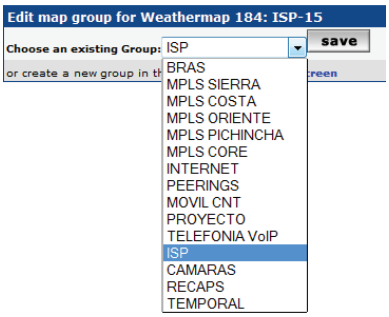


Figura B. 22: Añadir el mapa a un grupo

5) Para dar permisos de visualización se hace de la siguiente forma, se escoge el usuario de la lista desplegable *Allow*.

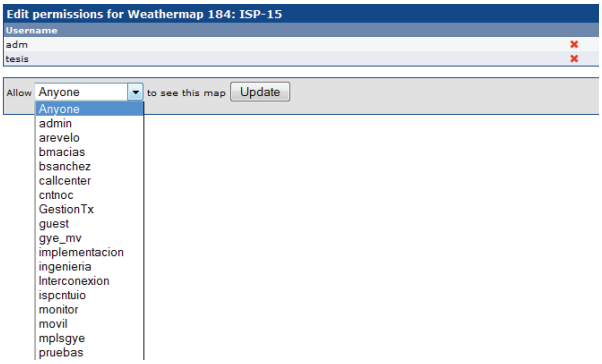


Figura B. 23: Opciones de permisos de visualización

6) Finalmente para poder visualizar el estado de los enlaces del mapa creado se presiona en la pestaña Watermap de la parte superior y se escoge el grupo

donde se encuentra el mapa, este caso grupo ISP, y se observa el diagrama de la VPLS.

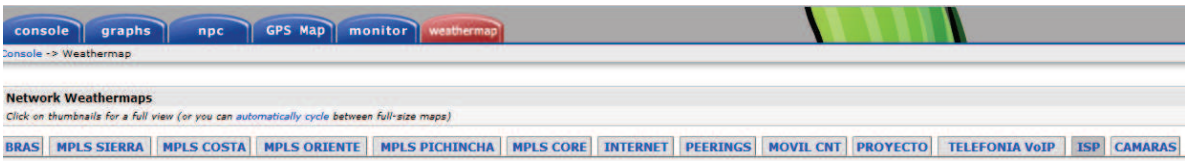


Figura B. 24: Visualización del mapa

ANEXO C

CONFIGURACIÓN DEL SERVICIO VPLS Y HVPLS

C. 1 CONFIGURACIÓN DE VPLS

- **Configuración equipo PE**

La interfaz conectada al equipo cliente está definida como modo trunck para recibir y enviar paquetes Ethernet con etiquetas VLAN.

Paso 1. Configurar la interfaz conectada al dispositivo CE.

	Comando	*Propósito*
Paso 1	`Router(config)#interface[tipo] [módulo/interfaz.subinterfaz]` `Router(config-if)# switchport`	Configurar la interfaz hacia el cliente como un switchport.
Paso 2	`Router(config-if)# switchport trunk encapsulation dot1q`	Configurar la interfaz para usar encapsulamiento dot1q.
Paso 3	`Router(config-if)# switchport trunk allowed vlan [vlan-id]`	Asignar una o lista de vlan permitidas.
Paso 4	`Router(config-if)# switchport access vlan [vlan-id]`	Asignar a la interfaz la VLAN asociada al cliente.

Tabla C. 1: Configuración hacia el equipo CE, vasado en 802.1Q

Paso 2. Definir la VFI y los neighbors asociados a la VPLS

	Comando	*Propósito*
Paso 1	`Router(config)# I2 vfi [vfi-name] manual`	Configuración de la instancia VPLS.
Paso 2	`Router(config-vfi)# vpn [vpn-id]`	Especificación del identificador VPN-ID para la VFI.
Paso 3	`Router(config-vfi)#neighbor [remote-PE-loopback] encapsulation mpls`	Especificación de los Router vecinos o de acceso a la VPLS

Tabla C. 2: Configuración de la VFI y Pseudowires

Paso 3: Asociar la VFI con la VLAN

	Comando	*Propósito*
Paso 1	`Router(config)#interface vlan [vlan-id]`	Se ingresa la configuración de la VLAN
Paso 2	`Router(config)#xconnect vfi [vfi-name]`	Se asocia la interfaz VLAN con la VFI.

Tabla C. 3: Asociación de la VFI a la VLAN

- Nota: Se debe tener una VFI configurada para que el comando sea aceptado.

C. 2 CONFIGURACION HVPLS

Para HVPLS se especifica las configuraciones en los equipos que dividen los 2 niveles, para el Acceso QinQ y para el acceso MPLS (EoMPLS).

C.2.1 ACCESO QinQ

- **Configuración equipo N-PE**

Paso 1: Creación de la VLAN

	Comando	*Propósito*
Paso 1	**`Router # configure terminal`**	Ingresar al modo de configuración global.
Paso 2	`Router(config)# vlan vlan-id`	Crear la VLAN a la que se asociara la interfaz conectada al CE.

Tabla C. 4: Creación de la VLAN – QinQ

Paso 2: Configurar la interfaz conectada al dispositivo U-PE, ver tabla 8.2

	Comando	Propósito
Paso 1	`Router(config)#interface[tipo] [módulo/interfaz.subinterfaz]` `Router(config-if)# switchport`	Ingresar a la interfaz hacia el U-PE y configurarla como switchport.
Paso 2	`Router(config-if)# switchport mode trunk`	Configurar el switch port como modo trunk.
Paso 3	`Router(config-if)# switchport trunk encapsulation dot1q`	Configurar la interfaz para usar encapsulamiento dot1q.
Paso 4	`Router(config-if)# switchport trunk allowed vlan vlan-id`	Asignar una o lista de vlan permitidas.

Tabla C. 5: Configuración de interfaz conectada al dispositivo U-PE – QinQ

Paso 3: Asociacion del circuito de conexión con la VFI

	Comando	Propósito
Paso 1	`Router(config)#interface vlan vlan-id`	Ingresamos a la configuración de la vlan
Paso 2	`Router(config)#xconnect vfi vfi-name`	Conectamos la VFI a la interfaz VLAN.

Tabla C. 6: Asociación de la VFI a la VLAN

- **Configuración equipo U-PE**

Paso 1: Configurar la interfaz conectada al dispositivo CE

	Comando	Propósito
Paso 1	`Router(config)#interface[tipo] [módulo/interfaz.subinterfaz]` `Router(config-if)# switchport`	Ingresar a la interfaz hacia dispositivo CE y configurarla como switchport.
Paso 2	`Router(config-if)# switchport mode access`	Configurar el switch port como modo acceso.
Paso 3	`Router(config-if)# switchport access vlan vlan-id`	Asignar el interfaz a un dominio que está representado por la VLAN.

	Comando	Propósito
Paso 4	`Router(config-if)# switchport mode dot1q-tunnel`	Configurar la interfaz para usar encapsulamiento dot1q.
Paso 5	`Router(config-if)# switchport trunk allowed vlan vlan-id`	Asignar una o lista de vlan permitidas.

Tabla C. 7: Configuración de interfaz conectada al dispositivo CE – QinQ

Paso 2: Configurar la interfaz conectada al dispositivo N-PE

	Comando	Propósito
Paso 1	`Router(config)#interface[tipo] [módulo/interfaz.subinterfaz]` `Router(config-if)# switchport`	Ingresar a la interfaz hacia dispositivo N-PE y configurarla como switchport.
Paso 2	`Router(config-if)# switchport mode trunk`	Configurar el switch port como modo trunk.
Paso 3	`Router(config-if)# switchport allowed vlan vlan-id`	Asignar una o lista de vlan permitidas.

Tabla C. 8: Configuración de interfaz conectada al dispositivo N-PE – QinQ

C.2.2 ACESSO EoMPLS

- **Configuración equipo N-PE**

Paso 1: Configurar la interfaz conectada al dispositivo U-PE

	Comando	Propósito
Paso 1	`Router(config)#interface[tipo]` `Router(config-if)# no switchport`	Ingresar a la interfaz hacia dispositivo U-PE y configurarla como no switchport.
Paso 2	`Router(config-subif)#ip address ip-address`	Asigna una dirección IP a la interfaz.
Paso 3	`Router(config-if)# mpls ip`	Configurar mpls.

Tabla C. 9: Configuración de interfaz conectada al dispositivo U-PE – EoMPLS

Paso 2: . Definir la VFI y la asociacion de la interfaz conectada al equipo U-PE

	Comando	Propósito
Paso 1	`Router(config)# I2 vfi vfi-name manual`	Crear la vfi multipunto con interconexión a los PE remotos de forma manual.
Paso 2	`Router(config-vfi)# vpn vpn-id`	Configura el ID de la VPN para la VFI.
Paso 3	`Router(config-vfi)#neighbor remote-PE-loopback encapsulation mpls`	Especifica la ID del router remoto y la encapsulación del pseudowire.
Paso 4	`Router(config-vfi)#neighbor remote-PE-loopback encapsulation mpls no split horizon`	Asegura que el tráfico pase a/desde del U-PE

Tabla C. 10: Configuración de la VFI y Pseudowires – EoMPLS

- **Configuración equipo U-PE**

Paso 1: Configurar la interfaz conectada al dispositivo CE

	Comando	Propósito
Paso 1	`Router(config)#interface[tipo] [módulo/interfaz.subinterfaz]` `Router(config-if)# switchport`	Ingresar a la interfaz hacia dispositivo CE y configurarla como switchport.
Paso 2	`Router(config-if)# switchport mode access`	Configurar el switch port como modo acceso.
Paso 3	`Router(config-if)# switchport access vlan vlan-id`	Asignar el interfaz a un dominio que está representado por la VLAN.

Tabla C. 11: Configuración de interfaz conectada al dispositivo CE

- **Paso 2: Asociar la VLAN a la VFI**

	Comando	Propósito
Paso 1	`Router(config)#interface vlan vlan-id`	Ingresar a la configuración de la Vlan.
Paso 2	`Router(config)#xconnect local vpn-ip encapsulation mpls`	Asociar la VLAN a la VFI

Tabla C. 12: Configuración de la interfaz de la VLAN – EoMPLS

Paso 3: Configurar la interfaz conectada al dispositivo N-PE

	Comando	*Propósito*
Paso 1	`Router(config)#interface[tipo]` `Router(config-if)# no switchport`	Ingresar a la interfaz hacia dispositivo U-PE y configurarla como no switchport.
Paso 2	`Router(config-subif)#ip address ip-address`	Asigna una dirección IP a la interfaz.
Paso 3	`Router(config-if)# mpls ip`	Configurar mpls.

Tabla C. 13: Configuración de la interfaz conectada al dispositivo N-PE – EoMPLS

C. 3 CONFIGURACIÓN DE VPLS CON SEGMENTACIÓN DEL VLANS

Los pasos 1 y 2 son iguales a la configuración de la VPLS, se debe cambiar únicamente el paso 3 de la siguiente manera:

Paso 3: Asociar la VFI con la VLAN

	Comando	*Propósito*
Paso 1	`Router(config)#interface vlan vlan-id`	Ingresamos a la configuración de la vlan creada para la segmentación
Paso 2	`Router(config)#xconnect vfi vfi-name`	Conectamos la VFI a la interfaz VLAN, la VLAN estará asociada a la VFI de la VLAN de acceso.

Tabla C. 14: Asociación de la VFI a la VLAN de acceso

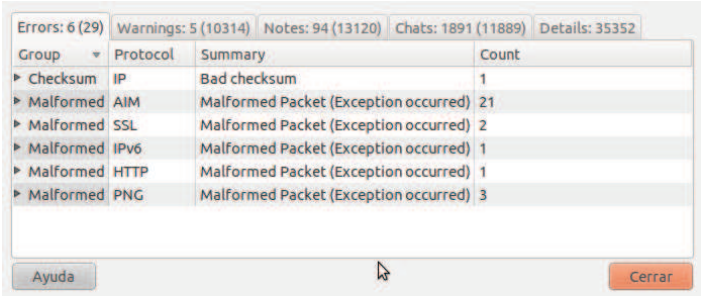
ANEXO D

RESULTADOS GENERALES DEL DIAGNÓSTICO DE LAS VPLSS- FASE INICIAL

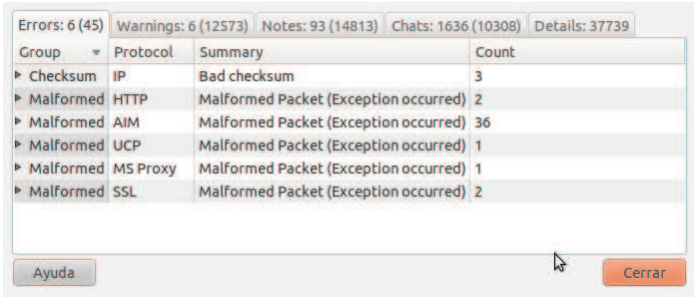
D. 1 RESULTADOS OBTENIDOS CON WIRESHARK MEDIANTE EXPERT COMPOSITE E IO GRAPHS

D.1.1 RESULTADOS DE WIRESHARK PARA EL ISP-2

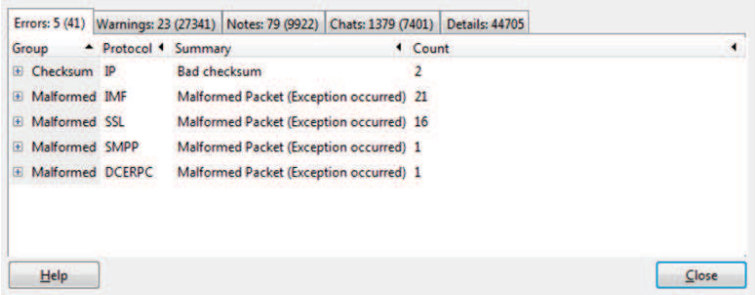
#Paquetes capturados: 42136



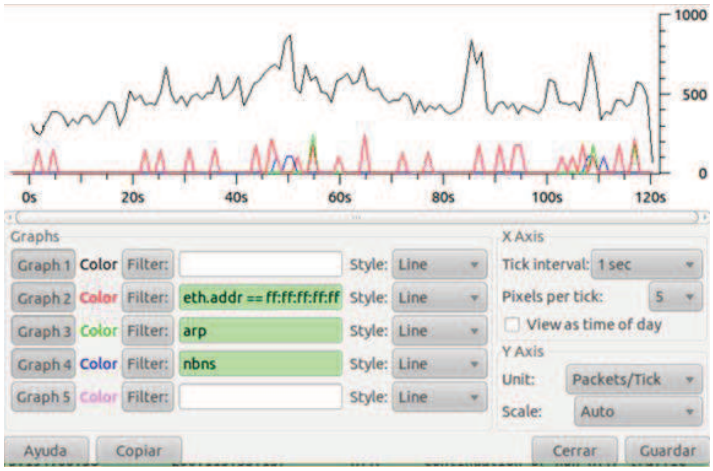
#Paquetes capturados: 52402

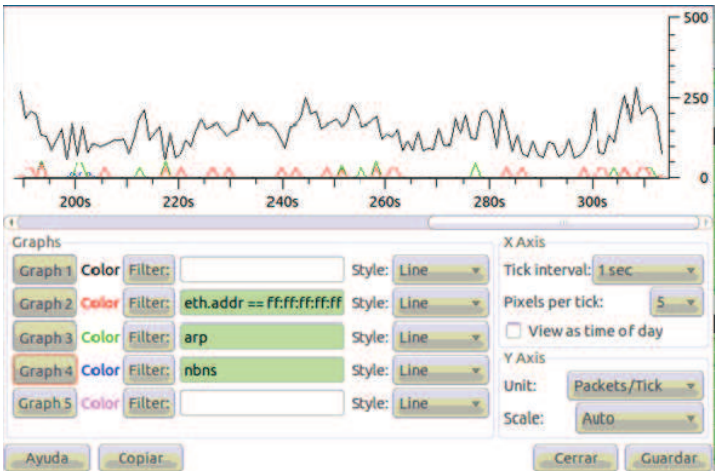


Paquetes capturados: 61903



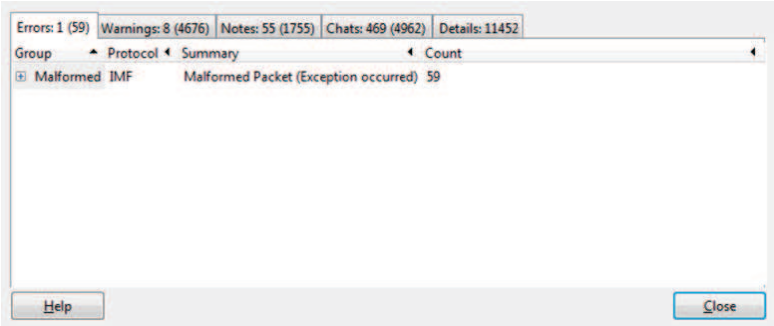

500
250
0
80s
100s
120s
140s
160s
180s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar


1000
500
0
0s
20s
40s
60s
80s
100s
120s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

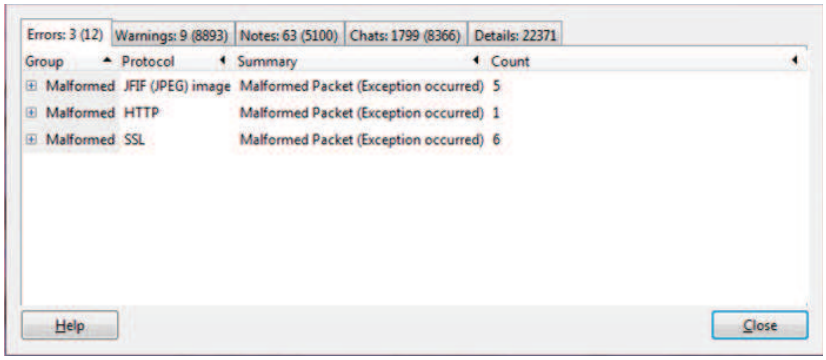

500
250
0
200s
220s
240s
260s
280s
300s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

D.1.2 RESULTADOS DE WIRESHARK PARA EL ISP-3

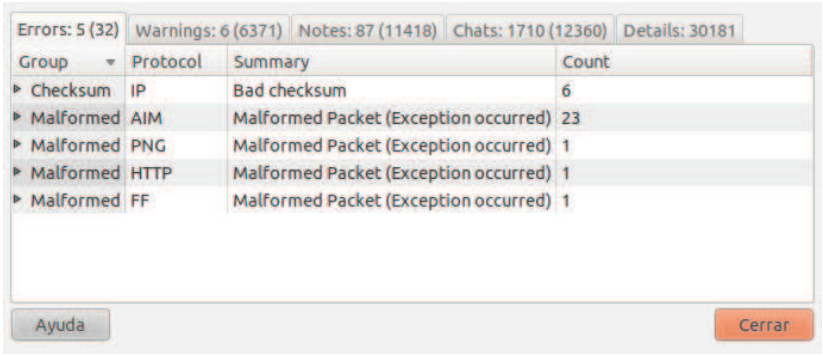
Paquetes capturados: 47912



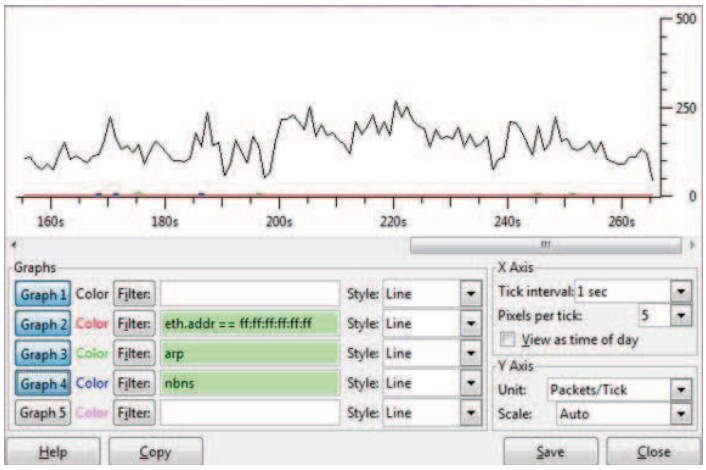
Paquetes capturados: 57321

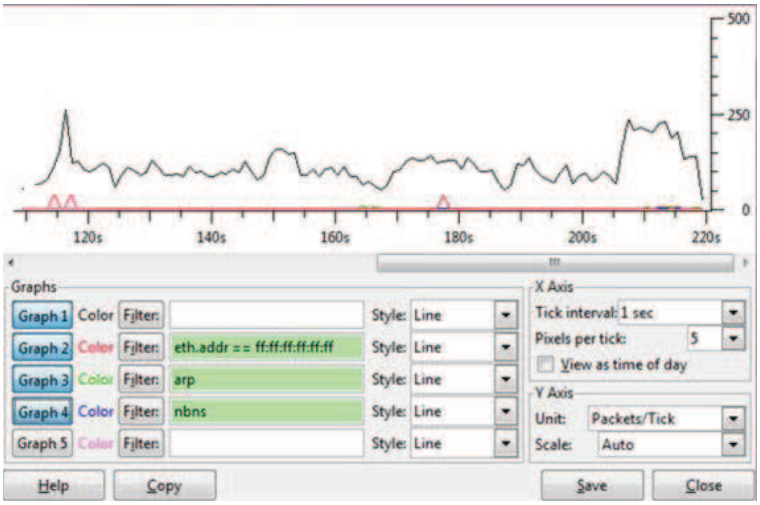


Paquetes capturados: 58110



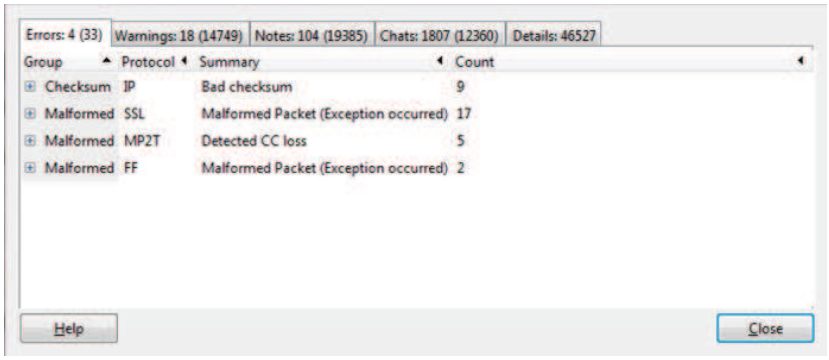

500
250
0
120s
140s
160s
180s
200s
220s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close


500
250
0
160s
180s
200s
220s
240s
260s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

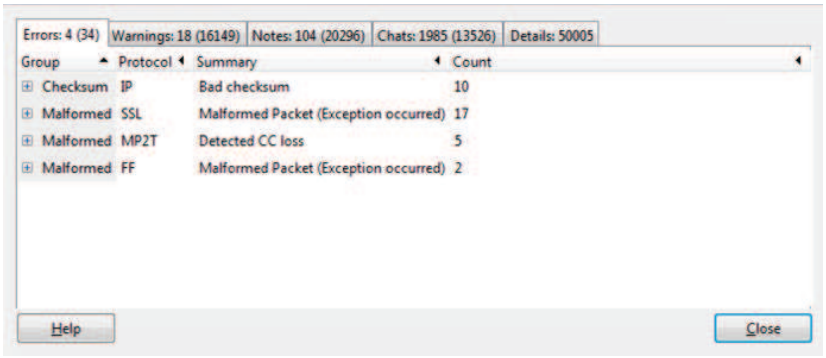

500
250
0
120s
140s
160s
180s
200s
220s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

D.1.3 RESULTADOS DE WIRESHARK PARA EL ISP-6

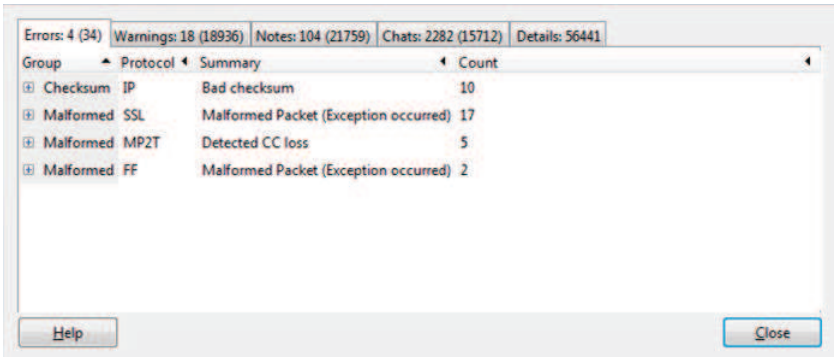
Paquetes capturados: 62132



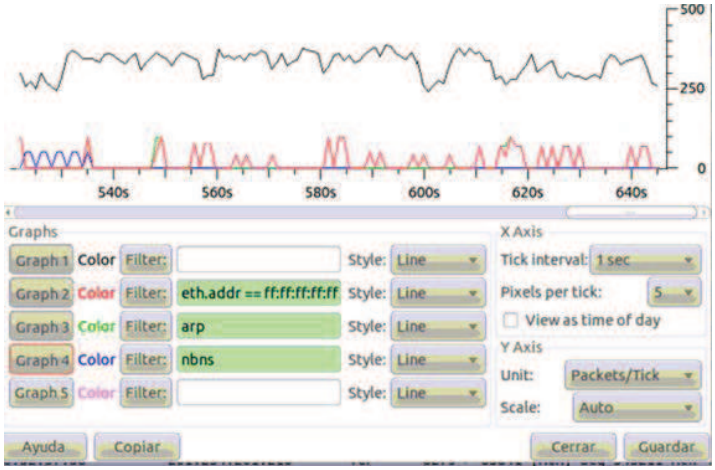
Paquetes capturados: 71410

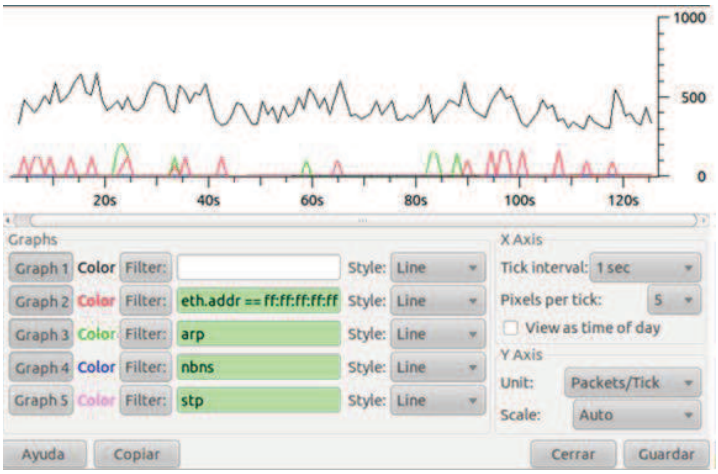


Paquetes capturados: 68345



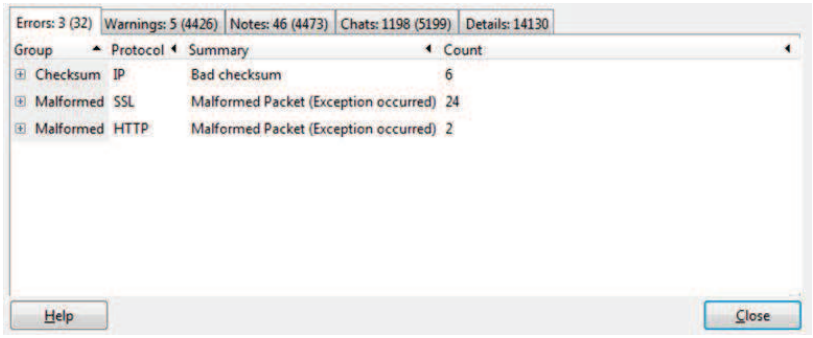

500
250
0
80s
100s
120s
140s
160s
180s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar


500
250
0
540s
560s
580s
600s
620s
640s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

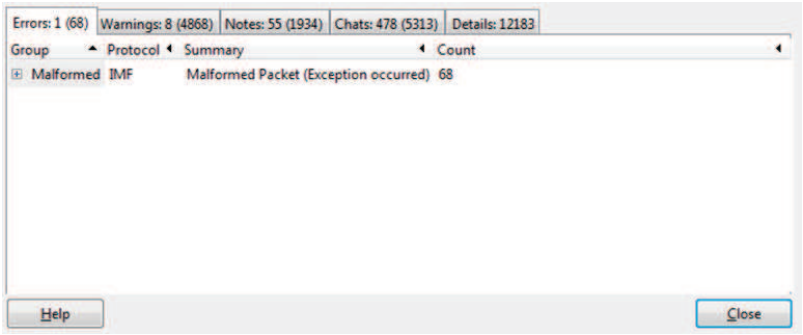

1000
500
0
20s
40s
60s
80s
100s
120s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: stp Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

D.1.4 RESULTADOS DE WIRESHARK PARA EL ISP-7

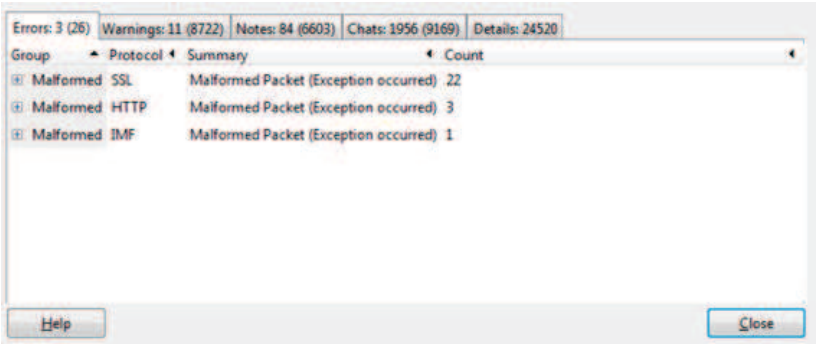
Paquetes capturados: 46588

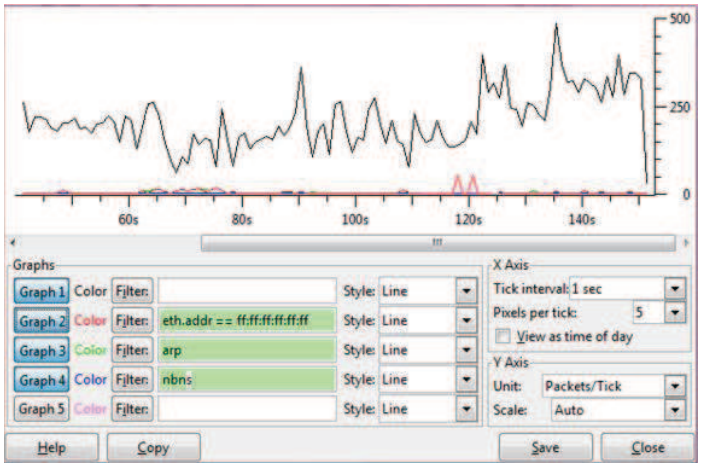


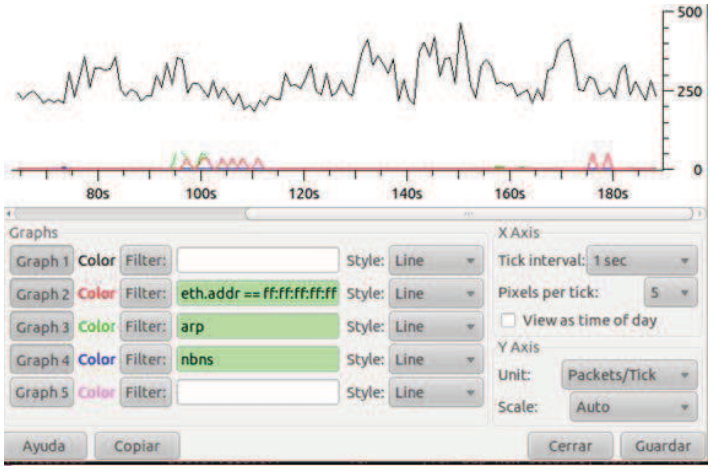
Paquetes capturados: 42115

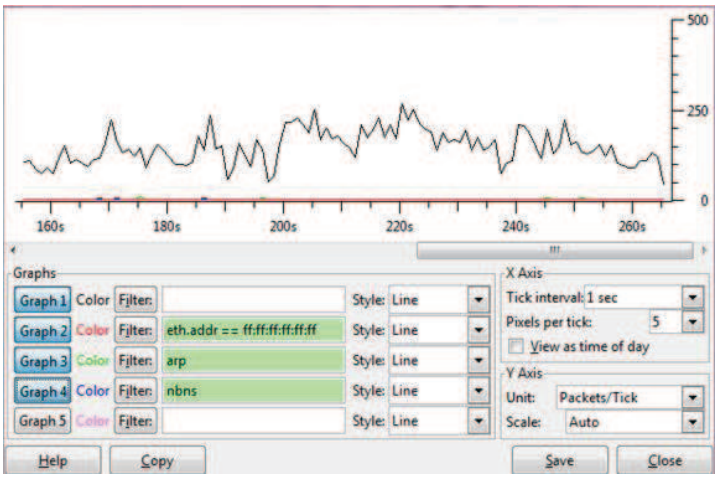


Paquetes capturados: 56487



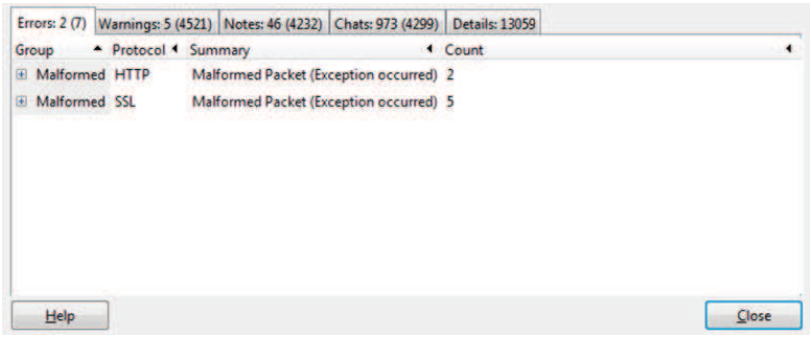

500
250
0
60s
80s
100s
120s
140s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close


500
250
0
80s
100s
120s
140s
160s
180s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

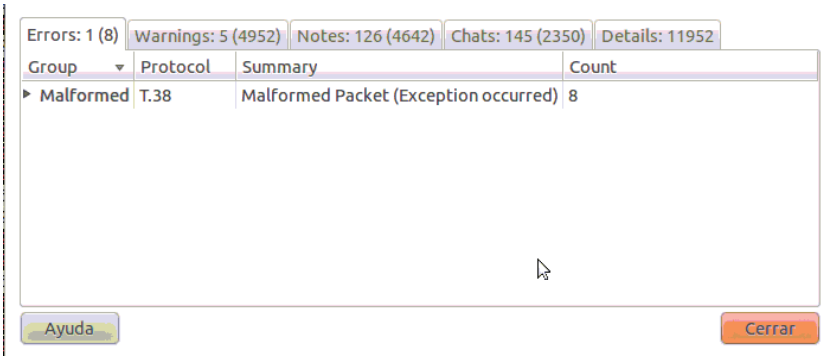

500
250
0
160s
180s
200s
220s
240s
260s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

D.1.5 RESULTADOS DE WIRESHARK PARA EL ISP-8

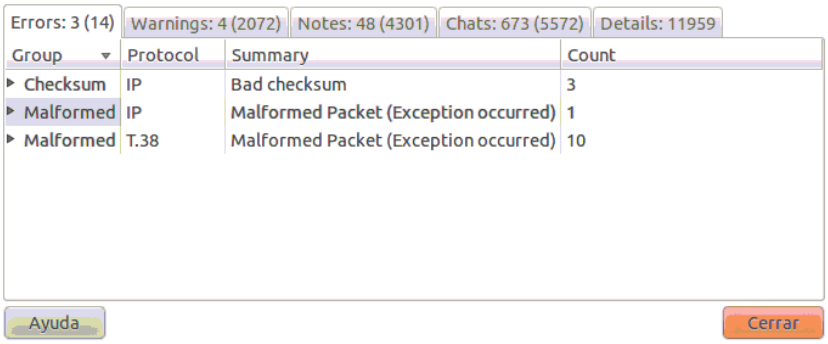
Paquetes capturados: 43098

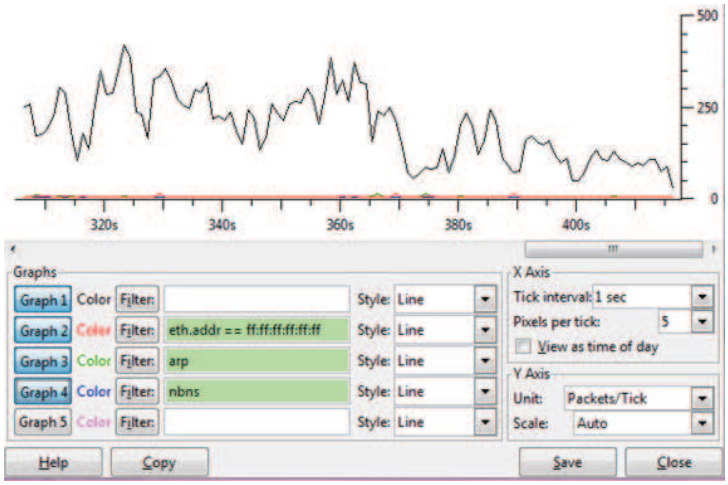


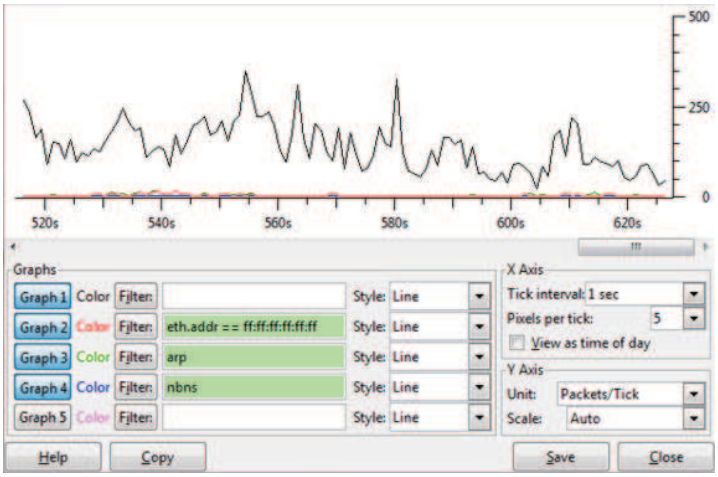
Paquetes capturados: 40229

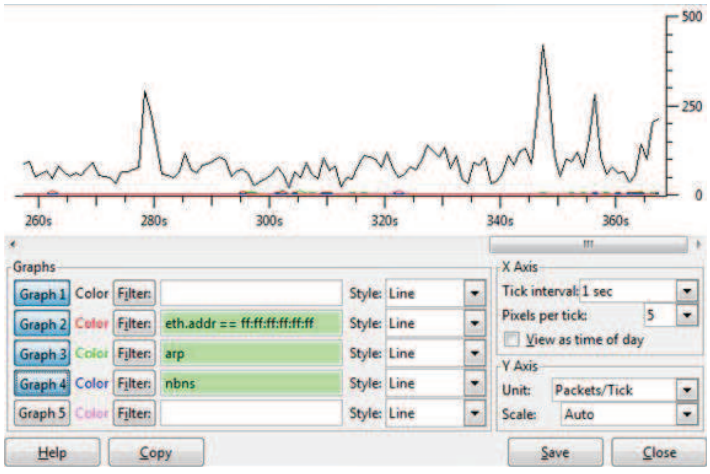


Paquetes capturados: 38714



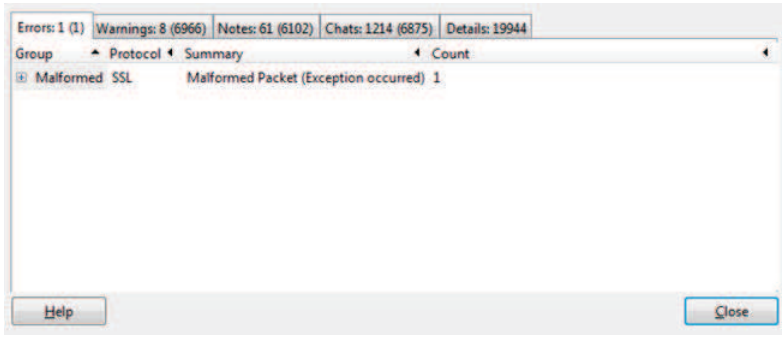

500
250
0
320s
340s
360s
380s
400s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close


500
250
0
520s
540s
560s
580s
600s
620s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

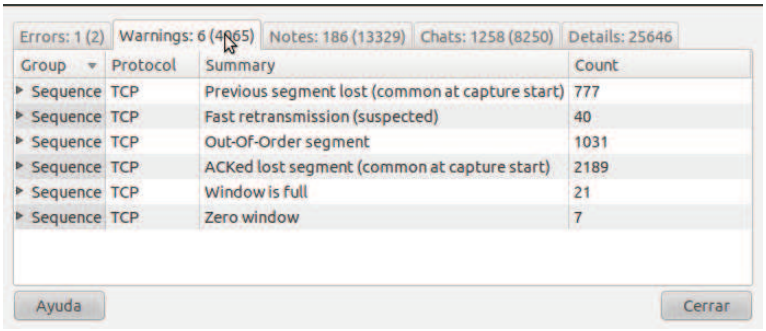

500
250
0
260s
280s
300s
320s
340s
360s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

D.1.6 RESULTADOS DE WIRESHARK PARA EL ISP-10

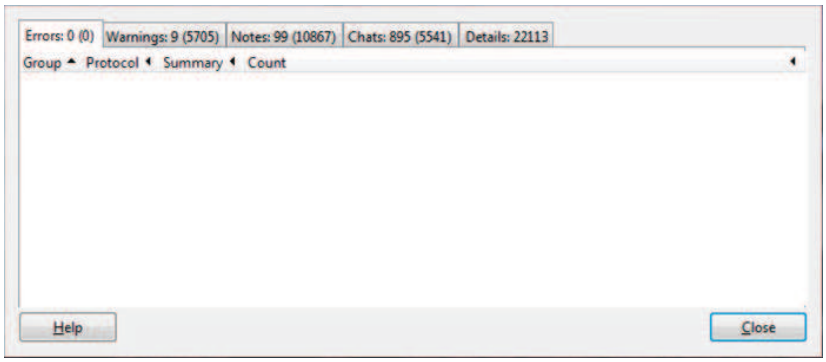
Paquetes capturados: 50410

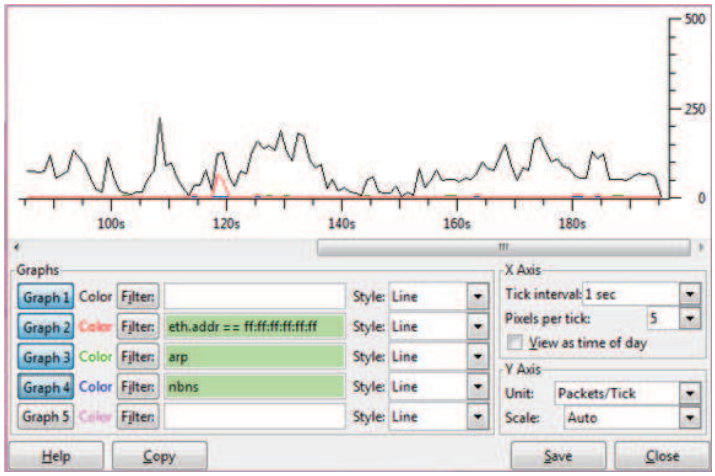


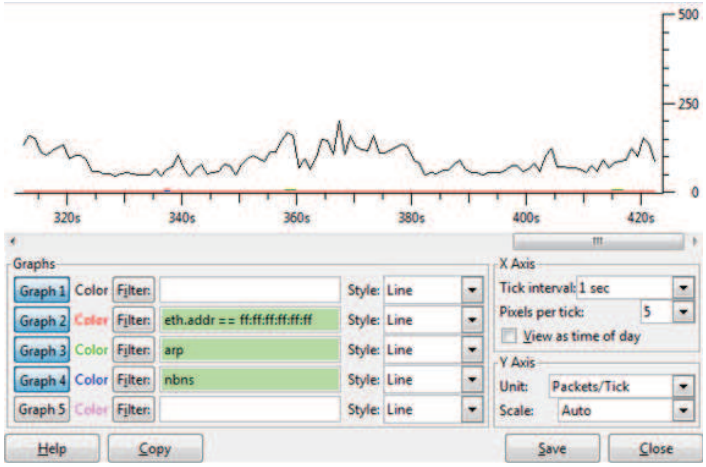
Paquetes capturados: 45120

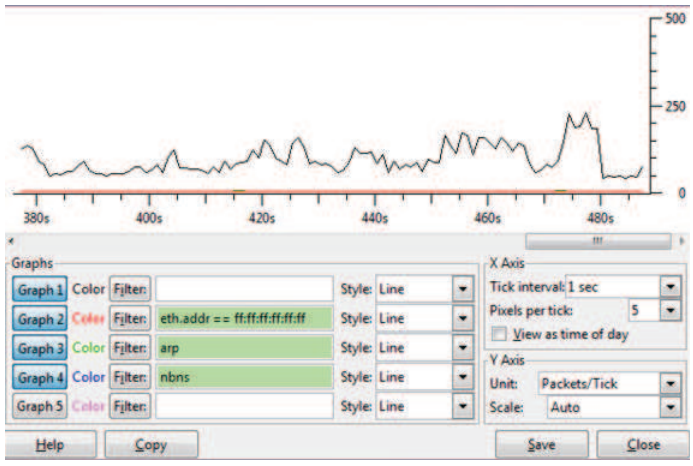


Paquetes capturados: 44665



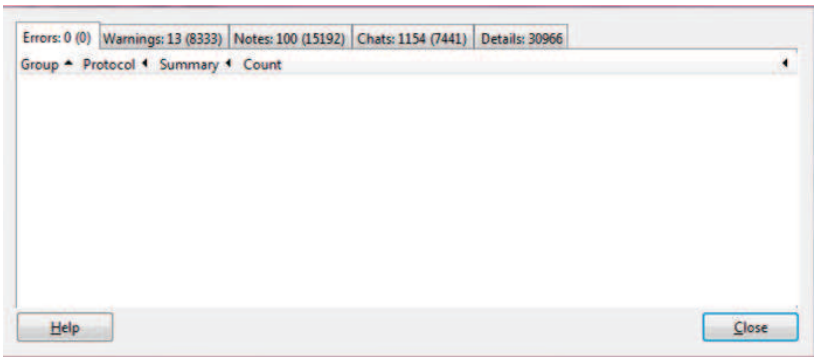

500
250
0
100s
120s
140s
160s
180s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close


500
250
0
320s
340s
360s
380s
400s
420s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

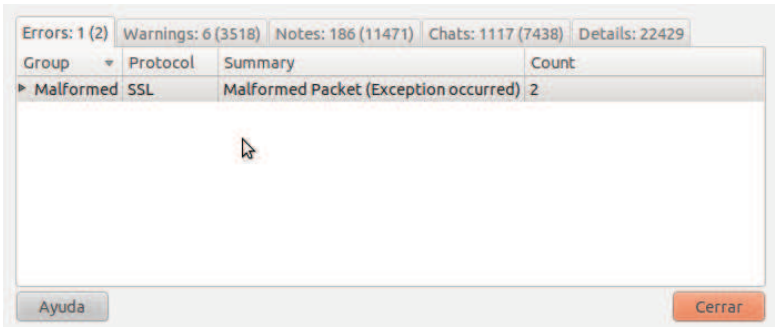

500
250
0
380s
400s
420s
440s
460s
480s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

D.1.7 RESULTADOS DE WIRESHARK PARA EL ISP-11

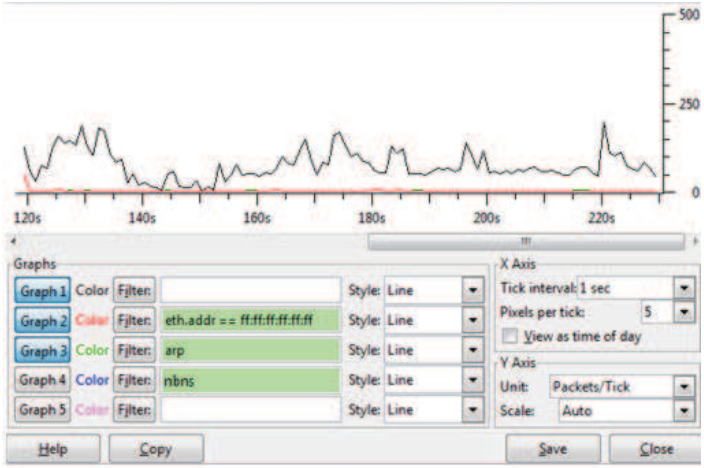
Paquetes capturados: 54233

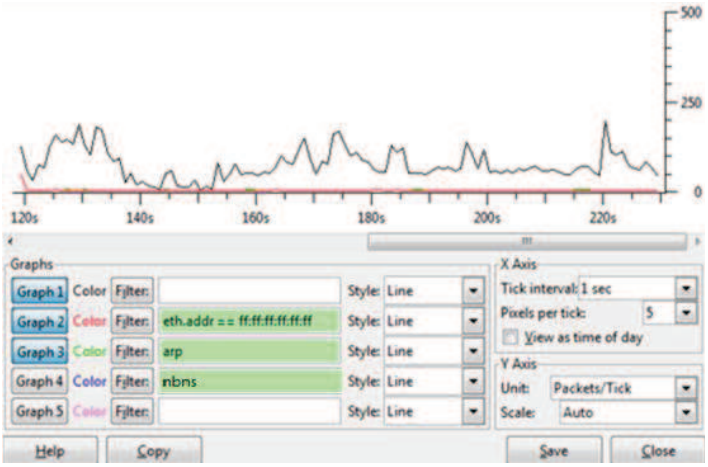


Paquetes capturados: 41257



Paquetes capturados: 56044

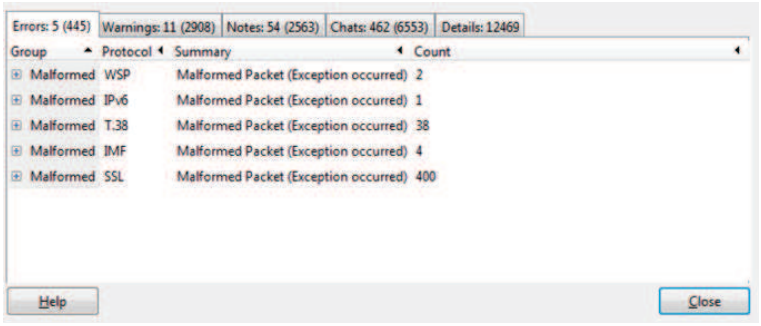

500
250
0
120s
140s
160s
180s
200s
220s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close


500
250
0
120s
140s
160s
180s
200s
220s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

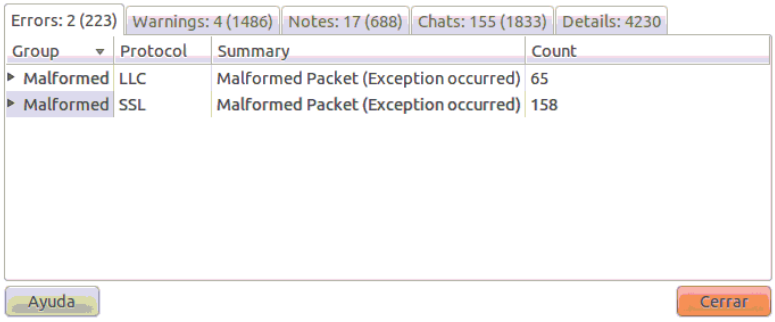

500
250
0
120s
140s
160s
180s
200s
220s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

D.1.8 RESULTADOS DE WIRESHARK PARA EL ISP-12

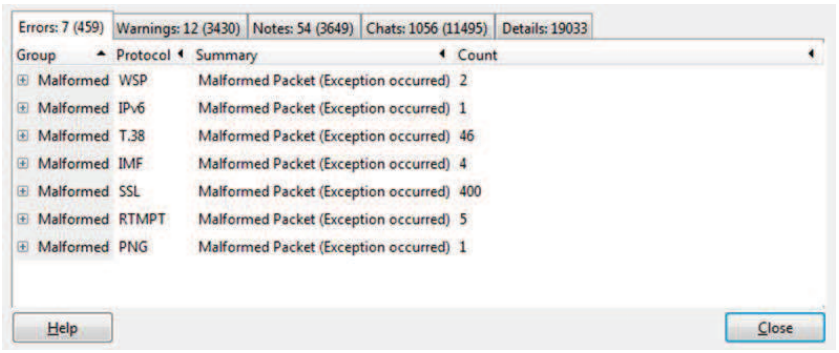
Paquetes capturados: 44415

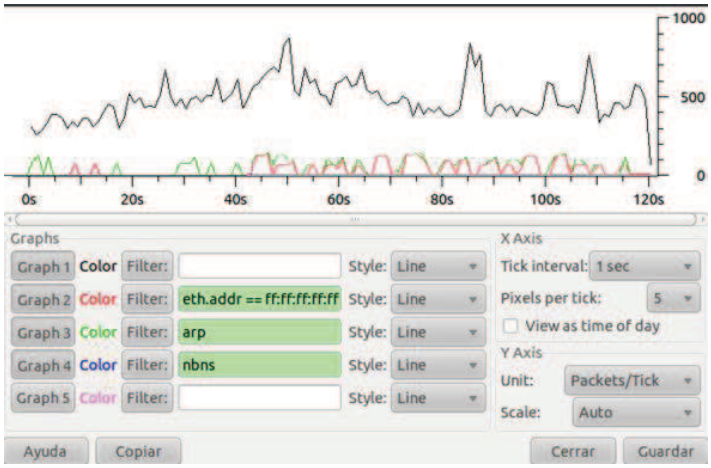


Paquetes capturados: 30211

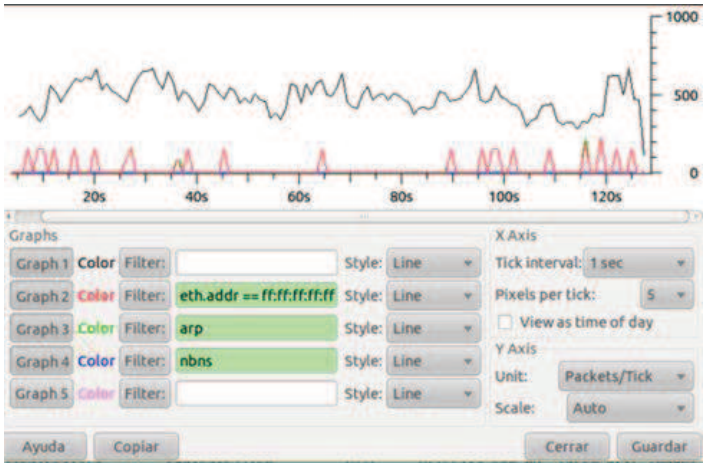


Paquetes capturados: 42596



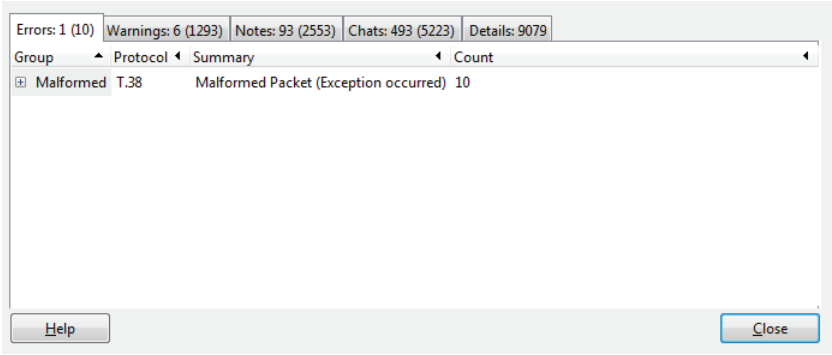

1000
500
0
0s
20s
40s
60s
80s
100s
120s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar


1000
500
0
100s
120s
140s
160s
180s
200s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

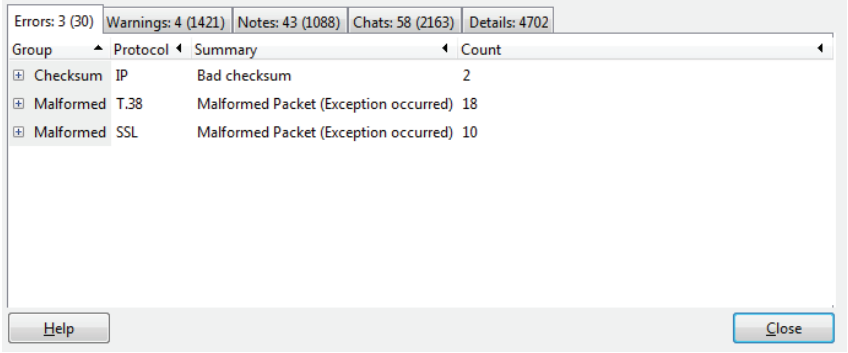

1000
500
0
20s
40s
60s
80s
100s
120s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

D.1.9 RESULTADOS DE WIRESHARK PARA EL ISP-13

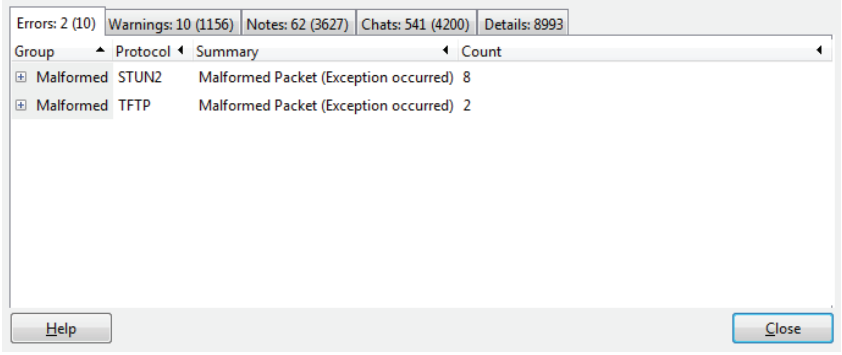
Paquetes capturados: 40511

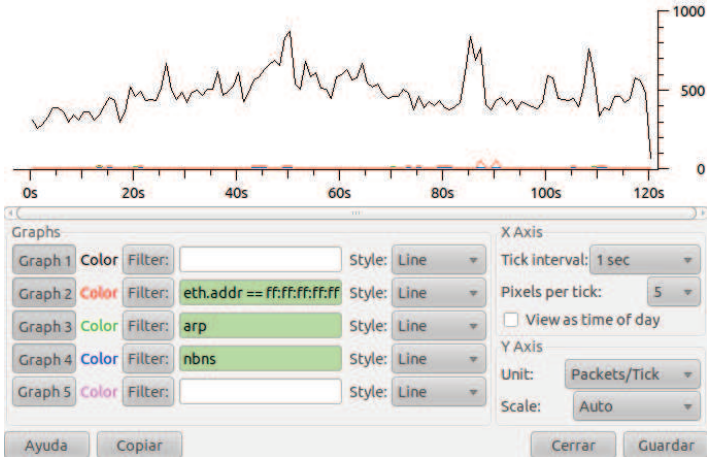


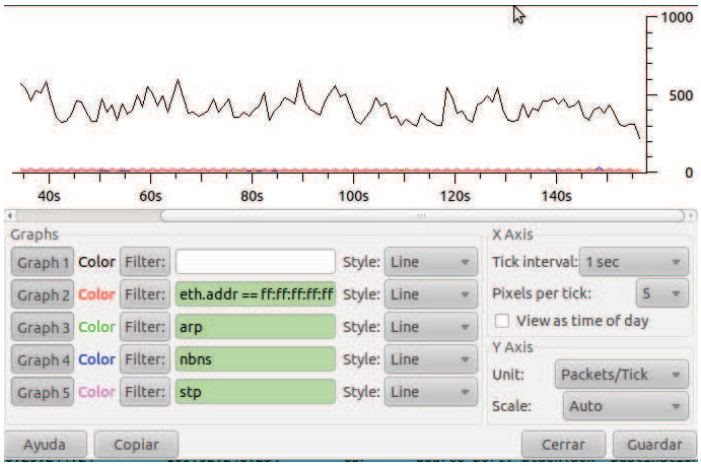
Paquetes capturados: 38103

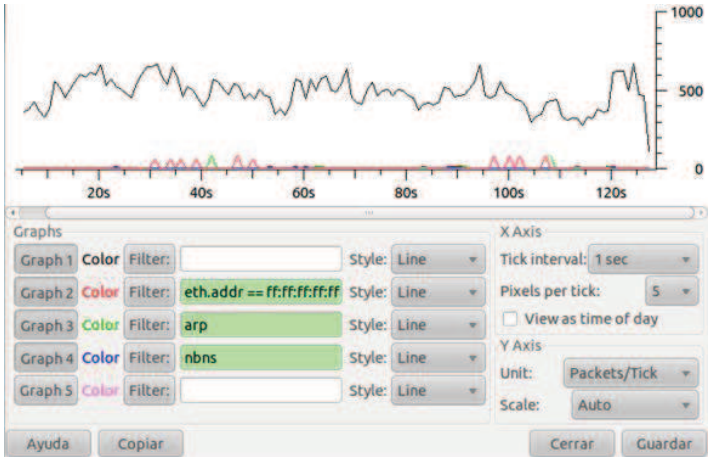


Paquetes capturados: 43874



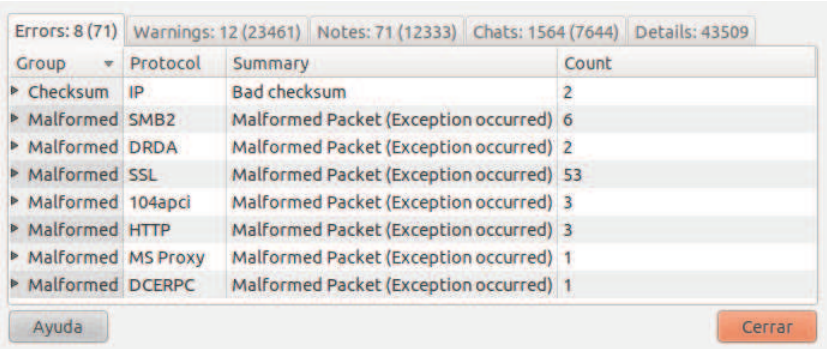

1000
500
0
0s
20s
40s
60s
80s
100s
120s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar


1000
500
0
40s
60s
80s
100s
120s
140s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: stp Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

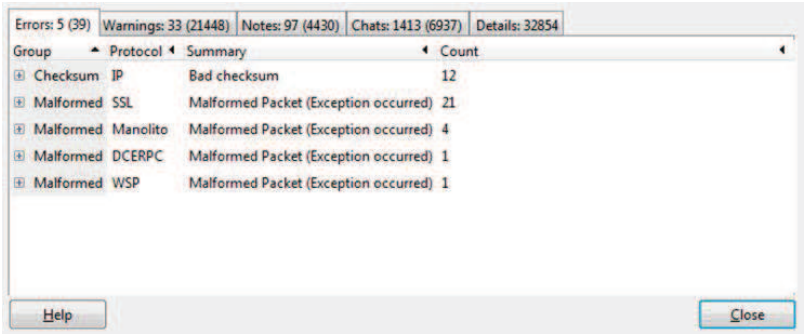

1000
500
0
20s
40s
60s
80s
100s
120s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

D.1.10 RESULTADOS DE WIRESHARK PARA LA IP FIJA

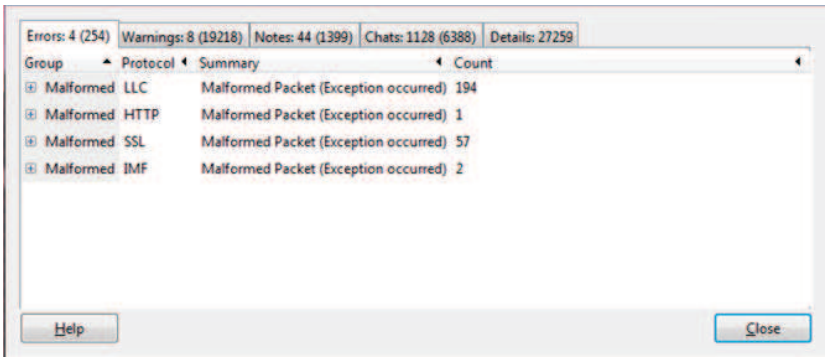
Paquetes capturados: 65301



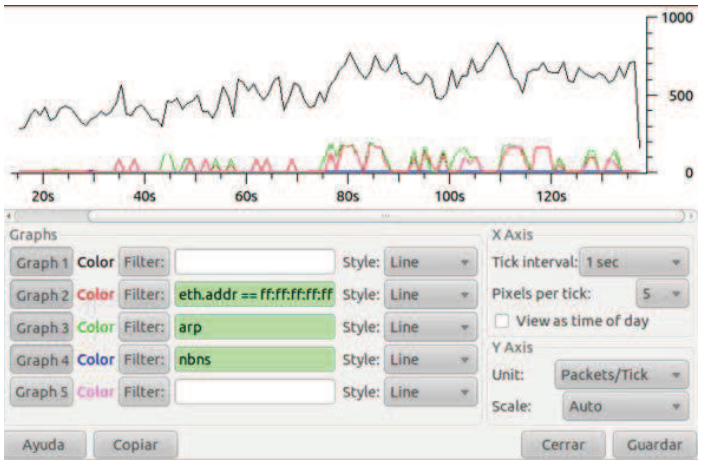
Paquetes capturados: 58124



Paquetes capturados: 59613



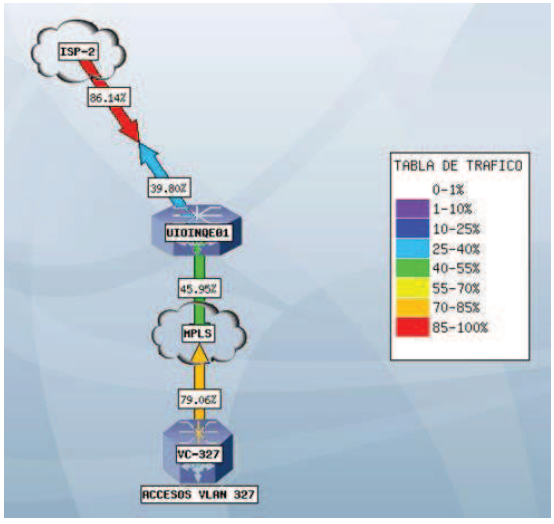

1000
500
0
20s
40s
60s
80s
100s
120s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: stp Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar


1000
500
0
20s
40s
60s
80s
100s
120s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Ayuda
Copiar
Cerrar
Guardar

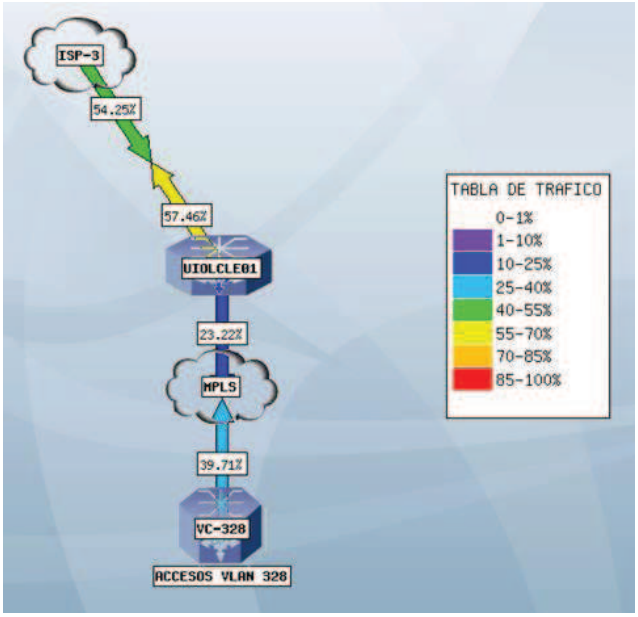

500
250
0
60s
80s
100s
120s
140s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: eth.addr == ff:ff:ff:ff:ff:ff Style: Line
Graph 3 Color Filter: arp Style: Line
Graph 4 Color Filter: nbns Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Help
Copy
Save
Close

D.2 RESULTADOS OBTENIDOS CON CACTI

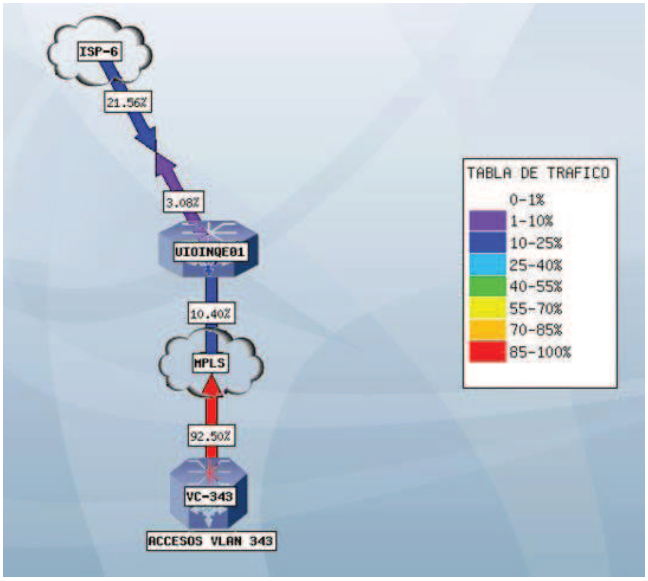
D.2.1 RESULTADO DE CACTI PARA EL ISP-2



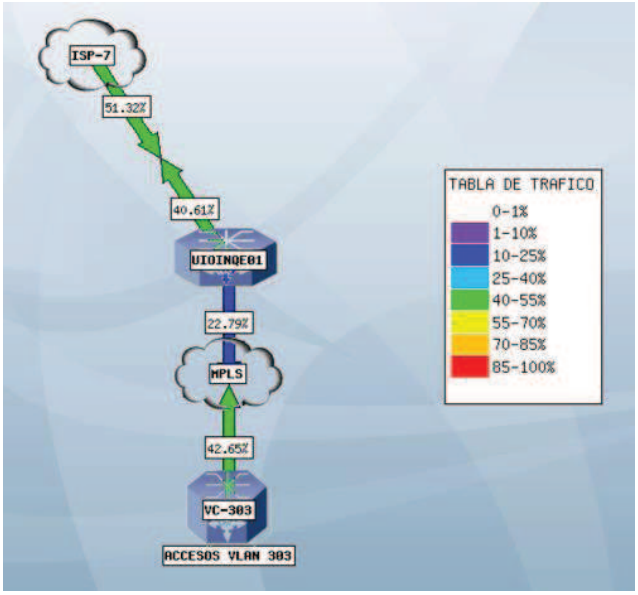
D.2.2 RESULTADO DE CACTI PARA EL ISP-3



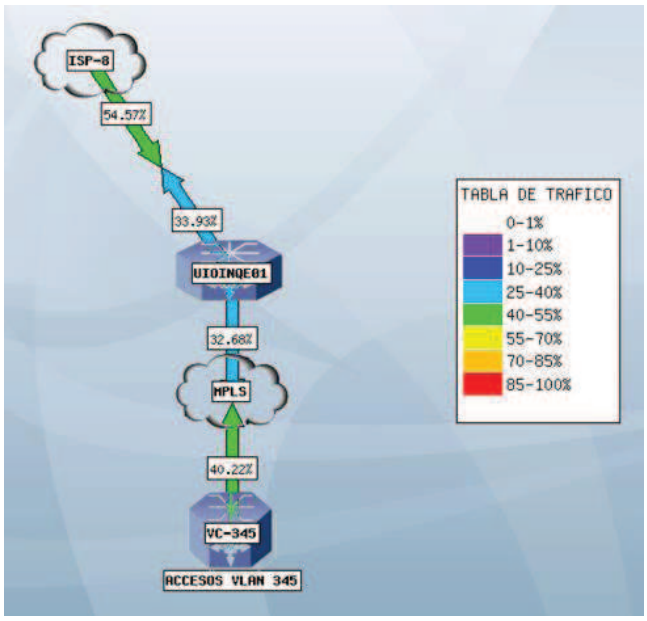
D.2.3 RESULTADO DE CACTI PARA EL ISP-6



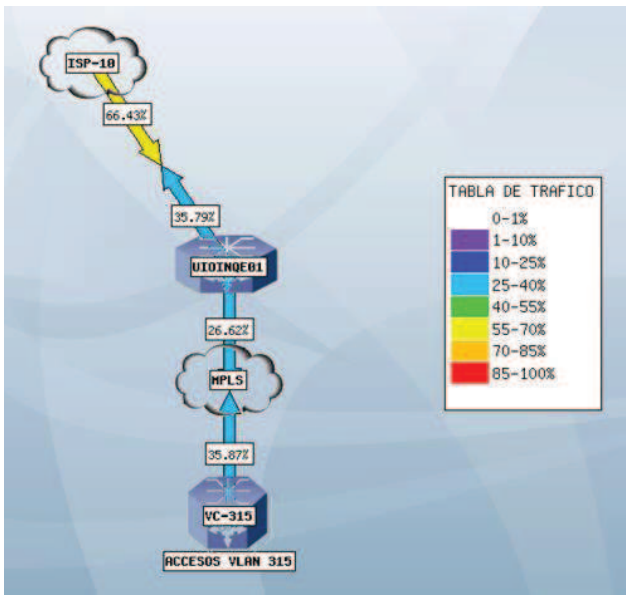
D.2.4 RESULTADO DE CACTI PARA EL ISP-7



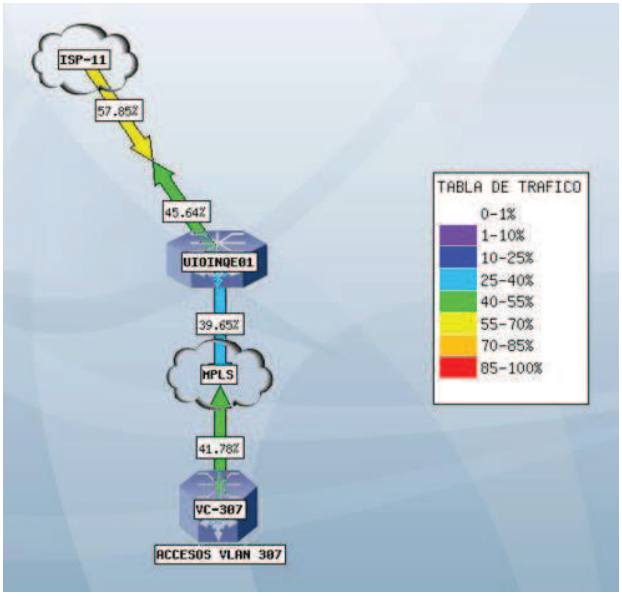
D.2.5 RESULTADO DE CACTI PARA EL ISP-8



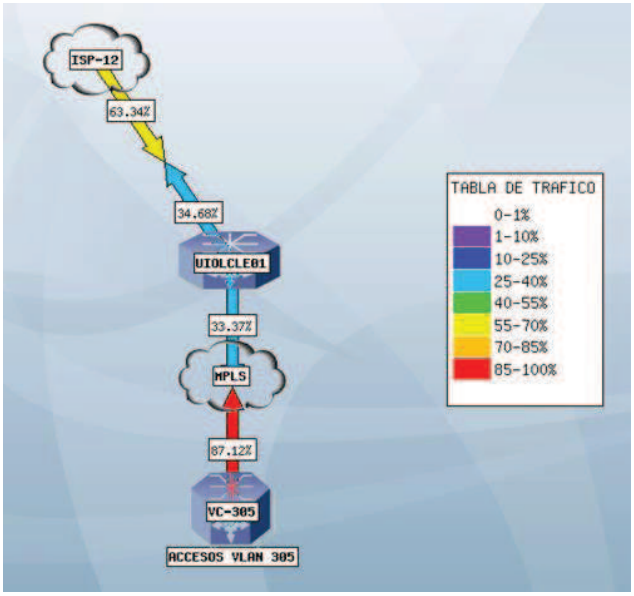
D.2.6 RESULTADO DE CACTI PARA EL ISP-10



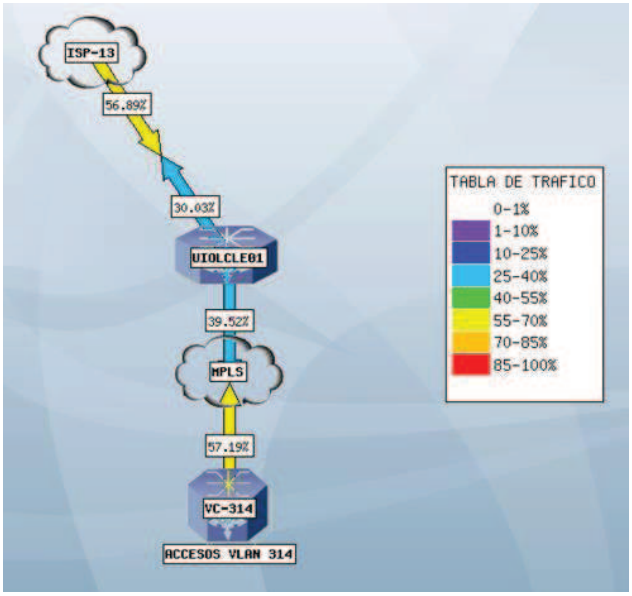
D.2.7 RESULTADO DE CACTI PARA EL ISP-11



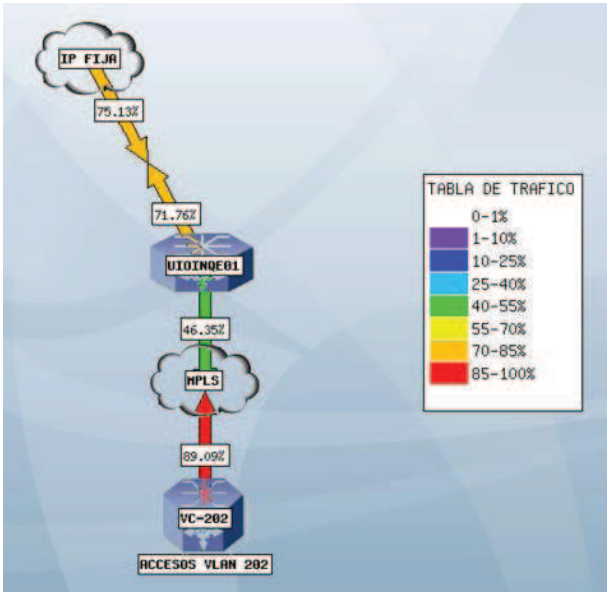
D.2.8 RESULTADO DE CACTI PARA EL ISP-12



D.2.9 RESULTADO DE CACTI PARA EL ISP-13



D.2.10 RESULTADO DE CACTI PARA LA IP FIJA



D.3 RESULTADOS OBTENIDOS CON COMANDOS IOS

D.3.1 RESULTADOS CON COMANDOS IOS PARA EL ISP-1

- **Ejemplo de muestras Mac tomadas con valor 0**

UIOLCLE01#show mac-address-table count vlan 313
MAC Entries for Vlan 313 :
Dynamic Address Count: 0
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 0
Total MAC Addresses Available: 65536

D.3.2 RESULTADOS CON COMANDOS IOS PARA EL ISP-2

- **Asociación de la VFI a la VLAN:**

UIOINQE01#show run interface vlan 327
interface Vlan327
description ### VPLS ISP-2 ###
mtu 1900
no ip address
xconnect vfi isp-2-dsl
end

- **Puertos por donde cruza la VLAN:**

UIOINQE01# show vlan all-port

VLAN	Name	Status	Ports
327	isp-2-dsl	active	Gi12/10, Gi12/24, Gi12/25 Gi12/35, Gi12/40, Gi12/41 Gi12/42, Gi12/43

- **Descripción de Interfaz troncal:**

UIOINQE01# show interface g12/10 description
Interface Status Protocol Description
Gi12/10 up up *** TRONCAL ISP-2***

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface g12/10
interface GigabitEthernet12/10
description *** TRONCAL ISP-2***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 180,181,200-203,258,261,300-330,345,346,348,350
switchport trunk allowed vlan add 353,357,360,363,401,408,413,416,422,425,436
switchport trunk allowed vlan add 444,447,450,451,461,465,466,470,497,503,506
switchport trunk allowed vlan add 514,516,519,523,527,530,542,549,588,699,841
switchport mode trunk
switchport nonegotiate
speed nonegotiate
flowcontrol send off
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 327

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-2-dsl \VFI	172.162.180.100	327	DOWN
VFI	isp-2-dsl \VFI	172.168.0.10	327	UP
VFI	isp-2-dsl \VFI	172.168.0.14	327	UP
VFI	isp-2-dsl \VFI	172.168.0.26	327	UP
VFI	isp-2-dsl \VFI	172.168.0.28	327	UP
VFI	isp-2-dsl \VFI	172.168.0.30	327	UP
VFI	isp-2-dsl \VFI	172.168.0.32	327	UP
VFI	isp-2-dsl \VFI	172.168.0.34	327	UP
VFI	isp-2-dsl \VFI	172.168.0.36	327	UP
VFI	isp-2-dsl \VFI	172.168.0.38	327	UP

VFI	isp-2-dsl \VFI	172.168.0.40	327	UP
VFI	isp-2-dsl \VFI	172.168.0.42	327	UP
VFI	isp-2-dsl \VFI	172.168.0.44	327	UP
VFI	isp-2-dsl \VFI	172.168.0.46	327	UP
VFI	isp-2-dsl \VFI	172.168.0.48	327	UP
VFI	isp-2-dsl \VFI	172.168.0.50	327	UP
VFI	isp-2-dsl \VFI	172.168.0.52	327	UP
VFI	isp-2-dsl \VFI	172.168.0.54	327	UP
VFI	isp-2-dsl \VFI	172.168.0.56	327	UP
VFI	isp-2-dsl \VFI	172.168.0.60	327	UP
VFI	isp-2-dsl \VFI	172.168.0.61	327	UP
VFI	isp-2-dsl \VFI	172.168.0.62	327	UP
VFI	isp-2-dsl \VFI	172.168.0.63	327	UP
VFI	isp-2-dsl \VFI	172.168.0.64	327	UP
VFI	isp-2-dsl \VFI	172.168.0.67	327	UP
VFI	isp-2-dsl \VFI	172.168.0.69	327	UP
VFI	isp-2-dsl \VFI	172.168.0.70	327	UP
VFI	isp-2-dsl \VFI	172.168.0.72	327	UP
VFI	isp-2-dsl \VFI	172.168.0.73	327	UP
VFI	isp-2-dsl \VFI	172.168.0.74	327	UP
VFI	isp-2-dsl \VFI	172.168.0.93	327	UP
VFI	isp-2-dsl \VFI	172.198.100.11	327	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-2-dsl
l2 vfi isp-2-dsl manual

vpn id 327
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.72 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.62 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls

neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.198.100.11 encapsulation mpls
neighbor 172.168.0.40 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.162.180.100 encapsulation mpls

- **Muestras de MAC aprendidas:**

UIOINQE01#show mac-address-table count vlan 327
MAC Entries for Vlan 327 :
Dynamic Address Count: 18
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 18
Total MAC Addresses Available: 98314

UIOINQE01#show mac-address-table count vlan 327
MAC Entries for Vlan 327 :
Dynamic Address Count: 11
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 11
Total MAC Addresses Available: 98314

# MUESTRAS	M A Cs Aprenidas I S P – 2									
MUESTRA 1	11	11	13	8	13	9	8	10	11	9
	5	9	10	8	11	13	13	8	6	5
	8	11	13	9	10	9	13	11	8	10
	7	5	6	10	9	9	6	6	4	5
MUESTRA 2	10	10	7	8	5	10	7	4	8	9
	10	11	13	11	7	7	5	4	4	4
	11	12	15	12	15	15	16	7	8	9
	4	4	6	7	10	11	16	15	15	14
MUESTRA 3	10	11	10	11	9	8	7	10	11	11
	5	5	7	8	6	7	11	14	11	14
	10	8	6	8	7	7	7	7	5	5
	11	19	11	11	14	13	11	7	5	5
MUESTRA 4	11	12	13	11	13	9	8	10	11	9
	11	9	10	9	11	11	13	8	6	5
	8	11	13	9	10	9	10	11	8	10
	7	11	13	10	9	9	5	6	4	5

D.3.3 RESULTADOS CON COMANDOS IOS PARA EL ISP-3

- **Asociación de la VFI a la VLAN:**

UIOLCLE01#show run interface vlan 328
interface Vlan328
description *** VPLS ISP-3***
mtu 1900
no ip address
xconnect vfi isp-3-dsl
end

- **Puertos por donde cruza la VLAN:**

UIOLCLE01# show vlan all-port

VLAN Name Status Ports
---- ------------ ------- --------- -----
328 isp-3-dsl active Fa2/4, Gi5/2

- **Descripción de Interfaz troncal:**

UIOLCLE01#show interface g5/2 description
Interface Status Protocol Description
Fa2/4 up up *** TRONCAL ISP-3**

- **Configuración de la Interfaz troncal:**

UIOLCLE01#show run interface fa2/4
interface FastEthernet2/4
description *** TRONCAL ISP-3***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 328,333,400,401,3274,3725,4069
switchport mode trunk
switchport nonegotiate
speed nonegotiate
flowcontrol send off
end

- **Estado de los equipos de acceso:**

UIOLCLE01#show mpls l2 vc 328

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-3-dsl \VFI	172.162.180.100	328	DOWN
VFI	isp-3-dsl \VFI	172.163.10.100	328	UP
VFI	isp-3-dsl \VFI	172.164.30.100	328	UP
VFI	isp-3-dsl \VFI	172.165.40.100	328	UP
VFI	isp-3-dsl \VFI	172.168.0.10	328	UP
VFI	isp-3-dsl \VFI	172.168.0.14	328	UP
VFI	isp-3-dsl \VFI	172.168.0.18	328	UP
VFI	isp-3-dsl \VFI	172.168.0.22	328	UP
VFI	isp-3-dsl \VFI	172.168.0.26	328	UP
VFI	isp-3-dsl \VFI	172.168.0.28	328	UP
VFI	isp-3-dsl \VFI	172.168.0.30	328	UP
VFI	isp-3-dsl \VFI	172.168.0.32	328	UP
VFI	isp-3-dsl \VFI	172.168.0.34	328	UP
VFI	isp-3-dsl \VFI	172.168.0.36	328	UP
VFI	isp-3-dsl \VFI	172.168.0.38	328	UP

VFI	isp-3-dsl \VFI	172.168.0.40	328	UP
VFI	isp-3-dsl \VFI	172.168.0.42	328	UP
VFI	isp-3-dsl \VFI	172.168.0.44	328	UP
VFI	isp-3-dsl \VFI	172.168.0.46	328	UP
VFI	isp-3-dsl \VFI	172.168.0.48	328	UP
VFI	isp-3-dsl \VFI	172.168.0.50	328	UP
VFI	isp-3-dsl \VFI	172.168.0.52	328	UP
VFI	isp-3-dsl \VFI	172.168.0.54	328	UP
VFI	isp-3-dsl \VFI	172.168.0.56	328	UP
VFI	isp-3-dsl \VFI	172.168.0.60	328	UP
VFI	isp-3-dsl \VFI	172.168.0.61	328	UP
VFI	isp-3-dsl \VFI	172.168.0.63	328	UP
VFI	isp-3-dsl \VFI	172.168.0.64	328	UP
VFI	isp-3-dsl \VFI	172.168.0.65	328	DOWN
VFI	isp-3-dsl \VFI	172.168.0.66	328	DOWN
VFI	isp-3-dsl \VFI	172.168.0.67	328	UP
VFI	isp-3-dsl \VFI	172.168.0.68	328	DOWN
VFI	isp-3-dsl \VFI	172.168.0.69	328	UP
VFI	isp-3-dsl \VFI	172.168.0.70	328	UP
VFI	isp-3-dsl \VFI	172.168.0.71	328	DOWN
VFI	isp-3-dsl \VFI	172.168.0.72	328	UP
VFI	isp-3-dsl \VFI	172.168.0.73	328	UP
VFI	isp-3-dsl \VFI	172.168.0.74	328	UP
VFI	isp-3-dsl \VFI	172.168.0.76	328	UP
VFI	isp-3-dsl \VFI	172.168.0.82	328	UP
VFI	isp-3-dsl \VFI	172.168.0.93	328	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOLCLE01#show run | b l2 vfi isp-3-dsl
l2 vfi isp-3-dsl manual

vpn id 328
neighbor 172.164.30.100 encapsulation mpls
neighbor 172.162.180.100 encapsulation mpls
neighbor 172.165.40.100 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.163.10.100 encapsulation mpls
neighbor 172.168.0.76 encapsulation mpls
neighbor 172.168.0.82 encapsulation mpls
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.72 encapsulation mpls

neighbor 172.168.0.71 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.68 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.66 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.40 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.22 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.18 encapsulation mpls

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOLCLE01#show mac-address-table count vlan 328
MAC Entries for Vlan 328 :
Dynamic Address Count: 5
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 5
Total MAC Addresses Available: 65536

UIOLCLE01#show mac-address-table count vlan 328
MAC Entries for Vlan 328 :
Dynamic Address Count: 9
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 9
Total MAC Addresses Available: 65536

# MUESTRA	MAC APRENDIDAS ISP - 3									
MUESTRA 1	9	9	9	9	9	9	9	9	9	10
	10	10	10	9	9	9	10	10	10	9
	9	9	9	9	9	9	9	9	9	10
	10	10	10	9	9	9	10	10	10	9
MUESTRA 2	10	9	10	9	8	9	10	9	8	10
	9	9	9	9	9	9	10	10	9	8
	10	9	10	9	8	9	10	9	8	10
	9	9	9	9	9	9	10	10	9	8
MUESTRA 3	12	12	12	12	12	11	12	11	12	12
	12	12	12	12	12	11	12	11	12	12
	12	12	12	12	12	11	12	11	12	12
	12	12	12	12	12	11	12	11	12	12
MUESTRA 4	9	9	9	9	9	9	9	9	9	10
	9	9	9	9	9	9	10	10	10	9
	9	9	9	9	9	9	9	9	9	10
	9	8	9	9	9	9	9	9	9	9

D.3.4 RESULTADOS CON COMANDOS IOS PARA EL ISP-4

- **Ejemplo de muestras Mac tomadas con valor igual a 0**

UIOINQE01#show mac-address-table count vlan 339
MAC Entries for Vlan 339 :
Dynamic Address Count: 0
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 0
Total MAC Addresses Available: 98304

D.3.5 RESULTADOS CON COMANDOS IOS PARA EL ISP-5

- **Ejemplo de muestras Mac tomadas con valor igual a 0**

```
UIOLCLE01#show mac-address-table count vlan 322
MAC Entries for Vlan 322 :
Dynamic Address Count:                0
Static Address (User-defined) Count:  0
Total MAC Addresses In Use:           0
Total MAC Addresses Available:        65536
```

D.3.6 RESULTADOS CON COMANDOS IOS PARA EL ISP-6

- **Asociación de la VFI a la VLAN:**

```
UIOINQE01#show run interface vlan 343
interface Vlan343
description ### VPLS ISP-6 ###
mtu 1900
no ip address
xconnect vfi isp-6-dsl
end
```

- **Puertos por donde cruza la VLAN:**

```
UIOLCLE01# show vlan all-port
VLAN       Name     Status                 Ports
------- ---------  ----------   -------------------------
343     isp-6-dsl   active       Gi12/25, Gi12/40, Gi12/41
                                 Gi12/42, Gi12/43, Gi13/39
```

- **Descripción de Interfaz troncal:**

```
UIOINQE01#show interface gi13/39 description
Interface          Status      Protocol         Description
Gi13/39              up            up       *** TRONCAL ISP-6***
```

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface gi13/39
interface GigabitEthernet13/39
description *** TRONCAL ISP-6***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 180,181,200-203,258,261,300-330,343,346,348,350
switchport trunk allowed vlan add 353,357,360,363,401,408,413,416,422,425,436
switchport trunk allowed vlan add 444,447,450,451,461,465,466,470,497,503,506
switchport trunk allowed vlan add 514,516,519,523,527,530,542,549,588,699,841
switchport trunk allowed vlan add 860,952,953,999
switchport mode trunk
switchport nonegotiate
speed nonegotiate
flowcontrol send off
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 343

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-6-dsl \VFI	172.161.20.100	343	UP
VFI	isp-6-dsl \VFI	172.161.30.100	343	UP
VFI	isp-6-dsl \VFI	172.161.40.100	343	UP
VFI	isp-6-dsl \VFI	172.162.10.100	343	UP
VFI	isp-6-dsl \VFI	172.162.20.100	343	UP
VFI	isp-6-dsl \VFI	172.163.10.100	343	UP
VFI	isp-6-dsl \VFI	172.163.20.100	343	UP
VFI	isp-6-dsl \VFI	172.163.30.100	343	UP
VFI	isp-6-dsl \VFI	172.164.30.100	343	UP
VFI	isp-6-dsl \VFI	172.165.10.100	343	UP
VFI	isp-6-dsl \VFI	172.165.40.100	343	UP
VFI	isp-6-dsl \VFI	172.165.60.100	343	UP
VFI	isp-6-dsl \VFI	172.166.30.100	343	UP
VFI	isp-6-dsl \VFI	172.167.10.100	343	UP
VFI	isp-6-dsl \VFI	172.168.0.10	343	UP
VFI	isp-6-dsl \VFI	172.168.0.14	343	UP
VFI	isp-6-dsl \VFI	172.168.0.28	343	UP
VFI	isp-6-dsl \VFI	172.168.0.32	343	UP

VFI	isp-6-dsl \VFI	172.168.0.34	343	UP
VFI	isp-6-dsl \VFI	172.168.0.38	343	UP
VFI	isp-6-dsl \VFI	172.168.0.40	343	UP
VFI	isp-6-dsl \VFI	172.168.0.42	343	UP
VFI	isp-6-dsl \VFI	172.168.0.46	343	UP
VFI	isp-6-dsl \VFI	172.168.0.52	343	UP
VFI	isp-6-dsl \VFI	172.168.0.65	343	DOWN
VFI	isp-6-dsl \VFI	172.168.0.75	343	DOWN
VFI	isp-6-dsl \VFI	172.168.0.76	343	UP
VFI	isp-6-dsl \VFI	172.168.0.77	343	DOWN
VFI	isp-6-dsl \VFI	172.168.0.81	343	DOWN
VFI	isp-6-dsl \VFI	172.168.0.84	343	UP
VFI	isp-6-dsl \VFI	172.168.0.86	343	DOWN
VFI	isp-6-dsl \VFI	172.168.0.87	343	UP
VFI	isp-6-dsl \VFI	172.168.0.93	343	DOWN
VFI	isp-6-dsl \VFI	172.198.100.33	343	DOWN
VFI	isp-6-dsl \VFI	172.198.100.210	343	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-6-dsl
l2 vfi isp-6-dsl manual

l2 vfi GLOBAL_CROSSING manual
 vpn id 343
 neighbor 172.162.10.100 encapsulation mpls
 neighbor 172.198.100.33 encapsulation mpls
 neighbor 172.168.0.84 encapsulation mpls
 neighbor 172.161.30.100 encapsulation mpls
 neighbor 172.163.20.100 encapsulation mpls
 neighbor 172.168.0.42 encapsulation mpls
 neighbor 172.168.0.46 encapsulation mpls
 neighbor 172.168.0.52 encapsulation mpls
 neighbor 172.168.0.87 encapsulation mpls
 neighbor 172.168.0.40 encapsulation mpls
 neighbor 172.168.0.34 encapsulation mpls
 neighbor 172.168.0.14 encapsulation mpls
 neighbor 172.168.0.10 encapsulation mpls
 neighbor 172.198.100.210 encapsulation mpls
 neighbor 172.168.0.77 encapsulation mpls
 neighbor 172.168.0.76 encapsulation mpls
 neighbor 172.168.0.81 encapsulation mpls
 neighbor 172.168.0.32 encapsulation mpls

neighbor 172.162.20.100 encapsulation mpls
neighbor 172.163.30.100 encapsulation mpls
neighbor 172.168.0.75 encapsulation mpls
neighbor 172.166.30.100 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 172.165.40.100 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.164.30.100 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.163.10.100 encapsulation mpls
neighbor 172.168.0.86 encapsulation mpls
neighbor 172.167.10.100 encapsulation mpls
neighbor 172.165.10.100 encapsulation mpls
neighbor 172.165.60.100 encapsulation mpls
neighbor 172.161.20.100 encapsulation mpls
neighbor 172.161.40.100 encapsulation mpls

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 343
MAC Entries for Vlan 343 :
Dynamic Address Count: 51
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 51
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 343
MAC Entries for Vlan 343 :
Dynamic Address Count: 41
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 41
Total MAC Addresses Available: 98304

#MUESTRA	MACs APRENDIDAS I S P - 6									
MUESTRA 1	51	41	50	47	56	51	51	51	57	58
	51	67	57	51	53	50	49	46	43	39
	21	44	46	43	45	45	55	46	47	50
	45	43	40	23	21	24	43	34	45	37
MUESTRA 2	40	45	40	41	58	56	51	56	61	50
	62	50	45	67	46	48	47	69	42	66
	63	49	50	43	45	47	52	51	50	49
	34	28	46	66	41	45	66	65	56	51
MUESTRA 3	51	50	43	49	50	56	51	51	43	49
	47	50	22	43	40	23	47	50	50	43
	50	43	45	47	52	51	50	49	49	50
	49	50	43	45	47	52	51	50	43	46
MUESTRA 4	65	67	71	70	45	67	23	40	50	65
	47	50	45	43	40	23	21	45	43	40
	43	40	23	61	24	43	64	52	51	50
	23	47	34	28	26	32	58	51	67	57

D.3.7 RESULTADOS CON COMANDOS IOS PARA EL ISP-7

- **Asociación de la VFI a la VLAN:**

UIOINQE01#show run interface vlan 303
interface Vlan303
description *** VPLS ISP-7 ***
mtu 1900
no ip address
xconnect vfi isp-7-dsl
end

- **Puertos por donde cruza la VLAN:**

UIOINQE01# show vlan all-port

```
VLAN    Name       Status                    Ports
------ -------- --------- -------------------------------------------------------------
303    isp-7-dsl   active    Gi12/2, Gi12/10, Gi12/25, Gi12/35, Gi12/40, Gi12/41
                             Gi12/42, Gi12/43
```

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface g12/2 description
Interface Status Protocol Description
Gi12/2 up up *** TRONCAL ISP-7***

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface g12/2
interface GigabitEthernet12/2
description *** TRONCAL ISP-7***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 180,181,200-203,258,261,300-330,345,346,348,350
switchport trunk allowed vlan add 353,357,360,363,401,408,413,416,422,425,436
switchport trunk allowed vlan add 444,447,450,451,461,465,466,470,497,503,506
switchport trunk allowed vlan add 514,519,523,527,530,542,549,588,699,841,860
switchport trunk allowed vlan add 952,953,999,3759
switchport mode trunk
switchport nonegotiate
speed nonegotiate
mls qos vlan-based
flowcontrol send off
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 303

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-7-dsl \VFI	172.161.10.100	303	UP
VFI	isp-7-dsl \VFI	172.161.20.100	303	UP
VFI	isp-7-dsl \VFI	172.161.30.100	303	UP
VFI	isp-7-dsl \VFI	172.162.20.100	303	DOWN
VFI	isp-7-dsl \VFI	172.163.10.100	303	UP
VFI	isp-7-dsl \VFI	172.163.30.100	303	UP
VFI	isp-7-dsl \VFI	172.163.40.100	303	UP
VFI	isp-7-dsl \VFI	172.164.30.100	303	UP
VFI	isp-7-dsl \VFI	172.165.40.100	303	UP
VFI	isp-7-dsl \VFI	172.168.0.10	303	UP
VFI	isp-7-dsl \VFI	172.168.0.14	303	UP

VFI	isp-7-dsl \VFI	172.168.0.26	303	UP
VFI	isp-7-dsl \VFI	172.168.0.28	303	UP
VFI	isp-7-dsl \VFI	172.168.0.30	303	UP
VFI	isp-7-dsl \VFI	172.168.0.32	303	UP
VFI	isp-7-dsl \VFI	172.168.0.34	303	UP
VFI	isp-7-dsl \VFI	172.168.0.36	303	UP
VFI	isp-7-dsl \VFI	172.168.0.38	303	UP
VFI	isp-7-dsl \VFI	172.168.0.40	303	UP
VFI	isp-7-dsl \VFI	172.168.0.42	303	UP
VFI	isp-7-dsl \VFI	172.168.0.44	303	UP
VFI	isp-7-dsl \VFI	172.168.0.46	303	UP
VFI	isp-7-dsl \VFI	172.168.0.48	303	UP
VFI	isp-7-dsl \VFI	172.168.0.50	303	UP
VFI	isp-7-dsl \VFI	172.168.0.52	303	UP
VFI	isp-7-dsl \VFI	172.168.0.54	303	UP
VFI	isp-7-dsl \VFI	172.168.0.56	303	UP
VFI	isp-7-dsl \VFI	172.168.0.60	303	UP
VFI	isp-7-dsl \VFI	172.168.0.61	303	UP
VFI	isp-7-dsl \VFI	172.168.0.64	303	UP
VFI	isp-7-dsl \VFI	172.168.0.65	303	UP
VFI	isp-7-dsl \VFI	172.168.0.67	303	UP
VFI	isp-7-dsl \VFI	172.168.0.69	303	UP
VFI	isp-7-dsl \VFI	172.168.0.70	303	UP
VFI	isp-7-dsl \VFI	172.168.0.72	303	UP
VFI	isp-7-dsl \VFI	172.168.0.73	303	UP
VFI	isp-7-dsl \VFI	172.168.0.75	303	DOWN
VFI	isp-7-dsl \VFI	172.168.0.76	303	UP
VFI	isp-7-dsl \VFI	172.168.0.77	303	DOWN
VFI	isp-7-dsl \VFI	172.168.0.78	303	UP
VFI	isp-7-dsl \VFI	172.168.0.80	303	DOWN
VFI	isp-7-dsl \VFI	172.168.0.82	303	UP
VFI	isp-7-dsl \VFI	172.168.0.84	303	UP
VFI	isp-7-dsl \VFI	172.168.0.87	303	DOWN
VFI	isp-7-dsl \VFI	172.168.0.93	303	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-7-dsl
l2 vfi isp-7-dsl manual

vpn id 303
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.82 encapsulation mpls
neighbor 172.168.0.78 encapsulation mpls
neighbor 172.168.0.87 encapsulation mpls

neighbor 172.163.40.100 encapsulation mpls
neighbor 172.165.40.100 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.72 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 172.168.0.75 encapsulation mpls
neighbor 172.168.0.84 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.77 encapsulation mpls
neighbor 172.168.0.80 encapsulation mpls
neighbor 172.168.0.76 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.40 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.164.30.100 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.163.10.100 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.163.30.100 encapsulation mpls
neighbor 172.162.20.100 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.161.30.100 encapsulation mpls
neighbor 172.161.20.100 encapsulation mpls
neighbor 172.161.10.100 encapsulation mpls

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 303
MAC Entries for Vlan 327 :
Dynamic Address Count: 78
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 78
Total MAC Addresses Available: 98314

UIOINQE01#show mac-address-table count vlan 303
MAC Entries for Vlan 327 :
Dynamic Address Count: 79
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 79
Total MAC Addresses Available: 9831

#MUESTRA	MACs APRENDIDAS I S P - 7									
MUESTRA 1	78	79	76	74	70	70	71	71	71	72
	74	76	74	71	71	72	74	73	74	76
	72	74	74	73	74	73	74	76	72	73
	76	74	76	71	74	71	74	74	71	74
MUESTRA 2	71	74	71	71	74	71	71	74	76	74
	71	71	72	74	73	74	76	76	74	76
	76	74	74	76	74	76	71	74	74	71
	71	74	74	73	74	73	74	76	72	73
MUESTRA 3	74	71	71	72	74	73	74	76	76	74
	74	71	71	74	76	74	76	74	74	76
	76	74	71	71	74	76	74	76	76	75
	74	73	74	76	76	74	76	71	74	74
MUESTRA 4	68	68	67	69	70	71	69	68	69	68
	71	68	69	70	71	70	69	69	70	69
	70	71	70	70	70	69	69	70	70	72
	70	67	68	70	72	71	72	72	72	72

D.3.8 RESULTADOS CON COMANDOS IOS PARA EL ISP-8

- **Asociación de la VFI a la VLAN:**

UIOINQE01#show run interface vlan 345
interface Vlan345
description ### VPLS ISP-8 ###
mtu 1900
no ip address
xconnect vfi isp-8-dsl
end

- **Puertos por donde cruza la VLAN:**

UIOINQE01# show vlan all-port
VLAN Name Status Ports
---- ---------- --------- ----------
345 isp-8-dsl active Gi12/25, Gi12/35, Gi12/40, Gi12/41
Gi12/42, Gi12/43, Gi13/32

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface g13/32 description

Interface Status Protocol Description

Gi13/32 up up *** TRONCAL ISP-8***

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface g13/32
interface GigabitEthernet13/32
description *** TRONCAL ISP-8***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 345,346,466,467,3107-3113,3310
switchport mode trunk
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 345

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-8-dsl \VFI	172.162.180.100	345	DOWN
VFI	isp-8-dsl \VFI	172.165.40.100	345	UP
VFI	isp-8-dsl \VFI	172.168.0.10	345	UP
VFI	isp-8-dsl \VFI	172.168.0.14	345	UP
VFI	isp-8-dsl \VFI	172.168.0.26	345	UP
VFI	isp-8-dsl \VFI	172.168.0.28	345	UP

VFI	isp-8-dsl \VFI	172.168.0.30	345	UP
VFI	isp-8-dsl \VFI	172.168.0.32	345	UP
VFI	isp-8-dsl \VFI	172.168.0.34	345	UP
VFI	isp-8-dsl \VFI	172.168.0.36	345	UP
VFI	isp-8-dsl \VFI	172.168.0.38	345	UP
VFI	isp-8-dsl \VFI	172.168.0.40	345	UP
VFI	isp-8-dsl \VFI	172.168.0.42	345	UP
VFI	isp-8-dsl \VFI	172.168.0.44	345	UP
VFI	isp-8-dsl \VFI	172.168.0.46	345	UP
VFI	isp-8-dsl \VFI	172.168.0.48	345	UP
VFI	isp-8-dsl \VFI	172.168.0.50	345	UP
VFI	isp-8-dsl \VFI	172.168.0.52	345	UP
VFI	isp-8-dsl \VFI	172.168.0.54	345	UP
VFI	isp-8-dsl \VFI	172.168.0.56	345	UP
VFI	isp-8-dsl \VFI	172.168.0.60	345	UP
VFI	isp-8-dsl \VFI	172.168.0.61	345	UP
VFI	isp-8-dsl \VFI	172.168.0.62	345	UP
VFI	isp-8-dsl \VFI	172.168.0.63	345	UP
VFI	isp-8-dsl \VFI	172.168.0.64	345	UP
VFI	isp-8-dsl \VFI	172.168.0.65	345	DOWN
VFI	isp-8-dsl \VFI	172.168.0.67	345	UP
VFI	isp-8-dsl \VFI	172.168.0.69	345	UP
VFI	isp-8-dsl \VFI	172.168.0.70	345	UP
VFI	isp-8-dsl \VFI	172.168.0.72	345	UP
VFI	isp-8-dsl \VFI	172.168.0.74	345	UP
VFI	isp-8-dsl \VFI	172.168.0.93	345	UP
VFI	isp-8-dsl \VFI	172.198.100.45	345	DOWN
VFI	isp-8-dsl \VFI	172.198.100.210	345	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-8-dsl
l2 vfi isp-8-dsl manual

vpn id 345
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls

neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.40 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.62 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.72 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls
neighbor 172.198.100.45 encapsulation mpls
neighbor 172.168.0.10 encapsulation mpls
neighbor 10.5.40.100 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.198.100.210 encapsulation mpls
neighbor 172.162.180.100 encapsulation mpls

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 345
MAC Entries for Vlan 345 :
Dynamic Address Count: 6
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 6
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 345
MAC Entries for Vlan 345 :
Dynamic Address Count: 6
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 6
Total MAC Addresses Available: 98304

#MUESTRAS	MACs APRENDIDAS I S P - 8									
MUESTRA 1	6	6	6	5	6	5	5	5	5	6
	6	6	6	6	6	6	6	6	5	5
	6	6	6	6	6	6	6	6	5	6
	6	6	5	5	6	5	5	6	5	5
MUESTRA 2	6	5	5	6	6	6	6	6	6	6
	5	5	5	5	5	5	6	6	6	6
	6	5	5	5	5	5	5	5	4	5
	6	6	5	6	5	5	6	5	6	5
MUESTRA 3	4	5	4	5	5	5	5	5	5	5
	5	5	5	4	5	4	5	5	5	4
	5	5	5	5	5	4	5	5	4	5
	5	5	4	5	5	4	5	5	4	5
MUESTRA 4	4	4	4	5	5	5	5	6	5	5
	5	5	5	4	5	4	5	6	5	6
	6	5	5	6	5	6	5	5	5	4
	5	6	5	5	5	5	6	5	5	5

D.3.9 RESULTADOS CON COMANDOS IOS PARA EL ISP-9

- **Ejemplo de muestras Mac tomadas con valor 0**

UIOLCLE01#show mac-address-table count vlan 352
MAC Entries for Vlan 352 :
Dynamic Address Count: 0
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 0
Total MAC Addresses Available: 65536

D.3.10 RESULTADOS CON COMANDOS IOS PARA EL ISP-10

- **Asociación de la VFI a la VLAN:**

UIOINQE01#show run interface vlan 315
interface Vlan315
description ### VPLS ISP-10 ###
mtu 1900
no ip address
xconnect vfi isp-10-dsl
end

- **Puertos por donde cruza la VLAN:**

UIOINQE01# show vlan all-port
VLAN Name Status Ports
---- ------------ --------- ---------
315 isp-15-dsl active Gi12/10, Gi12/21, Gi12/25, Gi12/35, Gi12/40, Gi12/41
Gi12/42, Gi12/43, Gi13/3

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface g13/3 description
Interface Status Protocol Description
Gi13/3 up up *** TRONCAL ISP-10***

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface g13/3
interface GigabitEthernet13/3
description *** TRONCAL ISP-10***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 315,332,805
switchport mode trunk
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 315

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-10-dsl \VFI	172.162.180.100	315	DOWN
VFI	isp-10-dsl \VFI	172.168.0.10	315	UP
VFI	isp-10-dsl \VFI	172.168.0.14	315	UP
VFI	isp-10-dsl \VFI	172.168.0.26	315	UP
VFI	isp-10-dsl \VFI	172.168.0.28	315	UP
VFI	isp-10-dsl \VFI	172.168.0.30	315	UP
VFI	isp-10-dsl \VFI	172.168.0.32	315	UP
VFI	isp-10-dsl \VFI	172.168.0.34	315	UP
VFI	isp-10-dsl \VFI	172.168.0.36	315	UP
VFI	isp-10-dsl \VFI	172.168.0.38	315	UP
VFI	isp-10-dsl \VFI	172.168.0.40	315	UP
VFI	isp-10-dsl \VFI	172.168.0.42	315	UP
VFI	isp-10-dsl \VFI	172.168.0.44	315	UP
VFI	isp-10-dsl \VFI	172.168.0.46	315	UP
VFI	isp-10-dsl \VFI	172.168.0.48	315	UP
VFI	isp-10-dsl \VFI	172.168.0.50	315	UP
VFI	isp-10-dsl \VFI	172.168.0.52	315	UP
VFI	isp-10-dsl \VFI	172.168.0.54	315	UP
VFI	isp-10-dsl \VFI	172.168.0.56	315	UP
VFI	isp-10-dsl \VFI	172.168.0.60	315	UP
VFI	isp-10-dsl \VFI	172.168.0.61	315	UP
VFI	isp-10-dsl \VFI	172.168.0.62	315	UP
VFI	isp-10-dsl \VFI	172.168.0.63	315	UP
VFI	isp-10-dsl \VFI	172.168.0.64	315	UP
VFI	isp-10-dsl \VFI	172.168.0.67	315	UP
VFI	isp-10-dsl \VFI	172.168.0.69	315	UP
VFI	isp-10-dsl \VFI	172.168.0.70	315	UP
VFI	isp-10-dsl \VFI	172.168.0.72	315	DOWN
VFI	isp-10-dsl \VFI	172.168.0.73	315	UP
VFI	isp-10-dsl \VFI	172.168.0.74	315	UP
VFI	isp-10-dsl \VFI	172.168.0.93	315	UP
VFI	isp-10-dsl \VFI	172.198.100.10	315	DOWN
VFI	isp-10-dsl \VFI	172.198.100.210	315	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-10-dsl
l2 vfi isp-10-adsl manual
 vpn id 315
 neighbor 172.168.0.74 encapsulation mpls
 neighbor 172.168.0.72 encapsulation mpls
 neighbor 172.168.0.70 encapsulation mpls
 neighbor 172.168.0.69 encapsulation mpls
 neighbor 172.168.0.67 encapsulation mpls
 neighbor 172.168.0.62 encapsulation mpls
 neighbor 172.168.0.61 encapsulation mpls
 neighbor 172.168.0.54 encapsulation mpls
 neighbor 172.168.0.52 encapsulation mpls
 neighbor 172.168.0.50 encapsulation mpls
 neighbor 172.168.0.93 encapsulation mpls
 neighbor 172.168.0.34 encapsulation mpls
 neighbor 172.168.0.56 encapsulation mpls
 neighbor 172.168.0.48 encapsulation mpls
 neighbor 172.168.0.42 encapsulation mpls
 neighbor 172.168.0.64 encapsulation mpls
 neighbor 172.168.0.60 encapsulation mpls
 neighbor 172.168.0.38 encapsulation mpls
 neighbor 172.168.0.14 encapsulation mpls
 neighbor 172.168.0.36 encapsulation mpls
 neighbor 172.168.0.40 encapsulation mpls
 neighbor 172.168.0.44 encapsulation mpls
 neighbor 172.168.0.46 encapsulation mpls
 neighbor 172.168.0.30 encapsulation mpls
 neighbor 172.168.0.32 encapsulation mpls
 neighbor 172.168.0.26 encapsulation mpls
 neighbor 172.168.0.28 encapsulation mpls
 neighbor 172.198.100.210 encapsulation mpls
 neighbor 172.198.100.10 encapsulation mpls
 neighbor 172.168.0.63 encapsulation mpls
 neighbor 172.168.0.10 encapsulation mpls
 neighbor 172.168.0.73 encapsulation mpls
 neighbor 172.162.180.100 encapsulation mpls

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 315
MAC Entries for Vlan 315 :
Dynamic Address Count: 6
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 6
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 315
MAC Entries for Vlan 315 :
Dynamic Address Count: 6
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 6
Total MAC Addresses Available: 98304

# MUESTRAS	MACs APRENDIDAS I S P - 10									
MUESTRA 1	6	6	6	6	6	6	6	6	7	7
	7	7	7	7	7	7	7	7	7	6
	7	7	7	7	7	7	7	7	7	7
	6	6	6	6	6	6	6	7	7	7
MUESTRA 2	9	8	8	8	8	8	10	10	10	10
	9	10	10	10	10	8	8	8	8	8
	10	9	10	9	9	9	10	9	9	9
	10	9	9	9	9	9	10	10	8	10
MUESTRA 3	7	7	7	7	7	7	7	7	7	7
	8	7	7	7	8	8	8	8	7	7
	8	8	8	8	8	8	7	8	7	8
	7	8	8	8	8	8	8	8	8	8
MUESTRA 4	9	9	9	9	9	9	9	9	9	9
	9	9	9	9	8	8	8	8	8	8
	9	9	8	8	8	8	8	8	8	9
	8	8	8	9	9	9	8	8	8	8

D.3.11 RESULTADOS CON COMANDOS IOS PARA EL ISP-11

- **Asociación de la VFI a la VLAN:**

UIOINQE01#show run interface vlan 307
interface Vlan307
description ### VPLS ISP-11 ###
mtu 1900
no ip address
xconnect vfi isp-11-dsl
end

- **Puertos por donde cruza la VLAN:**

UIOINQE01# show vlan all-port
VLAN Name Status Ports
---- ---------- --------- ---------------
307 isp-11-dsl active Fa2/1, Gi5/2, Gi12/10, Gi12/25, Gi12/35
Gi12/40, Gi12/41, Gi12/42, Gi12/43

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface fa2/1 description
Interface Status Protocol Description
Fa2/1 up up *** TRONCAL ISP-11***

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface fa2/1
interface FastEthernet2/1
description *** TRONCAL ISP-11**
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 307,338,2307,2339,2340,3307
switchport mode trunk
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 307

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-11-dsl \VFI	172.161.10.100	307	UP
VFI	isp-11-dsl \VFI	172.161.20.100	307	UP
VFI	isp-11-dsl \VFI	172.161.240.100	307	DOWN
VFI	isp-11-dsl \VFI	172.162.180.100	307	DOWN
VFI	isp-11-dsl \VFI	172.163.10.100	307	UP
VFI	isp-11-dsl \VFI	172.163.30.100	307	UP
VFI	isp-11-dsl \VFI	172.165.40.100	307	UP
VFI	isp-11-dsl \VFI	172.168.0.10	307	UP
VFI	isp-11-dsl \VFI	172.168.0.14	307	UP
VFI	isp-11-dsl \VFI	172.168.0.18	307	UP
VFI	isp-11-dsl \VFI	172.168.0.22	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.26	307	UP

VFI	isp-11-dsl \VFI	172.168.0.28	307	UP
VFI	isp-11-dsl \VFI	172.168.0.30	307	UP
VFI	isp-11-dsl \VFI	172.168.0.32	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.34	307	UP
VFI	isp-11-dsl \VFI	172.168.0.36	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.38	307	UP
VFI	isp-11-dsl \VFI	172.168.0.40	307	UP
VFI	isp-11-dsl \VFI	172.168.0.42	307	UP
VFI	isp-11-dsl \VFI	172.168.0.44	307	UP
VFI	isp-11-dsl \VFI	172.168.0.46	307	UP
VFI	isp-11-dsl \VFI	172.168.0.48	307	UP
VFI	isp-11-dsl \VFI	172.168.0.50	307	UP
VFI	isp-11-dsl \VFI	172.168.0.52	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.54	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.56	307	UP
VFI	isp-11-dsl \VFI	172.168.0.60	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.61	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.63	307	UP
VFI	isp-11-dsl \VFI	172.168.0.64	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.65	307	UP
VFI	isp-11-dsl \VFI	172.168.0.66	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.67	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.68	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.69	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.70	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.71	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.72	307	UP
VFI	isp-11-dsl \VFI	172.168.0.73	307	UP
VFI	isp-11-dsl \VFI	172.168.0.74	307	UP
VFI	isp-11-dsl \VFI	172.168.0.76	307	UP
VFI	isp-11-dsl \VFI	172.168.0.78	307	UP
VFI	isp-11-dsl \VFI	172.168.0.80	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.87	307	DOWN
VFI	isp-11-dsl \VFI	172.168.0.93	307	UP
VFI	isp-11-dsl \VFI	172.198.100.10	307	UP
VFI	isp-11-dsl \VFI	172.198.100.20	307	DOWN
VFI	isp-11-dsl \VFI	172.198.100.210	307	UP
VFI	isp-11-dsl \VFI	172.198.100.211	307	DOWN

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-11-dsl
l2 vfi isp-11-dsl manual
 vpn id 307
 neighbor 172.161.10.100 encapsulation mpls
 neighbor 172.198.100.10 encapsulation mpls
 neighbor 172.198.100.210 encapsulation mpls
 neighbor 172.162.180.100 encapsulation mpls

neighbor 172.168.0.14 encapsulation mpls
neighbor 172.165.40.100 encapsulation mpls
neighbor 172.163.30.100 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.163.10.100 encapsulation mpls
neighbor 172.168.0.78 encapsulation mpls
neighbor 172.168.0.87 encapsulation mpls
neighbor 172.168.0.76 encapsulation mpls
neighbor 172.198.100.20 encapsulation mpls
neighbor 172.168.0.80 encapsulation mpls
neighbor 172.198.100.211 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.72 encapsulation mpls
neighbor 172.168.0.71 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.68 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.66 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.40 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.22 encapsulation mpls
neighbor 172.168.0.18 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.161.20.100 encapsulation mpls
neighbor 172.161.240.100 encapsulation mpls

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 322
MAC Entries for Vlan 322 :
Dynamic Address Count: 26
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 26
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 322
MAC Entries for Vlan 322 :
Dynamic Address Count: 27
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 27
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 322
MAC Entries for Vlan 322 :
Dynamic Address Count: 26
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 26
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 322
MAC Entries for Vlan 322 :
Dynamic Address Count: 27
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 27
Total MAC Addresses Available: 98304

# MUESTRAS	MACs APRENDIDAS I S P - 11									
MUESTRA 1	26	27	26	27	26	27	26	27	27	26
	25	26	27	27	27	27	27	27	27	27
	27	25	27	27	27	27	26	27	27	27
	27	27	28	27	26	26	27	27	26	27
MUESTRA 2	24	24	24	25	26	27	27	26	25	26
	24	25	24	28	25	26	25	26	26	24
	26	25	27	25	27	26	27	25	28	25
	24	27	27	26	27	25	28	25	26	27
MUESTRA 3	26	26	25	27	25	24	26	26	26	27
	27	27	25	25	27	24	26	26	27	26
	27	27	24	24	26	25	25	24	26	25
	26	27	25	27	27	25	27	26	26	26
MUESTRA 4	27	25	27	26	26	25	28	25	26	27
	25	27	28	25	27	25	26	25	26	26
	25	26	27	25	25	28	25	26	26	26
	26	26	25	27	27	27	26	27	25	28

D.3.12 RESULTADOS CON COMANDOS IOS PARA EL ISP-12

- **Asociación de la VFI a la VLAN:**

UIOINQE011#show run interface vlan 305
interface Vlan305
description ### VPLS ISP-12###
mtu 1900
no ip address
xconnect vfi puntonetdsl
end

- **Puertos por donde cruza la VLAN:**

UIOINQE011# show vlan all-port
VLAN Name Status Ports
---- -------------- --------- ---
305 isp-12-dsl active Gi5/24, Gi12/2, Gi12/10, Gi12/25, Gi12/35, Gi12/38, Gi12/40, Gi12/41, Gi12/42, Gi12/43, Gi13/

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface g13/2 description
Interface Status Protocol Description
Gi13/2 up up *** TRONCAL ISP-12***

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface g13/2
interface GigabitEthernet13/2
description *** TRONCAL ISP-12 ***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 200-202,302,305,357,557,662,707,711,760,771,891
switchport trunk allowed vlan add 924,1406,1591,1615,1616,2923,3315,3925
switchport mode trunk
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 305

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-12-dsl \VFI	172.161.10.100	305	UP
VFI	isp-12-dsl \VFI	172.161.20.100	305	UP
VFI	isp-12-dsl \VFI	172.161.30.100	305	UP
VFI	isp-12-dsl \VFI	172.163.10.100	305	UP
VFI	isp-12-dsl \VFI	172.163.30.100	305	UP
VFI	isp-12-dsl \VFI	172.163.40.100	305	UP
VFI	isp-12-dsl \VFI	172.163.30.100	305	UP
VFI	isp-12-dsl \VFI	172.163.40.100	305	UP
VFI	isp-12-dsl \VFI	172.168.0.10	305	UP
VFI	isp-12-dsl \VFI	172.168.0.14	305	UP
VFI	isp-12-dsl \VFI	172.168.0.22	305	DOWN
VFI	isp-12-dsl \VFI	172.168.0.26	305	DOWN
VFI	isp-12-dsl \VFI	172.168.0.28	305	UP
VFI	isp-12-dsl \VFI	172.168.0.30	305	UP
VFI	isp-12-dsl \VFI	172.168.0.32	305	UP
VFI	isp-12-dsl \VFI	172.168.0.34	305	UP
VFI	isp-12-dsl \VFI	172.168.0.36	305	UP

VFI	isp-12-dsl \VFI	172.168.0.38	305	UP
VFI	isp-12-dsl \VFI	172.168.0.40	305	DOWN
VFI	isp-12-dsl \VFI	172.168.0.42	305	UP
VFI	isp-12-dsl \VFI	172.168.0.44	305	UP
VFI	isp-12-dsl \VFI	172.168.0.46	305	UP
VFI	isp-12-dsl \VFI	172.168.0.48	305	UP
VFI	isp-12-dsl \VFI	172.168.0.50	305	UP
VFI	isp-12-dsl \VFI	172.168.0.52	305	UP
VFI	isp-12-dsl \VFI	172.168.0.54	305	UP
VFI	isp-12-dsl \VFI	172.168.0.56	305	UP
VFI	isp-12-dsl \VFI	172.168.0.60	305	UP
VFI	isp-12-dsl \VFI	172.168.0.61	305	UP
VFI	isp-12-dsl \VFI	172.168.0.62	305	UP
VFI	isp-12-dsl \VFI	172.168.0.63	305	UP
VFI	isp-12-dsl \VFI	172.168.0.64	305	DOWN
VFI	isp-12-dsl \VFI	172.168.0.65	305	UP
VFI	isp-12-dsl \VFI	172.168.0.66	305	DOWN
VFI	isp-12-dsl \VFI	172.168.0.67	305	UP
VFI	isp-12-dsl \VFI	172.168.0.69	305	UP
VFI	isp-12-dsl \VFI	172.168.0.70	305	UP
VFI	isp-12-dsl \VFI	172.168.0.72	305	UP
VFI	isp-12-dsl \VFI	172.168.0.73	305	UP
VFI	isp-12-dsl \VFI	172.168.0.74	305	UP
VFI	isp-12-dsl \VFI	172.168.0.76	305	UP
VFI	isp-12-dsl \VFI	172.168.0.79	305	UP
VFI	isp-12-dsl \VFI	172.168.0.82	305	UP
VFI	isp-12-dsl \VFI	172.168.0.84	305	UP
VFI	isp-12-dsl \VFI	172.168.0.93	305	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-12-dsl
l2 vfi isp-12-dsl manual
 vpn id 305
 neighbor 172.168.0.79 encapsulation mpls
 neighbor 172.168.0.65 encapsulation mpls
 neighbor 172.168.0.62 encapsulation mpls
 neighbor 172.168.0.52 encapsulation mpls
 neighbor 172.168.0.50 encapsulation mpls
 neighbor 172.168.0.46 encapsulation mpls
 neighbor 172.168.0.44 encapsulation mpls
 neighbor 172.168.0.67 encapsulation mpls

neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.22 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.66 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.163.10.100 encapsulation mpls
neighbor 172.168.0.82 encapsulation mpls
neighbor 172.161.30.100 encapsulation mpls
neighbor 172.168.0.76 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.168.0.72 encapsulation mpls
neighbor 172.163.30.100 encapsulation mpls
neighbor 172.163.30.100 encapsulation mpls
neighbor 172.161.20.100 encapsulation mpls
neighbor 172.168.0.40 encapsulation mpls
neighbor 172.163.40.100 encapsulation mpls
neighbor 172.161.10.100 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.163.40.100 encapsulation mpls
neighbor 172.168.0.84 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls

- **Muestras MAC:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 305
MAC Entries for Vlan 305 :

Dynamic Address Count: 249
Static Address (User-defined) Count: 1
Total MAC Addresses In Use: 250
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 305
MAC Entries for Vlan 305 :
Dynamic Address Count: 249
Static Address (User-defined) Count: 1
Total MAC Addresses In Use: 250
Total MAC Addresses Available: 98304

# MUESTRAS	MACs APRENDIDAS I S P - 12									
MUESTRA 1	250	250	250	250	200	81	104	120	147	156
	248	247	240	235	243	225	220	201	218	217
	214	215	214	214	215	214	215	214	215	216
	240	235	243	225	220	201	218	217	216	215
MUESTRA 2	240	235	243	225	220	201	218	217	216	215
	235	243	225	220	201	218	207	216	147	156
	235	243	225	220	101	208	217	216	215	216
	140	243	204	225	101	120	104	171	114	215
MUESTRA 3	250	250	250	250	200	81	104	120	147	156
	248	247	240	235	243	225	220	201	218	217
	214	215	214	214	215	214	215	214	215	216
	240	235	243	225	220	201	218	217	216	215
MUESTRA 4	240	215	243	125	220	201	218	217	216	215
	235	113	225	220	201	218	217	216	147	156
	235	243	225	120	201	218	217	216	215	216
	240	243	214	225	201	120	104	171	214	215

D.3.13 RESULTADOS CON COMANDOS IOS PARA EL ISP-13

- **Asociación de la VFI a la VLAN:**

UIOLCLE01#show run interface vlan 314
interface Vlan314
description ### VPLS ISP-13 ###
mtu 1900
no ip address
xconnect vfi isp-13-dsl
end

- **Puertos por donde cruza la VLAN:**

UIOLCLE01# show vlan all-port

```
VLAN       Name         Status    Ports
------  ------------  --------- ---------------
314      isp-13-dsl    active    Fa2/40, Gi5/2
```

- **Descripción de Interfaz troncal:**

UIOLCLE01#show interface fa2/40 description
Interface Status Protocol Description
Fa2/40 up up *** TRONCAL ISP-13***

- **Configuración de la Interfaz troncal:**

UIOLCLE01#show run interface fa2/40
interface FastEthernet2/40
description *** TRONCAL ISP-13**
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 314,356,587,3278
switchport mode trunk
end

- **Estado de los equipos de acceso:**

UIOLCLE01#show mpls l2 vc 314

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-13-dsl \VFI	172.163.30.100	314	UP
VFI	isp-13-dsl \VFI	172.168.0.10	314	UP
VFI	isp-13-dsl \VFI	172.168.0.14	314	UP
VFI	isp-13-dsl \VFI	172.168.0.18	314	UP
VFI	isp-13-dsl \VFI	172.168.0.22	314	DOWN
VFI	isp-13-dsl \VFI	172.168.0.26	314	UP
VFI	isp-13-dsl \VFI	172.168.0.28	314	UP

VFI	isp-13-dsl \VFI	172.168.0.30	314	UP
VFI	isp-13-dsl \VFI	172.168.0.32	314	UP
VFI	isp-13-dsl \VFI	172.168.0.34	314	UP
VFI	isp-13-dsl \VFI	172.168.0.36	314	UP
VFI	isp-13-dsl \VFI	172.168.0.38	314	UP
VFI	isp-13-dsl \VFI	172.168.0.40	314	UP
VFI	isp-13-dsl \VFI	172.168.0.42	314	UP
VFI	isp-13-dsl \VFI	172.168.0.44	314	UP
VFI	isp-13-dsl \VFI	172.168.0.46	314	UP
VFI	isp-13-dsl \VFI	172.168.0.48	314	UP
VFI	isp-13-dsl \VFI	172.168.0.50	314	UP
VFI	isp-13-dsl \VFI	172.168.0.52	314	UP
VFI	isp-13-dsl \VFI	172.168.0.54	314	UP
VFI	isp-13-dsl \VFI	172.168.0.56	314	UP
VFI	isp-13-dsl \VFI	172.168.0.60	314	UP
VFI	isp-13-dsl \VFI	172.168.0.61	314	UP
VFI	isp-13-dsl \VFI	172.168.0.63	314	UP
VFI	isp-13-dsl \VFI	172.168.0.64	314	UP
VFI	isp-13-dsl \VFI	172.168.0.65	314	DOWN
VFI	isp-13-dsl \VFI	172.168.0.66	314	DOWN
VFI	isp-13-dsl \VFI	172.168.0.67	314	UP
VFI	isp-13-dsl \VFI	172.168.0.68	314	DOWN
VFI	isp-13-dsl \VFI	172.168.0.69	314	UP
VFI	isp-13-dsl \VFI	172.168.0.70	314	UP
VFI	isp-13-dsl \VFI	172.168.0.71	314	DOWN
VFI	isp-13-dsl \VFI	172.168.0.72	314	UP
VFI	isp-13-dsl \VFI	172.168.0.73	314	DOWN
VFI	isp-13-dsl \VFI	172.168.0.74	314	DOWN
VFI	isp-13-dsl \VFI	172.168.0.79	314	UP
VFI	isp-13-dsl \VFI	172.168.0.80	314	DOWN
VFI	isp-13-dsl \VFI	172.168.0.93	314	UP
VFI	isp-13-dsl \VFI	172.198.100.19	314	UP
VFI	isp-13-dsl \VFI	172.198.100.23	314	DOWN
VFI	isp-13-dsl \VFI	172.198.100.25	314	DOWN
VFI	isp-13-dsl \VFI	172.198.100.27	314	DOWN
VFI	isp-13-dsl \VFI	172.198.100.45	314	DOWN
VFI	isp-13-dsl \VFI	172.198.100.210	314	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOLCLE01#show run | b l2 vfi isp-13-dsl
l2 vfi isp-13-dsl manual

vpn id 314
neighbor 172.163.30.100 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls

```
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.168.0.22 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 172.168.0.66 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.68 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.71 encapsulation mpls
neighbor 172.168.0.72 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.18 encapsulation mpls
neighbor 172.198.100.45 encapsulation mpls
neighbor 172.198.100.25 encapsulation mpls
neighbor 172.198.100.27 encapsulation mpls
neighbor 172.198.100.210 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.168.0.80 encapsulation mpls
neighbor 172.198.100.23 encapsulation mpls
neighbor 172.168.0.79 encapsulation mpls
neighbor 172.168.0.40 encapsulation mpls
neighbor 172.198.100.19 encapsulation mpls
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
```

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOLCLE01#show mac-address-table count vlan 314
MAC Entries for Vlan 314 :
Dynamic Address Count: 13
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 13
Total MAC Addresses Available: 65536

UIOLCLE01#show mac-address-table count vlan 314
MAC Entries for Vlan 314 :
Dynamic Address Count: 13
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 13
Total MAC Addresses Available: 65536

UIOLCLE01#show mac-address-table count vlan 314
MAC Entries for Vlan 314 :
Dynamic Address Count: 13
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 13
Total MAC Addresses Available: 65536

UIOLCLE01#show mac-address-table count vlan 314
MAC Entries for Vlan 314 :
Dynamic Address Count: 13
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 13
Total MAC Addresses Available: 65536

# MUESTRAS	MACs APRENDIDAS I S P - 13									
MUESTRA 1	13	13	13	13	13	13	13	13	13	13
	13	13	13	13	13	12	13	13	13	13
	11	12	11	12	13	11	13	13	12	12
	12	12	11	11	11	12	11	12	12	13
MUESTRA 2	6	7	6	7	8	6	7	6	7	6
	8	6	6	7	7	7	7	8	8	8
	7	8	6	6	7	6	8	6	7	8
	6	6	6	7	7	6	7	6	7	8
MUESTRA 3	10	11	12	11	10	11	11	11	10	11
	11	11	11	10	11	12	11	10	11	12
	12	11	10	11	11	11	10	11	12	11
	10	11	10	10	12	10	11	10	12	11
MUESTRA 4	11	13	11	12	11	13	13	13	13	11
	11	12	11	12	12	13	13	11	12	12
	13	12	13	12	12	11	13	13	13	12
	12	12	11	12	12	13	11	11	12	12

D.3.14 RESULTADOS CON COMANDOS IOS PARA EL ISP-14

- **Ejemplo de muestras Mac tomadas con valor 0**

UIOINQE01#show mac-address-table count vlan 312
MAC Entries for Vlan 312:
Dynamic Address Count: 0
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 0
Total MAC Addresses Available: 98304

D.3.14 RESULTADOS CON COMANDOS IOS PARA EL ISP-16

- **Ejemplo de muestras Mac tomadas con valor 0**

UIOINQE01#show mac-address-table count vlan 309

MAC Entries for Vlan 309 :
Dynamic Address Count: 66
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 66
Total MAC Addresses Available: 98304

D.3.15 RESULTADOS CON COMANDOS IOS PARA LA IP FIJA

- **Asociación de la VFI a la VLAN:**

UIOINQE01#show run interface vlan 202
interface Vlan202
description ### IP-FIJA ###
mtu 1900
no ip address
xconnect vfi ip-fija
end

- **Puertos por donde cruza la VLAN:**

UIOINQE01# show vlan all-port
VLAN Name Status Ports
---- ---------- --------- ----------
202 ip-fija active Gi5/24, Gi12/10, Gi12/21, Gi12/22, Gi12/25, Gi12/35
Gi12/38, Gi12/40, Gi12/41, Gi12/42, Gi12/43, Gi4/0/1

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface g5/2 description
Interface Status Protocol Description
Gi4/0/1 up up *** TRONCAL ISP***

- **Configuración de la Interfaz troncal:**

interface GigabitEthernet4/0/1
description *** TRONCAL ISP***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 202,304,309,312,349,363,2923,3101,3102,3106-3109,3112,3113…..
switchport mode trunk
switchport nonegotiate
speed nonegotiate
flowcontrol send off

- **Estado de los equipos de acceso:**

UIONQE01#show mpls l2 vc 202
interface GigabitEthernet4/0/1
description *** TRONCAL ISP ***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 202,304,309,312,349,363,2923,3101,3102,3106-3109,3112,3113…..
switchport mode trunk
switchport nonegotiate
speed nonegotiate
flowcontrol send off

- **Estado de los equipos de acceso:**

UIONQE01#show mpls l2 vc 202

Local intf	Local circuit	Dest address	VC ID	Status
VFI	ip-fija \VFI	172.161.10.100	202	UP
VFI	ip-fija \VFI	172.161.20.100	202	UP
VFI	ip-fija \VFI	172.161.30.100	202	UP
VFI	ip-fija \VFI	172.161.40.100	202	UP
VFI	ip-fija \VFI	172.162.10.100	202	UP
VFI	ip-fija \VFI	172.162.20.100	202	UP
VFI	ip-fija \VFI	172.163.10.100	202	UP
VFI	ip-fija \VFI	172.163.20.100	202	UP
VFI	ip-fija \VFI	172.163.40.100	202	UP
VFI	ip-fija \VFI	172.164.30.100	202	UP
VFI	ip-fija \VFI	172.165.30.100	202	UP
VFI	ip-fija \VFI	172.165.60.100	202	UP
VFI	ip-fija \VFI	172.166.10.100	202	UP
VFI	ip-fija \VFI	172.166.30.100	202	UP
VFI	ip-fija \VFI	172.167.20.100	202	UP
VFI	ip-fija \VFI	172.168.0.22	202	UP
VFI	ip-fija \VFI	172.168.0.26	202	UP
VFI	ip-fija \VFI	172.168.0.28	202	DOWN
VFI	ip-fija \VFI	172.168.0.34	202	DOWN
VFI	ip-fija \VFI	172.168.0.38	202	UP
VFI	ip-fija \VFI	172.168.0.42	202	UP
VFI	ip-fija \VFI	172.168.0.48	202	DOWN
VFI	ip-fija \VFI	172.168.0.56	202	UP
VFI	ip-fija \VFI	172.168.0.60	202	UP
VFI	ip-fija \VFI	172.168.0.64	202	UP

VFI	ip-fija \VFI	172.168.0.65	202	UP
VFI	ip-fija \VFI	172.168.0.67	202	UP
VFI	ip-fija \VFI	172.168.0.78	202	UP
VFI	ip-fija \VFI	172.168.0.87	202	DOWN
VFI	ip-fija \VFI	172.168.0.93	202	DOWN
VFI	ip-fija \VFI	172.168.0.95	202	DOWN
VFI	ip-fija \VFI	10.20.100.10	202	DOWN
VFI	ip-fija \VFI	10.20.100.11	202	UP
VFI	ip-fija \VFI	10.20.100.34	202	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi ip-fija
l2 vfi ip-fija manual

vpn id 202
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.164.30.100 encapsulation mpls
neighbor 10.20.100.11 encapsulation mpls
neighbor 172.168.0.87 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 10.20.100.10 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.163.40.100 encapsulation mpls
neighbor 172.161.20.100 encapsulation mpls
neighbor 172.162.20.100 encapsulation mpls
neighbor 172.163.20.100 encapsulation mpls
neighbor 172.162.10.100 encapsulation mpls
neighbor 172.166.10.100 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.95 encapsulation mpls
neighbor 172.163.10.100 encapsulation mpls
neighbor 172.166.30.100 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.161.30.100 encapsulation mpls
neighbor 172.165.30.100 encapsulation mpls
neighbor 172.161.40.100 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.78 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls

neighbor 172.168.0.22 encapsulation mpls
neighbor 172.167.20.100 encapsulation mpls
neighbor 10.20.100.34 encapsulation mpls
neighbor 172.165.60.100 encapsulation mpls
neighbor 172.161.10.100 encapsulation mpls

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 202
MAC Entries for Vlan 202:
Dynamic Address Count: 218
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 218
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 202
MAC Entries for Vlan 202 :
Dynamic Address Count: 220
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 220
Total MAC Addresses Available: 98304

# MUESTRAS	MACs APRENDIDAS IP FIJA									
MUESTRA 1	218	220	211	201	203	194	199	203	199	157
	220	211	195	197	211	211	205	209	210	157
	122	84	83	205	219	81	102	219	218	217
	89	90	201	202	203	220	218	216	220	221
MUESTRA 2	122	84	83	205	219	81	102	219	218	217
	89	90	201	202	203	220	218	216	220	221
	216	109	89	220	219	221	225	210	156	297
	160	157	158	211	212	156	210	210	209	170
MUESTRA 3	203	211	218	217	209	157	89	201	218	214
	202	201	200	157	158	89	90	201	218	217
	209	82	216	211	221	222	223	221	209	201
	201	201	202	217	218	211	203	203	204	201
MUESTRA 4	212	214	220	110	214	210	209	89	220	185
	90	89	90	210	211	212	89	90	210	211
	187	91	200	201	203	210	187	154	150	201
	218	203	202	201	99	90	89	90	210	202

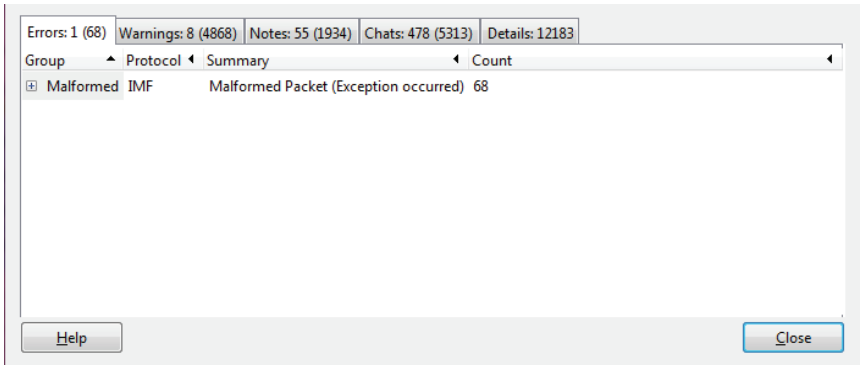
ANEXO E

RESULTADOS GENERALES DEL DIAGNÓSTICO DE LAS VPLSS- FASE FINAL

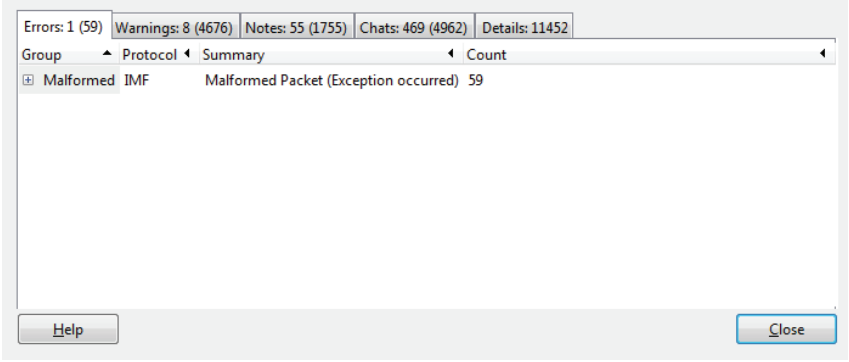
E. 1 RESULTADOS FINALES OBTENIDOS CON WIRESHARK MEDIANTE EXPERT COMPOSITE E IO GRAPHS

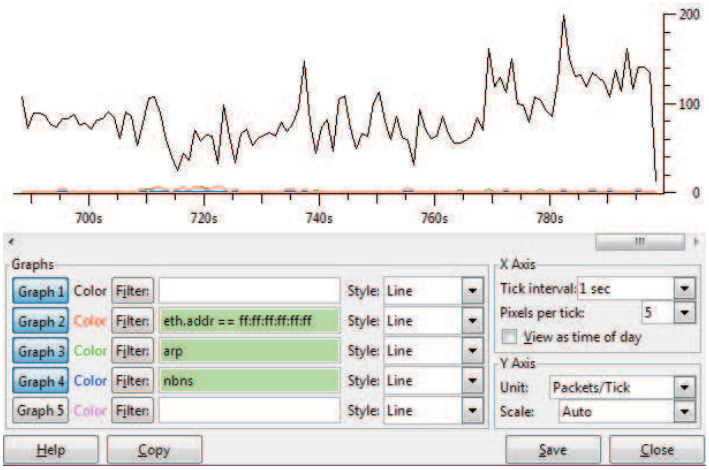
E.1.1 RESULTADOS FINALES DE WIRESHARK PARA EL ISP-2

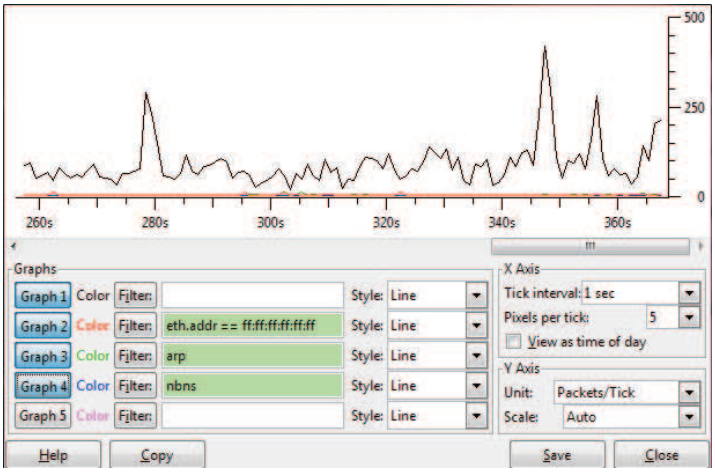
Paquetes capturados: 37176



Paquetes capturados: 40319



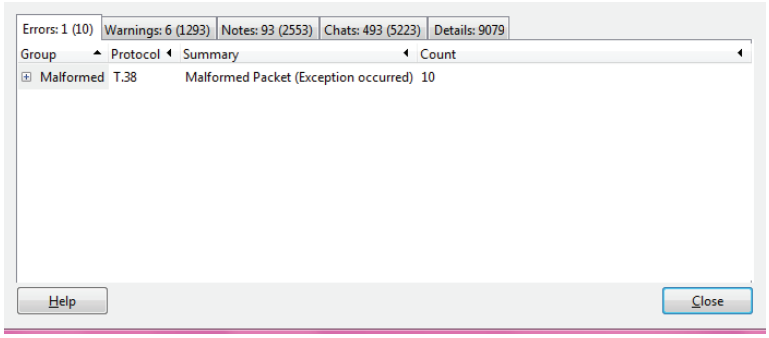




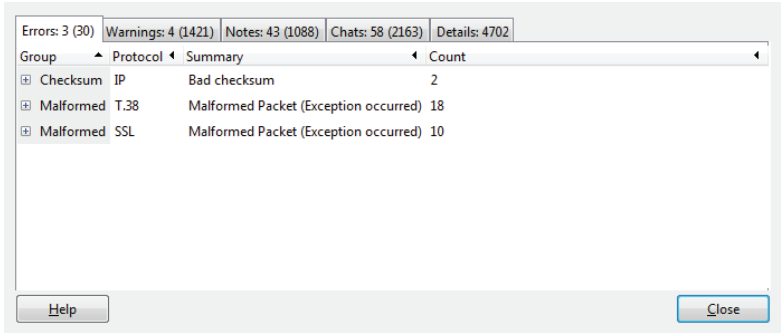
E.1.2 RESULTADOS FINALES DE WIRESHARK PARA EL ISP-6

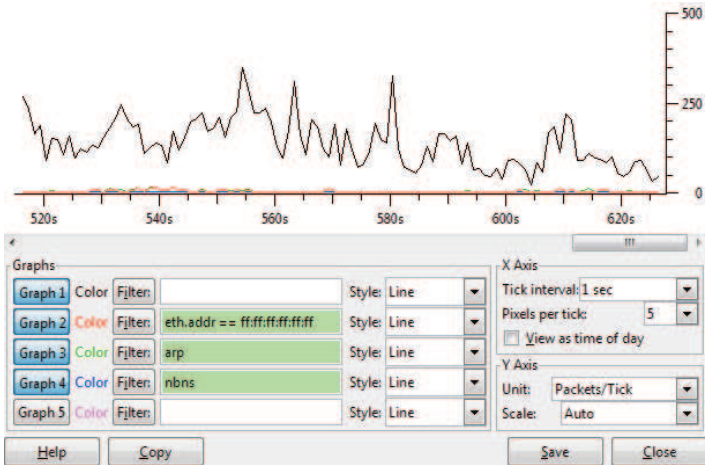
- **VLAN 2911**

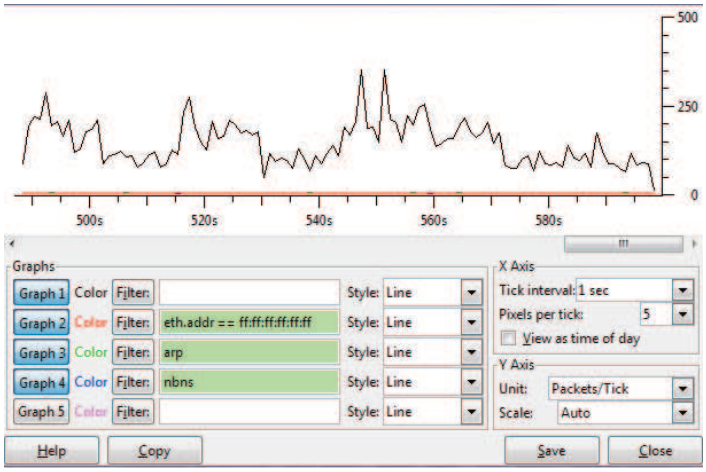
Paquetes capturados: 37142



Paquetes capturados: 35912

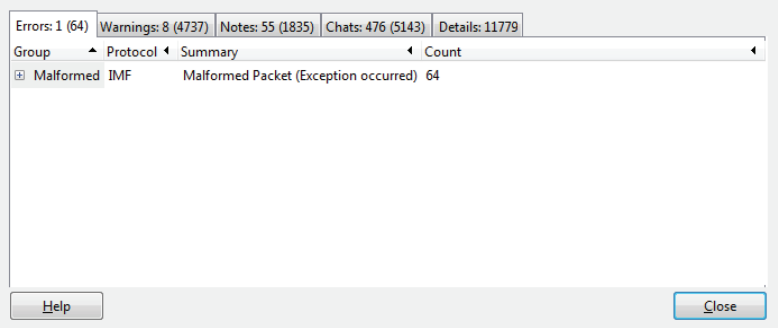




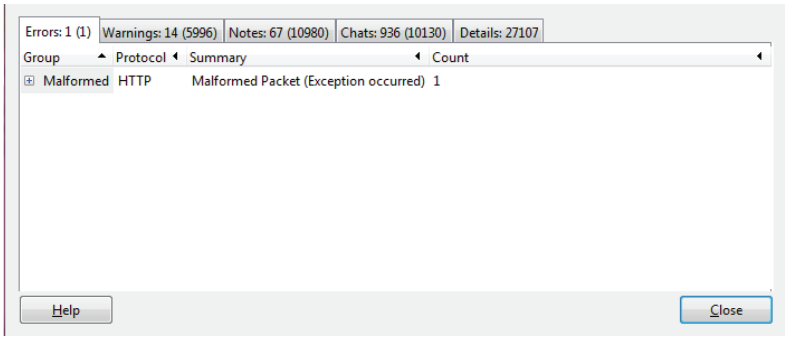


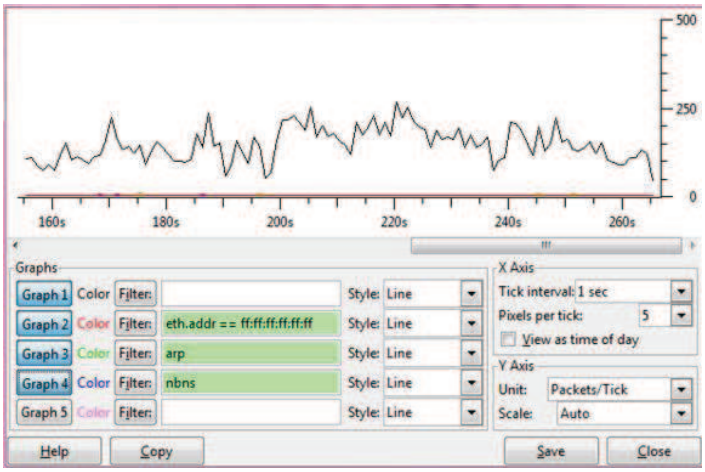
- **VLAN 2912**

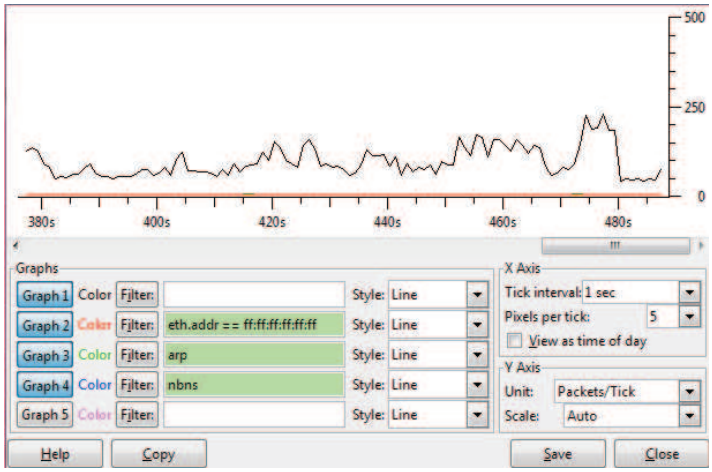
Paquetes capturados: 39518



Paquetes capturados: 41150



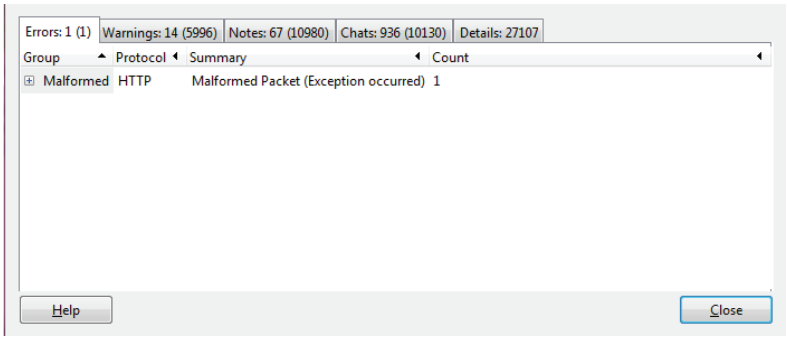




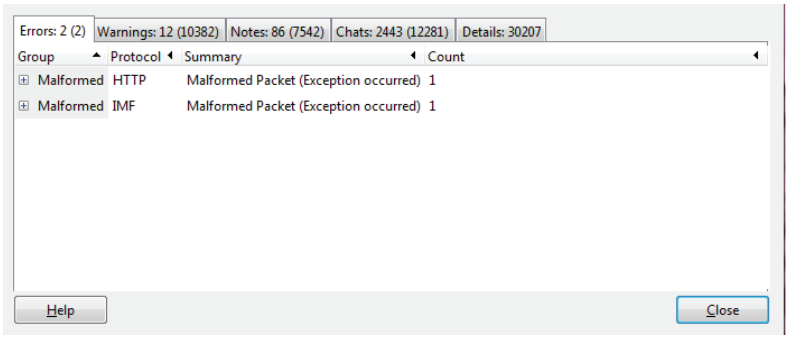
E.1.3 RESULTADOS FINALES DE WIRESHARK PARA EL ISP-12

- **VLAN 305**

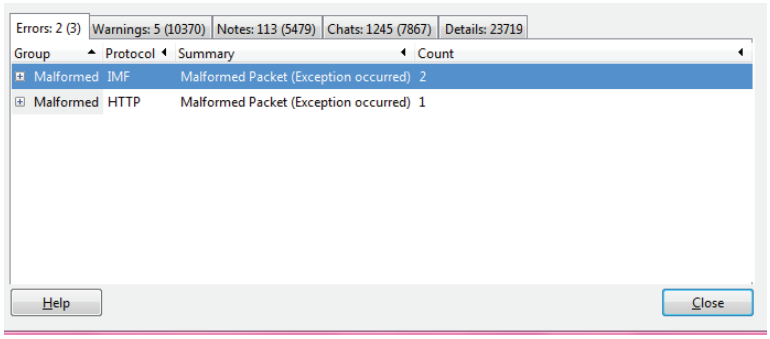
Paquetes capturados: 41150



Paquetes capturados: 67661

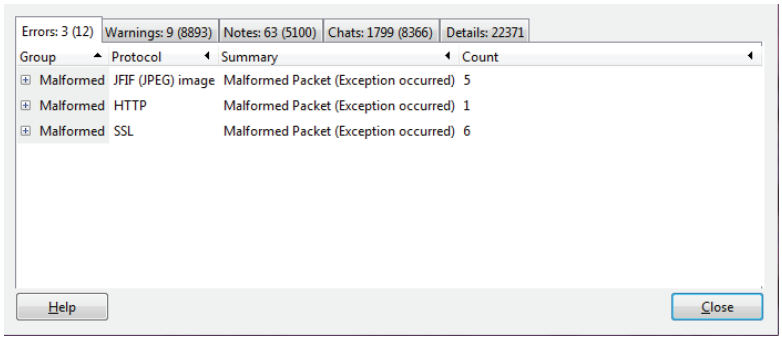


Paquetes capturados: 59525

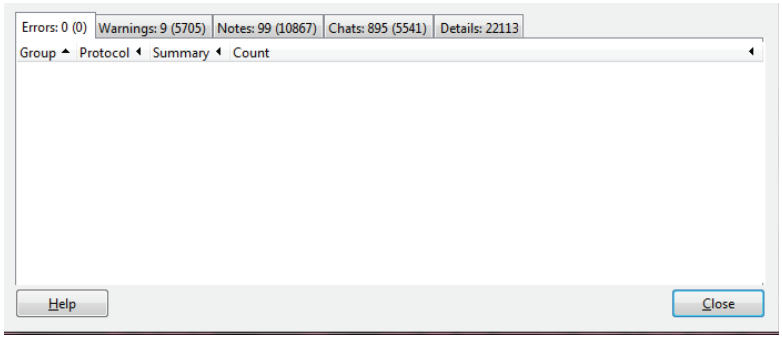


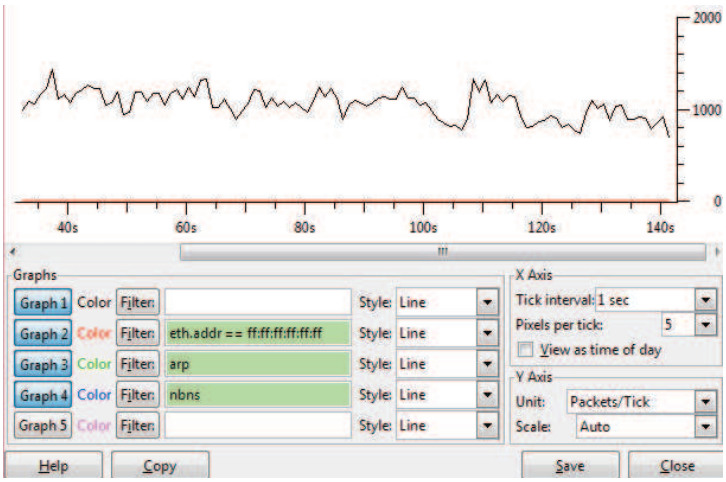
- **VLAN 366**

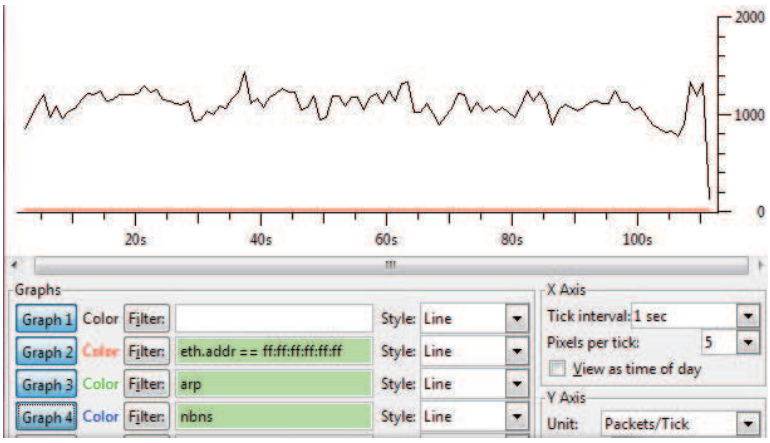
Paquetes capturados: 55624



Paquetes capturados: 48624

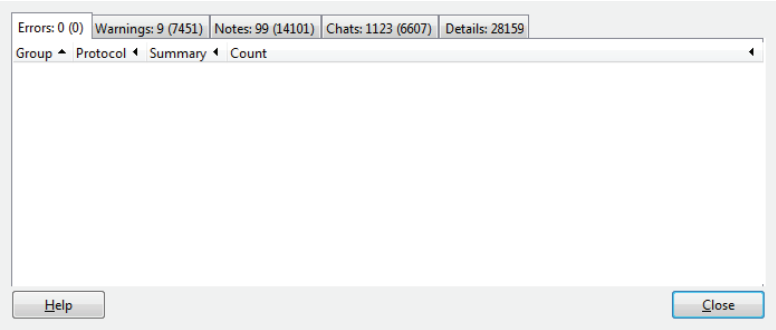




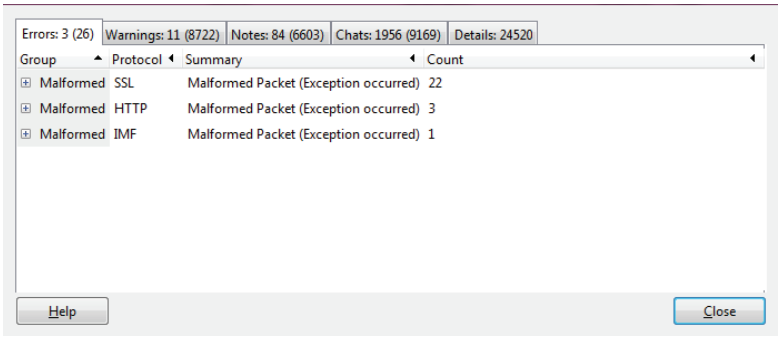


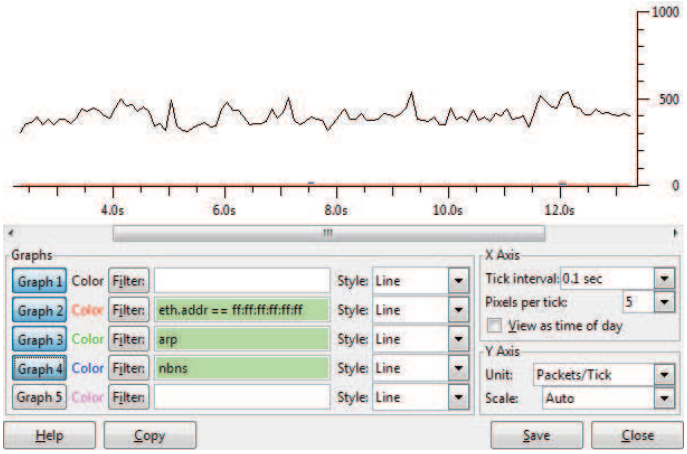
- **VLAN 367**

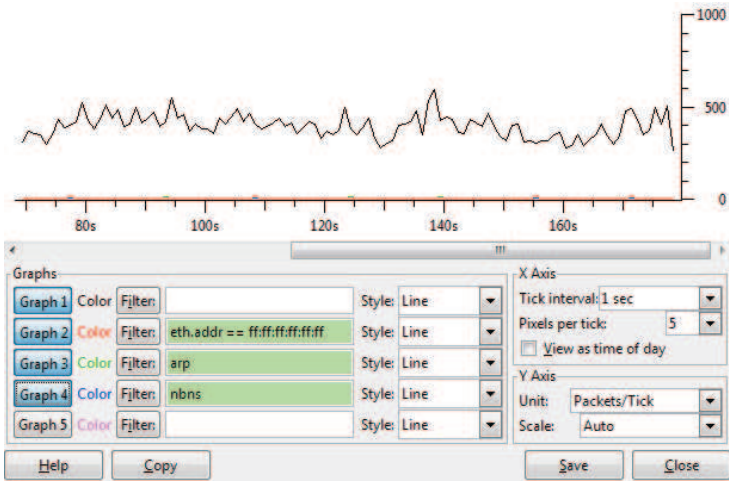
Paquetes capturados: 58182



Paquetes capturados: 61310



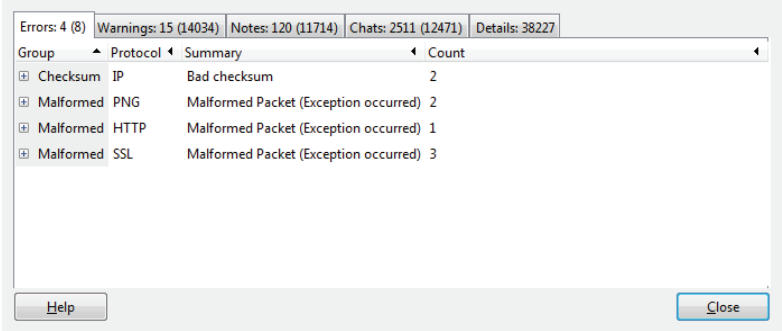




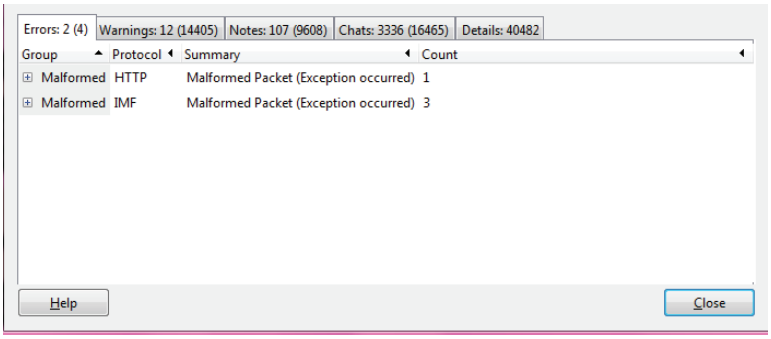
E.1.4 RESULTADOS FINALES DE WIRESHARK PARA EL ISP-15

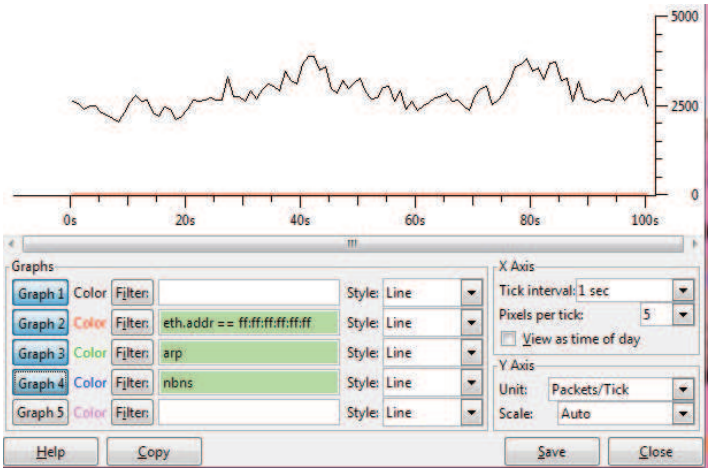
- **VLAN 304**

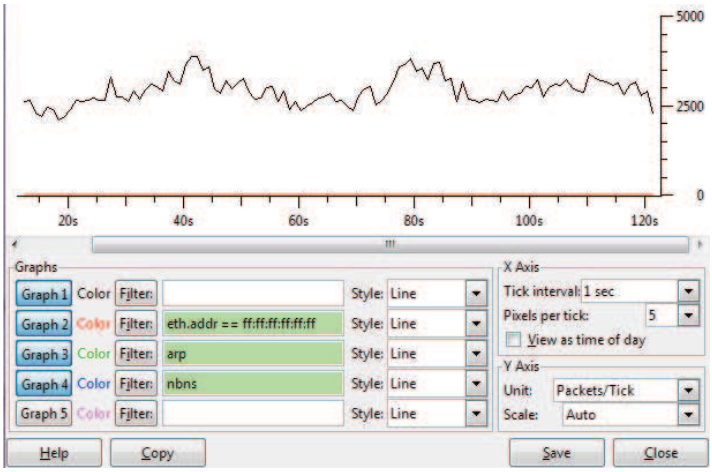
Paquetes capturados: 81958



Paquetes capturados: 78233

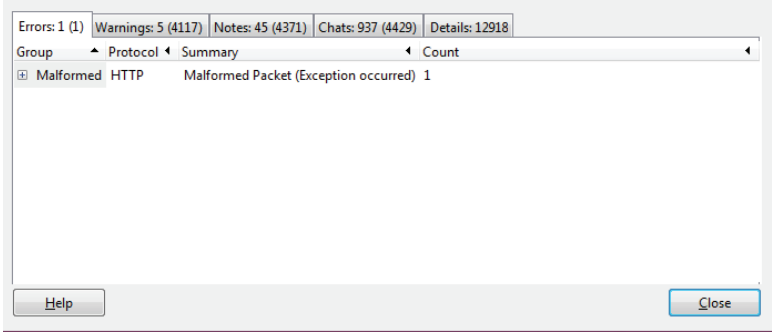




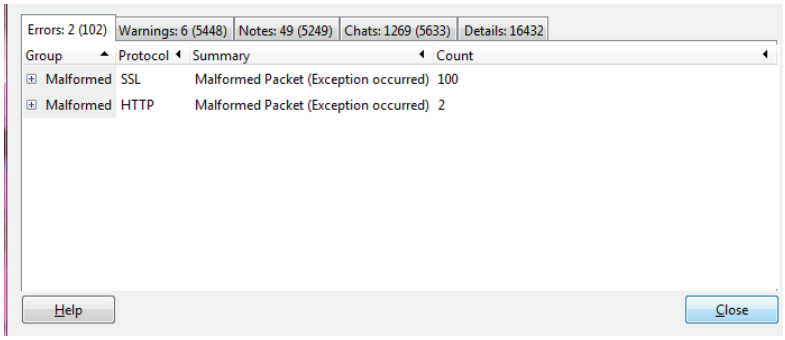


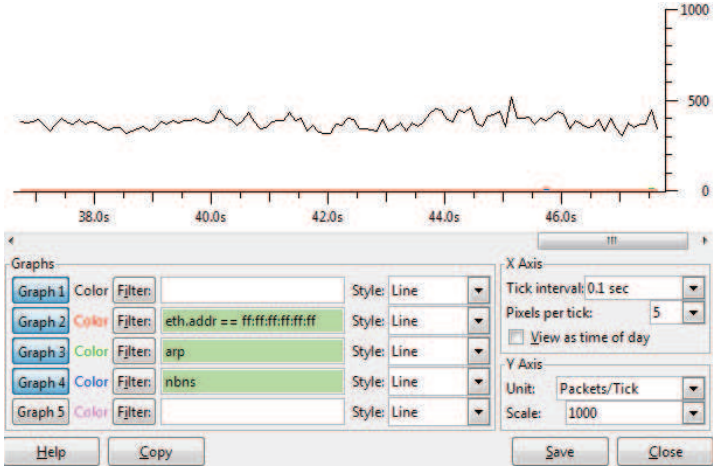
- **VLAN 310**

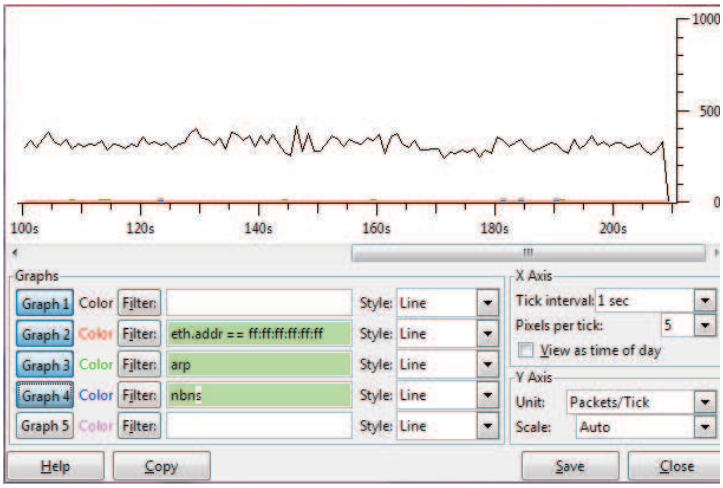
Paquetes capturados: 52988



Paquetes capturados: 58004



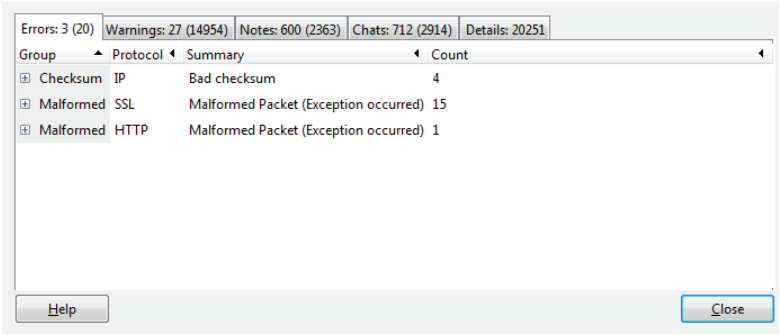




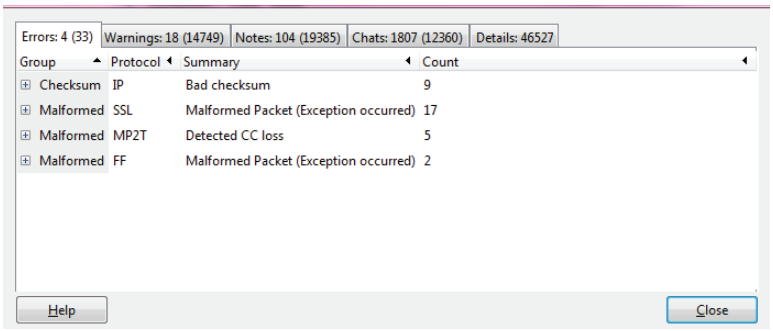
E.1.5 RESULTADOS FINALES DE WIRESHARK PARA LA IP FIJA

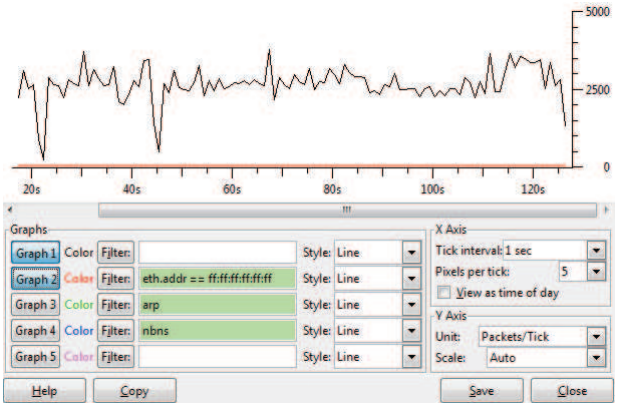
- **VLAN 3370**

Paquetes capturados: 96980



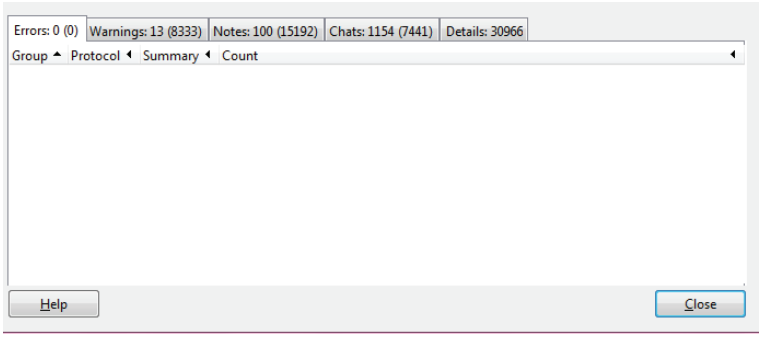
Paquetes capturados: 93611



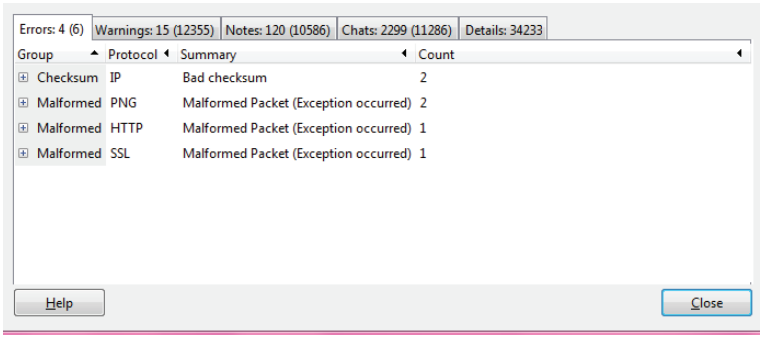


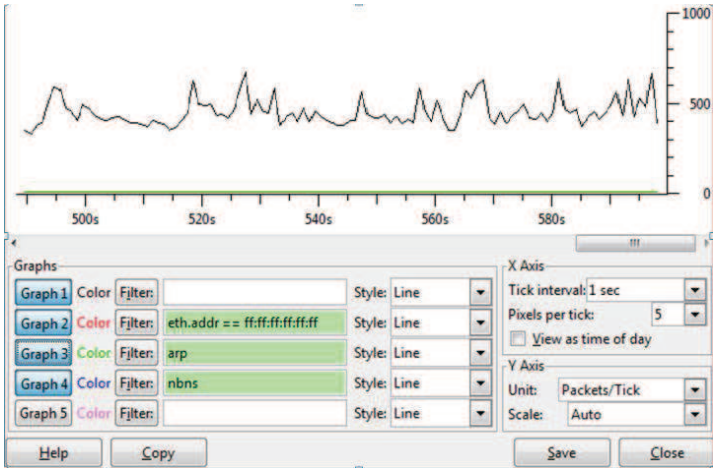
- **VLAN 3372**

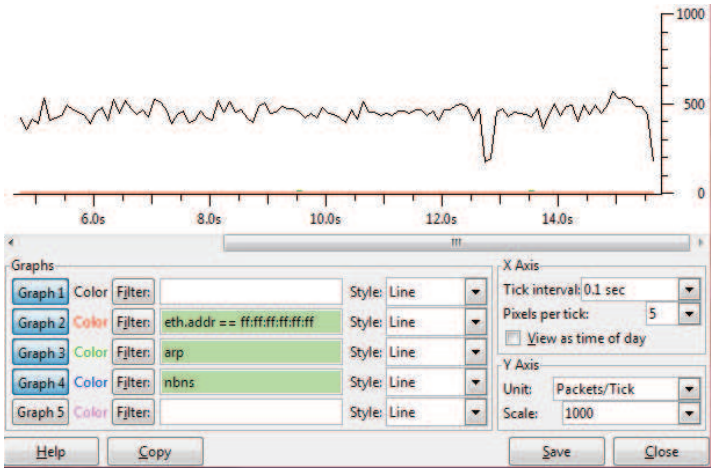
Paquetes capturados 62108



Paquetes capturados: 72433

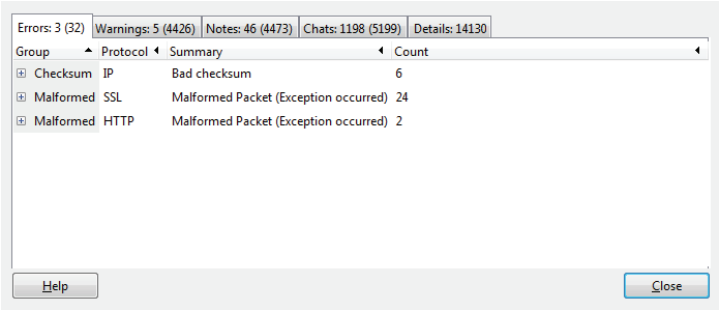




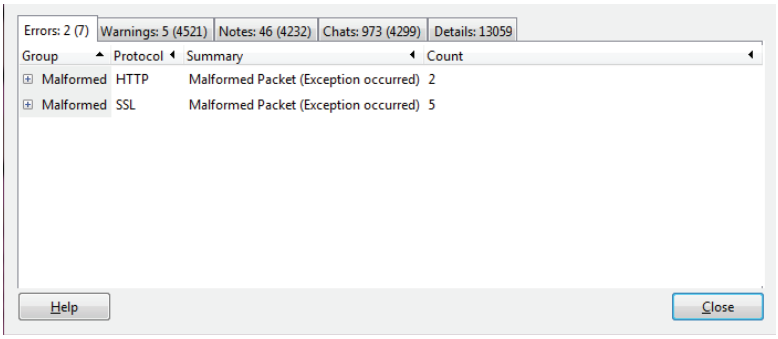


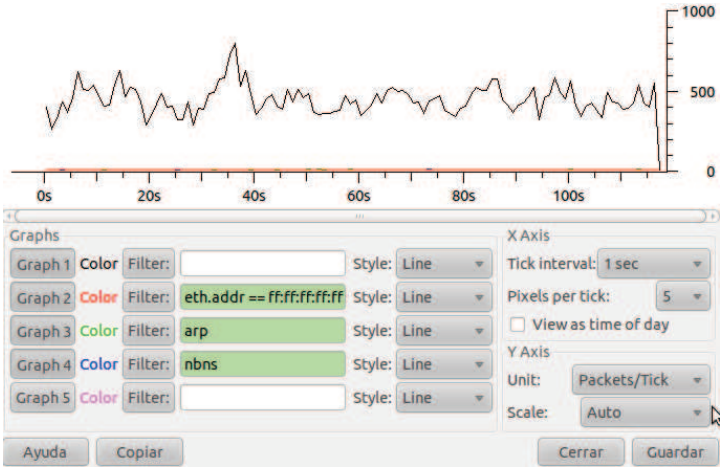
- **VLAN 3374**

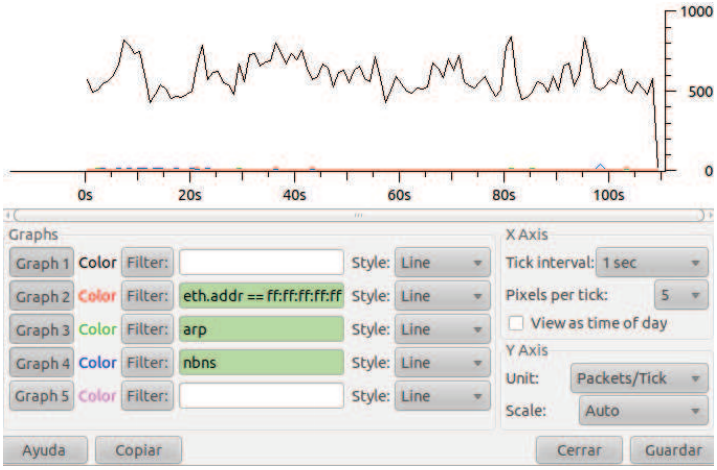
Paquetes capturados 42108



Paquetes capturados 56010

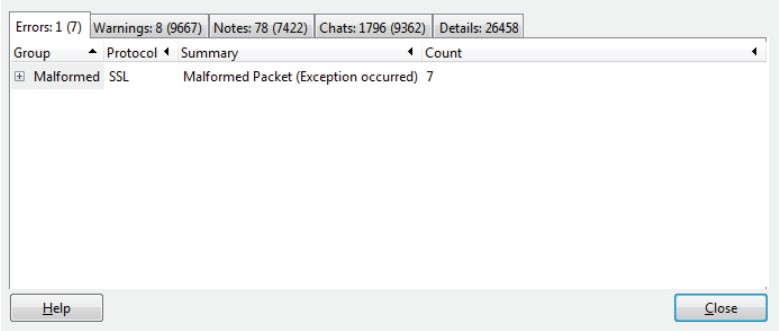




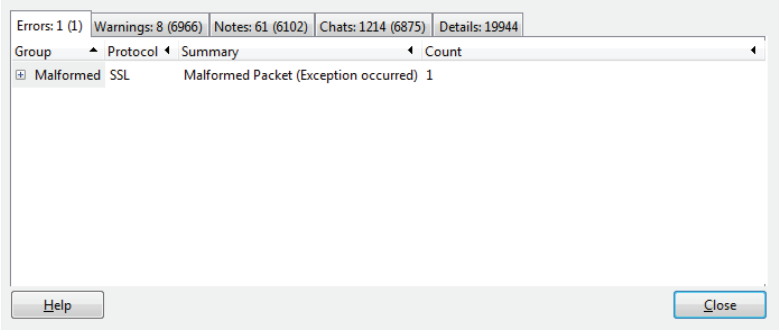


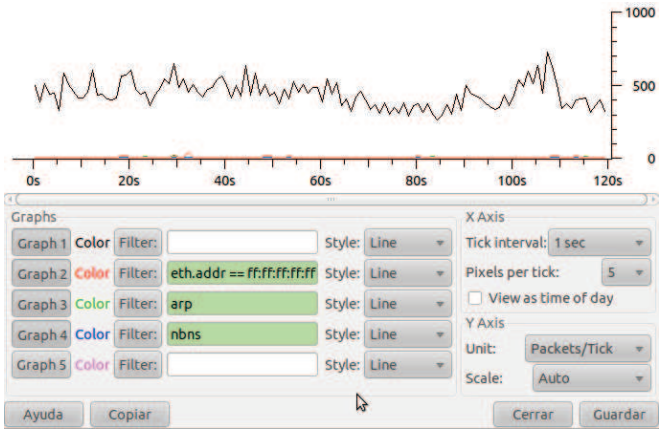
- **VLAN 3376**

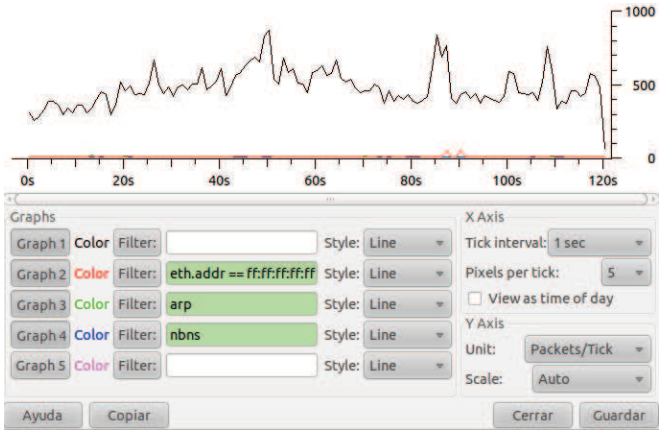
Paquetes capturados 66725



Paquetes capturados 58020

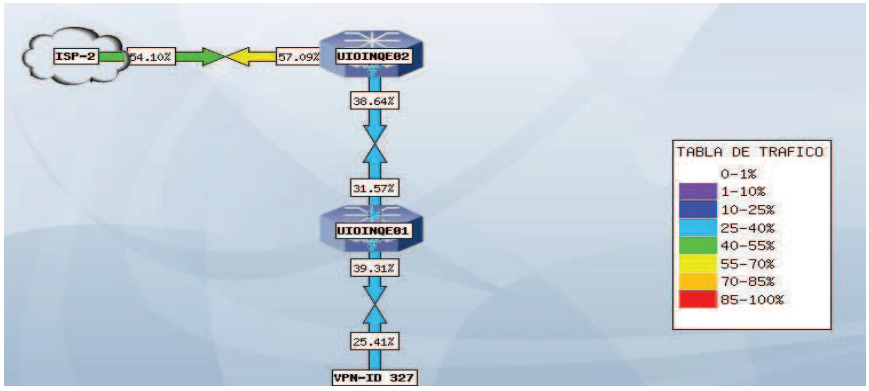




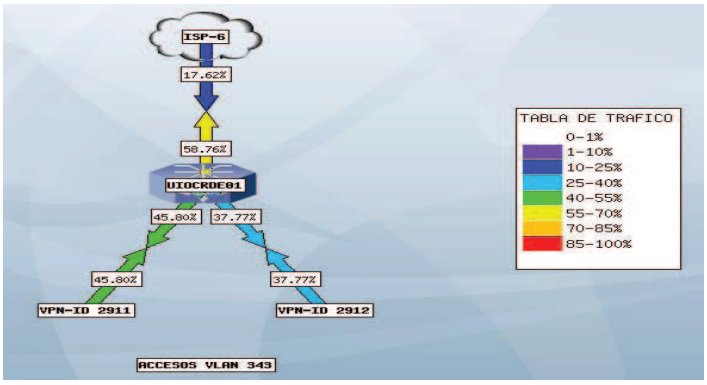


E.2 RESULTADOS FINALES OBTENIDOS CON CATI

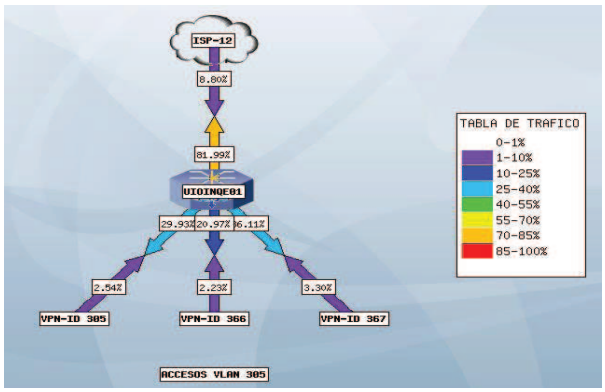
E.2.1 RESULTADOS FINALES CON CACTI PARA EL ISP-2



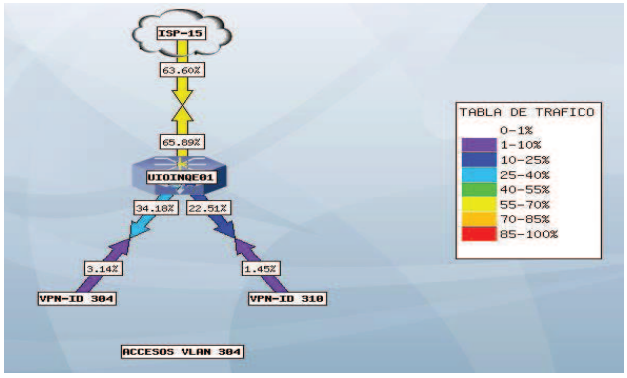
E.2.2 RESULTADOS FINALES CON CACTI PARA EL ISP-6



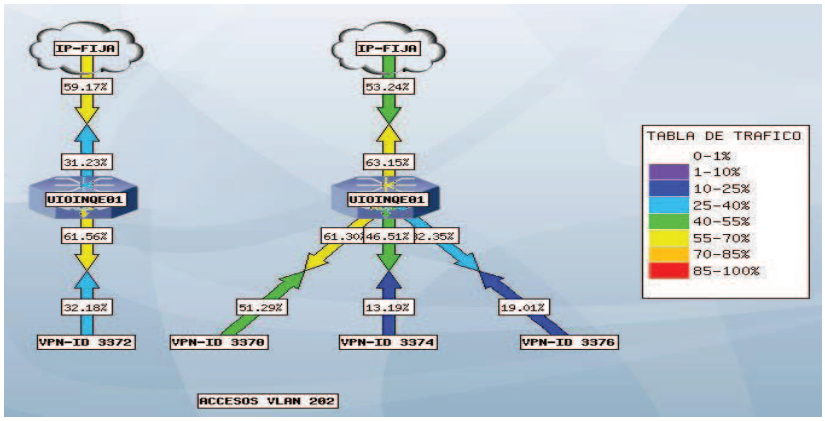
E.2.3 RESULTADOS FINALES CON CACTI PARA EL ISP-12



E.2.4 RESULTADOS FINALES CON CACTI PARA EL ISP-15



E.2.5 RESULTADOS FINALES CON CACTI PARA LA IP FIJA



E.3 RESULTADOS FINALES OBTENIDOS CON COMANDOS IOS

E.3.1 RESULTADOS FINALES CON COMANDOS IOS PARA EL ISP-2

- **Asociación de la VFI a la VLAN:**

UIOINQE01#show run interface vlan 327
interface Vlan327
description ### VPLS ISP-2 ###
mtu 1900
no ip address
xconnect vfi isp-2-dsl

end

- **Puertos por donde cruza la VLAN:**

UIOINQE01# show vlan all-port

VLAN	Name	Status	Ports
327	isp-2-dsl	active	Gi12/10, Gi12/24, Gi12/25 Gi12/35, Gi12/40, Gi12/41 Gi12/42, Gi12/43, Gi4/0/1

- **Descripción de Interfaz troncal:**

UIOINQE01# show interface g12/10 description

Interface	Status	Protocol	Description
Gi4/0/1	up	up	*** Link UIOINQE02***

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface g4/0/1
interface GigabitEthernet4/0/1
description *** TRONCAL ISP-2***
switchport
switchport trunk encapsulation dot1q
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 327,312,349,363,2923,3101,3102,3106
switchport mode trunk
switchport nonegotiate
speed nonegotiate
flowcontrol send off
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 327

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-2-dsl \VFI	172.168.0.10	327	UP
VFI	isp-2-dsl \VFI	172.168.0.14	327	UP
VFI	isp-2-dsl \VFI	172.168.0.26	327	UP
VFI	isp-2-dsl \VFI	172.168.0.28	327	UP
VFI	isp-2-dsl \VFI	172.168.0.30	327	UP
VFI	isp-2-dsl \VFI	172.168.0.32	327	UP
VFI	isp-2-dsl \VFI	172.168.0.34	327	UP
VFI	isp-2-dsl \VFI	172.168.0.36	327	UP
VFI	isp-2-dsl \VFI	172.168.0.38	327	UP
VFI	isp-2-dsl \VFI	172.168.0.40	327	UP
VFI	isp-2-dsl \VFI	172.168.0.42	327	UP

VFI	isp-2-dsl \VFI	172.168.0.44	327	UP
VFI	isp-2-dsl \VFI	172.168.0.46	327	UP
VFI	isp-2-dsl \VFI	172.168.0.48	327	UP
VFI	isp-2-dsl \VFI	172.168.0.50	327	UP
VFI	isp-2-dsl \VFI	172.168.0.52	327	UP
VFI	isp-2-dsl \VFI	172.168.0.54	327	UP
VFI	isp-2-dsl \VFI	172.168.0.56	327	UP
VFI	isp-2-dsl \VFI	172.168.0.60	327	UP
VFI	isp-2-dsl \VFI	172.168.0.61	327	UP
VFI	isp-2-dsl \VFI	172.168.0.62	327	UP
VFI	isp-2-dsl \VFI	172.168.0.63	327	UP
VFI	isp-2-dsl \VFI	172.168.0.64	327	UP
VFI	isp-2-dsl \VFI	172.168.0.67	327	UP
VFI	isp-2-dsl \VFI	172.168.0.69	327	UP
VFI	isp-2-dsl \VFI	172.168.0.70	327	UP
VFI	isp-2-dsl \VFI	172.168.0.72	327	UP
VFI	isp-2-dsl \VFI	172.168.0.73	327	UP
VFI	isp-2-dsl \VFI	172.168.0.74	327	UP
VFI	isp-2-dsl \VFI	172.168.0.93	327	UP
VFI	isp-2-dsl \VFI	172.198.100.11	327	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-2-dsl
l2 vfi isp-2-dsl manual

vpn id 327
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.72 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.62 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls

neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.198.100.11 encapsulation mpls no split horizon
neighbor 172.168.0.40 encapsulation mpls
neighbor 172.168.0.93 encapsulation mpls
neighbor 172.162.180.100 encapsulation mpls

- **Muestras de MAC aprendidas:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 327
MAC Entries for Vlan 327 :
Dynamic Address Count: 8
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 8
Total MAC Addresses Available: 98314

UIOINQE01#show mac-address-table count vlan 327
MAC Entries for Vlan 327 :
Dynamic Address Count: 8
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 8
Total MAC Addresses Available: 98304

# MUESTRAS	MACs APRENDIDAS I S P - 2									
MUESTRA 1	8	8	8	8	8	7	7	7	7	7
	7	7	7	7	7	7	7	8	8	8
	8	8	8	8	8	8	8	8	8	8
	8	8	8	8	8	8	8	8	8	8
MUESTRA 2	10	11	11	11	11	11	11	11	11	11
	10	10	10	10	10	10	10	10	10	10
	11	11	11	11	11	11	10	10	10	11
	11	11	11	10	11	10	10	10	10	11
MUESTRA 3	7	7	7	7	7	7	7	7	7	7
	7	7	7	7	7	7	7	7	7	7
	7	7	7	7	7	7	7	7	7	7
	7	7	7	7	7	7	7	7	7	7
MUESTRA 4	7	7	8	6	6	6	6	6	6	6
	6	6	6	6	6	6	7	7	7	7
	6	6	6	6	6	6	7	7	7	7
	8	8	8	8	8	8	8	8	8	8

E.3.2 RESULTADOS FINALES CON COMANDOS IOS PARA EL ISP-6

- **Asociación de la VFI a la VLAN 2911:**

UIOINQE01#show run interface vlan 2911
interface Vlan2911
description ### VPLS ISP-6 ZONA QUITO NORTE###
mtu 1900
no ip address
xconnect vfi isp-6-dsl
end

- **Asociación de la VFI a la VLAN 2912:**

UIOINQE01#show run interface vlan 2912
interface Vlan2912
description ### VPLS ISP-6 ZONA QUITO SUR, VALLES Y PROVIN###
mtu 1900
no ip address
xconnect vfi isp-6-dsl2
end

- **Puertos por donde cruzan las VLANs:**

UIOLCLE01# show vlan all-port
VLAN Name Status Ports
------- --------- ---------- -----------
2911 isp-6-dsl1active fa2/22
2912 isp-6-dsl2 active fa2/22

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface fa2/12 description
Interface Status Protocol Description
Fa2/22 up up *** TRONCAL ISP-6***

- **Configuración de la Interfaz troncal:**

UIOCRDE01#show run interface fa2/22
interface FastEthernet2/22
description *** TRONCAL ISP-6***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 371,539,1300-1304,1325,2208,2803,2804,2808,2809
switchport trunk allowed vlan add 2813,2819,2823,2824,2901-2915,2918-2923
switchport trunk allowed vlan add 2925-2928,2931-2937,2939-2949,2955,2961
switchport mode trunk
mtu 9216
spanning-tree bpdufilter enable
end

- **Estado de los equipos de acceso:**

UIOCRDE01#show mpls l2 vc 2911

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-6-dsl \VFI	172.161.110.100	343	UP
VFI	isp-6-dsl \VFI	172.164.30.100	343	UP
VFI	isp-6-dsl \VFI	172.165.60.100	343	UP
VFI	isp-6-dsl \VFI	172.167.10.100	343	UP

UIOCRDE01#show mpls l2 vc 2912

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-6-dsl2 \VFI	172.161.20.100	343	UP
VFI	isp-6-dsl2 \VFI	172.165.10.100	343	UP
VFI	isp-6-dsl2 \VFI	172.166.20.100	343	UP
VFI	isp-6-dsl2 \VFI	172.168.0.14	343	UP
VFI	isp-6-dsl2 \VFI	172.168.0.40	343	UP
VFI	isp-6-dsl2 \VFI	172.165.0.44	343	UP
VFI	isp-6-dsl2 \VFI	172.160.54.100	343	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

```
UIOCRDE01#show run | b l2 vfi isp-6-dsl
l2 vfi isp-6-dsl manual
l2 vfi manual
 vpn id 2911
 neighbor 172.161.110.100 encapsulation mpls
 neighbor 172.164.30.100 encapsulation mpls
 neighbor 172.165.60.100 encapsulation mpls
 neighbor 172.167.10.100 encapsulation mpls
```

```
UIOCRDE01#show run | b l2 vfi isp-6-dsl2
l2 vfi isp-6-dsl2 manual
l2 vfi manual
 vpn id 2912
 neighbor 172.161.20.100 encapsulation mpls
 neighbor 172.165.10.100 encapsulation mpls
 neighbor 172.166.20.100 encapsulation mpls
 neighbor 172.168.0.14 encapsulation mpls
 neighbor 172.168.0.40 encapsulation mpls
 neighbor 172.165.0.44 encapsulation mpls
 neighbor 172.160.54.100 encapsulation mpls
```

- **Muestras de MAC aprendidas VLAN 2911:**

Ejemplo de muestras Mac tomadas:

```
UIOCRDE01#show mac-address-table count vlan 2911
MAC Entries for Vlan 2911:
Dynamic Address Count:                10
```

Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 10
Total MAC Addresses Available: 65536

UIOCRDE01#show mac-address-table count vlan 2911
MAC Entries for Vlan 2911:
Dynamic Address Count: 11
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 11
Total MAC Addresses Available: 65536

- **Muestras de MAC aprendidas VLAN 2912:**

UIOCRDE01#show mac-address-table count vlan 2912
MAC Entries for Vlan 2912:
Dynamic Address Count: 12
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 12
Total MAC Addresses Available: 65536

UIOCRDE01#show mac-address-table count vlan 2912
MAC Entries for Vlan 2912:
Dynamic Address Count: 12
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 12
Total MAC Addresses Available: 65536

#MUESTRAS	MACs APRENDIDAS I S P - 6									
MUESTRA 1 2911	10	11	11	11	11	11	10	11	11	11
	10	11	11	11	11	10	10	10	10	10
	10	10	10	11	11	11	11	11	11	11
	11	11	11	11	11	10	10	10	10	11
MUESTRA 1 2912	9	9	8	8	8	8	8	8	8	9
	9	8	8	8	8	8	8	8	9	9
	8	9	9	8	8	9	8	8	8	8
	8	9	9	9	9	9	9	9	9	8
MUESTRA 2 2911	12	12	12	11	12	11	11	11	12	11
	12	12	12	12	12	12	11	11	11	11
	11	11	11	11	11	11	11	11	11	11
	11	11	12	12	12	12	12	12	12	12
MUESTRA 2 2912	7	6	6	6	7	7	7	7	7	7
	6	7	6	7	6	6	7	7	7	6
	6	7	6	7	8	8	8	8	8	8
	6	6	6	6	6	6	6	8	7	7

E.3.3 RESULTADOS FINALES CON COMANDOS IOS PARA EL ISP-12

- **Asociación de la VFI a la VLAN 305:**

UIOINQE011#show run interface vlan 305
interface Vlan305
description ### VPLS ISP-12 ZONA QUITO NORTE###
mtu 1900
no ip address
xconnect vfi isp-2-dsl1
end

- **Asociación de la VFI a la VLAN 366:**

UIOINQE011#show run interface vlan 366
interface Vlan366
description ### VPLS ISP-12 ZONA QUITO SUR###
mtu 1900
no ip address
xconnect vfi isp-2-dsl2
end

- **Asociación de la VFI a la VLAN 367:**

UIOINQE011#show run interface vlan 367
interface Vlan367
description ### VPLS ISP-12 ZONA VALLES Y PROVIN###
mtu 1900
no ip address
xconnect vfi isp-2-dsl3
end

- **Puertos por donde cruza las VLAN:**

UIOINQE011# show vlan all-port
VLAN Name Status Ports
---- -------------- --------- ---
305 isp-12-dsl1 active Gi5/24, Gi12/2, Gi12/10, Gi12/25, Gi12/35, Gi12/38, Gi12/40, Gi12/41, Gi12/42, Gi12/43, Gi13/2

366 isp-12-dsl2 activate Gi13/2
367 isp-12-dsl3 activate Gi13/2

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface g13/2 description
Interface Status Protocol Description
Gi13/2 up up *** TRONCAL ISP-12***

- **Configuración de la Interfaz troncal:**

UIOINQE01#show run interface g13/2
interface GigabitEthernet13/2
description *** TRONCAL ISP-12 ***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 305,366,367,376,1305,2910,3000,3111,3114,3127
switchport trunk allowed vlan add 3129-3132,3135-3139,3142,3148,3152,3164
switchport trunk allowed vlan add 3175-3177,3179,3180,3184,3186,3200,3232,3241
switchport trunk allowed vlan add 3243,3244,3251,3290,3301,3318,3320,3335,3341
switchport trunk allowed vlan add 3344,3737,3756,4076,4082,4085switchport mode trunk
end

- **Estado de los equipos de acceso:**

UIOINQE01#show mpls l2 vc 305

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-12-dsl1 \VFI	172.168.0.10	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.14	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.42	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.46	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.48	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.50	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.60	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.61	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.62	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.63	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.64	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.65	305	UP

VFI	isp-12-dsl1 \VFI	172.168.0.67	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.69	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.70	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.73	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.74	305	UP
VFI	isp-12-dsl1 \VFI	172.168.0.79	305	UP

UIOINQE01#show mpls l2 vc 366

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-12-dsl2 \VFI	172.168.0.28	305	UP
VFI	isp-12-dsl2 \VFI	172.168.0.30	305	UP
VFI	isp-12-dsl2 \VFI	172.168.0.32	305	UP
VFI	isp-12-dsl2 \VFI	172.168.0.36	305	UP
VFI	isp-12-dsl2 \VFI	172.168.0.56	305	UP

UIOINQE01#show mpls l2 vc 367

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-12-dsl3 \VFI	172.161.10.100	365	UP
VFI	isp-12-dsl3 \VFI	172.161.20.100	365	UP
VFI	isp-12-dsl3 \VFI	172.161.30.100	365	UP
VFI	isp-12-dsl3 \VFI	172.163.30.100	365	UP
VFI	isp-12-dsl3 \VFI	172.163.40.100	365	UP
VFI	isp-12-dsl3 \VFI	172.164.30.100	365	UP
VFI	isp-12-dsl3 \VFI	172.165.40.100	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.26	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.34	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.38	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.40	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.72	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.76	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.82	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.84	365	UP
VFI	isp-12-dsl3 \VFI	172.168.0.93	365	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-12-dsl1

l2 vfi isp-12-dsl manual

```
 vpn id 305
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.62 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls
neighbor 172.168.0.79 encapsulation mpls
```

UIOINQE01#show run | b l2 vfi isp-12-dsl2

```
l2 vfi isp-12-dsl2 manual
 vpn id 366
neighbor 172.168.0.28 encapsulation mpls
neighbor 172.168.0.30 encapsulation mpls
neighbor 172.168.0.32 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
```

UIOINQE01#show run | b l2 vfi isp-12-dsl3

```
l2 vfi isp-12-dsl3 manual
 vpn id 367

neighbor   172.161.10.100 encapsulation mpls
neighbor   172.161.20.100 encapsulation mpls
neighbor   172.161.30.100 encapsulation mpls
neighbor   172.163.30.100 encapsulation mpls
neighbor   172.163.40.100 encapsulation mpls
neighbor   172.164.30.100 encapsulation mpls
neighbor   172.165.40.100 encapsulation mpls
neighbor   172.168.0.26    encapsulation mpls
neighbor   172.168.0.34    encapsulation mpls
neighbor   172.168.0.38    encapsulation mpls
```

```
neighbor   172.168.0.40    encapsulation mpls
neighbor   172.168.0.72    encapsulation mpls
neighbor   172.168.0.76    encapsulation mpls
neighbor   172.168.0.82    encapsulation mpls
neighbor   172.168.0.84    encapsulation mpls
neighbor   172.168.0.93    encapsulation mpls
```

- **Muestras MAC VLAN 305:**

Ejemplo de muestras Mac tomadas:

```
UIOINQE01#show mac-address-table count vlan 305
MAC Entries for Vlan 305 :
Dynamic Address Count:                366
Static Address (User-defined) Count:  1
Total MAC Addresses In Use:           367
Total MAC Addresses Available:        98304

UIOINQE01#show mac-address-table count vlan 305
MAC Entries for Vlan 305 :
Dynamic Address Count:                366
Static Address (User-defined) Count:  1
Total MAC Addresses In Use:           367
Total MAC Addresses Available:        98304
```

- **Muestras MAC VLAN 366:**

Ejemplo de muestras Mac tomadas

```
UIOINQE01#show mac-address-table count vlan 366
MAC Entries for Vlan 366 :
Dynamic Address Count:                131
Static Address (User-defined) Count:  0
Total MAC Addresses In Use:           131
Total MAC Addresses Available:        98304


UIOINQE01#show mac-address-table count vlan 366
MAC Entries for Vlan 366:
Dynamic Address Count:                131
Static Address (User-defined) Count:  0
Total MAC Addresses In Use:           131
Total MAC Addresses Available:        98304
```

- **Muestras MAC VLAN 367:**

Ejemplo de muestras Mac tomadas

UIOINQE01#show mac-address-table count vlan 367
MAC Entries for Vlan 367:
Dynamic Address Count: 194
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 194
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 367
MAC Entries for Vlan 367:
Dynamic Address Count: 194
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 194
Total MAC Addresses Available: 98304

MUESTRA 1	MACs APRENDIDAS I S P - 12									
MUESTRA 1 305	107	107	107	107	107	107	104	106	100	108
	105	106	105	106	107	105	107	106	106	108
	107	107	107	107	106	106	105	105	105	105
	107	105	106	105	106	105	106	105	105	106
MUESTRA 1 366	121	121	121	121	121	121	121	121	121	121
	120	120	121	121	121	121	121	121	121	121
	121	121	120	120	121	121	120	120	120	120
	121	121	121	121	121	121	121	121	121	121
MUESTRA 1 367	94	93	92	91	92	94	94	90	93	94
	94	93	91	94	93	93	93	93	93	95
	93	93	91	94	92	92	92	90	93	96
	94	93	92	92	92	91	91	91	94	95

MUESTRA 2	MACs APRENDIDAS I S P - 12									
MUESTRA 2 305	106	106	107	107	106	107	105	106	110	108
	115	105	106	106	117	115	117	116	116	108
	108	108	108	105	106	104	107	108	110	106
	107	105	106	105	106	105	106	105	105	105
MUESTRA 2 366	122	121	121	121	122	122	120	121	121	122
	120	120	121	121	121	121	120	121	121	122
	121	120	120	120	120	121	120	121	122	120
	121	120	120	120	121	120	121	121	120	122
MUESTRA 2 367	94	92	92	91	92	94	94	90	93	94
	94	94	91	94	95	93	93	94	94	95
	93	93	91	95	92	92	92	90	93	95
	94	94	93	92	92	91	91	94	94	95

E.3.4 RESULTADOS FINALES CON COMANDOS IOS PARA EL ISP-15

- **Asociación de la VFI a la VLAN 304:**

UIOINQE01#show run interface vlan 304
interface Vlan304
description ### VPLS ISP-15 ZONA QUITO NORTE ###
mtu 1900
no ip address
xconnect vfi isp-15-dsl
end

- **Asociación de la VFI a la VLAN 310:**

UIOINQE01#show run interface vlan 310
interface Vlan310
description ### VPLS ISP-15 ZONA QUITO SUR, VALLES Y PROVIN ###
mtu 1900
no ip address
xconnect vfi isp-15-dsl2
end

- **Puertos por donde cruza la VLAN:**

UIOINQE01# show vlan all-port
VLAN Name Status Ports
---- ---------- --------- ----------
305 isp-15-dsl active Gi10/1, Gi12/25, Gi12/35, Gi12/41
Gi12/42, Gi12/43

Gi5/24, Gi10/1, Gi12/10, Gi12/25
310isp-15-dsl2 active Gi12/35, Gi12/40, Gi12/41, Gi12/42, Gi12/43

- **Descripción de Interfaz troncal:**

UIOINQE01#show interface g10/1 description
Interface Status Protocol Description
Gi10/1 up up *** TRONCAL ISP-15***

- **Configuración de la Interfaz troncal:**

interface GigabitEthernet10/1
description *** TRONCAL ISP-15***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 304,310,311,339,340,2043,2925,2963,3044,3333
switchport trunk allowed vlan add 3349-3352,3355,3736,3750,3752,3753,3755,3757
switchport trunk allowed vlan add 3774-3778,3791,3868,3893,3903,3907,3909,3911
switchport trunk allowed vlan add 3922,3942,3949,3963,3964,3966,3967,3978,3989
switchport trunk allowed vlan add 3991-3995
switchport mode trunk

- **Estado de los equipos de acceso:**

UIOLCLE01#show mpls l2 vc 304

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-15-dsl \VFI	172.168.0.10	304	UP
VFI	isp-15-dsl \VFI	172.168.0.14	304	UP
VFI	isp-15-dsl \VFI	172.168.0.42	304	UP
VFI	isp-15-dsl \VFI	172.168.0.44	304	UP
VFI	isp-15-dsl \VFI	172.168.0.46	304	UP

VFI	isp-15-dsl \VFI	172.168.0.48	304	UP
VFI	isp-15-dsl \VFI	172.168.0.50	304	UP
VFI	isp-15-dsl \VFI	172.168.0.52	304	UP
VFI	isp-15-dsl \VFI	172.168.0.54	304	UP
VFI	isp-15-dsl \VFI	172.168.0.60	304	UP
VFI	isp-15-dsl \VFI	172.168.0.61	304	UP
VFI	isp-15-dsl \VFI	172.168.0.62	304	UP
VFI	isp-15-dsl \VFI	172.168.0.63	304	UP
VFI	isp-15-dsl \VFI	172.168.0.64	304	UP
VFI	isp-15-dsl \VFI	172.168.0.67	304	UP
VFI	isp-15-dsl \VFI	172.168.0.69	304	UP
VFI	isp-15-dsl \VFI	172.168.0.70	304	UP
VFI	isp-15-dsl \VFI	172.168.0.73	304	UP
VFI	isp-15-dsl \VFI	172.168.0.74	304	UP

- **Estado de los equipos de acceso:**

UIOLCLE01#show mpls l2 vc 310

Local intf	Local circuit	Dest address	VC ID	Status
VFI	isp-15-dsl2 \VFI	172.1.172.100	310	UP
VFI	isp-15-dsl2 \VFI	172.1.20.100	310	UP
VFI	isp-15-dsl2 \VFI	172.1.30.100	310	UP
VFI	isp-15-dsl2 \VFI	172.2.172.100	310	UP
VFI	isp-15-dsl2 \VFI	172.2.20.100	310	UP
VFI	isp-15-dsl2 \VFI	172.20.100.10	310	UP
VFI	isp-15-dsl2 \VFI	172.3.172.100	310	UP
VFI	isp-15-dsl2 \VFI	172.3.20.100	310	UP
VFI	isp-15-dsl2 \VFI	172.3.30.100	310	UP
VFI	isp-15-dsl2 \VFI	172.3.40.100	310	UP
VFI	isp-15-dsl2 \VFI	172.4.30.100	310	UP
VFI	isp-15-dsl2 \VFI	172.5.40.100	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.26	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.28	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.30	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.32	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.34	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.36	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.38	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.40	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.44	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.56	310	UP

VFI	isp-15-dsl2 \VFI	172.168.0.76	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.78	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.82	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.84	310	UP
VFI	isp-15-dsl2 \VFI	172.168.0.93	310	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi isp-15-dsl
l2 vfi isp-15-dsl manual
vpn id 304
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.62 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.67 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls
neighbor 172.168.0.74 encapsulation mpls

UIOINQE01#show run | b l2 vfi isp-15-dsl2
l2 vfi isp-15-dsl2 manual
vpn id 310
neighbor 172.1.172.100 encapsulation mpls
neighbor 172.1.20.100 encapsulation mpls
neighbor 172.1.30.100 encapsulation mpls
neighbor 172.2.172.100 encapsulation mpls
neighbor 172.2.20.100 encapsulation mpls
neighbor 172.20.100.10 encapsulation mpls
neighbor 172.3.172.100 encapsulation mpls
neighbor 172.3.20.100 encapsulation mpls
neighbor 172.3.30.100 encapsulation mpls
neighbor 172.3.40.100 encapsulation mpls

```
neighbor 172.4.30.100  encapsulation mpls
neighbor 172.5.40.100  encapsulation mpls
neighbor 172.168.0.26  encapsulation mpls
neighbor 172.168.0.28  encapsulation mpls
neighbor 172.168.0.30  encapsulation mpls
neighbor 172.168.0.32  encapsulation mpls
neighbor 172.168.0.34  encapsulation mpls
neighbor 172.168.0.36  encapsulation mpls
neighbor 172.168.0.38  encapsulation mpls
neighbor 172.168.0.40  encapsulation mpls
neighbor 172.168.0.44  encapsulation mpls
neighbor 172.168.0.56  encapsulation mpls
neighbor 172.168.0.76  encapsulation mpls
neighbor 172.168.0.78  encapsulation mpls
neighbor 172.168.0.82  encapsulation mpls
neighbor 172.168.0.84  encapsulation mpls
neighbor 172.168.0.93  encapsulation mpls
```

- **Muestras de MAC aprendidas VLAN 304:**

Ejemplo de muestras Mac tomadas:

```
UIOINQE01#show mac-address-table count vlan 304
MAC Entries for Vlan 304:
Dynamic Address Count:                  81
Static Address (User-defined) Count:  0
Total MAC Addresses In Use:           81
Total MAC Addresses Available:        98304
```

```
UIOINQE01#show mac-address-table count vlan 304
MAC Entries for Vlan 304:
Dynamic Address Count:                  81
Static Address (User-defined) Count:  0
Total MAC Addresses In Use:           81
Total MAC Addresses Available:        98304
```

- **Muestras de MAC aprendidas VLAN 310:**

```
UIOINQE01#show mac-address-table count vlan 310
MAC Entries for Vlan 310 :
Dynamic Address Count:                  47
Static Address (User-defined) Count:  0
```

Total MAC Addresses In Use: 47
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 310
MAC Entries for Vlan 310 :
Dynamic Address Count: 47
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 47
Total MAC Addresses Available: 98304

E.3.5 RESULTADOS FINALES CON COMANDOS IOS PARA LA IP FIJA

- **Asociación de la VFI a las VLANs:**

UIOINQE01#show run interface vlan 3370
interface Vlan3370
description ### VPLS IP FIJA ZONA QUITO NORTE###
mtu 1900
no ip address
xconnect vfi ip-fija-dsl1
end

UIOINQE01#show run interface vlan 3372
interface Vlan3372
description ### VPLS IP FIJA ZONA QUITO SUR###
mtu 1900
no ip address
xconnect vfi ip-fija-dsl12
end

UIOINQE01#show run interface vlan 3374
interface Vlan3374
description ### VPLS IP FIJA ZONA PRONORTE###
mtu 1900
no ip address
xconnect vfi ip-fija-dsl3
end

UIOINQE01#show run interface vlan 3376
interface Vlan3376
description ### VPLS IP FIJA ZONA PRONSUR###
mtu 1900

```
no ip address
xconnect vfi ip-fija-dsl4
end
```

- **Puertos por donde cruzan las VLAN:**

```
UIOINQE01# show vlan all-port
VLAN    Name       Status          Ports
---- ----------- --------- --------  ----------
3370    ip-fija-dsl1    active          Gi12/8
3372    ip-fija-dsl2    active    Gi12/5
3374    ip-fija-dsl3    active          Gi12/8
3376    ip-fija-dsl4    active          Gi12/8
```

- **Descripción de las Interfaces troncales:**

```
UIOINQE01#show interface g12/8 description
Interface    Status      Protocol       Description
Gi12/8         up          up       *** Link UIOINQB01 G7/0/1***
Gi12/5         up          up       *** Link UIOINQB01 G4/0/1***
```

- **Configuración de la Interfaz tronca Gi12/8:**

```
interface GigabitEthernet12/8
description *** Link UIOINQB01 G7/0/1***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 202,206,3354,3370,3374-3397,3474-3497,3556
switchport mode trunk
switchport nonegotiate
speed nonegotiate
flowcontrol send off
```

Configuración de la Interfaz tronca Gi12/5:

```
interface GigabitEthernet12/5
description *** Link UIOINQB01 G4/0/1***
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 3372
switchport mode trunk
```

switchport nonegotiate
speed nonegotiate
flowcontrol send off

- **Estado de los equipos de acceso:**

UIONQE01#show mpls l2 vc 3370

Local intf	Local circuit	Dest address	VC ID	Status
VFI	ip-fija-dsl1 \VFI	172.168.0.34	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.36	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.38	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.4	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.42	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.44	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.46	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.48	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.50	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.52	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.54	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.56	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.60	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.61	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.62	202	UP
VFI	ip-fija-dsl1 \VFI	172.168.0.63	202	UP

UIONQE01#show mpls l2 vc 3372

Local intf	Local circuit	Dest address	VC ID	Status
VFI	ip-fija-dsl2 \VFI	172.168.0.10	202	UP
VFI	ip-fija-dsl2 \VFI	172.168.0.14	202	UP
VFI	ip-fija-dsl2 \VFI	172.168.0.26	202	UP
VFI	ip-fija-dsl2 \VFI	172.168.0.64	202	UP
VFI	ip-fija-dsl2 \VFI	172.168.0.65	202	UP
VFI	ip-fija-dsl2 \VFI	172.168.0.69	202	UP
VFI	ip-fija-dsl2 \VFI	172.168.0.70	202	UP
VFI	ip-fija-dsl2 \VFI	172.168.0.73	202	UP

UIONQE01#show mpls l2 vc 3374

Local intf	Local circuit	Dest address	VC ID	Status
VFI	ip-fija-dsl3 \VFI	172.161.10.100	202	UP
VFI	ip-fija-dsl3 \VFI	172.161.20.100	202	UP
VFI	ip-fija-dsl3 \VFI	172.161.30.100	202	UP

VFI	ip-fija-dsl3 \VFI	172.161.40.100	202	UP
VFI	ip-fija-dsl3 \VFI	172.161.10.100	202	UP
VFI	ip-fija-dsl3 \VFI	172.162.20.100	202	UP
VFI	ip-fija-dsl3 \VFI	172.163.10.100	202	UP
VFI	ip-fija-dsl3 \VFI	172.163.20.100	202	UP
VFI	ip-fija-dsl3 \VFI	172.163.30.100	202	UP
VFI	ip-fija-dsl3 \VFI	172.163.40.100	202	UP

UIONQE01#show mpls l2 vc 3376

Local intf	Local circuit	Dest address	VC ID	Status
VFI	ip-fija-ds4 \VFI	172.165.30.100	202	UP
VFI	ip-fija-dsl4 \VFI	172.176.165.100	202	UP

- **Encapsulación de los Pseudowires hacia los equipos PEs de acceso:**

UIOINQE01#show run | b l2 vfi ip-fija-dsl1
l2 vfi ip-fija-dsl1 manual
vpn id 3370
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.4 encapsulation mpls
neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.62 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls

UIOINQE01#show run | b l2 vfi ip-fija-dsl2
l2 vfi ip-fija-dsl2 manual
vpn id 3372
neighbor 172.168.0.34 encapsulation mpls
neighbor 172.168.0.36 encapsulation mpls
neighbor 172.168.0.38 encapsulation mpls
neighbor 172.168.0.4 encapsulation mpls

neighbor 172.168.0.42 encapsulation mpls
neighbor 172.168.0.44 encapsulation mpls
neighbor 172.168.0.46 encapsulation mpls
neighbor 172.168.0.48 encapsulation mpls
neighbor 172.168.0.50 encapsulation mpls
neighbor 172.168.0.52 encapsulation mpls
neighbor 172.168.0.54 encapsulation mpls
neighbor 172.168.0.56 encapsulation mpls
neighbor 172.168.0.60 encapsulation mpls
neighbor 172.168.0.61 encapsulation mpls
neighbor 172.168.0.62 encapsulation mpls
neighbor 172.168.0.63 encapsulation mpls

UIOINQE01#show run | b l2 vfi ip-fija-dsl3
l2 vfi ip-fija-dsl3 manual
vpn id 3374
neighbor 172.168.0.10 encapsulation mpls
neighbor 172.168.0.14 encapsulation mpls
neighbor 172.168.0.26 encapsulation mpls
neighbor 172.168.0.64 encapsulation mpls
neighbor 172.168.0.65 encapsulation mpls
neighbor 172.168.0.69 encapsulation mpls
neighbor 172.168.0.70 encapsulation mpls
neighbor 172.168.0.73 encapsulation mpls

UIOINQE01#show run | b l2 vfi ip-fija-dsl4
l2 vfi ip-fija-dsl4 manual
vpn id 3376
neighbor 172.165.30.100 encapsulation mpls
neighbor 172.176.165.100 encapsulation mpls

- **Muestras de MAC aprendidas VLAN 3370:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 3370
MAC Entries for Vlan 3370:
Dynamic Address Count: 1089
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 1089
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 3370

MAC Entries for Vlan 3370:
Dynamic Address Count: 1089
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 1089
Total MAC Addresses Available: 98304

- **Muestras de MAC aprendidas VLAN 3372:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 3372
MAC Entries for Vlan 3372:
Dynamic Address Count: 106
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 106
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 3372
MAC Entries for Vlan 3372:
Dynamic Address Count: 106
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 106
Total MAC Addresses Available: 98304

- **Muestras de MAC aprendidas VLAN 3374:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 3374
MAC Entries for Vlan 3374:
Dynamic Address Count: 44
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 44
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 3374
MAC Entries for Vlan 3374:
Dynamic Address Count: 44
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 44
Total MAC Addresses Available: 98304

- **Muestras de MAC aprendidas VLAN 3376:**

Ejemplo de muestras Mac tomadas:

UIOINQE01#show mac-address-table count vlan 3376
MAC Entries for Vlan 3376:
Dynamic Address Count: 61
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 61
Total MAC Addresses Available: 98304

UIOINQE01#show mac-address-table count vlan 3376
MAC Entries for Vlan 3376:
Dynamic Address Count: 61
Static Address (User-defined) Count: 0
Total MAC Addresses In Use: 61
Total MAC Addresses Available: 98304

# MUESTRA 1	MACs Aprendidas I P F I J A									
MUESTRA 3370	79	78	77	78	80	81	80	77	76	80
	77	77	78	79	77	78	78	79	77	76
	75	77	79	79	79	78	75	75	75	78
	75	77	79	78	78	79	75	75	75	78
MUESTRA 3372	106	106	106	106	106	106	106	107	107	107
	108	106	106	106	106	106	106	106	106	106
	106	106	106	106	106	106	106	106	106	106
	106	106	106	106	106	106	106	106	106	106
MUESTRA 3374	44	44	44	44	44	44	44	44	44	44
	44	44	44	44	44	44	44	44	44	44
	44	44	44	44	44	44	44	44	44	44
	44	44	44	44	44	44	44	44	44	44
MUESTRA 3376	61	61	61	61	61	61	61	61	61	61
	60	60	60	60	60	60	60	60	60	60
	61	61	61	61	61	61	61	61	61	61
	61	61	61	61	61	60	60	61	61	61

MUESTRA 2	MACs Aprendidas I P F I J A									
MUESTRA 3370	79	78	77	78	78	78	78	78	78	78
	78	77	78	79	77	78	78	79	77	76
	78	77	79	78	78	75	75	76	77	78
	79	77	79	78	78	79	78	79	77	78
MUESTRA 3372	106	106	106	106	106	101	101	101	101	105
	105	106	105	105	105	105	102	102	102	102
	102	105	106	105	106	106	102	102	102	102
	106	106	106	105	106	107	105	106	106	105
MUESTRA 3374	50	50	50	50	50	50	50	50	50	50
	50	50	50	50	50	50	50	50	50	50
	50	50	50	50	50	50	50	50	50	50
	50	50	50	50	50	50	50	50	51	51
MUESTRA 3376	62	62	62	62	62	62	62	62	62	62
	63	62	62	62	62	62	62	62	62	62
	61	62	62	62	62	62	62	62	62	62
	63	63	63	63	63	63	63	63	63	63

ANEXO F

FORMALIDAD DE ACEPTACIÓN DE RESULTADOS

F. 1 ASPECTOS GENERALES

F.1.1 OBJETIVO GENERAL

Verificar que el proyecto de titulación presentado por Mariuxi Gisselle Hidalgo Jumbo y Evelyn Patricia Montero Revelo cumple con el objetivo general planteado “Analizar y optimizar el servicio VPLS, que ofrece la CNT a sus clientes ISPs sobre su Red MPLS, para el planteamiento de alternativas de solución y mejores prácticas, y estudiar la escalabilidad del servicio usando la tecnología HVPLS”, y con los requerimientos del Área O&M Plataforma IP/MPLS.

F.1.2 DERECHOS DEL DOCUMENTO

El presente documento ha sido elaborado por quienes realizaron el presente proyecto de titulación, supervisado y evaluado por el Responsable de la red IP/MPLS de la CNT E.P.

F.2 PROCEDIMIENTO REALIZADO

F.2.1 DESCRIPCIÓN GENERAL

El proceso realizado para cumplir con el objetivo del proyecto de titulación se basó en el monitoreo de las VPLSs, para determinar los problemas que presentaban los ISPs seleccionados y para posteriormente aplicar la optimización al servicio de cada uno, presentando además un estudio de escalabilidad.

F.2.2 CUMPLIMIENTO DEL PROCESO

- Se diagnosticó la situación inicial de las VPLSs y se determinó los problemas que presentaban, haciendo uso de Wireshark, Cacti y comandos IOS de Cisco.

- Se planteó y aplicó soluciones para contrarrestar los problemas inicialmente encontrados con criterios para cada caso, entre esto segmentación de VLAN y migración de troncales.
- Se verificó el éxito de la solución mediante la comparación entre los resultados iniciales y finales de los ISPs que presentaron problemas.
- Como mejora al monitoreo de las VPLSs se implementó un servidor en la red interna de CNT E.P., con acceso remoto mediante la herramienta VNC (Virtual Network Control) permitiendo el uso de Wireshark. La figura F.1 presenta el esquema utilizado.

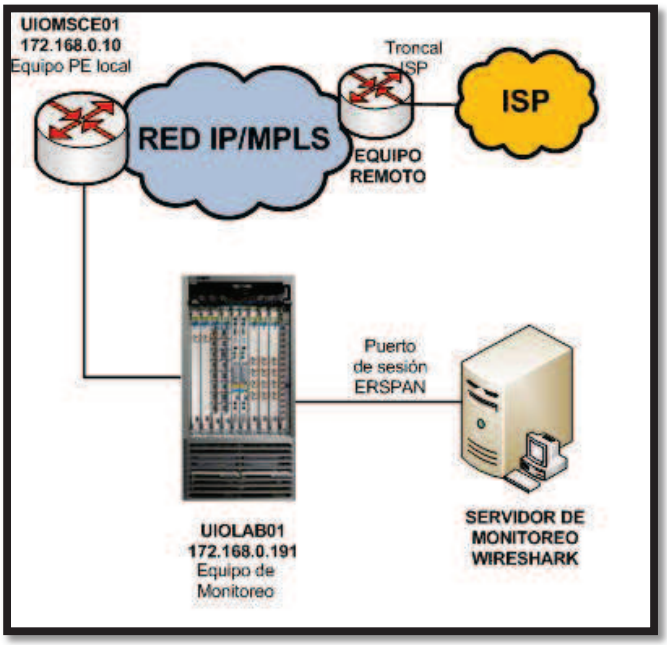


Figura F.1: Escenario utilizado para el monitoreo de tráfico con Wireshark

- Mediante Cacti se realizaron los diagramas respectivos de cada ISP con el fin de observar el tráfico cursado por la troncal y la VPLS, contribuyendo a un monitoreo constante.
- Se realizó la depuración a nivel de configuraciones de líneas de comando innecesarias, eliminando VPLSs inactivas y equipos de acceso DOWN de cada VPLS.

- Se realizó el estudio y prototipo de escalabilidad para el ISP-2 de manera exitosa y con planteamientos propuestos para un crecimiento topológico a futuro. La figura F.2 presenta el esquema utilizado.

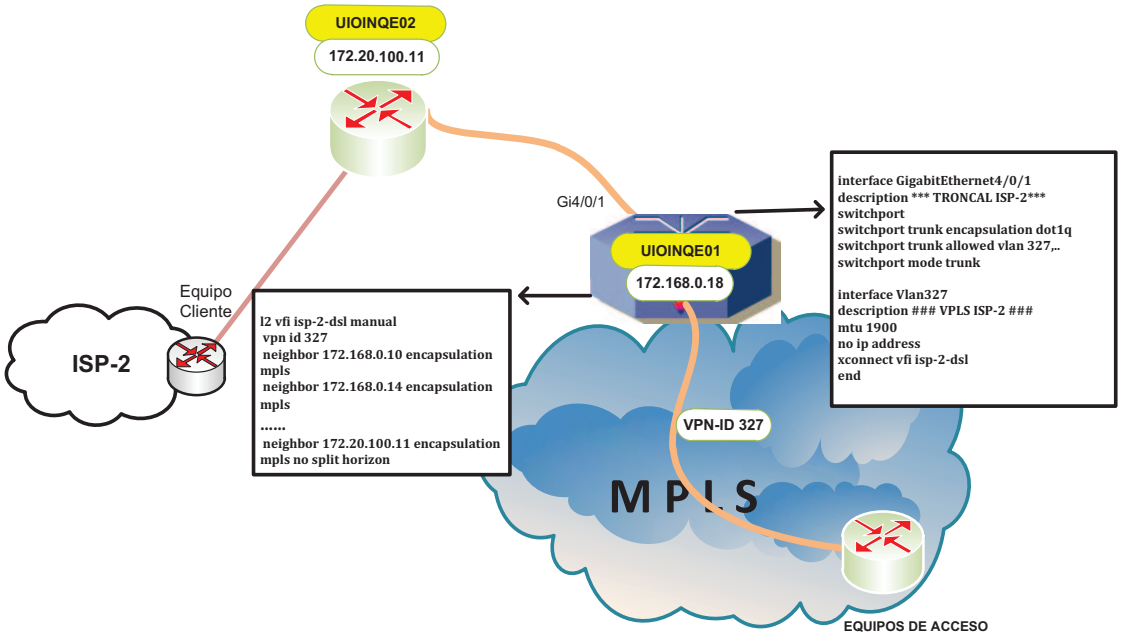


Figura F.2: Escenario utilizado para HVPLS en ISP-2

- Se presentó un manual de mejores prácticas referente al servicio VPLS para que pueda ser utilizado por el personal del Área O&M Plataforma IP/MPLS.

F.3 PRESENTACIÓN DE RESULTADOS

Las evaluaciones finales realizadas por el Responsable de la red IP/MPLS CNT E.P., deben tener como criterio CUMPLIÓ en la presentación de resultados de la tabla F.1; en la tabla F.2 se selecciona que ISPs presentaron problemas en su análisis inicial, a que ISPs se aplicó solución y a cuál de ellos se aplicó HVPLS.

OPTIMIZACIÓN Y ESCALABILIDAD DEL SERVICIO VPLS CNT E.P.			
PROCEDIMIENTO	**DESCRIPCIÓN**	**CUMPLIÓ**	**NO CUMPLIÓ**
SEGMENTACIÓN DE VLANs	Segmentación de las VPLSs de los ISPs con problemas, por número de usuarios con resultados exitosos.	✓	
DIMENSIONAMIENTO DE TRONCALES	Distribución de tráfico a diferentes puertos troncales, con resultados exitosos.	✓	
MONITOREO CON CACTI	Creación de diagramas de las VPLSs para monitoreo constante de tráfico.	✓	
DEPURACIÓN DE VPLSs	Transparencia y organización en la configuración del servicio de cada VPLS.	✓	
MONITOREO DE VPLSs CON ACCESO REMOTO	Servidor de acceso remoto VNC, sobre sistema operativo Linux Ubuntu 9.04, con Wireshark para realizar el monitoreo.	✓	
ESTUDIO DE ESCALABILIDAD	Estudio y prototipo de escalabilidad para el ISP-2 con resultados exitosos.	✓	

Tabla F.1: Cumplimiento de resultados

ISPs de estudio	Se detectó problemas	Se aplicó solución	HVPLS
ISP 1			
ISP 2	✓		✓
ISP 3			
ISP 4			
ISP 5			
ISP 6	✓	✓	
ISP 7			
ISP-8			
ISP-9			
ISP-10			
ISP-11			
ISP-12	✓	✓	
ISP-13			
ISP-14			
ISP-15	✓	✓	
ISP-16			
IP-FIJA	✓	✓	

Tabla F.2: Resumen de ISPs analizados

F.4 PROCEDIMIENTO DE ACEPTACIÓN

En su testimonio los responsables de llevar a cabo estas pruebas firman este documento como una aceptación de resultados.

Responsable de la red IP/MPLS CNT E.P.	Fecha	Firma
Ing. Andrés Almeida		

Responsables de la ejecución de la solución:	Fecha	Firma
Gisselle Hidalgo		
Evelyn Montero		

ANEXO G

COTIZACIONES DE EQUIPOS

G. 1 COTIZACIÓN ANDEAN TRADE

andean trade GROUP
www.andean-trade.com

OFERTA ECONÓMICA

CODIGO	DESCRIPCIÓN	CANT.	PU	TOTAL
	MARCA: CISCO			
CISCO7606-S	Cisco 7606-S Chassis	1	S/ -	S/ -
7606S-RSP720C-P	Cisco 7606S Chassis6-slotRSP720-3CPS	1	S/ 29.900,00	S/ 29.900,00
S76GI0-152040	Cisco 7600-RSP720 IOS IP SERVICES	1	S/ 3.986,67	S/ 3.986,67
RSP720-3C-GE	Cisco 7600 Route Switch Processor 720Gbps fabric PFC3C GE	1	S/ -	S/ -
2700W-AC/6	Dummy ID 2700 W AC Power Supply for 7606/7606-S	1	S/ -	S/ -
CAB-7513AC	AC POWER CORD NORTH AMERICA (110V)	2	S/ -	S/ -
PWR-2700-AC	2700W AC power supply for CISCO7606	1	S/ -	S/ -
PWR-2700-AC	2700W AC power supply for CISCO7606	1	S/ 2.392,00	S/ 2.392,00
FAN-MOD-6DHS	High Speed Fan Module for CISCO7606-S Chassis	1	S/ -	S/ -
CISCO7613-S	Cisco 7613-S Chassis	1	S/ -	S/ -
FAN-MOD-13DHS	High Speed Fan Module for CISCO7613-S Chassis	1	S/ -	S/ -
7613S-RSP720C-P	Cisco 7613S Chassis13-slotRSP720-3CPS	1	S/ 37.470,68	S/ 37.470,68
RSP720-3C-GE	Cisco 7600 Route Switch Processor 720Gbps fabric PFC3C GE	1	S/ -	S/ -
S76GI0K9-152040	Cisco 7600-RSP720 IOS IP SERVICES GSH	1	S/ 3.986,67	S/ 3.986,67
6000W-AC	6000 W AC Power Supply for Cisco 7609/7613	1	S/ 1.594,67	S/ 1.594,67
WS-CAC-6000W	Cat6500 6000W AC Power Supply	1	S/ -	S/ -
WS-CAC-6000W	Cat6500 6000W AC Power Supply	1	S/ 3.986,67	S/ 3.986,67
CAB-7513AC	AC POWER CORD NORTH AMERICA (110V)	4	S/ -	S/ -
ME-3600X-24TS-M	ME3600X Ethernet Access Switch 24 10/100/1000 + 2 10GE SFP+	1	S/ 7.172,01	S/ 7.172,01
S360XV9ST-152040	Cisco ME 360X SERIES IOS UNIVERSAL TAR	1	S/ -	S/ -
PWR-ME3KX-AC	ME3600X /ME3800X AC Power Supply	1	S/ 793,35	S/ 793,35
PWR-ME3KX-AC	ME3600X /ME3800X AC Power Supply	1	S/ 793,35	S/ 793,35
ME3600X-A	ME3600X Advanced Metro IP Access License	1	S/ 3.185,35	S/ 3.185,35
ME3600X-10G	ME3600X 10GE Upgrade License	1	S/ 2.388,01	S/ 2.388,01
CAB-AC-ME	AC power cord (North America)	2	S/ -	S/ -
	SUB TOTAL			S/ 97.649,41

Atentamente,

Irene Brito
Responsable
ANDEANTRADE

ISO 9001
icontec
SC 6828-1

G. 2 COTIZACIÓN TOTALTEK

TOTALTEK
tecnología y servicio

CISCO7606-S	Cisco 7606-S Chassis	1	$0.00	$0.00
S764AEK9-122330RE	Cisco 7600-RSP720 IOS ADVANCED ENTERPRISE SERVICES SSH	1	$10,781.25	$10,781.25
RSP720-3C-GE	Cisco 7600 Route Switch Processor 720Gbps fabric PFC3C GE	1	$0.00	$0.00
2700W-AC/6	Dummy ID 2700 W AC Power Supply for 7606/7606-S	1	$0.00	$0.00
7606S-RSP720C-P	Cisco 7606S Chassis6-slotRSP720-3CPS	1	$26,953.13	$26,953.13
CAB-7513AC	AC POWER CORD NORTH AMERICA (110V)	1	$0.00	$0.00
PWR-2700-AC	2700W AC power supply for CISCO7606	1	$0.00	$0.00
FAN-MOD-6SHS	High Speed Fan Module for CISCO7606-S Chassis	1	$0.00	$0.00
CONNECTOR-KIT	Connector Kit	1	$0.00	$0.00
CISCO7613-S	Cisco 7613-S Chassis	1	$0.00	$0.00
7613S-RSP720C-P	Cisco 7613S Chassis13-slotRSP720-3CPS	1	$33,777.66	$33,777.66
RSP720-3C-GE	Cisco 7600 Route Switch Processor 720Gbps fabric PFC3C GE	1	$0.00	$0.00
S764AEK9-122330RE	Cisco 7600-RSP720 IOS ADVANCED ENTERPRISE SERVICES SSH	1	$10,781.25	$10,781.25
3000W-AC	3000W AC Power Supply (select cable)	1	$0.00	$0.00
WS-CAC-3000W	Catalyst 6500 3000W AC power supply	1	$0.00	$0.00
CAB-7513AC	AC POWER CORD NORTH AMERICA (110V)	1	$0.00	$0.00
FAN-MOD-13SHS	High Speed Fan Module for CISCO7613-S Chassis	1	$0.00	$0.00
CONNECTOR-KIT	Connector Kit	1	$0.00	$0.00
ME-3600X-24TS-M	ME3600X Ethernet Access Switch 24 10/100/1000 + 2 10GE SFP+	1	$6,466.16	$6,466.16
S360XVT-152020	Cisco ME 360X SERIES IOS UNIVERSAL W/O CRYPTO TAR	1	$0.00	$0.00
CAB-ME-CON	Console Cable for ME Products	1	$0.00	$0.00
PWR-ME3KX-AC	ME3600X /ME3800X AC Power Supply	1	$715.16	$715.16
ME3600X-I	ME3600X Metro IP Access license	1	$0.00	$0.00
CAB-AC-ME	AC power cord (North America)	1	$0.00	$0.00
ME-FANTRAY	ME3600X/ME3800X Fan Tray	1	$0.00	$0.00
	SERVICIOS SMARNET			
CON-SNT-C7606S	CISCO7606-S	1	$0.00	$0.00
CON-SNT-7606RCP	7606S-RSP720C-P	1	$2,431.77	$2,431.77
CON-SNT-CISCO760	CISCO7613-S	1	$0.00	$0.00
CON-SNT-7613SRS7	7613S-RSP720C-P	1	$3,047.82	$3,047.82
CON-SNT-M36X24TS	ME-3600X-24TS-M	1	$595.83	$595.83

Subtotal	$95,509.02
12% IVA	$11,461.08
Total	$106,970.10

ANEXO H

MANUAL DE MEJORES PRÁCTICAS


CORPORACIÓN NACIONAL DE TELECOMUNICACIONES E.P.
MANUAL DE MEJORES PRÁCTICAS PARA EL SERVICIO
Configuraciones, Manejo y Seguridad
Realizado por: Gisselle Hidalgo y Evelyn Montero
2013
Área O&M Plataforma IP/MPLS de CNT E.P

CONTENIDO

INTRODUCCIÓN Y PRESENTACIÓN

Las VPNs (redes privadas virtuales) han evolucionado de forma imponente desde su introducción.

Al surgir las redes MPLS (Multiprotocol Label Switching/ Multiprotocolo de conmutación de etiquetas), la aceptación de los proveedores de servicio a las VPNs basadas en MPLS fue de gran magnitud ya que permiten ofrecer fácil suministro de servicios masivos a los usuarios.

Los diferentes tipos de VPN basadas en MPLS pueden clasificarse de distintas formas, VPNs en capa 3 y 2.

Actualmente la CNT E.P., es el principal proveedor de servicios de telecomunicaciones en el país, uno de los servicios que ofrece es el VPNs en capa 2 sobre su red IP/MPLS denominado VPLS (Virtual Private LAN Service/Servicio Virtual Privado LAN).

El Manual de Mejores Prácticas busca ser una guía para empresas vinculadas al servicio VPLS que deseen alcanzar la satisfacción de sus clientes, mediante la implementación de procedimientos orientados a mejorar el servicio.

Este manual se centra en los fundamentos de VPLS y H-VPLS (VPLS jerárquico), y está dirigido a los proveedores de servicios masivos con un core MPLS que requieran implementar esta solución y de manera puntual al personal del Área O&M Plataforma IP/MPLS de CNT E.P., teniendo como finalidad facilitarles un conjunto de mejores prácticas para el manejo del servicio VPLS.

Para lograr esto el presente manual proporciona pautas para configuración, manejo y seguridad del servicio VPLS, adicionalmente brinda conceptos básicos relacionados al servicio, éste documento ha sido extraído del proyecto de titulación denominado "ANÁLISIS Y OPTIMIZACIÓN DEL SERVICIO VIRTUAL LAN PRIVADO (VPLS), QUE OFRECE LA CNT EP A SUS CLIENTES ISPs SOBRE SU RED MPLS, Y ESTUDIO DE ESCALABILIDAD USANDO TECNOLOGÍA HVPLS".

Esperamos que los conceptos y herramientas brindadas en este Manual sean de utilidad para las empresas de telecomunicaciones que buscan exceder las expectativas de sus clientes.

OBJETIVO GENERAL

El objetivo general del presente documento es lograr que las empresas vinculadas al sector de las telecomunicaciones, conozcan del servicio VPLS y apliquen las mejores practicas para lograr un correcto funcionamiento del servicio.

1 CONOCER EL SERVICIO VPLS

1.1 ¿QUÉ ES EL SERVICIO VPLS?

VPLS se construye sobre la pila de protocolos MPLS, es un servicio que crea Redes Privadas sobre estructuras basadas en Ethernet, y emula toda la funcionalidad de una red de área local completa independiente de su localidad geográfica, sus siglas representan:

- "Virtual" implica una separación lógica del tráfico del cliente.
- "Privada" significa que existe un dominio de conmutación aislado.
- "LAN" se refiere a la Red de Área Local que consta de un solo dominio, por cliente.
- "Servicio" significa que el proveedor de servicio es quien asegura la prestación.

1.2 ¿COMO FUNCIONA EL SERVICIO?

- **ELEMENTOS QUE INTERVIENEN EN EL FUNCIONAMIENTO**

Una red VPLS está conformada por equipos PEs, equipos clientes CEs, Pseudowires y una instancia VPLS, como se indica en el figura 1.1.

Figura 1.1: Modelo de referencia VPLS

- **EQUIPO PE (PROVIDER EDGE ROUTER/ ENRUTADOR DE BORDE HACIA EL PROVEEDOR)**

Localizados en la frontera de la red MPLS, proporcionan al usuario la interface de acceso a la red.

- **EQUIPO CE (CUSTOMER EDGE/ ENRUTADOR DE BORDE HACIA EL CLIENTE)**

Situado en las instalaciones del cliente y conectado al Equipo PE, el circuito de conexión entre el CE y el PE es ethernet.

- **PSEUDOWIRE**

Circuito virtual que está formado por un par de LSPs unidireccionales punto-a-punto de un solo salto, uno en cada dirección, en la figura 1.2 se presenta el modelo de un pseudowire.

Figura 1.2: Modelo de un Pseudowire

- **INSTANCIA VPLS VFI (VIRTUAL FORWARDING INTERFACES/ INTERFAZ DE REENVÍO VIRTUAL)**

Las VFI se crean en los equipos PEs, es aquí en donde se aplican todas las decisiones de reenvío de cada VPLS.

- **FUNCIONAMIENTO**

El funcionamiento de VPLS está dado por la creación de una malla completa de túneles LSPs entre todos los equipos PEs que participan en el servicio sobre la red MPLS.
Se forma entonces una instancia VPLS y es identificada por un VFI-ID; cada par de PEs realiza una sesión dirigida, en la que se indica qué etiqueta

VC se usa para enviar paquetes hacia la VFI especifica, creándose así los respectivos pseudowires o conexiones virtuales.

El equipo CE primero encapsula el tráfico de capa 2 sobre Ethernet incluyendo la VLAN asociada a la VFI para luego ser enviadas al Router PE de borde.

Para cada trama entrante, el PE de borde retira la cabecera de acceso junto con el preámbulo, y posteriormente el PE selecciona el VC y el túnel LSP e inserta la etiqueta interior VC y la etiqueta del túnel MPLS. En el núcleo MPLS los paquetes son conmutados a través de etiquetas y son enviados hacia el PE de salida.

Cuando el PE de salida recibe el paquete, este retira la etiqueta de túnel e inspecciona la información de la etiqueta interna y de acuerdo a la tabla FIB que contiene todas las direcciones MAC y el identificador de las interfaces aprendidas, conoce la instancia VFI a la que la trama pertenece.

En la figura 1.3 se presenta la encapsulación de la trama en el transporte sobre la red MPLS.

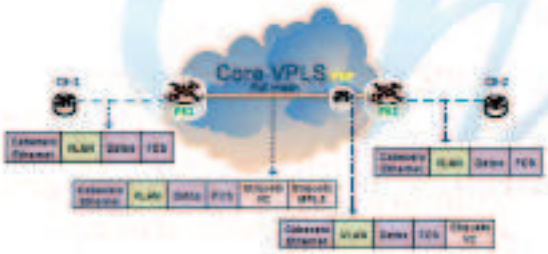


Figura 1.3: Encapsulación de la trama en la VPLS

Todos los enlaces de la misma región VPLS se definen como mesh, de forma que el tráfico que reciben los PEs, no se reenvía utilizando aquellos enlaces tipo mesh dentro de la VPLS ya que se aplicando la regla del horizonte dividido. Está regla indica que si un equipo recibe una trama por una interfaz, éste reenvía la trama por todas las interfaces que tiene conectadas excepto por la interfaz que recibió la trama.

2 CONOCER LOS REQUERIMIENTOS QUE TIENE PARA SER IMPLEMENTADO

2.1 ¿SOBRE QUÉ ARQUITECTURA DE RED FUNCIONA?

MPLS es una arquitectura especificada por la IETF, que trata sobre el encaminamiento, envío y conmutación de los flujos de tráfico a través de la red. Se basa en la conmutación de paquetes por medio de etiquetas de señalización previamente establecidas.

Dentro de las principales aplicaciones de una Red MPLS tenemos la implementación de redes privadas virtuales, las VPNs se construyen a base de conexiones realizadas sobre una infraestructura compartida.

Las VPNs de capa dos sobre MPLS denominadas VPLS necesitan de la infraestructura de MPLS para establecer su propio servicio.

2.2 ¿QUE EQUIPOS SOPORTAN EL SERVICIO?

- **Equipo PE**

El servicio VPLS al ser implementado sobre MPLS necesita de equipos PEs que trabajen bajo esta arquitectura y que soporten VPNs capa 2.

Una buena selección de los equipos se realiza de acuerdo a los requerimientos de la red del proveedor, los mínimos requeridos para el soportar VPNs capa 2 sobre MPLS son:

- Funcionalidad MPLS, con manejo de VPNs.
- Velocidad alcanzada mayor a 1Gbps.
- Soporte de fibra óptica monomodo y multimodo.
- Puertos Gigabit Ethernet autosensing 10/100/1000 Mbps.
- Soporte de protocolos en capa 2 como: VLAN Trunk Protocol (VTP), IEEE 802.1q.
- Soporte de protocolos en capa 3 como: OSPF, BGPv4.
- Soporte de protocolos de señalización como: RSVP, LDP.

A pesar que en el mercado actual existen varios marcas que ofrecen equipos que soportan MPLS y VPNs capa 2; por confiabilidad y criterios de estabilidad en la capa de core y distribución de la red deben utilizar equipos de la marca CISCO de la serie 7600 que se ajustan a las prestaciones del servicio.

2.8 ¿QUÉ TAMAÑO MÍNIMO DE MTU SE REQUIERE?

Para asegurar que no va a existir fragmentación de paquetes en la red, el tamaño del paquete en MPLS debe ser igual o menor que la trama de mayor tamaño a transportan en la red, este puede ser configurado dependiendo del tráfico cursado y así establecer el tamaño de los paquetes de manera eficiente, los requerimientos mínimos de MTU para evitar fragmentación se definen a continuación:

MTU-IP: 1500 bytes (Valor estándar)
Cabecera Ethernet y FCS: 18 bytes
Etiqueta VLAN: 4 bytes
2 Etiquetas MPLS (Tunel +VC): 8 bytes

El tamaño total de la trama para uso específico de VPLS es: 1530 bytes

1530 bytes

La infraestructura de cada proveedor depende de los servicios que ofrezca, por lo tanto no se tiene definido un valor máximo de MTU ya que cada equipo interno puede añadir cabeceras de diferentes tamaños, se ha definido teóricamente que el valor mínimo de MTU para las VPLSs es de 1530 bytes, de tal manera se recomienda utilizar un valor mayor a este para evitar problemas de fragmentación.

3 REALIZAR UNA CORRECTA ADMINISTRACIÓN Y CONFIGURACIÓN

3.1 ¿CÓMO SE PUEDE REALIZAR UNA CORRECTA ADMINISTRACIÓN?

Se debe conocer los principales comandos para poder realizar una revisión de la configuración, se cita algunos ejemplos:

- Para indicar los puertos por donde cruza la VLAN. Se puede obtener la descripción de cada uno e identificar cual es la troncal del cliente.

Router#show vlan all-port

- Para identificar los neighboors conectados vía Pseudowire o Spoke en la VPLS específica y si están activos o no.

Router#show vfi "nombre-vpls"

- Para indentificar el tipo de encapsulación del túnel y las propiedades del pseudowire usado para emular el circuito virtual de los neighboors conectados.

Router#show run | begin l2 vfi "nombre-vpls"

- Para indicar la tabla de MAC aprendida asociada a la vlan. Se puede verificar si la VLAN está en uso cuando se tenga como resultado MACs aprendidas.

Router#show mac-address-table vlan vlan-id

- Para indicar las MACs aprendidas de cada VLAN. Se puede determinar si existe variación de MACs.

Router#show mac-address-table count vlan vlan-id

- Para verificar que la sesión dirigida LDP este funcionando. Su salida indica los pseudowires creados para el transporte de tramas de capa 2

a través de la red troncal MPLS su principal función es identificar el estado del Pseudo wire ya sea activo o desactivo. Si se omite el vc-id se despliega todos los VC creados en el equipo.

Router#show mpls l2 vc vc-id

- Para verificar por cada equipo de acceso el estado del VC, la interfaz de salida hacia el PE remoto, la etiqueta local y remota, el tamaño del MTU y la descripción de la interfaz troncal de la VPLS.

Router#show mpls l2 vc vc-id detail

3.2 ¿COMO SE REALIZA LA CONFIGURACIÓN EN EL EQUIPO PE?

Se debe realizar los siguientes pasos de configuración:

Paso 1. Configurar la interfaz conectada al dispositivo CE.

En este paso se configura las interfaces en el router PE conectadas al equipo CE del cliente, ver tabla 3.1.

	Comando	Propósito
Paso 1	Router(config)#interface[tipo] [modulo/interfaz.subinterfaz] Router(config-if)# switchport	Configurar la interfaz hacia el cliente como un switchport.
Paso 2	Router(config-if)# switchport trunk encapsulation dot1q	Configurar la interfaz para usar encapsulamiento dot1q
Paso 3	Router(config-if)# switchport trunk allowed vlan [vlan-id]	Asignar una o lista de vlan permitidas.

Tabla 3.1: Configuración hacia el equipo CE, basado en 802.1Q .

Paso 2. Definir la VFI y la asociacion de la interfaz conectada al equipo CE.

En este paso se configura la VFI, despues de definirla se asocia a uno o más circuitos de conexión (interfaces, subinterfaces, o circuitos virtuales). El vfi especifica el ID de la VPN de una instancia VPLS, las direcciones de otros PE en esta ámbito y el tipo de señalización del túnel y la encapsulación de cada neighboor asociado a la misma instancia, ver tabla 3.2.

	Comando	Propósito
Paso	Router(config)# l2 vfi [vfi-name] manual	Configuración de la instancia VPLS.
Paso	Router(config-vfi)# vpn [vpn-id]	Especificación del identificador VPN-ID para la VFI.
Paso	Router(config-vfi)#neighbor [remote-PE-loopback] encapsulation mpls	Especificación de los Router vecinos o de acceso a la VPLS

Tabla 3.2: Configuración de la VFI y Pseudowires.

Nota: En la actualidad, el modo manual es la única opción disponible para la provisión de múltiples puntos VFI.

- Asociación del circuito de conexión con la VFI, ver tabla 3.3.

	Comando	Propósito
Paso 1	Router(config)#interface vlan [vlan-id]	Se ingresa la configuración de la VLAN
Paso 2	Router(config)#xconnect vfi [vfi-name]	Se asocia la interfaz VLAN con la VFI.

Tabla 3.3: Asociación de la VFI a la VLAN .

Nota: Se debe tener una VFI configurada para que el comando sea aceptado.

3.3 ¿QUE PERSONAL DEBE ESTAR CAPACITADO?

La capacitación debe ir dirigida al perfeccionamiento técnico del trabajador para que éste se desempeñe eficientemente en las funciones a él asignadas. Se plantean las siguientes tips:

Tip #1: La capacitación del personal debe ir dirigida al personal que esté de alguna forma involucrado en

el manejo del servicio VPLS con temas que aborden en su totalidad la funcionabilidad del mismo.

Tip #2: La capacitación debe incluir la parte práctica, como por ejemplo la realización de laboratorios en donde el personal pueda interactuar con equipos y de tal manera que pueda observar de una forma más apegada a la realidad el comportamiento del servicio.

Tip #3: La capacitación debe ser en grupos pequeños ya que la resolución de dudas o inquietudes será más eficaz.

Tip #4: Se debe realizar una capacitación de manera frecuente, debido a que las Telecomunicaciones están en constante evolución.

Tip # 5: Se debe capacitar al personal sobre el proceder ético en el entorno de trabajo de acuerdo a los reglamento de la empresa.

4 GARANTIZAR UN ALTO RENDIMIENTO Y DISPONIBILIDAD

4.1 ¿COMO SE GARANTIZA UN ALTO RENDIMIENTO?

Se debe garantizar que los equipos participantes del servicio, no ocupen sus recursos de una manera innecesaria.

Las VPLS al emular una red LAN extendida tiende a ser vulnerable a los problemas que presenta tener un único dominio de difusión.

El problema principal radica en dominios de difusión de gran tamaño pueden llegar a producir tormentas de broadcast y ocupar recursos de procesamiento mayores a los equipos.

- **Segmentación de VLANs como solución a grandes dominios de broadcast**

Este método hace uso de múltiples VFIs (Interfaz Virtual de Envío) en lugar de utilizar una sola VFI para la malla completa de pseudowires, por lo que la carga de replicación de origen se reduce de acuerdo al número de VFI creadas, además el utilizar múltiples VFI como se indica en la figura 5.1, permite mitigar el requisito de aprendizaje MAC y el dominio de broadcast es reducido ya que hay menos usuarios.

Figura 4.1: Únicos VFI vs. Múltiplec VFI

- **Configuración de la segmentación de VLANs**

Paso 1. Configurar la interfaz conectada al dispositivo CE.

	Comando	Propósito
Paso 1	Router(config)#interface[tipo] [modulo/interfaz.subinterfaz] Router(config-if)# switchport	Configurar la interfaz hacia el cliente como un switchport.
Paso 2	Router(config-if)# switchport trunk encapsulation dot1q	Configurar la interfaz para usar encapsulamiento dot1q.
Paso 3	Router(config-if)# switchport trunk allowed vlan [vlan-id]	Asignar una o lista de vlan permitidas.

Tabla 4.1: Configuración hacia el equipo CE, basado en 802.1Q .

Paso 2. Definir la VFI y la asociacion de la interfaz conectada al equipo CE.

	Comando	Propósito
Paso	Router(config)# l2 vfi [vfi-name] manual	Configuración de la instancia VPLS.
Paso	Router(config-vfi)# vpn [vpn-id]	Especificación del identificador VPN-ID para la VFI.
Paso	Router(config-vfi)#neighbor [remote-PE-loopback] encapsulation mpls	Especificación de los Router vecinos o de acceso a la VPLS

Tabla 4.2: Configuración de la VFI y Pseudowires.

Paso 3: Asociar la VFI con la VLAN.

	Comando	Propósito
Paso 1	Router(config)#interface vlan [vlan-id]	Ingresamos a la configuración de la vlan creada para la segmentación
Paso 2	Router(config)#xconnect vfi [vfi-name]	Conectamos la VFI a la interfaz VLAN, la VLAN estará asociada a la VFI de la VLAN de acceso.

Tabla 4.3: Asociación de la VFI a la VLAN

4.2 ¿COMO SE GARANTIZA UNA ALTA DISPONIBILIDAD?

Ante la falla de algún equipo PE o la caída de un enlace de conexión, se debe planificar un esquema de redundancia para garantizar que el servicio cumpla la disponibilidad de acuerdo a los parámetros SLA establecidos del proveedor.

En VPLS se pueden planificar los siguientes esquemas de redundancia.

- Redundancia de Pseudowires y conexión al CE

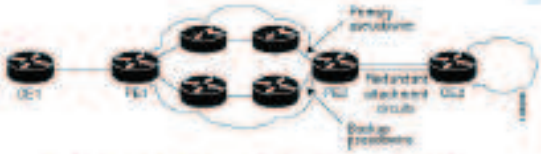


Figura 4.2: Redundancia de Pseudowires y VC

- Redundancia de Pseudowires, conexión al CE y equipo CE

Figura 4.3: Redundancia de Pseudowires, VC y CE routers

- Redundancia de Pseudowires, conexión al CE, equipo CE y equipo PE

Figura 4.5: Redundancia de Pseudowires, VC, CE routers y PE routers

5 CONSIDERAR CRITERIOS DE CRECIMIENTO Y PLANIFICAR ALTERNATIVAS DE ESCALABILIDAD

La tecnología VPLS ha logrado desplegar la prestación de servicios a través de una red basada en Ethernet de una manera fiable y flexible, sin embargo requiere de mejoras a niveles de operaciones sobre todo cuando se lleva esta tecnología a gran escala.

La escalabilidad para cualquier tipo de servicio o tecnología puede ser vista desde diferentes perspectivas y lograr el resultado requerido. Para el caso puntual del servicio VPLS se considera como criterio de escalabilidad el crecimiento de la red a nivel topológico y de usuarios.

5.1 ¿QUE IMPLICA UN CRECIMIENTO TOPOLÓGICO?

Si es necesario incluir un equipo PE ya sea para agregar un nuevo sitio a una instancia o incluir una nueva VPLS, los equipos PEs tiene que actualizar todas las tablas de los PEs asociados a la misma, trayendo consigo una nueva replicación de paquetes, provocando una carga en el plano de datos y en el plano de control debido a la detección automática del nuevo punto, y la complejidad de mallado completo de LSP entre los PEs participantes, como se indica en la figura 5.1.

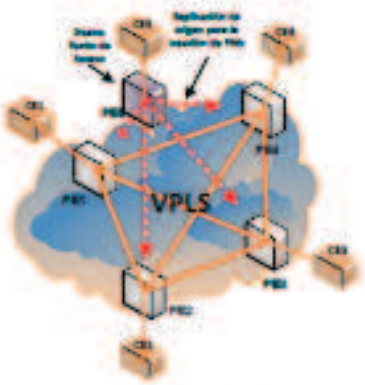


Figura 6. 1: Nuevo punto VPLS.

6.2 ¿QUÉ IMPLICA UN CRECIMIENTO DE USUARIOS?

Cada ISPs cliente puede crecer a nivel corporativo representando un incremento de número de usuarios a su red.

El crecimiento de usuarios en las VPLS implica un mayor tamaño en sus dominios de difusión, el tener grandes cantidades de usuarios en un mismo PE implica que la replicación de paquetes se realice hacia todos ellos, creando una sobrecarga de señalización en el equipo PE.

6.3 ¿QUÉ SE PUEDE APLICAR COMO ESCALABILIDAD ANTE CRECIMIENTO TOPOLÓGICO?

El servicio jerárquico denominado H-VPLS se construye sobre las bases de la solución VPLS. Esta arquitectura define niveles de jerarquía donde se define una región central o Core, a la cual se conectan las regiones de nivel inferior.

HVPLS trata de solucionar el crecimiento topológico del servicio VPLS, creando nuevos puntos de replicación fuera del mallado VPLS, de tal manera que minimiza la cantidad de replicaciones de entrada necesarias para el transporte de tráfico.

HVPLS utiliza un nodo como N-PE y otro como U-PE; al ser la conexión de estos dos puntos de tipo spoke la regla del "horizonte dividido" no se aplica, de tal manera que el tráfico recibido de la región VPLS será reenviado únicamente al equipo U-PE, como lo indica la figura 5.2.

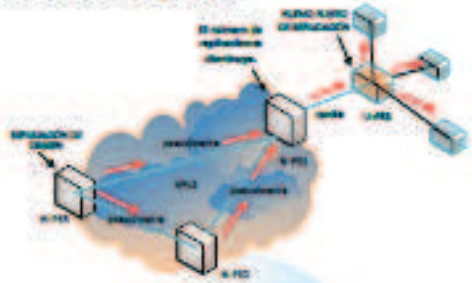


Figura 6. 2: Creación de nuevo punto de replicación

Si HVPLS añade un nuevo dispositivo U-PE este requiere la configuración del router N-PE local al que se conecta, pero no requiere señalización alguna con otros routers N-PE o dispositivos U-PE, ya que el mallado original VPLS se mantiene como muestra en la figura 5.3.

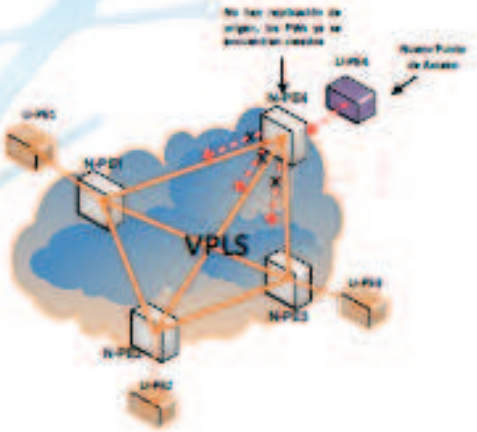


Figura 6. 3: Nuevo punto de acceso en HVPLS

- **CONFIGURACIÓN DE HVPLS**

Para HVPLS se especifica las configuraciones en los equipos que dividen los 2 niveles, para el Acceso QinQ y para el acceso MPLS (EoMPLS).

- **ACCESO QinQ**

Configuración Equipo N-PE

Paso 1: Se crea la VLAN, ver tabla 5.1.

	Comando	Propósito
Paso 1	Router # configure terminal	Ingresar al modo de configuración global.
Paso 2	Router(config)# vlan vlan-id	Crear la VLAN a la que se asociara la interfaz conectada al CE.

Tabla 5.1: Creación VLAN - QinQ .

Paso 2: Configurar la interfaz conectada al dispositivo U-PE, ver tabla 5.2.

	Comando	Propósito
Paso 1	Router(config)#interface[tipo] [modulo/interfaz.subinterfaz] Router(config-if)# switchport	Ingresar a la interfaz hacia el U-PE y configurarla como switchport.
Paso 2	Router(config-if)# switchport mode trunk	Configurar el switch port como modo trunk.
Paso 3	Router(config-if)# switchport trunk encapsulation dot1q	Configurar la interfaz para usar encapsulamiento dot1q.
Paso 4	Router(config-if)# switchport trunk allowed vlan vlan-id	Asignar una o lista de vlan permitidas.

Tabla 5.2: Configuración de interfaz conectada al dispositivo U-PE - QinQ.

Paso 3: Asociacion del circuito de conexion con la VFI, ver tabla 5.3.

	Comando	Propósito
Paso 1	Router(config)#interface vlan vlan-id	Ingresamos a la configuración de la vlan
Paso 2	Router(config)#xconnect vfi vfi-name	Conectamos la VFI a la interfaz VLAN.

Tabla 5.3: Asociación de la VFI a la VLAN.

Configuración Equipo U-PE

Paso 1: Configurar la interfaz conectada al dispositivo CE, ver tabla 5.4.

	Comando	Propósito
Paso 1	Router(config)#interface[tipo] [modulo/interfaz.subinterfaz] Router(config-if)# switchport	Ingresar a la interfaz hacia dispositivo CE y configurarla como switchport.
Paso 2	Router(config-if)# switchport mode access	Configurar el switch port como modo acceso.
Paso 3	Router(config-if)# switchport access vlan vlan-id	Asignar el interfaz a un dominio que está representado por la VLAN.
Paso 4	Router(config-if)# switchport mode dot1q-tunnel	Configurar la interfaz para usar encapsulamiento dot1q.
Paso 5	Router(config-if)# switchport trunk allowed vlan vlan-id	Asignar una o lista de vlan permitidas.

Tabla 5.4: Configuración de interfaz conectada al dispositivo CE - QinQ.

Paso 2: Configurar la interfaz conectada al dispositivo N-PE, ver tabla 5.5.

	Comando	Propósito
Paso 1	Router(config)#interface[tipo] [modulo/interfaz.subinterfaz] Router(config-if)# switchport	Ingresar a la interfaz hacia dispositivo N-PE y configurarla como switchport.
Paso 2	Router(config-if)# switchport mode trunk	Configurar el switch port como modo trunk.
Paso 3	Router(config-if)# switchport allowed vlan vlan-id	Asignar una o lista de vlan permitidas.

Tabla 5.5: Configuración de interfaz conectada al dispositivo N-PE - QinQ.

- **ACCESO EoMPLS**

Configuración Equipo N-PE

Paso 1: Configurar la interfaz conectada al dispositivo U-PE, ver tabla 5.6.

	Comando	Propósito
Paso 1	Router(config)#interface[tipo] Router(config-if)# no switchport	Ingresar a la interfaz hacia dispositivo U-PE y configurarla como no switchport.
Paso 2	Router(config-subif)#ip address ip-address	Asigna una dirección IP a la interfaz.
Paso 3	Router(config-if)# mpls ip	Configurar mpls.

Tabla 5.6: Configuración de interfaz conectada al dispositivo U-PE – EoMPLS.

Paso 2: . Definir la VFI y la asociacion de la interfaz conectada al equipo U-PE, ver tabla 5.7.

	Comando	Propósito
Paso 1	Router(config)# l2 vfi vfi-name manual	Crear la vfi multipunto con interconexión a los PE remotos de forma manual.
Paso 2	Router(config-vfi)# vpn vpn-id	Configura el ID de la VPN para la VFI.
Paso 3	Router(config-vfi)#neighbor remote-PE-loopback encapsulation mpls	Especifica la ID del router remoto y la encapsulacion del pseudowire.
Paso 4	Router(config-vfi)#neighbor remote-PE-loopback encapsulation mpls no split horizon	Asegura que el trafico pase aldesde del U-PE

Tabla 5.7: Configuración de la VFI y Pseudowires – EoMPLS.

Configuración Equipo U-PE

Paso 1: Configurar la interfaz conectada al dispositivo CE, ver tabla 5.8.

	Comando	Propósito
Paso 1	Router(config)#interface[tipo] [módulo/interfaz.subinterfaz] Router(config-if)# switchport	Ingresar a la interfaz hacia dispositivo CE y configurarla como switchport.
Paso 2	Router(config-if)# switchport mode access	Configurar el switch port como modo acceso.
Paso 3	Router(config-if)# switchport access vlan *vlan-id*	Asignar el interfaz a un dominio que esta representado por la VLAN.

Tabla 5.8: Configuración de interfaz conectada al dispositivo CE.

Paso 2: Configurar la interfaz de vlan, ver tabla 5.9.

	Comando	Propósito
Paso 1	Router(config)#interface vlan vlan-id	Ingresar a la configuración de la Vlan.
Paso 2	Router(config)#xconnect local vpn-ip encapsulation mpls	

Tabla 5.9: Configuración de la interfaz de la VLAN – EoMPLS

Paso 3: Configurar la interfaz conectada al dispositivo N-PE, ver tabla 5.10.

	Comando	Propósito
Paso 1	Router(config)#interface[tipo] Router(config-if)# no switchport	Ingresar a la interfaz hacia dispositivo U-PE y configurarla como no switchport.
Paso 2	Router(config-subif)#ip address ip-address	Asigna una dirección IP a la interfaz.
Paso 3	Router(config-if)# mpls ip	Configurar mpls.

Tabla 5.10: Configuración de interfaz conectada al dispositivo N-PE – EoMPLS

5.4 ¿QUÉ SE PUEDE APLICAR COMO ESCALABILIDAD ANTE CRECIMIENTO DE USUARIOS?

Una solución frente al gran crecimiento de usuarios que implica un dominio de broadcast muy grandes es la segmentación de la VPLS en VLANs, esta segmentación depende de los criterios del administrador en los que se debe tomar en cuenta todos los parámetros relacionados al servicio.

6 PROTEGER LA RED Y APLICAR POLÍTICAS DE SEGURIDAD

6.1 ¿CÓMO SE PUEDE PROTEGER LA RED Y QUÉ POLÍTICAS SE PUEDE APLICAR?

En base al análisis de seguridad en las VPLS se plantean las siguientes recomendaciones:

- **Ocultamiento de la infraestructura de la red IP/MPLS**

Es imprescindible que los equipos de la red IP/MPLS del proveedor de servicio se oculte de las redes de clientes y de la red Internet. Para lograr el ocultamiento se establece direccionamiento IP privado sobre los equipos PE y P, de esta forma estos equipos se ocultan de Internet permitiendo aislar los posibles ataques con este origen.

- **Reducir al mínimo y asegurar el acceso a los equipo PE**

Limitar el acceso a los dispositivos dentro del alcance del control de la entidad operativa, es decir los clientes no tienen acceso a los equipo PE y desde el equipo PE no se tiene acceso al equipo CE, para esto se puede realizar lo siguiente:

- ✓ Definir y aplicar las ACL para acceso remoto.
- ✓ Utilizar servidores AAA centralizados para controlar el acceso.
- ✓ Proteger el acceso a los puertos de consola y auxiliar
- ✓ Uso de SSH para el acceso remoto.
- ✓ Limitar el acceso SNMP a servidores específicos a través de ACL.
- ✓ Facilitar el acceso de solo lectura y solo SNMP.
- ✓ Implementar DMZ usando IDS y firewalls para proteger las redes contra intrusiones.
- ✓ Usar MD5 para la LDP en el núcleo.
- ✓ Configuración de contraseñas de acceso al equipo.

- **Abstenerse de utilizar VLAN 1 para llevar todo el tráfico de datos**

- **Habilitación de comandos para minimizar impacto de ataque a los equipos**

Los siguientes comandos permiten mejorar las respuestas de equipo (para su administración) en caso de un ataque basado en inundación de tráfico, mientras que los TCP keepalives permiten prevenir sesiones truncadas en caso de desconexiones repentinas. Comandos a aplicar:

- ✓ scheduler allocate
- ✓ service tcp-keepalives-in
- ✓ service tcp-keepalives-out

- **Habilitación de traps**

Habilitación de traps generados por eventos o cambios de configuración en los equipos.

- ✓ loggin traps
- ✓ logging event link-status default
- ✓ snmp-server enable traps vtp
- ✓ snmp-server enable traps vlancreate
- ✓ snmp-server enable traps vlandelete
- ✓ snmp-server enable traps envmon
- ✓ snmp-server enable traps stackwise
- ✓ snmp-server enable traps config
- ✓ snmp-server enable traps hsrp
- ✓ snmp-server enable traps ipmulticast

- **Prevención frente a ataques de equipo cliente**

El administrador de red de cada entidad cliente debe garantizar que en su red se mantengan establecidas las políticas necesarias de seguridad que limiten al máximo cualquier ataque que se puede generar a nivel interno o externo.

7 GLOSARIO

ACL: Lista de reglas para determinar los permisos de acceso en equipos de redes.

ADMINISTRADOR DE RED: Posición laboral en las que los ingenieros se ven involucrados en redes de computadoras, o sea, las personas que se encargan de la administración de la red.

ATAQUES A LA SEGURIDAD: Se produce cuando un atacante utiliza vulnerabilidades y fallos en la seguridad a diferentes niveles, para intentar comprometer la seguridad de una red.

BGP: (Border Gateway Protocol/ Protocolo de Borde) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

BYTE: Es una unidad de información utilizada como un múltiplo del bit. Equivale a 8 bits.

CE: Equipo cliente en la red MPLS.

CONMUTADOR: Dispositivo analógico de lógica de interconexión de redes de computadoras.

CONMUTACIÓN: Establecimiento, por parte de una red de comunicaciones, de un intercambio de bloques de información (o "paquetes") con un tamaño específico entre dos puntos, un emisor y un receptor.

CORE: Núcleo de red encargado de proporcionar conectividad entre los distintos puntos de acceso y que permite enlazar diferentes servicios.

DIRECCIÓN MAC: Control de acceso al medio, es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red, conocido también como dirección física.

DMZ: (Demilitarized zone/Zona Desmilitarizada) es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet; su objetivo es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa.

DOMINIO DE BROADCAST: Área lógica en una red de ordenadores en la que cualquier ordenador conectado a la red puede transmitir directamente a cualquier otro en el dominio sin precisar ningún dispositivo de encaminamiento.

ENCAPSULACIÓN: Mecanismo que consiste en organizar datos y métodos de una estructura, evitando el acceso a datos por cualquier otro medio distinto a los especificados.

EoMPLS: Ethernet sobre MPLS, ofrece servicios de determinación de rutas en grandes redes.

ESCALABILIDAD: Capacidad de mejorar recursos para ofrecer una mejora (idealmente) lineal en la capacidad de servicio.

ETHERNET: Conocido como estándar IEEE 802.3, es un estándar de transmisión de datos para redes de área local.

ETIQUETA: Conocido como tag, es una palabra clave asignada a un dato almacenado en un repositorio.

FCS: Es un conjunto de bits adjuntos al final de la trama Ethernet utilizado para verificar la integridad de la información recibida mediante una "secuencia" de verificación de trama incorrecta, también conocido como CRC o checksum.

FIB: Tabla de Información de Envío, contiene una lista de rutas ordenadas para una búsqueda más óptima. Esta tabla además contiene el siguiente salto (next-hop).

FIREWALL: Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

HORIZONTE DIVIDIDO: Es una técnica de enrutamiento el cual evita que la información acerca de las rutas salga por la interfaz del Router a través de cual se recibió dicha información.

VPLS: (Virtual Private LAN Service/Servicio de LAN privada virtual) es una forma de proporcionar Ethernet multipunto a multipunto basado en la comunicación sobre redes IP / MPLS. Permite sitios dispersos geográficamente compartir un dominio de difusión Ethernet.

H-VPLS: (Hierarchical VPLS/VPLS Jerárquica), es una forma de proporcionar Ethernet multipunto a multipunto basado en la comunicación sobre redes IP / MPLS de manera jerárquica.

IDS: Sistema de detección de intrusos usado para detectar accesos no autorizados a un computador o a una red.

IEE 802.1q: Conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas.

IETF: (Internet Engineering Task Force/Fuerza de Tareas de Ingeniería de Internet), es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

INTERNET: Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

CISCO IOS: Software utilizado en la gran mayoría de routers (encaminadores) y switches (conmutadores) de Cisco Systems.

IP: Protocolo de Internet para comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI.

IPSEC: Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

LAN: Red de área local, es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada.

LDP: Es un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.

LSP: Label Switched Path, es el intercambio de rutas por etiqueta, una ruta sobre una red MPLS.

MD5: Es un algoritmo de generación de firmas. Un hash es una cadena de letras y números que resulta del cálculo sobre una cadena de origen.

MESH: Una red mesh es una red múltiplemente unida, en la cual los nodos tienen más de una conexión con más de un nodo diferente. No necesariamente deben conectarse todos contra todos, este es un caso especial que se denomina full-mesh, mientras que el caso genérico suele denominarse partial-mesh, por oposición

MPLS: (MultiProtocol Label Switching/ Multiprotocolo de envío de etiquetas) es una tecnología que usa etiquetas para hacer decisiones de reenvío de tráfico.

MTU: (Maximum Transfer Unit/Unidad Máxima de Transferencia) expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones.

NEIGHBOORS: (Vecinos) router o switches que están conectados localmente a un equipo.

N-PE: (Network- Provider Edge Router/ Router del Proveedor de Red) es el dispositivo de nivel superior, el cual está conectado en base a una malla completa VPLS con los otros dispositivos N-PE que participan en el servicio.

OSPF: (Open Shortest Path First/ El camino más corto primero) protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link State Algorithm) para calcular la ruta más corta posible. Usa cost como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona.

PAYLOAD: (área de datos) contiene los datos que se desean trasladar.

PE: (Provider Edge Router/ Enrutador de Borde hacia el Proveedor), equipo ubicado en el borde de la red MPLS para desempeñar las funciones tradicionales de encaminamiento y proporcionar conectividad a sus usuarios.

POLÍTICAS DE SEGURIDAD: Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de .

PREÁMBULO: Primer campo de la trama Ethernet indica el inicio de la trama y tienen el objeto de que el dispositivo que lo recibe detecte una nueva trama y se sincronice.

PROTOCOLO: Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

PSEUDOWIRE: Circuito virtual que está formado por un par de LSPs unidireccionales punto-a-punto de un solo salto, uno en cada dirección

QinQ: Estándar 802.1ad (Provider Bridges/ Puentes de red de Proveedores) de red ethernet, que permite incluir varias cabeceras de Vlan en un trama ethernet.

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI (modelo de interconexión de sistemas abiertos/open system interconnection). Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra.

RSVP: (Resource Reservation Protocol/ Protocolo de reserva de recursos) protocolo de la capa de transporte diseñado para reservar los canales o rutas en redes internet para la transmisión por unidifusión y multidifusión con escalabilidad y robustez

SEÑALIZACIÓN: Comunicación que se da entre los equipos de telecomunicaciones, entre centros de procesamiento, entre la central y el abonado o entre bloques de software, para el establecimiento y liberación de las llamadas, o para intercambiar información de gestión, tarificación, mantenimiento, etc.

Servidor AAA: El servidor AAA valida a los usuarios que intentan acceder a la infraestructura de networking de la institución, consultando la base de datos de usuarios, si el usuario no es encontrado o la contraseña es incorrecta, el servidor rechaza la petición de acceso del usuario, y no le permite hacer uso de los recursos ofrecidos en la institución.

SNMP: (Simple Network Management Protocol/ Protocolo Simple de Administración de Red o SNMP) protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

SPOKE: En la arquitectura Hub and Spoke es el dispositivo de usuario final que se conecta a través de spoke-pseudowires a un equipo central denominado Hub.

SSH: (Secure Shell / Intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

TIPS: Sugerencia o recomendación.

TRÁFICO: Cantidad de datos enviados y recibidos dentro de una red.

TRAMA: Unidad de medida de la información en la capa de enlace del modelo OSI, que no es más que la segmentación de los datos trasladándolos por medio de paquetes.

TRIPLE PLAY: Empaquetamiento de servicios y contenidos audiovisuales (voz, banda ancha y televisión).

TRONCAL: Puerto de gran capacidad utilizado para interconectar varios clientes.

TUNEL MPLS: Es un camino MPLS (para cierto tráfico o FEC) establecido entre puntos extremos, formado por LSP unidireccionales.

U-PE: User PE / PE DE USUARIO (U-PE): Es el dispositivo de nivel inferior que se conecta directamente al dispositivo cliente CE y tiene una conexión única al dispositivo correspondiente de la red Troncal MPLS. VC

VC: (Virtual Circuit/ Circuito Virtual)sistema de comunicación por el cual los datos de un usuario origen pueden ser transmitidos a otro usuario destino a través de más de un circuito de comunicaciones real durante un cierto periodo de tiempo, pero en el que la conmutación es transparente para el usuario.

VFI: (Virtual Forwarding Interfaces/ Interfaz de Reenvío Virtual) se crean en los equipos PEs, es aquí en donde se aplican todas las decisiones de reenvío de cada VPLS.

VLAN: Virtual LAN Network/Red de área local virtual) es un método de crear redes lógicamente independientes dentro de una misma red física.

VPN: (Virtual Private Network/ Red Virtual Privada), es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

WAN: (Wide Area Network/ Red de área amplia) es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente o cualquier red en la cual no estén en un mismo edificio todos sus miembros.

8 BIBLIOGRAFÍA

- "L2VPN Pseudowire Redundancy" http://www.cisco.com/en/US/docs/ios/wan/configconfiguide/wan_l2vpn_pw_red_external_docbdoc_D90De4b1805e9066_4container_external_ddocbas_090De4b1814cdd7c.html
- http://integrared.blogspot.com/2009/06/mejores-practicas-en-configuraciones-de.html
- http://www.cisco.com/en/US/products/ps6648/products_ios_protocol_option_home.html
- CLERCQ J, WITTERS J, SUNIL K, Tutorial Técnico VPLS, Revista de Telecomunicaciones de Alcatel, 2004.
- Tesis: ANÁLISIS Y OPTIMIZACIÓN DEL SERVICIO VIRTUAL LAN PRIVADO (VPLS), QUE OFRECE LA CNT EP A SUS CLIENTES ISPs SOBRE SU RED MPLS, Y ESTUDIO DE ESCALABILIDAD USANDO TECNOLOGÍA HVPLS.