UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA MECÁNICA ELECTRÓNICA Y AMBIENTAL

CARRERA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"DISEÑO E IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL REDUNDANTE USANDO BGP Y GLBP PARA LA COMPAÑÍA DELOSI"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

CHOQUEHUANCA PALOMINO, YOLVI ALEX

Villa El Salvador
2016

Dedicatoria

A mis padres
Naseancino Choquehuanca y
Norma Palomino

Agradecimiento

.

Quiero agradecer a Dios por tener a mi lado a las personas que hicieron posible que conclúyase los estudios en la universidad y por darme todas esas bonitas y satisfactorias experiencias.

A mis padres, hermanas y hermano, por darme esa confianza única y ser partícipes en mi crecimiento profesional.

Al Magister Fredy Campos, por su apoyo en la realización de este proyecto de ingeniería.

A mis amigos de la carrera, porque una de las mejores experiencias que tuve fue compartir el compañerismo y camaradería en la universidad.

Por último, a todas las personas que en algún momento han ayudado de una u otra manera a que logre este objetivo de ser profesional.

Índice

Lista de figuras

Lista de tablas

Introducción

El presente trabajo de investigación se denomina: “Diseño e implementación de una red privada virtual redundante usando BGP y GLBP para la compañía “Delosi” para optar el título de Ingeniero Electrónico y Telecomunicaciones.

En el mundo empresarial actual, el compartir información es un punto esencial para su crecimiento y debido a eso, desde hace mucho tiempo se estandarizaron tecnologías que suplieran esas necesidades como son las líneas arrendadas que se utilizaban para interconectar sedes de una compañía pero que fueron siendo reemplazadas por tecnologías como VPN junto con protocolos como BGP sobre medios compartidos que no tienen las desventajas de las líneas arrendadas,

Este proyecto está enfocado a implementar un servicio de RPV que pueda proveer interconexión de una oficina remota a su sede principal y con la posibilidad de establecer niveles de Clases de Servicio (CoS) junto con un protocolo ideal para este tipo de servicios como BGP junto con el protocolo GLBP para aumentar la disponibilidad de la red y el balanceo de carga.

La estructura que hemos seguido en este proyecto se compone de tres capítulos. El primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico y el tercer capítulo corresponde al desarrollo del proyecto.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

Las líneas arrendadas línea privada local (LPL) proporcionan capacidad dedicada permanente y se utilizan mucho para armar redes WAN. Son la conexión tradicional de preferencia, pero presentan una serie de desventajas. Una desventaja es que los clientes pagan por líneas arrendadas con una capacidad fija. Sin embargo, el tráfico WAN suele variar, y parte de la capacidad queda sin utilizar. Además, la capacidad de crecimiento es limitada en cuando a número de sedes a comunicar, cada terminal necesita una interfaz física individual en el router lo que disminuye la capacidad de convergencia de servicios por lo que se plantea es implementar una red privada virtual. También existen problemas de disponibilidad debido a que solo existe un solo enlace hacia la nube SDH y que será mejorada con el protocolo GLBP.

1.1 Descripción de la Realidad Problemática

"Delosi" es un grupo empresarial que opera once (11) marcas, muchas de ellas de renombre internacional. Las franquicias a su cargo en el Perú son Starbucks, Pinkberry, Chili's, KFC, Pizza Hut, Burger King, y la franquicia donde se realizará las mejoras es KFC localizado en avenida Pardo, y cual se dedicada a la comercialización de comidas rápidas, en el desarrollo de este proyecto se mencionará solo la compañía que la engloba.

Conociendo la realidad en cuanto a los objetivos de optimización de servicios que posee la compañía "Delosi" que repercute en su productividad. Esta empresa posee servicios como de telefonía analógica independiente, con otra infraestructura y equipos que las de la red de datos , por otro lado los datafonos también conocidos como maquinas pos que posee comparten el ancho de banda con el tráfico de otras operaciones pudiendo realizarse transacciones sin garantías de reenvió, El tráfico de la red de "Delosi" se transporta por un servicio llamado LPL (línea privada local)administrado por un proveedor de servicios, este servicio se usa para conectar la sede remota con la principal y una desventajas, en este servicio es que la capacidad de convergencia de servicios es escaso en comparación con la propuesta a implementar, esto debido a que el servicio LPL es una línea dedicada basada en tecnología SDH (tecnología digital) donde al cliente se le proporciona todo el ancho de banda disponible en el medio como una fibra óptica para conectar la sede remota a principal y donde el proveedor de servicios tiene poco control, haciendo muy difícil implementar otros servicios

sobre la misma infraestructura como adicionar servicios de telefonía IP como troncales SIP o telefonía analógica, servicios de internet optimizado para los clientes de delosi, toda esto repercute no solo en la capacidad de producción. También, el hecho de tener una administración de un solo equipo aliviana la labor de los proveedores. Además, cada terminal necesita una interfaz física individual en el router para que pueda conectarse a otras sedes lo cual afecta lo objetivos económicos ya que cada dispositivo es arrendado por el proveedor, también cuando la demanda de ancho de banda se incrementa el aumento se hace en escalas de tecnologías digital como son de E1 a E2.o E3 y no posee la granularidad intermedia, Para ello se implementará un servicio de VPN. Adicional al problema ya mencionado se suma el hecho de que “Delosi” solo tiene un enlace hacia el proveedor de servicios específicamente hacia el POP Alcanfores, lo que lo hace vulnerable a posibles cortes de servicios por lo que resulta también necesario implementar redundancia

1.2 Justificación del problema

El propósito de implementar este proyecto de telecomunicaciones beneficiara a la compañía “Delosi” en la productividad debido a que los servicios son mejor administrada. En la conexión remota a su sede principal puede realizarse fácilmente el aumento de capacidad de ancho de banda de forma remota ya que se utiliza interfaces Ethernet cuya capacidad están en el orden de los 100Mbps. Este proyecto permite obtener la convergencia de servicios sobre

misma infraestructura (mismo router, línea de fibra, recurso en el switch de agregación), para tener acceso a los servidores MasterCard y VISA mediante la VRF del POS y a su vez tener acceso a los servidores de la sede principal de "Delosi" mediante otro circuito (VPN), como consecuencia de ello se mejora las características de escalabilidad y crecimiento de la red. Además se incrementara la disponibilidad del servicio vía el enlace redundante utilizando el protocolo GLBP, esto asegura la continuidad en el proceso de ventas.

1.3 Delimitación de la investigación.

Este proyecto comprende el diseño e implementación solo en la sede remota dado que la red corre que está conformado por los router MPLS (P y PE) ya están preparados por el proveedor y listos para soportar la VPN. Adicionalmente para validar nuestro diseño se simulara la red del proveedor de forma básica mediante la herramienta GNS3.

1.3.1 Teórica

Comprende las redes privadas virtuales basadas en MPLS con BGP y disponibilidad basada en GLBP para LAN

1.3.2 Espacial:

Desde la sede remota de la compañía "Delosi" al punto de presencia (POP) del proveedor de servicios CLARO.

1.3.3 Temporal:

Comprende el periodo JUNIO 2016 A JULIO 2016

1.4 Formulación de problema

¿Se podría diseñar e implementar una red privada virtual usando BGP y GLBP?

1.4.1 Problemas específicos

PE1. ¿Cómo se podría diseñar una red privada virtual redundante usando BGP y GLBP?

PE2. ¿Cómo implementar una red privada virtual redundante usando BGP y GLBP?

1.5 Objetivos

Diseñar e Implementar una red privada virtual con redundancia usando BGP y GLBP.

1.5.1 Objetivos específicos

OE1. Diseñar una red privada virtual redundante usando BGP y GLBP

OE.2 Implementar una red privada virtual redundante usando BGP y GLBP

.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes

A lo largo de la investigación, se encontraron varias tesis que sirvieron de ayuda para el presente trabajo, entre ellas están:

Damián, R. (2008) "*Transmisión de voz, video y datos en redes privadas virtuales VPN/MPLS*". Este estudio surge porque se necesita analizar el impacto de su implementación, medir los beneficios y desventajas de esta evolución. *El modelo de diseño de redes VPN/MPLS es necesario para comprender como esta tecnología puede ser implementada sobre casos reales de transmisión de voz y datos.*

También se obtuvo aporte del presente trabajo: Junior B. (2014) "Propuesta de migración hacia una red MPLS para la empresa consumibles ", Quien concluye que la interconexión de redes constituye una tendencia fuerte en el manejo de transporte de información, debido a que los requerimientos de los usuarios son más complejos día a día y varían rápidamente. Las soluciones de

interconexión deben ser cada vez más cómodas y fáciles de implementar. Las VPN ofrecen una alternativa en este aspecto debido a su flexibilidad y a la filosofía con la que han sido creadas.

Por ultimo también se tomó como base el siguiente trabajo: Ricardo A. (2012) *"Estudio e implementación de una solución MPLS-VPN sobre múltiples sistemas autónomos"*. En el que realizó la propuesta técnica en la cual se describe el escenario general al que se enfrenta un proveedor de servicio para brindar servicios VPN a grandes distancias. Se logró elaborar un plan de trabajo que permita lograr la conectividad de extremo a extremo y aprovechar los beneficios que este tipo de redes ofrece.

2.2 Base teórica

2.2.1. MPLS

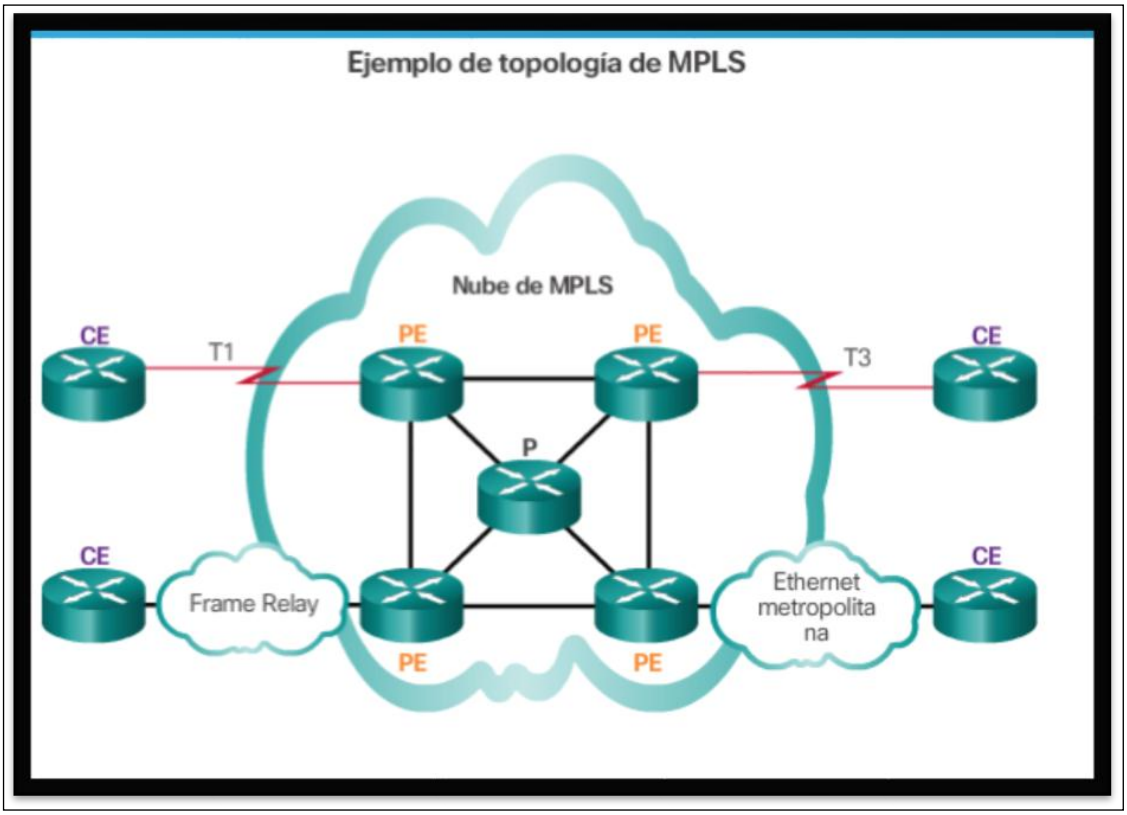
Según Netacad Cisco Systems (2016) la define como una tecnología WAN multiprotocolo de alto rendimiento que envía los datos de un router al siguiente según las etiquetas de ruta de destino corta, en vez de las direcciones de red IP.

MPLS tiene varias características que la definen. Es multiprotocolo, lo que significa que tiene la capacidad de transportar cualquier contenido, incluido tráfico IPv4, IPv6, Ethernet, ATM, DSL y Frame Relay. Usa etiquetas que le señalan al router qué hacer con un paquete. Las etiquetas identifican las rutas entre router distantes en lugar de entre terminales, y

mientras MPLS enruta paquetes IPv4 e IPv6 efectivamente, todo lo demás se conmuta.

MPLS es una tecnología de proveedor de servicios. Las líneas arrendadas entregan bits entre sitios, y Frame Relay y WAN Ethernet entregan tramas entre los sitios. Sin embargo, MPLS puede entregar cualquier tipo de paquete entre sitios. MPLS puede encapsular paquetes de diversos protocolos de red. Admite una amplia variedad de tecnologías WAN, que incluyen los enlaces de portadoras T y E, Carrier Ethernet, ATM, Frame Relay y DSL

Netacad Cisco Systems describe un ejemplo de topología de la Figura 2-1, se muestra cómo se utiliza MPLS. Observe que los diferentes sitios se pueden conectar a la nube MPLS mediante diferentes tecnologías de acceso. En la ilustración, CE hace referencia al perímetro del cliente, PE es el router perimetral del proveedor que agrega y quita etiquetas, y P es un router interno del proveedor que conmuta paquetes con etiquetas MPLS.



Nota: MPLS es principalmente una tecnología WAN de proveedor de servicios.
Fuente: “Ejemplo topología MPLS” Netacad Cisco Systems (2016).

Figura 2.1 Topología MPLS

2.2.1.1 Principales ventajas de MPLS

Entre las ventajas de la tecnología MPLS se pueden resaltar:

- Conmutación rápida de paquetes basado en etiquetas y no direcciones IP destino.
- Redes de clientes totalmente independientes, Lavado (2010).
- Es multi-protocolo tanto hacia arriba (L3) como hacia abajo.
- Trabaja con QoS (Calidad de Servicio) basado en marcación de paquetes.
- La creación de una nueva VPN sólo implica la creación del circuito de acceso y del enrutamiento.

- Permite aplicar Ingeniería de Tráfico (TE).
- Uso eficiente del ancho de banda en accesos (full-mesh virtual).

2.2.1.2 Esquema básico de funcionamiento

Para entender el funcionamiento de MPLS, se deben tener claros los términos que describen su arquitectura.

Términos principales utilizados en MPLS

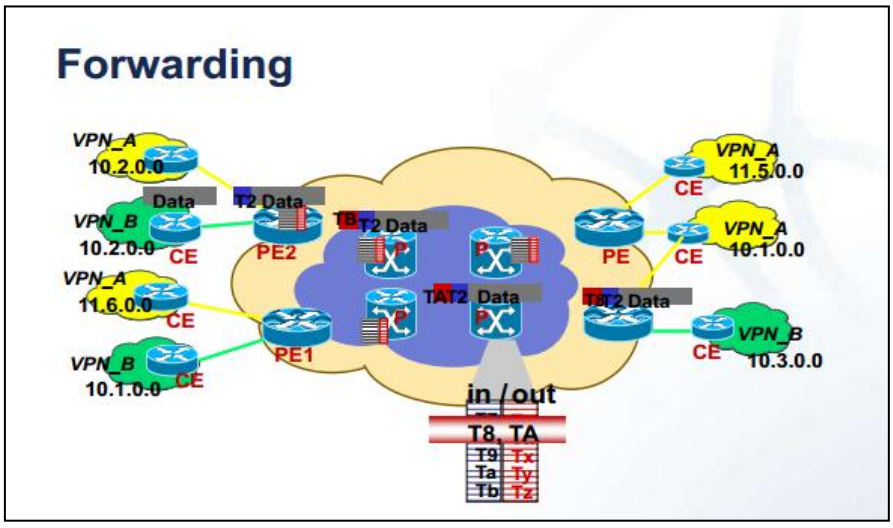
- Según García (2010) *Label Swtiching Router* (LSR) es un nodo interno de la red MPLS capaz de conmutar y enrutar paquetes analizando la etiqueta adicionada a cada uno de estos.
- Edge Label Switch Router (LSR) o Label Edge Router (LER) Nodo de borde que maneja tráfico entrante y saliente de la red MPLS. El Edge LSR de entrada adiciona la etiqueta a MPLS a cada paquete y el de salida la extrae y enruta según la capa de Red, planteó García (2009).
- Según Lavado (2010) nos dice que Label Distribution Protocol (LDP) es un protocolo que establece sesiones TCP entre LSR/LERs para intercambiar las etiquetas que estos utilizarán para la conmutación de paquetes.
- Lavado (2010) menciona que Tag Distribution Protocol (TDP) es un protocolo similar a LDP, propietario de Cisco.
- Lavado (2010) manifiesta que Label Information Base (LIB) es una base de datos formada en un LSR/LER que contiene información de etiquetas e interfaces asociadas a las redes destino.
- Lavado (2010) menciona que Forwarding Equivalence Class (FEC) que es una clase que agrupa un conjunto de paquetes que se enviarán en base a una

característica común (dirección destino, clase QoS, etc.). Los paquetes que pertenezcan al mismo FEC, usarán el mismo camino a lo largo de toda la red MPLS y la misma etiqueta de salida.

- Los autores como García (2009) y Lavado (2010) mencionan que Label Switched Path (LSP) es un Camino unidireccional definido con QoS y formado por una secuencia de LSRs sobre el cual se envían los paquetes que pertenecen al mismo FEC.
- García (2009) Traffic Engineering (TE) nos dice que es un proceso de control de flujo de tráfico a través de la red, que optimiza el uso de recursos con el objetivo de mejorar su rendimiento.

2.2.1.3 Modo de operación

La Figura 2-2 muestra como MPLS puede funcionar usando etiquetas a fin de poder soportar múltiples redes privadas virtuales sobre sobra la misma plataforma.



Fuente: “Reenvió de etiquetas MPLS”. Alvez (2016)

Figura 2.2 Operación MPLS.

Según Morales (2006) nos dice que primero, se establece un LSP entre los routers que van a transmitir el tráfico FEC. Los LSPs hacen las veces de túneles de transporte e incluyen los parámetros QoS específicos del flujo, que sirven para determinar la cantidad de recursos a reservar para el LSP y las políticas de desechado y la cola de procesos en cada LSR.

Morales (2006) también nos dice que para intercambiar información los routers MPLS usan los protocolos LDP o TDP. Cada flujo de tráfico FEC es asignado a una etiqueta particular. La asignación de nombres y rutas se puede realizar manualmente o bien a través del protocolo empleado.

Morales (2006) nos dice cuando un paquete ingresa al dominio MPLS, el Edge LSR determina los servicios de red que requiere. Luego, asigna el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía. Si no existe ningún LSP, el router de borde trabaja en conjunto con los demás LSRs para definirlo. Una vez dentro del dominio MPLS, en cada LSR que recibe el paquete se llevan a cabo los siguientes procesos.

- Se retira la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete.
- Se envía el paquete al siguiente LSR dentro del LSP.
- Morales (2006) finalmente nos dice que el LSR de salida “abre” la etiqueta y lee el encabezado IP para enviarlo a su destino final.

2.2.1.4 Arquitectura MPLS

A continuación de describen los principales elementos que conforman una red MPLS.

a) Componentes lógicos

Lavado (2010) nos dice que la arquitectura MPLS comprende dos componentes lógicos principales:

- Plano de Control (control plane): Hace el intercambio de etiquetas y rutas en capa 3.
- Plano de Datos (data plane): Reenvía los paquetes basado en las etiquetas.

b) Componentes físicos

Pepepnjak y et. (2002) menciona que un término muy importante en MPLS es el Label Switch Router (LSR). Cualquier router o switch que implemente procedimientos de distribución de etiquetas y pueda enviar paquetes basándose en etiquetas se encuentra en esta categoría. Los diferentes tipos de LSR pueden ser descritos dependiendo de la arquitectura donde se encuentren como Edge-LSRs (LSRs de borde), ATM-LSRs, y ATM Edge-LSRs.

Este autor también plantea que un Edge-LSR es un router que realiza ya sea label imposition (o push action) o label disposition (o pop action) en el borde de la red MPLS. *Label imposition* es el acto de anteponer etiquetas a un paquete en el punto donde ingresa al dominio MPLS. *Label disposition*, por otro lado, es el acto de remover la última etiqueta de un paquete en el punto de salida para luego enviarlo a un vecino fuera del dominio MPLS.

Pepepnjak y et. (2002) nos dice que cualquier LSR que tenga vecinos que no tienen implementado MPLS es considerado un Edge-LSR. Sin embargo, si ese LSR tiene interfaces que se conectan a un ATM-LSR a través de MPLS, también

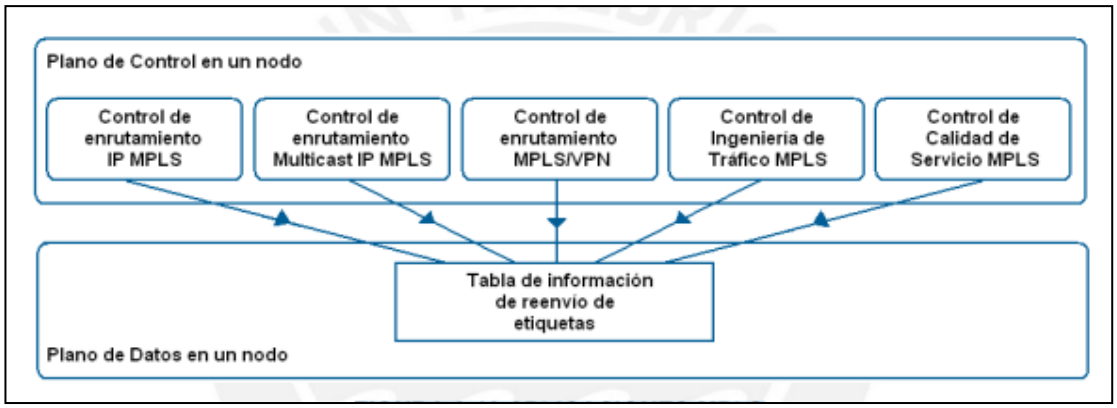
se considera un ATM Edge-LSR. Los Edge-LSRs usan una tabla de reenvío IP tradicional con la información adicional de etiquetado, para poder etiquetar y desetiquetar los paquetes.

Un ATM-LSR es un switch ATM que puede actuar como un LSR. El ATM-LSR realiza enrutamiento IP y asignación de etiquetas en el plano de control y reenvía los paquetes utilizando mecanismos de conmutación ATM tradicional (ATM cell switching) en el plano de datos. En otras palabras, la matriz de conmutación de un switch ATM es utilizada como una tabla de reenvío de un nodo MPLS. Lo switches ATM tradicionales, pueden ser reasignados como ATM-LSRs a través de una actualización del software de su componente de control, Pepepnjak y et. (2002).

2.2.1.5 Aplicaciones de MPLS

Pepepnjak y et. (2002) mencionó que MPLS permite la integración de routers tradicionales y switches ATM en un backbone IP (arquitectura IP+ATM). Sin embargo, su verdadero potencial se encuentra en otras aplicaciones que van desde ingeniería de tráfico hasta Redes Privadas Virtuales punto a punto (peer-to-peer Virtual Private Networks). Todas ellas usan una funcionalidad del plano de

control similar al plano de control del enrutamiento IP. La figura 2-3 muestra la interacción entre estas aplicaciones y la matriz de conmutación de etiquetas.



Fuente: “Various MPLS Applications and Their Interactions” Pepepnjak y et. (2002)

Figura 2.3 Aplicaciones MPLS

2.2.2 VPNs

2.2.2.1 Definición

Una Red Privada Virtual (*VPN*) es una red virtual creada dentro de otra red, generalmente Internet, por lo que los requerimientos de seguridad son de alto nivel e importancia. El intercambio efectivo de paquetes y la QoS son servicios de alta importancia en el manejo de redes virtuales privadas Morales (2006). La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a través de la infraestructura de un proveedor de servicios. Esto es posible ya que la tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se

encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles sólo en redes privadas

MPLS provee un mecanismo eficiente para el manejo de redes privadas virtuales. De esta manera el tráfico de una red privada “atraviesa” la Internet eficazmente y de manera transparente para el usuario, eliminando cualquier tráfico externo y protegiendo la información.

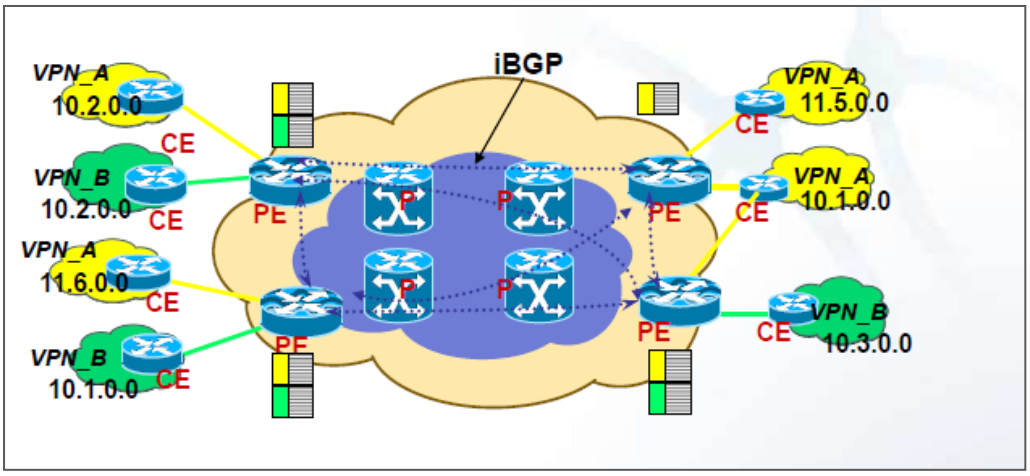
Las VPN creadas con tecnología MPLS tienen una mayor capacidad de expansión y son más flexibles en cualquier red, principalmente IP. MPLS se encarga de reenviar (*forward*) paquetes a través de túneles privados utilizando

Etiquetas que actúan como códigos postales. Dicha etiqueta tiene un identificador que la aísla a esa VPN, más adelante se mostrara ampliamente el funcionamiento de las etiquetas.

Según Morales (2006) menciona que las ventajas principales de implementar MPLS en VPN son:

- Maximizar la capacidad de ampliación.
- Actualización transparente para el usuario.
- Utilización óptima de los recursos de la red.
- Diferenciación entre servicios.
- Reducción de costos mediante consolidación de servicios.
- Seguridad y rapidez de transmisión de información.
- Uso de tecnología de vanguardia.

La Figura 2-4 muestra un esquema básico de funcionamiento de una VPN basada en MPLS donde coexisten dos VPNs A y B.



Fuente: “Reenvió de etiquetas MPLS”. Alvez, R. (s. f).

Figura 2.4 Esquema de una VPN

El equivalente lógico de la red VPN que se muestra en la Figura 2-4 sería un enlace privado punto a punto (peer-topeer), que es sumamente costoso si se trata de extender la red a grandes distancias, debido al requerimiento de cableado y equipos en la localidad a la cual se quiera llegar.

2.2.2.2 Razones para implementar una VPN en término general

- Reducción de Costos

  Según Limari (2004) menciona que para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto). En su lugar, se puede emplear un acceso ADSL o *metroethernet.* Es de bajo costo, brinda un ancho de banda alto y está disponible en la

mayoría de zonas urbanas. Los usuarios remotos móviles podrán ahorrar costos de llamadas telefónicas de larga distancia, realizándolas a través de un acceso local a Internet.

- Alta Seguridad

  Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, comparables con una red punto a punto. Protocolos como 3DES (Triple data encryption standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan un alto nivel de seguridad al sistema. También se emplean varios niveles de autenticación para el acceso a la red privada mediante llaves de acceso, para validar la identidad del usuario, Limari (2004).

- Escalabilidad

  No es necesario realizar inversiones adicionales para agregar usuarios a la red. El servicio se provee con dispositivos y equipos configurables y manejables. La desarrollada infraestructura de los proveedores de Internet hace innecesario realizar un enlace físico que puede significar una gran inversión de dinero y de tiempo, Limari (2004).

- Compatibilidad con tecnologías de banda ancha

  Una VPN puede aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ADSL o ISDN. Con ello brinda un alto grado de flexibilidad al momento de

configurar la red. Se pueden emplear tecnologías como Voz sobre IP (VoIP), que permiten ahorrar en telefonía de larga distancia, Limari (2004)

- Mayor Productividad

  Una VPN da un nivel de acceso durante mayor tiempo, que significa una mayor productividad de los usuarios de la RED. Además, con la consecutiva reducción en las necesidades de espacio físico, se fomenta el teletrabajo, Limari (2004).

2.2.2.3 VPNs según necesidades empresariales

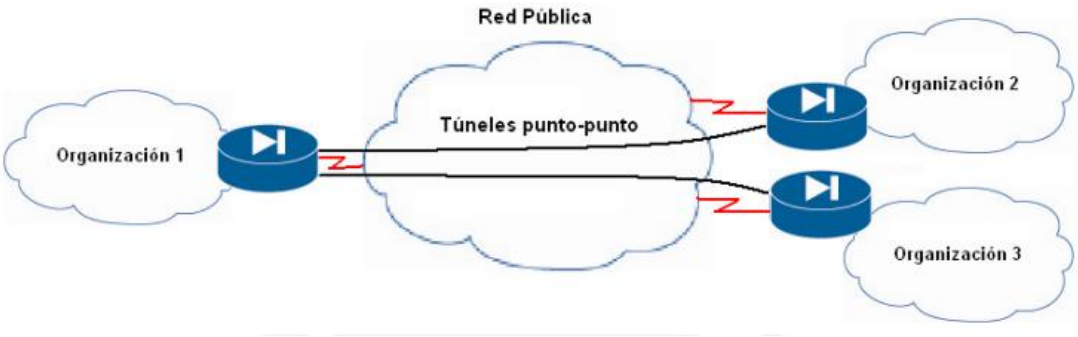
Según Pepelnjak & Guichard (2002) nos menciona que una empresa u organización normalmente implementa una VPN para satisfacer las necesidades de comunicación dentro de la organización (intranet), comunicación con otras organizaciones (extranet) y acceso de usuarios desde dispositivos móviles, computadoras en casa u oficinas remotas.

Este autor Pepelnjak & Guichard (2002) también nos plantea cómo las soluciones que cubren estas necesidades abarcan la gran mayoría de topologías y tecnologías que los proveedores de servicios VPN ofrecen. La diferencia se encuentra en el nivel de seguridad que maneja cada tipo de implementación.

En el caso de la intranet, el tráfico enviado suele no estar bien protegido por los hosts finales o los firewalls con los que cuenten. Por lo tanto, la solución VPN para este tipo de comunicación debe ofrecer altos niveles de aislamiento y seguridad. Además, el servicio debe contar con calidad de servicio (QoS) garantizada para procesos críticos. Por dichas razones, una organización no suele optar por utilizar la red de Internet, pues no se puede contar con calidad de

servicio de extremo a extremo, aislamiento o seguridad que las conexiones dentro de la empresa requieren.

Por otro lado, Pepelnjak & Guichard (2002) nos menciona que las conexiones con otras empresas (extranet) generalmente se encuentran entre locales centrales de las organizaciones, para las cuales se usan dispositivos de seguridad dedicados, como firewalls o equipos de encriptación. Se muestra un ejemplo en la figura 2-5 donde la organización 1 posee tunes encriptados hacia las organizaciones 2 y 3. Estas conexiones no suelen contar con requerimientos rigurosos de calidad de servicio, por lo que son adecuadas para montar en ellas la comunicación. Por ello, el tráfico entre empresas se envía mayormente a través de Internet.



Fuente: “Typical Extranet Setup” Pepelnjak & Guichard (2002)

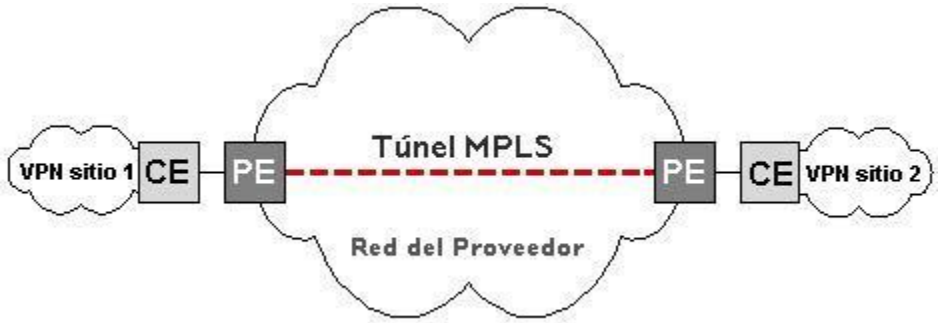
Figura 2.5 Modelo de red extranet

Los usuarios remotos acceden a la red corporativa desde ubicaciones desconocidas y no fijas. Esto produce problemas de seguridad entre los extremos del enlace, que se resuelven aplicando tecnologías de encriptación o contraseñas de un solo uso. Por lo tanto, el nivel de seguridad requerido para estas redes,

llamadas VPDN (Virtual Private Dial-up Network), es significativamente menor que para redes Intranet.

2.2.2.4 Modelo MPLS-VPN

Para entender el funcionamiento de una red MPLS VPN, es necesario conocer los términos P (Reuter interno del proveedor), PE (router frontera del proveedor) y CE (router frontera de cliente que solicita el servicio). Se entiende como sitio a las intranets de los clientes que están separados físicamente pero lógicamente unidos vía una VPN, en la figura 2.6 muestra la apariencia del modelo MPLS-VPN donde participan los elementos esenciales de este escenario como son los CEs y PEs.



Fuente: “Investigación de Redes VPN con Tecnología MPLS” Morales, B. (2006).

Figura 2.6 VPN CON MPLS Habilitado.

a) Funcionamiento.

Cada VPN está asociada con una o más instancias de Ruteo/Reenvío Virtual llamadas (*VRF*). Una VRF determina la membresía que tiene el cliente conectado al router PE de la compañía proveedora del servicio. Cada VRF está

compuesta por una tabla de ruteo IP, una tabla de Reenvío Express de Cisco (*CEF*), un grupo de interfaces que utilizan dicha tabla y un conjunto de reglas y parámetros del protocolo de ruteo que controlan la información que se incluye en la tabla de ruteo. Las VRF contienen las rutas disponibles en la VPN que pueden ser accesadas por los sitios de los clientes, cada sitio puede estar suscrito a varias VPN, pero solo a un VRF. Para prevenir que no salga ni entre tráfico fuera de la VPN, cada VRF tiene guardada información de reenvío de paquetes en las tablas IP y CEF".

b) Comunidades Ruta Objetivo VPN

Según Morales (2006) nos menciona que la distribución de información de la Red de Paquetes Cognoscitiva (*CPN*) se controla mediante el uso de comunidades ruta objetivo VPN. Las comunidades BGP extendidas se encargan de dicha distribución, mediante el siguiente procedimiento".

- Cuando una nueva ruta VPN entra por un router CE, esta ingresa al protocolo BGP y añade sus atributos a la lista de comunidades extendidas ruta objetivo. Los valores de esta lista se obtienen de la lista de exportación de rutas objetivo relacionadas con la VRF de donde se obtuvo la nueva ruta.
- Adicionalmente, cada VRF incluye también una lista de importación de comunidades extendidas ruta objetivo, esta lista define los atributos que una comunidad extendida ruta objetivo debe tener para que la ruta pueda ser importada al RF.

c) Distribución BGP de información de Ruteo VPN

En una red VPN MPLS, los router PE pueden obtener el prefijo IP (IPv4) de los router CE por configuración estática. Esto mediante una sesión BGP con el router CE o mediante RIP. Después de esta operación el router PE lo convierte en un prefijo VPN-IPv4 al añadirle 8 bits de Distintivo de Ruta (*RD*) que como su nombre lo dice, sirve para distinguir la ruta. Este nuevo prefijo sirve para identificar la dirección del cliente sin importar donde este y si su dirección es global o local, única o común. El RD se obtiene del VRF del router PE en cuestión, Morales (2006).

BGP es el encargado de distribuir la información de capacidad de alcance (*reachability*) a los prefijos VPN-IPv4. Cuando la distribución se lleva PE-PE, cuando se lleva a cabo entre los dominios IP tenemos BGP externo (*eBGP*) por medias sesiones PE-CE.

Adicionalmente, BGP lleva acabo la propagación de la información de capacidad de alcance mediante las extensiones multiprotocolo BGP en donde se extiende BGP para proveer soporte para direcciones multiprotocolo como IPv6 e IPX. Esta última acción asegura que todos los miembros de la VPN reciban todas las rutas de las demás VPNs para que pueda haber comunicación entre todas. Acabó dentro del dominio IP tenemos BGP interno (*iBGP*) por medio de sesiones PE-PE, cuando se lleva a cabo entre los dominios IP tenemos BGP externo (*eBGP*) por medio sesiones PE-CE.

Adicionalmente, nos menciona Morales (2006) que BGP lleva acabo la propagación de la información de capacidad de alcance mediante las extensiones multiprotocolo BGP en donde se extiende BGP para proveer soporte para

direcciones multiprotocolo como IPv6 e IPX. Esta última acción asegura que todos los miembros de la VPN reciban todas las rutas de las demás VPNs para que pueda haber comunicación entre todas

d) Reenvío MPLS en VPNs

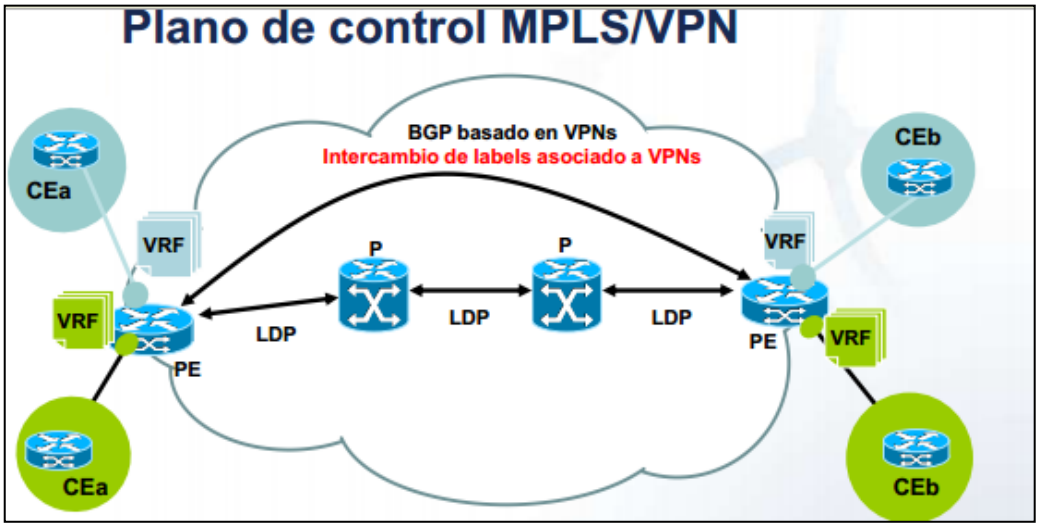
El reenvío de paquetes en una red VPN con tecnología MPLS se basa en la información de ruteo almacenada en las tablas VRF (ruteo y CEF). Los router PE añaden una etiqueta a cada prefijo que obtienen de los router CE, el prefijo incluye información de capacidad de alcance de los demás router PE. Es un proceso de etiquetado como el que se lleva acabo con los LER y LSR, Morales (2006)

a) Entra el paquete que proviene de un router CE al router PE, este le añade una etiqueta y lo envía.

b) Cuando el mensaje etiquetado llega al PE destino, este lee y quita la etiqueta para mandar el paquete al CE descrito en la etiqueta.

El reenvío de etiquetas a través del eje troncal del proveedor se puede basar en conmutación dinámica de etiquetas o en Caminos de Ingeniería de Tráfico.

En todo momento los paquetes que viajan por el *backbone* llevan dos etiquetas, la primera tiene la dirección del router PE y la segunda indica cómo el router PE debe de reenviar el paquete al router CE. Cuando el router PE recibe el paquete, lo que hace es leer la etiqueta, quitarla y reenviarla al destino marcado en la segunda etiqueta" Morales (2006) en la figura 2.7 muestra el intercambio de etiquetas asociados a VPNs mediante la extensión multiprotocolo BGP (MP-BGP).



Fuente: “Reenvió de etiquetas MPLS”. Morales (2006)

Figura 2.7 Reenvió de etiquetas**.**

2.2.3 Protocolo BGP

2.2.3.1 Definición.

El protocolo Border Gateway Protocol (BGP) se estableció como un estándar de Internet en 1989 y fue definido originalmente en la RFC_1105, adoptándose como un protocolo para la comunicación entre dominios dentro de la comunicación EGP. La versión actual es la BGP-4, que se adoptó en 1995 y ha sido definida en la RFC 1771. BGP-4 soporta CIDR (Classless Inter Domain Routing) y es el protocolo de enrutamiento que actualmente se usa de forma mayoritaria para encaminar la información entre sistemas autónomos, ya que ha demostrado ser fácilmente escalable, estable y dotado de los mecanismos necesarios para soportar políticas de encaminamiento complicadas. A partir de

ahora cuando se nombre al protocolo BGP, se está haciendo mención de la versión BGP-4.

BGP continúa desarrollándose a través del trabajo del proceso de los estándares de Internet en el IETF. Como los requisitos del encaminamiento de Internet cambian, el protocolo BGP se extiende para continuar proporcionando mecanismos que controlen la información de encaminamiento y soporten los nuevos requisitos. Por eso, la RFC básica ha sido extendida por varias RFCs posteriores, TELDAT (2008).

2.2.3.2 Mecanismos del Protocolo

El protocolo BGP utiliza el protocolo TCP para establecer una conexión segura entre dos extremos BGP en el puerto 179. Una sesión TCP se establece exactamente entre cada par para cada sesión del BGP. Ninguna información de encaminamiento puede ser intercambiada hasta que se ha establecido la sesión TCP. Esto implica la existencia previa de conectividad IP para cada par de extremos BGP. Para dotarlo de mayor seguridad, se pueden usar firmas MD5 para verificar cada segmento TCP.

Se dice que BGP es un protocolo de encaminamiento vectorial, porque almacena la información de encaminamiento como combinación entre el destino y las características de la ruta para alcanzar ese destino. El protocolo utiliza un proceso de selección determinista de la ruta para seleccionar la mejor dentro de las múltiples rutas factibles, usando las cualidades de la ruta como criterios. Las características como por ejemplo el retardo, la utilización del enlace o el número de saltos no se consideran dentro de este proceso. El proceso de selección de la

ruta es la clave para comprender y establecer las políticas del protocolo BGP y se analizarán más adelante.

Al igual que la mayoría de los protocolos del tipo IGP, BGP envía solamente una actualización completa del encaminamiento una vez que se establece una sesión BGP, enviando posteriormente sólo cambios incrementales. BGP únicamente recalcula la información de encaminamiento concerniente a estas actualizaciones, no existiendo proceso que actualice toda su información de encaminamiento como los cálculos del SPF en el OSPF o el IS-IS. Aunque la convergencia IGP puede ser más rápida, un IGP no está preparado para soportar el número de las rutas empleadas en el encaminamiento inter-dominio. Un IGP también carece de las cualidades de ruta que el BGP lleva, y que son esenciales para seleccionar la mejor ruta y construir políticas de encaminamiento. BGP es el único protocolo adecuado para el uso entre sistemas autónomos, debido a la ayuda inherente que las políticas sobre rutas proporcionan para el encaminamiento. Estas políticas permiten que se acepte o rechacé la información de cambio de encaminamiento antes de que se utilice para tomar decisiones de envío. Esta capacidad da a los operadores de red un alto grado de protección contra información de encaminamiento que puede ser no deseada, y así controlar la información de encaminamiento según sus necesidades particulares, TELDAT (2008).

2.2.3.3 Criterio de selección de rutas

El protocolo BGP trabaja con una tabla privada de rutas que incluye tanto las rutas de la tabla de rutas activas del equipo, como las rutas aprendidas por

BGP de todos los vecinos. En la tabla de rutas de BGP puede haber varias rutas para ir al mismo destino, de las que se seleccionan sólo las más prioritarias para instalarlas en la tabla de rutas activas del equipo. Para ello el protocolo BGP maneja diversos parámetros que determinan la prioridad de cada ruta. En los siguientes apartados se describen los parámetros que el protocolo BGP emplea en el proceso de selección de rutas, TELDAT (2008).

a) Preferencia (Distancia administrativa)

La Preferencia de una ruta equivale a la Distancia Administrativa entre protocolos en el equipo. Este parámetro es el más prioritario a la hora de seleccionar una ruta para instalarla en la tabla de rutas activas del equipo. Cada protocolo tiene un valor de Preferencia por defecto. Estos valores se resumen en la tabla 2.1.

Tabla 2-1 *"Distancia administrativo" TELDAT (2008).*

Preferencia	Protocolo de routing
0	Rutas directamente conectadas.
10	Protocolo OSPF (Open Shortest Path First).
60	Rutas estáticas.
100	RIP (Routing Information Protocol).
150	Rutas OSPF externas.
170	BGP (Border Gateway Protocol).

b) Preferencia *(tie-breaker)*

El parámetro Preferencia2, también llamado tie-breaker, sirve para resolver casos de conflicto entre dos rutas de la misma Preferencia, TELDAT (2008).

c) Métrica (MULTI_EXIT_DISC)

La Métrica indica el coste de la ruta, y sólo es comparable entre rutas de un mismo protocolo o. El significado de la métrica se define para cada protocolo. Por ejemplo, en RIP indica el número de saltos hasta el destino. La Métrica en BGP hereda el valor del atributo MULTI_EXIT_DISC, TELDAT (2008).

d) Métrica2 (LOCAL_PREF)

Este parámetro en BGP hereda el valor del atributo LOCAL_PREF. Si no se ha asignado ningún valor (se muestra -1) se considera de máxima preferencia TELDAT (2008).

e) AS-path

En una ruta aprendida por BGP el AS-path indica a través de qué Sistemas Autónomos se ha aprendido dicha ruta, TELDAT (2008).

f) Eligiendo una ruta

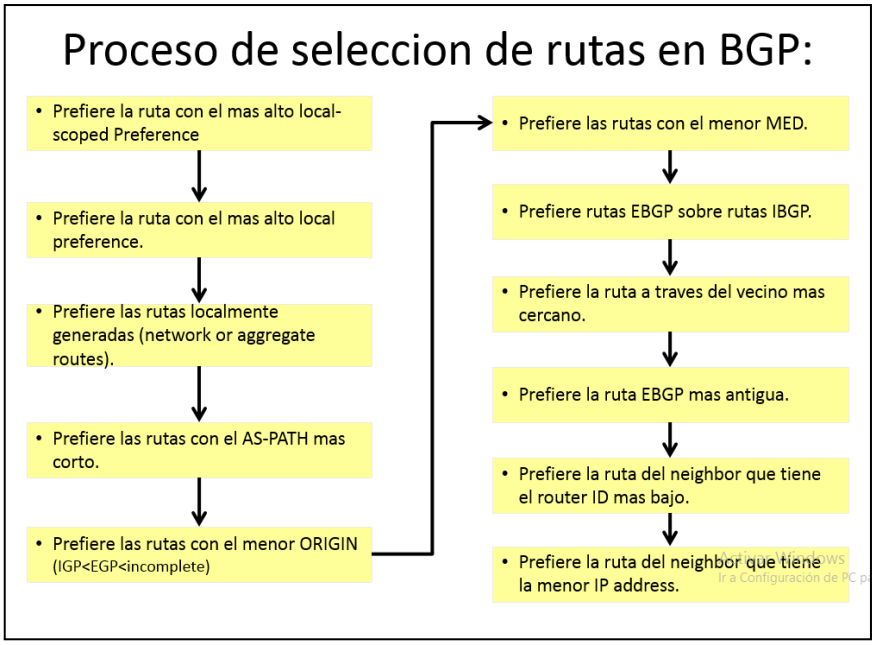
El protocolo BGP utiliza las siguientes reglas para elegir la mejor ruta o salto a un determinado destino, TELDAT (2008).

La ruta con la menor Preferencia (Distancia Administrativa) es la elegida. Si dos rutas tienen la misma Preferencia, se elige la ruta con la menor Preferencia2.

Si las dos rutas se han aprendido por BGP se aplican los siguientes criterios:

- Se prefiere la ruta con mayor Métrica2 (LOCAL_PREF). Si no se ha asignado valor de Métrica2 (aparece –1) se considera el valor máximo.
- Una ruta con información de AS-path es preferida frente a otra sin AS-path.
- Entre dos rutas con AS-path, provenientes del mismo AS, y con información de Métrica, se prefiere aquella que tiene menor valor de Métrica (MULTI_EXIT_DISC).
- Entre dos rutas con AS-path distintos, se prefiere la de origen IGP, y si no la de origen EGP.
- Entre dos rutas con AS-path distinto y con mismo origen, se prefiere la de AS-path de menor longitud.
- Una ruta aprendida desde IGP es preferida a una aprendida desde EGP. La ruta menos preferida es la que se obtiene indirectamente de un IGP que la ha obtenido de un EGP.
- Si ambas rutas se aprendieron del mismo protocolo y el mismo AS, se usa la que tenga la menor Métrica.
- Se prefieren las rutas instalables en la tabla de rutas activas del equipo frente a las rutas no instalables.
- Se prefiere la ruta que tenga siguiente salto con el valor de dirección IP más bajo.

En la Figura 2.8 muestra el proceso de selección de rutas de forma esquemática cuando el protocolo BGP recibe prefijos de vecinos BGP.



Fuente “Capacitación CLARO”

Figura 2.8 Selección de rutas

2.2.4 Calidad de servicio a los servicios diferenciados.

2.2.4.1 Definición

Servicios diferenciados (DiffServ) es un nuevo modelo en el cual el tráfico es procesado a través de sistemas intermedios con prioridades relativas en base al campo Tipo de servicios (ToS). El estándar DiffServ reemplaza la especificación original para definir la prioridad del paquete. DiffServ aumenta el número de niveles de prioridad definibles al reasignar los bits de un paquete de IP para que se les haga una marcación prioritaria.

Según Cisco Systems (s. f) nos dice que la arquitectura de DiffServ define el campo del DiffServ (DS), que reemplaza el campo de la TOS en el IPv4 para tomar las decisiones del Per-Hop Behavior (PHB) sobre la clasificación de

paquetes y las funciones de condicionamiento del tráfico, tales como medición y marcar.

Los RFC no dictan la manera de implementar los PHB; ésta es la responsabilidad del vendedor. El Cisco implementa las técnicas de colocación en cola que pueden basar su PHB en el IP precedence o el valor del DSCP en el encabezado IP de un paquete. De acuerdo con el DSCP o el IP precedence, el tráfico se puede poner en una clase del servicio determinado. A los paquetes incluidos en una clase de servicio se los trata del mismo modo.

2.2.4.2 Código de punto de servicio diferenciado.

Pérez (2013) también nos menciona que los seis *Most Significant Bits* del campo del *DiffServ* se llaman como el DSCP. Los dos bits más más recientes del Currently Unused (CU) del campo del DiffServ no fueron definidos dentro de la arquitectura del campo DiffServ; éstos ahora se utilizan como bits de la notificación de congestión explícita (ECN). El routers en el borde de la red clasifica los paquetes y las marcas con el IP precedente o el valor del DSCP en una red Diffserv. Otros dispositivos de red en la base que soportan el uso del Diffserv el valor del DSCP en el encabezado IP de seleccionar una conducta PHB para el paquete y de proporcionar al tratamiento apropiado.

Los diagramas de la figura 2-9, 2-10 en esta sección muestran una comparación entre el *Byte ToS* y el campo del *DiffServ.*

Byte ToS

P2	P1	P0	T2	C1	T0	CU1	CU0

Figura 2.9 Campo BYTE TOS

Fuente" Implementación de políticas de calidad de servicio. Cisco Systems (s. f)

- Bits de la precedencia-tres del IP (P2 al P0)
- Bits del retardo, del rendimiento de procesamiento y de la Confiabilidad-tres (T2 al T0)
- CU (actualmente sin usar) - dos bits (CU1-CU0)

Campo DiffServ.

DS5	DS4	DS3	DS2	DS1	DS0	ECN	ECN

Figura 2.10 Campo Diffserv

Fuente" Implementación de políticas de calidad de servicio. Cisco Systems (s. f)

- Bits de DSCP-six (DS5-DS0)
- Bits de ECN-two

El campo *DiffServ* estandarizado del paquete está indicado con un valor para que el paquete reciba un tratamiento de reenvío especial o PHB, en cada nodo de la red.

El valor por defecto DSCP es 000 000. El Selector de clase DSCP es los valores que son posteriores - compatible con el IP precedence. Al convertir entre

el IP precedence y el DSCP, corresponder con los tres bits más significativos. En otras palabras: IP Prec 5 (101) maps to IP DSCP 101 000

Estándar DiffServ utiliza los mismos bits de precedencia (el bits-DS5, el DS4 y el DS3 más significativos) para la Configuración de prioridad, pero clarifica más lejos las definiciones, ofreciendo la granularidad más fina con el uso de los tres bits siguientes en el DSCP. El DiffServ reorganiza y retitula los Niveles de precedencia (todavía definidos por los tres bits más significativo del DSCP) en las ocho categorías descritas en la figura 2.11 donde se escalan los niveles de mejor esfuerzo (los niveles se explican en el mayor detalle en este documento), Cisco Systems (s. f).

.

Nivel de precedencia	Descripción
7	Permanece igual (la capa de enlace y el protocolo de ruteo se mantienen activos)
6	Permanece igual (utilizado para protocolos de IP Routing)
5	Express Forwarding (EF)
4	Clase 4
3	Clase 3
2	Clase 2
1	Clase 1
0	El mejor esfuerzo

Fuente" Implementación de políticas de calidad de servicio, Cisco Systems (s. f)

Figura 2.11 Nivel de precedencia

Con este sistema, un dispositivo da la prioridad al tráfico por la clase primero. Después distingue y da la prioridad al tráfico de la mismo-clase, tomando la probabilidad de caída en consideración.

Estándar DiffServ no especifica una definición precisa “punto bajo,” “media de la probabilidad de caída,” y del “colmo”. No todos los dispositivos reconocen las configuraciones del DiffServ (DS2 y DS1); y aun cuando estas configuraciones se reconocen, ellas no accionan necesariamente la misma acción de reenvío de PHB en cada nodo de red. Cada nodo implementa su propia respuesta basada en cómo se configura, Cisco Systems (s. f).

2.2.4.3 Reenvió asegurado (AF) PHB

Se describe como los medios para que un dominio del abastecedor DS ofrezca diversos niveles de aseguramientos de la expedición para los paquetes del IP recibidos de un dominio del cliente DS. La expedición asegurada PHB garantiza una cierta cantidad de anchura de banda a una clase del AF y permite el acceso a la anchura de banda adicional, si está disponible. Hay cuatro clases del AF, AF1x con AF4x. Dentro de cada clase, existen tres probabilidades de caída. Dependiendo de la política de una red dada, los paquetes se pueden seleccionar para un PHB basado en el rendimiento de procesamiento requerido, retardo, jitter, pérdida o según la prioridad del acceso a los servicios de red.

Las clases 1 a 4 se refieren como clases del AF. La figura 2-12 ilustra la codificación DSCP para especificar la clase AF con la probabilidad. Los bits DS5,

DS4 y DS3 definen la clase; los bits DS2 y DS1 especifican la probabilidad de caída; el dígito binario DS0 es siempre cero, Cisco Systems (s. f).

Nivel	Clase 1	Clase 2	Clase 3	Clase 4
Bajo	001010 AF11 DSCP 10	010010 AF21 DSCP 18	011010 AF31 DSCP 26	100010 AF41 DSCP 34
Medio	001100 AF12 DSCP 12	010100 AF 22 DSCP 20	011100 AF32 DSCP 28	100100 AF42 DSCP 36
Alto	001110 AF13 DSCP 14	010110 AF23 DSCP 22	011110 AF33 DSCP 30	100110 AF43 DSCP 38

Fuente" Implementación de políticas de calidad de servicio, Cisco Systems (s. f)

Figura 2.12 Codificación DSCP con probabilidad.

2.2.4.4 Uso de campo DSCP

Puede usar el campo DSCP de tres maneras:

- Classifier—Selecciona un paquete basándose en los contenidos de algunas porciones del encabezado del paquete y aplica PHB en base a las características del servicio definidas por el valor DSCP. Pérez (2013).
- Marcador—Configure el campo DSCP según el perfil de tráfico, Pérez (2013).

- Medición de la adecuación del control—al perfil del tráfico mediante una función de formación o de eliminación, Pérez (2013).

2.2.4.5 Clasificación de paquetes.

La clasificación de paquetes implica el usar de un descriptor del tráfico para categorizar un paquete dentro de un grupo específico y el hacer del paquete accesible para QoS que dirige en la red. Usar la clasificación de paquetes, le puede tráfico del SCR_INVALID en los niveles de prioridad múltiples o una Clase de servicio (CoS). Pérez (2013)

Puede utilizar listas de acceso (ACL) o el comando match en el modular QoS CLI para hacer que coincidan los valores DSCP, la figura 2.13 muestra cómo se clásica el tráfico con el comando match utilizando el valor de DCSP como valor de coincidencia.

```
Router(config)# class-map match-all VOIP
 1751-uut1(config-cmap)# match ip dscp ?
   <0-63>   Differentiated services codepoint value
   af11     Match packets with AF11 dscp (001010)
   af12     Match packets with AF12 dscp (001100)
   af13     Match packets with AF13 dscp (001110)
   af21     Match packets with AF21 dscp (010010)
   af22     Match packets with AF22 dscp (010100)
   af23     Match packets with AF23 dscp (010110)
   af31     Match packets with AF31 dscp (011010)
   af32     Match packets with AF32 dscp (011100)
   af33     Match packets with AF33 dscp (011110)
   af41     Match packets with AF41 dscp (100010)
   af42     Match packets with AF42 dscp (100100)
   af43     Match packets with AF43 dscp (100110)
   cs1      Match packets with CS1(precedence 1) dscp (001000)
   cs2      Match packets with CS2(precedence 2) dscp (010000)
   cs3      Match packets with CS3(precedence 3) dscp (011000)
   cs4      Match packets with CS4(precedence 4) dscp (100000)
   cs5      Match packets with CS5(precedence 5) dscp (101000)
   cs6      Match packets with CS6(precedence 6) dscp (110000)
   cs7      Match packets with CS7(precedence 7) dscp (111000)
   default  Match packets with default dscp (000000)
   ef       Match packets with EF dscp (101110)
 Router1(config-cmap)# match ip dscp af31
```

Fuente" Implementación de políticas de calidad de servicio "Cisco Systems (s. f)

Figura 2.13 Clasificación de tráfico.

2.2.4.6 Marcación

El DSCP se puede fijar a un valor deseado en el borde de la red para hacerla fácil para que los dispositivos del núcleo clasifiquen el paquete según las indicaciones de la sección de la clasificación de paquetes y proporcionen a un nivel conveniente de servicio. La marca del paquete en base a la clase se puede utilizar para fijar el valor del DSCP como se muestra en la figura 2.14 donde el valor del campo Servicio diferenciado del tráfico de la clase management es ajustado a un valor de 8. Pérez (2013).

```
policy-map pack-multimedia-5M

!--- Creates a policy map named pack-multimedia-5M.

  class management


!--- Specifies the policy to be created for the
!--- traffic classified by class management.


    bandwidth 50
    set ip dscp 8

!--- Sets the DSCP value of the packets matching
!--- class management to 8.

  class C1
    priority 1248
    set ip dscp 40
  class voice-signalling
    bandwidth 120
    set ip dscp 24
```

Fuente" Implementación de políticas de calidad de servicio "Cisco Systems (s. f)

Figura 2.14 Marcación de paquetes.

2.2.5 Protocolo de redundancia de primer salto.

2.2.5.1 Definición.

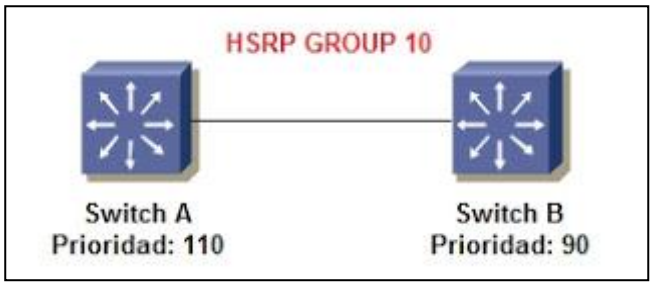
HSRP, VRRP Y GLBP son protocolos de redundancia de gateway, cuyo propósito es que si la puerta de enlace de una Vlan o red cae, otro switch o router automáticamente asuman el control de dicha puerta de enlace, evitando así una caída en la red para los equipos que usan esa gateway. El funcionamiento consiste en que un grupo de switch o router sean configurados para que entre ellos formen un router virtual, con una IP, en cuyo grupo un switch o router asume el control de principal, si este cae, otro switch o router del grupo asume su control con la misma IP, por lo que los usuarios cuya puerta de enlace sea esa IP, podrán continuar comunicándose sin problemas. HSRP, VRRP y GLBP se basan en ofrecer ese servicio, pero cada uno con características determinadas, Pérez, D. (2013).

2.2.5.2 HSRP (protocolo de router de respaldo de salto).

HSRP es un protocolo propietario de Cisco. En HSRP un grupo de switch de capa 3 o routers forman un virtual, con el fin de dar redundancia de puerta de enlace. Los switchs tienen dos roles, activo, que es el que está actuando como puerta de enlace activa de los equipos, y standby, que es el que en caso de que el activo caiga, el standby toma su rol y se convierte en activo. El activo será el switch que tenga una prioridad mayor, por defecto todos switchs tienen una prioridad de 100, pero se puede cambiar. Si varios switchs tienen la misma prioridad, el activo será el que tenga una IP mayor configurada en su interfaz.

En standby sólo puede haber un switch, que será el siguiente en mayor prioridad al activo, o el siguiente en IP más alta en su interfaz. Cuando el activo cae, el standby pasa a ser activo, y se recalcula otro standby en el grupo de switchs que forman el router virtual.

Cuando se usa HSRP y STP a la vez, hay que tener en cuenta que el switch activo de HSRP sea el mismo que el switch root Bridge de STP, así nos evitamos problemas de bucles. Esto lo logramos poniendo a ese switch una prioridad HSRP mayor que la de los demás switchs del grupo [DAN2016]. La figura 2.15 Muestra un escenario con HSRP donde hay dos switches que pertenecen a un grupo HSRP con distintas prioridades.



Fuente “CCNP SWITCH”, Pérez, D. (2013*)*.

Figura 2.15 Escenario HSRP

2.2.5.3 VRRP (Protocolo de redundancia de router virtual):

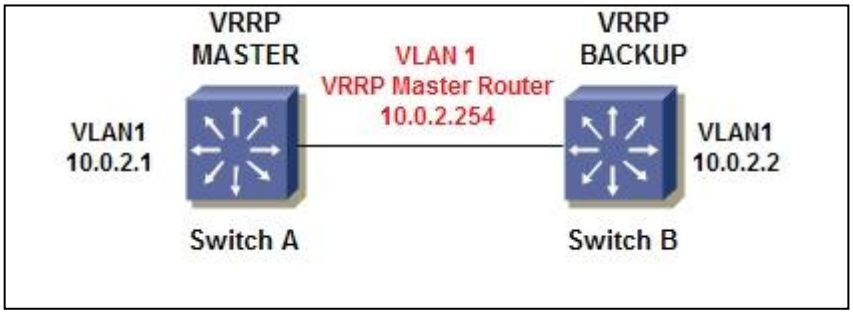
Según Pérez, D. (2013*)*, la finalidad de VRRP es la misma que la de HSRP, dar servicio de redundancia de gateway, con varias diferencias

- HSRP es propietario de Cisco, VRRP es un IEEE estándar.
- En HSRP se pueden configurar 16 grupos como máximo, en VRRP 255.
- HSRP usa un switch como activo y otro como standby, VRRP usa un switch como master, y todos los demás como backups.

- Los tiempos de hello y holdtime son más cortos en VRRP.
- VRRP soporta encriptación en la autenticación (HMAC/MD5).

Cuando el switch que esta como master cae, uno de los que está en backup toma el rol de master, para determinar que switch toma el control, se lleva a cabo un cálculo entre todos ellos en los que entran en juego diferentes intervalos de tiempo. En definitiva, todos los switchs hacen un cálculo, y a el que menos tiempo le dé, es el primero en enviar paquetes al resto de switchs, por lo cual se convierte en master,

Los intervalos de tiempo de hello también se pueden configurar en VRRP, a diferencia de HSRP, en VRRP se configuran en el master y los backups aprenden esos intervalos del master, según nos indica Pérez, D. (2013). La figura 2.16 muestra un escenario con VRRP donde el switch A es el master y el switch B es el backup.



Fuente “CCNP SWITCH”, Pérez, D. (2013).

Figura 2.16 Escenario VRRP

2.2.5.4 GLBP (protocolo de balanceo de carga de salida)

GLBP es otro protocolo de puerta de enlace redundante como HSRP y VRRP, pero la principal diferencia es que GLBP sí ofrece balanceo de carga por sí solo entre varios switchs.

Para lograr esto, a parte de una IP virtual, también es necesario una MAC virtual para cada uno de los switchs del grupo. De esta forma todos tendrían la misma IP virtual pero diferentes MAC. A los equipos se les configura como puerta de enlace la IP virtual, y cuando estos hagan un ARP a esa IP (la primera comunicación que hacen) se les devuelve una MAC de algún switch miembro del grupo de GLBP, de esta forma todos los equipos tendrían como puerta de enlace la misma IP, pero no saldrían todos a través del mismo switch ya que en las respuestas del ARP a cada equipo se le habrá entregado una MAC diferente. Por ejemplo, si tenemos 3 switchs (A, B y C) formando un grupo de GLBP, los 3 tendrán la misma IP virtual, pero cada uno una MAC virtual diferente. Si tenemos 3 equipos en la Vlan, a los 3 se les configurará la misma IP como puerta de enlace, pero obtendrán diferentes MAC, al equipo 1 se le dará la MAC del switch A, por lo tanto el equipo 1 se comunicará a través de éste switch, a el equipo 2 se le dará la MAC del switch B, por lo tanto se comunicará a través del switch B, y así sucesivamente logrando el balanceo de carga.

Entre los switchs del mismo grupo de GLBP se selecciona a uno como AVG (Active virtual gateway) y a todos los demás del grupo como AVF (Active virtual forwarder). El AVG será el encargado de asignar MACs virtuales a los switchs de su mismo grupo, y también es el encargado de responder a las peticiones ARP de los equipos.

A los equipos que soliciten un ARP se les da una MAC de forma consecutiva, es decir, si por ejemplo tenemos 3 switchs (A, B y C) y 6 equipos, al primer equipo que solicite un ARP, se le dará la MAC de A, al segundo la MAC de

B, al tercero la MAC de C, al cuarto la MAC de A, al quinto la MAC de B y al sexto la MAC de C.

Si algún switch cae, su MAC virtual es asignado a otro switch, de tal forma que algún switch tendría más de una MAC virtual, de esta manera no hay equipos que se queden sin red. La figura 2.17 muestra un escenario con GLBP, donde Switch A es el Gateway virtual activo y el Switch B solo es un reenviador virtual activo, Pérez, D. (2013*)*.

Fuente “CCNP SWITCH”, Pérez, D. (2013*)*.

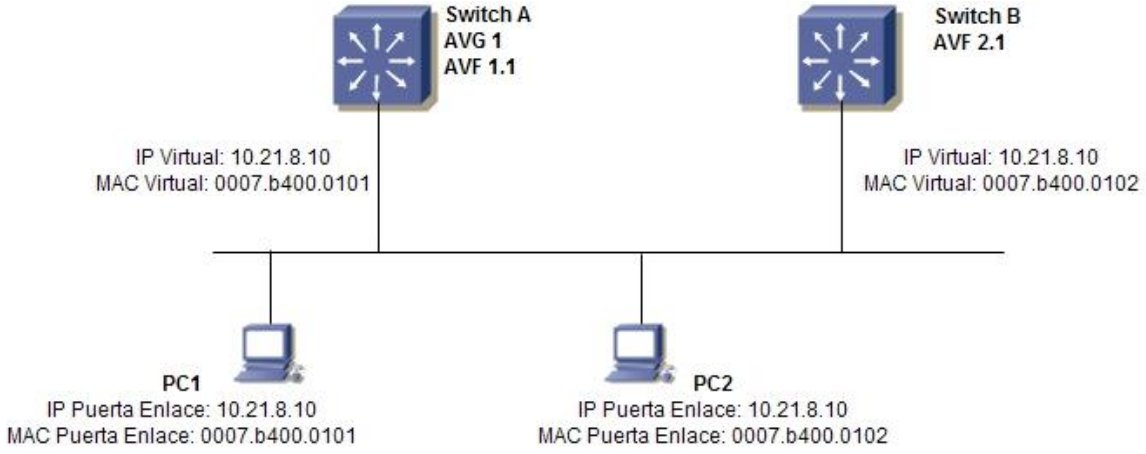


Figura 2.17 Escenario GLBP.

2.3 Marco Conceptual

Una RPV (VPN) es una plataforma de red convergente para la transmisión de voz, datos y vídeo sobre protocolo IP y basado en tecnología MPLS.

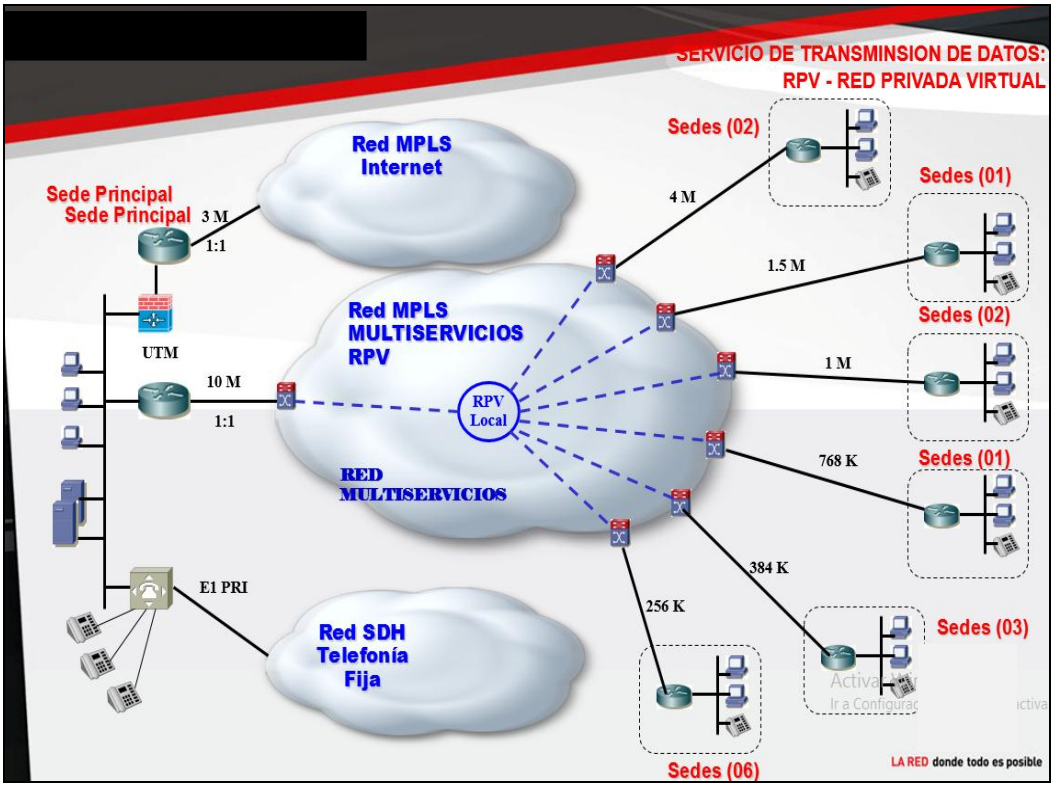
Añade a la tradicional interconexión de oficinas remotas la posibilidad de establecer niveles de Clases de Servicio (CoS) adecuadas para las aplicaciones de datos no críticos, datos críticos, voz y video.

Al aplicar políticas de calidad de servicio (QoS) sobre el ancho de banda contratado, se configura el servicio asegurando un ancho de banda mínimo para cada tipo de tráfico y al mismo tiempo se define una política de encolamiento diferencial de paquetes en función de la Clase de Servicio en caso de que ocurra un incidente de congestión.

Ventajas:

- Le permite desplegar una plataforma segura y fiable tanto para los usuarios como para las aplicaciones
- Comunicación instantánea desde cualquier lugar y en cualquier momento
- Posibilidad de ofrecer múltiples servicios y aplicaciones a través de una infraestructura común.
- Simplifica la operación de la red y su ampliación a lo largo del tiempo
- Mejor aprovechamiento de los recursos, y mayor visibilidad y rendimiento
- Reducción del Coste Total de Propiedad (TCO)
- Prepara a su red para el futuro, permitiéndola crecer a la vez que su negocio
- Integración transparente con una amplia variedad de productos y servicios relacionados

La figura 2.18 muestra un servicio de RPV (VPN) que integra varias sedes y a su vez puede ser interconectada con otros servicios como Internet y la red SDH.



Fuente “capacitación claro”

Figura 2.18 Servicio de transmisión de datos.

CAPÍTULO III: DISEÑO Y DESCRIPCIÓN DEL SISTEMA

3.1. Análisis de sistema

3.1.1 Requerimiento de ancho de banda para las clases de servicio.

Los datos de requerimientos de ancho de banda para las dos VPNs y la cantidad distribuida para cada clase de servicio son proporcionadas por el ingeniero residente de "Delosi" quienes dan soporte a su red, estos datos se describen en la tabla 3.1 y 3.2 para las dos VPN a implementar y son solicitados de acuerdo a la sección 2.3.3 CALIDAD DE SERVICIO donde especifica cómo deben venir marcados los paquete (valor de DSCP en el campo de servicio diferenciado del encabezado IP) y que redes deben pertenecer a qué clase de servicio para que sean marcados y aplicar las políticas a realizar frente a una congestión de tráfico.

Tabla 3-1 *Requerimiento de ancho de banda la para red de "Delosi"*.

ITEM	COS5(clase de servicio)	COS3(clase de servicio)	COS2(clase de servicio)	Total ancho de banda
TIPO DE TRÁFICO	voz	Datos críticos	Datos transacciones	
PRIORIDAD	Máxima	Máxima	Normal	
IP DSCP	Cs5	Cs2	Cs1	
ANCHO DE BANDA	512kbps	1024kbps	512kbps	2048kbps
POLITICA APLICABLE AL TRAFICO EXC	Se descarta	Se remarca como P1	No aplica	
APLICACIONES	Telefonía IP	Aplicaciones de Datos críticas para el negocio como el tráfico generado por la caja registradora	Datos de aplicaciones de negocio, intranet.	
Al tráfico de que red es aplicado.	192.168.99.0 a cualquier destino.	Cualquier origen a los servidores de los cajeros.	Trafico restante.	

Tabla 3-2 *Requerimiento de ancho de banda para red de* POS.

ITEM	COS3(clase de servicio)	Total ancho de banda
TIPO DE TRÁFICO	Datos críticos	
PRIORIDAD	Máxima	
IP DSCP	Cs2	
ANCHO DE BANDA	64kbps	64kbps
POLITICA APLICABLE AL TRAFICO EXCEDENTE	Se descarta	
APLICACIONES	Aplicaciones de datos críticas para el negocio como el tráfico generado por la maquinas POS.	
Al tráfico de que red es aplicado.	De 172.21.99.0 a cualquier destino.	

3.1.2 Análisis de protocolos.

Como se mencionó en el transcurso de este proyecto se diseñara e implementara una red privada virtual en la sede remota para que pueda tener acceso hacia la sede principal. Para ello primero se realizara el diseño, la simulación y finalmente la implementación,

3.1.2.1. Análisis de GNS3.

Para la simulación se dispondrá de esta herramienta GNS3 que sumamente eficaz ya que se puede realizar una simulación casi real porque se utilizan los mismos IOS de cisco y no están limitados en comando como lo son con el simulador packet tracert. Los IOS que se seleccionaron son los que soportan los protocolos a utilizar como son BGP, GLBP, TACACS, Q&S, SNMP Y NETFLOW,

3.1.2.2. Análisis de GLBP.

Este protocolo se utiliza en lugar de HSRP debido a que si ofrece balanceo de carga por si solo entre varios switch por que no solo utiliza una mac virtual sino varias de acuerdo al número de router dentro del grupo GLBP las ventajas se detallan en la tabla 3.3.

Tabla 3-3 *Comparación GLBP Y HSRP.*

GLBP	HSRP
Utiliza solo un grupo para realizar el balanceo	Utiliza varios grupos para tratar de distribuir la carga
Maneja solo una dirección virtual.	Maneja varias direcciones virtuales.
Fácil administración de protocolo por el hecho de tener menos configuración.	Engorrosa administración de protocolo debido a la creación de múltiples grupos
Variedad de métodos de balanceo de carga.	El único método es el de crear múltiples direcciones virtuales.

3.1.2.3. Análisis de protocolo BGP.

El enrutamiento estará a cargo de BGP quien tendrá incluida dos contextos de enrutamiento una para la red DELOSI y otra para la red POS, se utiliza este protocolo para intercambiar prefijos tanto con los vecinos EBGP y con los vecinos IBGP, IBGP es necesario debido a que se necesita un respaldo a nivel de red para cualquiera de nuestros CPE en caso ocurra problemas en la detección por parte de GLBP, se utiliza este protocolo por las siguientes razones.

- Los IGP escogen la ruta en base a una métrica.
- BGP nos permite implementar políticas, cada prefijo maneja una serie de características llamadas atributos.
- Tiene la posibilidad de extender sus funcionalidades usando las capabilities
- Usado ampliamente por los ISP debido a su flexibilidad.
- Permite manejar las miles de rutas o network que hay en un sistema autónomo.

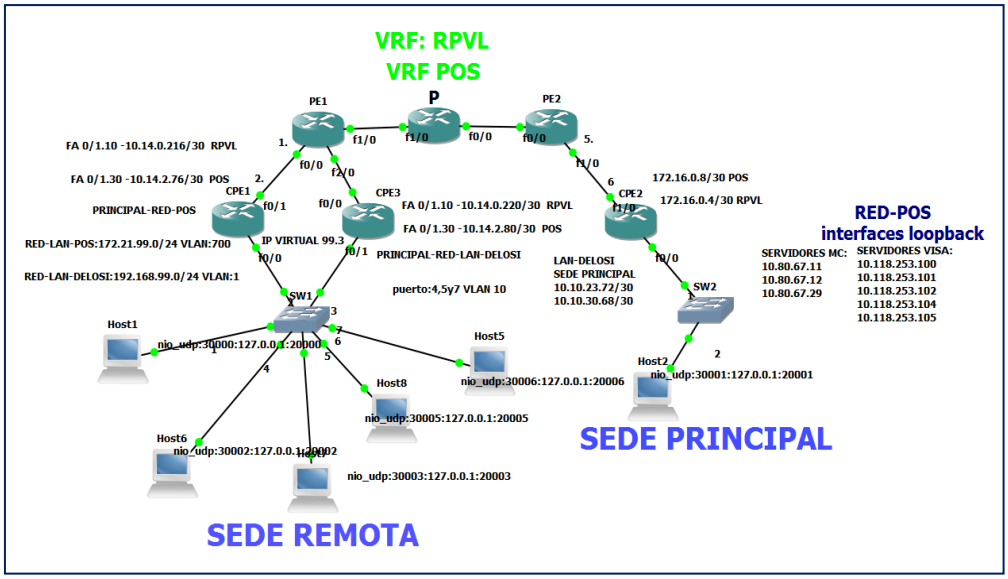
3.1.2.4. Análisis de implementación de políticas

La optimización del uso de recursos de ancho de banda estará a cargo de las políticas de marcado y políticas de asignación de recursos de acuerdo a la clase de servicio que ingrese a nuestro router, para nuestro proyecto en la red DELOSI se tiene tres clases de servicios identificados con el campo de servicio diferenciado del encabezado IP con el valor de CS1, CS2 y CS5. En la red POS solo se tiene la clase de servicio CS2, todas estas políticas deben configurarse en la dirección saliente a la interfaz WAN de los router CPE.

3.1.2.5. Análisis de topología

La figura 3.1 muestra la topología a implementar, el cual refleja la sede remota que está compuesta por red de DELOSI y la red de POS de los dispositivos datafonos que tienen salida a la nube MPLS mediante dos routers, donde el tráfico de cada red de la sede pasa a través de su respectivo router habiendo así una distribución de carga y actuando cada router como el respaldo del otro, esto gracias a GLBP. Ambas redes son independientes y están aisladas debido al uso de VRF, siendo eso un objetivo.

La red mpls de claro simulada en gns3 no se detallara en este trabajo, solo es utilizado como medio demostrativo y tratar de asemejar la simulación a un escenario real, siendo solo materia de estudio los CPE de lado remoto.



Fuente: Creación propia

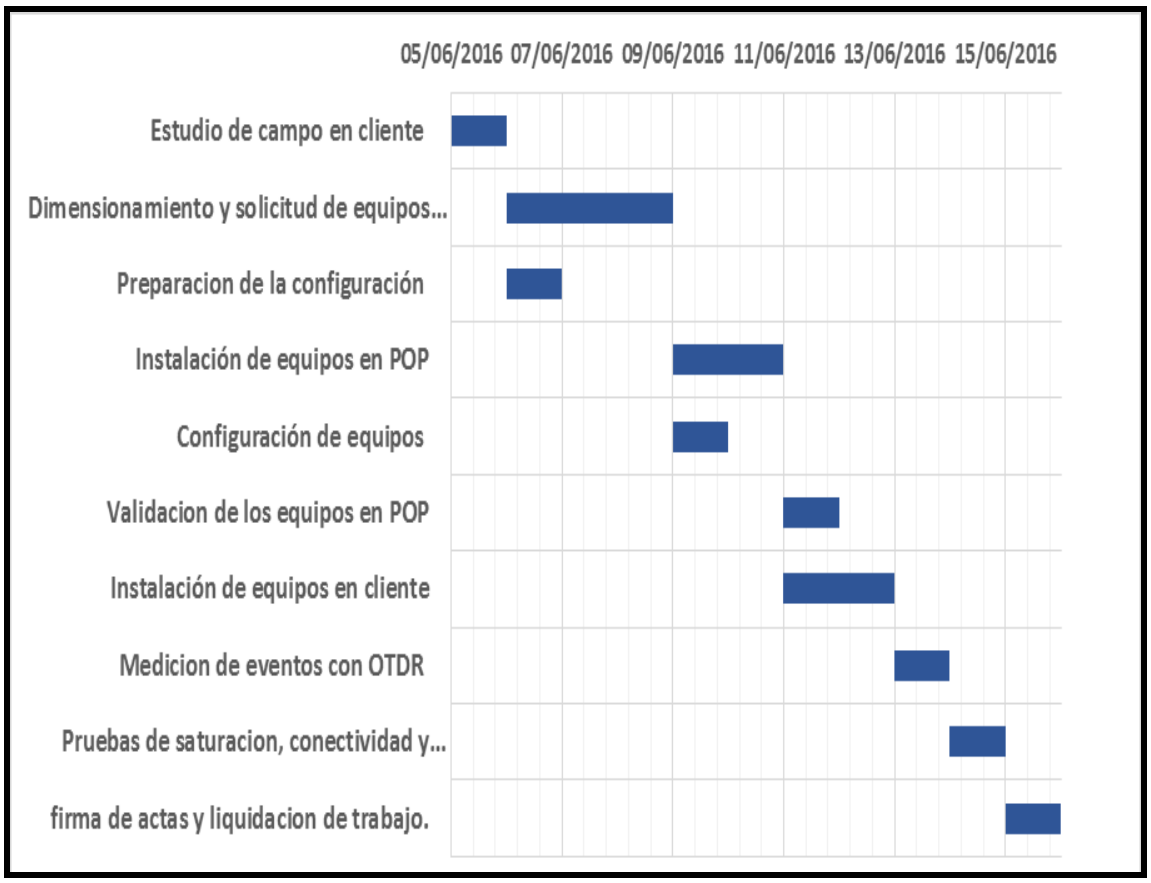
Figura 3.1 Topología simulada

3.1.3 Plan de implementación.

- Se llevaron a cabo un conjunto de actividades coordinadas y controladas, con fechas de inicio y final, llevadas a cabo para conseguir el objetivo, que es la simulación e implementación de una VPN de acuerdo con requerimientos especificados por "Delosi", incluyendo restricciones de tiempo, costo y recursos.
- Las actividades son las siguientes:
- Estudio de campo en cliente: Se realiza una visita en las instalaciones de DELOSI para dimensionar el cableado, verificar la disponibilidad de tomas de corriente, determinación de instalación de gabinetes si no hay espacio en rack existente.
- Dimensionamiento y solicitud de equipos: Esta etapa consta en determinar los equipos a instalar de acuerdo a los estudios de campo, que incluye el modelo de router, tipo de convertidores de medio, medida de jumper y clave patch corp, tipo de gabinete. Luego se realiza la solicitud de equipos a CLARO y la solicitud de materiales a almacén de ente ejecutador.
- Preparación de configuración: Mediante el requerimiento descritos en la sección 3.1.1 "Requerimientos de ancho de banda "y el plan de direccionamiento descrito en la sección 3.2.1.2 "Plan de direccionamiento" se realiza la plantilla de configuración.

- Instalación de equipos en POP (punto de presencia): Se instala el jumper de fibra óptica y cable UTP desde los recursos asignados hacia los ODF.
- Configuración de equipos: Se realiza la carga de plantilla a los dos router, verificando que no se borre de la memoria.
- Validación de equipos en POP: Se simula un escenario cliente en POP para validar recursos asignados en switch de agregación y router PE, también de los convertidores de medios y jumper a llevar a “Delosi”
- Instalación de equipos en cliente: Se realiza el montaje del gabinete y estabilizadores, para posteriormente montar sobre ello los media converter y router.
- Medición de eventos con OTDR: Para validar un óptimo desempeño de infraestructura de cableado de fibra óptica se determina la atenuación en los empalmes, conectores, y la potencia de recepción y verificar que este dentro de los márgenes.
- Pruebas de saturación, conectividad y elaboración de check-list: Se valida que el ancho de banda de las clases de servicio sean los solicitados, y haiga conectividad hacia la sede principal, realizando a su vez captura de pruebas de las mismas para la elaboración de check-list.
- Firma de actas y liquidación de trabajo.

La figura 3.2 refleja el diagrama de *Gantt* del antes descrito:



Fuente: Hecho por el autor de este trabajo.

Figura 3.2 Diagrama de Ganntt

En la Figura 3-2 detalla las actividades realizadas con sus respectivos periodos de duración, como podrá notarse no existe simultaneidad en la elaboración de ciertas actividades y otras son dependientes de otras en su proceso de ejecución.

3.1.4 Justificación Económica.

El presente proyecto de ingeniería que se presenta frente a una solución antigua (LPL), no solo se sustenta debido a las bondades técnicas mencionadas en el desarrollo de esta investigación, sino que también se sostiene económicamente como se verá a continuación.

Las líneas privadas locales son enlaces punto a punto; porque es transparente, dedicado, privada y exclusivo para sus comunicaciones, ya que dispone del ancho de banda del enlace total contratado. Esto genera que sus costos son superiores a los de una RPV (VPN), donde los medios en la nube MPLS son compartidos por el tráfico de múltiples RPVs, y proporcionan casi los mismos tiempos de retardo que LPL, reduciendo así las tarifas al cliente final.

Este beneficio permite que el servicio sea más rentable y que los servicios de RPV contratados se puedan añadir a otros, como las de líneas troncales IP, etc.

La tabla 3.4, 3.5, 3.6 y 3.7 describen la comparación de costos entre LPL y RPV para los ancho de banda empleados en este proyecto.

Para la RED RPVL (DELOSI) los precios se obtienen por clase de servicio para un ancho de banda de 512kbps en Cos5 es $217.98, para CoS2 con 1024kbps es $ 237.48, para CoS1 con 512kbps es $166.11 dando $621.57 para el ancho de banda total. Se toma en cuenta un horizonte de tres años en base al tiempo de contrato. Tanto los costos de instalación como los de acceso son pagos que se hacen una sola vez.

Tabla 3-4 *Costos de servicios LPL para RED POS*

LPL para RED POS			
AÑO	2016	2017	2018
DETALLE DE EGRESOS			
COSTO DE B/W 64kbps anual	$4762.68	$4762.69	$4762.70
COSTO DE ACCESO	-	-	-
COSTO DE INSTALACIÓN	$991.6	-	-
TOTAL EGRESOS ANUAL	$5754.28	$4762.69	$4762.69

TOTAL 1: 5754.28+ 4762.69+ 4762.69 = 15278.66

Tabla 3-5 *Costos de servicios RPV para RED POS*

RPV para RED POS			
AÑO	2016	2017	2018
DETALLE DE EGRESOS			
COSTO DE B/W 64kbps anual	$1002.12	$1002.13	$1002.14
COSTO DE ACCESO	$991.6	-	-
COSTO DE INSTALACIÓN	$767.0	-	-
TOTAL EGRESOS ANUAL	$1974.88	$1002.13	$1002.13

TOTAL 2: 1974.88 + 1002.13 + 1002.13= 3979.14
TOTAL 1 – TOTAL 2= 11299.52

Tabla 3-6 *Costos de servicios LPL para red "Delosi"*

LPL para RED DELOSI			
AÑO	2016	2017	2018
DETALLE DE EGRESOS			
COSTO DE B/W 2048kbps anual	$14352	$14353	$14354
COSTO DE ACCESO	-	-	-
COSTO DE INSTALACIÓN	$991.6	-	-
TOTAL EGRESOS ANUAL	$15343.6	$14353	$14353

TOTAL 1= 15343.6 + 14353 + 14353 = 44049.6

Tabla 3-7 *Costos de servicios RPV para RED DELOSI (RPVL)*

RPV para RED DELOSI			
AÑO	**2016**	**2017**	**2018**
DETALLE DE EGRESOS			
COSTO DE B/W 2048kbps anual	$7458.84	$7458.85	$7458.86
COSTO DE ACCESO	$910.69		
COSTO DE INSTALACIÓN	$767.0		
TOTAL EGRESOS ANUAL	$9136.53	$7458.85	$7458.85

TOTAL 2= 9136.53 + 7458.85 + 7458.85 = 24054.23

TOTAL 1 - TOTAL 2=19995.37

Como se puede notar hay una diferencia significativa respecto a los servicios de LPL y RPV esto debido a que los pagos mensuales son menores en el RPV esto optimiza los recursos asignados a os servicios contratados por DELOSI, siendo así una alternativa rentable a implementar.

3.2 DISEÑO, SIMULACIÓN E IMPLEMENTACIÓN DEL SISTEMA

3.2.1 Diseño.

El diseño está orientado a la topología física y lógica de la sede remota, también al plan de direccionamiento.

3.2.1.1. Diseño de topología:

En esta sección se dispondrá de una topología simple a nivel físico pero complejo a nivel lógico.

A nivel WAN se dispone de una topología point-to-point hacia la principal, que es donde se concentra todos los servidores y por ende solo necesita un

enlace hacia dicha sede por lo que la topología será como la que se muestra en la figura 3.3

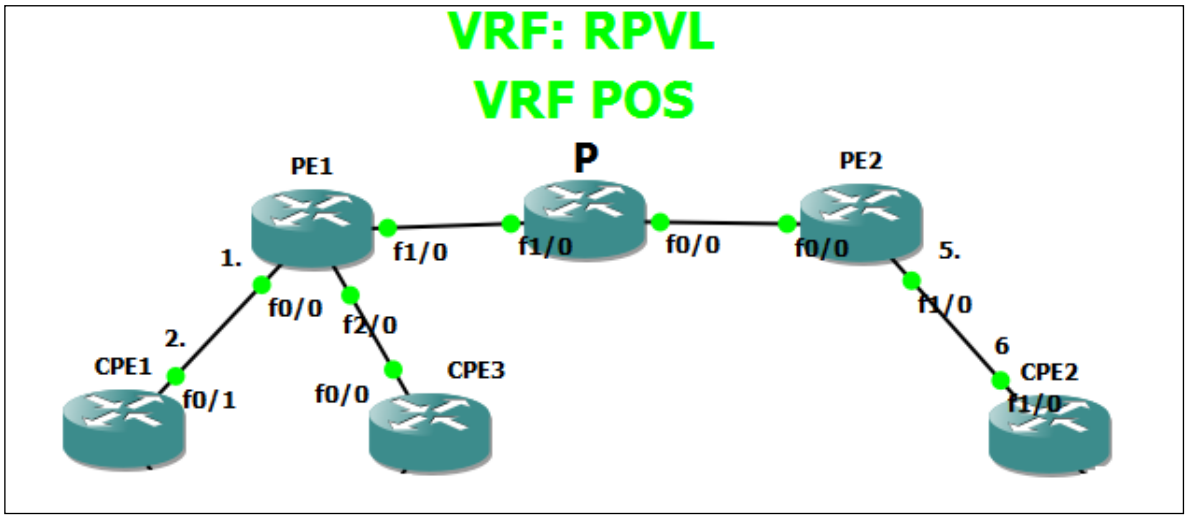


Figura 3.3 Topología POINT-TO-POINT

A nivel LAN se utiliza una topología en capas de núcleo contraído, donde la capa de núcleo está formada por los router CPE y la capa de acceso solo por un switch, pero cabe recalcar que solo se utiliza un switch porque solo es usado de manera demostrativo y la compañía DELOSI podría realizar unas mejoras en cuanto a la disponibilidad en la capa de conmutación por parte de los switch, la FIGURA 3.4 muestra esta topología.

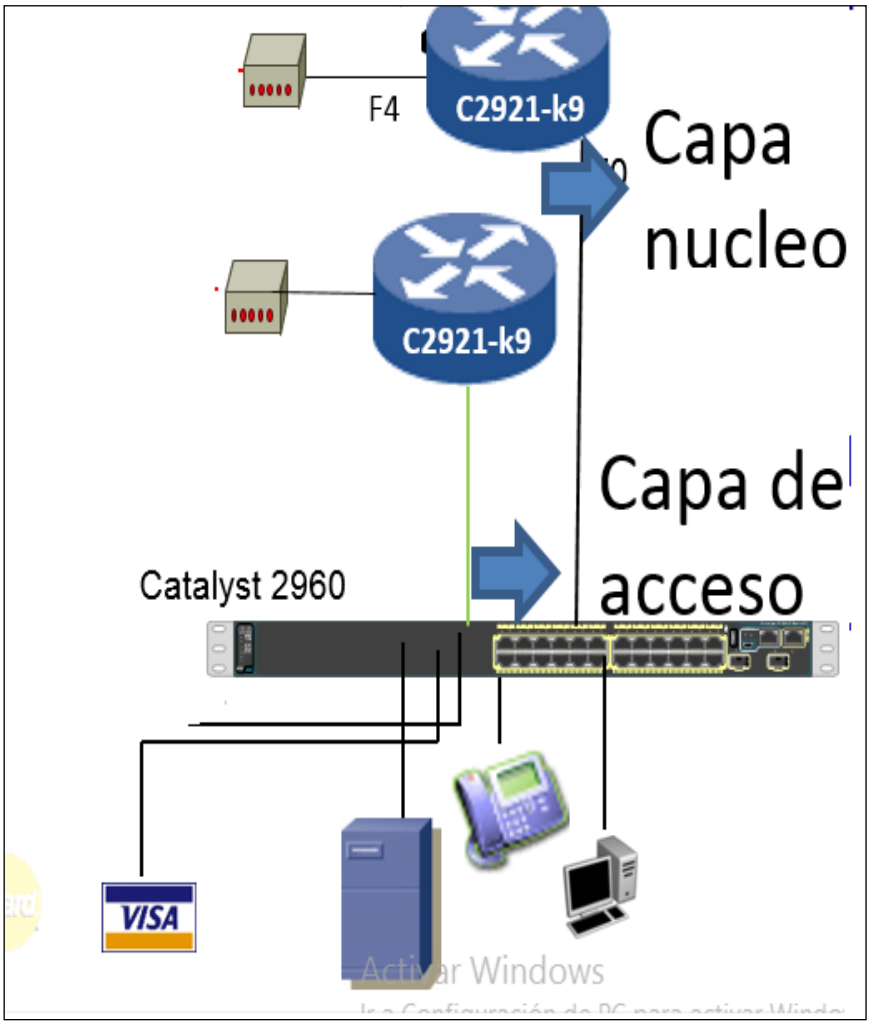


Figura 3.4 Topología en capas de núcleo contraído

3.2.1.2. Plan de direccionamiento

Primero se realizará el direccionamiento concerniente a nuestra topología para ello tenemos la siguiente tabla de direccionamiento TABLA 3-8.

Tabla 3-8 *Plan de direccionamiento.*

DISPOSITIVO	INTERFACE	DIRECCION	DEFAULT
ROUTER CPE1	FasEthernet 0/1.10	10.14.0.218	N/A
	FasEthernet 0/1.30	10.14.2.78	N/A
	FasEthernet 0/0	192.168.99.1	N/A
	FasEthernet 0/0.700	172.21.99.1	N/A
	Loopback 0	10.232.45.54	N/A
ROUTER CPE3	FasEthernet 0/0.10	10.14.0.222	N/A
	FasEthernet 0/0.30	10.14.2.82	N/A
	FasEthernet 0/1	192.168.99.2	N/A
	FastEthernet0/1.700	172.21.99.2	N/A
	Loopback0	10.232.45.55	N/A
ROUTER PE1	FastEthernet0/0.10	10.14.0.217	N/A
	FastEthernet0/0.30	10.14.2.77	N/A
	FastEthernet2/0.10	10.14.0.221	N/A
	FastEthernet2/0.30	10.14.2.81	N/A
	Loopback0	1.1.1.1	N/A
HOST1	Vlan 1	192.168.99.4	192.168.99.3
HOST6	Vlan 1	192.168.99.5	192.168.99.3
HOST5	Vlan 1	192.168.99.6	192.168.99.3
HOST7	Vlan 700	172.21.99.4	172.21.99.3
HOST7	Vlan 700	172.21.99.5	172.21.99.3

3.2.2 Simulación

3.2.2.1 Requisitos de los elementos a utilizar.

Los routers que se utilizan en esta simulación son routers de servicios integrados (ISR) Cisco 2691 con IOS de Cisco versión C2691-ADcompleto.BIN, pero para la implementación se utilizó los router 2901 con IOS de Cisco versión c2900-universalk9-mz.SPA.153-3.M5.bin. Los switches que se utilizan son Cisco Catalyst 2960s con IOS de Cisco versión 15.0 (2) (imagen de lanbasek9). Se pueden utilizar otros routers, switches y otras versiones del IOS de Cisco. Según el modelo y la versión de IOS de Cisco, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en la simulación, para la simulación de los PE se utilizó el router 7200 con IOS c7200-p-mz.124-8a.image, los servidores MasterCard, visa y 3.2.2.2

- Routers (Cisco 2691 con IOS de Cisco C2691-ADcompleto.BIN o similar).
- Routers (Cisco7200 con IOS c7200-p-mz.124-8a.image o similar).
- switches (Cisco 2960 con IOS de Cisco versión 15.0 (2), imagen lanbasek9 o similar).
- 5 computadoras (que serán simuladas con VPCS).
- SIMULADOR GNS3 versión 1.4.6.

3.2.2.2 CONFIGURACIÓN DE DISPOSITIVOS.

PARTE 1: : Configurar los parámetros básicos de dispositivos.

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos del router, como las direcciones IP de las interfaces, el routing, el acceso

a los dispositivos y las contraseñas como aparecen en la FIGURA 3.5, 3.6, 3.7, 3.8 3.9, 3.10, 3.11, 3.12.

ROUTER CPE1:

```
!
interface Loopback0
 description LOOPBACK DE GESTION
 ip address 10.232.45.54 255.255.255.255
!
```

Figura 3.5 Configuración de interfaces**.**

```
!
interface FastEthernet0/1.10
 description Enlace WAN RPVL ACCESO 2 MBPS CID:504172
 encapsulation dot1Q 794
 ip address 10.14.0.218 255.255.255.252
!
interface FastEthernet0/1.30
 description ENLACE WAN 64 KBPS - POS CID:3818639
 encapsulation dot1Q 2763
 ip vrf forwarding 700
 ip address 10.14.2.78 255.255.255.252
 no ip redirects
!
interface FastEthernet0/1.700
 encapsulation dot1Q 700
!
interface FastEthernet1/0
 no ip address
```

Figura 3.6 Configuración de interfaces.

```
interface FastEthernet0/0
 description Interface LAN - DELOSI Sede KFC PARDO
 ip address 192.168.99.1 255.255.255.0
 duplex auto
 speed auto
```

Figura 3.7 Configuración de interfaces.

ROUTER CPE3:

```
!
interface FastEthernet0/0.10
 encapsulation dot1Q 794
 ip address 10.14.0.222 255.255.255.252
!
interface FastEthernet0/0.30
 encapsulation dot1Q 2763
 ip vrf forwarding 700
 ip address 10.14.2.82 255.255.255.252
!
```

Figura 3.8 Configuración de interfaces.

```
!
interface Loopback0
 description LOOPBACK DE GESTION
 ip address 10.232.45.55 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
```

Figura 3.9 Configuración de interfaces.

```
!
interface FastEthernet0/1
 ip address 192.168.99.2 255.255.255.0
 duplex auto
 speed auto
 glbp 1 ip 192.168.99.3
 glbp 1 priority 150
 glbp 1 preempt
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
!
interface FastEthernet0/1.700
 description LAN-POS
 encapsulation dot1Q 700
 ip vrf forwarding 700
 ip address 172.21.99.2 255.255.255.0
```

Figura 3.10 Configuración de interfaces.

PE1

```
!
interface FastEthernet1/0
 ip address 10.0.0.2 255.255.255.252
 duplex half
 mpls ip
!
interface FastEthernet2/0
 no ip address
 duplex half
!
interface FastEthernet2/0.10
 description ENLACE-BACKUP-WAN-RPVL
 encapsulation dot1Q 794
 ip vrf forwarding site1
 ip address 10.14.0.221 255.255.255.252
!
interface FastEthernet2/0.30
 description ENLACE-BACKUP-WAN-POS
 encapsulation dot1Q 2763
 ip vrf forwarding site1pos
 ip address 10.14.2.81 255.255.255.252
 --More--
```

Figura 3.11 Configuración de interfaces.

```
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex half
!
interface FastEthernet0/0.10
 description ENLACE-WAN-Rpvl
 encapsulation dot1Q 794
 ip vrf forwarding site1
 ip address 10.14.0.217 255.255.255.252
!
interface FastEthernet0/0.30
 description ENLACE-WAN-POS
 encapsulation dot1Q 2763
 ip vrf forwarding site1pos
 ip address 10.14.2.77 255.255.255.252
!
```

Figura 3.12 Configuración de interfaces.

PARTE 2: *CREAN DE* VRF.

Creamos la instancia de enrutamiento 700 para la red POS como se muestra en la figura 3.13. Cada VRF está compuesta por una tabla de enrutamiento IP.

PARA LOS ROUTER CPE1 Y CPE3:

```
!
!
ip vrf 700
!
!
```

Figura 3.13 Creación de VRF

PARTE 3: FILTRADO DE PREFIJOS.

En esta parte se realizara la selección de rutas que se ingresaran en la tabla BGP y las rutas que se enviaran al vecino BGP que este caso es el PE todo esto para evitar loops de datos y destinos que innecesariamente se instalarían en la tabla BGP y posteriormente en la tabla de enrutamiento, para se harán uso de los Prefix Lists que son introducidos en BGP porque son una forma eficiente de filtrado muy rápido porque buscan el prefijo de las direcciones dadas por el administrador y la búsqueda es muy rápida. Los Prefix Lists se pueden editar. La modificación de ACLs es bastante compleja. A demás son fáciles de configurar y usar, pero antes de aplicarlos es necesario definir el criterio del Prefix List. La FIGURA 3.14 y 3.15 muestra la configuración de IP PREFIX-LIST una herramienta de coincidencia más versátil que las listas de acceso las direcciones ip que aparecen son las redes de nuestra LAN y las redes de la sede principal.

ROUTER CPE1:

```
ip prefix-list Red_LAN_DATOS seq 10 permit 192.168.99.0/24
ip prefix-list Red_LAN_DATOS seq 15 permit 10.232.45.54/32
!
ip prefix-list Red_POS seq 10 permit 172.21.99.0/24
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
ip prefix-list Redes_ONLY_POS seq 10 permit 10.80.67.10/32
ip prefix-list Redes_ONLY_POS seq 11 permit 10.80.67.11/32
ip prefix-list Redes_ONLY_POS seq 12 permit 10.80.67.12/32
ip prefix-list Redes_ONLY_POS seq 13 permit 10.80.67.29/32
ip prefix-list Redes_ONLY_POS seq 20 permit 10.118.253.99/32
ip prefix-list Redes_ONLY_POS seq 21 permit 10.118.253.100/32
ip prefix-list Redes_ONLY_POS seq 22 permit 10.118.253.101/32
ip prefix-list Redes_ONLY_POS seq 23 permit 10.118.253.102/32
ip prefix-list Redes_ONLY_POS seq 24 permit 10.118.253.104/32
ip prefix-list Redes_ONLY_POS seq 25 permit 10.118.253.105/32
ip prefix-list Redes_ONLY_POS seq 26 permit 10.10.1.0/30
access-list 1 permit 192.168.10.0 0.0.0.255
!
```

Figura 3.14 Creación de listas de prefijos.

ROUTER CPE3:

```
!
ip prefix-list Red_LAN_DATOS seq 10 permit 192.168.99.0/24
ip prefix-list Red_LAN_DATOS seq 15 permit 10.232.45.54/32
!
ip prefix-list Red_POS seq 10 permit 172.21.99.0/24
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
ip prefix-list Redes_ONLY_POS seq 10 permit 10.80.67.10/32
ip prefix-list Redes_ONLY_POS seq 11 permit 10.80.67.11/32
ip prefix-list Redes_ONLY_POS seq 12 permit 10.80.67.12/32
ip prefix-list Redes_ONLY_POS seq 13 permit 10.80.67.29/32
ip prefix-list Redes_ONLY_POS seq 20 permit 10.118.253.99/32
ip prefix-list Redes_ONLY_POS seq 21 permit 10.118.253.100/32
ip prefix-list Redes_ONLY_POS seq 22 permit 10.118.253.101/32
ip prefix-list Redes_ONLY_POS seq 23 permit 10.118.253.102/32
ip prefix-list Redes_ONLY_POS seq 24 permit 10.118.253.104/32
ip prefix-list Redes_ONLY_POS seq 25 permit 10.118.253.105/32
ip prefix-list Redes_ONLY_POS seq 26 permit 10.10.1.0/30
access-list 1 permit 172.21.99.0 0.0.0.255
!
```

Figura 3.15 Creación de listas de prefijos.

PARTE 4: CREACION DE COINCIDENCIA Y APLICACIÓN DE POLITICAS.

Para ello se utilizara el comando route-map que tiene muchas aplicaciones ya sea para ajustar los atributos sobre los prefijos que coinciden en este contexto, la FIGURA 3.16 Y 317 muestran cómo aplicar los criterios de coincidencia y que política aplicar para esa coincidencia, en la parte 5 se verá como estos route-map son invocados dentro de la configuración de BGP.

ROUTER CPE1:

```
!
route-map SET_POS_COMM permit 10
 description Anuncia a la RED POS
 match ip address prefix-list Red_POS
!
route-map From_VPN_POS deny 10
 description denegacion de Redes Lans y Redes Lan internas
 match ip address prefix-list Red_POS
!
route-map From_VPN_POS permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_ONLY_POS
!
route-map From_VPN_DATOS deny 10
 description denegacion de Redes Lans y Redes Lan internas
 match ip address prefix-list Red_LAN_DATOS
!
route-map From_VPN_DATOS permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
!
```

Figura 3.16 Creación de mapas de rutas.

ROUTER CPE3:

```
!
route-map SET_POS_COMM permit 10
 description Anuncia a la RED POS
 match ip address prefix-list Red_POS
!
route-map From_VPN_POS deny 10
 description denegacion de Redes Lans y Redes Lan internas
 match ip address prefix-list Red_POS
!
route-map From_VPN_POS permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_ONLY_POS
!
route-map From_VPN_DATOS deny 10
 description denegacion de Redes Lans y Redes Lan internas
 match ip address prefix-list Red_LAN_DATOS
!
route-map From_VPN_DATOS permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
!
!
```

Figura 3.17 Creación de mapas de rutas.

PARTE 5: CONFIGURACIÓN DE BGP PARA EL SERVICIO DE RPVL (VPN-local) y POS.

El protocolo de Gateway de frontera BGP, permite la comunicación entre dominios por lo que su implementación debe ser únicamente en las fronteras de una Red. Para la conexión de sitios locales con sitios remotos mediante VPNs, este protocolo es muy usual ya que además permite ser trabajado como protocolo de interiores y se utiliza para la comunicación específica entre dispositivos de frontera.

En esta parte se configurara EBGP entre el PE1 con el sistema autónomo 100 y CPE1 con el sistema autónomo 64516 para que las rutas de la redes LAN de delosi y POS sean publicadas hacia la sede principal y a su vez recibir prefijos

de red de la sede principal, claro utilizando políticas basadas en atributos. Se configuran dos contextos de enrutamiento BGP una para la red RPVL y otra para la red POS. Las FIGURAS 3.18 y 3.19 muestran el contexto de enrutamiento para la tabla de enrutamiento tradicional allí está incluida dos vecindades BGP una con el PE y otra con el CPE3 de backup, esta sesión adicional es para asegurar que cuando ocurra un problema a nivel de capa 3 en el enlace WAN hacia el proveedor los paquetes que están destinados hacia CPE1 desde la red LAN sean redireccionados hacia CPE3 y puedan salir hacia la SEDE PRINCIPAL y como se mencionó en la parte 4, las políticas de filtrado son invocados en esta sección mediante el comando route-map From_VPN_DATOS en la dirección entrante para que tenga efecto sobre los prefijos que son publicados por el PE.

ROUTER CPE1:

```
!
router bgp 64516
 bgp log-neighbor-changes
 neighbor WAN_CLIENTE peer-group
 neighbor WAN_CLIENTE remote-as 100
 neighbor LAN-CLIENTE peer-group
 neighbor LAN-CLIENTE remote-as 64516
 neighbor 10.14.0.217 peer-group WAN_CLIENTE
 neighbor 10.14.0.217 description Enlace WAN - RPVL Cliente
 neighbor 192.168.99.2 peer-group LAN-CLIENTE
 neighbor 192.168.99.2 description IBGB-LAN
 !
 address-family ipv4
  neighbor WAN_CLIENTE send-community both
  neighbor WAN_CLIENTE soft-reconfiguration inbound
  neighbor WAN_CLIENTE route-map From_VPN_DATOS in
  neighbor LAN-CLIENTE soft-reconfiguration inbound
  neighbor 10.14.0.217 activate
  neighbor 192.168.99.2 activate
  no auto-summary
  no synchronization
  network 10.232.45.54 mask 255.255.255.255
  network 192.168.99.0
 exit-address-family
 !
```

Figura 3.18 Configuración de BGP

ROUTER CPE3:

```
!
router bgp 64516
 bgp log-neighbor-changes
 neighbor WAN-CLIENTE peer-group
 neighbor WAN-CLIENTE remote-as 100
 neighbor LAN-CLIENTE-BACKUP peer-group
 neighbor LAN-CLIENTE-BACKUP remote-as 64516
 neighbor 10.14.0.221 peer-group WAN-CLIENTE
 neighbor 10.14.0.221 description Enlace WAN-BACKUP-RPVL
 neighbor 192.168.99.1 peer-group LAN-CLIENTE-BACKUP
 neighbor 192.168.99.1 description IBGP-LAN-backup
 !
 address-family ipv4
  neighbor WAN-CLIENTE send-community both
  neighbor WAN-CLIENTE soft-reconfiguration inbound
  neighbor WAN-CLIENTE route-map From_VPN_DATOS in
  neighbor LAN-CLIENTE-BACKUP soft-reconfiguration inbound
  neighbor 10.14.0.221 activate
  neighbor 192.168.99.1 activate
  no auto-summary
  no synchronization
  network 10.232.45.55 mask 255.255.255.255
  network 192.168.99.0
 exit-address-family
 !
```

Figura 3.19 Configuración de BGP

Se crea como se muestra en la FIGURA 3.20 Y 3.21 un contexto de enrutamiento para la VRF 700 que contiene las rutas para la red POS.

ROUTER CPE1:

```
 !
 address-family ipv4 vrf 700
  neighbor WAN_RPVL_POS peer-group
  neighbor WAN_RPVL_POS remote-as 100
  neighbor WAN_RPVL_POS send-community both
  neighbor WAN_RPVL_POS soft-reconfiguration inbound
  neighbor WAN_RPVL_POS route-map From_VPN_POS in
  neighbor WAN_RPVL_POS route-map SET_POS_COMM out
  neighbor 10.14.2.77 peer-group WAN_RPVL_POS
  neighbor 10.14.2.77 description Enlace WAN VPN POS
  neighbor 10.14.2.77 activate
  neighbor 172.21.99.2 remote-as 64516
  neighbor 172.21.99.2 activate
  neighbor 172.21.99.2 soft-reconfiguration inbound
  no synchronization
  network 172.21.99.0 mask 255.255.255.0
 exit-address-family
!
```

Figura 3.20 Configuración de BGP para VRF 700

ROUTER CPE3:

```
!
address-family ipv4 vrf 700
 neighbor WAN_RPVL_POS peer-group
 neighbor WAN_RPVL_POS remote-as 100
 neighbor WAN_RPVL_POS send-community both
 neighbor WAN_RPVL_POS soft-reconfiguration inbound
 neighbor WAN_RPVL_POS route-map From_VPN_POS in
 neighbor WAN_RPVL_POS route-map SET_POS_COMM out
 neighbor 10.14.2.81 peer-group WAN_RPVL_POS
 neighbor 10.14.2.81 description ENLACE wan BACKUP-POS
 neighbor 10.14.2.81 activate
 neighbor 172.21.99.1 remote-as 64516
 neighbor 172.21.99.1 activate
 neighbor 172.21.99.1 soft-reconfiguration inbound
 no synchronization
 network 172.21.99.0 mask 255.255.255.0
exit-address-family
!
```

Figura 3.21 Configuración de BGP para VRF 700

PARTE 6: CONFIGURACIÓN DE PROTOCOLO DE REDUNDANCIA DE PRIMER SALTO GLBP.

ROUTER CPE1:

```
!
interface FastEthernet0/0
 description Interface LAN - DELOSI Sede KFC PARDO
 ip address 192.168.99.1 255.255.255.0
 duplex auto
 speed auto
 glbp 1 ip 192.168.99.3
 glbp 1 preempt
!
interface FastEthernet0/0.700
 description LAN POS CID:3818639
 encapsulation dot1Q 700
 ip vrf forwarding 700
 ip address 172.21.99.1 255.255.255.0
 glbp 2 ip 172.21.99.3
 glbp 2 priority 150
 glbp 2 preempt
!
```

Figura 3.22 Configuración de GLBP

La figura 3-22 muestra como el router CPE1 es el router principal para la red POS debido a que tiene la prioridad más alta y es backup para la red de DELOSI.

ROUTER CPE3

```
!
interface FastEthernet0/1
 ip address 192.168.99.2 255.255.255.0
 duplex auto
 speed auto
 glbp 1 ip 192.168.99.3
 glbp 1 priority 150
 glbp 1 preempt
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
!
interface FastEthernet0/1.700
 description LAN-POS
 encapsulation dot1Q 700
 ip vrf forwarding 700
 ip address 172.21.99.2 255.255.255.0
 glbp 2 ip 172.21.99.3
 glbp 2 preempt
!
```

Figura 3.23 Configuración de GLBP

La figura 3-23 muestra como el router CPE3 es el router principal para la red de DELOSI debido a que tiene la prioridad más alta y es backup para la red POS

3.2.3 Implementación

3.2.3.1 Pasos seguidos para la implementación

- Los recursos en el PE ya están habilitados, como la creación de VRF con los RD, el enrutamiento BGP y los servidores TACACS están operativos.
- Se realiza una validación del servicio en el punto de presencia (POP) con los convertidores de medios, jumper de fibra óptica y nuestro router ya configurado para descartar problemas en el PE y switch metro Ethernet en caso haya un problema cuando se lleve el router a la sede de “Delosi” y deducir que el problema este en el medio de planta externa.

- Una vez realizada la validación del servicio con nuestros equipos, se procedió a realizar la instalación en el gabine del cliente por personal encargado.
- Se realiza las pruebas en presencia del personal responsable para asegurarle que el servicio está operativo y se sugirió que realice sus propias pruebas así como la saturación por tipo de servicio.

3.2.3.2 Configuración final en router de sede remota:

Para la implementación se adiciono configuración adicional como.

- La agregación de comandos para la autenticación con servidores tacacs,
- Comandos para la habilitación de envió y almacenamiento de mensajes de SYSLOG.

Solo se muestra la configuración del router principal, debido a que el router de backup tiene una configuración muy parecida.

```
Current configuration: 8735 bytes
!
! Last configuration change at 09:55:22 GMT Tue Jan 19 2016 by p.inchicsana756
Version 15.3
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
service password-encryption
!
hostname rDELOSI_PARDO
!
boot-start-marker
```

```
boot-end-marker
!
aqm-register-fnf
!
logging buffered 9000
enable secret 5 $1$yIIX$xI.TDb37Wf.4ySX2KrJNu0
!
aaa new-model
!
aaa authentication login default group tacacs+ enable
aaa authentication enable default group tacacs+ enable
aaa authorization commands 1 default group tacacs+ none
aaa authorization commands 15 default group tacacs+ none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting network default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
!
aaa session-id common
clock timezone GMT -5 0
!
ip vrf 700
description VPN POS
rd 64516:700
!
no ip domain lookup
ip name-server 200.24.191.11
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
license udi pid C881-K9 sn FJC1943E37J
!
class-map match-any qos2_vrf700
match ip dscp cs2
class-map match-any qos5
match ip dscp cs5
match ip dscp cs6
class-map match-any qos1
```

match ip dscp cs1
class-map match-any qos2
match ip dscp cs2
class-map match-any P2
match ip dscp cs2
match access-group name qos2
class-map match-any P5
match ip dscp cs5
match access-group name qos5
class-map match-any P2_vrf700
match ip dscp cs2
match access-group name qos2_vrf700
!
policy-map SetDspLan
class P5
set ip dscp cs5
class P2
set ip dscp cs2
class class-default
set ip dscp cs1
policy-map SetDscpLan_vrf700
class P2_vrf700
set ip dscp cs2
class class-default
set ip dscp cs2
policy-map wan_vrf700
class qos2_vrf700
bandwidth 64
police 64000 12000 24000 conform-action transmit exceed-action drop violate-action drop
class class-default
fair-queue
policy-map wan
class qos5
priority 512
police 512000 96000 192000 conform-action transmit exceed-action drop violate-action drop
class qos2
bandwidth 1024
police 1024000 192000 384000 conform-action transmit exceed-action set-dscp-transmit cs1

```
violate-action set-dscp-transmit cs1
class qos1
bandwidth 512
class class-default
fair-queue
policy-map Shape2048
class class-default
shape average 2049000
service-policy wan
policy-map Shape64_vrf700
class class-default
shape average 65000
service-policy wan_vrf700
policy-map SetDscpLan
class P5
set ip dscp cs5
class P2
set ip dscp cs2
class class-default
set ip dscp cs1
!
i interface Loopback0
 description LOOPBACK DE GESTION
 ip address 10.232.45.54 255.255.255.255
!
Interface GigaEthernet0/0
 description Interface LAN - DELOSI Sede KFC PARDO
 ip address 192.168.99.1 255.255.255.0
 duplex auto
 speed auto
 glbp 1 ip 192.168.99.3
 glbp 1 preempt
!
interface GigaEthernet0/0.700
 description LAN POS CID:3818639
 encapsulation dot1Q 700
 ip vrf forwarding 700
 ip address 172.21.99.1 255.255.255.0
 glbp 2 ip 172.21.99.3
 glbp 2 priority 150
 glbp 2 preempt
```

```
!
interface GigaEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigaEthernet0/1.3
!
interface GigaEthernet0/1.10
 description Enlace WAN RPVL ACCESO 2 MBPS CID:504172
 encapsulation dot1Q 794
 ip address 10.14.0.218 255.255.255.252
!
interface GigaEthernet0/1.30
 description ENLACE WAN 64 KBPS - POS CID:3818639
 encapsulation dot1Q 2763
 ip vrf forwarding 700
 ip address 10.14.2.78 255.255.255.252
 no ip redirects
!

!!
router bgp 64516
 bgp log-neighbor-changes
 neighbor WAN_CLIENTE peer-group
 neighbor WAN_CLIENTE remote-as 12252
 neighbor LAN-CLIENTE peer-group
 neighbor LAN-CLIENTE remote-as 64516
 neighbor 10.14.0.217 peer-group WAN_CLIENTE
 neighbor 10.14.0.217 description Enlace WAN - RPVL Cliente
 neighbor 192.168.99.2 peer-group LAN-CLIENTE
 neighbor 192.168.99.2 description IBGB-LAN
 !
 address-family ipv4
  neighbor WAN_CLIENTE send-community both
  neighbor WAN_CLIENTE soft-reconfiguration inbound
  neighbor WAN_CLIENTE route-map From_VPN_DATOS in
  neighbor LAN-CLIENTE soft-reconfiguration inbound
  neighbor 10.14.0.217 activate
  neighbor 192.168.99.2 activate
  no auto-summary
```

```
  no synchronization
  network 10.232.45.54 mask 255.255.255.255
  network 192.168.99.0
 exit-address-family
 !
 address-family ipv4 vrf 700
  neighbor WAN_RPVL_POS peer-group
  neighbor WAN_RPVL_POS remote-as 12252
  neighbor WAN_RPVL_POS send-community both
  neighbor WAN_RPVL_POS soft-reconfiguration inbound
  neighbor WAN_RPVL_POS route-map From_VPN_POS in
  neighbor WAN_RPVL_POS route-map SET_POS_COMM out
  neighbor 10.14.2.77 peer-group WAN_RPVL_POS
  neighbor 10.14.2.77 description Enlace WAN VPN POS
  neighbor 10.14.2.77 activate
  neighbor 172.21.99.2 remote-as 64516
  neighbor 172.21.99.2 activate
  neighbor 172.21.99.2 soft-reconfiguration inbound
  no synchronization
  network 172.21.99.0 mask 255.255.255.0
 exit-address-family!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip bgp-community new-format
!
ip tacacs source-interface Loopback0
!
ip access-list extended qos2
permit ip any host 192.168.233.1
permit ip any host 192.168.233.2
permit ip any host 192.168.233.3
ip access-list extended qos2_vrf700
permit ip 172.21.99.0 0.0.0.255 any
ip access-list extended qos5
permit ip host 192.168.99.130 any
permit ip host 192.168.99.131 any
permit ip host 192.168.99.132 any
permit ip host 192.168.99.133 any
permit ip host 192.168.99.134 any
```

```
!
ip prefix-list Red_LAN_DATOS seq 10 permit 192.168.99.0/24
ip prefix-list Red_LAN_DATOS seq 15 permit 10.232.45.54/32
!
ip prefix-list Red_POS seq 10 permit 172.21.99.0/24
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
ip prefix-list Redes_ONLY_POS seq 10 permit 10.80.67.10/32
ip prefix-list Redes_ONLY_POS seq 11 permit 10.80.67.11/32
ip prefix-list Redes_ONLY_POS seq 12 permit 10.80.67.12/32
ip prefix-list Redes_ONLY_POS seq 13 permit 10.80.67.29/32
ip prefix-list Redes_ONLY_POS seq 20 permit 10.118.253.99/32
ip prefix-list Redes_ONLY_POS seq 21 permit 10.118.253.100/32
ip prefix-list Redes_ONLY_POS seq 22 permit 10.118.253.101/32
ip prefix-list Redes_ONLY_POS seq 23 permit 10.118.253.102/32
ip prefix-list Redes_ONLY_POS seq 24 permit 10.118.253.104/32
ip prefix-list Redes_ONLY_POS seq 25 permit 10.118.253.105/32
ip prefix-list Redes_ONLY_POS seq 26 permit 10.10.1.0/30
logging source-interface Loopback0
logging host 10.192.17.27
!
route-map SET_POS_COMM permit 10
description Anuncia a la RED POS
match ip address prefix-list Red_POS
!
route-map SET_DATOS_COMM permit 10
description Setear Comunidad 200 a la RED POS
match ip address prefix-list Red_LAN_DATOS
set community 12252:200
!
route-map From_VPN_POS deny 10
description denegacion de Redes Lans y Redes Lan internas
match ip address prefix-list Red_POS
!
route-map From_VPN_POS permit 20
description Permitir las demas Redes de Sedes Remotas
match ip address prefix-list Redes_ONLY_POS
!
route-map From_VPN_DATOS deny 10
description denegacion de Redes Lans y Redes Lan internas
```

```
match ip address prefix-list Red_LAN_DATOS
!
route-map From_VPN_DATOS permit 20
description Permitir las demas Redes de Sedes Remotas
match ip address prefix-list Redes_All
!
tacacs-server host 10.192.17.27
tacacs-server key 7 15220A021E2F392F293E2524040611060F
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
line con 0
password 7 063006354D08070C0A011344
no modem enable
line aux 0
line vty 0 4
session-timeout 10 output
password 7 02300D4F0A40013443580856
transport input all
scheduler allocate 20000 1000
end
```

3.2.3.3 Arquitectura final en producción de “Delosi”

Como puede observarse en la FIGURA 3.24 la sede PARDO de DELOSI ya puede disponer de los servicios que puede brindar la red MPLS de un proveedor como puede ser la adición de servicios como TRONCALES SIP sobre MPLS, INTERNET OPTIMIZADO debido a que la VPN implementada puede coexistir con muchas otras sin la necesidad de instalar router por cada servicio adicional esto gracias a VRF en los router.

El hecho de que el cliente (Empresa DELOSI) piense que su sede principal y sucursales poseen enlaces dedicados para conectarse entre sí, es uno de los objetivos principales de la implementación de conexiones VPNs entre la matriz y las agencias. Las sede remota de la compañía DELOSI pueden acceder a los distintos aplicativos que su sede Principal les pueda ofrecer por medio de conexiones VPN en MPLS.

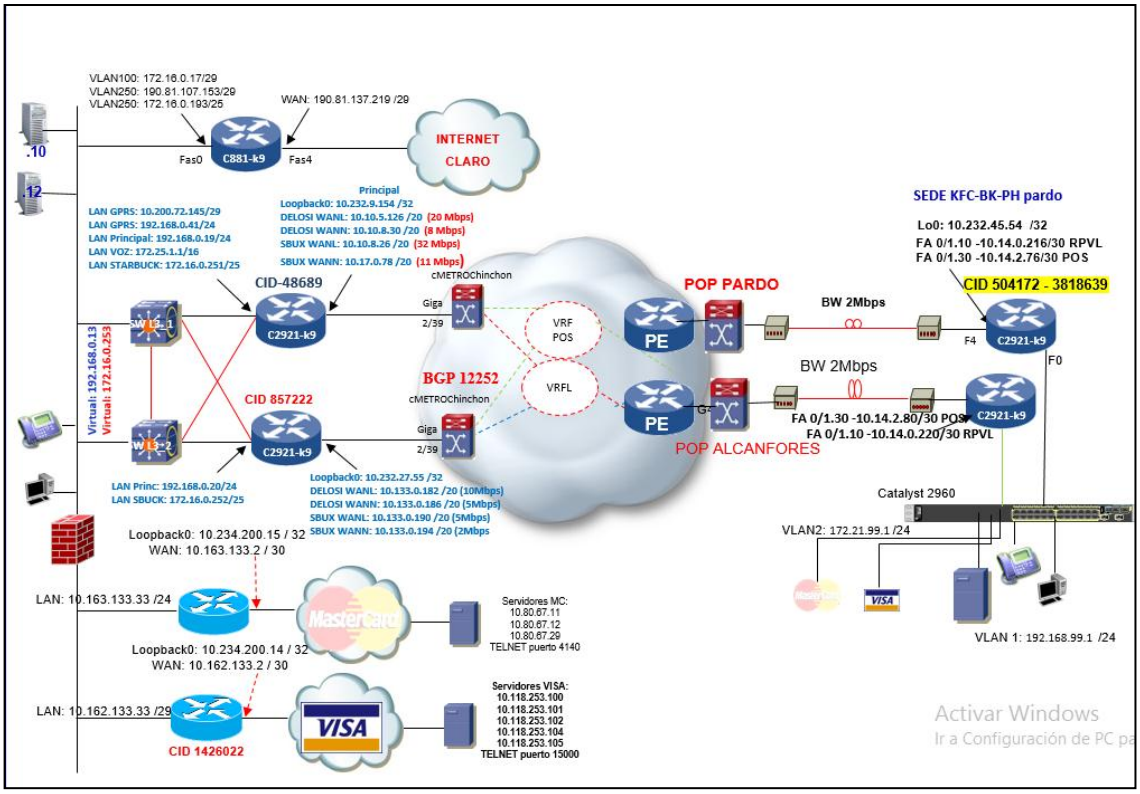


Figura 3.24 Arquitectura final de DELOSI.

3.3 Revisión y consolidación de resultados

3.3.1 Resultado de topología final simulada.

Como resultado final tenemos la siguiente topología simulada en el GNS3: esta simulación se asemeja a un ámbito real, donde dos redes físicamente muy distantes pueden comportarse como una sola red sin importar las limitaciones geográficas, esto gracias a las bondades de MPLS en la nube de red del proveedor donde se ejecuta ingeniería de tráfico, calidad de servicio, esto permite ofrecer a DELOSI no solo tener conexión a su sede principal, sino también adquirir servicios adicionales sobre la misma infraestructura como se demostró con la convergencia de las VPN de delosi y de POS. A todo esto se añadió la gestión de tráfico por medio de clases políticas y clases de tráfico para manejar el tráfico en momentos de congestión y también políticas de prevención de congestión.

La disponibilidad no podía dejarse de lado por lo que se añadió un enlace redundante cuyo ancho de banda es distribuido para el tráfico de las redes, esto se logró mediante GLBP que no solo trabaja en la redundancia sino que también trabaja en lo que es la distribución de carga por los dos router que se tiene en la sede remota.

Como resultado final tenemos la siguiente topología simulada en el GNS3 de la figura 3.25,

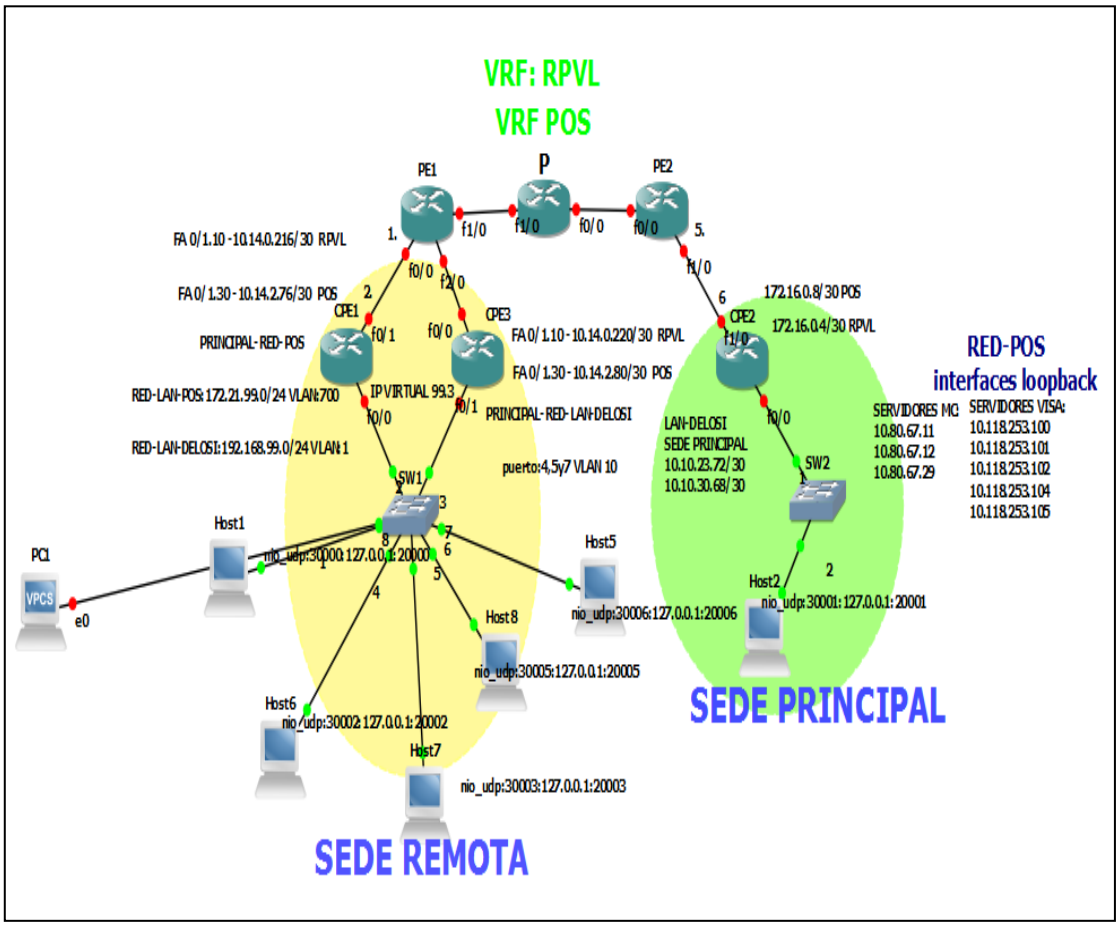


Figura 3.25 Topología final simulada.

3.3.2 Revisión de BGP en router CPE.

Este protocolo es responsable de importar y exportar rutas en nuestro router CPE a su vez que provee respaldo al sistema de redundancia. También es utilizado en el router PE para el intercambio de etiquetas VPN mediante MP-BGP y IBGP para el intercambio de rutas entre PE.

Se utilizara el comando show ip bgp summary y show ip bgp:

La figura 3.26, 3.27, 3.28, 3,29 muestra el estado de los vecinos BGP e IBGP.

```
CPE1#show ip bgp sum
BGP router identifier 10.232.45.54, local AS number 64516
BGP table version is 10, main routing table version 10
8 network entries using 960 bytes of memory
14 path entries using 728 bytes of memory
8/5 BGP path/bestpath attribute entries using 992 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 3 (at peak 3) using 96 bytes of memory
BGP using 2824 total bytes of memory
BGP activity 21/0 prefixes, 39/2 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.14.0.217     4   100      11       7       10    0    0 00:02:17        5
192.168.99.2    4 64516       9       9       10    0    0 00:02:07        7
CPE1#
```

Figura 3.26 Estado de vecinos BGP para cpe1 para red “Delosi”.

```
CPE3#show ip bgp summary
BGP router identifier 10.232.45.55, local AS number 64516
BGP table version is 10, main routing table version 10
8 network entries using 960 bytes of memory
14 path entries using 728 bytes of memory
8/5 BGP path/bestpath attribute entries using 992 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 3 (at peak 3) using 96 bytes of memory
BGP using 2824 total bytes of memory
BGP activity 21/0 prefixes, 39/2 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.14.0.221     4   100      14      10       10    0    0 00:05:26        5
192.168.99.1    4 64516      12      12       10    0    0 00:05:18        7
CPE3#
```

Figura 3.27 Estado de vecinos BGP para cpe3 para red “Delosi”

```
CPE1#show ip bgp vpnv4 vrf 700 summary
BGP router identifier 10.232.45.54, local AS number 64516
BGP table version is 12, main routing table version 12
13 network entries using 1820 bytes of memory
23 path entries using 1564 bytes of memory
8/2 BGP path/bestpath attribute entries using 992 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 3 (at peak 3) using 96 bytes of memory
BGP using 4520 total bytes of memory
3 received paths for inbound soft reconfiguration
BGP activity 21/0 prefixes, 39/2 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.14.2.77      4   100      15      12       12    0    0 00:07:39        9
172.21.99.2     4 64516      13      13       12    0    0 00:07:27       10
CPE1#
```

Figura 3.28 Estado de vecinos BGP para cpe1 para red pos

```
CPE3#show ip bgp vpnv4 vrf 700 sum
BGP router identifier 10.232.45.55, local AS number 64516
BGP table version is 12, main routing table version 12
13 network entries using 1820 bytes of memory
23 path entries using 1564 bytes of memory
8/2 BGP path/bestpath attribute entries using 992 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 3 (at peak 3) using 96 bytes of memory
BGP using 4520 total bytes of memory
3 received paths for inbound soft reconfiguration
BGP activity 21/0 prefixes, 39/2 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.14.2.81      4   100      19      16       12    0    0 00:11:17        9
172.21.99.1     4 64516      17      17       12    0    0 00:11:08       10
CPE3#
```

Figura 3.29 Estado de vecinos BGP para CPE3 para red POS

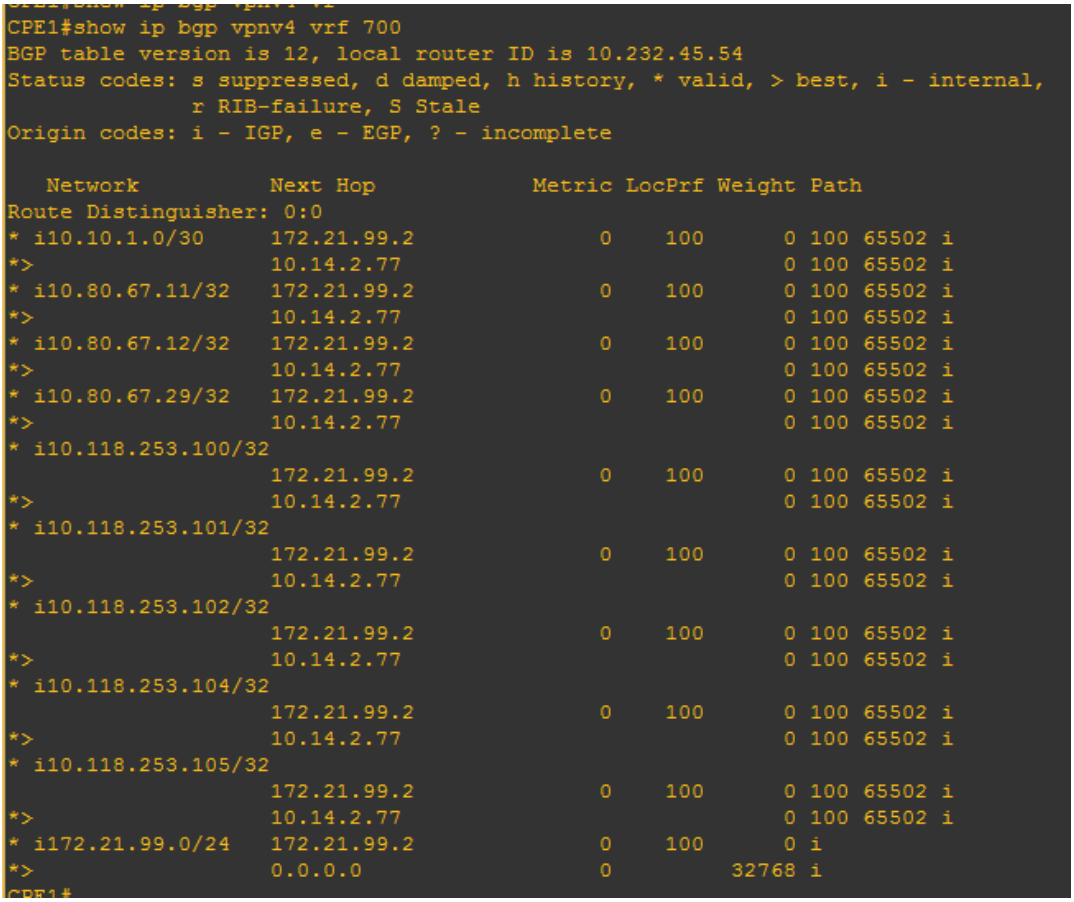
La figura 3.30, 3.31, 3.32, 3.33. Muestra la tabla BGP con sus respectivos atributos.

```
CPE1#show ip bgp
BGP table version is 10, local router ID is 10.232.45.54
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i10.10.23.72/30   10.14.0.221              0    100      0 100 65502 i
*>                  10.14.0.217                           0 100 65502 i
* i10.10.30.68/30   10.14.0.221              0    100      0 100 65502 i
*>                  10.14.0.217                           0 100 65502 i
r i10.14.0.216/30   10.14.0.221              0    100      0 100 ?
r>                  10.14.0.217              0             0 100 ?
* i10.14.0.220/30   10.14.0.221              0    100      0 100 ?
*>                  10.14.0.217              0             0 100 ?
*> 10.232.45.54/32  0.0.0.0                  0         32768 i
*>i10.232.45.55/32  192.168.99.2             0    100      0 i
* i172.16.0.4/30    10.14.0.221              0    100      0 100 ?
*>                  10.14.0.217                           0 100 ?
* i192.168.99.0     192.168.99.2             0    100      0 i
*>                  0.0.0.0                  0         32768 i
CPE1#
```

Figura 3.30 Tabla BGP para red de Delosi del Reuter CPE1

```
CPE3#show ip bgp
BGP table version is 10, local router ID is 10.232.45.55
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
* i10.10.23.72/30   10.14.0.217              0    100      0 100 65502 i
*>                  10.14.0.221                           0 100 65502 i
* i10.10.30.68/30   10.14.0.217              0    100      0 100 65502 i
*>                  10.14.0.221                           0 100 65502 i
* i10.14.0.216/30   10.14.0.217              0    100      0 100 ?
*>                  10.14.0.221              0             0 100 ?
r i10.14.0.220/30   10.14.0.217              0    100      0 100 ?
r>                  10.14.0.221              0             0 100 ?
*>i10.232.45.54/32  192.168.99.1             0    100      0 i
*> 10.232.45.55/32  0.0.0.0                  0         32768 i
* i172.16.0.4/30    10.14.0.217              0    100      0 100 ?
*>                  10.14.0.221                           0 100 ?
* i192.168.99.0     192.168.99.1             0    100      0 i
*>                  0.0.0.0                  0         32768 i
CPE3#
```

Figura 3.31 Tabla BGP para red de Delosi del router CPE3



```
CPE1#show ip bgp vpnv4 vrf 700
BGP table version is 12, local router ID is 10.232.45.54
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 0:0
* i10.10.1.0/30     172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i10.80.67.11/32   172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i10.80.67.12/32   172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i10.80.67.29/32   172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i10.118.253.100/32
                    172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i10.118.253.101/32
                    172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i10.118.253.102/32
                    172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i10.118.253.104/32
                    172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i10.118.253.105/32
                    172.21.99.2              0    100      0 100 65502 i
*>                  10.14.2.77                            0 100 65502 i
* i172.21.99.0/24   172.21.99.2              0    100      0 i
*>                  0.0.0.0                  0         32768 i
CPE1#
```

Figura 3.32 Tabla BGP para red de pos del router CPE1

```
CPE3#show ip bgp VPNv4 vrf 700
BGP table version is 12, local router ID is 10.232.45.55
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 0:0
* i10.10.1.0/30     172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i10.80.67.11/32   172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i10.80.67.12/32   172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i10.80.67.29/32   172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i10.118.253.100/32
                    172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i10.118.253.101/32
                    172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i10.118.253.102/32
                    172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i10.118.253.104/32
                    172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i10.118.253.105/32
                    172.21.99.1              0    100      0 100 65502 i
*>                  10.14.2.81                            0 100 65502 i
* i172.21.99.0/24   172.21.99.1              0    100      0 i
*>                  0.0.0.0                  0         32768 i
CPE3#
```

Figura 3.33 Tabla BGP para red de pos del router CPE3

3.3.3 Revisión de tablas de enrutamiento.

Como se muestra en la figura3.34, 3.35,3.36, 3.37 las tablas contienen ,los destinos hacia la sede principal como servidores de MasterCard, visa, la granja de servidores de la DELOSI donde se encuentra su base de datos, cada destino con un siguiente salto en común que la dirección de la interfaz perteneciente a la VRF donde pertenece la sede remota.

```
CPE1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 1 subnets
B       172.16.0.4 [20/0] via 10.14.0.217, 00:30:35
C    192.168.99.0/24 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
B       10.10.30.68/30 [20/0] via 10.14.0.217, 00:30:35
B       10.10.23.72/30 [20/0] via 10.14.0.217, 00:30:35
B       10.14.0.220/30 [20/0] via 10.14.0.217, 00:31:05
C       10.14.0.216/30 is directly connected, FastEthernet0/1.10
B       10.232.45.55/32 [200/0] via 192.168.99.2, 00:31:22
C       10.232.45.54/32 is directly connected, Loopback0
CPE1#
```

Figura 3.34 Tabla de enrutamiento tradicional para CPE1

```
CPE3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/30 is subnetted, 1 subnets
B       172.16.0.4 [20/0] via 10.14.0.221, 00:32:09
C    192.168.99.0/24 is directly connected, FastEthernet0/1
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
B       10.10.30.68/30 [20/0] via 10.14.0.221, 00:32:09
B       10.10.23.72/30 [20/0] via 10.14.0.221, 00:32:09
C       10.14.0.220/30 is directly connected, FastEthernet0/0.10
B       10.14.0.216/30 [20/0] via 10.14.0.221, 00:32:39
C       10.232.45.55/32 is directly connected, Loopback0
B       10.232.45.54/32 [200/0] via 192.168.99.1, 00:33:00
CPE3#
```

Figura 3.35 Tabla de enrutamiento tradicional para CPE3

```
CPE1#show ip route vrf 700

Routing Table: 700
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.21.0.0/24 is subnetted, 1 subnets
C       172.21.99.0 is directly connected, FastEthernet0/0.700
     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
B       10.10.1.0/30 [20/0] via 10.14.2.77, 00:36:38
B       10.80.67.29/32 [20/0] via 10.14.2.77, 00:36:38
B       10.80.67.11/32 [20/0] via 10.14.2.77, 00:36:38
B       10.80.67.12/32 [20/0] via 10.14.2.77, 00:36:38
C       10.14.2.76/30 is directly connected, FastEthernet0/1.30
B       10.118.253.101/32 [20/0] via 10.14.2.77, 00:36:41
B       10.118.253.100/32 [20/0] via 10.14.2.77, 00:36:41
B       10.118.253.102/32 [20/0] via 10.14.2.77, 00:36:41
B       10.118.253.105/32 [20/0] via 10.14.2.77, 00:36:43
B       10.118.253.104/32 [20/0] via 10.14.2.77, 00:36:43
CPE1#
```

Figura 3.36 Tabla de enrutamiento de red pos para CPE1

```
Routing Table: 700
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.21.0.0/24 is subnetted, 1 subnets
C       172.21.99.0 is directly connected, FastEthernet0/1.700
     10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
B       10.10.1.0/30 [20/0] via 10.14.2.81, 00:42:29
B       10.80.67.29/32 [20/0] via 10.14.2.81, 00:42:29
B       10.80.67.11/32 [20/0] via 10.14.2.81, 00:42:29
B       10.80.67.12/32 [20/0] via 10.14.2.81, 00:42:29
C       10.14.2.80/30 is directly connected, FastEthernet0/0.30
B       10.118.253.101/32 [20/0] via 10.14.2.81, 00:42:33
B       10.118.253.100/32 [20/0] via 10.14.2.81, 00:42:33
B       10.118.253.102/32 [20/0] via 10.14.2.81, 00:42:33
B       10.118.253.105/32 [20/0] via 10.14.2.81, 00:42:33
B       10.118.253.104/32 [20/0] via 10.14.2.81, 00:42:33
CPE3#
```

Figura 3.37 Tabla de enrutamiento de red pos para CPE3

3.3.4 Verificación de VRFs

El router de DELOSI ejecuta dos instancias de enrutamiento mediante el concepto de VRF una para cada VPN implementada.

El comando show ip vrf muestra ello en la figura3.38 Y 3.39:

```
CPE1#show ip vrf
  Name                             Default RD          Interfaces
  700                              <not set>           Fa0/0.700
                                                       Fa0/1.30

CPE1#
```

Figura 3.38 Verificación de VRF en router CPE1

```
CPE3#SHO IP VRF
  Name                             Default RD          Interfaces
  700                              <not set>           Fa0/0.30
                                                       Fa0/1.700

CPE3#
```

Figura 3.39 Verificación de VRF en router CPE3

3.3.5 Verificación de funcionamiento de GLBP.

GLBP es una solución propietaria de Cisco para la redundancia y balanceo de carga en una red IP. A su vez permite la selección automática y recuperación simultánea de los fallas de router de primer salto, también proporciona equilibrio de carga a través de múltiples puertas de enlace (Router) mediante una única dirección IP virtual y múltiples direcciones MAC. Cada host está configurado con la misma dirección IP virtual, y todos los routers en el grupo de router virtual participan en el envío de paquetes.

Se utilizará el comando show glbp brief para ver el estado del router como AVG Y AVF, ello es mostrado en la figura 3.40 Y 3.41.

```
CPE1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Fa0/0       1    -   100 Standby  192.168.99.3    192.168.99.2    local
Fa0/0       1    1   -   Listen   0007.b400.0101  192.168.99.2    -
Fa0/0       1    2   -   Active   0007.b400.0102  local           -
Fa0/0.700   2    -   150 Active   172.21.99.3     local           172.21.99.2
Fa0/0.700   2    1   -   Active   0007.b400.0201  local           -
Fa0/0.700   2    2   -   Listen   0007.b400.0202  172.21.99.2     -
CPE1#
```

Figura 3.40 Estado de CPE1 como AVG y AVF en GLBP

Como puede verse CPE1 es router activo para AVG y activo para AVF para la MAC 0007.b400.0201en el grupo 2 y router standby para AVG y activo para AVF para la MAC 0007.b400.0102 en el grupo 1.

```
CPE3#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Fa0/1       1    -   150 Active   192.168.99.3    local           192.168.99.1
Fa0/1       1    1   -   Active   0007.b400.0101  local           -
Fa0/1       1    2   -   Listen   0007.b400.0102  192.168.99.1    -
Fa0/1.700   2    -   100 Standby  172.21.99.3     172.21.99.1     local
Fa0/1.700   2    1   -   Listen   0007.b400.0201  172.21.99.1     -
Fa0/1.700   2    2   -   Active   0007.b400.0202  local           -
CPE3#
```

Figura 3.41 Estado de CPE3 como AVG y AVF en GLBP

Como puede verse CPE3 es router activo para AVG y activo para AVF para la MAC 0007.b400.0101 en el grupo 1 y router standby para AVG y activo para AVF para la MAC 0007.b400.0202 en el grupo 2.

3.3.6 Demostración de funcionamiento de GLBP.

Para ello primero se desactivara la interface LAN del router CPE1 y se verá como el router CPE3 cambia de rol para los grupos GLBP. La figura 3.42 muestra ello.

```
CPE3#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Fa0/1       1    -   150 Active   192.168.99.3    local           unknown
Fa0/1       1    1   -   Active   0007.b400.0101  local           -
Fa0/1       1    2   -   Active   0007.b400.0102  local           -
Fa0/1.700   2    -   100 Active   172.21.99.3     local           unknown
Fa0/1.700   2    1   -   Active   0007.b400.0201  local           -
Fa0/1.700   2    2   -   Active   0007.b400.0202  local           -
CPE3#
```

Figura 3.42 Cambio de estado de CPE3 para los grupos GLBP**.**

Lo mismo se realiza para CPE3, se desactivara la interface LAN del router CPE3 y se verá como el router CPE1 cambia de rol para los grupos GLBP. La figura 3.43 muestra ello.

```
CPE1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Fa0/0       1    -   100 Active   192.168.99.3    local           unknown
Fa0/0       1    1   -   Active   0007.b400.0101  local           -
Fa0/0       1    2   -   Active   0007.b400.0102  local           -
Fa0/0.700   2    -   150 Active   172.21.99.3     local           unknown
Fa0/0.700   2    1   -   Active   0007.b400.0201  local           -
Fa0/0.700   2    2   -   Active   0007.b400.0202  local           -
CPE1#
```


Figura 3.43 Cambio de estado de CPE1 para los grupos GLBP.

Como puede observarse en las figuras anteriores un router soporta toda la carga para de la red LAN cuando el otro cae, esto se demuestra viendo los estados, por ejemplo en la última figura CPE1 es AVG para ambos grupos GLBP y AVF para todas las direcciones MAC virtuales.

3.3.7 Verificación de conectividad hacia la sede principal.

Mediante el envío de paquetes icmp o más conocido como ping se verificará la conectividad hacia un host en la sede principal para la red de DELOSI, Los destinos en la sede principal para la red POS son los servidores de MC Y VISA. Las figuras 3.44, 3.45, 3.46 muestran la prueba y la tabla 3.9 muestra los destinos.

Tabla 3-9 *Destinos de sede principal.*

NRO DE SERVIDOR VISA	DIRECCIÓN IP
1	10.118.253.100
2	10.118.253.101
3	10.118.253.102
4	10.118.253.104
5	10.118.253.105
NRO DE SERVIDOR MC	
1	10.80.67.11
2	10.80.67.12
3	10.80.67.29

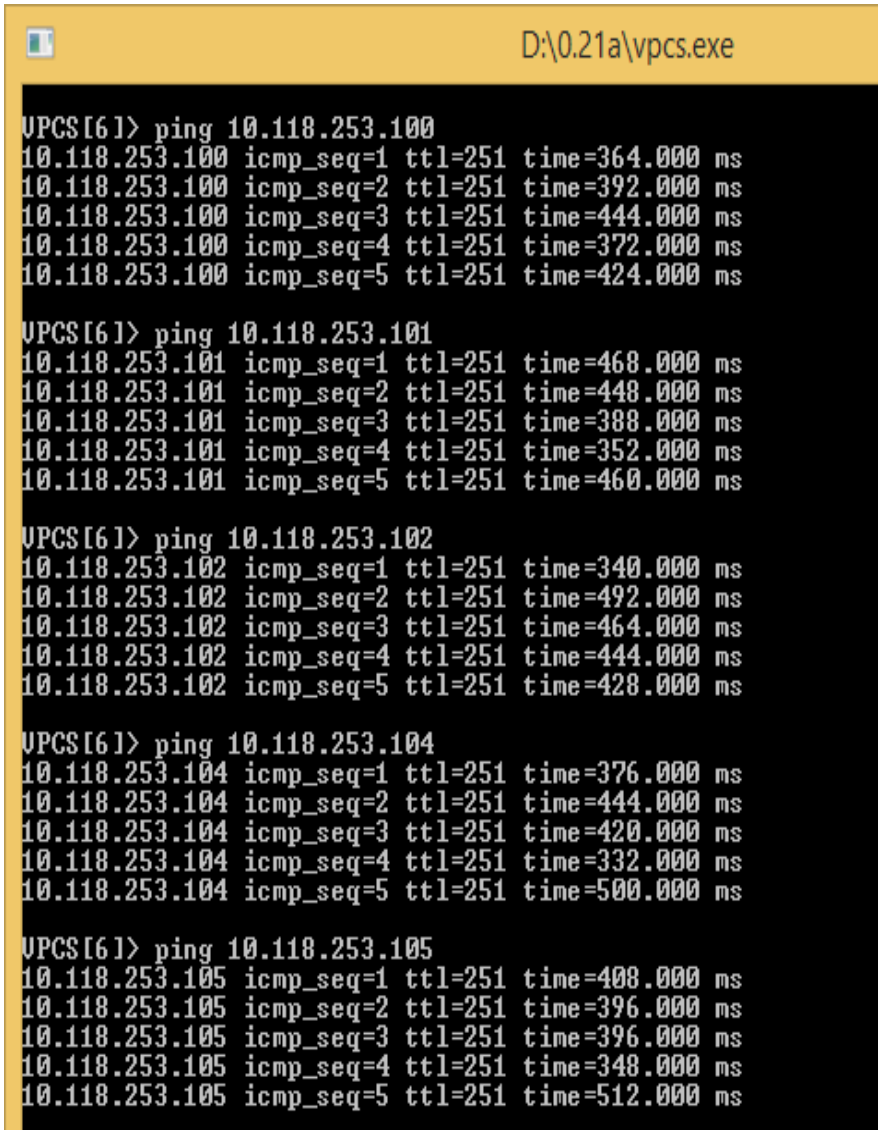


Figura 3.44 Ping de PC virtual hacia todos los servidores visa.

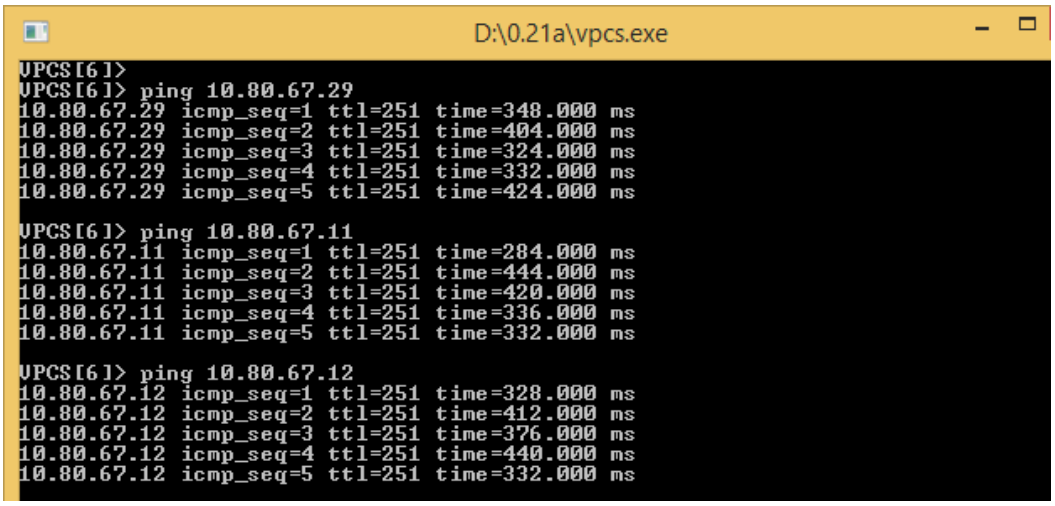


Figura 3.45 Ping de pc virtual hacia todos los servidores MasterCard.

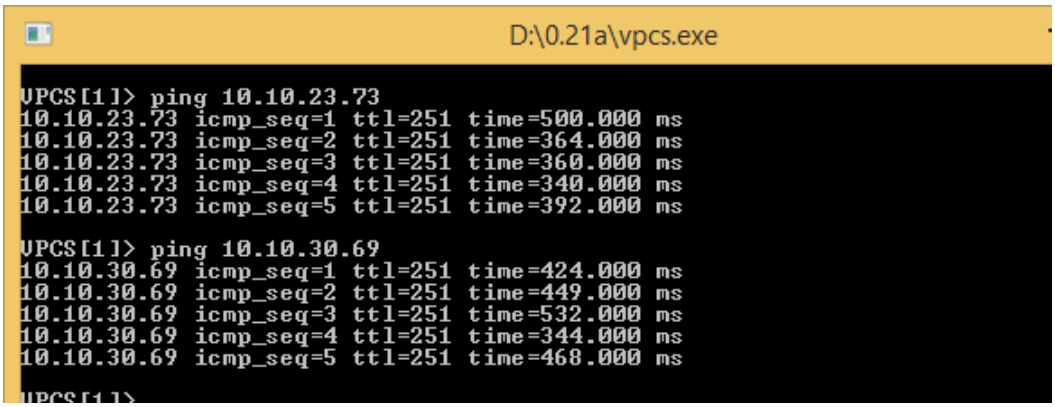


Figura 3.46 Ping de pc virtual hacia destino en la red de “Delosi”.

3.3.8 Verificación de las políticas de gestión de ancho de banda y marcado.

Como el tráfico de la red de DELOSI y POS que sale hacia la sede principal está distribuido entre los routers, donde la red POS sale por CPE1 y la red de DELOSI (RPVL) sale por CPE 3, se procede a hacer la saturación y observación de las políticas en su respectivo router. Las figuras 3.47, 3.48, 3.49, 3.50, 3.51 muestran el proceso de saturación por clase de servicio.

```
Service-policy output: Shape64_vrf700

  Class-map: class-default (match-any)
    2117 packets, 2282112 bytes
    5 minute offered rate 64000 bps, drop rate 0 bps
    Match: any
    Traffic Shaping
         Target/Average   Byte   Sustain   Excess    Interval  Increment
           Rate           Limit  bits/int  bits/int  (ms)      (bytes)
          65000/65000     1950   7800      7800      120       975

      Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
      Active Depth                         Delayed   Delayed   Active
      -      1         2107      2272812   1218      1271359   yes

    Service-policy : wan_vrf700

      Class-map: qos2_vrf700 (match-any)
        2095 packets, 2280430 bytes
        5 minute offered rate 64000 bps, drop rate 0 bps
        Match: ip dscp cs2 (16)
          2095 packets, 2280430 bytes
          5 minute rate 64000 bps
        Queueing
          Output Queue: Conversation 25
          Bandwidth 64 (kbps)Max Threshold 64 (packets)
          (pkts matched/bytes matched) 1215/1271589
       (depth/total drops/no-buffer drops) 1/0/0
        police:
            cir 64000 bps, bc 12000 bytes, be 24000 bytes
          conformed 2086 packets, 2271668 bytes; actions:
            transmit
          exceeded 9 packets, 8762 bytes; actions:
            drop
          violated 0 packets, 0 bytes; actions:
```

Figura 3.47 Ancho de banda de clase de servicio 2 para la red pos en CPE1.

Como puede observarse se obtuvo el ancho de banda de 64kbps especificado para la clase de servicio 3 de la red POS, validando nuestra configuración.

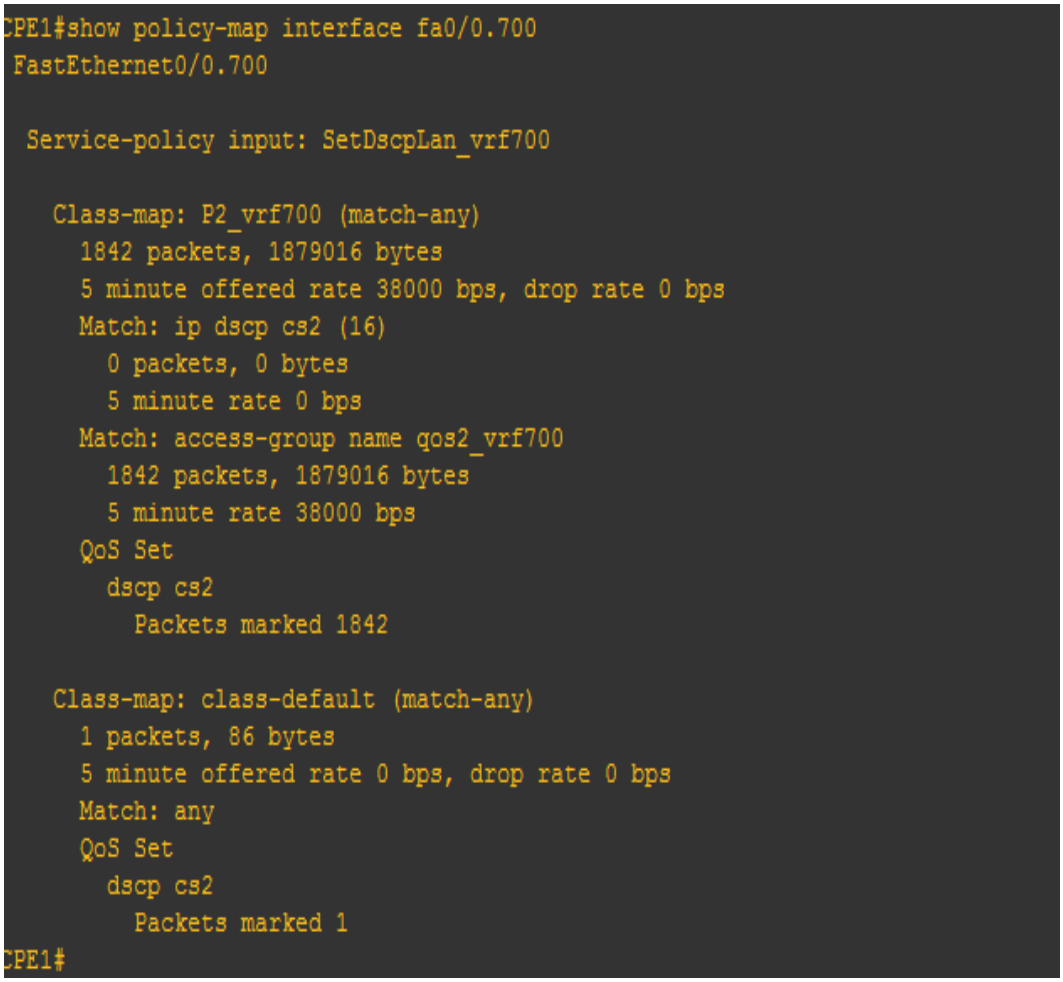


Figura 3.48 Paquetes marcados como clase de servicio 2 para la red pos en CPE1.

La marcación se da a todos los paquete pertenecientes a la red POS debido a que solo son las maquinas POS las que están conectadas. El proceso de marcado es importante debido a que asegura que los paquetes sean clasificados y por lo tanto afectados por las políticas correspondientes a dicha clase.

CPE3

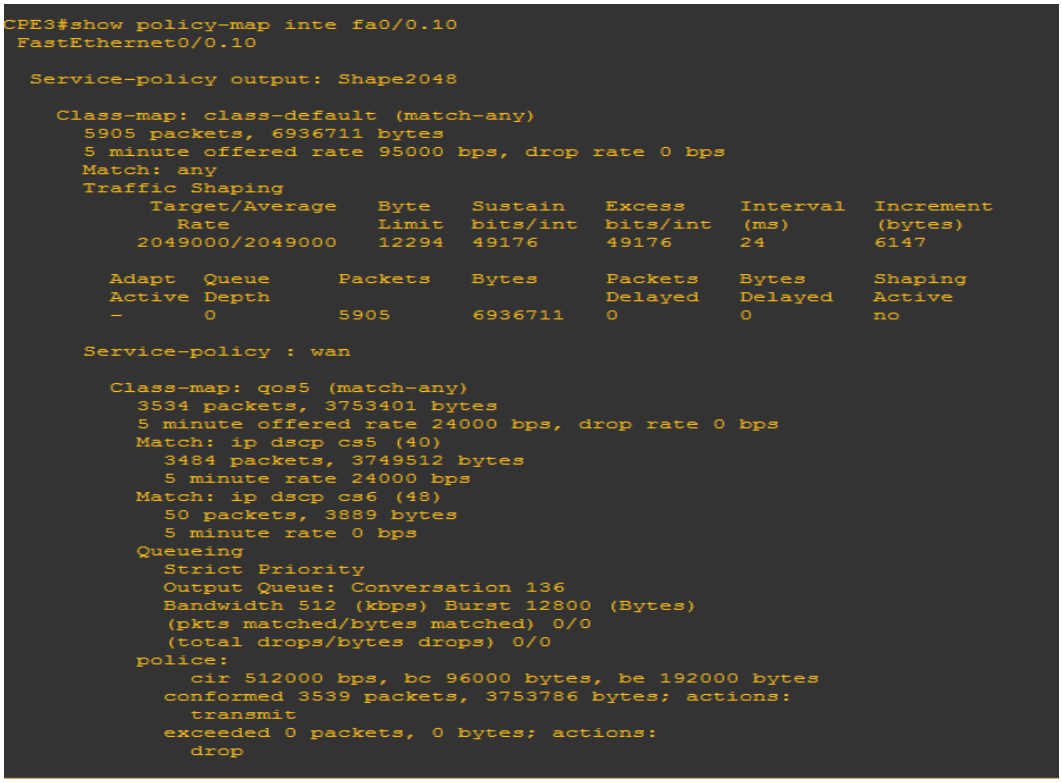


Figura 3.49 Ancho de banda de clase de servicio 5 para la red RPVL en cpe3

Como puede observarse el valor que señala la parte offered, que quiere decir que la clase de servicio 5 está ocupando 24kbps de los 512kbps que demuestra que los paquetes están siendo marcados y afectados por las políticas.

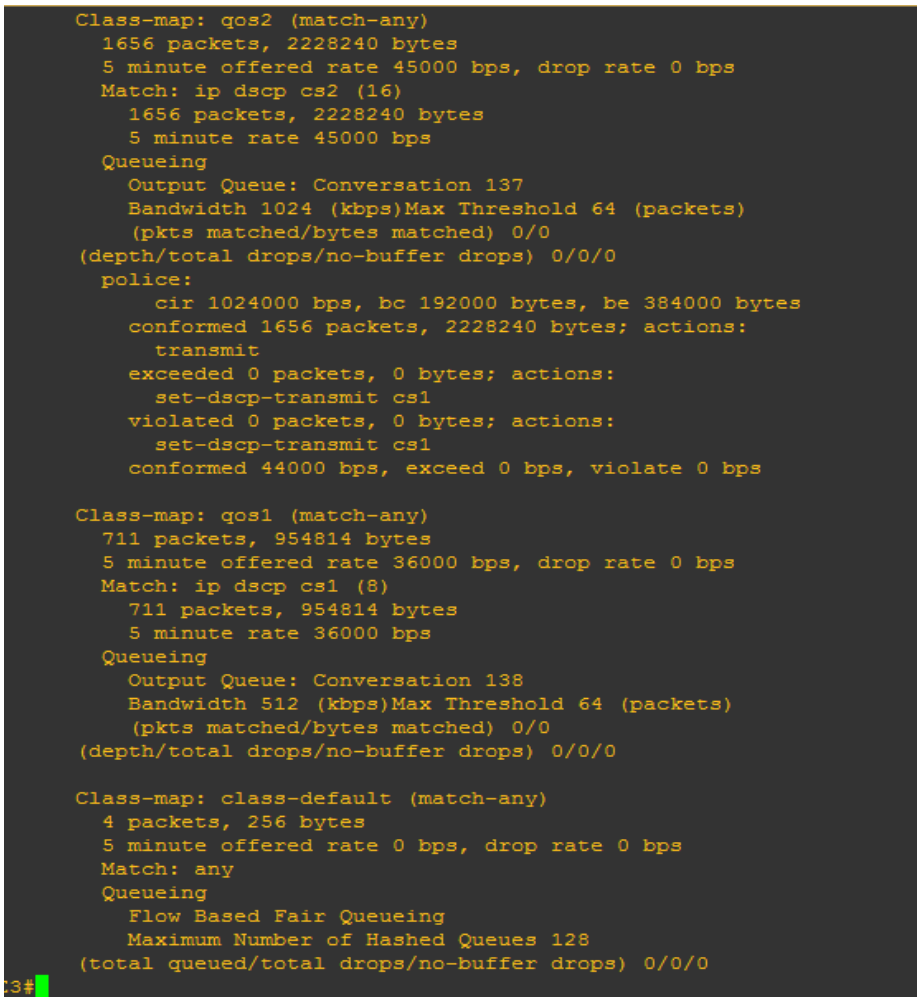
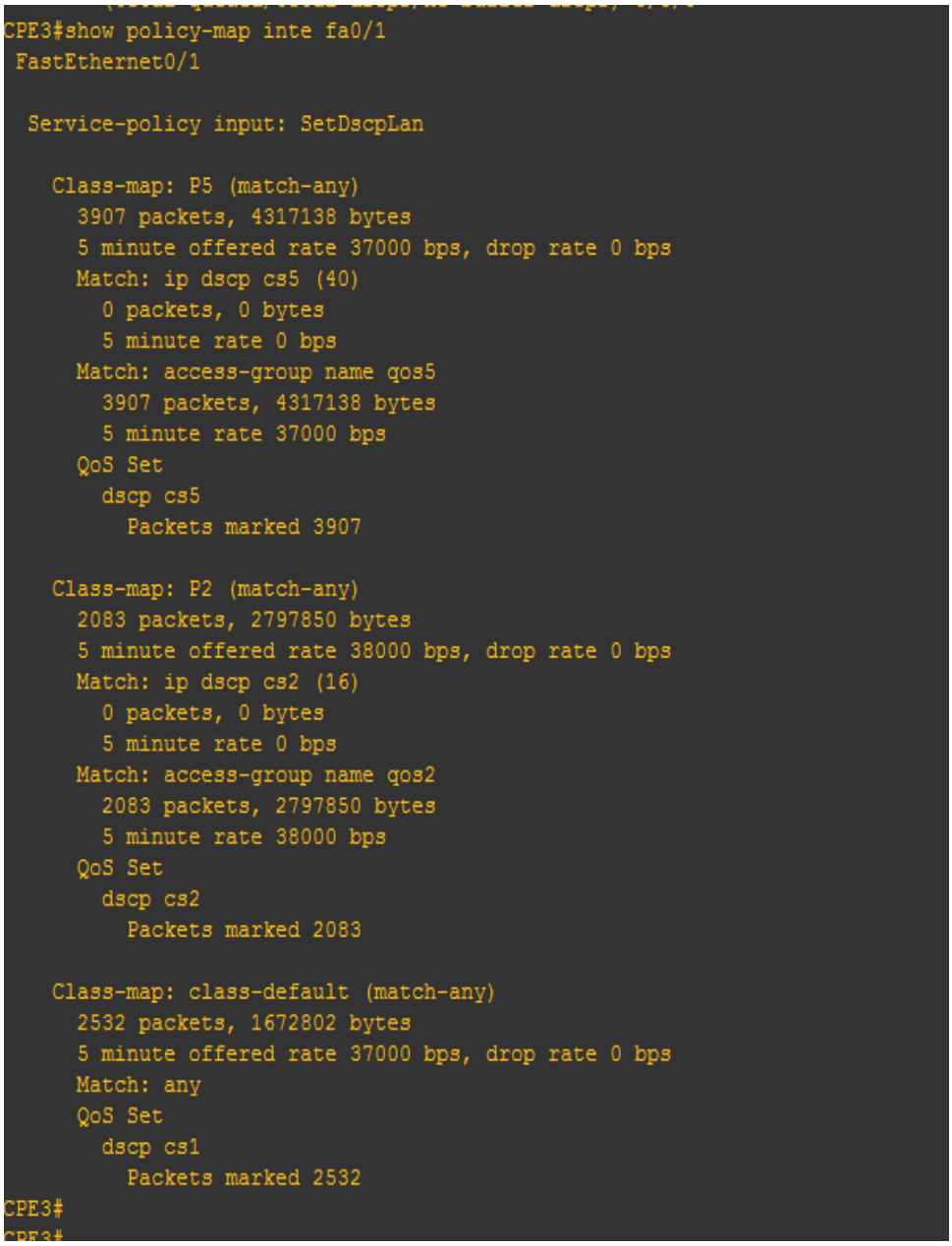


Figura 3.50 Ancho de banda de clase de servicio 2 y 1 para la red RPVL en cpe3.

Como puede observarse el valor que señala la parte offered, quiere decir que la clase de servicio 2 está ocupando 45kbps de los 1024kbps reservados y la clase 1 está ocupando 36kbps de los 512kbps que demuestra que los paquetes están siendo marcados y afectados por las políticas.

No se pudo llegar al ancho de banda especificado debido a las limitaciones de procesamiento y memoria de computador donde corre GNS3.



```
CPE3#show policy-map inte fa0/1
 FastEthernet0/1

  Service-policy input: SetDscpLan

    Class-map: P5 (match-any)
      3907 packets, 4317138 bytes
      5 minute offered rate 37000 bps, drop rate 0 bps
      Match: ip dscp cs5 (40)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: access-group name qos5
        3907 packets, 4317138 bytes
        5 minute rate 37000 bps
      QoS Set
        dscp cs5
          Packets marked 3907

    Class-map: P2 (match-any)
      2083 packets, 2797850 bytes
      5 minute offered rate 38000 bps, drop rate 0 bps
      Match: ip dscp cs2 (16)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: access-group name qos2
        2083 packets, 2797850 bytes
        5 minute rate 38000 bps
      QoS Set
        dscp cs2
          Packets marked 2083

    Class-map: class-default (match-any)
      2532 packets, 1672802 bytes
      5 minute offered rate 37000 bps, drop rate 0 bps
      Match: any
      QoS Set
        dscp cs1
          Packets marked 2532
CPE3#
```

Figura 3.51 Marcación de paquetes para la clase de servicio 5, 2 y 1 para la red RPVL en CPE3

Conclusiones

- La comunicación otorgada por la VPN es muy transparente porque permite establecer un enlace de comunicación directo entre dos computadoras, sin preocuparse de la infraestructura física de la red existente y de los equipos que la conforman.
- Se presentó una solución para DELOSI para que pueda migrar hacia una red MPLS de un proveedor de servicios donde pueden converger todos sus servicios en una misma plataforma.
- El protocolo BGP presenta muchas opciones para forzar medidas administrativas de rutas que garantizan una tabla de enrutamiento eficiente.
- GLBP provee alta disponibilidad en la red además de distribuir la carga sin la necesidad de administrar números grupos y utilizando solo una dirección virtual.
- La gestión de tráfico para afrontar momentos de congestión provee una solución a los cuellos de botella en la salida de tráfico y a la fácil solución de aumentar el ancho de banda.

Recomendaciones

- Si por algunos motivos la compañía “Delosi” desea incrementar la capacidad de sus enlaces deberá considerar cambiar el router CPE debido a que cada modelo posee limitaciones en cuanto a procesamiento y se sabe que a mayor comando ejecutado mayor es el procesamiento.
- En la implementación de BGP se debe tener en cuenta que por cada red añadida no solo se tiene que realizar la configuración de la interfaces sino que también conllevan a la agregación de la misma en la lista de prefijos y en BGP con el comando network.
- Cuando se trabaje con GLBP se debe considerar las capacidades del router cuando se defina la elección del AVG debido a que esto aumenta la carga sobre el router, en caso se esté utilizando diferentes modelos.
- Tener en cuenta que no se debe de saturar el ancho de banda mínimo sumado a los picos de ancho de banda configurado para el cos5 de lo contrario descartara paquetes.

Referencias

Cisco Systems (s. f) *Implementación de políticas de calidad de servicio (QoS) con DSCP.* Recuperado de http://www.cisco.com/cisco/web/support/LA/7 /73/ 73469_dscpvalues.html. Última fecha de consulta: 19 de julio 2016.

Pérez, D. (2013*).Blog: CCNP SWITCH- Alta disponibilidad y redundancia, HSRP, VRRP Y GLBP*. Recuperado de http://desdelacli.blogspot.pe/2013/03/ccnp-switch-alta-disponibilidad-y.html. Última fecha de consulta: 20 de julio 2016.

García, G. G. (2009).Tesis de Grado: *Propuesta de Migración de la Red NGN de una Operadora Implementada en IP hacia MPLS*. Pontificia Universidad Católica del Perú.

NETACAD CISCO SYSTEMS (2016).*Infraestructura WAN privada* Recuperado de https://static-course assets.s3.amazonaws .com/CN503/ es/index.html#2.2.2.7 Última fecha de consulta: 08 de Julio 2016.

Lavado, G. (2010). *MPLS-Multiprotocol Label Switching. Versión 1.0 Modo de Compatibilidad* [Presentación Power Point]. Última fecha de consulta: 07 de Julio 2016.

Limari R. V. (2004).Tesis de Grado: *Protocolos de Seguridad para Redes Privadas Virtuales (VPN).* Universidad Austral de Chile Valdivia, Chile. Recuperado de http://cybertesis.Uach .cl/tesis/uach/2004/bmfcil732p/doc/ bmfcil732p.pdf. Última fecha de consulta: 20 de JULIO 2016.

Mahmoud, M. (2008). *Comentario del 25 de Diciembre de 2008 a Inter - AS MPLS VPN – The Whole Story.* Recuperado de URL:http://www.networkers-online.com/ blog/2008/12/inter-as-mpls-vpn-thewhole-story-updated-dec-2008/Última fecha de consulta: 28 de Mayo 2012.

Morales, B. (2006).*Tesis de Grado: Investigación de Redes VPN con Tecnología MPLS.* Universidad de las Américas Puebla, México. Recuperado de: http://catarina.udlap. mx/ u _dl_a/tales/documentos/lis/morales _d_l/ capítulo2. Última fecha de consulta: 15 de julio de 2016.

Pepelnjak, I. & Guichard, J.(2002). *MPLS and VPN Architectures*. Editor: Cisco Press, Estados Unidos. Recuperado de https://www.coursehero.com/file/p7uerj5/Figure-1-7-Various -MPLS-Applications-and-Their-Interactions-Every-MPLS/ Última fecha de consulta: 20 de Julio 2016.

Alvez, R. (s. f). *Fundamentos de MPLS/VPN.* [Presentación Power Point].Recuperado de https://www.cert.uy/ wps/wcm/ connect/certuy/c3df385c-1582-4986-94b9-98c974496fbe/

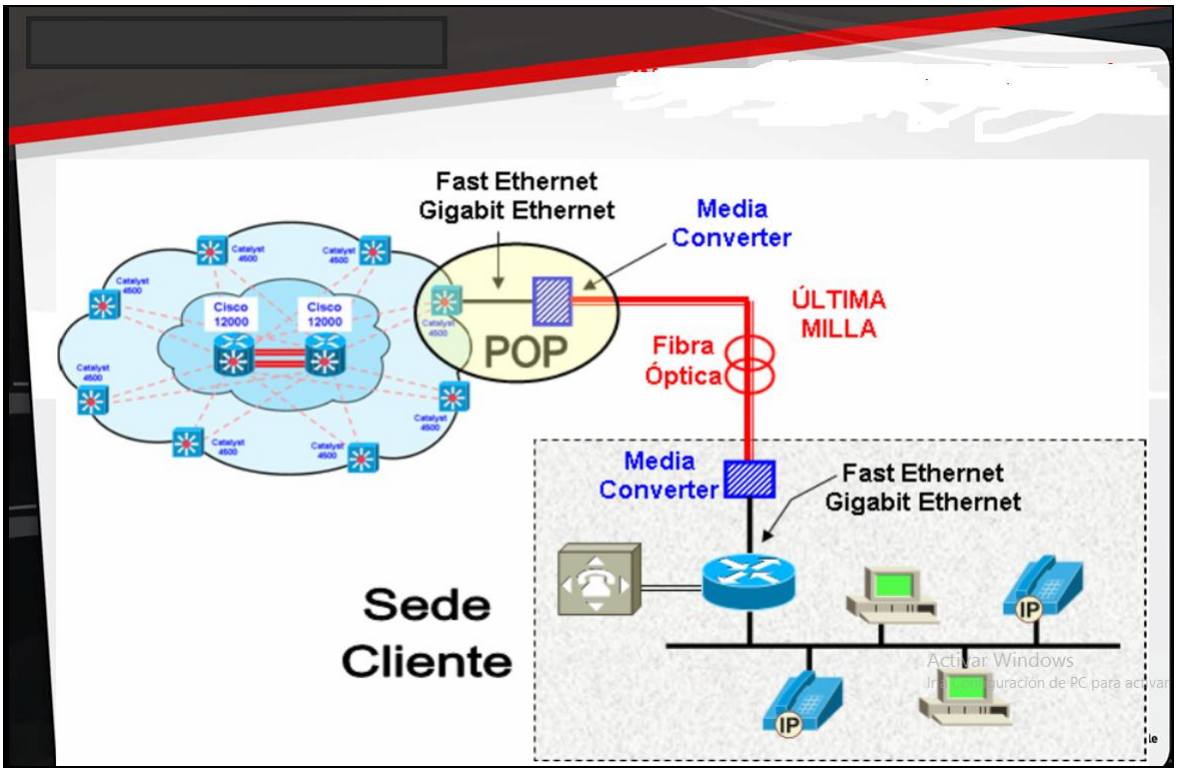
Presentaci%C3%B3n+02+-+MPLS-VPN.pdf?MOD=AJPERES. Última fecha de consulta: 20 de Julio 2016.

TELDAT Doc. Dm763 Rev.10.5 (2008). *Protocolo BGP* Recuperado:http://www.lab.dit.upm.es/~labrst/config/manuales-teldat/Dm763v10-5_Protocolo_BGP.pdf. Última fecha de consulta: 20 de Julio 2016.

CORPORACION CLARO (s.f). *Servicios corporativos, Tarifas transmisión de datos*. Recuperado de http://www.claro.com.pe/portal/recursos/pe/pdf/Claro_ Local_ Private_lines.pdf.Última fecha de consulta: 21 de Julio 2016.

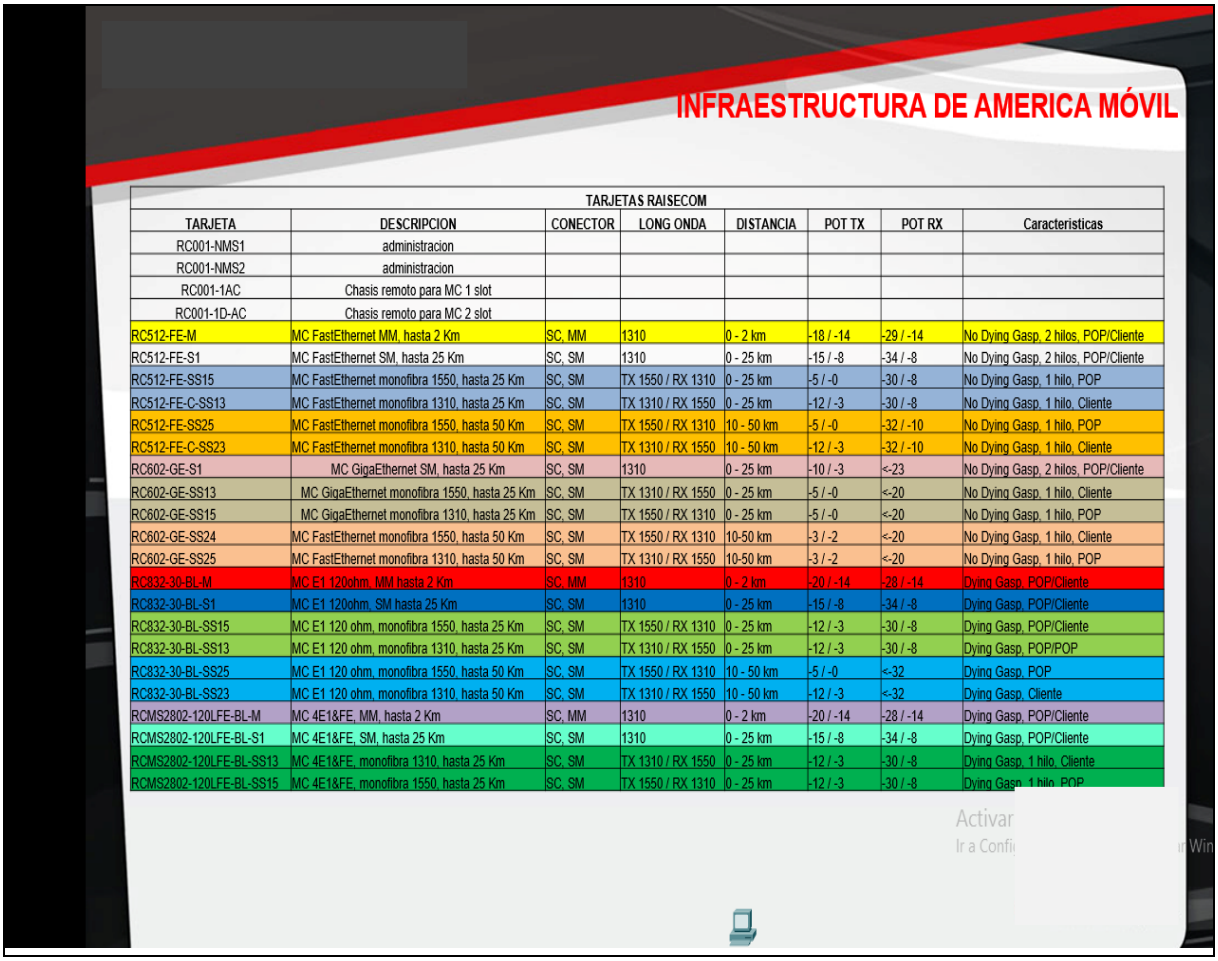
CORPORACION CLARO (s.f). *Servicios corporativos, Tarifas transmisión de datos* Recuperado de http://www.claro.com.pe/portal/recursos/pe/pdf/RPV Local_5CoS.pdf. Última fecha de consulta: 21 de Julio 2016.

ANEXOS



Anexo 1 Infraestructura de América Móvil

Fuente: Capacitación claro

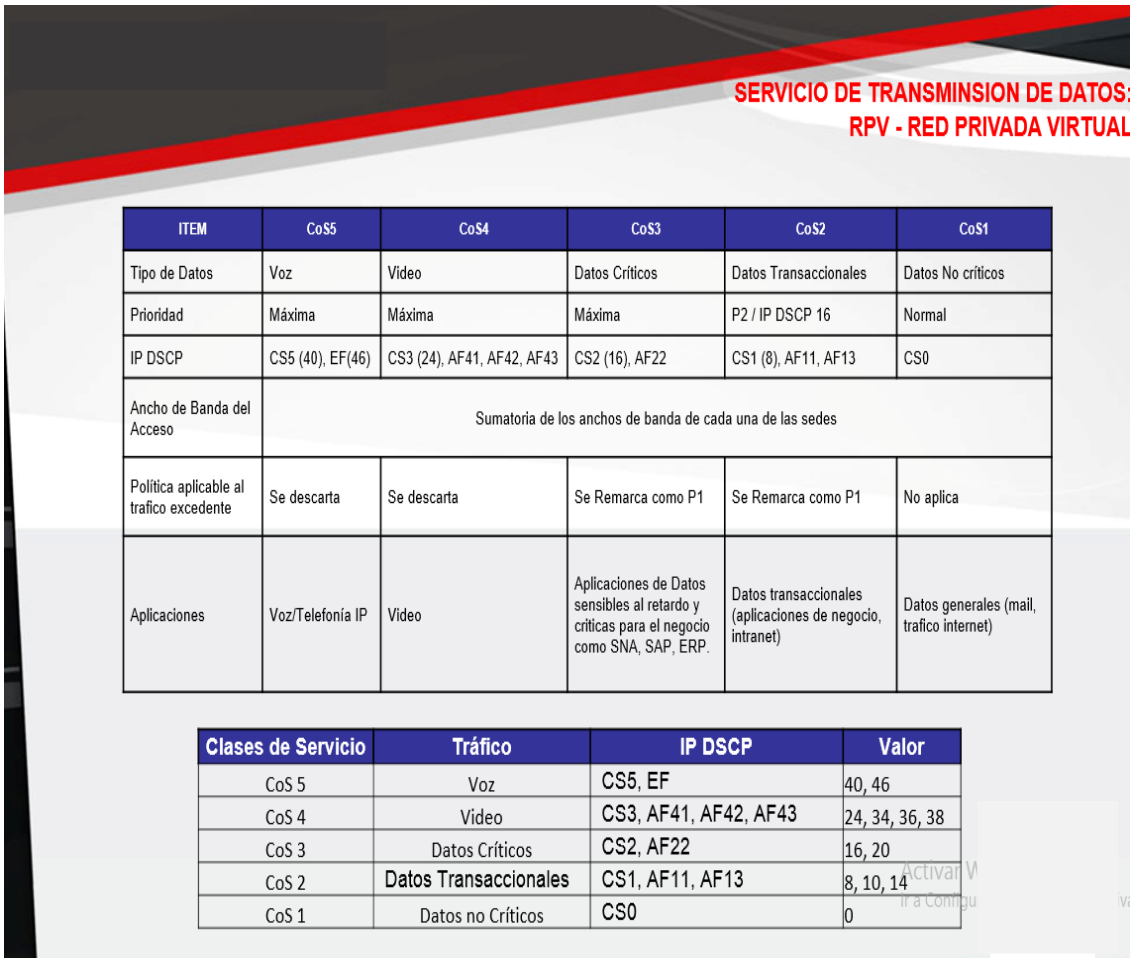


TARJETAS RAISECOM

TARJETA	DESCRIPCION	CONECTOR	LONG ONDA	DISTANCIA	POT TX	POT RX	Caracteristicas
RC001-NMS1	administracion						
RC001-NMS2	administracion						
RC001-1AC	Chasis remoto para MC 1 slot						
RC001-1D-AC	Chasis remoto para MC 2 slot						
RC512-FE-M	MC FastEthernet MM, hasta 2 Km	SC, MM	1310	0 - 2 km	-18 / -14	-29 / -14	No Dying Gasp, 2 hilos, POP/Cliente
RC512-FE-S1	MC FastEthernet SM, hasta 25 Km	SC, SM	1310	0 - 25 km	-15 / -8	-34 / -8	No Dying Gasp, 2 hilos, POP/Cliente
RC512-FE-SS15	MC FastEthernet monofibra 1550, hasta 25 Km	SC, SM	TX 1550 / RX 1310	0 - 25 km	-5 / -0	-30 / -8	No Dying Gasp, 1 hilo, POP
RC512-FE-C-SS13	MC FastEthernet monofibra 1310, hasta 25 Km	SC, SM	TX 1310 / RX 1550	0 - 25 km	-12 / -3	-30 / -8	No Dying Gasp, 1 hilo, Cliente
RC512-FE-SS25	MC FastEthernet monofibra 1550, hasta 50 Km	SC, SM	TX 1550 / RX 1310	10 - 50 km	-5 / -0	-32 / -10	No Dying Gasp, 1 hilo, POP
RC512-FE-C-SS23	MC FastEthernet monofibra 1310, hasta 50 Km	SC, SM	TX 1310 / RX 1550	10 - 50 km	-12 / -3	-32 / -10	No Dying Gasp, 1 hilo, Cliente
RC602-GE-S1	MC GigaEthernet SM, hasta 25 Km	SC, SM	1310	0 - 25 km	-10 / -3	<-23	No Dying Gasp, 2 hilos, POP/Cliente
RC602-GE-SS13	MC GigaEthernet monofibra 1550, hasta 25 Km	SC, SM	TX 1310 / RX 1550	0 - 25 km	-5 / -0	<-20	No Dying Gasp, 1 hilo, Cliente
RC602-GE-SS15	MC GigaEthernet monofibra 1310, hasta 25 Km	SC, SM	TX 1550 / RX 1310	0 - 25 km	-5 / -0	<-20	No Dying Gasp, 1 hilo, POP
RC602-GE-SS24	MC FastEthernet monofibra 1550, hasta 50 Km	SC, SM	TX 1550 / RX 1310	10-50 km	-3 / -2	<-20	No Dying Gasp, 1 hilo, Cliente
RC602-GE-SS25	MC FastEthernet monofibra 1310, hasta 50 Km	SC, SM	TX 1310 / RX 1550	10-50 km	-3 / -2	<-20	No Dying Gasp, 1 hilo, POP
RC832-30-BL-M	MC E1 120ohm, MM hasta 2 Km	SC, MM	1310	0 - 2 km	-20 / -14	-28 / -14	Dying Gasp, POP/Cliente
RC832-30-BL-S1	MC E1 120ohm, SM hasta 25 Km	SC, SM	1310	0 - 25 km	-15 / -8	-34 / -8	Dying Gasp, POP/Cliente
RC832-30-BL-SS15	MC E1 120 ohm, monofibra 1550, hasta 25 Km	SC, SM	TX 1550 / RX 1310	0 - 25 km	-12 / -3	-30 / -8	Dying Gasp, POP/Cliente
RC832-30-BL-SS13	MC E1 120 ohm, monofibra 1310, hasta 25 Km	SC, SM	TX 1310 / RX 1550	0 - 25 km	-12 / -3	-30 / -8	Dying Gasp, POP/POP
RC832-30-BL-SS25	MC E1 120 ohm, monofibra 1550, hasta 50 Km	SC, SM	TX 1550 / RX 1310	10 - 50 km	-5 / -0	<-32	Dying Gasp, POP
RC832-30-BL-SS23	MC E1 120 ohm, monofibra 1310, hasta 50 Km	SC, SM	TX 1310 / RX 1550	10 - 50 km	-12 / -3	<-32	Dying Gasp, Cliente
RCMS2802-120LFE-BL-M	MC 4E1&FE, MM, hasta 2 Km	SC, MM	1310	0 - 2 km	-20 / -14	-28 / -14	Dying Gasp, POP/Cliente
RCMS2802-120LFE-BL-S1	MC 4E1&FE, SM, hasta 25 Km	SC, SM	1310	0 - 25 km	-15 / -8	-34 / -8	Dying Gasp, POP/Cliente
RCMS2802-120LFE-BL-SS13	MC 4E1&FE, monofibra 1310, hasta 25 Km	SC, SM	TX 1310 / RX 1550	0 - 25 km	-12 / -3	-30 / -8	Dying Gasp, 1 hilo, Cliente
RCMS2802-120LFE-BL-SS15	MC 4E1&FE, monofibra 1550, hasta 25 Km	SC, SM	TX 1550 / RX 1310	0 - 25 km	-12 / -3	-30 / -8	Dying Gasp, 1 hilo, POP

Anexo 2 Modelo de convertidores de medio.

Fuente: Capacitación claro

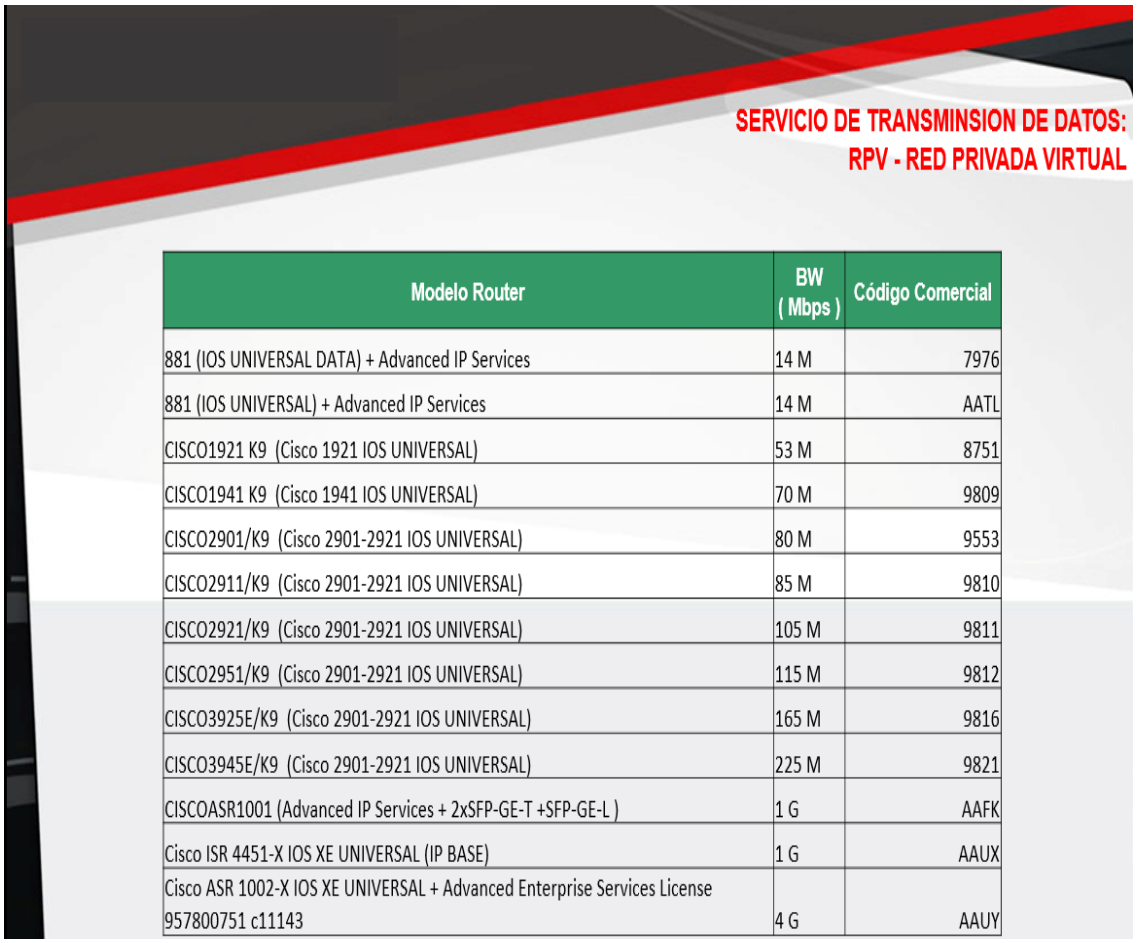


ITEM	CoS5	CoS4	CoS3	CoS2	CoS1
Tipo de Datos	Voz	Video	Datos Críticos	Datos Transaccionales	Datos No críticos
Prioridad	Máxima	Máxima	Máxima	P2 / IP DSCP 16	Normal
IP DSCP	CS5 (40), EF(46)	CS3 (24), AF41, AF42, AF43	CS2 (16), AF22	CS1 (8), AF11, AF13	CS0
Ancho de Banda del Acceso	Sumatoria de los anchos de banda de cada una de las sedes				
Política aplicable al trafico excedente	Se descarta	Se descarta	Se Remarca como P1	Se Remarca como P1	No aplica
Aplicaciones	Voz/Telefonía IP	Video	Aplicaciones de Datos sensibles al retardo y criticas para el negocio como SNA, SAP, ERP.	Datos transaccionales (aplicaciones de negocio, intranet)	Datos generales (mail, trafico internet)

Clases de Servicio	Tráfico	IP DSCP	Valor
CoS 5	Voz	CS5, EF	40, 46
CoS 4	Video	CS3, AF41, AF42, AF43	24, 34, 36, 38
CoS 3	Datos Críticos	CS2, AF22	16, 20
CoS 2	Datos Transaccionales	CS1, AF11, AF13	8, 10, 14
CoS 1	Datos no Críticos	CS0	0

Anexo 3 Tabla de clases de servicio.

Fuente: Capacitación claro



Modelo Router	BW (Mbps)	Código Comercial
881 (IOS UNIVERSAL DATA) + Advanced IP Services	14 M	7976
881 (IOS UNIVERSAL) + Advanced IP Services	14 M	AATL
CISCO1921 K9 (Cisco 1921 IOS UNIVERSAL)	53 M	8751
CISCO1941 K9 (Cisco 1941 IOS UNIVERSAL)	70 M	9809
CISCO2901/K9 (Cisco 2901-2921 IOS UNIVERSAL)	80 M	9553
CISCO2911/K9 (Cisco 2901-2921 IOS UNIVERSAL)	85 M	9810
CISCO2921/K9 (Cisco 2901-2921 IOS UNIVERSAL)	105 M	9811
CISCO2951/K9 (Cisco 2901-2921 IOS UNIVERSAL)	115 M	9812
CISCO3925E/K9 (Cisco 2901-2921 IOS UNIVERSAL)	165 M	9816
CISCO3945E/K9 (Cisco 2901-2921 IOS UNIVERSAL)	225 M	9821
CISCOASR1001 (Advanced IP Services + 2xSFP-GE-T +SFP-GE-L)	1 G	AAFK
Cisco ISR 4451-X IOS XE UNIVERSAL (IP BASE)	1 G	AAUX
Cisco ASR 1002-X IOS XE UNIVERSAL + Advanced Enterprise Services License 957800751 c11143	4 G	AAUY

Anexo 4 Capacidad de B/W de router.

Fuente: Capacitación claro

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Densidad de ranuras y servicios				
Aceleración de cifrado integrada en hardware (IPSec + SSL)	Sí	Sí	Sí	Sí
Sesiones de Cisco Unified SRST	35	50	100	250
Sesiones de Cisco Unified CCME	35	50	100	150
Total de puertos WAN 10/100/1000 integrados	2	3	3	3
Puertos basados en RJ-45	2	3	3	3
Puertos basados en SFP (el uso del puerto SFP desactiva el puerto RJ-45 correspondiente)	0	0	1	1
Ranuras para módulos de servicio	0	1	1	2
Ranuras para módulos de servicio de doble ancho (el uso de una ranura de doble ancho ocupará todas las ranuras para módulos de servicio de ancho simple del router Cisco 2900)	0	0	1	1
Ranuras para EHWIC	4	4	4	4
Ranuras para EHWIC de doble ancho (el uso de una ranura para EHWIC de doble ancho ocupará dos ranuras para EHWIC)	2	2	2	2
Ranuras para ISM	1	1	1	1
Ranuras para DSP (PVDM) integradas	2	2	3	3
Memoria DRAM ECC DDR2 - Predeterminada	512 MB	512 MB	512 MB	512 MB
Memoria (DRAM ECC DDR2) - Máxima	2 GB	2 GB	2 GB	2 GB
Memoria Compact Flash (externa) - Predeterminada	Ranura 0: 256 MB Ranura 1: nada	Ranura 0: 256 MB Ranura 1: nada	Ranura 0: 256 MB Ranura 1: nada	Ranura 0: 256 MB Ranura 1: nada
Memoria Compact Flash (externa) - Máxima	Ranura 0: 4 GB Ranura 1: 4 GB	Ranura 0: 4 GB Ranura 1: 4 GB	Ranura 0: 4 GB Ranura 1: 4 GB	Ranura 0: 4 GB Ranura 1: 4 GB
Ranuras para memoria flash USB 2.0 externa (tipo A)	2	2	2	2
Puerto de consola USB (tipo B; hasta 115,2 kbps)	1	1	1	1
Puerto serie de consola	1	1	1	1
Puerto serie auxiliar	1	1	1	1
Fuentes de alimentación	CA y PoE	CA, PoE y CC*	CA, PoE y CC*	CA, PoE y CC*
Compatibilidad con RPS (externo)	No	Cisco RPS 2300	Cisco RPS 2300	Cisco RPS 2300
Especificaciones de alimentación				
Voltaje de entrada de CA	Rango automático de 100 a 240 VCA	Rango automático de 100 a 240 VCA	Rango automático de 100 a 240 VCA	Rango automático de 100 a 240 VCA
Frecuencia de entrada de CA	47 a 63 Hz	47 a 63 Hz	47 a 63 Hz	47 a 63 Hz
Rango de CA de entrada de la fuente de alimentación de CA (máx.)	1,5 a 0,6 A	2,2 a 1,0 A	3,4 a 1,4 A	3,4 a 1,4 A
Impulso transitorio de corriente de entrada de CA	<50 A	<50 A	<50 A	<50 A
Consumo normal de energía (sin módulos)	40 W	50 W	60 W	70 W
Potencia máxima con fuente de alimentación de CA	150 W	210 W	320 W	340 W

Anexo 5 Data-sheet router 2901

Fuente: CISCO SYSTEM

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Potencia máxima con fuente de alimentación PoE (plataforma únicamente)	175 W	250 W	370 W	405 W
Potencia PoE máxima en terminales desde una fuente de alimentación PoE	130 W	200 W	280 W	370 W
Capacidad de potencia PoE máxima en terminales con PoE aumentada	N/D	750 W	750 W	750 W
Especificaciones físicas				
Dimensiones (Al x An x Pr)	44,5 x 438,2 x 439,4 mm (1,75 x 17,25 x 17,3 pulg.)	44,5 x 438,2 x 304,9 mm (3,5 x 17,25 x 12 pulg.)	88,9 x 438,2 x 469,9 mm (3,5 x 17,25 x 18,5 pulg.)	88,9 x 438,2 x 469,9 mm (3,5 x 17,25 x 18,5 pulg.)
Altura de bastidor	1 RU (unidad de bastidor)	2 RU	2 RU	2 RU
Montaje en bastidor EIA de 48,3 cm (19 pulg.)	Incluido	Incluido	Incluido	Incluido
Montaje en bastidor EIA de 58,4 cm (23 pulg.)	Opcional	Opcional	Opcional	Opcional
Montaje en pared (consulte la guía de instalación para averiguar la orientación aprobada)	Sí	Sí	No	No
Peso con fuente de alimentación de CA (sin módulos)	6,1 kg (13,4 libras)	8,2 kg (18 libras)	13,2 kg (29 libras)	13,2 kg (29 libras)
Peso con fuente de alimentación PoE y CA (sin módulos)	6,5 kg (14,3 libras)	8,6 kg (19 libras)	13,6 kg (30 libras)	13,6 kg (30 libras)
Peso normal totalmente configurado	7,3 kg (16 libras)	9,5 kg (21 libras)	15,5 kg (34 libras)	15,5 kg (34 libras)
Flujo de aire	Desde el frente hacia el lateral	Desde un lateral hacia el otro lateral	Desde el frente hacia la parte posterior	Desde el frente hacia la parte posterior
Kit de flujo de aire opcional	N/D	Desde el frente hacia la parte posterior	N/D	N/D
Especificaciones ambientales				
Condiciones de funcionamiento				
Temperatura: altitud máxima de 1800 m (5906 pies)	0 a 40 °C (32 a 104 °F)	0 a 40 °C (32 a 104 °F)	0 a 40 °C (32 a 104 °F)	0 a 40 °C (32 a 104 °F)
Temperatura: altitud máxima de 3000 m (9843 pies)	0 a 25 °C (32 a 77 °F)	0 a 40 °C (32 a 104 °F)	0 a 40 °C (32 a 104 °F)	0 a 40 °C (32 a 104 °F)
Temperatura: altitud máxima de 4000 m (13.123 pies)	N/D	0 a 30 °C (32 a 86 °F)	0 a 30 °C (32 a 86 °F)	0 a 30 °C (32 a 86 °F)
Temperatura: altitud máxima de 1800 m (5906 pies) a corto plazo (según NEBS)	N/D	-5 a 50 °C (23 a 122 °F)	N/D	-5 a 50 °C (23 a 122 °F)
Altitud	3000 m (10.000 pies)	4000 m (13.000 pies)	3000 m (10.000 pies)	4000 m (13.000 pies)
Humedad relativa	10 a 85%	5 a 85%	10 a 85%	5 a 85%
Humedad a corto plazo (según NEBS)	N/D	5 a 90%, pero sin exceder 0,024 kg de agua por kg de aire seco	N/D	N/D
Acústica: presión sonora (normal/máxima)	41/53 dBA	51,8/62,9 dBA	54,4/67,4 dBA	54,4/67,4 dBA
Acústica: potencia sonora (normal/máxima)	49/61 dBA	58,5/70,3 dBA	62,6/74,5 dBA	62,6/74,5 dBA
Condiciones para el transporte y almacenamiento				
Temperatura	-40 a 70 °C (-40 a 158 °F)	-40 a 85 °C (-40 a 176 °F)	-40 a 70 °C (-40 a 158 °F)	-40 a 70 °C (-40 a 158 °F)
Humedad relativa	5 a 95%	5 a 95%	5 a 95%	5 a 95%
Altitud	4570 m (15.000 pies)	4570 m (15.000 pies)	4570 m (15.000 pies)	4570 m (15.000 pies)
Conformidad reglamentaria				
Seguridad	UL 60950-1 CAN/CSA C22.2 Nº 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 Nº 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 Nº 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 Nº 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1

Anexo 6 Data-sheet router 2901

Fuente: CISCO SYSTEM