UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE INGENIERÍA

INGENIERÍA ELECTRÓNICA

PROYECTO DE GRADO

"DISEÑO DE RED CORPORATIVA WAN/LAN BASADO EN EL PROTOCOLO MPLS CON DIRECCIONAMIENTO DUAL-STACK (IPv4-IPv6)"

POSTULANTE: Univ. EDSON CRISTIAN GUERRA CALLISAYA

TUTOR: ING. ÁLVARO RAMÍREZ PATIÑO

LA PAZ – BOLIVIA

2021

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE INGENIERIA

LA FACULTAD DE INGENIERIA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) Visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) Copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) Copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la cita o referencia correspondiente en apego a las normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

DEDICATORIA

Dedico el presente proyecto de grado a mi familia, que de manera incondicional me apoyaron en cumplir mis sueños y alcanzar mis metas lo cual han sido mi mayor fuente de inspiración.

A mi abuelo Eliodoro Guerra, con la seguridad que desde el cielo se siente muy orgulloso por este logro, para mí es un ejemplo a seguir y me enseño que todo se puede lograr en la vida, alentándome a seguir adelante para así alcanzar cada una de mis metas.

AGRADECIMIENTO

En primer lugar agradezco a Dios por todas las oportunidades que me ha dado, por todas las puertas que me abrió, por su provisión diaria y todo su amor con el que me ha mantenido hasta el día de hoy, y por darme la oportunidad de honrarle a mi familia con este logro, agradezco a mi mamá, Eustaquia Callisaya, por sus enseñanzas, esfuerzos y ser un gran ejemplo para mi vida, a mi Papá, Renso Guerra, por todos sus consejos, palabras y apoyo que me brindo.

Agradezco a mi tutor el Ingeniero Álvaro Ramírez Patiño por todo su apoyo, paciencia, orientación, confianza y motivación hacia mi persona, a lo largo del desarrollo del presente proyecto de grado, también agradezco al Ingeniero Gonzalo Caba por sus consejos y orientaciones, y a todos los Ingenieros que, a lo largo de mi formación profesional, me han transmitido sus conocimientos con dedicación y llegaron a ser admirables en nuestra carrera.

RESUMEN

Ante la necesidad de las empresas corporativas de contar con redes de transmisión de datos fiables, ágiles, convergentes y en tiempo real, se requiere que el desarrollo de la infraestructura incorpore en su diseño estas características y optimice el uso de los recursos, garantizando la disponibilidad de los servicios.

Aplicando este concepto, en el presente Proyecto se desarrolla el diseño de una Red Corporativa Nacional de Transmisión de datos basada en MPLS para una empresa dedicada al rubro de las Telecomunicaciones.

La Ingeniería del Proyecto plantea implementar MPLS en las Redes LAN/WAN de la empresa. Se asume que se alquilaran servicios de transmisión de datos (VPN Capa 2) de un proveedor local para interconectar las sedes nacionales y locales.

Por otra parte, ante el surgimiento de IPv6 y la presencia actual de IPv4 se pretende que ambos protocolos coexistan, por lo que se implementara el direccionamiento Dual – Stack, lo cual permitirá a la compañía estar preparada, cuando la transición de IPv4 a IPv6 se haya completado, logrando así que la compañía no realice gastos en renovación de equipos de su red ni en el rediseño de la misma en un periodo a largo plazo.

ABSTRACT

Given the need for corporate companies to have reliable, agile, convergent and real-time data transmission networks, the development of the infrastructure is required to incorporate these characteristics into their design and optimize the use of resources, guaranteeing availability of services.

Applying this concept, this project develops the design of a National Corporate Network for Data Transmission based on MPLS for a company dedicated to Telecommunications.

Project Engineering proposes to implement MPLS on the company's LAN/WAN networks. It is assumed that data transmission services (VPN Layer 2) were rented from a local provider to interconnect national and local headquarters.

On the other hand, given the emergence of IPv6 and the current presence of IPv4, it is intended that both protocols coexist, so the Dual - Stack addressing will be implemented, which will allow the company to be prepared, when the transition from IPv4 to IPv6 is has completed, thus ensuring that the company does not incur expenses in the renewal of equipment in its network or in the redesign of it in a long-term period.

ÍNDICE GENERAL

LISTA DE FIGURAS

LISTA DE TABLAS

Glosario de Términos

AS (Automous System: Sistema Autónomo)

ATM (Asynchronous Transfer Mode: Modo de Transferencia Asincrónico)

AToM (Any Transport over MPLS: Cualquier Transporte sobre una Red MPLS)

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

BoS (Bottom of Stack: Parte Inferior de la Pila)

CBWFQ (Class-Based Weighted Fair Queuing: Colas Ponderadas Basadas en Clase)

CE (Customer Edge: Equipo del Cliente)

DNS (Domain Name System: Sistema de Nombres de Dominio)

DS (Differentiated Services: Servicios Diferenciados)

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

ELSR (Edge Label Switching Routing: Enrutamiento de Conmutación de Etiquetas en el Borde)

FEC (Forwarding Equivalence Class: Clase de Equivalencia de Reenvío)

FIB (Forwarding Information Base: Base de Información de Reenvío)

HDLC (High-Level Data Link Control: Control de Enlace de Datos de Alto Nivel)

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

IPSec (Internet Protocol Security: Protocolo de Seguridad de Internet)

IPv4 (Internet Protocol version 4: Protocolo de Internet versión 4)

IPv6 (Internet Protocol version 6: Protocolo de Internet versión 6)

ISP (Internet Service Provider: Proveedor de Servicios de Internet)

L2TP (Layer 2 Tunnelling Protocol: Protocolo de Tunelización de Capa 2)

LAN (Local Area Network: Red de Área Local)

LDP (Label Distribution Protocol: Protocolo de Distribución de Etiquetas)

LER (Label Edge Router: Router de Borde de Etiquetado)

LFIB (Label Forwarding Information Base: Base de Información de Reenvío de Etiquetas)

LIB (Label Information Base: Base de Información de Etiquetas)

LLQ (Low-Latency Queuing: Colas de Baja Latencia)

LSP (Label Switched Path: Ruta de Conmutación de Etiquetas)

LSR (Label Switching Router: Router Conmutador de Etiquetas)

MPLS (Multi Protocol Label Switching: Conmutación de Etiquetas Multiprotocolo)

NAT (Network Address Translation: Traducción de Direcciones de Red)

OSI (Open System Interconnection: Modelo de Interconexión de Sistemas Abiertos)

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

P (Provider: Proveedor)

PBX (Private Branch Exchange: Centralita Privada)

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

PE (Provider Edge: Borde del Proveedor)

PPP (Point-to-Point Protocol: Protocolo Punto a Punto)

PPTP (Point to Point Tunneling Protocol: Protocolo de Tunelización de Punto a Punto)

PQ (Priority Queueing: Colas de Prioridad)

QoS (Quality of Service: Calidad de Servicio)

SIP (Session Initiation Protocol: Protocolo de Inicio de Sesión)

SNMP (Simple Network Management Protocol: Protocolo Simple de Administración de Red)

TCP (Transmission Control Protocol: Protocolo de Control de Transmisión)

TTL (Time To Live: Tiempo de Vida de un Paquete)

UDP (User Datagram Protocol: Protocolos de Datagramas de Usuario)

VLAN (Virtual Local Area Network: Red de Área Local Virtual)

VoIP (Voice over IP: Voz sobre IP)

VPN (Virtual Private Network: Red Privada Virtual)

WAN (Wide Area Network: Red de Área Amplia)

CAPITULO I
INTRODUCCIÓN

1.1. INTRODUCCIÓN

Hoy en día, ante el constante crecimiento y demanda de tráfico de los dispositivos o terminales, surge la necesidad de garantizar la gran capacidad de procesamiento y encaminamiento de los paquetes, además de realizar una priorización de paquetes, según la aplicación que lo requiera.

Es ahí donde encontramos a MPLS (Multi Protocol Label Switching, Conmutación de Etiquetas Multiprotocolo), creada para redes que permitan interactuar con diferentes protocolos y tecnologías sin que se presente ningún conflicto entre ellas, además de ofrecer características que mejoren la experiencia del usuario final, escalabilidad, rendimiento y mejor uso del ancho de banda.

Por otra parte, al tener una enorme cantidad de dispositivos que acceden a contenidos y servicios de Internet, implica el agotamiento de direcciones IPv4, por lo tanto, la mayoría de las redes tienen asignadas direcciones IPv4, siendo necesario realizar una transición de IPv4 a IPv6, para ello se puede recurrir a la técnica de Dual-Stack (Dos pilas de protocolos), la cual permite que IPv4 e IPV6 coexistan en la misma red.

En los últimos años, las empresas corporativas requieren la optimización de su tráfico, diferenciación de clases de servicio, y seguridad; por lo que la implementación del protocolo MPLS a la red corporativa es de mucho beneficio para la empresa.

1.2. ANTECEDENTES

Las Telecomunicaciones permiten realizar el intercambio de información de diversas fuentes (empresas, instituciones, universidades, etc.), dando lugar a la integración de tráficos diversos (datos, videos, audio, etc.) sobre una misma red, aplicando de esta manera plenamente el concepto de convergencia.

Debido a ello surgieron varias tecnologías de transporte y se desarrollaron protocolos con el objetivo de optimizar la transmisión de datos. Así es que nace el protocolo IP, que es la base fundamental de Internet, el cual regula la transmisión de paquetes de datos entre las redes. Sin embargo, al tratarse de un protocolo no orientado a la conexión, sino más bien al del “mejor esfuerzo (best effort)”, no garantiza que los paquetes lleguen a su destino, ni ofrece una determinada calidad de servicio (QoS).

A medida que las aplicaciones en general y las corporativas en particular requieren de infraestructuras de red con mayor y mejor rendimiento, Internet representa un medio insatisfactorio para alcanzar estas crecientes necesidades. Este hecho se pone de manifiesto particularmente en aplicaciones en tiempo real como VoIP, Video, etc., donde la calidad de la transmisión de datos se ve seriamente afectada, ocasionando percepción de intermitencia, latencia y lentitud en los usuarios.

Por lo expuesto, las Empresas Corporativas requieren la implementación de Redes de Datos fiables, sólidas, convergentes y de fácil administración.

1.3. PROBLEMÁTICA

Actualmente, las Empresas Corporativas en el rubro de Telecomunicaciones con presencia Local, Nacional e Internacional, requieren trabajar sobre Redes de Transmisión de Datos Eficientes, de alta disponibilidad y seguras, donde la dependencia de terceros es estrictamente necesaria. En tal sentido, su diseño debe garantizar la confidencialidad del tráfico cursado y autogestión.

Por otra parte, ante el agotamiento rápido de direcciones IPv4, debido al crecimiento exponencial de dispositivos que se conectan a la red de Internet, llevan a la necesidad de implementar IPv6. Sin embargo, el diseño de IPv6 no es compatible con el de su predecesor IPv4 lo que retrasa el desarrollo de la migración completa de IPv4 a IPv6. Por lo que se tiene que emplear mecanismos de transición para lograr este objetivo.

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

Diseñar una Red Corporativa WAN/LAN, implementando el protocolo MPLS con la técnica de transición Dual-Stack (IPv4-IPv6), brindando calidad de servicio, seguridad y uso eficiente del ancho de banda.

1.4.2. OBJETIVOS ESPECÍFICOS

- Determinar la arquitectura de red óptima para la implementación del protocolo MPLS en la Red Corporativa.

- Estimar la cantidad de dispositivos que conformaran las Redes LAN/WAN.

- Establecer los requerimientos de Ancho de Banda que requerirá cada elemento en la Red.

- Analizar los distintos tipos de tráfico que se pueden cursar en la Red, de tal forma de otorgar prioridad al tráfico crítico para la empresa.

- Elaborar una planificación para la coexistencia de los protocolos IPv4 e IPv6 mediante el mecanismo de transición Dual-Stack.

- Definir los elementos de Red de BackBone, en función a las características y especificaciones técnicas que se adecuen al modelo de Red diseñado.

- Realizar un análisis económico Costo/Beneficio, para evaluar la factibilidad del Proyecto, en función a los elementos de Red que comprenderá la misma.

- Realizar en la medida de las posibilidades una implementación del proyecto, mediante algún simulador de redes.

1.5. JUSTIFICACIÓN

1.5.1. JUSTIFICACIÓN ACADÉMICA

Entender el funcionamiento, arquitectura y dispositivos que conforman una red MPLS, para aplicar al diseño de la red corporativa, y conocer las ventajas y beneficios que brinda esta tecnología.

1.5.2. JUSTIFICACIÓN TECNOLÓGICA

La implementación del protocolo MPLS ofrece diversos beneficios a operadores de servicio y/o empresas, como la escalabilidad, tolerancia a fallas, y la posibilidad de una única salida a internet para toda la compañía.

Por otra parte, la implementación del direccionamiento IPv6 a la red, permitirá a la empresa estar lista, cuando la transición de IPv4 a IPv6 se haya completado a nivel global, por lo que no tendrá que realizar gastos extras en la arquitectura de la red.

1.5.3. JUSTIFICACIÓN SOCIOECONÓMICA

La implementación de una red basada en el protocolo MPLS, permitirá a la empresa gestionar la prioridad del tráfico (telefonía, video, datos, etc), tener mayor seguridad y privacidad entre las sedes que la conforman, realizar menos gastos de mantenimiento a la red y fácil migración que otras soluciones existentes.

1.6. ALCANCES

El desarrollo del Proyecto consiste en el diseño de una red MPLS con direccionamiento dual-stack (IPv4-IPv6), con caso de aplicación para una Empresa ficticia. La decisión de implementación de la metodología de diseño del presente Proyecto quedara en decisión de las Empresas interesadas.

Se determinará la arquitectura óptima para la implementación de la Tecnología MPLS en la Red ajustándose a los requerimientos de la Empresa, que permita brindar Calidad de Servicio, eficiencia y rendimiento óptimo en la Red.

Se realizará la cuantificación de la cantidad de hosts que conformaran las Redes WAN/LAN y el Ancho de Banda promedio que requerirá cada elemento. Se analizará las distintas clases de tráfico en la red de tal forma de aplicar políticas de Calidad de Servicio para cada una de las mismas.

Se realizará una planificación del direccionamiento IP y definición de los Anchos de Banda requeridos para los enlaces Nacionales (WAN) y la salida del tráfico de la Empresa a la red de Internet.

Se asume que se alquilarán recursos de un proveedor de servicios de Transmisión de Datos para el transporte nacional y local del tráfico generado en la Red. El proveedor garantizará la disponibilidad requerida para este tipo de servicios.

CAPITULO II
MARCO TEÓRICO

2.1. Tecnologías WAN

Las operaciones WAN se centran principalmente en la capa física (capa 1 del modelo OSI) y en la capa de enlace de datos (capa 2 del modelo OSI). En general, los estándares de acceso WAN describen métodos de distribución de la capa física y requisitos de la capa de enlace de datos. Los requisitos de la capa de enlace de datos incluyen asignación de direcciones físicas, control de flujo y encapsulamiento.

Los protocolos de capa 1 describen la manera de proporcionar conexiones eléctricas, mecánicas, operativas y funcionales a los servicios de un proveedor de servicios de comunicación.

Los protocolos de capa 2 definen la forma en que se encapsulan los datos para la transmisión a una ubicación remota, así como los mecanismos para transferir las tramas resultantes. Se usa una variedad de tecnologías diferentes, como el protocolo punto a punto (PPP), Frame Relay, ATM, WAN Ethernet y algunos otros. Algunos de estos protocolos usan el mismo entramado básico o un subconjunto del mecanismo de control de enlace de datos de alto nivel (HDLC).

2.1.1. Frame Relay

La retransmisión de tramas (Frame Relay) es una tecnología WAN multiacceso sin difusión (NBMA) simple de capa 2 que se utiliza para interconectar las redes LAN de una empresa. Para conectarse a varios sitios mediante PVC, se puede usar una única interfaz de router. Los PVC se usan para transportar tráfico de voz y datos entre origen y destino y admiten velocidades de datos de hasta 4 Mb/s, si bien algunos proveedores ofrecen velocidades aún mayores.

2.1.2. ATM

La tecnología del modo de transferencia asíncrona (ATM) puede transferir voz, video y datos a través de redes privadas y públicas. Se construye sobre una

arquitectura basada en celdas, en vez de una arquitectura basada en tramas. Las celdas ATM tienen siempre una longitud fija de 53 bytes. La celda ATM contiene un encabezado ATM de 5 bytes, seguido de 48 bytes de contenido ATM. Las celdas pequeñas y de longitud fija son adecuadas para transportar tráfico de voz y video, debido a que este tipo de tráfico no admite retrasos. El tráfico de voz y video no tiene que esperar a que se transmitan paquetes de datos más grandes.

La celda ATM de 53 bytes es menos eficaz que las tramas y los paquetes más grandes de Frame Relay. Además, la celda ATM tiene por lo menos 5 bytes de sobrecarga por cada contenido de 48 bytes. Una línea ATM típica necesita casi un 20% más de ancho de banda que Frame Relay para transportar el mismo volumen de datos de capa de red.

ATM se diseñó para ser extremadamente escalable y para admitir las velocidades de enlace de T1/E1 a OC-12 (622 Mb/s) y más. ATM ofrece PVC y SVC, si bien los PVC son más comunes con las WAN. Al igual que sucede con otras tecnologías de uso compartido, ATM permite varios VC en una única conexión de línea arrendada al perímetro de la red.

2.1.3. WAN Ethernet

Originalmente, Ethernet se desarrolló para que fuera una tecnología de acceso a LAN. En un principio, Ethernet no era conveniente como tecnología de acceso WAN porque, en ese momento, la longitud de cable máxima era un kilómetro. No obstante, los estándares de Ethernet más recientes que utilizan cables de fibra óptica hicieron de Ethernet una opción de acceso WAN razonable. Por ejemplo, el estándar IEEE 1000BASE-LX admite longitudes de cable de fibra óptica de 5 km, mientras que el estándar IEEE 1000BASE-ZX admite longitudes de cable de hasta 70 km.

Los proveedores de servicios ahora ofrecen servicio WAN Ethernet con cableado de fibra óptica. El servicio WAN Ethernet se puede conocer con distintos nombres, incluidos Ethernet metropolitana (MetroE), Ethernet por MPLS (EoMPLS) y el servicio de LAN privada virtual (VPLS).

Beneficios de una WAN Ethernet:

- **Reducción de gastos y administración:** WAN Ethernet proporciona una red de conmutación de capa 2 con un ancho de banda elevado que es capaz de administrar datos, voz y video en la misma infraestructura. Esta característica aumenta el ancho de banda y elimina las conversiones costosas a otras tecnologías WAN. La tecnología permite que las empresas conecten varios sitios en un área metropolitana, entre sí y a Internet, de forma económica.

- **Fácil integración con las redes existentes:** WAN Ethernet se conecta fácilmente a las LAN Ethernet existentes, lo que reduce los costos y el tiempo de instalación.

- **Productividad mejorada de la empresa:** WAN Ethernet permite que las empresas aprovechen las aplicaciones IP para mejorar la productividad, como las comunicaciones IP alojadas, VoIP y transmisión y difusión de video.

2.2. MPLS (Multiprotocol Label Switching)

2.2.1. Definición de MPLS

MPLS (Multi Protocol Label Switching, Conmutación de Etiquetas Multiprotocolo), es una tecnología de reenvío de paquetes, que utiliza las etiquetas para tomar decisiones de reenvío de datos; cuya finalidad es brindar soluciones de conmutación multinivel, que permita la transmisión de diferentes tipos de tráfico (paquetes IP, tráfico de Voz, tráfico de Video, etc.), y priorizar cada uno de estos.

Las etiquetas MPLS se anuncian entre routers para que puedan crear una asignación de etiqueta a etiqueta, estas se adjuntan a los paquetes IP, lo que permite a los routers reenviar el tráfico mirando solamente la etiqueta y no la dirección IP de destino.

De esta forma el análisis del encabezado de capa 3 (Red) del modelo OSI, se realiza solo una vez (cuando el paquete ingresa al dominio MPLS), disminuyendo la sobrecarga de reenvío en los routers principales.

2.2.2. Beneficios de MPLS

- La necesidad de aumentar la velocidad de procesamiento en la CPU de los routers, ya que el proceso de conmutación de paquetes IP se considera muy lenta. Un router reenvía un paquete IP buscando la dirección IP de destino en el encabezado IP, y debe encontrar la mejor ruta en su tabla de enrutamiento, esta búsqueda puede resultar muy compleja debido a la cantidad de bits a analizar: 32 bits (en el caso de IPv4) o 128 bits (en el caso de IPv6), por lo que el analizar solamente un valor de una etiqueta MPLS (campo de 20 bits), agiliza el proceso de enrutamiento en una red con MPLS.

- Una de las razones por las que el protocolo IP, domina el mundo de las redes, es debido a que puede transportar muchas tecnologías a través de él. Sin embargo, no solamente se transportan datos, en la actualidad también se transporta telefonía sobre IP, video, etc. Por lo que al usar MPLS con IP se amplía las posibilidades de transportar otros protocolos (IPv4, IPv6, HDLC, PPP y otras tecnologías de capa 2) sobre un paquete IP de capa 3.

- Las Empresas Corporativas al implementar MPLS, podrán gestionar el tráfico cursado en sus redes, permitiendo diferenciar los flujos de tráfico (Calidad de Servicio), conjuntamente aplicando Ingeniería de Tráfico, las operaciones en la red serán eficientes y fiables, pero al mismo tiempo, la utilización de los recursos de la red y el rendimiento serán óptimos.

2.2.3. Estructura de MPLS

El elemento más importante para MPLS es la etiqueta (Label), esta es un identificador corto, de cuatro bytes (32 bits), de longitud fija y localmente significativo que se utiliza para identificar una Clase de Equivalencia de Reenvío (FEC). La

etiqueta que se coloca en un paquete particular representa el FEC al que se asigna a ese paquete.

Figura 1: Cabecera MPLS
Fuente: CiscoPress MPLS Fundamentals

Etiqueta: Es el valor de la etiqueta que identifica una FEC (con significado local).

EXP: Bits de uso experimental, se utilizan únicamente para calidad de servicio (QoS).

BoS (Bottom of Stack): Bit que se pone en "1" si la etiqueta está en la parte inferior de la pila, cero para el resto. La pila es la colección de etiquetas (puede ser una sola etiqueta o varias) que se encuentran en la parte superior del paquete.

TTL (Time To Live): 8 bits que tienen la misma función que el campo TTL encontrado en una cabecera IP, simplemente se reduce en 1 en cada salto, su función principal es evitar que un paquete se quede atascado en un bucle de enrutamiento.

2.2.3.1. Pila de Etiquetas MPLS

En un proceso de enrutamiento de un paquete, puede ocurrir que los routers (compatibles con MPLS) necesiten más de una etiqueta para enrutar el paquete a través de la red, para ello se realiza un apilamiento de etiquetas, de manera que se forma una pila de etiquetas (Label Stack), donde la primera etiqueta es denominada "etiqueta superior" y la última etiqueta "etiqueta inferior". En el medio podríamos tener cualquier cantidad de etiquetas (Figura 2).

Dos aplicaciones que necesitan más de una etiqueta son MPLS VPN y AToM, los cuales colocan dos etiquetas en la pila de etiquetas.

Etiqueta	EXP	0	TTL
Etiqueta	EXP	0	TTL
Etiqueta	EXP	0	TTL
.			
.			
.			
Etiqueta	EXP	1	TTL

Figura 2: Estructura de la Pila de Etiquetas
Fuente: CiscoPress MPLS Fundamentals

En la Figura 2, también podemos observar el comportamiento del bit BoS, el cual tiene un valor de 0 para todas las etiquetas, excepto para la etiqueta inferior, en esta última el bit BoS se establece en 1.

2.2.3.2. Codificación de MPLS

El modelo de referencia OSI consiste en 7 capas, (Ver Figura 3):

Figura 3: Modelo OSI
Fuente: CCNA 1 v6.0

La capa Física (Capa 1) describe los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas para la transmisión de bits desde y hacia un dispositivo de la red.

La capa de Enlace de Datos (Capa 2) permite a las capas superiores acceder a los medios, acepta paquetes de Capa 3 y los empaqueta en tramas, algunos ejemplos de datos en la Capa 2 son: HDLC, PPP, Frame Relay y Ethernet. La importancia de esta capa es solo el enlace entre dos máquinas. Lo que significa que el encabezado de esta capa siempre se reemplaza por la máquina en el otro extremo del enlace.

La capa de Red (Capa 3) se preocupa del formato de los paquetes, para intercambiar los datos individuales en la red entre terminales identificados, el protocolo más conocido en esta capa es IP.

MPLS no es un protocolo de Capa 2, porque la encapsulación de Capa 2 todavía está presente en los paquetes etiquetados. MPLS tampoco es realmente un protocolo de Capa 3 porque el protocolo de Capa 3 todavía está presente. Por lo tanto, MPLS es una capa intermedia (Capa 2.5) entre el encabezado de Capa 2 y el encabezado de Capa 3. Es en esta ubicación donde se encuentra la pila de etiquetas (Label Stack) (Ver Figura 4).

Figura 4: Encapsulación para un Paquete Etiquetado
Fuente: CiscoPress MPLS Fundamentals

Debido a que la pila de etiquetas se coloca delante del encabezado de Capa 3 u otro protocolo transportado, se debe tener nuevos valores para el campo de Protocolo de Capa 2, para indicar que lo que sigue al encabezado de Capa 2 es un paquete etiquetado MPLS.

El campo de Protocolo de la Capa de Enlace de Datos es un valor que indica qué tipo de carga útil es lo que lleva la trama de Capa 2 (Ver Tabla 1).

Tipo de Encapsulacin de Capa 2	Nombre de Identificador de Protocolo de Capa 2	Valor (Hexadecimal)
PPP	Campo de Protocolo PPP	0281
Ethernet/802.3 LLC/SNAP	Valor de Ethertype	8847
HDLC	Protocolo	8847
Frame Relay	NLPID (Network Level Protocol ID)	80

Tabla 1: Valores identificadores del protocolo MPLS
para los tipos de encapsulación de Capa 2
Fuente: CiscoPress MPLS Fundamentals

ATM no figura en la Tabla 1, porque utiliza una forma única de encapsular la etiqueta.

2.2.4. Arquitectura de una Red MPLS

En la arquitectura de una red MPLS se deben identificar primeramente los elementos principales que conforman la misma, para poder describir su funcionamiento, a continuación, se detallan los equipamientos principales:

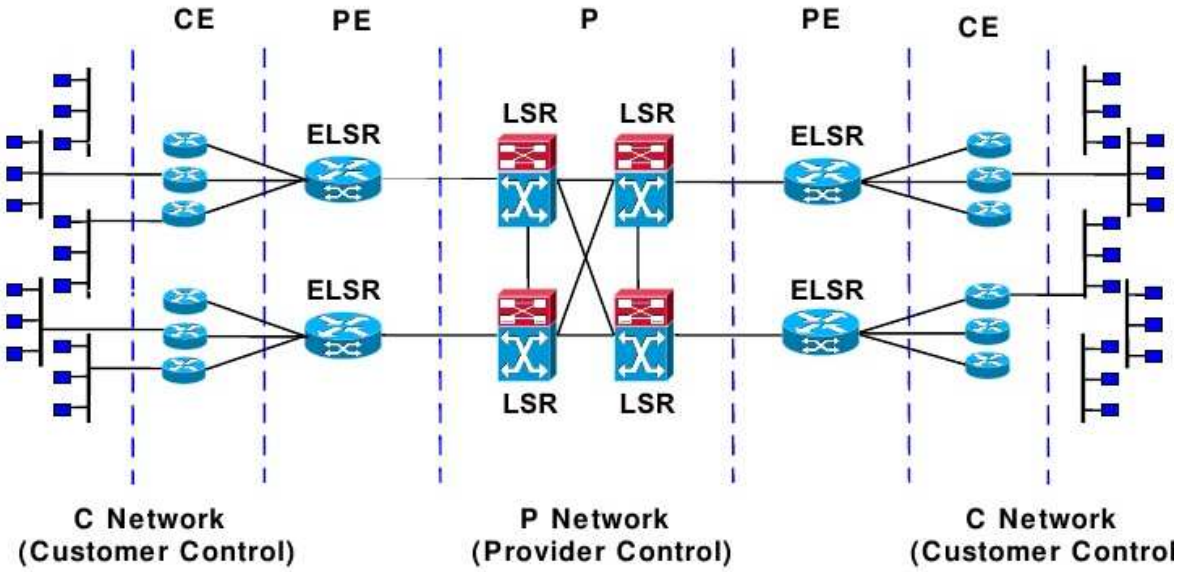


Figura 5: Arquitectura de una red MPLS
Fuente: De Brouwer, 2008

- **LSR (Label Switch Router). –** Es un router conmutador de etiquetas que admite MPLS. Es capaz de entender etiquetas MPLS y de recibir y transmitir un paquete etiquetado en un enlace de datos. Existen tres tipos de LSR en una red MPLS:
  - LSRs de Entrada. - Los LSR de entrada reciben un paquete que aún no está etiquetado, insertan una etiqueta (pila) delante del paquete y lo envían sobre un enlace de datos.
  - LSRs de Salida. - Los LSR de salida reciben paquetes etiquetados, eliminan las etiquetas y los envían sobre un enlace de datos. Los LSR de entrada y salida son denominados LSR de borde.
  - LSRs Intermedios. - Los LSR intermedios reciben un paquete etiquetado entrante, realizan la operación de cambiar el paquete y enviarlo en el enlace de datos correcto.

Un LSR puede hacer tres operaciones: meter, sacar o intercambiar etiquetas.

- **CE (Customer Edge). -** Equipo instalado con el cliente y que tiene comunicación con el equipo PE.

- **FEC (Forward Equivalence Class). -** Una clase de equivalencia de reenvío (FEC) es un grupo o flujo de paquetes que se reenvían a lo largo del mismo camino y se tratan igual con respecto al tratamiento de reenvío. Todos los paquetes pertenecientes a la misma FEC tienen la misma etiqueta. Sin embargo, no todos los paquetes que tienen la misma etiqueta pertenecen la misma FEC, porque sus valores de EXP (Calidad de Servicio) pueden diferir; el tratamiento de reenvío podría ser diferente, y podrían pertenecer a una FEC diferente. El router que decide qué paquetes pertenecen a una determinada FEC es el LSR de Ingreso.

- **LSP (Label Switched Path). -** Una ruta de cambio de etiqueta (LSP) es una secuencia de LSRs que cambian un paquete etiquetado a través de una red MPLS o parte de una red MPLS.

En la figura 6, se observa el camino que sigue el paquete en la red MPLS y que este es unidireccional.

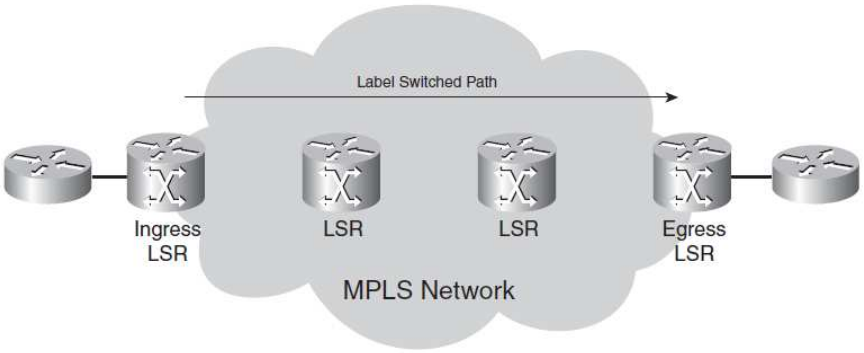


Figura 6: Un LSP a través de una red MPLS
Fuente: CiscoPress MPLS Fundamentals

Por otra parte, el LSR de Ingreso de un LSP no es necesariamente el primer router que etiqueta el paquete. El paquete podría ya haber sido etiquetado por un LSR anterior, sería el caso de un LSP anidado (Figura 7), es decir un LSP dentro de otro LSP). Un ejemplo de LSP anidado es de un túnel de respaldo de ingeniería de tráfico.

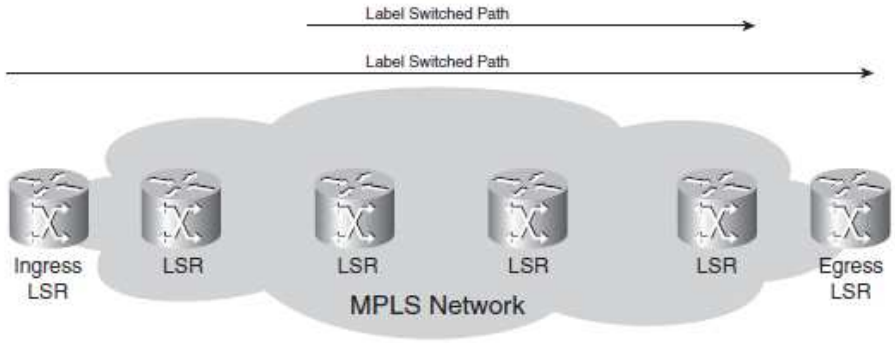


Figura 7: LSP anidado
Fuente: CiscoPress MPLS Fundamentals

LDP (Label Distribution Protocol). - Es un protocolo que usan los LSR para la asignación de etiquetas, se basa en las métricas IGP utilizadas en la red, negociando etiquetas salto a salto. El protocolo LDP presenta la ventaja de negociar etiquetas y establecer caminos automáticamente entre los routers LDP para los destinos en la FEC. Este comportamiento hace que el protocolo sea fácil de implementar y configurar, pero poco flexible y escalable.

Label Information Base (LIB). - Es la tabla de etiquetas que manejan los LSR. Relaciona la pareja (interfaz de entrada - etiqueta de entrada) con (interfaz de salida - etiqueta de salida).

Forwarding Information Base (FIB). - Es la tabla de rutas del router, pero con soporte hardware, basado en CEF. Esta tabla se actualiza automáticamente a petición de los protocolos de routing.

Label Forwarding Information Base (LFIB). - Es la tabla que asocia las etiquetas con los destinos o rutas de capa 3 y la interfaz de salida en el router, indicándole al router lo que tiene que hacer: poner o quitar etiqueta.

Con lo descrito anteriormente, para que la asignación de etiquetas sea de manera única, MPLS se conforma por un plano de control y un plano de datos.

- **Plano de Control. -** Es la encargada de llevar a cabo tareas destinadas a determinar la disponibilidad del acceso hacia una red destino. Por lo tanto, el plano de control contiene toda la información de direccionamiento de capa 3. Algunos ejemplos comunes acerca de las funciones de la capa de control es el intercambio de información por parte de los protocolos de enrutamiento tales como OSPF y BGP. Por lo tanto, el intercambio de información acerca del direccionamiento IP es una función del plano de control, además de todas las funciones que cumplen aquellos protocolos responsables del intercambio de etiquetas entre enrutadores vecinos tal como el protocolo de distribución de etiquetas.

- **Plano de Datos. -** Lleva a cabo tareas relacionadas con el reenvió de paquetes. Esos paquetes pueden ser ya sea paquetes IP o paquetes IP etiquetados. La información en el plano de datos, tal como el valor que llevan las etiquetas, se obtienen del plano de control.

2.2.5. Operación de MPLS

La implementación de MPLS para el reenvío de paquetes implica los siguientes cuatro pasos:

- Asignación de etiquetas MPLS. (por los LSR)
- Establecimiento de sesión MPLS LDP o TDP. (entre LSR / ELSR)
- Distribución de etiquetas MPLS. (usando un protocolo de distribución de etiquetas)
- Retención de etiquetas MPLS.

La operación de MPLS generalmente implica que los LSR adyacentes formen una sesión LDP, asignen etiquetas locales a los prefijos de destino e intercambien estas etiquetas en sesiones LDP establecidas. Al finalizar el intercambio de etiquetas entre los LSR adyacentes, las estructuras de control y datos de MPLS, FIB, LIB y LFIB, se completan y el router está listo para reenviar información del plano de datos en función de los valores de la etiqueta.

Asignación de etiquetas MPLS

Los protocolos de enrutamiento IP indican que tan accesible es una red destino y son los encargados de generar secuencias de saltos para los paquetes dentro de una red. El mismo proceso debe implementarse para los routers o dispositivos que forman parte del dominio MPLS para conocer las etiquetas asignadas a las redes de destino por los routers vecinos.

El protocolo de distribución de etiquetas (LDP o TDP) asigna e intercambia etiquetas entre LSR adyacentes en un dominio MPLS después del establecimiento de la

sesión. Como se mencionó anteriormente, las etiquetas se pueden asignar globalmente (por router) o por interfaz en un router.

Establecimiento de la sesión LDP

Después de la asignación de etiquetas en un router, estas etiquetas se distribuyen entre los LSR conectados directamente si las interfaces entre ellos están habilitadas para el reenvío de MPLS. Esto se hace utilizando LDP o el protocolo de distribución de etiquetas (TDP). TDP está en desuso y, por defecto, LDP es el protocolo de distribución de etiquetas. TDP y LDP funcionan de la misma manera, pero no son interoperables.

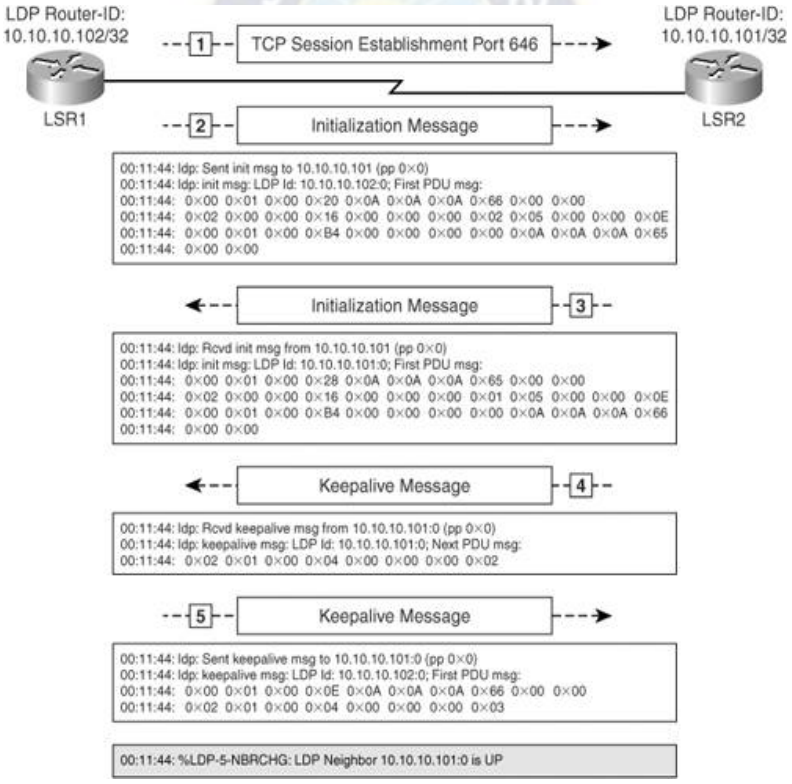


Figura 8: Ejemplo de Establecimiento de sesión LDP
Fuente: CiscoPress MPLS Fundamentals

Hay cuatro categorías de mensajes LDP:

- *Mensajes de descubrimiento:* Anuncian y mantienen la presencia de un LSR en la red.

- *Mensajes de sesión:* Establecen, mantienen y eliminan sesiones entre LSR.
- *Mensajes publicitarios:* Anuncian las asignaciones de etiquetas a las FEC.
- *Mensajes de notificación:* Muestran errores de señal.

Todos los mensajes LDP siguen el formato de tipo, longitud, valor (TLV). LDP usa el puerto TCP 646, y el LSR con la ID de enrutador LDP más alta abre una conexión al puerto 646 de otro LSR; el procedimiento para establecer la sesión LDP es el siguiente:

1. Las sesiones LDP se inician cuando un LSR envía saludos periódicos (usando la multidifusión UDP en 224.0.0.2) en las interfaces habilitadas para el reenvío de MPLS. Si otro LSR está conectado a esa interfaz (y la interfaz está habilitada para MPLS), el LSR conectado directamente intenta establecer una sesión con la fuente de los mensajes de saludo LDP. El LSR con la ID de enrutador LDP más alta es el LSR activo. El LSR activo intenta abrir una conexión TCP con el LSR pasivo (LSR con una ID de enrutador inferior) en el puerto TCP 646 (LDP).

2. El LSR activo luego envía un mensaje de inicialización al LSR pasivo, que contiene información como el tiempo de mantenimiento de la sesión, el método de distribución de etiquetas, la longitud máxima de la PDU y la ID LDP del receptor, y si la detección de bucle está habilitada.

3. El LDP pasivo LSR responde con un mensaje de inicialización si los parámetros son aceptables. Si los parámetros no son aceptables, el LDP LSR pasivo envía un mensaje de notificación de error.

4. El LSR pasivo envía un mensaje keepalive (mantener activa la sesión) al LSR activo después de enviar un mensaje de inicialización.

5. El LSR activo envía keepalive al LDP pasivo LSR, y aparece la sesión LDP. En este momento, se pueden intercambiar asignaciones de etiquetas FEC entre los LSR.

Distribución de etiquetas MPLS con LDP

En un dominio MPLS que ejecuta LDP, se asigna una etiqueta a un prefijo de destino que se encuentra en el FIB, y se distribuye a los vecinos ascendentes en el dominio MPLS después del establecimiento de la sesión. Las etiquetas que son de importancia local en el enrutador se intercambian con LSR adyacentes durante la distribución de etiquetas. La unión de etiquetas de un prefijo específico para una etiqueta local y una etiqueta de siguiente salto se almacena en las estructuras LFIB y LIB. Los métodos de distribución de etiquetas utilizados en MPLS son los siguientes:

- *Downstream on demand:* Este modo de distribución de etiquetas permite que un LSR solicite explícitamente al router downstream del siguiente salto una asignación de etiquetas a un prefijo de destino particular y, por lo tanto, se conoce como distribución de etiquetas de bajada sobre demanda.

- *Unsolicited downstream:* Este modo de distribución de etiquetas permite que un LSR distribuya enlaces a un LSR upstream que no los ha solicitado explícitamente y se denomina distribución de etiqueta de bajada no solicitada.

En la Figura 9, se muestra los dos modos de distribución de etiquetas entre R1 R2. En el proceso de downstream, el LSR R2 solicita una etiqueta para el destino 172.16.10.0., R1 responde con una asignación de etiquetas de la etiqueta 17 para 172.16.10.0. En el proceso de distribución unsolicited downstream, R1 no espera una solicitud de asignación de etiquetas para el prefijo 172.16.10.0, sino que envía la información de asignación de etiquetas al LSR R2 ascendente.

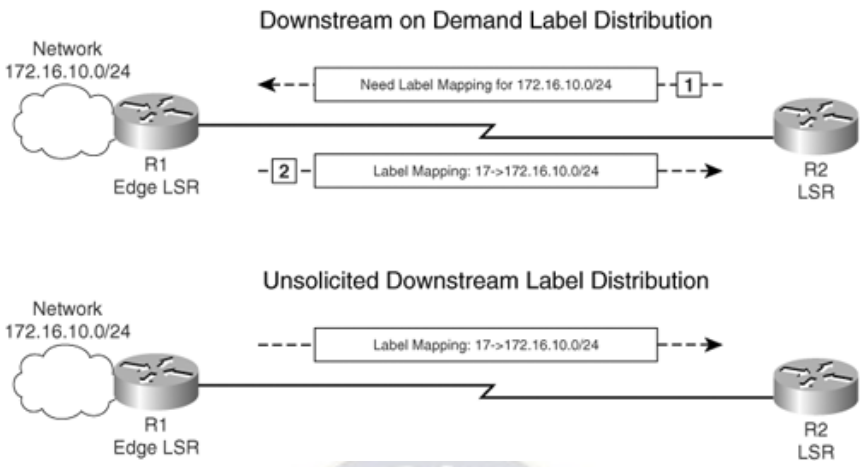


Figura 9: Tipos de distribución de etiquetas
Fuente: CiscoPress MPLS Fundamentals

2.2.6. Aplicaciones de MPLS

Son muchos los beneficios que brinda una red MPLS, sobre todo aplicaciones enfocadas a un uso corporativo.

Entre las aplicaciones que podemos encontrar, tenemos:

- **Ingeniería de Tráfico:** La idea de ingeniería de tráfico es utilizar de manera óptima la infraestructura de la red, incluidos los enlaces que están infrautilizados. Esto significa que la ingeniería de tráfico debe ofrecer la posibilidad de dirigir el tráfico a través de la red por caminos diferentes del camino preferido, que es el camino de menor costo proporcionado por el enrutamiento IP. Con la ingeniería de tráfico implementada en la red MPLS, se podría tener el tráfico destinado a un determinado prefijo o con una determinada calidad de flujo de servicio desde el punto A hasta el punto B por un camino diferente del camino de menor costo.

- **MPLS Redes Privadas Virtuales:** Es una implementación extendida de la tecnología del MPLS. Su popularidad ha crecido exponencialmente desde que se inventó, y sigue creciendo de forma constante. Aunque la mayoría de los proveedores de servicios lo han implementado como un reemplazo de los servicios de Frame Relay y ATM, MPLS VPN está viendo ahora un creciente

interés de las grandes empresas que lo ven como el siguiente paso en su diseño de red. La MPLS VPN puede proporcionar escalabilidad y dividir la red en redes separadas más pequeñas, lo que a menudo es necesario en las redes de empresas más grandes, donde la infraestructura de TI común tiene que ofrecer redes aisladas a los departamentos individuales.

- **MPLS y Calidad de Servicio (QoS):** Los tres bits EXP, se llaman experimentales, pero en realidad se usan para QoS. Se pueden usar estos bits EXP para programar el paquete y decidir mediante políticas de Calidad de Servicio la precedencia de caída y la prioridad de cada clase de tráfico que se genere en la red.

2.3. Clases de Tráfico

2.3.1. Voz sobre IP (VoIP)

El objetivo comúnmente utilizado en el diseño de redes para soportar VoIP es el objetivo especificado por el estándar G.114 de la UIT, que establece un retardo máximo de 150 ms (unidireccional) de extremo a extremo (de boca a oído).

El ancho de banda para los paquetes de voz, requiere un rango de prioridad garantizado de 20 a 320 kbps por llamada (dependiendo de la frecuencia de muestreo, el códec y la sobrecarga en la Capa 2), este ancho de banda se puede aprovisionar con mucha precisión porque los paquetes de voz son de tamaño constante (una función del códec).

En la tabla 2, se puede observar los distintos códecs, tamaño del payload, frecuencia de muestreo y ancho de banda requerido para cada uno, que son utilizados para la transmisión de Voz sobre las redes IP.

Codec Information				Bandwidth Calculations			
Codec & Bit Rate (Kbps)	Codec Sample Size (Bytes)	Codec Sample Interval (ms)	Mean Opinion Score (MOS)	Voice Payload Size (Bytes)	Voice Payload Size (ms)	Packets Per Second (PPS)	Bandwidth Ethernet (Kbps)
G.711 (64 Kbps)	80 Bytes	10 ms	4.1	160 Bytes	20 ms	50	87.2 Kbps
G.729 (8 Kbps)	10 Bytes	10 ms	3.92	20 Bytes	20 ms	50	31.2 Kbps
G.723.1 (6.3 Kbps)	24 Bytes	30 ms	3.9	24 Bytes	30 ms	33.3	21.9 Kbps
G.723.1 (5.3 Kbps)	20 Bytes	30 ms	3.8	20 Bytes	30 ms	33.3	20.8 Kbps
G.726 (32 Kbps)	20 Bytes	5 ms	3.85	80 Bytes	20 ms	50	55.2 Kbps
G722_64k (64 Kbps)	80 Bytes	10 ms	4.13	160 Bytes	20 ms	50	87.2 Kbps

Tabla 2: Códecs de voz para VoIP
Fuente: https://www.cisco.com/c/en/us/support/docs/voice/voice-quality/7934-bwidth-consume.html

2.3.2. Videoconferencias

Esta clase de tráfico interactivo en tiempo real, está destinado a aplicaciones de video unidireccional (unicast o multicast); el retardo máximo (unidireccional) no debe ser superior a los 200 ms. El ancho de banda aprovisionado variará según la resolución, la tasa de imágenes por segundo, los componentes de datos adicionales y el códec, este último es una herramienta importante para aliviar la sobrecarga en la red que puede generar esta clase de tráfico. La compresión funciona comparando las diferencias entre los cuadros de imagen, lo que significa que el ancho de banda está relacionado directamente con el movimiento y fluidez que exista en el video.

Existe varias tecnologías de compresión MJPEG, MPEG-4, H.264, los cuales dependen de la aplicación y la necesidad de uso. Para el diseño se trabajará con el códec H.264, ya que ofrece una mejor compresión en relación calidad de video/ancho de banda.

Ancho de Banda	Resolución	FPS
384 Kbps	CIF	30 fps
512 Kbps	4CIF	15 fps +
768 Kbps	4CIF	30 fps
1 Mbps	HD720	15 fps +
2 Mbps	HD720	30 fps
4 Mbps	HD720	60 fps
6 Mbps	HD1080	30 fps
7 Mbps	HD1080	60 fps

Tabla 3: Ancho de Banda – videoconferencias (Códec H.264 High)
Fuente: https://searchunifiedcommunications.techtarget.com/tip/Business-video-conferencing-setup-Calculating-bandwidth-requirements

2.3.3. Videovigilancia

Esta clase no tiene requisitos estrictos de latencia o fluctuación de fase. Sin embargo, los requisitos estrictos de pérdida (particularmente para los flujos HD) pueden requerir un servicio de prioridad estricta. La admisión de esta clase debe controlarse (ya sea mediante mecanismos de control de admisión o mediante aprovisionamiento explícito de ancho de banda).

A continuación, se muestra algunos perfiles de tráfico de videovigilancia:

- 720P 60FPS: 4 Mb/s
- 1080p 10FPS (estático): 0.5 – 0.625 Mb/s
- 1080P 30FPS (en movimiento): 5 Mb/s
- 5MP 15FPs (panorámica): 3.5 Mb/s
- 4K 30FPS: 7 Mb/s
- 4K 10 FPS (modo nocturno): 24 Mb/s

Fuente: https://ipvm.com/reports/bandwidth-guide-for-video-networks

2.3.4. Señalización de Llamada

La clase de servicio de señalización está destinada al tráfico de señalización de

llamadas que admite telefonía VoIP y video; esencialmente, este tráfico es el tráfico del plano de control para la infraestructura de telefonía de voz y video. A este tráfico se le puede asignar un ancho de banda moderadamente garantizado pero dedicado.

Los protocolos de control de sesión configuran, mantienen y eliminan la llamada o la sesión de audio o video. Los dos tipos más comunes de protocolos de control de sesión se conocen como H.323 y SIP:

- **SIP (Protocolo de inicio de sesión):** SIP funciona para mensajes de audio y video (VoIP y Video sobre IP). Creado como una alternativa H.323, SIP se utiliza principalmente para establecer y desconectar llamadas de video y voz a través de Internet. También se usa para modificar la conexión durante la llamada, como agregar un participante adicional. SIP se basa en un protocolo de " solicitud-respuesta ", que acepta solicitudes de una computadora y devuelve respuestas de la otra.

- **H.323:** Representa el estándar en las llamadas VoIP porque permite que el audio, el video y los datos funcionen juntos sin problemas a través de redes basadas en paquetes. H.323 se creó originalmente teniendo en cuenta las videoconferencias y hoy admite efectivamente la funcionalidad multimedia para VoIP. Se lo considera el estándar para transmitir audio, video y datos porque actúa sobre el plano control y la gestión de llamadas para sesiones individuales y de múltiples participantes. También se puede utilizar para conexiones locales y para conectar usuarios que trabajan para la misma compañía en diferentes ubicaciones geográficas.

2.3.5. Datos Críticos

La mayoría de las empresas tienen varias aplicaciones de datos que atraviesan sus redes, por lo que cada una ellas se deben considerar como críticas (con la excepción del tráfico *Best Effort* y Scavenger) para el negocio de la empresa. Este tráfico se puede clasificar en tres clases:

- **Control de red:** La clase de servicio Control de red está destinada al tráfico del plano de control de la red, que se requiere para el funcionamiento confiable de la infraestructura de red, por lo que este tráfico no debe descartarse. Ejemplo de este tráfico son los protocolos de enrutamiento.

- **Datos Transaccionales (datos de baja latencia):** Son aplicaciones interactivas de datos de primer plano, son aplicaciones de las cuales los usuarios esperan una respuesta, a través de la red, para continuar con sus tareas. La latencia excesiva en los tiempos de respuesta de las aplicaciones en primer plano afecta directamente la productividad del usuario. Ejemplos de estas aplicaciones incluyen componentes de datos de aplicaciones de colaboración multimedia, aplicaciones de planificación de recursos empresariales (ERP), aplicaciones de gestión de relaciones con clientes (CRM), aplicaciones de bases de datos, etc.

- **Datos masivos (datos de alto rendimiento):** Son aplicaciones de las cuales los usuarios no están esperando una respuesta, a través de la red, para continuar con sus tareas; es decir son flujos de tráfico no interactivos en segundo plano, como transferencias de archivos grandes, distribución de contenido, sincronización de bases de datos, operaciones de copia de seguridad y correo electrónico.

A continuación, se muestra algunas estimaciones de Anchos de Banda para determinadas aplicaciones realizados por Proveedores de Servicio (ISP):

- Correo Electrónico: 1 Mb/s
- Búsqueda Online: 0.33 Mb/s
- Compartir archivos: 0.5 Mb/s
- Backup: 2 Mb/s
- Servicios en la nube: 1.5 Mb/s

Fuente: https://business.frontier.com/blog/how-much-bandwidth-does-my-business-need/

2.4. Calidad de Servicio (QoS)

Las modernas aplicaciones multimedia en tiempo real, como la telefonía IP, la telepresencia, la difusión de vídeo y la videovigilancia IP son extremadamente sensibles a los retrasos en la entrega y crean demandas de calidad de servicio (QoS) únicas en una red. Cuando los paquetes se entregan utilizando un modelo de entrega de mejor esfuerzo, es posible que no lleguen en orden o de manera oportuna, y que se caigan. En el caso del vídeo, esto puede dar lugar a la pixelización de la imagen, video entrecortado, el audio y el video no están sincronizados, o no hay video en absoluto. En el caso del audio, podría causar eco, superposición de hablantes, habla ininteligible y distorsionada, cortes de voz, largos intervalos de silencio y caída de llamadas.

Existen tres modelos diferentes de implementación de QoS:

- **Best effort:** La Calidad de Servicio no está habilitada para este modelo. Se utiliza para el tráfico que no requiere ningún tratamiento especial.

- **Integrated Services (IntServ):** Las aplicaciones señalan a la red para hacer una reserva de ancho de banda e indican que requieren un tratamiento especial de Calidad de Servicio. Para poder proporcionar QoS de extremo a extremo, todos los nodos, incluyendo los puntos finales que ejecutan las aplicaciones, necesitan apoyar, construir y mantener el estado de ruta RSVP para cada flujo. Este es el mayor inconveniente de IntServ porque significa que no puede escalar bien en grandes redes que podrían tener miles o millones de flujos debido a la gran cantidad de flujos de RSVP que habría que mantener.

- **Differentiated Services (DiffServ):** La red identifica las clases que requieren un tratamiento especial de Calidad de Servicio, lo que la hace altamente escalable; características de la QoS (como ancho de banda y retraso) se manejan en base a salto por salto con políticas de QoS que se definen de forma independiente en cada dispositivo de la red. DiffServ divide el tráfico

IP en clases y lo marca en función de los requisitos de la empresa, de modo que a cada una de las clases se le puede asignar un nivel de servicio diferente.

Antes de aplicar cualquier mecanismo de Calidad de Servicio, el tráfico IP debe ser identificado y clasificado en diferentes clases, según los requisitos de la empresa. Los dispositivos de red utilizan la clasificación para identificar el tráfico IP como perteneciente a una clase específica.

La marcación de paquetes es un mecanismo de Calidad de Servicio que mapea un paquete cambiando un campo dentro del encabezado con un descriptor de tráfico, para que se distinga de otros paquetes durante la aplicación de otros mecanismos de calidad de servicio (como la remarcación, la vigilancia, las colas o la evitación de congestiones).

Los siguientes son descriptores de tráfico, usados para el marcado de paquetes:

- Capa 2: 802.1Q/p Class of Service (CoS) bits
- Capa 2.5: MPLS Experimental (EXP) bits
- Capa 3: Differentiated Services Code Points (DSCP) e IP Precedence

Con respecto al marcado de paquetes en Capa 3, la tabla 4 incluye todos los campos PHB de DSCP (DF, CS, AF y EF) con sus valores decimales y binarios equivalentes. Esta tabla también puede utilizarse para ver qué valor de precedencia IP corresponde a cada PHB.

Una contribución importante que realizo la IETF fue la caracterización de las clases de tráfico y cómo deben ser identificadas y tratadas, los comportamientos de las principales clases de tráfico son especificados mediante la RFC 4594, como se observa en la tabla 5; debido a que las 12 clases de tráfico identificadas en la RFC son demasiado granulares para las realidades prácticas de muchas implementaciones de redes, este modelo puede simplificarse en un modelo de 8 clases y ajustarse al campo EXP de la etiqueta MPLS.

DSCP Class	DSCP Value Bin	Decimal Value Dec	Drop Probability	Equivalent IP Precedence Value
DF (CS0)	000 000	0		0
CS1	001 000	8		1
AF11	001 010	10	Low	1
AF12	001 100	12	Medium	1
AF13	001 110	14	High	1
CS2	010 000	16		2
AF21	010 010	18	Low	2
AF22	010 100	20	Medium	2
AF23	010 110	22	High	2
CS3	011 000	24		3
AF31	011 010	26	Low	3
AF32	011 100	28	Medium	3
AF33	011 110	30	High	3
CS4	100 000	32		4
AF41	100 010	34	Low	4
AF42	100 100	36	Medium	4
AF43	100 110	38	High	4
CS5	101 000	40		5
EF	101 110	46		5
CS6	110 000	48		6
CS7	111 000	56		7

Tabla 4: DSCP PHB con valores equivalentes decimales-binarios e IPP
Fuente: CCNP and CCIE Enterprise Core

Application Class	Per-Hop Behavior	Application Examples
VoIP Telephony	EF	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Cisco IP Video Surveillance / Cisco Enterprise TV
Realtime Interactive	CS4	Cisco TelePresence
Multimedia Conferencing	AF4	Cisco Jabber, WebEx
Multimedia Streaming	AF3	Cisco Digital Media System (VoDs)
Network Control	CS6	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signaling	CS3	SCCP, SIP, H.323
Ops / Admin / Mgmt (OAM)	CS2	SNMP, SSH, Syslog
Transactional Data	AF2	ERP Apps, CRM Apps, Database Apps
Bulk Data	AF1	E-mail, FTP, Backup Apps, Content Distribution
Best Effort	DF	Default Class
Scavenger	CS1	YouTube, iTunes, BitTorrent, Xbox Live

Tabla 5: RFC 4594 - Modelo de 12 Clases de Tráfico
Fuente: Quality of Service for Rich-Media & Cloud Networks

2.4.1. Algoritmos de Colas de QoS

El manejo de la congestión implica una combinación de colas y programación. Las colas (también conocidas como "buffering") son el almacenamiento temporal de los paquetes sobrantes. Las colas se activan cuando una interfaz de salida experimenta congestión y se desactivan cuando la congestión desaparece. La congestión es detectada por el algoritmo de colas cuando una cola de hardware de Capa 1 presente en las interfaces físicas, conocida como anillo de transmisión (Tx-ring o TxQ), está llena y cuando el anillo Tx-ring ya no está lleno, indica que no hay congestión en la interfaz, y la cola está desactivada. La congestión puede ocurrir por una de estas dos razones:

- La interfaz de entrada es más rápida que la de salida.
- La interfaz de salida recibe paquetes de múltiples interfaces de entrada.

Existen varios algoritmos de colas disponibles que proporcionan un ancho de banda de tráfico en tiempo real, sensible al retardo y garantías de retardo, sin dejar de lado otros tipos de tráfico:

CBWFQ (Colas Ponderadas Basadas en Clase): Permite la creación de hasta 256 colas, es decir 256 clases de tráfico. Cada cola es atendida en base al ancho de banda asignado a esa clase. Con el CBWFQ, la clasificación de paquetes se hace en base a descriptores de tráfico como marcas de QoS, protocolos, ACLs, e interfaces de entrada. El ancho de banda asignado a una clase es el mínimo ancho de banda que se entrega a la clase durante la congestión. El algoritmo CBWFQ por sí mismo no proporciona una garantía de latencia y sólo es adecuado para el tráfico de datos que no es en tiempo real.

LLQ (Cola de baja latencia): Fue desarrollado para cumplir con los requisitos del tráfico en tiempo real, como la voz. El tráfico asignado a la cola de prioridad estricta es atendido hasta su ancho de banda asignado antes de que otras colas del CBWFQ sean atendidas. Proporciona garantías tanto de latencia como de ancho de banda al tráfico en tiempo real de alta prioridad. Se pueden definir múltiples clases

de tráfico en tiempo real, y se pueden dar garantías de ancho de banda separadas a cada uno.

La figura 10 nos permite observar la arquitectura del algoritmo CBWFQ en combinación con el de LLQ.

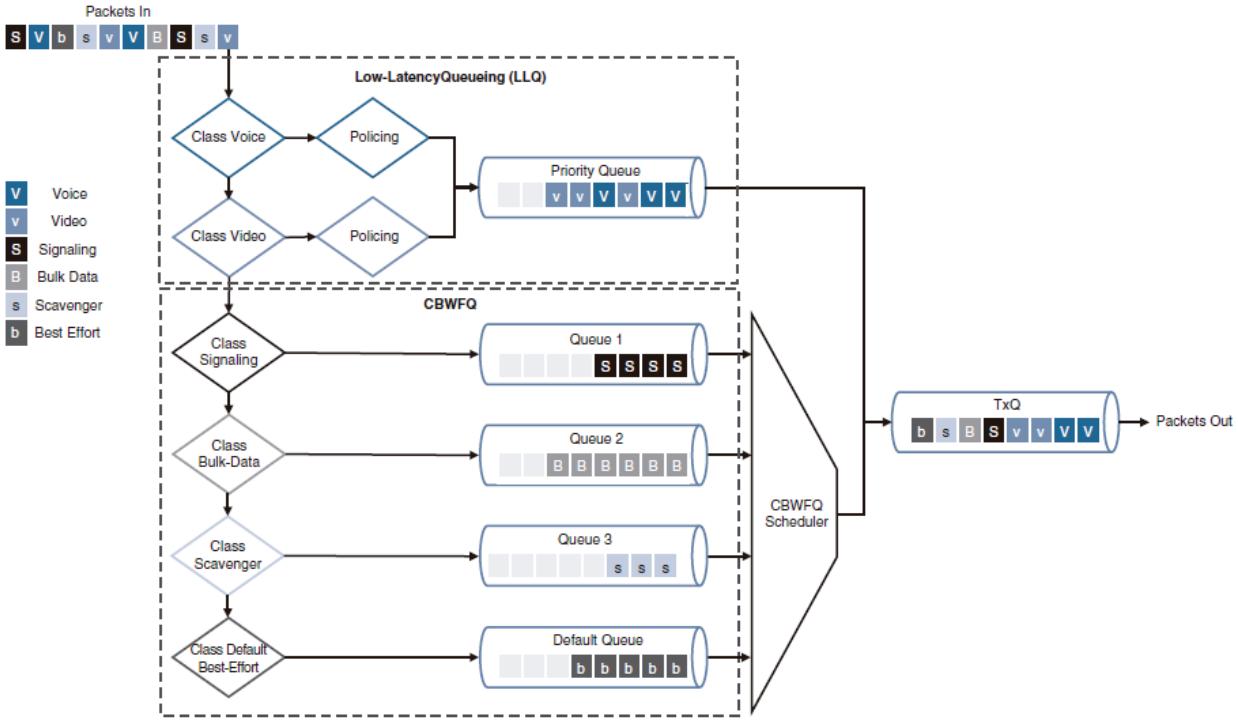


Figura 10: Arquitectura CBWFQ con LLQ
Fuente: CCNP and CCIE Enterprise Core

2.5. Protocolo IPv6

A principios de la década de 1990, los problemas con IPv4 preocuparon al Grupo de trabajo de ingeniería de Internet (IETF) que, en consecuencia, comenzó a buscar un reemplazo. Esto tuvo como resultado el desarrollo de IP versión 6 (IPv6). IPv6 supera las limitaciones de IPv4 y representa una mejora importante con características que se adaptan mejor a las demandas de red actuales y previsibles.

Las mejoras de IPv6 incluyen lo siguiente:

- Mayor espacio de direcciones: Las direcciones IPv6 se basan en el direccionamiento jerárquico de 128 bits en comparación con los 32 bits de IPv4.
- Mejor manejo de paquetes: Se redujo la cantidad de campos del encabezado de IPv6 para hacerlo más simple.
- Se elimina la necesidad de NAT: Al tener un número tan grande de direcciones IPv6 públicas, la NAT entre las direcciones IPv4 privadas y públicas ya no es necesaria. Esto evita algunos problemas de aplicación inducidos por NAT que tuvieron algunas aplicaciones que necesitan conectividad completa.

El espacio de direcciones IPv4 de 32 bits ofrece aproximadamente 4 294 967 296 direcciones únicas. Una de las principales mejoras de diseño de IPv6 con respecto a IPv4 es el encabezado de IPv6 simplificado.

2.5.1. Encapsulamiento IPv6

Una de las mejoras de diseño más importantes de IPv6 con respecto a IPv4 es el encabezado simplificado de IPv6.

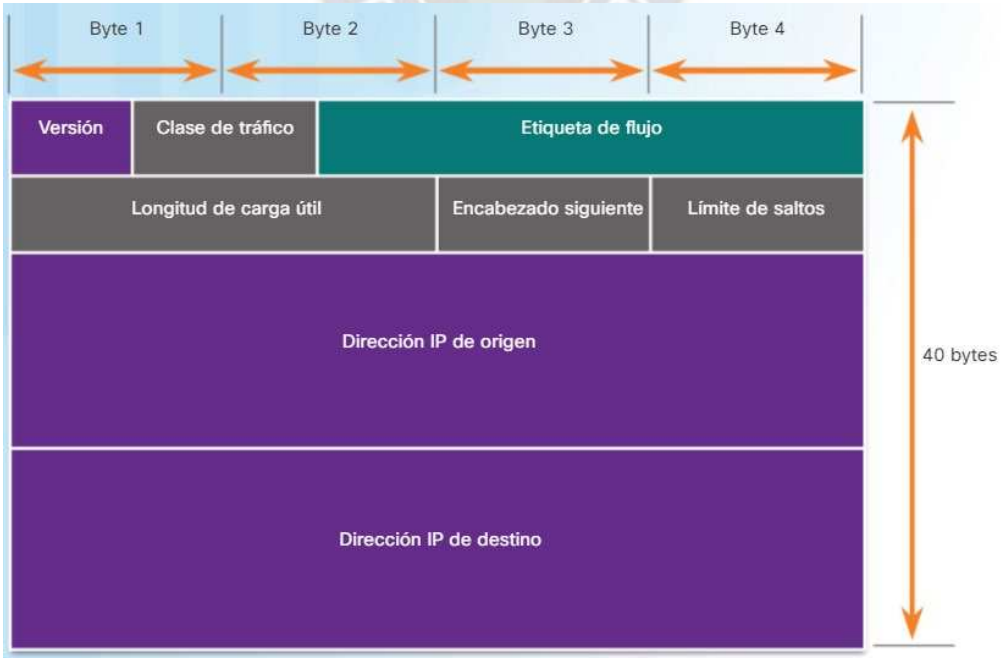


Figura 11: Encabezado IPv6
Fuente: CCNA 1 v6.0

Como se muestra en la Figura 11, en IPv6 algunos campos permanecen iguales respecto al encabezado de IPv4, mientras que a otros se les cambió el nombre y la posición, y algunos campos de IPv4 ya no son necesarios. El encabezado de IPv6, consta de 40 octetos (principalmente debido a la longitud de las direcciones de IPv6 de origen y de destino).

Los campos del encabezado de paquetes IPv6 incluyen lo siguiente:

- **Versión:** Este campo contiene un valor binario de 4 bits establecido en 0110 que lo identifica como un paquete IP versión 6.
- **Clase de tráfico:** Este campo de 8 bits es el equivalente al campo DS de IPv4.
- **Etiqueta de flujo:** Este campo de 20 bits sugiere que todos los paquetes con la misma etiqueta de flujo reciben el mismo tipo de manejo de los routers.
- **Longitud de contenido:** Este campo de 16 bits indica la longitud de la porción de datos o la longitud de contenido del paquete IPv6.
- **Encabezado siguiente:** Este campo de 8 bits es el equivalente al campo protocolo de IPv4. Es un valor que indica el tipo de contenido de datos que lleva el paquete, lo que permite que la capa de red transmita la información al protocolo de capa superior apropiado.
- **Límite de saltos:** Este campo de 8 bits reemplaza al campo TTL de IPv4. Cada router que reenvía el paquete reduce este valor en 1. Cuando llega a cero, se descarta el paquete y se envía un mensaje de tiempo superado de ICMPv6 al host de origen que indica que el paquete no llegó a destino porque excedió el límite de saltos.
- **Dirección IPv6 de origen**: es un campo de 128 bits que identifica la dirección IPv6 del host emisor.

- **Dirección IPv6 de destino**: es un campo de 128 bits que identifica la dirección IPv6 del host receptor.

Un paquete IPv6 también puede contener encabezados de extensión (EH), que proveen información optativa de la capa de red. Los encabezados de extensión son opcionales y están ubicados entre el encabezado de IPv6 y el contenido. Los EH se usan para fragmentar, dar seguridad, admitir la movilidad y otras acciones.

2.5.2. Tipos de direcciones IPv6

Existen tres tipos de direcciones IPv6:

- **Unidifusión:** una dirección IPv6 de unidifusión identifica de manera única una interfaz de un dispositivo habilitado para IPv6. Las direcciones IPv6 de origen deben ser direcciones de unidifusión.

- **Multidifusión:** las direcciones IPv6 de multidifusión se usan para enviar un único paquete IPv6 a varios destinos.

- **Difusión por proximidad:** una dirección IPv6 de difusión por proximidad es cualquier dirección IPv6 de unidifusión que puede asignarse a varios dispositivos. Los paquetes enviados a una dirección de difusión por proximidad se enrutan al dispositivo más cercano que tenga esa dirección.

A diferencia de IPv4, IPv6 no tiene una dirección de difusión. Sin embargo, existe una dirección IPv6 de multidifusión de todos los nodos que brinda básicamente el mismo resultado.

2.5.2.1. Longitud de prefijo IPv6

IPv6 utiliza la longitud de prefijo para representar la porción de prefijo de la dirección. IPv6 no utiliza la notación decimal punteada de máscara de subred. La longitud de prefijo se utiliza para indicar la porción de red de una dirección IPv6 mediante el formato de dirección IPv6/longitud de prefijo.

La longitud de prefijo puede ir de 0 a 128. Una longitud de prefijo IPv6 típica para LAN y la mayoría de los demás tipos de redes es /64. Esto significa que la porción de prefijo o de red de la dirección tiene una longitud de 64 bits, lo cual deja otros 64 bits para la ID de interfaz (porción de host) de la dirección.

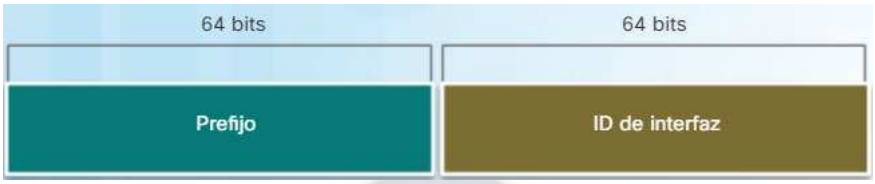


Figura 12: Longitud de prefijo IPv6
Fuente: CCNA 1 v6.0

2.5.2.2. Direcciones IPv6 de unidifusión

Las direcciones IPv6 de unidifusión identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Un paquete que se envía a una dirección de unidifusión es recibido por la interfaz que tiene asignada esa dirección. Como sucede con IPv4, las direcciones IPv6 de origen deben ser direcciones de unidifusión. Las direcciones IPv6 de destino pueden ser direcciones de unidifusión o de multidifusión.

Los tipos de direcciones IPv6 de unidifusión más comunes son las direcciones de unidifusión globales (GUA) y las direcciones de unidifusión link-local.

- **Unidifusión global**: Las direcciones de unidifusión globales son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas. Las direcciones de unidifusión globales pueden configurarse estáticamente o asignarse de forma dinámica.

- **Link-local:** Las direcciones link-local se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las direcciones link-local se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no

se pueden enrutar más allá del enlace. En otras palabras, los routers no reenvían paquetes con una dirección de origen o de destino link-local.

- **Local única:** Las direcciones IPv6 locales únicas tienen ciertas similitudes con las direcciones privadas RFC 1918 para IPv4, se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Estas direcciones no deberían poder enrutarse en la IPv6 global, y no deberían traducirse hacia direcciones IPv6 globales.

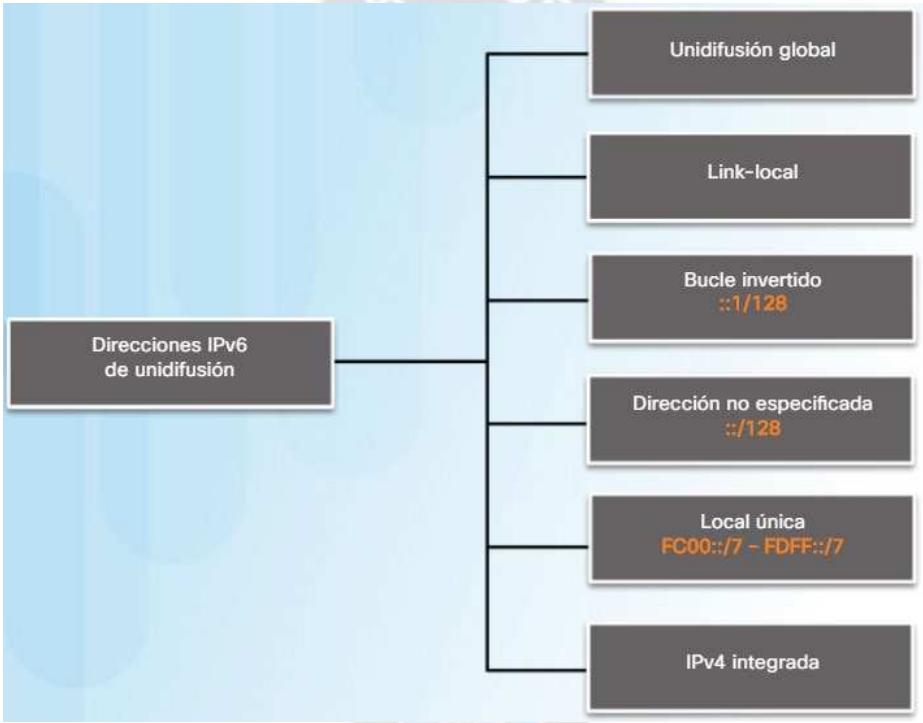


Figura 13: Tipos de Direcciones IPv6 de unidifusión
Fuente: CCNA 1 v6.0

2.5.2.3. Direcciones IPv6 de multidifusión

Las direcciones IPv6 de multidifusión son similares a las direcciones IPv4 de multidifusión. Las direcciones de multidifusión se utilizan para enviar un único paquete a uno o más destinos (grupo de multidifusión). Las direcciones IPv6 de multidifusión tienen el prefijo FF00::/8.

Existen dos tipos de direcciones IPv6 de multidifusión:

- Dirección de multidifusión asignada
- Dirección de multidifusión de nodo solicitado

2.6. Coexistencia IPv4-IPv6

El agotamiento del espacio de direcciones IPv4 es el factor que motiva la migración a IPv6. Debido al aumento de la conexión a Internet en todo el mundo, las direcciones IPv4 ya no son suficientes como para admitir este crecimiento. Como se muestra en la Figura 14, a cuatro de cinco RIR se les agotaron las direcciones IPv4.

Figura 14: Fechas de Agotamiento de las direcciones IPv4 de RIR
Fuente: CCNA 1 v6.0

No hay una única fecha para realizar la transición completa a IPv6. Por lo que IPv4 e IPv6 coexistirán. El IETF creó diversos protocolos y herramientas para ayudar a los administradores de redes a migrar las redes a IPv6.

Las técnicas de migración pueden dividirse en tres categorías:

- Dual-Stack IPv4-IPv6
- Tunelización
- Traducción

2.6.1. Dual-Stack IPv4-IPv6

Este es uno de los métodos más utilizados en los procesos de transición, debido a que utiliza un nodo de doble pila IPv6/IPv4, que puede llegar a comunicarse tanto como un nodo IPv4 ó como un nodo IPv6, para lograr este proceso cada nodo IPv6/IPv4 debe tener configurado los dos tipos de direcciones.

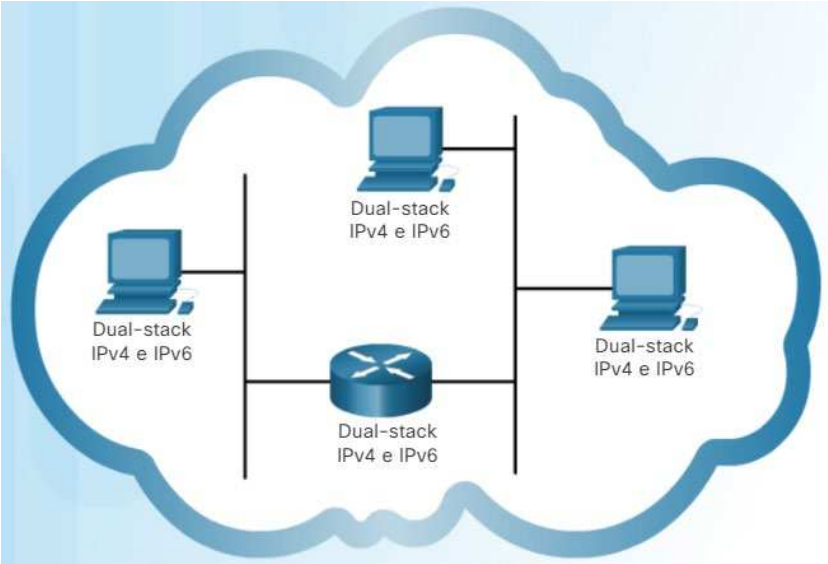


Figura 15: Dual-Stack IPv4-IPv6
Fuente: CCNA 1 v6.0

La implementación del método Dual Stack permite activar o desactivar una de las pilas, por este motivo un nodo puede tener 3 modos de funcionamiento:

- Cuando la pila IPV4 esta activada y la pila IPV6 desactivada, se comporta como un solo nodo IPV4.
- Cuando la pila IPV6 esta activada y la pila IPV4 desactivada, se comporta como un solo nodo IPV6.
- Cuando se habilitan las pilas IPV4 e IPV6, el nodo puede utilizar los dos protocolos.

Un nodo IPv4/IPv6 utiliza una dirección para cada versión de protocolo.

2.6.2. Tunelización

Este método permite transmitir paquetes IPv6 por medio de una infraestructura IPv4, es decir se encapsula el contenido del paquete IPv6 en un paquete IPv4.

El nodo IPv6 que hace frontera con el túnel, toma el paquete IPv6, y lo pone en el campo de datos de un paquete IPv4. Este paquete IPv4 tiene como dirección de destino el nodo IPv6 en la parte final del túnel y es enviado al primer nodo IPv4 que conforma el túnel. Los nodos IPv4 del túnel encaminan el paquete, sin tener constancia de que el paquete IPv4 que están manejando contiene un paquete IPv6. Finalmente, cuando el paquete llega al extremo receptor IPv6 del túnel, este determina que el paquete IPv4 contiene un paquete IPv6 que debe ser extraído.

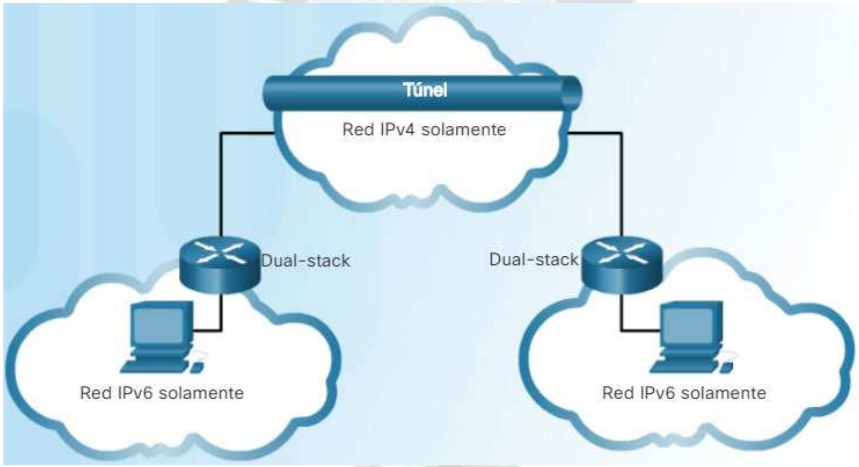


Figura 16: Tunelización
Fuente: CCNA 1 v6.0

2.6.3. Traducción de direcciones

Este método de traducción permite un enrutamiento transparente de la comunicación entre nodos que sólo poseen soporte a una versión del protocolo IP, o que utilizan Doble Pila. Además, pueden operar de diversas formas o en capas distintas, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa, realizando conversiones de direcciones, o actuando en el intercambio del tráfico TCP a UDP.

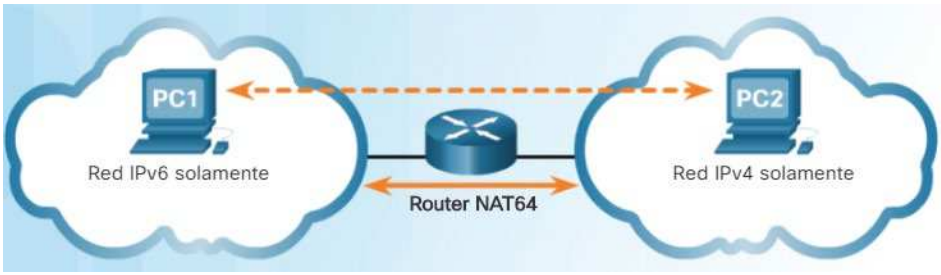


Figura 17: Traducción de direcciones
Fuente: CCNA 1 v6.0

2.7. Protocolos de Enrutamiento

Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la elección de los mejores caminos que realiza el protocolo.

2.7.1. Enrutamiento Estático

Las rutas estáticas consumen menos ancho de banda que los protocolos de enrutamiento dinámico. No se utiliza ningún ciclo de CPU para calcular y comunicar las rutas. La ruta de destino siempre es la misma, por lo que este tipo de enrutamiento se lo utiliza generalmente como una ruta por defecto, para comunicar todos los datos de salida que genere la compañía a la red de Internet.

2.7.2. Enrutamiento Dinámico

El propósito es mantener la información de enrutamiento actualizada, escogiendo el mejor camino hacia las redes de destino y poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible, en base a métricas.

Un sistema autónomo (AS) es un conjunto de routers bajo una administración común, como una empresa o una organización. Los ejemplos típicos de AS son la red interna de una empresa y la red de un proveedor de servicios.

2.7.2.1. Protocolos de Gateway Interior (IGP)

Se utiliza para el enrutamiento dentro de un AS. También se lo denomina “enrutamiento interno de AS”. Los IGP incluyen RIP, EIGRP, OSPF e IS-IS.

2.7.2.1.1. OSPF (Open Shortest Path First)

OSPF versión 2 (OSPFv2) se encuentra disponible para IPv4, mientras que OSPF versión 3 (OSPFv3) se encuentra disponible para IPv6. La distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. OSPF tiene una distancia administrativa predeterminada de 110 (en dispositivos Cisco).

Las características de OSPF son las siguientes:

- Eficaz
- Convergencia rápida
- Escalable

2.7.2.2. Protocolos de Gateway Exterior (EGP)

Se utiliza para el enrutamiento entre distintos AS. El protocolo de Gateway Fronterizo (BGP), es el único EGP viable actualmente.

2.7.2.2.1. BGP (Border Gateway Protocol)

BGP permite el encaminamiento de los paquetes IP que se intercambian entre los distintos AS. Para ello, es necesario el intercambio de prefijos de rutas entre los diferentes AS de forma dinámica, lo cual se lleva a cabo mediante el establecimiento de sesiones BGP entre AS, sobre conexiones TCP.

BGP dispone de dos comportamientos:

- **Internal BGP (iBGP):** Se utiliza dentro de un único AS y se suele utilizar para comunicar dos routers BGP situados en el mismo AS.

- **External BGP (eBGP):** Envía información de enrutamiento entre AS.

CAPITULO III
DISEÑO DE LA RED CORPORATIVA

3.1. Planteamiento de la Red

A medida que una empresa crece, también aumentan sus requisitos de tráfico de datos. Las compañías dependen de la infraestructura de red para proporcionar servicios esenciales. Las indisponibilidades de red pueden provocar pérdidas de ganancias y de clientes. Por lo que se debe diseñar e implementar una red empresarial que sea escalable y de alta disponibilidad.

La red debe admitir el intercambio de diversos tipos de tráfico de red, entre ellos archivos de datos, correo electrónico, telefonía IP y aplicaciones de video para varias unidades empresariales. Todas las redes empresariales deben cumplir los siguientes requisitos:

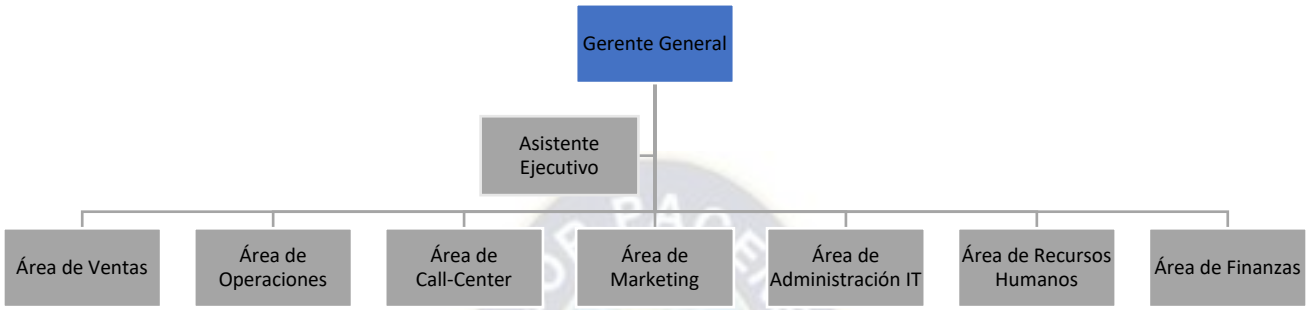
- Admitir aplicaciones fundamentales.
- Admitir el tráfico de redes convergentes.
- Admitir las diversas necesidades comerciales.
- Proporcionar un control administrativo centralizado.

En base a los requerimientos de las empresas detallados anteriormente, se realizará el análisis y diseño de la Red Corporativa, estableciendo aspectos técnicos, como el tráfico que se cursará al interior de la red en base a los servicios requeridos, brindar conectividad segura con Calidad de Servicio para garantizar que ciertos tipos de tráfico, como voz y video, tengan prioridad respecto al tráfico sin plazos, como el correo electrónico y la navegación web, realizar un estudio de tráfico de cada servicio para hacer uso eficiente del ancho de banda de la Red Corporativa.

3.2. Caracterización de la Red

3.2.1. Estructura administrativa interna de la Corporación

El organigrama de referencia será el siguiente:



A continuación, una breve descripción del objetivo de cada área.

Área de Ventas

- Gestionar recursos para entregar la oferta en alineación con la estrategia de la empresa.

Área de Operaciones

- Asignación adecuada de los recursos para satisfacer las categorías, mercados y requerimientos funcionales de la empresa.

Área de Call–Center

- Centro de comunicación y atención a los consumidores.

Área de Marketing

- Estimular innovación y enfoque en el consumidor en toda la operación.

Área de Administración IT

- Gestionar y desarrollar sistemas de información que contribuyan con la administración de la empresa.

Área de Recursos Humanos

- Responsable de la Gestión de Recursos Humanos de la empresa.

Área de Finanzas

- Planificar y dirigir las operaciones administrativas y financieras de la empresa.

3.2.2. Esquema de la Red

La empresa tendrá presencia geográfica en tres ciudades de Bolivia: La Paz, Cochabamba y Santa Cruz, la sede de La Paz será el punto central de la Red Corporativa, (localización del Data Center, Call-Center y la conexión de la empresa con la red de Internet).

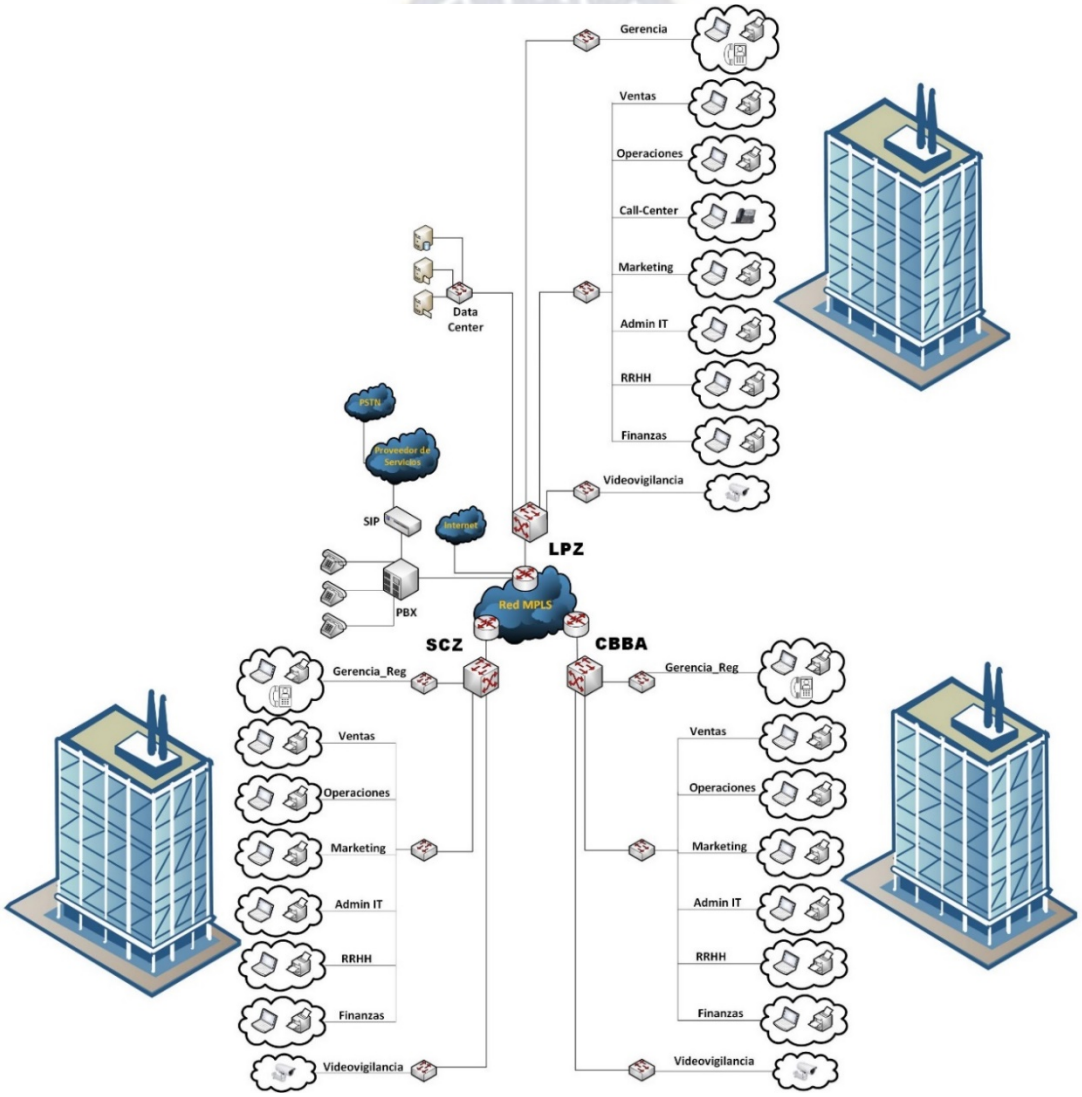


Figura 18: Esquema de la Red Corporativa

3.2.3. Estudio y Análisis de Tráfico

En base a la cantidad de dispositivos que conformaran la red, se procederá a realizar un análisis del ancho de banda requerido por cada uno de los mismos, a fin de evitar cuellos de botella, que afecten de forma negativa al rendimiento de la red y se haga un uso eficiente del ancho de banda.

De tal manera que la capacidad de ancho de banda a alquilar a un proveedor de servicios, para la red de transmisión de datos entre las sucursales de la empresa sea la necesaria, para los usos y propósitos de la compañía.

Así mismo, también se realizará un estudio de los tipos de clases de tráfico que se cursaran por la red, con el objetivo de aplicar políticas de Calidad de Servicio, otorgando prioridad al tráfico en tiempo real (voz y video) y a los datos que sean críticos para la empresa.

Sede La Paz:

Área	PCs	Teléfonos IP	Total
Gerencia	9	9	18
Data Center	2	1	3
Ventas	11	11	22
Operaciones	12	12	24
Call-Center	20	20	40
Marketing	10	10	20
Administración IT	10	10	20
Recursos Humanos	10	10	20
Finanzas	7	7	14
Total	91	90	**181**

Tabla 6: Dispositivos de red – La Paz

- Se asignará un total de 8 impresoras, 12 cámaras IP de las cuales 2 estarán ubicadas en el Data-Center, 2 en el área de Call-Center y los 8 restantes en las demás áreas.

Resultando un total de 201 dispositivos de red en la sede de La Paz.

Sede Cochabamba:

Área	PCs	Teléfonos IP	Total
Gerencia Regional	6	6	12
Data - Center	1	1	2
Ventas	9	9	18
Operaciones	10	10	20
Marketing	7	7	14
Administración IT	7	7	14
Recursos Humanos	8	8	16
Finanzas	6	6	12
Total	54	54	**108**

Tabla 7: Dispositivos de red – Cochabamba

- Se asignará un total de 7 impresoras, 9 cámaras IP de las cuales 1 estará ubicado en el Data-Center, y los 8 restantes en las demás áreas.

Resultando un total de 124 dispositivos de red en la sede de Cochabamba.

Sede Santa Cruz:

Área	PCs	Teléfonos IP	Total
Gerencia Regional	6	6	12
Data - Center	1	1	2
Ventas	10	10	20
Operaciones	11	11	22
Marketing	9	9	18
Administración IT	8	8	16
Recursos Humanos	9	9	18
Finanzas	6	6	12
Total	60	60	**120**

Tabla 8: Dispositivos de red – Santa Cruz

- Se asignará un total de 7 impresoras, 9 cámaras IP de las cuales 1 estará ubicado en el Data-Center, y los 8 restantes en las demás áreas.

Resultando un total de 136 dispositivos de red en la sede de Santa Cruz.

Resultando un total de 461 equipos de red, que conformarán la red corporativa, de las cuales 201 están ubicadas en la sede de La Paz, 124 en Cochabamba y 136 en Santa Cruz.

3.2.4. Dimensionamiento de la Red

Es necesario clasificar los tipos de tráfico que atravesarán la red, de tal manera que se ajuste al campo EXP de 3 bits de la etiqueta MPLS. Simplificando el modelo de 12 clases sugerido en la RFC 4594 a un modelo de 8 clases como se observa en la Figura 19.

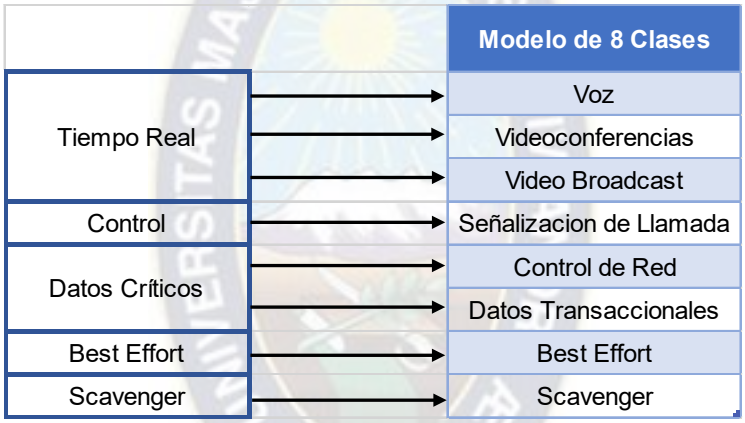


Figura 19: Modelo de Estrategia de Calidad de Servicio

Una vez compilada toda la información necesaria (cantidad de dispositivos finales en la red y las clases de tráfico que pueden atravesar en la misma), es momento de calcular y analizar el ancho de banda necesario, de tal forma que se garantice la disponibilidad de los servicios, así como el rendimiento óptimo de la red.

Requerimientos por servicio:

- **Datos para aplicaciones:** Para, servicios tales como correo electrónico, navegación por internet, audio streaming, se asignará un ancho de banda promedio de 512 Kbps por usuario. Por otra parte, el overbooking (tasa de reúso del ancho de banda) será de 20%, debido a que este tráfico no se considera crítico para el desarrollo y operación de una empresa.

- **Datos transaccionales:** Dispositivos que hacen uso de software en la nube, plataformas de carga y descarga de archivos/imágenes de bases de datos y aplicaciones internas de la red: Sistemas de punto de venta, ERPs (Enterprise Resourse Planning) y/o CRMs (Customer Resource Management), se encuentran en esta categoría de servicios. Se asignará un ancho de banda de 1.25 Mbps por usuario, el overbooking para este servicio será de 30%.

- **VoIP:** Para teléfonos IP, debido al hecho que la calidad de voz es el factor más importante en este servicio, el códec que se usará es el G.729 aplicado a redes basadas en Ethernet lo que resulta en un ancho de banda aproximado de 32 Kbps por terminal:

$$Ancho\ de\ Banda = tamaño\ del\ paquete * PPS$$

$$PPS = velocidad\ del\ códec \mid tamaño\ payload$$

$$tamaño\ del\ paquete = cabecera\ L2 + cabecera\ IP|UDP|RTP + tamaño\ payload$$

De la tabla 5, obtenemos los valores de los parámetros del códec G.729:

$$tamaño\ del\ paquete = 18\ (L2) + 40\ (IP|UDP|RTP) + 20\ (payload) = 78\ bytes$$

$$PPS = 8\ Kbps\ (Vel.códec) \mid 20\ bytes\ (payload) = 50\ PPS$$

$$Ancho\ de\ Banda = 78\ bytes * 50$$

$$\boxed{\boldsymbol{Ancho\ de\ Banda = 31.2\ Kbps}}$$

Como la voz es un servicio de tiempo real, el overbooking será de 100%, esto significa que en cualquier momento habrá recursos disponibles de red para este servicio.

- **Videoconferencias:** Para este servicio, se puede asignar un ancho de banda de 6 Mbps (para una resolución de 1080p30) por sesión de video (basado en el estándar H.264 con alta calidad de video), sin embargo, para el cálculo asumiremos una calidad media que requeriría un ancho de banda de 2 Mbps (720p30), el overbooking será del 40%, garantizando que en cualquier momento se puedan realizar sin ningún inconveniente cuatro de diez llamadas de video.

- **Videovigilancia:** El ancho de banda de este servicio, de igual forma dependerá de la resolución, tasa de imágenes por segundo, códec de compresión de video, para el diseño se tomará en cuenta las siguientes características: resolución de 1080p, compresión del códec a usar H.264 HEVC - high quality y tasa de imágenes por segundo de 20 FPS, para ello se requerirá un ancho de banda aproximado de 2.2 Mbps (Fuente: https://www.cctvcalculator.net/en/calculations/bandwidth-calculator/)

La asignación de ancho de banda dependerá principalmente de las funciones que desempeñe cada usuario en la empresa. No es lo mismo analizar el tráfico que se genere en un área de recepción, que un tráfico generado por la gerencia (que puede incluir tráfico de videoconferencia).

Tomando en cuenta los requerimientos de servicios que se realizó previamente, el cálculo de ancho de banda en cada sede, se lo realizará para conocer la capacidad a alquilar al proveedor de servicios para la Red de Transporte de Datos en los enlaces WAN, así como también para alquilar el ancho de banda necesario para conectarse a la red de Internet.

- Ancho de Banda para conectarse a la red de Internet:

$$BW = \sum_{AREAS} \#usuarios_{AREA} * (BW_{DATOS\ AP} * OB_{DATOS\ AP} + BW_{VC} * OB_{VC})$$

Donde:

BW $_{DATOS\ AP}$ = Ancho de Banda - Datos de Aplicaciones = 512 Kbps

BW $_{VC}$ = Ancho de Banda - Videoconferencias = 2 Mbps

OB $_{DATOS\ AP}$ = Overbooking - Datos de Aplicaciones = 20%

OB $_{VC}$ = Overbooking - Videoconferencias = 40%

- Ancho de Banda en los enlaces WAN:

$$BW = \sum_{AREAS} \#usuarios_{AREA} * (BW_{DATOS} * OB_{DATOS} + BW_{VoIP} + BW_{VC} * OB_{VC})$$

Donde:

BW $_{DATOS}$ = Ancho de Banda - Datos de Aplicaciones y Transaccionales = 1.75 Mbps

BW $_{VoIP}$ = Ancho de Banda - Voz = 32 Kbps

BW $_{VC}$ = Ancho de Banda - Videoconferencias = 1.5 Mbps

OB $_{DATOS}$ = Overbooking - Datos Transaccionales = 30%

OB $_{VC}$ = Overbooking - Videoconferencias = 30%

Se adicionará un ancho de banda de 100 Kbps a los ejecutivos que componen la Gerencia de la empresa.

La Paz:

Área	Usuarios	BW Datos [Kbps]	BW Video IP [Kbps]	BW Total [Mbps]
Gerencia	9	612	2048	8.28
Data Center	2	512	-	0.20
Ventas	11	512	-	1.10
Operaciones	12	512	-	1.20
Call Center	20	512	-	2.00
Marketing	10	512	-	1.00
Administración IT	10	512	-	1.00
Recursos Humanos	10	512	-	1.00
Finanzas	7	512	-	0.70
			BW	**16.48**

Tabla 9: Ancho de Banda (Internet) - La Paz

Área	Usuarios	BW Datos [Kbps]	BW VoIP [Kbps]	BW Video IP [Kbps]	BW Total [Mbps]
Gerencia	9	-	32	2048	7.48
Data Center	2	-	32	-	0.06
Ventas	11	-	32	-	0.34
Operaciones	12	-	32	-	0.38
Marketing	10	-	32	-	0.31
Administración IT	10	-	32	-	0.31
Recursos Humanos	10	-	32	-	0.31
Finanzas	7	-	32	-	0.22
				BW	**9.42**

Tabla 10: Ancho de Banda (WAN) - La Paz

Cochabamba:

Área	Usuarios	BW Datos [Kbps]	BW Video IP [Kbps]	BW Total [Mbps]
Gerencia Regional	6	612	2048	5.52
Data - Center	1	512	-	0.10
Ventas	9	512	-	0.90
Operaciones	10	512	-	1.00
Marketing	7	512	-	0.70
Administración IT	7	512	-	0.70
Recursos Humanos	8	512	-	0.80
Finanzas	6	512	-	0.60
			BW	**10.32**

Tabla 11: Ancho de Banda (Internet) - Cochabamba

Área	Usuarios	BW Datos [Kbps]	BW VoIP [Kbps]	BW Video IP [Kbps]	BW Total [Mbps]
Gerencia Regional	6	1892	32	2048	8.31
Data - Center	1	1792	32	-	0.56
Ventas	9	1792	32	-	5.01
Operaciones	10	1792	32	-	5.56
Marketing	7	1792	32	-	3.89
Administración IT	7	1792	32	-	3.89
Recursos Humanos	8	1792	32	-	4.45
Finanzas	6	1792	32	-	3.34
				BW	**35.01**

Tabla 12: Ancho de Banda (WAN) - Cochabamba

Santa Cruz:

Área	Usuarios	BW Datos [Kbps]	BW Video IP [Kbps]	BW Total [Mbps]
Gerencia Regional	6	612	2048	5.52
Data - Center	1	512	-	0.10
Ventas	10	512	-	1.00
Operaciones	11	512	-	1.10
Marketing	9	512	-	0.90
Administración IT	8	512	-	0.80
Recursos Humanos	9	512	-	0.90
Finanzas	6	512	-	0.60
			BW	**10.92**

Tabla 13: Ancho de Banda (Internet) – Santa Cruz

Área	Usuarios	BW Datos [Kbps]	BW VoIP [Kbps]	BW Video IP [Kbps]	BW Total [Mbps]
Gerencia Regional	6	1892	32	2048	8.31
Data - Center	1	1792	32	-	0.56
Ventas	10	1792	32	-	5.56
Operaciones	11	1792	32	-	6.12
Marketing	9	1792	32	-	5.01
Administración IT	8	1792	32	-	4.45
Recursos Humanos	9	1792	32	-	5.01
Finanzas	6	1792	32	-	3.34
				BW	**38.35**

Tabla 14: Ancho de Banda (WAN) – Santa Cruz

Adicionalmente a estos resultados queda pendiente sumar el ancho de banda correspondiente a las cámaras IP, este tráfico de video IP estará principalmente en las redes LAN de cada sede, para el monitoreo respectivo.

Cuando se requiera acceder de forma remota (ya sea desde otra sucursal o a través de internet) a cualquier cámara IP, este tráfico consumirá un ancho de banda de la capacidad del enlace WAN respectivo, por lo que para el diseño se sumará el ancho de banda de solo una cámara IP (acceso remoto simultáneo en un momento dado).

3.2.5. Servicios a alquilarse

En base a las capacidades requeridas en cada sede de la empresa y el tráfico cursante en cada una de las mismas, procedemos a determinar los servicios a alquilarse de un proveedor de servicios.

- Red de Transporte de Datos
- Salida a Internet mediante un ISP

3.2.5.1. Red de Transporte de Datos

Se requerirá los siguientes anchos de banda en cada enlace WAN:

Enlace	BW (Sedes) + BW (Cámara IP)	BW Total [Mbps]
LPZ - CBBA	9.42(LPZ) + 35.01(CBBA) + 38.35(SCZ) + 2.2	**84.98**
LPZ - SCZ	9.42(LPZ) + 38.35(SCZ) + 35.01(CBBA) + 2.2	**84.98**

El servicio de Transporte de Datos que ofrezca un proveedor de servicios, debe ser un enlace con anchos de banda simétricos, ello significa que la capacidad total que debe ofrecer por enlace, será la suma de la velocidad de subida más la velocidad de bajada, para garantizar un rendimiento óptimo en la red, por lo que los anchos de banda requeridos en cada enlace son los siguientes:

Enlace	BW (UP/DOWN)
LPZ - CBBA	**42.49 Mbps**
LPZ - SCZ	**42.49 Mbps**

Tabla 15: Ancho de Banda (Enlaces WAN)

Cabe mencionar que la capacidad requerida en cada uno de los enlaces, se puede incrementar, conforme la empresa lo vea necesario (aumento de personal o incorporación de nuevas herramientas de producción para la empresa).

3.2.5.2. Salida a Internet mediante un ISP

El ancho de banda (simétrico) necesario para la comunicación entre la empresa y la red de Internet, es el siguiente:

ACCESO	BW
LPZ	16.48 Mbps
CBBA	10.32 Mbps
SCZ	10.92 Mbps
CÁMARA IP	2.2 Mbps
	39.92 Mbps

Tabla 16: Ancho de Banda (Acceso a Internet)

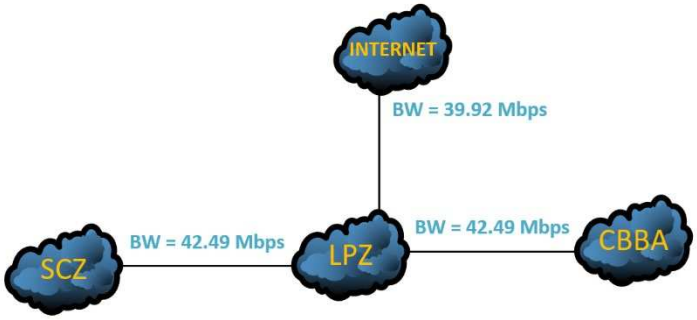


Figura 20: Alquiler de Servicios de Transporte de Datos y acceso a Internet

3.2.6. Definición y elección de los elementos de la Red

La elección de los dispositivos (routers y switches), para la verificación del diseño de la red, se lo realizará con equipos de la compañía Cisco, debido a la cantidad de dispositivos que se tiene a disposición para la implementación de la red, en un simulador virtual en comparación a equipos de otras marcas.

Router de borde WAN

En base al diseño propuesto, la sede en La Paz será el punto centralizado de todo el tráfico que requiera comunicarse desde o hacia la red de Internet y así mismo realizar consultas, transferencias de archivos, etc., a los servidores de la empresa.

Por lo que el router presente en el borde de la Red WAN, debe ser un dispositivo robusto, es decir que pueda procesar múltiples flujos de tráfico y servicios de red, provenientes de todas las sedes de la empresa.

El router ASR-920-12CZ-A de la serie ASR (Routers de Servicios Agregados), proporcionan un conjunto completo y escalable de servicios de capa 2 y capa 3. Tienen un alto rendimiento y bajo consumo de energía, ideal para redes empresariales comerciales con aplicaciones de voz, video y datos (triple play).

Especificaciones:

- Sistema Operativo: Cisco IOS XE
- Procesador: Dual-Core 1Ghz
- Memoria Bootflash: 2 GB
- Memoria DRAM: 4 GB
- Capacidad: 64 Gbps (de acuerdo a demanda)
- Puertos Ethernet: 2 puertos 10GE y 12 puertos 1GE (puertos de expansión)
- Dual Stack: IPv4 e IPv6
- Características: QoS, DHCP, DNS, IPSec, BGP, Bidirectional Forwarding Detection (BFD), DVMRP, EIGRP, GRE, HSRP, IGMPv3, IS-IS, MPLS, OSPF, PIM-SM, PIM-SSM, Policy-based routing (PBR), RIP-1, RIP-2, RSVP, Static IP routing, VRRP.

Router ASR-920-12CZ-A

Fuente: www.cisco.com

Modelo ASR 920	Puertos 1 GE	Puertos 10 GE
ASR-920-12CZ-A	Dispone de 12X1GE: 4 puertos SFP + 8 AMS (Detección Automática de Medios) Los primeros seis puertos (4 SFP + 2 AMS) son puertos sin licencia que están habilitados de forma predeterminada. Los últimos 6 puertos (6 AMS) son puertos con licencia.	Hay 2X10GE que operan en modo 1GE por defecto. Para operar en modo 10GE, se debe activar la licencia de actualización

El software Cisco IOS XE para esta serie ASR 920 proporciona un paquete modular, por lo que la habilitación de funciones requeridas para la red, se lo realiza por compra de licencias de software.

El router por defecto incluye la licencia **Metro Access**, sin embargo, en esta no se incluye la función de MPLS en el equipo. Para la habilitación de MPLS, se necesita la adquisición de la licencia **Advanced Metro IP Access**: ASR920-S-A.

Routers Sucursales

Como la cantidad de dispositivos y ancho de banda requerido en las ubicaciones de Cochabamba y Santa Cruz es menor respecto a la sede en La Paz, se elegirá el router ASR-920-4SZ-A, el cual tiene una densidad de puertos menor a su predecesor (ASR-920-12CZ-A).

Especificaciones:

- Sistema Operativo: Cisco IOS XE
- Procesador: Dual-Core 1Ghz
- Memoria Bootflash: 2 GB
- Memoria DRAM: 4 GB

- Capacidad: 64 Gbps (de acuerdo a demanda)
- Puertos Ethernet: 2 puertos 1GE y 4 puertos 1GE/10GE
- Dual Stack: IPv4 e IPv6

Router ASR-920-4SZ-A

Fuente: www.cisco.com

Modelo ASR 920	Puertos 1 GE	Puertos 10 GE
ASR-920-4SZ-A	Los dos puertos operan en modo 1GE de manera predeterminada y no se requiere licencia para activar estos puertos.	Hay puertos 4X10GE que operan en modo 1GE por defecto. Para operar en modo 10G, se debe activar la licencia de actualización

De igual forma el router incluye por defecto la licencia **Metro Access**, por lo que es necesario comprar la licencia **Advanced Metro IP Access**, para la habilitación de MPLS en el equipo.

Switches de Capa 2

Se empleará los Switches Cisco SG220-50P y SG220-26P de la serie 220 de Cisco, de 50 y 26 puertos Gigabit Ethernet respectivamente, los cuales brindan seguridad, rendimiento y permite disponer de una red empresarial sólida a un bajo coste.

Esta serie 220, incorpora acceso Gigabit Ethernet con opciones de alimentación Power over Ethernet (PoE) Plus, por lo que no solo se mejora la productividad de la empresa en la actualidad, sino que también se cumple con los requisitos en constante cambio de las redes del futuro. De esta manera se puede implantar soluciones avanzadas, como servicios de datos, voz y vídeo en una infraestructura convergente.

Especificaciones SG220-50P:

- Memoria CPU: 128 MB
- Memoria Flash: 32 MB
- Potencia: 375 W
- Puertos que admiten PoE: 48 puertos
- Qos: 8 niveles por puerto
- Tabla MAC: 8192 direcciones MAC
- VLAN: Admite 255 VLAN activas
- Puertos: 48 puertos GE y 2 GE (SFP)
- Capacidad de Switching: 100 Gbps
- Dual Stack: IPv4 e IPv6
- Tramas Jumbo: Admite tramas de hasta 9216

Switch Cisco SG220-50P
Fuente: www.cisco.com

Especificaciones SG220-26P:

- Memoria CPU: 128 MB
- Memoria Flash: 32 MB
- Potencia: 180 W
- Puertos que admiten PoE: 24 puertos
- Qos: 8 niveles por puerto
- Tabla MAC: 8192 direcciones MAC
- VLAN: Admite 255 VLAN activas

- Puertos: 24 puertos GE y 2 GE (SFP)
- Capacidad de Switching: 52 Gbps
- Dual Stack: IPv4 e IPv6
- Tramas Jumbo: Admite tramas de hasta 9216

Switch Cisco SG220-26P

Fuente: www.cisco.com

Switch para servidores

Se empleará el switch Cisco Catalyst 2960S-24TD-L de 24 puertos Gigabit Ethernet y 2 puertos Uplink de hasta 10 Gbps, la elección de este dispositivo es debido a la escalabilidad que ofrece, alta densidad de puertos con multivelocidad 10/100/1000 Mbps, calidad de servicio (QoS) y seguridad en la red tanto en IPv4 e IPv6.

Especificaciones 2960S-24TD-L:

- Memoria Flash: 128 MB
- DRAM: 64 MB
- Potencia: 39 W
- Qos: Clase de Servicio (CoS) y Servicios Diferenciados (DSCP)
- VLAN: Admite 255 VLAN activas
- Puertos: 24 puertos GE y 2 10GE (SFP+)
- Capacidad de Switching: 176 Gbps
- Dual Stack: IPv4 e IPv6
- Tramas Jumbo: Admite tramas de hasta 9216

Switch Cisco Catalyst 2960S-24TD-L

Fuente: www.cisco.com

Cantidad de routers y switches – La Paz:

- 1 Router Cisco ASR-920-12CZ-A

Puertos	Dispositivo
GE 0/0/0	Enlace LPZ - CBBA
GE 0/0/1	Switch SG220-50P
GE 0/0/2	Switch SG220-50P
GE 0/0/3	Switch SG220-26P
TGE 0/0/12	Switch 2960S-24TD-L
GE 0/0/4	Conexion a Internet
GE 0/0/5	Enlace LPZ - SCZ

La asignación de interfaces desde GE 0/0/0 - 5, es debido a que estos puertos ya vienen habilitados sin necesidad de una licencia adicional.

- 2 Switches Cisco SG220-50P

Switch SG220-50P	
Área	**Puertos**
Gerencia	9
Admin_IT	10
Operaciones	12
Finanzas	7
Impresoras	8
	46 Puertos

Switch SG220-50P	
Área	**Puertos**
Ventas	11
Marketing	10
RRHH	10
Camaras_IP	12
	43 Puertos

- 1 Switch Cisco SG220-26P

Switch SG220-26P	
Área	**Puertos**
Call_Center	20
	20 Puertos

- 1 Switch Cisco 2960S-24TD-L dedicado para el Data_Center de la empresa.

Cantidad de routers y switches – Cochabamba:

- 1 Router Cisco ASR-920-4SZ-A

Puertos	Dispositivo
GE 0/0/0	Enlace LPZ - CBBA
TGE 0/0/2	Switch SG220-50P
TGE 0/0/3	Switch SG220-50P

- 2 Switches Cisco SG220-50P

Switch SG220-50P	
Área	**Puertos**
Gerencia _Reg	6
Admin_IT	7
Operaciones	10
Finanzas	6
Impresoras	7
	36 Puertos

Switch SG220-50P	
Área	**Puertos**
Ventas	9
Marketing	7
RRHH	8
Camaras_IP	8
Data_Center	1
	33 Puertos

Cantidad de routers y switches – Santa Cruz:

- 1 Router Cisco ASR-920-4SZ-A

Puertos	Dispositivo
GE 0/0/0	Enlace LPZ - SCZ
TGE 0/0/2	Switch SG220-50P
TGE 0/0/3	Switch SG220-50P

- 2 Switches Cisco SG220-50P

Switch SG220-50P	
Área	**Puertos**
Gerencia _Reg	6
Admin_IT	8
Operaciones	11
Finanzas	6
Impresoras	7
	38 Puertos

Switch SG220-50P	
Área	**Puertos**
Ventas	10
Marketing	9
RRHH	9
Camaras_IP	8
Data_Center	1
	37 Puertos

3.2.7. Elección del sistema de respaldo de energía

Dotar de energía eléctrica por un tiempo limitado a dispositivos eléctricos/electrónicos cuando hay un corte eléctrico o caída de energía, protege contra anomalías del suministro eléctrico, como picos de voltaje, variaciones de voltaje y otros problemas que causan que los dispositivos eléctricos funcionen de manera anormal o en el peor de los casos se dañen. Por lo que es necesario contar con un Suministro de energía ininterrumpida (UPS), que permita que los componentes críticos para la operación de la empresa, tales como servidores, sistemas de control, dispositivos de red como routers, switches, sigan operando durante algún tiempo cuando sucede un apagón.

Para la elección del sistema de respaldo de energía adecuado en cada una de las sedes de la empresa, se establecerá la cantidad de Watts total que se va a conectar al UPS, considerando un margen de 20 % para no sobrecargar al sistema de respaldo, ya que este tiene una capacidad limitada de carga y para el diseño se determinará un tiempo de respaldo aproximado de 20 a 30 minutos.

Sistema de respaldo de energía – La Paz:

Cantidad	Equipo	Consumo por Dispositivo	Consumo Total
1	Router Cisco ASR-920-12CZ-A	115 W	115 W
1	Switch Cisco 2960S-24TD-L	40 W	40 W
2	Switch Cisco SG220-50P	375 W	750 W
1	Switch Cisco SG220-26P	180 W	180 W
3	Servidores	250 W	750 W
2	PCs Administracion	100 W	200 W
Consumo de Energia Total			**2035 W**

Tabla 17: Consumo de Energía – Componentes Críticos en La Paz

Se empleará el modelo APC Smart-UPS SRT 3000VA 230V + APC Smart-UPS SRT 96V 3kVA Battery Pack otorgando un tiempo de funcionamiento de 29 minutos.

Especificaciones:

- Potencia máx. configurable (vatios): 2.7Kilovatios
- Tensión de salida: Configurable para 220V
- Frecuencia de salida (sincronizada con la red eléctrica): 50/60 Hz +/- 3 Hz
- Puerto(s): RJ-45 Serial, Smart-Slot, USB
- Vida útil esperada de la batería (en años): 3 - 5

APC Smart-UPS SRT 3000VA 230V

Fuente: https://www.apc.com/shop/es/es/products/APC-Smart-UPS-SRT-3000-VA-230-V/P-SRT3000XLI

Sistema de respaldo de energía – Cochabamba:

Cantidad	Equipo	Consumo por Dispositivo	Consumo Total
1	Router Cisco ASR-920-4SZ-A	115 W	115 W
2	Switch Cisco SG220-50P	375 W	750 W
1	Servidores	250 W	250 W
1	PCs Administracion	100 W	250 W
Consumo de Energia Total			**1215 W**

Tabla 18: Consumo de Energía – Componentes Críticos en Cochabamba

Se empleará el modelo APC Smart-UPS SRT 1500VA 230V + APC Smart-UPS SRT 48V 1kVA 1.5kVA Battery Pack otorgando un tiempo de funcionamiento de 31 minutos.

Especificaciones:

- Potencia máx. configurable (vatios): 1.5Kilovatios
- Tensión de salida: Configurable para 220V
- Frecuencia de salida (sincronizada con la red eléctrica): 50/60 Hz +/- 3 Hz
- Puerto(s): RJ-45 Serial, Smart-Slot, USB
- Vida útil esperada de la batería (en años): 3 - 5

APC Smart-UPS SRT 1500VA 230V
Fuente: https://www.apc.com/shop/es/es/products/SAI-Smart-UPS-SRT-de-APC-1500-VA-230-V/P-SRT1500XLI

Sistema de respaldo de energía – Santa Cruz:

Cantidad	Equipo	Consumo por Dispositivo	Consumo Total
1	Router Cisco ASR-920-4SZ-A	115 W	115 W
2	Switch Cisco SG220-50P	375 W	750 W
1	Servidores	250 W	250 W
1	PCs Administracion	100 W	250 W
Consumo de Energia Total			**1215 W**

Tabla 19: Consumo de Energía – Componentes Críticos en Santa Cruz

Se empleará el modelo APC Smart-UPS SRT 1500VA 230V + APC Smart-UPS SRT 48V 1kVA 1.5kVA Battery Pack otorgando un tiempo de funcionamiento de 31 minutos.

Especificaciones:

- Potencia máx. configurable (vatios): 1.5Kilovatios
- Tensión de salida: Configurable para 220V
- Frecuencia de salida (sincronizada con la red eléctrica): 50/60 Hz +/- 3 Hz
- Puerto(s): RJ-45 Serial, Smart-Slot, USB
- Vida útil esperada de la batería (en años): 3 - 5

APC Smart-UPS SRT 1500VA 230V
Fuente: https://www.apc.com/shop/es/es/products/SAI-Smart-UPS-SRT-de-APC-1500-VA-230-V/P-SRT1500XLI

3.2.8. Topología de la Red

En la siguiente figura se observa la topología física de la red diseñada:

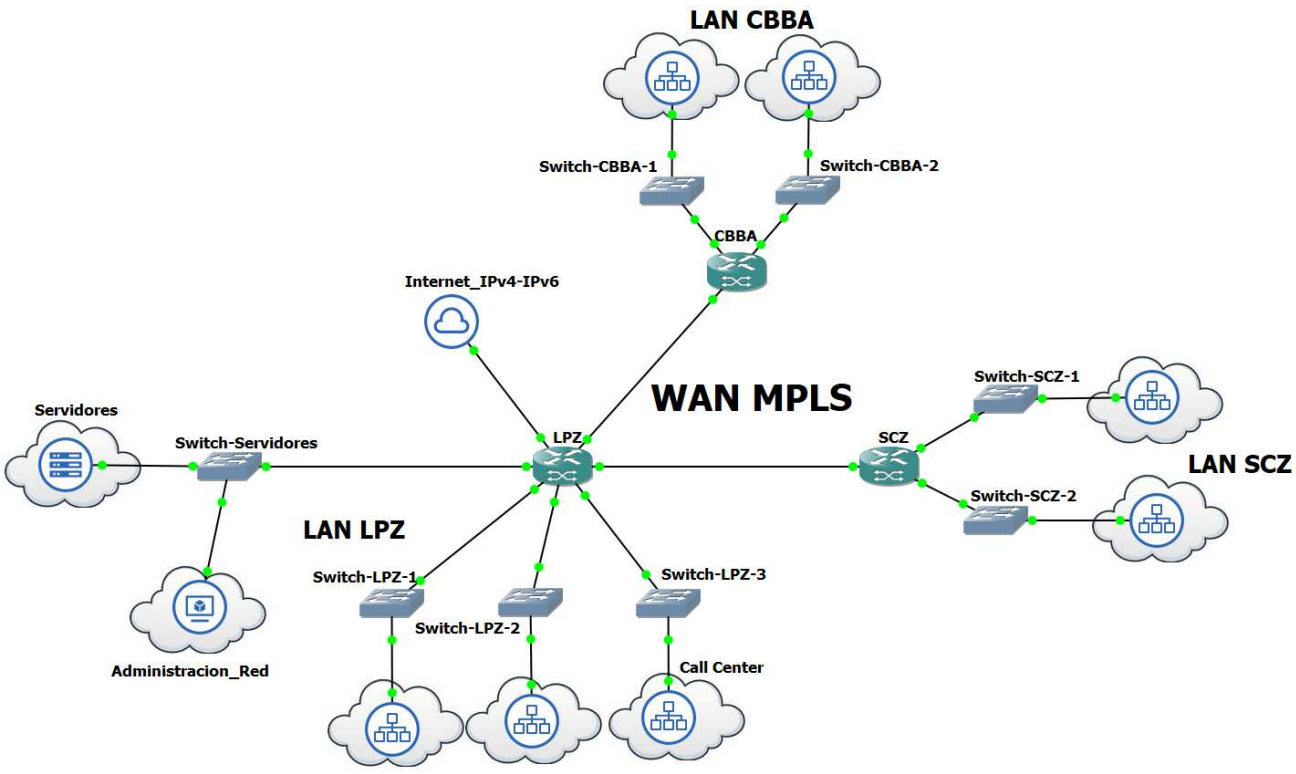


Figura 21: Topología Física de la Red

El diseño de la red, plantea dos enlaces activos en todo momento (LPZ – CBBA y LPZ – SCZ), por lo que el proveedor de servicios, garantizará la disponibilidad de la Red de Transmisión de Datos ante cualquier caída o falla de algún enlace.

3.2.9. Direccionamiento IP de la Red

El esquema de direccionamiento utilizará los espacios de dirección 10.0.0.0/24 (IPv4) para el núcleo MPLS; 2001:db8:acef::/48 (IPv6), 192.168.110.0/20, 192.168.120.0/20 y 192.168.130.0/20 (IPv4) para las redes LAN de la empresa.

3.2.9.1. Direccionamiento del Núcleo de la Red

Como se mencionó anteriormente la Red Corporativa contará con dos enlaces WAN activos, sin embargo, previendo un crecimiento que pueda lograr la empresa, para hasta 8 enlaces WAN, se dividirá el espacio de direcciones IPv4 para admitir 8 subredes, considerando:

Subred	Dirección de Red
	Primer Host
	Segundo Host
	Dirección de Broadcast

Figura 22: Direccionamiento para un enlace punto a punto

Asignación de direcciones de red IPv4, a los enlaces de la Red WAN Corporativa:

Red	**10.0.0.0/24**	**Enlace**
Subred 0:	10.0.0.0/30	LPZ - CBBA
Subred 1:	10.0.0.4/30	LPZ - SCZ
Subred 2:	10.0.0.8/30	N/A
	. . .	
Subred 7:	10.0.0.28/30	N/A

N/A: No Asignado

Tabla 20: Asignación de subredes IPv4

3.2.9.2. Direccionamiento de las redes LAN

El diseño del direccionamiento IPv4 en las redes LAN, se lo debe de realizar en base a la cantidad de hosts en cada VLAN, considerando una numeración ordenada y/o entendible, de tal forma que la resolución de problemas o asignación de direcciones a un determinado host, se lo realice de manera óptima.

La sede de La Paz usará el espacio de direcciones IPv4 192.168.110.0/20, de la cual se realizará una división en subredes de 512 direcciones de tal forma de asignar un sub espacio de direcciones de red a una cantidad determinada de áreas que componen una determinada LAN.

Dispositivo	**192.168.110.0/20**
Switch-LPZ-1	192.168.110.0/23
Switch-LPZ-2	192.168.111.0/23
Switch-LPZ-3	192.168.112.0/23
Switch-LPZ-4	192.168.113.0/23

Tabla 21: Subredes IPv4 – LAN de LPZ

Switch-LPZ-1

Switch SG220-50P	
Área	**Puertos**
Gerencia	9
Admin_IT	10
Operaciones	12
Finanzas	7
Impresoras	8
	46 Puertos

De acuerdo a la asignación de Áreas realizado en el Switch, se observa que 38 puertos (Gerencia + Admin_IT + Operaciones + Finanzas) deberán estar asignados a una VLAN de voz, para poder hacer uso de los teléfonos IP asignados a cada empleado.

Previendo un crecimiento en el personal o dispositivos que se incorporen a la Empresa, se asignará direcciones de red para una cantidad mayor de hosts en cada Área, de la que se tiene asignada en cada puerto del Switch. Considerando que la primera dirección disponible (figura 23) será designada como la puerta de enlace predeterminada de cada subred.

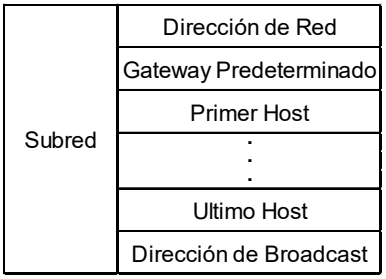


Figura 23: Direccionamiento de una subred

Número de VLAN	Nombre de VLAN	Dirección de red IPv4	Cantidad de Hosts
150	Voz_1	192.168.110.0/26	61
10	Gerencia	192.168.110.64/27	29
20	Admin_IT	192.168.110.96/27	29
30	Operaciones	192.168.110.128/27	29
40	Finanzas	192.168.110.160/27	29
80	Impresoras	192.168.110.192/27	29
200	Switch_LPZ_1	192.168.110.224/29	5

Tabla 22: Subneteo – Switch_LPZ_1

El proceso realizado anteriormente, se lo replicara en las demás áreas y de las redes LAN de CBBA y SCZ con los espacios de dirección 192.168.120.0/20 y 192.168.130.0/20 respectivamente.

Debido a la gran cantidad de direcciones disponibles con IPv6 el proceso de Subneteo ya no es requerido, teniendo la posibilidad de definir 2^{16} subredes, cada una con una longitud de prefijo /64, es decir 2^{64} direcciones disponibles para asignar en esa subred.

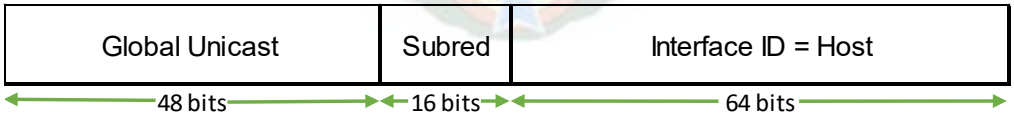


Figura 24: Subneteo en IPv6

El proceso explicado anteriormente, se lo aplicará a las redes LAN de LPZ, CBBA y SCZ con el espacio de direccionamiento 2001:db8:acef::/48. Considerando de igual forma la primera dirección disponible como la puerta de enlace predeterminada de cada subred.

Asignación de direcciones de red IPv4 e IPv6 en las redes LAN de la empresa:

Sede	Número de VLAN	Nombre de VLAN	Dirección de red IPv4	Dirección de red IPv6
LPZ	10	Gerencia	192.168.110.64/27	2001:db8:acef::/64
	110	Data_Center	192.168.113.0/27	2001:db8:acef:1::/64
	50	Ventas	192.168.111.64/27	2001:db8:acef:2::/64
	30	Operaciones	192.168.110.128/27	2001:db8:acef:3::/64
	100	Call_Center	192.168.112.0/26	2001:db8:acef:4::/64
	60	Marketing	192.168.111.96/27	2001:db8:acef:5::/64
	20	Admin_IT	192.168.110.96/27	2001:db8:acef:6::/64
	70	RRHH	192.168.111.128/27	2001:db8:acef:7::/64
	40	Finanzas	192.168.110.160/27	2001:db8:acef:8::/64
	80	Impresoras	192.168.110.192/27	2001:db8:acef:9::/64
	90	Camaras_IP	192.168.111.160/27	2001:db8:acef:a::/64
	150	Voz_1	192.168.110.0/26	2001:db8:acef:b::/64
	151	Voz_2	192.168.111.0/26	2001:db8:acef:c::/64
	152	Voz_3	192.168.113.40/30	2001:db8:acef:d::/64
	200	Switch_LPZ_1	192.168.110.224/29	2001:db8:acef:201::/64
	200	Switch_LPZ_2	192.168.111.192/29	2001:db8:acef:202::/64
	200	Switch_LPZ_3	192.168.112.64/29	2001:db8:acef:203::/64
	200	Administracion	192.168.113.32/29	2001:db8:acef:200::/64

Tabla 23: Asignación de VLAN en la red de La Paz

Sede	Número de VLAN	Nombre de VLAN	Dirección de red IPv4	Dirección de red IPv6
CBBA	10	Gerencia_Reg	192.168.120.64/27	2001:db8:acef:10::/64
	110	Data_Center	192.168.121.176/29	2001:db8:acef:11::/64
	50	Ventas	192.168.121.64/27	2001:db8:acef:12::/64
	30	Operaciones	192.168.120.128/27	2001:db8:acef:13::/64
	60	Marketing	192.168.121.96/27	2001:db8:acef:14::/64
	20	Admin_IT	192.168.120.96/27	2001:db8:acef:15:/64
	70	RRHH	192.168.121.128/27	2001:db8:acef:16:/64
	40	Finanzas	192.168.120.160/27	2001:db8:acef:17::/64
	80	Impresoras	192.168.120.192/28	2001:db8:acef:18::/64
	90	Camaras_IP	192.168.121.160/28	2001:db8:acef:19::/64
	150	Voz_1	192.168.120.0/26	2001:db8:acef:1a::/64
	151	Voz_2	192.168.121.0/26	2001:db8:acef:1b::/64
	200	Switch_CBBA_1	192.168.120.208/29	2001:db8:acef:205::/64
	200	Switch_CBBA_2	192.168.121.184/29	2001:db8:acef:206::/64

Tabla 24: Asignación de VLAN en la red de Cochabamba

Sede	Número de VLAN	Nombre de VLAN	Dirección de red IPv4	Dirección de red IPv6
SCZ	10	Gerencia_Reg	192.168.130.64/27	2001:db8:acef:20::/64
	110	Data_Center	192.168.131.176/29	2001:db8:acef:21::/64
	50	Ventas	192.168.131.64/27	2001:db8:acef:22::/64
	30	Operaciones	192.168.130.128/27	2001:db8:acef:23::/64
	60	Marketing	192.168.131.96/27	2001:db8:acef:24::/64
	20	Admin_IT	192.168.130.96/27	2001:db8:acef:25::/64
	70	RRHH	192.168.131.128/27	2001:db8:acef:26::/64
	40	Finanzas	192.168.130.160/27	2001:db8:acef:27::/64
	80	Impresoras	192.168.130.192/28	2001:db8:acef:28::/64
	90	Camaras_IP	192.168.131.160/28	2001:db8:acef:29::/64
	150	Voz_1	192.168.130.0/26	2001:db8:acef:2a::/64
	151	Voz_2	192.168.131.0/26	2001:db8:acef:2b::/64
	200	Switch-SCZ-1	192.168.130.208/29	2001:db8:acef:207::/64
	200	Switch-SCZ-2	192.168.131.184/29	2001:db8:acef:208::/64

Tabla 25: Asignación de VLAN en la red de Santa Cruz

Asignación de direcciones IPv4 e IPv6, a cada equipo de red:

Asignación	Dirección IPv4	Dirección IPv6
Gerencia 1	192.168.110.66	2001:db8:acef::2
Gerencia 2	192.168.110.67	2001:db8:acef::3
.	.	.
Gerencia 9	192.168.110.74	2001:db8:acef::a
Data_Center 1	192.168.113.2	2001:db8:acef:1::2
Data_Center 2	192.168.113.3	2001:db8:acef:1::3
.	.	.
Ventas 1	192.168.111.66	2001:db8:acef:2::2
Ventas 2	192.168.111.67	2001:db8:acef:2::3
.	.	.
Ventas 11	192.168.111.76	2001:db8:acef:2::c
Operaciones 1	192.168.110.130	2001:db8:acef:3::2
Operaciones 2	192.168.110.131	2001:db8:acef:3::3
.	.	.
Operaciones 12	192.168.110.141	2001:db8:acef:3::d
Call_Center 1	192.168.112.2	2001:db8:acef:4::2
Call_Center 2	192.168.112.3	2001:db8:acef:4::3
.	.	.
Call_Center 20	192.168.112.21	2001:db8:acef:4::15
Marketing 1	192.168.111.98	2001:db8:acef:5::2
Marketing 2	192.168.111.99	2001:db8:acef:5::3
.	.	.
Marketing 10	192.168.111.107	2001:db8:acef:5::b

Asignación	Dirección IPv4	Dirección IPv6
Admin_IT 1	192.168.110.98	2001:db8:acef:6::2
Admin_IT 2	192.168.110.99	2001:db8:acef:6::3
:	:	:
Admin_IT 10	192.168.110.107	2001:db8:acef:6::b
RRHH 1	192.168.111.130	2001:db8:acef:7::2
RRHH 2	192.168.111.131	2001:db8:acef:7::3
:	:	:
RRHH 10	192.168.111.139	2001:db8:acef:7::b
Finanzas 1	192.168.110.162	2001:db8:acef:8::2
Finanzas 2	192.168.110.163	2001:db8:acef:8::3
:	:	:
Finanzas 7	192.168.110.168	2001:db8:acef:8::8
Impresora 1	192.168.110.194	2001:db8:acef:9::2
Impresora 2	192.168.110.195	2001:db8:acef:9::3
:	:	:
Impresora 8	192.168.110.201	2001:db8:acef:9::9
Camara_IP 1	192.168.111.162	2001:db8:acef:a::2
Camara_IP 2	192.168.111.163	2001:db8:acef:a::3
:	:	:
Camara_IP 12	192.168.111.173	2001:db8:acef:a::d
Voz_1 - 1	192.168.110.2	2001:db8:acef:b::2
Voz_1 - 2	192.168.110.3	2001:db8:acef:b::3
:	:	:
Voz_1 - 38	192.168.110.39	2001:db8:acef:b::27
Voz_2 - 1	192.168.111.2	2001:db8:acef:c::2
Voz_2 - 2	192.168.111.3	2001:db8:acef:c::3
:	:	:
Voz_2 - 31	192.168.111.32	2001:db8:acef:c::20
Voz_3 - 1	192.168.113.42	2001:db8:acef:d::2
Administracion 1	192.168.113.35	2001:db8:acef:200::3
Administracion 2	192.168.113.36	2001:db8:acef:200::4

Tabla 26: Asignación de direcciones IP a los equipos de red – La Paz

Asignación	Dirección IPv4	Dirección IPv6
Gerencia 1	192.168.120.66	2001:db8:acef:10::2
Gerencia 2	192.168.120.67	2001:db8:acef:10::3
:	:	:
Gerencia 6	192.168.120.71	2001:db8:acef:10::7
Data_Center 1	192.168.121.178	2001:db8:acef:11::2
:	:	:
Ventas 1	192.168.121.66	2001:db8:acef:12::2
Ventas 2	192.168.121.67	2001:db8:acef:12::3
:	:	:
Ventas 9	192.168.121.74	2001:db8:acef:12::a

Asignación	Dirección IPv4	Dirección IPv6
Operaciones 1	192.168.120.130	2001:db8:acef:13::2
Operaciones 2	192.168.120.131	2001:db8:acef:13::3
.	.	.
Operaciones 10	192.168.120.139	2001:db8:acef:13::b
Marketing 1	192.168.121.98	2001:db8:acef:14::2
Marketing 2	192.168.121.99	2001:db8:acef:14::3
.	.	.
Marketing 7	192.168.121.104	2001:db8:acef:14::8
Admin_IT 1	192.168.120.98	2001:db8:acef:15::2
Admin_IT 2	192.168.120.99	2001:db8:acef:15::3
.	.	.
Admin_IT 7	192.168.120.104	2001:db8:acef:15::8
RRHH 1	192.168.121.130	2001:db8:acef:16::2
RRHH 2	192.168.121.131	2001:db8:acef:16::3
.	.	.
RRHH 8	192.168.121.137	2001:db8:acef:16::9
Finanzas 1	192.168.120.162	2001:db8:acef:17::2
Finanzas 2	192.168.120.163	2001:db8:acef:17::3
.	.	.
Finanzas 6	192.168.120.167	2001:db8:acef:17::7
Impresora 1	192.168.120.194	2001:db8:acef:18::2
Impresora 2	192.168.120.195	2001:db8:acef:18::3
.	.	.
Impresora 7	192.168.120.200	2001:db8:acef:18::8
Camara_IP 1	192.168.121.162	2001:db8:acef:19::2
Camara_IP 2	192.168.121.163	2001:db8:acef:19::3
.	.	.
Camara_IP 8	192.168.121.169	2001:db8:acef:19::9
Voz_1 - 1	192.168.120.2	2001:db8:acef:1a::2
Voz_1 - 2	192.168.120.3	2001:db8:acef:1a::3
.	.	.
Voz_1 - 29	192.168.120.30	2001:db8:acef:1a::1e
Voz_2 - 1	192.168.121.2	2001:db8:acef:1b::2
Voz_2 - 2	192.168.121.3	2001:db8:acef:1b::3
.	.	.
Voz_2 - 25	192.168.121.26	2001:db8:acef:1b::1a

Tabla 27: Asignación de direcciones IP a los equipos de red – Cochabamba

Asignación	Dirección IPv4	Dirección IPv6
Gerencia 1	192.168.120.66	2001:db8:acef:10::2
Gerencia 2	192.168.120.67	2001:db8:acef:10::3
.	.	.
Gerencia 6	192.168.120.71	2001:db8:acef:10::7
Data_Center 1	192.168.121.178	2001:db8:acef:11::2
.	.	.

Asignación	Dirección IPv4	Dirección IPv6
Ventas 1	192.168.121.66	2001:db8:acef:12::2
Ventas 2	192.168.121.67	2001:db8:acef:12::3
.	.	.
Ventas 9	192.168.121.74	2001:db8:acef:12::a
Operaciones 1	192.168.120.130	2001:db8:acef:13::2
Operaciones 2	192.168.120.131	2001:db8:acef:13::3
.	.	.
Operaciones 10	192.168.120.139	2001:db8:acef:13::b
Marketing 1	192.168.121.98	2001:db8:acef:14::2
Marketing 2	192.168.121.99	2001:db8:acef:14::3
.	.	.
Marketing 7	192.168.121.104	2001:db8:acef:14::8
Admin_IT 1	192.168.120.98	2001:db8:acef:15::2
Admin_IT 2	192.168.120.99	2001:db8:acef:15::3
.	.	.
Admin_IT 7	192.168.120.104	2001:db8:acef:15::8
RRHH 1	192.168.121.130	2001:db8:acef:16::2
RRHH 2	192.168.121.131	2001:db8:acef:16::3
.	.	.
RRHH 8	192.168.121.137	2001:db8:acef:16::9
Finanzas 1	192.168.120.162	2001:db8:acef:17::2
Finanzas 2	192.168.120.163	2001:db8:acef:17::3
.	.	.
Finanzas 6	192.168.120.167	2001:db8:acef:17::7
Impresora 1	192.168.120.194	2001:db8:acef:18::2
Impresora 2	192.168.120.195	2001:db8:acef:18::3
.	.	.
Impresora 7	192.168.120.200	2001:db8:acef:18::8
Camara_IP 1	192.168.121.162	2001:db8:acef:19::2
Camara_IP 2	192.168.121.163	2001:db8:acef:19::3
.	.	.
Camara_IP 8	192.168.121.169	2001:db8:acef:19::9
Voz_1 - 1	192.168.120.2	2001:db8:acef:1a::2
Voz_1 - 2	192.168.120.3	2001:db8:acef:1a::3
.	.	.
Voz_1 - 29	192.168.120.30	2001:db8:acef:1a::1e
Voz_2 - 1	192.168.121.2	2001:db8:acef:1b::2
Voz_2 - 2	192.168.121.3	2001:db8:acef:1b::3
.	.	.
Voz_2 - 25	192.168.121.26	2001:db8:acef:1b::1a

Tabla 28: Asignación de direcciones IP a los equipos de red – Santa Cruz

3.2.9.3. Tabla de asignación de direcciones a Routers y Switches

A continuación, se muestra las tablas de asignación de direcciones de red IPv4 e IPv6 a las interfaces de los equipos de red, así como la asignación de VLAN de administración de los equipos, para controlar y gestionar a los mismos, de manera remota.

Mencionar que las interfaces a ser asignadas diferirán con las de los equipos físicos reales, debido a que los modelos de routers y switches a simular en GNS3 no poseen interfaces 10 Gigabit Ethernet.

Dispositivo	Interfaz Fisica	Interfaz GNS3
LPZ Router Cisco ASR-920-12CZ-A	GE 0/0/0	GE 0/0
	GE 0/0/1	GE 1/0
	GE 0/0/2	GE 2/0
	GE 0/0/3	GE 3/0
	TGE 0/0/12	GE 4/0
	GE 0/0/4	GE 5/0
	GE 0/0/5	GE 6/0
CBBA Router Cisco ASR-920-4SZ-A	GE 0/0/0	GE 0/0
	TGE 0/0/2	GE 2/0
	TGE 0/0/3	GE 3/0
SCZ Router Cisco ASR-920-4SZ-A	GE 0/0/0	GE 0/0
	TGE 0/0/2	GE 2/0
	TGE 0/0/3	GE 3/0

Tabla 29: Asignación de las Interfaces de Routers en GNS3

Dispositivo	Puertos Fisicos	Puertos GNS3	Asignación VLAN
Switch_LPZ_1	GE 0/1 - 0/9	FE 0/1 - 0/9	VLAN 10,150
	GE 0/10 - 0/19	FE 0/10 - 0/19	VLAN 20,150
	GE 0/20 - 0/31	FE 0/20 - 0/31	VLAN 30,150
	GE 0/32 - 0/38	FE 0/32 - 0/38	VLAN 40,150
	GE 0/39 - 0/46	FE 0/39 - 0/46	VLAN 80,150
	GE 0/49	FE 0/0	VLAN 200
Switch_LPZ_2	GE 0/1 - 0/11	FE 0/1 - 0/11	VLAN 50,151
	GE 0/12 - 0/21	FE 0/12 - 0/21	VLAN 60,151
	GE 0/22 - 0/31	FE 0/22 - 0/31	VLAN 70,151
	GE 0/32 - 0/43	FE 0/32 - 0/43	VLAN 90,151
	GE 0/49	FE 0/0	VLAN 200
Switch_LPZ_3	GE 0/1 - 0/20	FE 0/1 - 0/20	VLAN 100
	GE 0/25	FE 0/0	VLAN 200
Administracion	GE 0/3 - 0/12	FE 0/3 - 0/12	VLAN 110
	TGE 0/0, GE 0/1 - 0/2	FE 0/0, FE 0/1 - 0/2	VLAN 200,152

Tabla 30: Asignación de puertos de Switches – La Paz

Dispositivo	Puertos Fisicos	Puertos GNS3	Asignación VLAN
Switch_CBBA_1	GE 0/1 - 0/6	FE 0/1 - 0/6	VLAN 10,150
	GE 0/7 - 0/13	FE 0/7 - 0/13	VLAN 20,150
	GE 0/14 - 0/23	FE 0/14 - 0/23	VLAN 30,150
	GE 0/24 - 0/29	FE 0/24 - 0/29	VLAN 40,150
	GE 0/30 - 0/36	FE 0/30 - 0/36	VLAN 80,150
	GE 0/49	FE 0/0	VLAN 200
Switch_CBBA_2	GE 0/1 - 0/9	FE 0/1 - 0/9	VLAN 50,151
	GE 0/10 - 0/16	FE 0/10 - 0/16	VLAN 60,151
	GE 0/17 - 0/24	FE 0/17 - 0/24	VLAN 70,151
	GE 0/25 - 0/32	FE 0/25 - 0/32	VLAN 90,151
	GE 0/33	FE 0/33	VLAN 110,151
	GE 0/49	FE 0/0	VLAN 200

Tabla 31: Asignación de puertos de Switches – Cochabamba

Dispositivo	Puertos Fisicos	Puertos GNS3	Asignación VLAN
Switch_SCZ_1	GE 0/1 - 0/6	FE 0/1 - 0/6	VLAN 10,150
	GE 0/7 - 0/14	FE 0/7 - 0/14	VLAN 20,150
	GE 0/15 - 0/25	FE 0/15 - 0/25	VLAN 30,150
	GE 0/26 - 0/31	FE 0/26 - 0/31	VLAN 40,150
	GE 0/32 - 0/38	FE 0/32 - 0/38	VLAN 80,150
	GE 0/49	FE 0/0	VLAN 200
Switch_SCZ_2	GE 0/1 - 0/10	FE 0/1 - 0/10	VLAN 50,151
	GE 0/11 - 0/19	FE 0/11 - 0/19	VLAN 60,151
	GE 0/20 - 0/28	FE 0/20 - 0/28	VLAN 70,151
	GE 0/29 - 0/36	FE 0/29 - 0/36	VLAN 90,151
	GE 0/37	FE 0/37	VLAN 110,151
	GE 0/49	FE 0/0	VLAN 200

Tabla 32: Asignación de puertos de Switches – Santa Cruz

Dispositivo	Interfaz	Dirección IPv4	Máscara de Subred	Gateway Predeterminado
		Dirección/prefijo IPv6		
Switch-LPZ-1	VLAN 200	192.168.110.226	255.255.255.248	192.168.110.225
		2001:db8:acef:201::2/64		2001:db8:acef:201::1
Switch-LPZ-2	VLAN 200	192.168.111.194	255.255.255.248	192.168.111.193
		2001:db8:acef:202::2/64		2001:db8:acef:202::1
Switch-LPZ-3	VLAN 200	192.168.112.66	255.255.255.248	192.168.112.65
		2001:db8:acef:203::2/64		2001:db8:acef:203::1
Administracion	VLAN 200	192.168.113.34	255.255.255.248	192.168.113.33
		2001:db8:acef:200::2/64		2001:db8:acef:200::1

Tabla 33: VLAN de administración – La Paz

Dispositivo	Interfaz	Dirección IPv4	Máscara de Subred	Gateway Predeterminado
		Dirección/prefijo IPv6		
LPZ	G0/0	10.0.0.1	255.255.255.252	N/A
		N/A		
	G1/0.10	192.168.110.65	255.255.255.224	N/A
		2001:db8:acef::1/64		
	G1/0.20	192.168.110.97	255.255.255.224	N/A
		2001:db8:acef:6::1/64		
	G1/0.30	192.168.110.129	255.255.255.224	N/A
		2001:db8:acef:3::1/64		
	G1/0.40	192.168.110.161	255.255.255.224	N/A
		2001:db8:acef:8::1/64		
	G1/0.80	192.168.110.193	255.255.255.224	N/A
		2001:db8:acef:9::1/64		
	G1/0.150	192.168.110.1	255.255.255.192	N/A
		2001:db8:acef:b::1/64		
	G1/0.200	192.168.110.225	255.255.255.248	N/A
		2001:db8:acef:201::1/64		
	G2/0.50	192.168.111.65	255.255.255.224	N/A
		2001:db8:acef:2::1/64		
	G2/0.60	192.168.111.97	255.255.255.224	N/A
		2001:db8:acef:5::1/64		
	G2/0.70	192.168.111.129	255.255.255.224	N/A
		2001:db8:acef:7::1/64		
	G2/0.90	192.168.111.161	255.255.255.224	N/A
		2001:db8:acef:a::1/64		
	G2/0.151	192.168.111.1	255.255.255.192	N/A
		2001:db8:acef:c::1/64		
	G2/0.200	192.168.111.193	255.255.255.248	N/A
		2001:db8:acef:202::1/64		
	G3/0.100	192.168.112.1	255.255.255.192	N/A
		2001:db8:acef:4::1/64		
	G3/0.200	192.168.112.65	255.255.255.248	N/A
		2001:db8:acef:203::1/64		
	G4/0.110	192.168.113.1	255.255.255.224	N/A
		2001:db8:acef:1::1/64		
	G4/0.152	192.168.113.41	255.255.255.252	N/A
		2001:db8:acef:d::1/64		
	G4/0.200	192.168.113.33	255.255.255.248	N/A
		2001:db8:acef:200::1/64		
	G5/0	181.188.178.225	255.255.255.252	N/A
		2001:db8:acef:f000::1/64		
	G6/0	10.0.0.5	255.255.255.252	N/A
		N/A		

Tabla 34: Asignación de direcciones de red a las interfaces del Router de La Paz

Dispositivo	Interfaz	Dirección IPv4	Máscara de Subred	Gateway Predeterminado
		Dirección/prefijo IPv6		
Switch-CBBA-1	VLAN 200	192.168.120.210	255.255.255.248	192.168.120.209
		2001:db8:acef:205::2/64		2001:db8:acef:205::1
Switch-CBBA-2	VLAN 200	192.168.121.186	255.255.255.248	192.168.121.185
		2001:db8:acef:206::2/64		2001:db8:acef:206::1

Tabla 35: VLAN de administración – Cochabamba

Dispositivo	Interfaz	Dirección IPv4	Máscara de Subred	Gateway Predeterminado
		Dirección/prefijo IPv6		
CBBA	G0/0	10.0.0.2	255.255.255.252	N/A
		N/A		
	G2/0.10	192.168.120.65	255.255.255.224	N/A
		2001:db8:acef:10::1/64		
	G2/0.20	192.168.120.97	255.255.255.224	N/A
		2001:db8:acef:15::1/64		
	G2/0.30	192.168.120.129	255.255.255.224	N/A
		2001:db8:acef:13::1/64		
	G2/0.40	120.168.120.161	255.255.255.224	N/A
		2001:db8:acef:17::1/64		
	G2/0.80	192.168.120.193	255.255.255.240	N/A
		2001:db8:acef:18::1/64		
	G2/0.150	192.168.120.1	255.255.255.192	N/A
		2001:db8:acef:1a::1/64		
	G2/0.200	192.168.120.209	255.255.255.248	N/A
		2001:db8:acef:205::1/64		
	G3/0.50	192.168.121.65	255.255.255.224	N/A
		2001:db8:acef:12::1/64		
	G3/0.60	192.168.121.97	255.255.255.224	N/A
		2001:db8:acef:14::1/64		
	G3/0.70	192.168.121.129	255.255.255.224	N/A
		2001:db8:acef:16::1/64		
	G3/0.90	192.168.121.161	255.255.255.240	N/A
		2001:db8:acef:19::1/64		
	G3/0.110	192.168.121.177	255.255.255.248	N/A
		2001:db8:acef:11::1/64		
	G3/0.151	192.168.121.1	255.255.255.192	N/A
		2001:db8:acef:1b::1/64		
	G3/0.200	192.168.121.185	255.255.255.248	N/A
		2001:db8:acef:206::1/64		

Tabla 36: Asignación de direcciones de red a las interfaces del Router de Cochabamba

Dispositivo	Interfaz	Dirección IPv4	Máscara de Subred	Gateway Predeterminado
		Dirección/prefijo IPv6		
Switch-SCZ-1	VLAN 200	192.168.130.210	255.255.255.248	192.168.130.209
		2001:db8:acef:207::2/64		2001:db8:acef:207::1
Switch-SCZ-2	VLAN 200	192.168.131.186	255.255.255.248	192.168.131.185
		2001:db8:acef:208::2/64		2001:db8:acef:208::1

Tabla 37: VLAN de administración – Santa Cruz

Dispositivo	Interfaz	Dirección IPv4	Máscara de Subred	Gateway Predeterminado
		Dirección/prefijo IPv6		
SCZ	G0/0	10.0.0.6	255.255.255.252	N/A
		N/A		
	G2/0.10	192.168.130.65	255.255.255.224	N/A
		2001:db8:acef:20::1/64		
	G2/0.20	192.168.130.97	255.255.255.224	N/A
		2001:db8:acef:25::1/64		
	G2/0.30	192.168.130.129	255.255.255.224	N/A
		2001:db8:acef:23::1/64		
	G2/0.40	120.168.130.161	255.255.255.224	N/A
		2001:db8:acef:27::1/64		
	G2/0.80	192.168.130.193	255.255.255.240	N/A
		2001:db8:acef:28::1/64		
	G2/0.150	192.168.130.1	255.255.255.192	N/A
		2001:db8:acef:2a::1/64		
	G2/0.200	192.168.130.209	255.255.255.248	N/A
		2001:db8:acef:207::1/64		
	G3/0.50	192.168.131.65	255.255.255.224	N/A
		2001:db8:acef:22::1/64		
	G3/0.60	192.168.131.97	255.255.255.224	N/A
		2001:db8:acef:24::1/64		
	G3/0.70	192.168.131.129	255.255.255.224	N/A
		2001:db8:acef:26::1/64		
	G3/0.90	192.168.131.161	255.255.255.240	N/A
		2001:db8:acef:29::1/64		
	G3/0.110	192.168.131.177	255.255.255.248	N/A
		2001:db8:acef:21::1/64		
	G3/0.151	192.168.131.1	255.255.255.192	N/A
		2001:db8:acef:2b::1/64		
	G3/0.200	192.168.131.185	255.255.255.248	N/A
		2001:db8:acef:208::1/64		

Tabla 38: Asignación de direcciones de red a las interfaces del Router de Santa Cruz

3.2.10. Topología Lógica de la Red

A continuación, se muestra la topología lógica de la red que se diseñó y se simulará para verificar el funcionamiento del presente proyecto.

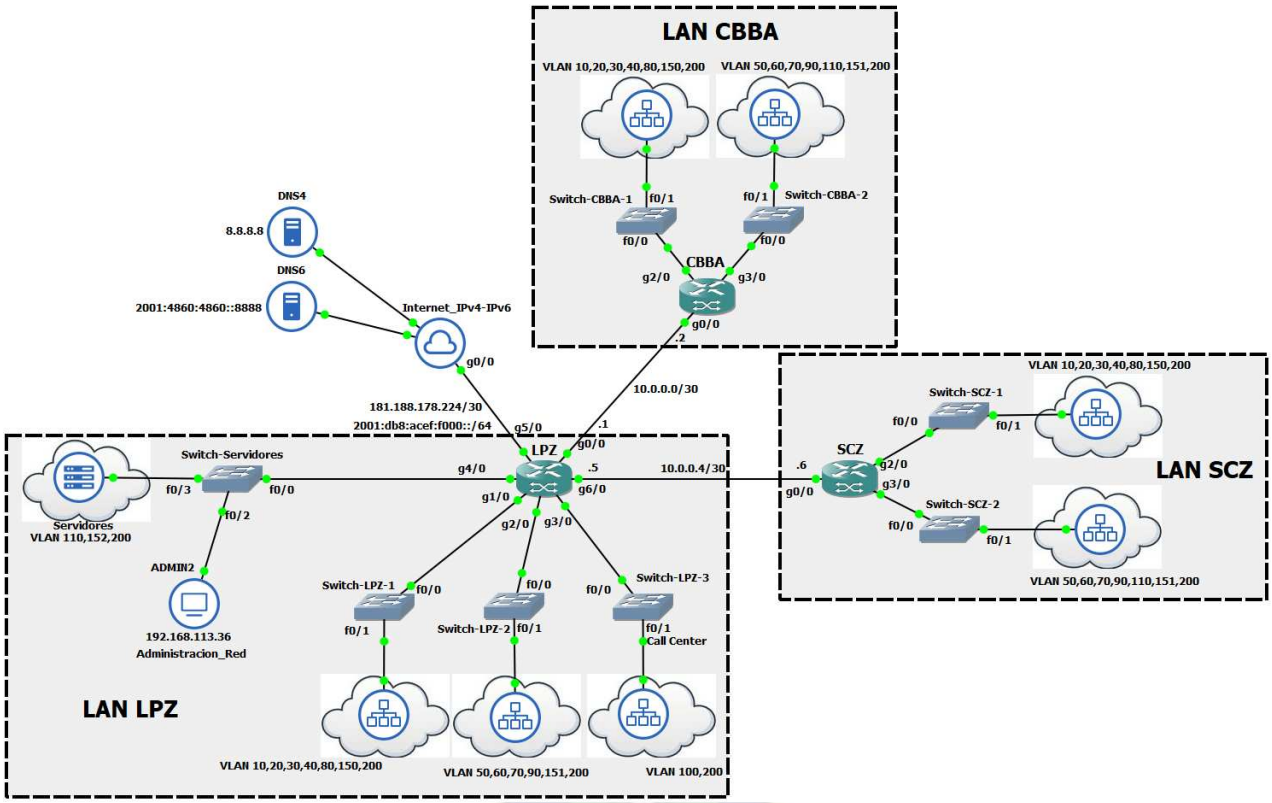


Figura 25: Topología Lógica de la Red

3.3. Diseño de Calidad de Servicio (QoS) de la Red

De acuerdo a la clasificación de tipos de tráfico (Figura 19), se hizo un diseño de modelo de QoS de 8 clases, ajustándose al tamaño del campo EXP (3 bits) de una etiqueta MPLS y adaptando estas clases de tráfico al modelo de QoS DiffServ, se obtiene las siguientes asignaciones:

Modelo de 8 Clases	EXP	PHB
Voz	5	EF
Videoconferencias	4	CS4
Video Broadcast	3	CS3
Señalizacion de Llamada	3	CS3
Control de Red	6	CS6
Datos Transaccionales	2	AF2
Best Effort	0	DF
Scavenger	1	CS1

Tabla 39: Clasificación y marcado del modelo de QoS

Para las clases de tráfico de Control de Red, Video Broadcast, Señalización de Llamada, Datos Transaccionales, Scavenger y Best Effort, se empleará el Mecanismo CBWFQ, el cual admite clases de tráfico definidas por el usuario. Y para las clases de tráfico de Voz y Videoconferencias, se empleará el mecanismo LLQ, ya que, al ser estas clases prioritarias, se enviarán antes que los paquetes de otras colas, con lo que se otorga un tratamiento preferencial a los datos susceptibles a la demora.

Clase deTráfico	PHB	Mecanismo	BW Asignado
Voz	EF	LLQ	10%
Videoconferencias	CS4	LLQ	23%
Señalizacion y Video Broadcast	CS3	CBWFQ	12%
Control de Red	CS6	CBWFQ	5%
Datos Transaccionales	AF2	CBWFQ	23%
Best Effort	DF	CBWFQ	25%
Scavenger	CS1	CBWFQ	2%

Tabla 40: Políticas de QoS al modelo de tráfico

CAPITULO IV
ANALISIS DE RESULTADOS

4.1. Simulación en el software GNS3

GNS3 es un simulador gráfico de red de código abierto, bajo licencia GPLv3, el cual permite diseñar topologías de red complejas de alta calidad y realizar simulaciones sobre las mismas. Los equipos de red simulados disponen de las funcionalidades de un equipo real, ya que ejecutan el mismo firmware que utilizaríamos en un equipo físico. Lo que nos permitirá diseñar una topología de red simulada lo más parecida posible a una situación real sin tener la necesidad de tener acceso a ningún equipo físico.

Para simular un equipo de red, se necesita tener la imagen del sistema operativo del mismo, sin embargo, la adquisición de esta imagen tiene un costo, en este caso a la empresa Cisco como se puede consultar en su página web: https://software.cisco.com/download/home. Por otra parte, existen algunos modelos de equipos de red: c7200, c3640, cuya imagen de sistema operativo se lo puede descargar de forma gratuita y además estos equipos tienen prestaciones similares a los equipos reales del proyecto, por lo que se los empleará en la simulación del proyecto.

4.2. Configuración de los routers y equipos de la Red

Una vez inicializada la red, se procede a configurar los equipos, mediante la ventana de *consola* de cada uno de los mismos.

En cada router, se creará y se hará uso de una interfaz ***loopback***, para poder recibir y enviar las actualizaciones de los protocolos de enrutamiento a utilizar en la red.

Dispositivo	Interfaz Loopback
Router - LPZ	10.10.10.1
Router - CBBA	10.10.10.2
Router - SCZ	10.10.10.3

Tabla 41: Interfaces Loopback - Routers

A continuación, se menciona las configuraciones realizadas:

- Asignación de direcciones de Red a Routers y Switches
- Configuración del protocolo de enrutamiento OSPFv2
- Configuración de MPLS en el núcleo de red IPv4
- Configuración de MP-BGP: para anunciar etiquetas MPLS de redes IPv6
- Configuración clasificación y políticas de QoS
- Configuración para la conexión a la red de Internet
- Configuración de NAT para direcciones IPv4
- Configuración de Listas de Acceso y acceso remoto mediante SSH

La habilitación de PoE (Power over Ethernet) en cada puerto de los switches, se lo realiza con el siguiente comando: ***power inline [auto | never]***, con la opción ***never*** el switch deja de suministrar energía en el puerto especificado.

Cabe mencionar que el modelo de switch simulado en GNS3 no dispone del comando mencionado anteriormente, razón por la cual no se observa la lista de comandos relacionados a PoE, que se emplearía en cada uno de los puertos de los switches.

4.3. Administración de la Red

Sin lugar a duda la administración de la red es la parte fundamental para que la compañía pueda funcionar correctamente en todo momento, para ello se necesita de herramientas de monitoreo y control centralizado, que permitan evaluar, monitorizar y solucionar el estado de la red.

Para lo cual se hará uso del software PRTG, para realizar el monitoreo de la red, con el cual obtendremos en tiempo real del tráfico existente en diferentes puntos de la red.

Primeramente, se tiene que habilitar el protocolo SNMP (Simple Network Management Protocol), en los dispositivos de red a administrar (Routers y Switches), para ello se hará uso del siguiente comando ***snmp-server community [NAME] ro***, en el modo de configuración global de cada dispositivo:

```
LPZ(config)# snmp-server community ADMIN1 ro

CBBA(config)# snmp-server community ADMIN1 ro

SCZ(config)# snmp-server community ADMIN1 ro

Switch-LPZ-1(config)# snmp-server community ADMIN1 ro

Switch-LPZ-2(config)# snmp-server community ADMIN1 ro

Switch-LPZ-3(config)# snmp-server community ADMIN1 ro

Switch-Administradores(config)# snmp-server community ADMIN1 ro

Switch-CBBA-1(config)# snmp-server community ADMIN1 ro

Switch-CBBA-2(config)# snmp-server community ADMIN1 ro

Switch-SCZ-1(config)# snmp-server community ADMIN1 ro

Switch-SCZ-2(config)# snmp-server community ADMIN1 ro
```

Lo siguiente será añadir cada dispositivo de red, a la herramienta de monitorización, para observar el tráfico entrante/saliente en las interfaces de los Routers y Switches:

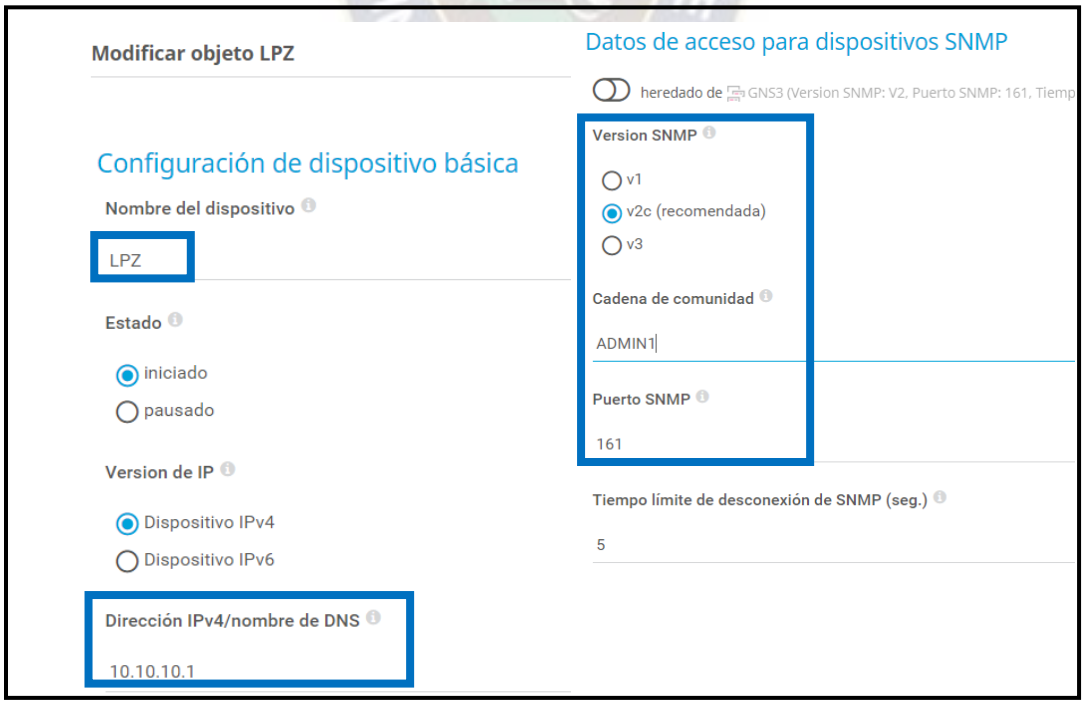


Figura 26: Configuración del Router LPZ en PRTG

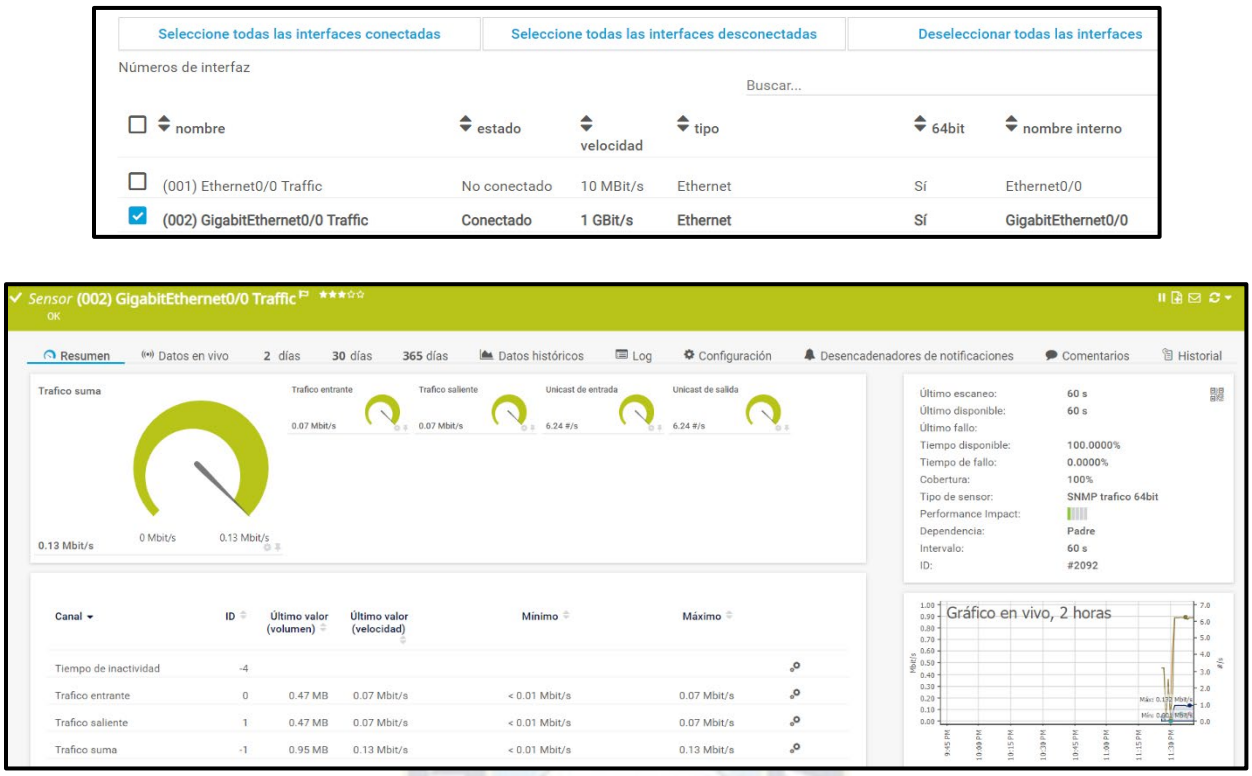


Figura 27: Asignación de un sensor de tráfico en la Interfaz GE 0/0 del Router LPZ

Como se observa en la figura 26, la adición de cada dispositivo (Router y/o Switch) a la herramienta de monitoreo, se lo hace introduciendo su dirección loopback o su dirección de red de la VLAN de ADMINISTRACION respectiva, además de las credenciales del protocolo SNMP necesaria de cada dispositivo. Las configuraciones para los demás dispositivos son similares, por lo que se omitirá la visualización de las mismas.

Por otra parte, para tener un control centralizado de la administración de todos los dispositivos de la red, se utilizará un cliente de acceso remoto “PUTTY”, el cual permitirá al administrador de la red, acceder de manera remota y segura a los dispositivos de la red mediante el protocolo SSH.

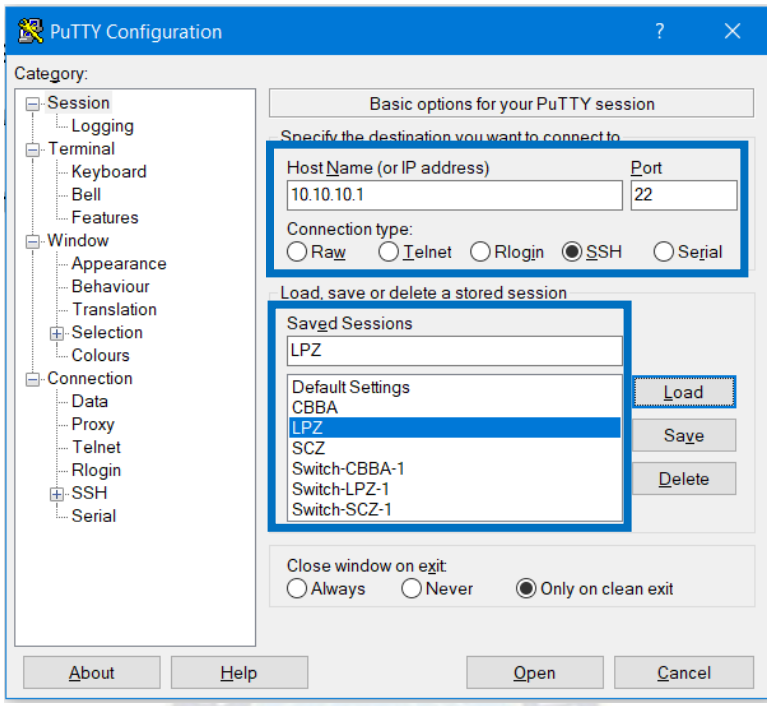


Figura 28: Sesiones de acceso remoto a dispositivos de red mediante PUTTY

4.4. Validación de configuración y análisis de pruebas

Verificación de la tabla de enrutamiento IPv4, de las direcciones de red conectadas directamente a cada interfaz de los routers y rutas estáticas por defecto.

Router LPZ:

```
LPZ#show ip route connected
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 181.188.178.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 181.188.178.226, GigabitEthernet5/0
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.0.0/30 is directly connected, GigabitEthernet0/0
L        10.0.0.1/32 is directly connected, GigabitEthernet0/0
C        10.0.0.4/30 is directly connected, GigabitEthernet6/0
L        10.0.0.5/32 is directly connected, GigabitEthernet6/0
C        10.10.10.1/32 is directly connected, Loopback0
      181.188.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        181.188.178.224/30 is directly connected, GigabitEthernet5/0
L        181.188.178.225/32 is directly connected, GigabitEthernet5/0
      192.168.110.0/24 is variably subnetted, 14 subnets, 4 masks
C        192.168.110.0/26 is directly connected, GigabitEthernet1/0.150
L        192.168.110.1/32 is directly connected, GigabitEthernet1/0.150
```

```
C        192.168.110.64/27 is directly connected, GigabitEthernet1/0.10
L        192.168.110.65/32 is directly connected, GigabitEthernet1/0.10
C        192.168.110.96/27 is directly connected, GigabitEthernet1/0.20
L        192.168.110.97/32 is directly connected, GigabitEthernet1/0.20
C        192.168.110.128/27 is directly connected, GigabitEthernet1/0.30
L        192.168.110.129/32 is directly connected, GigabitEthernet1/0.30
C        192.168.110.160/27 is directly connected, GigabitEthernet1/0.40
L        192.168.110.161/32 is directly connected, GigabitEthernet1/0.40
C        192.168.110.192/27 is directly connected, GigabitEthernet1/0.80
L        192.168.110.193/32 is directly connected, GigabitEthernet1/0.80
C        192.168.110.224/29 is directly connected, GigabitEthernet1/0.200
L        192.168.110.225/32 is directly connected, GigabitEthernet1/0.200
      192.168.111.0/24 is variably subnetted, 12 subnets, 4 masks
C        192.168.111.0/26 is directly connected, GigabitEthernet2/0.151
L        192.168.111.1/32 is directly connected, GigabitEthernet2/0.151
C        192.168.111.64/27 is directly connected, GigabitEthernet2/0.50
L        192.168.111.65/32 is directly connected, GigabitEthernet2/0.50
C        192.168.111.96/27 is directly connected, GigabitEthernet2/0.60
L        192.168.111.97/32 is directly connected, GigabitEthernet2/0.60
C        192.168.111.128/27 is directly connected, GigabitEthernet2/0.70
L        192.168.111.129/32 is directly connected, GigabitEthernet2/0.70
C        192.168.111.160/27 is directly connected, GigabitEthernet2/0.90
L        192.168.111.161/32 is directly connected, GigabitEthernet2/0.90
C        192.168.111.192/29 is directly connected, GigabitEthernet2/0.200
L        192.168.111.193/32 is directly connected, GigabitEthernet2/0.200
      192.168.112.0/24 is variably subnetted, 4 subnets, 3 masks
C        192.168.112.0/26 is directly connected, GigabitEthernet3/0.100
L        192.168.112.1/32 is directly connected, GigabitEthernet3/0.100
C        192.168.112.64/29 is directly connected, GigabitEthernet3/0.200
L        192.168.112.65/32 is directly connected, GigabitEthernet3/0.200
      192.168.113.0/24 is variably subnetted, 6 subnets, 4 masks
C        192.168.113.0/27 is directly connected, GigabitEthernet4/0.110
L        192.168.113.1/32 is directly connected, GigabitEthernet4/0.110
C        192.168.113.32/29 is directly connected, GigabitEthernet4/0.200
L        192.168.113.33/32 is directly connected, GigabitEthernet4/0.200
C        192.168.113.40/30 is directly connected, GigabitEthernet4/0.152
L        192.168.113.41/32 is directly connected, GigabitEthernet4/0.152
```

Router CBBA:

```
CBBA#show ip route connected
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.0.0.0/30 is directly connected, GigabitEthernet0/0
L        10.0.0.2/32 is directly connected, GigabitEthernet0/0
C        10.10.10.2/32 is directly connected, Loopback0
      192.168.120.0/24 is variably subnetted, 14 subnets, 5 masks
C        192.168.120.0/26 is directly connected, GigabitEthernet2/0.150
L        192.168.120.1/32 is directly connected, GigabitEthernet2/0.150
C        192.168.120.64/27 is directly connected, GigabitEthernet2/0.10
L        192.168.120.65/32 is directly connected, GigabitEthernet2/0.10
C        192.168.120.96/27 is directly connected, GigabitEthernet2/0.20
L        192.168.120.97/32 is directly connected, GigabitEthernet2/0.20
C        192.168.120.128/27 is directly connected, GigabitEthernet2/0.30
L        192.168.120.129/32 is directly connected, GigabitEthernet2/0.30
C        192.168.120.160/27 is directly connected, GigabitEthernet2/0.40
L        192.168.120.161/32 is directly connected, GigabitEthernet2/0.40
C        192.168.120.192/28 is directly connected, GigabitEthernet2/0.80
L        192.168.120.193/32 is directly connected, GigabitEthernet2/0.80
C        192.168.120.208/29 is directly connected, GigabitEthernet2/0.200
L        192.168.120.209/32 is directly connected, GigabitEthernet2/0.200
      192.168.121.0/24 is variably subnetted, 14 subnets, 5 masks
C        192.168.121.0/26 is directly connected, GigabitEthernet3/0.151
L        192.168.121.1/32 is directly connected, GigabitEthernet3/0.151
C        192.168.121.64/27 is directly connected, GigabitEthernet3/0.50
L        192.168.121.65/32 is directly connected, GigabitEthernet3/0.50
C        192.168.121.96/27 is directly connected, GigabitEthernet3/0.60
L        192.168.121.97/32 is directly connected, GigabitEthernet3/0.60
C        192.168.121.128/27 is directly connected, GigabitEthernet3/0.70
L        192.168.121.129/32 is directly connected, GigabitEthernet3/0.70
C        192.168.121.160/28 is directly connected, GigabitEthernet3/0.90
L        192.168.121.161/32 is directly connected, GigabitEthernet3/0.90
C        192.168.121.176/29 is directly connected, GigabitEthernet3/0.110
L        192.168.121.177/32 is directly connected, GigabitEthernet3/0.110
C        192.168.121.184/29 is directly connected, GigabitEthernet3/0.200
L        192.168.121.185/32 is directly connected, GigabitEthernet3/0.200
```

Router SCZ:

```
SCZ#show ip route connected
Gateway of last resort is 10.0.0.5 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.0.4/30 is directly connected, GigabitEthernet0/0
L        10.0.0.6/32 is directly connected, GigabitEthernet0/0
C        10.10.10.3/32 is directly connected, Loopback0
      192.168.130.0/24 is variably subnetted, 14 subnets, 5 masks
C        192.168.130.0/26 is directly connected, GigabitEthernet2/0.150
L        192.168.130.1/32 is directly connected, GigabitEthernet2/0.150
C        192.168.130.64/27 is directly connected, GigabitEthernet2/0.10
L        192.168.130.65/32 is directly connected, GigabitEthernet2/0.10
C        192.168.130.96/27 is directly connected, GigabitEthernet2/0.20
L        192.168.130.97/32 is directly connected, GigabitEthernet2/0.20
C        192.168.130.128/27 is directly connected, GigabitEthernet2/0.30
L        192.168.130.129/32 is directly connected, GigabitEthernet2/0.30
C        192.168.130.160/27 is directly connected, GigabitEthernet2/0.40
L        192.168.130.161/32 is directly connected, GigabitEthernet2/0.40
C        192.168.130.192/28 is directly connected, GigabitEthernet2/0.80
L        192.168.130.193/32 is directly connected, GigabitEthernet2/0.80
C        192.168.130.208/29 is directly connected, GigabitEthernet2/0.200
L        192.168.130.209/32 is directly connected, GigabitEthernet2/0.200
      192.168.131.0/24 is variably subnetted, 14 subnets, 5 masks
C        192.168.131.0/26 is directly connected, GigabitEthernet3/0.151
L        192.168.131.1/32 is directly connected, GigabitEthernet3/0.151
C        192.168.131.64/27 is directly connected, GigabitEthernet3/0.50
L        192.168.131.65/32 is directly connected, GigabitEthernet3/0.50
C        192.168.131.96/27 is directly connected, GigabitEthernet3/0.60
L        192.168.131.97/32 is directly connected, GigabitEthernet3/0.60
C        192.168.131.128/27 is directly connected, GigabitEthernet3/0.70
L        192.168.131.129/32 is directly connected, GigabitEthernet3/0.70
C        192.168.131.160/28 is directly connected, GigabitEthernet3/0.90
L        192.168.131.161/32 is directly connected, GigabitEthernet3/0.90
C        192.168.131.176/29 is directly connected, GigabitEthernet3/0.110
L        192.168.131.177/32 is directly connected, GigabitEthernet3/0.110
C        192.168.131.184/29 is directly connected, GigabitEthernet3/0.200
L        192.168.131.185/32 is directly connected, GigabitEthernet3/0.200
```

Verificación de la tabla de enrutamiento IPv6, de las direcciones de red conectadas directamente a cada interfaz de los routers y rutas estáticas por defecto.

Router LPZ:

```
LPZ#show ipv6 route connected
S   ::/0 [1/0]
C   2001:DB8:ACEF::/64 [0/0]
     via GigabitEthernet1/0.10, directly connected
C   2001:DB8:ACEF:1::/64 [0/0]
     via GigabitEthernet4/0.110, directly connected
C   2001:DB8:ACEF:2::/64 [0/0]
     via GigabitEthernet2/0.50, directly connected
C   2001:DB8:ACEF:3::/64 [0/0]
     via GigabitEthernet1/0.30, directly connected
C   2001:DB8:ACEF:4::/64 [0/0]
     via GigabitEthernet3/0.100, directly connected
C   2001:DB8:ACEF:5::/64 [0/0]
     via GigabitEthernet2/0.60, directly connected
C   2001:DB8:ACEF:6::/64 [0/0]
     via GigabitEthernet1/0.20, directly connected
C   2001:DB8:ACEF:7::/64 [0/0]
     via GigabitEthernet2/0.70, directly connected
C   2001:DB8:ACEF:8::/64 [0/0]
     via GigabitEthernet1/0.40, directly connected
C   2001:DB8:ACEF:9::/64 [0/0]
     via GigabitEthernet1/0.80, directly connected
C   2001:DB8:ACEF:203::/64 [0/0]
     via GigabitEthernet3/0.200, directly connected
C   2001:DB8:ACEF:F000::/64 [0/0]
     via GigabitEthernet5/0, directly connected
```

```
C   2001:DB8:ACEF:A::/64 [0/0]
     via GigabitEthernet2/0.90, directly connected
C   2001:DB8:ACEF:B::/64 [0/0]
     via GigabitEthernet1/0.150, directly connected
C   2001:DB8:ACEF:C::/64 [0/0]
     via GigabitEthernet2/0.151, directly connected
C   2001:DB8:ACEF:D::/64 [0/0]
     via GigabitEthernet4/0.152, directly connected
C   2001:DB8:ACEF:200::/64 [0/0]
     via GigabitEthernet4/0.200, directly connected
C   2001:DB8:ACEF:201::/64 [0/0]
     via GigabitEthernet1/0.200, directly connected
C   2001:DB8:ACEF:202::/64 [0/0]
     via GigabitEthernet2/0.200, directly connected
C   2001:DB8:ACEF:203::/64 [0/0]
     via GigabitEthernet3/0.200, directly connected
C   2001:DB8:ACEF:F000::/64 [0/0]
     via GigabitEthernet5/0, directly connected
```

Router CBBA:

```
CBBA#show ipv6 route connected
C   2001:DB8:ACEF:10::/64 [0/0]
     via GigabitEthernet2/0.10, directly connected
C   2001:DB8:ACEF:11::/64 [0/0]
     via GigabitEthernet3/0.110, directly connected
C   2001:DB8:ACEF:12::/64 [0/0]
     via GigabitEthernet3/0.50, directly connected
C   2001:DB8:ACEF:13::/64 [0/0]
     via GigabitEthernet2/0.30, directly connected
C   2001:DB8:ACEF:14::/64 [0/0]
     via GigabitEthernet3/0.60, directly connected
C   2001:DB8:ACEF:15::/64 [0/0]
     via GigabitEthernet2/0.20, directly connected
C   2001:DB8:ACEF:16::/64 [0/0]
     via GigabitEthernet3/0.70, directly connected
C   2001:DB8:ACEF:17::/64 [0/0]
     via GigabitEthernet2/0.40, directly connected
C   2001:DB8:ACEF:18::/64 [0/0]
     via GigabitEthernet2/0.80, directly connected
C   2001:DB8:ACEF:19::/64 [0/0]
     via GigabitEthernet3/0.90, directly connected
C   2001:DB8:ACEF:1A::/64 [0/0]
     via GigabitEthernet2/0.150, directly connected
C   2001:DB8:ACEF:1B::/64 [0/0]
     via GigabitEthernet3/0.151, directly connected
C   2001:DB8:ACEF:205::/64 [0/0]
     via GigabitEthernet2/0.200, directly connected
C   2001:DB8:ACEF:206::/64 [0/0]
     via GigabitEthernet3/0.200, directly connected
```

Router SCZ:

```
SCZ#show ipv6 route connected
C   2001:DB8:ACEF:20::/64 [0/0]
     via GigabitEthernet2/0.10, directly connected
C   2001:DB8:ACEF:21::/64 [0/0]
     via GigabitEthernet3/0.110, directly connected
C   2001:DB8:ACEF:22::/64 [0/0]
     via GigabitEthernet3/0.50, directly connected
C   2001:DB8:ACEF:23::/64 [0/0]
     via GigabitEthernet2/0.30, directly connected
C   2001:DB8:ACEF:24::/64 [0/0]
     via GigabitEthernet3/0.60, directly connected
C   2001:DB8:ACEF:25::/64 [0/0]
     via GigabitEthernet2/0.20, directly connected
C   2001:DB8:ACEF:26::/64 [0/0]
     via GigabitEthernet3/0.70, directly connected
C   2001:DB8:ACEF:27::/64 [0/0]
     via GigabitEthernet2/0.40, directly connected
     via GigabitEthernet3/0.200, directly connected
```

```
C   2001:DB8:ACEF:28::/64 [0/0]
     via GigabitEthernet2/0.80, directly connected
C   2001:DB8:ACEF:29::/64 [0/0]
     via GigabitEthernet3/0.90, directly connected
C   2001:DB8:ACEF:2A::/64 [0/0]
     via GigabitEthernet2/0.150, directly connected
C   2001:DB8:ACEF:2B::/64 [0/0]
     via GigabitEthernet3/0.151, directly connected
C   2001:DB8:ACEF:207::/64 [0/0]
     via GigabitEthernet2/0.200, directly connected
C   2001:DB8:ACEF:208::/64 [0/0]
     via GigabitEthernet3/0.200, directly connected
```

Verificación del núcleo de la red MPLS, protocolo de enrutamiento OSPF, intercambio de información de etiquetas entre routers vecinos mediante LDP, tabla de etiquetas locales y remotas.

Protocolo de enrutamiento OSPF:

```
LPZ#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.3        1   FULL/DR         00:00:35    10.0.0.6        GigabitEthernet6/0
10.10.10.2        1   FULL/DR         00:00:38    10.0.0.2        GigabitEthernet0/0
```

```
CBBA#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.1        1   FULL/BDR        00:00:38    10.0.0.1        GigabitEthernet0/0
```

```
SCZ#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.1        1   FULL/BDR        00:00:32    10.0.0.5        GigabitEthernet0/0
```

La información **Neighbor ID** indica el identificador asociado a cada router, para realizar el intercambio de información necesaria con el o los routers vecinos.

Protocolo de distribución de etiquetas (LDP):

```
LPZ#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.2:0; Local LDP Ident 10.10.10.1:0
        TCP connection: 10.10.10.2.22964 - 10.10.10.1.646
        State: Oper; Msgs sent/rcvd: 70/70; Downstream
        Up time: 00:12:32
        LDP discovery sources:
          GigabitEthernet0/0, Src IP addr: 10.0.0.2
        Addresses bound to peer LDP Ident:
          10.0.0.2        10.10.10.2      192.168.120.65  192.168.120.97
          192.168.120.129 192.168.120.161 192.168.120.193 192.168.120.1
          192.168.120.209 192.168.121.65  192.168.121.97  192.168.121.129
          192.168.121.161 192.168.121.177 192.168.121.1   192.168.121.185
    Peer LDP Ident: 10.10.10.3:0; Local LDP Ident 10.10.10.1:0
        TCP connection: 10.10.10.3.16085 - 10.10.10.1.646
        State: Oper; Msgs sent/rcvd: 70/69; Downstream
        Up time: 00:12:31
        LDP discovery sources:
          GigabitEthernet6/0, Src IP addr: 10.0.0.6
        Addresses bound to peer LDP Ident:
          10.0.0.6        10.10.10.3      192.168.130.65  192.168.130.97
          192.168.130.129 192.168.130.161 192.168.130.193 192.168.130.1
          192.168.130.209 192.168.131.65  192.168.131.97  192.168.131.129
          192.168.131.161 192.168.131.177 192.168.131.1   192.168.131.185
```

```
CBBA#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.1:0; Local LDP Ident 10.10.10.2:0
        TCP connection: 10.10.10.1.646 - 10.10.10.2.22964
        State: Oper; Msgs sent/rcvd: 71/72; Downstream
        Up time: 00:14:31
        LDP discovery sources:
          GigabitEthernet0/0, Src IP addr: 10.0.0.1
        Addresses bound to peer LDP Ident:
          10.0.0.1        10.10.10.1      192.168.110.65  192.168.110.97
          192.168.110.129 192.168.110.161 192.168.110.193 192.168.110.1
          192.168.110.225 192.168.111.65  192.168.111.97  192.168.111.129
          192.168.111.161 192.168.111.1   192.168.111.193 192.168.112.1
          192.168.112.65  192.168.113.1   192.168.113.41  192.168.113.33
          181.188.178.225 10.0.0.5
```

```
SCZ#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.1:0; Local LDP Ident 10.10.10.3:0
        TCP connection: 10.10.10.1.646 - 10.10.10.3.16085
        State: Oper; Msgs sent/rcvd: 72/72; Downstream
        Up time: 00:14:54
        LDP discovery sources:
          GigabitEthernet0/0, Src IP addr: 10.0.0.5
        Addresses bound to peer LDP Ident:
          10.0.0.1        10.10.10.1      192.168.110.65  192.168.110.97
          192.168.110.129 192.168.110.161 192.168.110.193 192.168.110.1
          192.168.110.225 192.168.111.65  192.168.111.97  192.168.111.129
          192.168.111.161 192.168.111.1   192.168.111.193 192.168.112.1
          192.168.112.65  192.168.113.1   192.168.113.41  192.168.113.33
          181.188.178.225 10.0.0.5
```

No.	Time	Source	Destination	Protocol	Length	Info
49	21.898960	10.10.10.2	10.10.10.1	LDP	118	Initialization Message
50	21.941277	10.10.10.1	10.10.10.2	LDP	126	Initialization Message Keep Alive Message
51	21.963188	10.10.10.2	10.10.10.1	LDP	72	Keep Alive Message
52	21.963188	10.10.10.2	10.10.10.1	TCP	590	44274 → 646 [ACK] Seq=83 Ack=73 Win=4056 Len=536 [TCP segmer
53	21.974158	10.10.10.1	10.10.10.2	TCP	590	646 → 44274 [ACK] Seq=73 Ack=619 Win=3510 Len=536 [TCP segme
54	21.974158	10.10.10.1	10.10.10.2	TCP	60	[TCP Window Update] 646 → 44274 [ACK] Seq=609 Ack=619 Win=4
55	21.985129	10.10.10.2	10.10.10.1	TCP	60	44274 → 646 [ACK] Seq=619 Ack=609 Win=4128 Len=0
56	21.985129	10.10.10.2	10.10.10.1	TCP	590	44274 → 646 [ACK] Seq=619 Ack=609 Win=4128 Len=536 [TCP segr
57	21.996101	10.10.10.2	10.10.10.1	LDP	522	Address Message Label Mapping Message Label Mapping Message
58	22.071860	10.10.10.1	10.10.10.2	TCP	590	646 → 44274 [ACK] Seq=609 Ack=619 Win=4128 Len=536 [TCP segr
59	22.071860	10.10.10.1	10.10.10.2	TCP	60	646 → 44274 [ACK] Seq=1145 Ack=1155 Win=4128 Len=0
60	22.071860	10.10.10.1	10.10.10.2	LDP	574	Address Message Label Mapping Message Label Mapping Message

Figura 29: Intercambio de etiquetas entre routers vecinos (LPZ - CBBA)

Mediante el programa Wireshark se sacó una captura del tráfico (protocolo LDP), en la figura 29 se puede observar el mensaje de inicialización y posteriormente el intercambio de información de etiquetas y prefijos de red, de cada router vecino, los cuales son 10.10.10.1: Router LPZ y 10.10.10.2: Router CBBA.

Ahora observaremos las etiquetas locales MPLS asignadas por cada router, a cada dirección de red.

Tabla LFIB - Router LPZ

```
LPZ#show mpls forwarding-table
Local      Outgoing   Prefix              Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id        Switched      interface

16         Pop Label  10.10.10.3/32       8976          Gi6/0      10.0.0.6
17         Pop Label  10.10.10.2/32       2540          Gi0/0      10.0.0.2
18         Pop Label  192.168.131.184/29  0             Gi6/0      10.0.0.6
19         Pop Label  192.168.131.176/29  0             Gi6/0      10.0.0.6
20         Pop Label  192.168.131.160/28  0             Gi6/0      10.0.0.6
21         Pop Label  192.168.131.128/27  0             Gi6/0      10.0.0.6
22         Pop Label  192.168.131.96/27   0             Gi6/0      10.0.0.6
23         Pop Label  192.168.131.64/27   0             Gi6/0      10.0.0.6
24         Pop Label  192.168.131.0/26    0             Gi6/0      10.0.0.6
25         Pop Label  192.168.130.208/29  0             Gi6/0      10.0.0.6
26         Pop Label  192.168.130.192/28  0             Gi6/0      10.0.0.6
27         Pop Label  192.168.130.160/27  0             Gi6/0      10.0.0.6
28         Pop Label  192.168.130.128/27  0             Gi6/0      10.0.0.6
29         Pop Label  192.168.130.96/27   0             Gi6/0      10.0.0.6
30         Pop Label  192.168.130.64/27   0             Gi6/0      10.0.0.6
31         Pop Label  192.168.130.0/26    0             Gi6/0      10.0.0.6
32         Pop Label  192.168.121.184/29  0             Gi0/0      10.0.0.2
33         Pop Label  192.168.121.176/29  0             Gi0/0      10.0.0.2
34         Pop Label  192.168.121.160/28  0             Gi0/0      10.0.0.2
35         Pop Label  192.168.121.128/27  0             Gi0/0      10.0.0.2
36         Pop Label  192.168.121.96/27   0             Gi0/0      10.0.0.2
37         Pop Label  192.168.121.64/27   0             Gi0/0      10.0.0.2
38         Pop Label  192.168.121.0/26    0             Gi0/0      10.0.0.2
39         Pop Label  192.168.120.208/29  0             Gi0/0      10.0.0.2
40         Pop Label  192.168.120.192/28  0             Gi0/0      10.0.0.2
41         Pop Label  192.168.120.160/27  0             Gi0/0      10.0.0.2
42         Pop Label  192.168.120.128/27  0             Gi0/0      10.0.0.2
43         Pop Label  192.168.120.96/27   0             Gi0/0      10.0.0.2
44         Pop Label  192.168.120.64/27   0             Gi0/0      10.0.0.2
45         Pop Label  192.168.120.0/26    0             Gi0/0      10.0.0.2
```

Tabla 42: Asignación etiquetas MPLS – Router LPZ

Tabla LFIB – Router CBBA

```
CBBA#show mpls forwarding-table
Local      Outgoing   Prefix              Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id        Switched      interface

16         16         10.10.10.3/32       0             Gi0/0      10.0.0.1
17         Pop Label  10.10.10.1/32       0             Gi0/0      10.0.0.1
18         18         192.168.131.184/29  0             Gi0/0      10.0.0.1
19         19         192.168.131.176/29  0             Gi0/0      10.0.0.1
20         20         192.168.131.160/28  0             Gi0/0      10.0.0.1
21         21         192.168.131.128/27  0             Gi0/0      10.0.0.1
22         22         192.168.131.96/27   0             Gi0/0      10.0.0.1
23         23         192.168.131.64/27   0             Gi0/0      10.0.0.1
24         24         192.168.131.0/26    0             Gi0/0      10.0.0.1
25         25         192.168.130.208/29  0             Gi0/0      10.0.0.1
26         26         192.168.130.192/28  0             Gi0/0      10.0.0.1
27         27         192.168.130.160/27  0             Gi0/0      10.0.0.1
28         28         192.168.130.128/27  0             Gi0/0      10.0.0.1
29         29         192.168.130.96/27   0             Gi0/0      10.0.0.1
30         30         192.168.130.64/27   0             Gi0/0      10.0.0.1
31         31         192.168.130.0/26    0             Gi0/0      10.0.0.1
32         Pop Label  192.168.113.40/30   0             Gi0/0      10.0.0.1
33         Pop Label  192.168.113.32/29   0             Gi0/0      10.0.0.1
34         Pop Label  192.168.113.0/27    0             Gi0/0      10.0.0.1
35         Pop Label  192.168.112.64/29   0             Gi0/0      10.0.0.1
36         Pop Label  192.168.112.0/26    0             Gi0/0      10.0.0.1
37         Pop Label  192.168.111.192/29  0             Gi0/0      10.0.0.1
38         Pop Label  192.168.111.160/27  0             Gi0/0      10.0.0.1
39         Pop Label  192.168.111.128/27  0             Gi0/0      10.0.0.1
40         Pop Label  192.168.111.96/27   0             Gi0/0      10.0.0.1
41         Pop Label  192.168.111.64/27   0             Gi0/0      10.0.0.1
42         Pop Label  192.168.111.0/26    0             Gi0/0      10.0.0.1
```

43	Pop Label	192.168.110.224/29	0	Gi0/0	10.0.0.1
44	Pop Label	192.168.110.192/27	0	Gi0/0	10.0.0.1
45	Pop Label	192.168.110.160/27	0	Gi0/0	10.0.0.1
46	Pop Label	192.168.110.128/27	0	Gi0/0	10.0.0.1
47	Pop Label	192.168.110.96/27	0	Gi0/0	10.0.0.1
48	Pop Label	192.168.110.64/27	0	Gi0/0	10.0.0.1
49	Pop Label	192.168.110.0/26	0	Gi0/0	10.0.0.1
50	Pop Label	10.0.0.4/30	0	Gi0/0	10.0.0.1

Tabla 43: Asignación etiquetas MPLS – Router CBBA

Tabla LFIB - Router SCZ

SCZ#show mpls forwarding-table

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
16	17	10.10.10.2/32	0	Gi0/0	10.0.0.5
17	Pop Label	10.10.10.1/32	0	Gi0/0	10.0.0.5
18	32	192.168.121.184/29	0	Gi0/0	10.0.0.5
19	33	192.168.121.176/29	0	Gi0/0	10.0.0.5
20	34	192.168.121.160/28	0	Gi0/0	10.0.0.5
21	35	192.168.121.128/27	0	Gi0/0	10.0.0.5
22	36	192.168.121.96/27	0	Gi0/0	10.0.0.5
23	37	192.168.121.64/27	0	Gi0/0	10.0.0.5
24	38	192.168.121.0/26	0	Gi0/0	10.0.0.5
25	39	192.168.120.208/29	0	Gi0/0	10.0.0.5
26	40	192.168.120.192/28	0	Gi0/0	10.0.0.5
27	41	192.168.120.160/27	0	Gi0/0	10.0.0.5
28	42	192.168.120.128/27	0	Gi0/0	10.0.0.5
29	43	192.168.120.96/27	0	Gi0/0	10.0.0.5
30	44	192.168.120.64/27	0	Gi0/0	10.0.0.5
31	45	192.168.120.0/26	0	Gi0/0	10.0.0.5
32	Pop Label	192.168.113.40/30	0	Gi0/0	10.0.0.5
33	Pop Label	192.168.113.32/29	0	Gi0/0	10.0.0.5
34	Pop Label	192.168.113.0/27	0	Gi0/0	10.0.0.5
35	Pop Label	192.168.112.64/29	0	Gi0/0	10.0.0.5
36	Pop Label	192.168.112.0/26	0	Gi0/0	10.0.0.5
37	Pop Label	192.168.111.192/29	0	Gi0/0	10.0.0.5
38	Pop Label	192.168.111.160/27	0	Gi0/0	10.0.0.5
39	Pop Label	192.168.111.128/27	0	Gi0/0	10.0.0.5
40	Pop Label	192.168.111.96/27	0	Gi0/0	10.0.0.5
41	Pop Label	192.168.111.64/27	0	Gi0/0	10.0.0.5
42	Pop Label	192.168.111.0/26	0	Gi0/0	10.0.0.5
43	Pop Label	192.168.110.224/29	0	Gi0/0	10.0.0.5
44	Pop Label	192.168.110.192/27	0	Gi0/0	10.0.0.5
45	Pop Label	192.168.110.160/27	0	Gi0/0	10.0.0.5
46	Pop Label	192.168.110.128/27	0	Gi0/0	10.0.0.5
47	Pop Label	192.168.110.96/27	0	Gi0/0	10.0.0.5
48	Pop Label	192.168.110.64/27	0	Gi0/0	10.0.0.5
49	Pop Label	192.168.110.0/26	0	Gi0/0	10.0.0.5
50	Pop Label	10.0.0.0/30	0	Gi0/0	10.0.0.5

Tabla 44: Asignación etiquetas MPLS – Router SCZ

Cabe aclarar que los valores de las etiquetas que asigna cada router, pueden ser distintas, ya que estas se generan de forma aleatoria.

Como se observa en las tablas 42, 43 y 44, no aparecen las etiquetas asignadas a las direcciones de red IPv6, ya que como se mencionó anteriormente, estas no se anuncian de forma nativa a través del protocolo LDP, sino mediante el protocolo BGP, como se muestra a continuación:

Router LPZ:

```
LPZ#show bgp ipv6 unicast nexthops

 # Paths   Nexthop Address
       1   2001:DB8:ACEF:F000::2
      14   ::FFFF:10.10.10.2
      14   ::FFFF:10.10.10.3

LPZ#show bgp ipv6 unicast summary

BGP router identifier 10.10.10.1, local AS number 100
48 network entries using 8064 bytes of memory
48 path entries using 4992 bytes of memory
```

```
LPZ#show bgp ipv6 unicast labels
   Network                    Next Hop                   In label/Out label
   ::/0                       2001:DB8:ACEF:F000::2      46/nolabel
   2001:DB8:ACEF:10::/64      ::FFFF:10.10.10.2          nolabel/51
   2001:DB8:ACEF:11::/64      ::FFFF:10.10.10.2          nolabel/52
   2001:DB8:ACEF:12::/64      ::FFFF:10.10.10.2          nolabel/53
   2001:DB8:ACEF:13::/64      ::FFFF:10.10.10.2          nolabel/54
   2001:DB8:ACEF:14::/64      ::FFFF:10.10.10.2          nolabel/55
   2001:DB8:ACEF:15::/64      ::FFFF:10.10.10.2          nolabel/56
   2001:DB8:ACEF:16::/64      ::FFFF:10.10.10.2          nolabel/57
   2001:DB8:ACEF:17::/64      ::FFFF:10.10.10.2          nolabel/58
   2001:DB8:ACEF:18::/64      ::FFFF:10.10.10.2          nolabel/59
   2001:DB8:ACEF:19::/64      ::FFFF:10.10.10.2          nolabel/60
   2001:DB8:ACEF:1A::/64      ::FFFF:10.10.10.2          nolabel/61
   2001:DB8:ACEF:1B::/64      ::FFFF:10.10.10.2          nolabel/62
   2001:DB8:ACEF:20::/64      ::FFFF:10.10.10.3          nolabel/51
   2001:DB8:ACEF:21::/64      ::FFFF:10.10.10.3          nolabel/52
   2001:DB8:ACEF:22::/64      ::FFFF:10.10.10.3          nolabel/53
   2001:DB8:ACEF:23::/64      ::FFFF:10.10.10.3          nolabel/54
   2001:DB8:ACEF:24::/64      ::FFFF:10.10.10.3          nolabel/55
   2001:DB8:ACEF:25::/64      ::FFFF:10.10.10.3          nolabel/56
   2001:DB8:ACEF:26::/64      ::FFFF:10.10.10.3          nolabel/57
   2001:DB8:ACEF:27::/64      ::FFFF:10.10.10.3          nolabel/58
   2001:DB8:ACEF:28::/64      ::FFFF:10.10.10.3          nolabel/59
   2001:DB8:ACEF:29::/64      ::FFFF:10.10.10.3          nolabel/60
   2001:DB8:ACEF:2A::/64      ::FFFF:10.10.10.3          nolabel/61
   2001:DB8:ACEF:2B::/64      ::FFFF:10.10.10.3          nolabel/62
   2001:DB8:ACEF:205::/64     ::FFFF:10.10.10.2          nolabel/63
   2001:DB8:ACEF:206::/64     ::FFFF:10.10.10.2          nolabel/64
   2001:DB8:ACEF:207::/64     ::FFFF:10.10.10.3          nolabel/63
   2001:DB8:ACEF:208::/64     ::FFFF:10.10.10.3          nolabel/64
```

Router CBBA:

```
CBBA#show bgp ipv6 unicast nexthops

 # Paths   Nexthop Address
      20   ::FFFF:10.10.10.1
      14   ::FFFF:10.10.10.3

CBBA#show bgp ipv6 unicast summary

BGP router identifier 10.10.10.2, local AS number 100
48 network entries using 8064 bytes of memory
48 path entries using 4992 bytes of memory
```

```
CBBA#show bgp ipv6 unicast labels
   Network                    Next Hop                   In label/Out label
   ::/0                       ::FFFF:10.10.10.1          nolabel/46
   2001:DB8:ACEF::/64         ::FFFF:10.10.10.1          nolabel/47
   2001:DB8:ACEF:1::/64       ::FFFF:10.10.10.1          nolabel/48
   2001:DB8:ACEF:2::/64       ::FFFF:10.10.10.1          nolabel/49
   2001:DB8:ACEF:3::/64       ::FFFF:10.10.10.1          nolabel/50
   2001:DB8:ACEF:4::/64       ::FFFF:10.10.10.1          nolabel/51
   2001:DB8:ACEF:5::/64       ::FFFF:10.10.10.1          nolabel/52
   2001:DB8:ACEF:6::/64       ::FFFF:10.10.10.1          nolabel/53
   2001:DB8:ACEF:7::/64       ::FFFF:10.10.10.1          nolabel/54
   2001:DB8:ACEF:8::/64       ::FFFF:10.10.10.1          nolabel/55
```

```
   2001:DB8:ACEF:9::/64         ::FFFF:10.10.10.1              nolabel/56
   2001:DB8:ACEF:A::/64         ::FFFF:10.10.10.1              nolabel/57
   2001:DB8:ACEF:B::/64         ::FFFF:10.10.10.1              nolabel/58
   2001:DB8:ACEF:C::/64         ::FFFF:10.10.10.1              nolabel/59
   2001:DB8:ACEF:D::/64         ::FFFF:10.10.10.1              nolabel/60
   2001:DB8:ACEF:20::/64        ::FFFF:10.10.10.3              nolabel/51
   2001:DB8:ACEF:21::/64        ::FFFF:10.10.10.3              nolabel/52
   2001:DB8:ACEF:22::/64        ::FFFF:10.10.10.3              nolabel/53
   2001:DB8:ACEF:23::/64        ::FFFF:10.10.10.3              nolabel/54
   2001:DB8:ACEF:24::/64        ::FFFF:10.10.10.3              nolabel/55
   2001:DB8:ACEF:25::/64        ::FFFF:10.10.10.3              nolabel/56
   2001:DB8:ACEF:26::/64        ::FFFF:10.10.10.3              nolabel/57
   2001:DB8:ACEF:27::/64        ::FFFF:10.10.10.3              nolabel/58
   2001:DB8:ACEF:28::/64        ::FFFF:10.10.10.3              nolabel/59
   2001:DB8:ACEF:29::/64        ::FFFF:10.10.10.3              nolabel/60
   2001:DB8:ACEF:2A::/64        ::FFFF:10.10.10.3              nolabel/61
   2001:DB8:ACEF:2B::/64        ::FFFF:10.10.10.3              nolabel/62
   2001:DB8:ACEF:200::/64       ::FFFF:10.10.10.1              nolabel/61
   2001:DB8:ACEF:201::/64       ::FFFF:10.10.10.1              nolabel/62
   2001:DB8:ACEF:202::/64       ::FFFF:10.10.10.1              nolabel/63
   2001:DB8:ACEF:203::/64       ::FFFF:10.10.10.1              nolabel/64
   2001:DB8:ACEF:207::/64       ::FFFF:10.10.10.3              nolabel/63
   2001:DB8:ACEF:208::/64       ::FFFF:10.10.10.3              nolabel/64
   2001:DB8:ACEF:F000::/64      ::FFFF:10.10.10.1              nolabel/65
```

Router SCZ:

```
SCZ#show bgp ipv6 unicast nexthops

 # Paths   Nexthop Address
      20   ::FFFF:10.10.10.1
      14   ::FFFF:10.10.10.2
```

```
SCZ#show bgp ipv6 unicast summary

BGP router identifier 10.10.10.3, local AS number 100
48 network entries using 8064 bytes of memory
48 path entries using 4992 bytes of memory
```

```
SCZ#show bgp ipv6 unicast labels
   Network                      Next Hop                       In label/Out label
   ::/0                         ::FFFF:10.10.10.1              nolabel/46
   2001:DB8:ACEF::/64           ::FFFF:10.10.10.1              nolabel/47
   2001:DB8:ACEF:1::/64         ::FFFF:10.10.10.1              nolabel/48
   2001:DB8:ACEF:2::/64         ::FFFF:10.10.10.1              nolabel/49
   2001:DB8:ACEF:3::/64         ::FFFF:10.10.10.1              nolabel/50
   2001:DB8:ACEF:4::/64         ::FFFF:10.10.10.1              nolabel/51
   2001:DB8:ACEF:5::/64         ::FFFF:10.10.10.1              nolabel/52
   2001:DB8:ACEF:6::/64         ::FFFF:10.10.10.1              nolabel/53
   2001:DB8:ACEF:7::/64         ::FFFF:10.10.10.1              nolabel/54
   2001:DB8:ACEF:8::/64         ::FFFF:10.10.10.1              nolabel/55
   2001:DB8:ACEF:9::/64         ::FFFF:10.10.10.1              nolabel/56
   2001:DB8:ACEF:A::/64         ::FFFF:10.10.10.1              nolabel/57
   2001:DB8:ACEF:B::/64         ::FFFF:10.10.10.1              nolabel/58
   2001:DB8:ACEF:C::/64         ::FFFF:10.10.10.1              nolabel/59
   2001:DB8:ACEF:D::/64         ::FFFF:10.10.10.1              nolabel/60
   2001:DB8:ACEF:10::/64        ::FFFF:10.10.10.2              nolabel/51
   2001:DB8:ACEF:11::/64        ::FFFF:10.10.10.2              nolabel/52
   2001:DB8:ACEF:12::/64        ::FFFF:10.10.10.2              nolabel/53
   2001:DB8:ACEF:13::/64        ::FFFF:10.10.10.2              nolabel/54
   2001:DB8:ACEF:14::/64        ::FFFF:10.10.10.2              nolabel/55
   2001:DB8:ACEF:15::/64        ::FFFF:10.10.10.2              nolabel/56
   2001:DB8:ACEF:16::/64        ::FFFF:10.10.10.2              nolabel/57
   2001:DB8:ACEF:17::/64        ::FFFF:10.10.10.2              nolabel/58
   2001:DB8:ACEF:18::/64        ::FFFF:10.10.10.2              nolabel/59
   2001:DB8:ACEF:19::/64        ::FFFF:10.10.10.2              nolabel/60
   2001:DB8:ACEF:1A::/64        ::FFFF:10.10.10.2              nolabel/61
   2001:DB8:ACEF:1B::/64        ::FFFF:10.10.10.2              nolabel/62
   2001:DB8:ACEF:200::/64       ::FFFF:10.10.10.1              nolabel/61
   2001:DB8:ACEF:201::/64       ::FFFF:10.10.10.1              nolabel/62
   2001:DB8:ACEF:202::/64       ::FFFF:10.10.10.1              nolabel/63
   2001:DB8:ACEF:203::/64       ::FFFF:10.10.10.1              nolabel/64
   2001:DB8:ACEF:205::/64       ::FFFF:10.10.10.2              nolabel/63
   2001:DB8:ACEF:206::/64       ::FFFF:10.10.10.2              nolabel/64
   2001:DB8:ACEF:F000::/64      ::FFFF:10.10.10.1              nolabel/65
```

La notación ***::FFFF***: indica que es una dirección IPv4 mapeada a IPv6 (debido a que el núcleo de la red está configurada sobre IPv4).

Por otra parte, se puede observar que cada router, tiene conocimiento de las 48 direcciones IPv6 presentes en la red, las cuales son anunciadas y almacenadas en cada uno de los mismos.

Verificación y análisis de pruebas de MPLS:

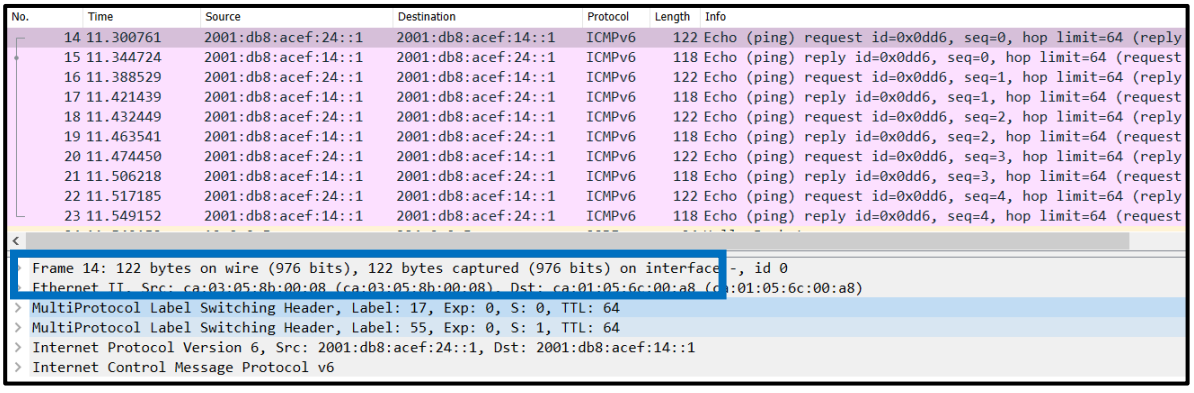
Si una red LAN de SCZ se quiere comunicar con una red LAN de CBBA, ejemplo el área de Marketing de CBBA (2001:db8:acef:14::1/64), las etiquetas MPLS que se colocaran al paquete, serán las siguientes:

```
SCZ#show ipv6 cef 2001:db8:acef:14::1
2001:DB8:ACEF:14::/64
  nexthop 10.0.0.5 GigabitEthernet0/0 label 17 55
```

```
SCZ#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing    Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         17         10.10.10.2/32    0             Gi0/0       10.0.0.5
```

```
SCZ#show bgp ipv6 unicast labels
   Network                 Next Hop              In label/Out label
   2001:DB8:ACEF:14::/64   ::FFFF:10.10.10.2     nolabel/55
```

```
SCZ#ping 2001:db8:acef:14::1 source 2001:db8:acef:24::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACEF:14::1, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:ACEF:24::1
!!!!!
```

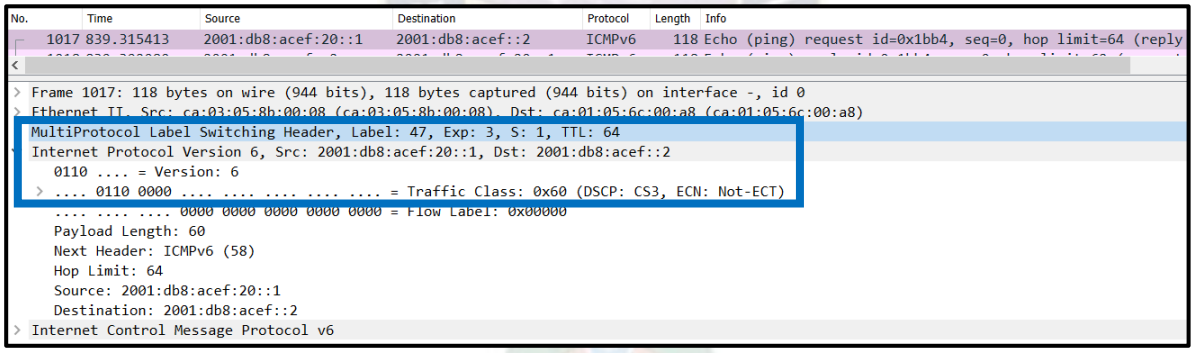


Como se observa la etiqueta superior tiene el valor de ***17***, la cual corresponde al router de siguiente salto (LPZ); la segunda etiqueta tiene el valor ***55***, la cual corresponde a la etiqueta asociada a la red LAN (2001:db8:acef:14::/64) y además el bit de BoS es igual a 1, lo que significa que esta es la última etiqueta.

Verificación y análisis de pruebas de las políticas de QoS:

Se emitirá un ping, con el campo de Clase de Tráfico (Cabecera - IPv6) modificado a un valor de CS3, desde una LAN de SCZ hasta una LAN de LPZ.

```
SCZ#ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:acef::2
Repeat count [5]: 25
Source address or interface: 2001:db8:acef:20::1
Precedence [0]: 3
Type escape sequence to abort.
Sending 25, 100-byte ICMP Echos to 2001:DB8:ACEF::2, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:ACEF:20::1
!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (25/25), round-trip min/avg/max = 24/29/72 ms
```




```
SCZ#show policy-map interface gigabitEthernet 0/0
    Class-map: CS3 (match-any)
      25 packets, 2950 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: mpls experimental topmost 3
        25 packets, 2950 bytes
        5 minute rate 0 bps
      Match:  dscp cs3 (24)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue limit 400 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 25/2950
      bandwidth 12% (120000 kbps)
```

```
LPZ#show policy-map interface gigabitEthernet 6/0
    Class-map: CS3 (match-any)
      25 packets, 2950 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: mpls experimental topmost 3
        25 packets, 2950 bytes
        5 minute rate 0 bps
      Match:  dscp cs3 (24)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
      queue limit 400 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 25/2950
      bandwidth 12% (120000 kbps)
```

Como se observa en los resultados, la política de QoS aplicada a las interfaces de salida de los routers funciona de acuerdo al diseño propuesto, ambos routers identifican correctamente la clase de servicio CS3 de los paquetes enviados y los clasifican en la clase de política respectiva.

Verificación y análisis de pruebas de denegación del protocolo Telnet:

- ✓ Intento de conexión desde la red de Internet:

```
DNS6#telnet 2001:db8:acef::1
Trying 2001:DB8:ACEF::1 ...
% Destination unreachable; gateway or host down
```

Source	Destination	Protocol	Length	Info
fe80::8888	fe80::1	ICMPv6	86	Neighbor Solicitation for fe80::1 from ca:0c:06:13:00:08
fe80::1	fe80::8888	ICMPv6	78	Neighbor Advertisement fe80::1 (rtr, sol)
ca:0c:06:13:00:08	ca:0c:06:13:00:08	LOOP	60	Reply
ca:01:05:6c:00:8c	ca:01:05:6c:00:8c	LOOP	60	Reply
fe80::8888	ff02::1	ICMPv6	118	Router Advertisement from ca:0c:06:13:00:08
fe80::1	ff02::1	ICMPv6	118	Router Advertisement from ca:01:05:6c:00:8c
2001:4860:4860::8888	2001:db8:acef::1	TCP	78	34740 → 23 [SYN] Seq=0 Win=4128 Len=0 MSS=516
2001:db8:acef:f000::1	2001:4860:4860::8888	ICMPv6	126	Destination Unreachable (Administratively prohibited)

- ✓ Intento de conexión desde un host en la red de la empresa:

```
C:\Users\Cristian>telnet 2001:db8:acef:20::1
Connecting To 2001:db8:acef:20::1...Could not open connection to the host, on port 23: Connect failed
```

Source	Destination	Protocol	Length	Info
2001:db8:acef:200::1	2001:db8:acef:200::3	ICMPv6	86	Neighbor Advertisement 2001:db8:acef:200::1 (rtr, sol, ov
2001:db8:acef:200::3	2001:db8:acef:20::1	TCP	94	35446 → 23 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 SACK_PERM
fe80::de71:2752:c9b3:…	ff02::1:ff00:0	ICMPv6	86	Neighbor Solicitation for :: from 00:0c:29:31:78:a2
2001:db8:acef:200::1	2001:db8:acef:200::3	ICMPv6	142	Destination Unreachable (Administratively prohibited)

Se puede verificar que en ambos intentos de conexión (mediante el protocolo Telnet), se prohibe el alcanze de la conexión al destino cuyo puerto sea 23.

Verificación y análisis de pruebas de denegación del protocolo SSH:

- ✓ Conexión desde la red de Internet:

```
DNS6#ssh -l router_LPZ 2001:db8:acef::1
Password:
LPZ#exit

[Connection to 2001:db8:acef::1 closed by foreign host]
```

Source	Destination	Protocol	Length	Info
2001:4860:4860::8888	2001:db8:acef::1	TCP	78	29916 → 22 [SYN] Seq=0 Win=4128 Len=0 MSS=516
2001:db8:acef::1	2001:4860:4860::8888	TCP	78	22 → 29916 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=51

- ✓ Conexión desde un host de la red de la empresa:

```
C:\Users\Cristian>ssh -c aes256-cbc router_LPZ@10.10.10.1
Password:
LPZ#exit
Connection to 10.10.10.1 closed by remote host.
Connection to 10.10.10.1 closed.
```

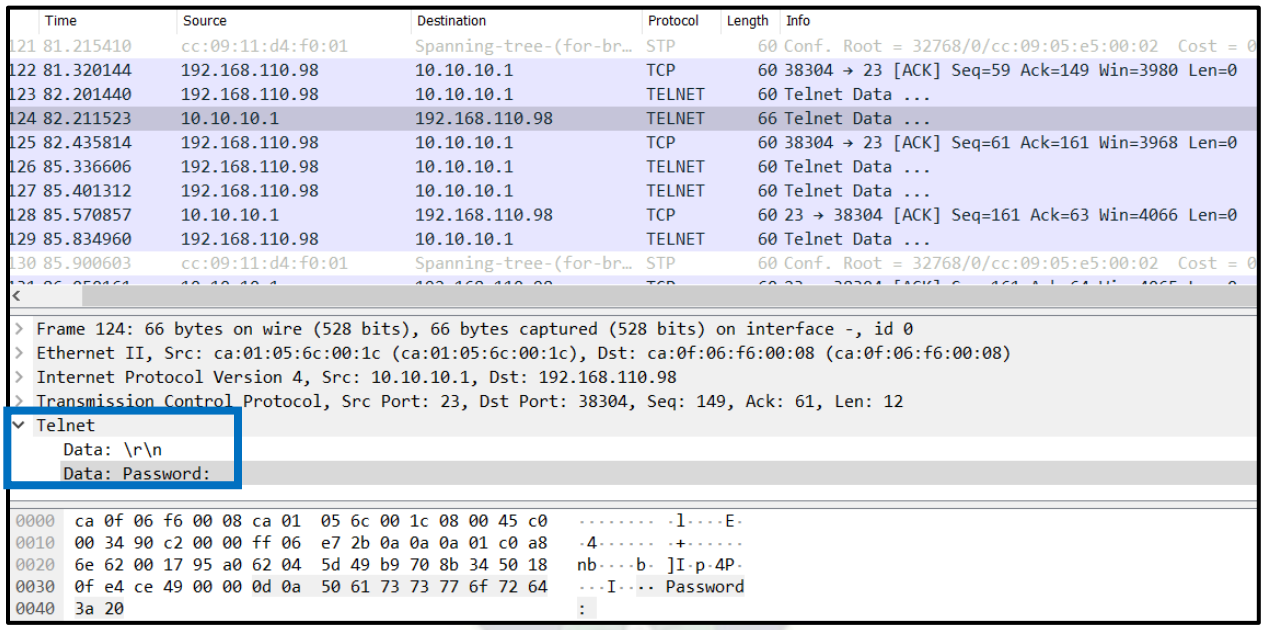
Source	Destination	Protocol	Length	Info
192.168.113.35	10.10.10.1	TCP	74	45420 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
10.10.10.1	192.168.113.35	TCP	64	22 → 45420 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460

Se puede verificar que en ambos intentos de conexión (mediante el protocolo SSH), esta resulta exitosa; ademas cabe aclarar que para establecer conexión con el destino se necesita conocer el ***nombre de usuario*** y ***contrasena*** del mismo.

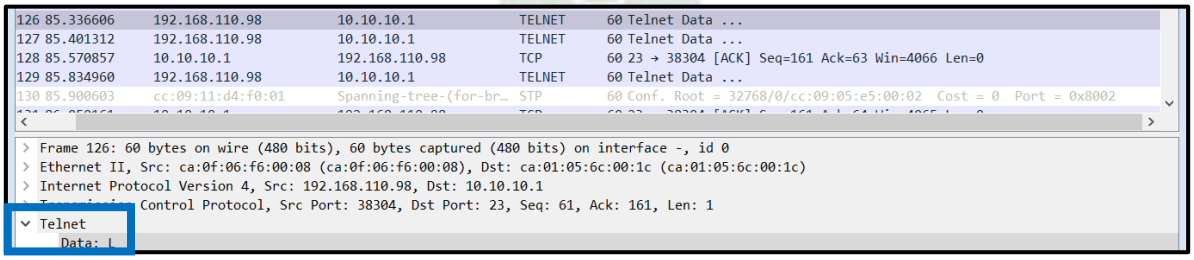
El principal beneficio que ofrece SSH respecto a Telnet es que la informacion que se transmite entre cliente – servidor va encriptada, por lo que imposibilita que terceros extraigan informacion; lo contrario pasa con Telnet, ya que con ayuda de un capturador de tráfico (como Wireshark) se puede obtener nombres de usuario, contrasenas, etc., como se muestra a continuacion:

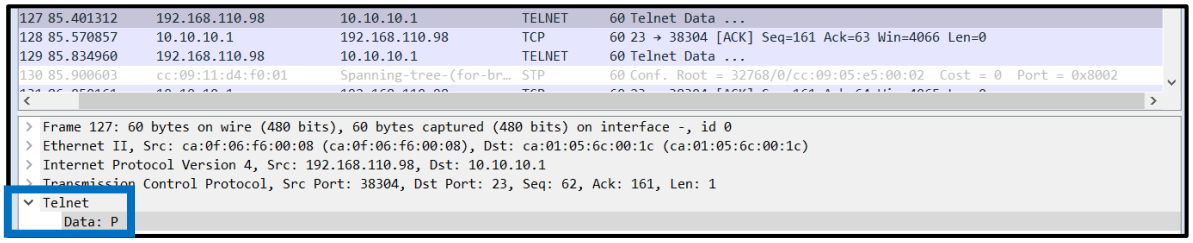
```
Host_LPZ#telnet 10.10.10.1
Trying 10.10.10.1 ... Open

User Access Verification
Username: router_LPZ
Password:
```

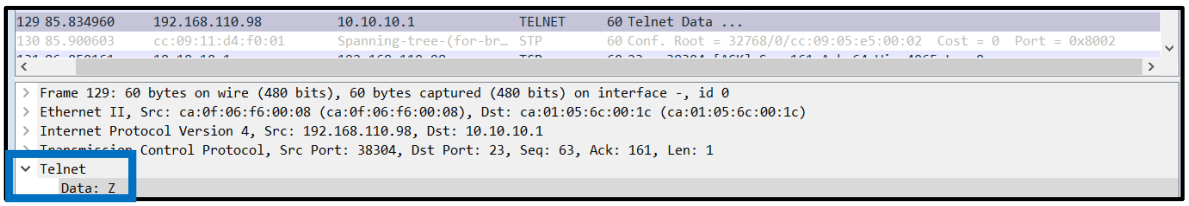
Texto ***Password:*** visible:



Contraseña ***LPZ_1111*** visible para la conexión remota con el ***router_LPZ***:







Claramente se puede observar que toda la información que se transmite, es visible, por lo que uno podría extraer fácilmente datos confidenciales que se estuvieran transmitiendo.

CAPITULO V
ANALISIS ECONOMICO

5.1. Análisis Económico del Proyecto

Cotización de los equipos de la red:

Cantidad	Equipo	Serie	Costo por Unidad	Costo Total
1	Router Cisco ASR-920-12CZ-A	ASR 920	$ 1,884.00	$ 1,884.00
2	Router Cisco ASR-920-4SZ-A	ASR 920	$ 1,289.00	$ 2,578.00
1	Switch Cisco 2960S-24TD-L	2960-S	$ 570.00	$ 570.00
6	Switch Cisco SG220-50P	220	$ 729.00	$ 4,374.00
1	Switch Cisco SG220-26P	220	$ 434.00	$ 434.00
Costo Total de los Equipos				**$ 9,840.00**

Tabla 45: Costo Total – Equipos de Red

Licencias del software de Cisco:

Cantidad	Descripcion	Licencia	Costo por Unidad	Costo Total
3	Cisco IOS Advanced Metro IP Access - License	ASR920-S-A	$ 1,831.00	$ 5,493.00
1	Cisco ASR920 Series - 2 ports 10GE license	ASR920-10G-2	$ 941.00	$ 941.00
Costo Total de las Licencias				**$ 6,434.00**

Tabla 46: Costo Total – Licencias de Software

Módulos SFP / SFP+:

Cantidad	Descripcion	SFP	Costo por Unidad	Costo Total
6	10 GBASE-SR SFP	SFP-10G-SR	$ 30.00	$ 180.00
4	1000BASE-T SFP	SFP-GE-T	$ 24.00	$ 96.00
Costo Total de Modulos SFP/SFP+				**$ 276.00**

Tabla 47: Costo Total – Módulos SFP/SFP+

Licencia de la herramienta de monitoreo PRTG:

Licencia PRTG 500
$1,750

Cotización del sistema de respaldo de energía:

Cantidad	Equipo	Costo por Unidad	Costo Total
1	APC Smart-UPS SRT 3000VA 230V + APC Smart-UPS SRT 96V 3kVA Battery Pack	$ 4,840.00	$ 4,840.00
2	APC Smart-UPS SRT 1500VA 230V + APC Smart-UPS SRT 48V 1kVA 1.5kVA	$ 2,576.00	$ 5,152.00
Costo Total del sistema de Respaldo de Energia			**$ 9,992.00**

Sumando todos los valores de cotización, se tiene el siguiente costo de inversión total:

Costo Total de Inversión
$28,292

Tabla 48: Costo Total de Inversión

Alquiler de servicios de un ISP:

Servicio	AXS	Entel	Tigo
Enlace de Datos 45 Mbps			Bs. 50000
Internet Dedicado 40 Mbps	Bs. 7200	Bs. 3740	Bs. 9300

Respecto al costo de los servicios de VPN de capa 2 e Internet Corporativo, estos son referenciales y obtenidos de la página web de cada proveedor, teniendo así el siguiente costo referencial mensual de alquiler:

Alquiler Mensual de Servicios
Bs. 53,740

Tabla 49: Costo Referencial Mensual – Alquiler de Servicios

Costo del consumo de electricidad de los dispositivos de backbone de la red:

Consumo [Watts]	Equipo	Cantidad en LPZ	Cantidad en CBBA	Cantidad en SCZ
115 W	Router Cisco ASR-920-12CZ-A	1	-	-
115 W	Router Cisco ASR-920-4SZ-A	-	1	1
40 W	Switch Cisco 2960S-24TD-L	1	-	-
375 W	Switch Cisco SG220-50P	2	2	2
180 W	Switch Cisco SG220-26P	1	-	-
Consumo Total [kWh]		781.2 kWh	622.8 kWh	622.8 kWh
Costo por [kWh]		0,73 Bs	1,04 Bs	0,93 Bs
Costo Total [Bs]		**570,28 Bs**	**647,71 Bs**	**579,20 Bs**

Tabla 50: Costo Referencial Mensual – Consumo de Electricidad por sede

5.2. Relación Costo/Beneficio

Es necesario que en todo proyecto se realice el análisis económico, de esta manera podemos determinar la rentabilidad y la factibilidad del mismo; en este sentido se hará la comparación especifica de costos, entre el diseño de una red corporativa implementando su propia Red IP MPLS, con un diseño alternativo en el que se alquile una Red de Transmisión de Datos + Red IP MPLS que puede otorgar un ISP.

El análisis económico se lo realizara en base a los costos de los servicios que ofrece la empresa Tigo, debido a que estos se pueden verificar entrando a su sitio web: www.tigo.com.bo.

El servicio de VPN - MPLS Nacional que ofrece la empresa Tigo tiene como máximo 15 Mbps de ancho de banda, razón por la cual el análisis se lo hará en base a este ancho de banda.

Alquiler de la Red de Transporte de Datos, para una red corporativa con su propia Red IP MPLS:

ISP - Tigo			
Servicio	**Costo Mensual**	**Periodo de Alquiler**	**Costo Anual**
Enlace de Datos 15 Mbps	Bs. 20,225	12 Meses	**Bs. 242,700**

Alquiler de la Red de Transmisión de Datos + Red IP MPLS del ISP:

ISP - Tigo			
Servicio	**Costo Mensual**	**Periodo de Alquiler**	**Costo Anual**
Enlace de Datos + MPLS 15 Mbps	Bs. 61,420	12 Meses	**Bs. 737,040**

Si se realiza una comparación de los flujos de caja entre los dos servicios que ofrece el ISP, se observa claramente la diferencia de costos, y el beneficio a la empresa en el sentido de minimizar gastos, en la implementación de una red corporativa que cuente con una Red IP MPLS, justificándose de esa manera el diseño del presente proyecto, además de las ventajas, como la configuración de QoS, ancho de Banda, control de tráfico, entre otras, que el o los administradores de la empresa pueden configurar en la red, de acuerdo a las necesidades que esta tuviera.

5.3. Comparación de costos con diferentes marcas de los equipos que conforman la red

Evaluación del proyecto con equipos de la marca Mikrotik:

	Cisco	**Mikrotik**
Caracteristicas	**ASR-920-12CZ-A**	**CCR1036-8G-2S+EM**
Sistema Operativo	Cisco IOS XE	RouterOS
Procesador	Dual Core - 1 Ghz	36 cores - 1.2 Ghz
Memoria DRAM	4 Gb	8 Gb
Capacidad	64 Gbps	28 Gbps
Puertos	12-1GE, 2-10GE(SFP+)	8-1GE, 2-10GE(SFP+)
Costo	**$ 1884**	**$ 1295**

	Cisco	Mikrotik
Caracteristicas	**ASR-920-4SZ-A**	**CCR1036-8G-2S+**
Sistema Operativo	Cisco IOS XE	RouterOS
Procesador	Dual Core - 1 Ghz	36 cores - 1.2 Ghz
Memoria DRAM	4 Gb	4 Gb
Capacidad	64 Gbps	28 Gbps
Puertos	2-1GE, 4-10GE(SFP+)	8-1GE, 2-10GE(SFP+)
Costo	**$ 1289**	**$ 1095**

	Cisco	Mikrotik
Caracteristicas	**SG220-26P**	**CRS328-24P-4S+RM**
Memoria RAM	128 MB	512 MB
Memoria Flash	32 MB	16 MB
Puertos PoE	24 puertos	24 puertos
Capacidad	52 Gbps	128 Gbps
Puertos	24-1GE, 2-1GE(SFP)	24-1GE, 4-10GE(SFP+)
Costo	**$ 434**	**$ 379**

	Cisco	Mikrotik
Caracteristicas	**SG220-50P**	**CRS354-48G-4S+2Q+RM**
Memoria RAM	128 MB	64 MB
Memoria Flash	32 MB	16 MB
Puertos PoE	48 puertos	-
Capacidad	100 Gbps	336 Gbps
Puertos	48-1GE, 2-1GE(SFP)	48-1GE, 4-10GE(SFP+)
Costo	**$ 729**	**$ 499**

	Cisco	Mikrotik
Caracteristicas	**2960S-24TD-L**	**CRS326-24S+2Q+RM**
Memoria RAM	128 MB	64 MB
Memoria Flash	32 MB	16 MB
Capacidad	176 Gbps	640 Gbps
Puertos	24-1GE, 2-10GE(SFP+)	24-10GE(SFP+)
Costo	**$ 570**	**$ 499**

Tabla 51: Comparación de costos con la marca Mikrotik

Se tiene un costo de inversión inicial de $ 7,357.00

Flujo de Caja (Ingresos – Egresos) en un periodo de 3 años:

Flujo de Caja	$ 2,483.00	$ 3,103.00	$ 3,258.00

Cálculo del VAN (Valor Actual Neto), asumiendo una tasa de descuento del 3%:

$$VAN = -7357 + \frac{2483}{(1+0.03)^1} + \frac{3103}{(1+0.03)^2} + \frac{3258}{(1+0.03)^3}$$

$$\boxed{VAN = 960.09}$$

Cálculo del TIR (Tasa Interna de Retorno):

$$0 = -7357 + \frac{2483}{(1+k)^1} + \frac{3103}{(1+k)^2} + \frac{3258}{(1+k)^3}$$

$$\boxed{TIR = 9.353\ \%}$$

Evaluación del proyecto con equipos de la marca Huawei:

	Cisco	Huawei
Caracteristicas	**SG220-26P**	**S1730S-S24P4S-A**
Memoria RAM	128 MB	1024 MB
Memoria Flash	32 MB	512 MB
Puertos PoE	24 puertos	24 puertos
Capacidad	52 Gbps	168 Gbps
Puertos	24-1GE, 2-1GE(SFP)	24-1GE, 4-1GE(SFP)
Costo	**$ 434**	**$ 466**

	Cisco	Huawei
Caracteristicas	**SG220-50P**	**S1730S-S48P4S-A**
Memoria RAM	128 MB	1024 MB
Memoria Flash	32 MB	512 MB
Puertos PoE	48 puertos	48 puertos
Capacidad	100 Gbps	216 Gbps
Puertos	48-1GE, 2-1GE(SFP)	48-1GE, 4-1GE(SFP)
Costo	**$ 729**	**$ 353**

	Cisco	Huawei
Caracteristicas	**2960S-24TD-L**	**S1730S-S24T4X-A**
Memoria RAM	128 MB	1024 MB
Memoria Flash	32 MB	512 MB
Capacidad	176 Gbps	168 Gbps
Puertos	24-1GE, 2-10GE(SFP+)	24-10GE, 4-10GE(SFP+)
Costo	**$ 570**	**$ 282**

Tabla 52: Comparación de costos con la marca Huawei

Se tiene un costo de inversión inicial de $ 7,328.00

Flujo de Caja (Ingresos – Egresos) en un periodo de 3 años:

Flujo de Caja	$ 2,512.00	$ 3,140.00	$ 3,297.00

Cálculo del VAN (Valor Actual Neto), asumiendo una tasa de descuento del 3%:

$$VAN = -7328 + \frac{2512}{(1+0.03)^1} + \frac{3140}{(1+0.03)^2} + \frac{3297}{(1+0.03)^3}$$

$$\boxed{VAN = 1087.81}$$

Cálculo del TIR (Tasa Interna de Retorno):

$$0 = -7328 + \frac{2512}{(1+k)^1} + \frac{3140}{(1+k)^2} + \frac{3297}{(1+k)^3}$$

$$\boxed{TIR = 0.102\ \%}$$

En la comparación con equipos de la marca Juniper, sus productos (Routers y Switches) presentan especificaciones que sobrepasan las requeridas al diseño del proyecto, lo que resulta en un costo elevado de estos equipos, por lo que se descarta la comparación de algún equipo de la marca Juniper.

De acuerdo a las especificaciones, costos y la disponibilidad de estos equipos de red, se tiene la siguiente elección de dispositivos, que satisfacen los requerimientos del presente proyecto:

Equipo	Marca	Modelo
Router de borde WAN	Cisco	ASR-920-12CZ-A
Routers Sucursales	Cisco	ASR-920-4SZ-A
Switch L2 - 26 Puertos	Mikrotik	CRS328-24P-4S+RM
Switch L2 - 50 Puertos	Mikrotik	CRS354-48G-4S+2Q+RM
Switch - Servidores	Mikrotik	CRS326-24S+2Q+RM

Tabla 53: Elección de equipos de red

Con la elección de estos equipos se tiene un costo de inversión inicial de $ 8,334.00

La elección de usar Routers de la marca Cisco en lugar de los de la marca Mikrotik, es debido a que estos últimos disponen solamente de una capacidad de hasta 28 Gbps comparados a los 64 Gbps del Router Cisco, por lo que ante un crecimiento de personal y/o servicios nuevos en la Empresa, implicaría un aumento en el procesamiento de paquetes y en el uso del ancho de banda, teniendo que realizar la compra de otro equipo de red para satisfacer esas necesidades.

Flujo de Caja en un periodo de 3 años:

Flujo de Caja	$ 1,506.00	$ 2,801.00	$ 5,391.00

Cálculo del VAN (Valor Actual Neto), asumiendo una tasa de descuento del 3%:

$$VAN = -8334 + \frac{1506}{(1+0.03)^1} + \frac{2801}{(1+0.03)^2} + \frac{5391}{(1+0.03)^3}$$

$$\boxed{VAN = 701.88}$$

Cálculo del TIR (Tasa Interna de Retorno):

$$0 = -8334 + \frac{1506}{(1+k)^1} + \frac{2801}{(1+k)^2} + \frac{5391}{(1+k)^3}$$

$$\boxed{TIR = 6.57\ \%}$$

En base a los resultados obtenidos: TIR superior a la tasa de descuento y el VAN mayor que cero, indicando que los beneficios superan a los costos se puede aceptar la elección de equipos realizada.

CAPITULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

La tecnología MPLS permite que proveedores de servicio o como en este caso empresas corporativas, incrementen la fiabilidad y confianza en sus redes, además de beneficiarse de una reducción en los tiempos de transmisión de información.

Se diseñó y simuló una Red Corporativa MPLS WAN/LAN jerárquica, de alta confiabilidad, escalable y rápida convergencia que permite transmitir varios tipos de servicios; esta fragmentación en capas independientes permitirá modificar partes de la red (agregar nuevos servicios y/o dispositivos), sin realizar importantes actualizaciones en hardware, sino en software (compra de licencias adicionales) para activar los nuevos servicios requeridos por la empresa.

Se realizo un análisis de los distintos tipos de clases de tráfico que pueden cursar la red, de tal manera de conocer los requerimientos de anchos de banda requeridos por cada uno de los mismos, logrando así determinar la capacidad necesaria de los servicios a ser alquilados a un Proveedor de Servicios para la Red de Transmisión de Datos y la conexión a la red de Internet de la Empresa.

Se implementó un modelo de QoS de servicios diferenciados (DiffServ) para evitar posibles congestiones en la red, priorizando el tráfico en tiempo real (sensible a retardos) como son la voz y video, garantizando la calidad de servicio en la red corporativa.

Al soportar varios protocolos entre ellos IPv4 e IPv6, la implementación de MPLS en el backbone de la red corporativa, permite la coexistencia de ambos protocolos de red: IPv4 e IPv6 (Dual - Stack), por lo que la empresa podrá conectarse tanto a dispositivos, páginas web, servidores, etc., con direcciones de red IPv4 como aquellos con direcciones de red IPv6, hasta que la migración total de la red de Internet a IPv6 se haya completado.

Hoy en día es muy importante establecer todo tipo de conexiones a través de protocolos seguros y cifrados para evitar que terceros intercepten la información, por lo que se implementó listas de acceso para denegar el tráfico del protocolo de Telnet, ya que este protocolo establece comunicaciones sin cifrar (como se verificó en las pruebas realizadas), por lo que su uso expondría a la red ante posibles ataques. Es así que se configuró el protocolo SSH en los dispositivos que conforman la red, para de esta forma se tenga conexiones remotas seguras y cifradas, interna o externamente a la Red Corporativa.

6.2. Recomendaciones

El análisis previo a la implementación de una red MPLS, la escalabilidad, jerarquía, calidad de servicio, seguridad son características importantes a ser consideradas dentro del diseño de una red.

El tipo de equipamiento que se elegirá en una red MPLS debe ser evaluado y se debe considerar que cumpla con las características tanto en hardware como en software para la implementación de la arquitectura de red.

Calculado de ancho de banda teórico necesario para la red, es recomendable realizar una medición de tráfico por cada sucursal de la empresa, para realizar la corrección necesaria de la capacidad del enlace contratado. Por lo que sería recomendable sobredimensionar los enlaces contratados, con la desventaja de incurrir en gastos adicionales.

BIBLIOGRAFIA

[1] Luc De Ghein, CCIE No. 1897, “MPLS Fundamentals”, 1 edition, Cisco Press, 2006

[2] Cisco, “MPLS WAN Technology Design Guide”, 2014

[3] Santiago Alvarez, CCIE No. 3621, “QoS for IP/MPLS Networks”, Cisco Press, 2006

[4] Tim Szigeti, CCIE No. 9794; Robert Barton, CCIE No. 6660; Christina Hattingh, Kenneth; Briley, Jr., CCIE No. 9754, “End-to-End QoS Network Design”, second edition, Cisco Press, 2013

[5] Wendell Odom, CCIE No. 1624, “CCNA 200-301 Volume 1 Official Cert Guide”, Cisco Press, 2020

[6] Wendell Odom, CCIE No. 1624, “CCNA 200-301 Volume 2 Official Cert Guide”, Cisco Press, 2020

[7] Ing. José Campero, “Multiprotocol Label Switching (MPLS)”, Seminario de Telecomunicaciones ETN – 1024

[8] Cisco Network Academy, “Necesidad de utilizar IPv6”, CCNAv6

[9] Ronny Omar Cruz Granja, “Despliegue de IPv6 en un backbone MPLS/IPv4 para un Proveedor de Servicios”, Escuela Superior Politécnica del Litoral (ESPOL), 2015

[10] Ing. Dulce María Vélez Vera, “DISEÑO Y SIMULACION EN GNS3 DE UNA RED MULTISERVICIOS MPLS PARA MEDIANAS EMPRESAS EN EL ECUADOR”, Universidad Católica de Santiago de Guayaquil, 2018

[11] https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/ 10103-dscpvalues.html, Cisco, “Implementing Quality of Service Policies with DSCP”, 2008

ANEXOS

Anexo 1: Asignación de direcciones de red en los Routers y Switches

Asignación de direcciones de red en el Router LPZ

Comando	Funcion
no shutdown	Habilitar Interfaz
ip cef	Optimiza el rendimiento y escalabilidad de la red IPv4
ipv6 cef	Optimiza el rendimiento y escalabilidad de la red IPv6
ip address	Asignar una direccion de red IPv4
ipv6 address	Asignar una direccion de red IPv6
ipv6 unicast-routing	Activar reenvio de trafico IPv6
encapsulation dot1q	Habilitacion de 802.1Q

```
Router>enable
Router#configure terminal
Router(config)#hostname LPZ
LPZ(config)#ip cef
LPZ(config)#ipv6 unicast-routing
LPZ(config)#ipv6 cef
LPZ(config)#no ip domain lookup
LPZ(config)#interface Loopback0
LPZ(config-if)# ip address 10.10.10.1 255.255.255.255
LPZ(config-if)#interface GigabitEthernet0/0
LPZ(config-if)# ip address 10.0.0.1 255.255.255.252
LPZ(config-if)# no shutdown
LPZ(config-if)#interface GigabitEthernet1/0
LPZ(config-if)# no shutdown
LPZ(config-if)#interface GigabitEthernet1/0.10
LPZ(config-subif)# encapsulation dot1Q 10
LPZ(config-subif)# ip address 192.168.110.65 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF::1/64
LPZ(config-subif)#interface GigabitEthernet1/0.20
LPZ(config-subif)# encapsulation dot1Q 20
LPZ(config-subif)# ip address 192.168.110.97 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:6::1/64
LPZ(config-subif)#interface GigabitEthernet1/0.30
LPZ(config-subif)# encapsulation dot1Q 30
LPZ(config-subif)# ip address 192.168.110.129 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:3::1/64
LPZ(config-subif)#interface GigabitEthernet1/0.40
LPZ(config-subif)# encapsulation dot1Q 40
LPZ(config-subif)# ip address 192.168.110.161 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:8::1/64
```

```
LPZ(config-subif)#interface GigabitEthernet1/0.80
LPZ(config-subif)# encapsulation dot1Q 80
LPZ(config-subif)# ip address 192.168.110.193 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:9::1/64
LPZ(config-subif)#interface GigabitEthernet1/0.150
LPZ(config-subif)# encapsulation dot1Q 150
LPZ(config-subif)# ip address 192.168.110.1 255.255.255.192
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:B::1/64
LPZ(config-subif)#interface GigabitEthernet1/0.200
LPZ(config-subif)# encapsulation dot1Q 200 native
LPZ(config-subif)# ip address 192.168.110.225 255.255.255.248
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:201::1/64
LPZ(config-subif)#interface GigabitEthernet2/0
LPZ(config-if)# no shutdown
LPZ(config-if)#interface GigabitEthernet2/0.50
LPZ(config-subif)# encapsulation dot1Q 50
LPZ(config-subif)# ip address 192.168.111.65 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:2::1/64
LPZ(config-subif)#interface GigabitEthernet2/0.60
LPZ(config-subif)# encapsulation dot1Q 60
LPZ(config-subif)# ip address 192.168.111.97 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:5::1/64
LPZ(config-subif)#interface GigabitEthernet2/0.70
LPZ(config-subif)# encapsulation dot1Q 70
LPZ(config-subif)# ip address 192.168.111.129 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:7::1/64
LPZ(config-subif)#interface GigabitEthernet2/0.90
LPZ(config-subif)# encapsulation dot1Q 90
LPZ(config-subif)# ip address 192.168.111.161 255.255.255.224
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:A::1/64
LPZ(config-subif)#interface GigabitEthernet2/0.151
LPZ(config-subif)# encapsulation dot1Q 151
LPZ(config-subif)#interface GigabitEthernet2/0.200
LPZ(config-subif)# encapsulation dot1Q 200 native
LPZ(config-subif)# ip address 192.168.111.193 255.255.255.248
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:202::1/64
LPZ(config-subif)#interface GigabitEthernet3/0
LPZ(config-if)# no shutdown
LPZ(config)#interface GigabitEthernet3/0.100
LPZ(config-subif)# encapsulation dot1Q 100
LPZ(config-subif)# ip address 192.168.112.1 255.255.255.192
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:4::1/64
```

```
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:D::1/64
LPZ(config-subif)#interface GigabitEthernet4/0.200
LPZ(config-subif)# encapsulation dot1Q 200 native
LPZ(config-subif)# ip address 192.168.113.33 255.255.255.248
LPZ(config-subif)# ipv6 address FE80::1 link-local
LPZ(config-subif)# ipv6 address 2001:DB8:ACEF:200::1/64
LPZ(config-subif)#interface GigabitEthernet5/0
LPZ(config-if)# no shutdown
LPZ(config-if)# ip address 181.188.178.225 255.255.255.252
LPZ(config-if)# ipv6 address 2001:DB8:ACEF:F000::1/64
LPZ(config-if)#interface GigabitEthernet6/0
LPZ(config-if)# ip address 10.0.0.5 255.255.255.252
LPZ(config-if)# no shutdown
```

Asignación de direcciones de red en el Router CBBA

```
Router>enable
Router#configure terminal
Router(config)#hostname CBBA
CBBA(config)#ip cef
CBBA(config)#ipv6 unicast-routing
CBBA(config)#ipv6 cef
CBBA(config)#no ip domain lookup
CBBA(config)#interface Loopback0
CBBA(config-if)# ip address 10.10.10.2 255.255.255.255
CBBA(config-if)#interface GigabitEthernet0/0
CBBA(config-if)# ip address 10.0.0.2 255.255.255.252
CBBA(config-if)# no shutdown
CBBA(config-if)#interface GigabitEthernet2/0
CBBA(config-if)# no shutdown
CBBA(config-if)#interface GigabitEthernet2/0.10
CBBA(config-subif)# encapsulation dot1Q 10
CBBA(config-subif)# ip address 192.168.120.65 255.255.255.224
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:10::1/64
CBBA(config-subif)#interface GigabitEthernet2/0.20
CBBA(config-subif)# encapsulation dot1Q 20
CBBA(config-subif)# ip address 192.168.120.97 255.255.255.224
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:15::1/64
CBBA(config-subif)#interface GigabitEthernet2/0.30
CBBA(config-subif)# encapsulation dot1Q 30
CBBA(config-subif)# ip address 192.168.120.129 255.255.255.224
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:13::1/64
CBBA(config-subif)#interface GigabitEthernet2/0.40
CBBA(config-subif)# encapsulation dot1Q 40
CBBA(config-subif)# ip address 192.168.120.161 255.255.255.224
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:17::1/64
CBBA(config-subif)#interface GigabitEthernet2/0.80
CBBA(config-subif)# encapsulation dot1Q 80
CBBA(config-subif)# ip address 192.168.120.193 255.255.255.240
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:18::1/64
CBBA(config-subif)#interface GigabitEthernet2/0.150
CBBA(config-subif)# encapsulation dot1Q 150
CBBA(config-subif)# ip address 192.168.120.1 255.255.255.192
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:1a::1/64
CBBA(config-subif)#interface GigabitEthernet2/0.200
CBBA(config-subif)# encapsulation dot1Q 200 native
CBBA(config-subif)# ip address 192.168.120.209 255.255.255.248
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:205::1/64
```

```
CBBA(config-subif)#interface GigabitEthernet3/0
CBBA(config-if)# no shutdown
CBBA(config)#interface GigabitEthernet3/0.50
CBBA(config-subif)# encapsulation dot1Q 50
CBBA(config-subif)# ip address 192.168.121.65 255.255.255.224
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:12::1/64
CBBA(config-subif)#interface GigabitEthernet3/0.60
CBBA(config-subif)# encapsulation dot1Q 60
CBBA(config-subif)# ip address 192.168.121.97 255.255.255.224
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:14::1/64
CBBA(config-subif)#interface GigabitEthernet3/0.70
CBBA(config-subif)# encapsulation dot1Q 70
CBBA(config-subif)# ip address 192.168.121.129 255.255.255.224
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:16::1/64
CBBA(config-subif)#interface GigabitEthernet3/0.90
CBBA(config-subif)# encapsulation dot1Q 90
CBBA(config-subif)# ip address 192.168.121.161 255.255.255.240
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:19::1/64
CBBA(config-subif)#interface GigabitEthernet3/0.110
CBBA(config-subif)# encapsulation dot1Q 110
CBBA(config-subif)# ip address 192.168.121.177 255.255.255.248
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:11::1/64
CBBA(config-subif)#interface GigabitEthernet3/0.151
CBBA(config-subif)# encapsulation dot1Q 151
CBBA(config-subif)# ip address 192.168.121.1 255.255.255.192
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:1b::1/64
CBBA(config-subif)#interface GigabitEthernet3/0.200
CBBA(config-subif)# encapsulation dot1Q 200 native
CBBA(config-subif)# ip address 192.168.121.185 255.255.255.248
CBBA(config-subif)# ipv6 address FE80::2 link-local
CBBA(config-subif)# ipv6 address 2001:DB8:ACEF:206::1/64
```

Asignación de direcciones de red en el Router SCZ

```
Router>enable
Router#configure terminal
Router(config)#hostname SCZ
SCZ(config)#ip cef
SCZ(config)#ipv6 unicast-routing
SCZ(config)#ipv6 cef
SCZ(config)#no ip domain lookup
SCZ(config)#interface Loopback0
SCZ(config-if)# ip address 10.10.10.3 255.255.255.255
SCZ(config-if)#interface GigabitEthernet0/0
SCZ(config-if)# ip address 10.0.0.6 255.255.255.252
SCZ(config-if)# no shutdown
SCZ(config-if)#interface GigabitEthernet2/0
SCZ(config-if)# no shutdown
SCZ(config-if)#interface GigabitEthernet2/0.10
SCZ(config-subif)# encapsulation dot1Q 10
SCZ(config-subif)# ip address 192.168.130.65 255.255.255.224
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:20::1/64
SCZ(config-subif)#interface GigabitEthernet2/0.20
SCZ(config-subif)# encapsulation dot1Q 20
SCZ(config-subif)# ip address 192.168.130.97 255.255.255.224
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:25::1/64
SCZ(config-subif)#interface GigabitEthernet2/0.30
SCZ(config-subif)# encapsulation dot1Q 30
SCZ(config-subif)# ip address 192.168.130.129 255.255.255.224
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:23::1/64
SCZ(config-subif)#interface GigabitEthernet2/0.40
SCZ(config-subif)# encapsulation dot1Q 40
SCZ(config-subif)# ip address 192.168.130.161 255.255.255.224
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:27::1/64
SCZ(config-subif)#interface GigabitEthernet2/0.80
SCZ(config-subif)# encapsulation dot1Q 80
SCZ(config-subif)# ip address 192.168.130.193 255.255.255.240
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:28::1/64
SCZ(config-subif)# interface GigabitEthernet2/0.150
SCZ(config-subif)# encapsulation dot1Q 150
SCZ(config-subif)# ip address 192.168.130.1 255.255.255.192
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:2A::1/64
SCZ(config-subif)# interface GigabitEthernet2/0.200
SCZ(config-subif)# encapsulation dot1Q 200 native
SCZ(config-subif)# ip address 192.168.130.209 255.255.255.248
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:207::1/64
```

```
SCZ(config-subif)#interface GigabitEthernet3/0
SCZ(config-if)# no shutdown
SCZ(config)#interface GigabitEthernet3/0.50
SCZ(config-subif)# encapsulation dot1Q 50
SCZ(config-subif)# ip address 192.168.131.65 255.255.255.224
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:22::1/64
SCZ(config-subif)#interface GigabitEthernet3/0.60
SCZ(config-subif)# encapsulation dot1Q 60
SCZ(config-subif)# ip address 192.168.131.97 255.255.255.224
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:24::1/64
SCZ(config-subif)#interface GigabitEthernet3/0.70
SCZ(config-subif)# encapsulation dot1Q 70
SCZ(config-subif)# ip address 192.168.131.129 255.255.255.224
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:26::1/64
SCZ(config-subif)#interface GigabitEthernet3/0.90
SCZ(config-subif)# encapsulation dot1Q 90
SCZ(config-subif)# ip address 192.168.131.161 255.255.255.240
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:29::1/64
SCZ(config-subif)#interface GigabitEthernet3/0.110
SCZ(config-subif)# encapsulation dot1Q 110
SCZ(config-subif)# ip address 192.168.131.177 255.255.255.248
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:21::1/64
SCZ(config-subif)#interface GigabitEthernet3/0.151
SCZ(config-subif)# encapsulation dot1Q 151
SCZ(config-subif)# ip address 192.168.131.1 255.255.255.192
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:2B::1/64
SCZ(config-subif)#interface GigabitEthernet3/0.200
SCZ(config-subif)# encapsulation dot1Q 200 native
SCZ(config-subif)# ip address 192.168.131.185 255.255.255.248
SCZ(config-subif)# ipv6 address FE80::3 link-local
SCZ(config-subif)# ipv6 address 2001:DB8:ACEF:208::1/64
```

Asignación de direcciones de red y VLANs en los Switches

Comando	Funcion
vlan [#num] name	Crear una VLAN
interface vlan [#num]	Configurar una VLAN con funciones de Capa 3
switchport mode trunk	Configurar un puerto com o extremo de un enlace troncal
switchport trunk native vlan [#num]	Especificar una VLAN nativa distinta de VLAN1
switchport trunk allowed vlan [#num]	Especificar las VLAN que se permite en el enlace troncal

```
Switch-LPZ-1(config)#ipv6 unicast-routing
Switch-LPZ-1(config)#no ip domain lookup
Switch-LPZ-1#vlan database
Switch-LPZ-1(vlan)#vlan 10 name Gerencia
Switch-LPZ-1(vlan)#vlan 20 name Admin_IT
Switch-LPZ-1(vlan)#vlan 30 name Operaciones
Switch-LPZ-1(vlan)#vlan 40 name Finanzas
Switch-LPZ-1(vlan)#vlan 80 name Impresoras
Switch-LPZ-1(vlan)#vlan 150 name Voz_1
Switch-LPZ-1(vlan)#vlan 200 name Switch-LPZ-1
Switch-LPZ-1(config)#interface vlan 200
Switch-LPZ-1(config-if)#ip address 192.168.110.226 255.255.255.248
Switch-LPZ-1(config-if)#ipv6 address 2001:DB8:ACEF:201::2/64
Switch-LPZ-1(config)#ip route 0.0.0.0 0.0.0.0 192.168.110.225
Switch-LPZ-1(config)#ipv6 route ::/0 2001:DB8:ACEF:201::1
Switch-LPZ-1(config)#!
Switch-LPZ-1(config)#interface FastEthernet 0/0
Switch-LPZ-1(config-if)#no shutdown
Switch-LPZ-1(config-if)#switchport mode trunk
Switch-LPZ-1(config-if)#switchport trunk native vlan 200
Switch-LPZ-1(config-if)#switchport trunk allowed vlan 10,20,30,40,80,150,200
```

```
Switch-LPZ-2(config)#ipv6 unicast-routing
Switch-LPZ-2(config)#no ip domain lookup
Switch-LPZ-2#vlan database
Switch-LPZ-2(vlan)#vlan 50 name Ventas
Switch-LPZ-2(vlan)#vlan 60 name Marketing
Switch-LPZ-2(vlan)#vlan 70 name RRHH
Switch-LPZ-2(vlan)#vlan 90 name Camaras_IP
Switch-LPZ-2(vlan)#vlan 151 name Voz_2
Switch-LPZ-2(vlan)#vlan 200 name Switch-LPZ-2
Switch-LPZ-2(config)#interface vlan 200
Switch-LPZ-2(config-if)#ip address 192.168.111.194 255.255.255.248
Switch-LPZ-2(config-if)#ipv6 address 2001:DB8:ACEF:202::2/64
Switch-LPZ-2(config)#ip route 0.0.0.0 0.0.0.0 192.168.111.193
Switch-LPZ-2(config)#ipv6 route ::/0 2001:DB8:ACEF:202::1
Switch-LPZ-2(config)#!
Switch-LPZ-2(config)#interface FastEthernet 0/0
Switch-LPZ-2(config-if)#no shutdown
Switch-LPZ-2(config-if)#switchport mode trunk
Switch-LPZ-2(config-if)#switchport trunk native vlan 200
Switch-LPZ-2(config-if)#switchport trunk allowed vlan 50,60,70,90,151,200
```

```
Switch-LPZ-3(config)#ipv6 unicast-routing
Switch-LPZ-3(config)#no ip domain lookup
Switch-LPZ-3#vlan database
Switch-LPZ-3(vlan)#vlan 100 name Call_Center
Switch-LPZ-3(vlan)#vlan 200 name Switch-LPZ-3
Switch-LPZ-3(config)#interface vlan 200
Switch-LPZ-3(config-if)#ip address 192.168.112.66 255.255.255.248
Switch-LPZ-3(config-if)#ipv6 address 2001:DB8:ACEF:203::2/64
Switch-LPZ-3(config)#ip route 0.0.0.0 0.0.0.0 192.168.112.65
Switch-LPZ-3(config)#ipv6 route ::/0 2001:DB8:ACEF:203::1
Switch-LPZ-3(config)#!
Switch-LPZ-3(config)#interface FastEthernet 0/0
Switch-LPZ-3(config-if)#no shutdown
Switch-LPZ-3(config-if)#switchport mode trunk
Switch-LPZ-3(config-if)#switchport trunk native vlan 200
Switch-LPZ-3(config-if)#switchport trunk allowed vlan 100,200
```

```
Switch-Servidores(config)#ipv6 unicast-routing
Switch-Servidores(config)#no ip domain lookup
Switch-Servidores#vlan database
Switch-Servidores(vlan)#vlan 110 name Data_Center
Switch-Servidores(vlan)#vlan 152 name Voz_3
Switch-Servidores(vlan)#vlan 200 name Administracion
Switch-Servidores(config)#interface vlan 200
Switch-Servidores(config-if)#ip address 192.168.113.34 255.255.255.248
Switch-Servidores(config-if)#ipv6 address 2001:DB8:ACEF:200::2/64
Switch-Servidores(config)#ip route 0.0.0.0 0.0.0.0 192.168.113.33
Switch-Servidores(config)#ipv6 route ::/0 2001:DB8:ACEF:200::1
Switch-Servidores(config)#!
Switch-Servidores(config)#interface FastEthernet 0/0
Switch-Servidores(config-if)#no shutdown
Switch-Servidores(config-if)#switchport mode trunk
Switch-Servidores(config-if)#switchport trunk native vlan 200
Switch-Servidores(config-if)#switchport trunk allowed vlan 110,152,200
```

```
Switch-CBBA-1(config)#ipv6 unicast-routing
Switch-CBBA-1(config)#no ip domain lookup
Switch-CBBA-1#vlan database
Switch-CBBA-1(vlan)#vlan 10 name Gerencia_Reg
Switch-CBBA-1(vlan)#vlan 20 name Admin_IT
Switch-CBBA-1(vlan)#vlan 30 name Operaciones
Switch-CBBA-1(vlan)#vlan 40 name Finanzas
Switch-CBBA-1(vlan)#vlan 80 name Impresoras
Switch-CBBA-1(vlan)#vlan 150 name Voz_1
Switch-CBBA-1(vlan)#vlan 200 name Switch-CBBA-1
```

```
Switch-CBBA-1(config)#interface vlan 200
Switch-CBBA-1(config-if)#ip address 192.168.120.210 255.255.255.248
Switch-CBBA-1(config-if)#ipv6 address 2001:DB8:ACEF:205::2/64
Switch-CBBA-1(config)#ip route 0.0.0.0 0.0.0.0 192.168.120.209
Switch-CBBA-1(config)#ipv6 route ::/0 2001:DB8:ACEF:205::1
Switch-CBBA-1(config)#!
Switch-CBBA-1(config)#interface FastEthernet 0/0
Switch-CBBA-1(config-if)#no shutdown
Switch-CBBA-1(config-if)#switchport mode trunk
Switch-CBBA-1(config-if)#switchport trunk native vlan 200
Switch-CBBA-1(config-if)#switchport trunk allowed vlan 10,20,30,40,80,150,200
```

```
Switch-CBBA-2(config)#ipv6 unicast-routing
Switch-CBBA-2(config)#no ip domain lookup
Switch-CBBA-2#vlan database
Switch-CBBA-2(vlan)#vlan 50 name Ventas
Switch-CBBA-2(vlan)#vlan 60 name Marketing
Switch-CBBA-2(vlan)#vlan 70 name RRHH
Switch-CBBA-2(vlan)#vlan 90 name Camaras_IP
Switch-CBBA-2(vlan)#vlan 110 name Data_Center
Switch-CBBA-2(vlan)#vlan 151 name Voz_2
Switch-CBBA-2(vlan)#vlan 200 name Switch-CBBA-2
Switch-CBBA-2(config)#interface vlan 200
Switch-CBBA-2(config-if)#ip address 192.168.121.186 255.255.255.248
Switch-CBBA-2(config-if)#ipv6 address 2001:DB8:ACEF:206::2/64
Switch-CBBA-2(config)#ip route 0.0.0.0 0.0.0.0 192.168.121.185
Switch-CBBA-2(config)#ipv6 route ::/0 2001:DB8:ACEF:206::1
Switch-CBBA-2(config)#!
Switch-CBBA-2(config)#interface FastEthernet 0/0
Switch-CBBA-2(config-if)#no shutdown
Switch-CBBA-2(config-if)#switchport mode trunk
Switch-CBBA-2(config-if)#switchport trunk native vlan 200
Switch-CBBA-2(config-if)#switchport trunk allowed vlan 50,60,70,90,110,151,200
```

```
Switch-SCZ-1(config)#ipv6 unicast-routing
Switch-SCZ-1(config)#no ip domain lookup
Switch-SCZ-1#vlan database
Switch-SCZ-1(vlan)#vlan 10 name Gerencia_Reg
Switch-SCZ-1(vlan)#vlan 20 name Admin_IT
Switch-SCZ-1(vlan)#vlan 30 name Operaciones
Switch-SCZ-1(vlan)#vlan 40 name Finanzas
Switch-SCZ-1(vlan)#vlan 80 name Impresoras
Switch-SCZ-1(vlan)#vlan 150 name Voz_1
Switch-SCZ-1(vlan)#vlan 200 name Switch-SCZ-1
Switch-SCZ-1(config)#interface vlan 200
```

```
Switch-SCZ-1(config-if)#ip address 192.168.130.210 255.255.255.248
Switch-SCZ-1(config-if)#ipv6 address 2001:DB8:ACEF:207::2/64
Switch-SCZ-1(config)#ip route 0.0.0.0 0.0.0.0 192.168.130.209
Switch-SCZ-1(config)#ipv6 route ::/0 2001:DB8:ACEF:207::1
Switch-SCZ-1(config)#!
Switch-SCZ-1(config)#interface FastEthernet 0/0
Switch-SCZ-1(config-if)#switchport mode trunk
Switch-SCZ-1(config-if)#no shutdown
Switch-SCZ-1(config-if)#switchport trunk native vlan 200
Switch-SCZ-1(config-if)#switchport trunk allowed vlan 10,20,30,40,80,150,200
```

```
Switch-SCZ-2(config)#ipv6 unicast-routing
Switch-SCZ-2(config)#no ip domain lookup
Switch-SCZ-2#vlan database
Switch-SCZ-2(vlan)#vlan 50 name Ventas
Switch-SCZ-2(vlan)#vlan 60 name Marketing
Switch-SCZ-2(vlan)#vlan 70 name RRHH
Switch-SCZ-2(vlan)#vlan 90 name Camaras_IP
Switch-SCZ-2(vlan)#vlan 110 name Data_Center
Switch-SCZ-2(vlan)#vlan 151 name Voz_2
Switch-SCZ-2(vlan)#vlan 200 name Switch-SCZ-2
Switch-SCZ-2(config)#interface vlan 200
Switch-SCZ-2(config-if)#ip address 192.168.131.186 255.255.255.248
Switch-SCZ-2(config-if)#ipv6 address 2001:DB8:ACEF:208::2/64
Switch-SCZ-2(config)#ip route 0.0.0.0 0.0.0.0 192.168.131.185
Switch-SCZ-2(config)#ipv6 route ::/0 2001:DB8:ACEF:208::1
Switch-SCZ-2(config)#!
Switch-SCZ-2(config)#interface FastEthernet 0/0
Switch-SCZ-2(config-if)#no shutdown
Switch-SCZ-2(config-if)#switchport mode trunk
Switch-SCZ-2(config-if)#switchport trunk native vlan 200
Switch-SCZ-2(config-if)#switchport trunk allowed vlan 50,60,70,90,110,151,200
```

Anexo 2: Configuración del protocolo de enrutamiento OSPFv2

```
LPZ(config)#router ospf 10
LPZ(config-router)# router-id 10.10.10.1
LPZ(config-router)# network 10.10.10.1 0.0.0.0 area 0
LPZ(config-router)# network 10.0.0.0 0.0.0.3 area 0
LPZ(config-router)# network 10.0.0.4 0.0.0.3 area 0
LPZ(config-router)# network 192.168.110.0 0.0.31.255 area 0
LPZ(config-router)# default-information originate
```

```
CBBA(config)#router ospf 10
CBBA(config-router)# router-id 10.10.10.2
CBBA(config-router)# network 10.10.10.2 0.0.0.0 area 0
CBBA(config-router)# network 10.0.0.0 0.0.0.3 area 0
CBBA(config-router)# network 192.168.120.0 0.0.1.255 area 0
```

```
SCZ(config)#router ospf 10
SCZ(config-router)# router-id 10.10.10.3
SCZ(config-router)# network 10.10.10.3 0.0.0.0 area 0
SCZ(config-router)# network 10.0.0.4 0.0.0.3 area 0
SCZ(config-router)# network 192.168.130.0 0.0.1.255 area 0
```

Anexo 3: Configuración de MPLS en el núcleo de Red IPv4

```
LPZ(config)#mpls ip
LPZ(config)#mpls ldp router-id Loopback0
LPZ(config)#mpls label protocol ldp
LPZ(config)#interface GigabitEthernet0/0
LPZ(config-if)#mpls ip
LPZ(config)#interface GigabitEthernet6/0
LPZ(config-if)#mpls ip
```

```
CBBA(config)#mpls ip
CBBA(config)#mpls ldp router-id Loopback0
CBBA(config)#mpls label protocol ldp
CBBA(config)#interface GigabitEthernet0/0
CBBA(config-if)#mpls ip
```

```
SCZ(config)#mpls ip
SCZ(config)#mpls ldp router-id Loopback0
SCZ(config)#mpls label protocol ldp
SCZ(config)#interface GigabitEthernet0/0
SCZ(config-if)#mpls ip
```

Anexo 4: Configuración de Multiprotocol BGP (MP – BGP)

Comando	Funcion
router bgp [AS]	Habilitar el protocolo de enrutamiento BGP
neighbor [x.x.x.x] remote-as [AS]	Especificar un vecino en un AS
neighbor [x.x.x.x] update-source [interfaz]	Establecer la conexion usando una interfaz
neighbor [x.x.x.x] activate	Habilitar el intercambio de informacion
neighbor [x.x.x.x] send-label	Habilitar el intercambio de etiquetas MPLS

```
LPZ(config)#router bgp 100
LPZ(config-router)# bgp router-id 10.10.10.1
LPZ(config-router)# bgp log-neighbor-changes
LPZ(config-router)# no bgp default ipv4-unicast
LPZ(config-router)# neighbor 10.10.10.2 remote-as 100
LPZ(config-router)# neighbor 10.10.10.2 update-source Loopback0
LPZ(config-router)# neighbor 10.10.10.3 remote-as 100
LPZ(config-router)# neighbor 10.10.10.3 update-source Loopback0
LPZ(config-router)# address-family ipv6
LPZ(config-router-af)# redistribute connected
LPZ(config-router-af)# redistribute static
LPZ(config-router-af)# default-information originate
LPZ(config-router-af)# neighbor 10.10.10.2 activate
LPZ(config-router-af)# neighbor 10.10.10.2 send-label
LPZ(config-router-af)# neighbor 10.10.10.3 activate
LPZ(config-router-af)# neighbor 10.10.10.3 send-label
```

```
CBBA(config)#router bgp 100
CBBA(config-router)# bgp router-id 10.10.10.2
CBBA(config-router)# bgp log-neighbor-changes
CBBA(config-router)# no bgp default ipv4-unicast
CBBA(config-router)# neighbor 10.10.10.1 remote-as 100
CBBA(config-router)# neighbor 10.10.10.1 update-source Loopback0
CBBA(config-router)# neighbor 10.10.10.3 remote-as 100
CBBA(config-router)# neighbor 10.10.10.3 update-source Loopback0
CBBA(config-router)# address-family ipv6
CBBA(config-router-af)# redistribute connected
CBBA(config-router-af)# neighbor 10.10.10.1 activate
CBBA(config-router-af)# neighbor 10.10.10.1 send-label
CBBA(config-router-af)# neighbor 10.10.10.3 activate
CBBA(config-router-af)# neighbor 10.10.10.3 send-label
```

```
SCZ(config)#router bgp 100
SCZ(config-router)# bgp router-id 10.10.10.3
SCZ(config-router)# bgp log-neighbor-changes
SCZ(config-router)# no bgp default ipv4-unicast
SCZ(config-router)# neighbor 10.10.10.1 remote-as 100
SCZ(config-router)# neighbor 10.10.10.1 update-source Loopback0
SCZ(config-router)# neighbor 10.10.10.2 remote-as 100
SCZ(config-router)# neighbor 10.10.10.2 update-source Loopback0
SCZ(config-router)# address-family ipv6
SCZ(config-router-af)# redistribute connected
SCZ(config-router-af)# neighbor 10.10.10.1 activate
SCZ(config-router-af)# neighbor 10.10.10.1 send-label
SCZ(config-router-af)# neighbor 10.10.10.2 activate
SCZ(config-router-af)# neighbor 10.10.10.2 send-label
```

Anexo 5: Configuración de QoS

Configuración de clasificación y políticas de QoS - LPZ

```
LPZ(config)#class-map match-any EF
LPZ(config-cmap)#  description Voz
LPZ(config-cmap)# match mpls experimental topmost 5
LPZ(config-cmap)# match dscp ef
LPZ(config-cmap)#class-map match-any CS1
LPZ(config-cmap)#  description Scavenger
LPZ(config-cmap)# match mpls experimental topmost 1
LPZ(config-cmap)# match dscp cs1
LPZ(config-cmap)#class-map match-any CS3
LPZ(config-cmap)#  description Video Broadcast y Senalizacion
LPZ(config-cmap)# match mpls experimental topmost 3
LPZ(config-cmap)# match dscp cs3
LPZ(config-cmap)#class-map match-any CS4
LPZ(config-cmap)#  description Video Conferencias
LPZ(config-cmap)# match mpls experimental topmost 4
LPZ(config-cmap)# match dscp cs4
LPZ(config-cmap)#class-map match-any CS6
LPZ(config-cmap)#  description Control de Red
LPZ(config-cmap)# match mpls experimental topmost 6
LPZ(config-cmap)# match dscp cs6
LPZ(config-cmap)#class-map match-any AF2
LPZ(config-cmap)#  description Datos Transaccionales
LPZ(config-cmap)# match mpls experimental topmost 2
LPZ(config-cmap)# match dscp cs2
LPZ(config-cmap)#policy-map QoS_LPZ
LPZ(config-pmap)# class EF
LPZ(config-pmap-c)#  priority percent 10
LPZ(config-pmap-c)# class CS4
LPZ(config-pmap-c)#  priority percent 23
LPZ(config-pmap-c)# class CS6
LPZ(config-pmap-c)#  bandwidth percent 5
LPZ(config-pmap-c)# class CS3
LPZ(config-pmap-c)#  bandwidth percent 12
LPZ(config-pmap-c)# class AF2
LPZ(config-pmap-c)#  bandwidth percent 23
LPZ(config-pmap-c)# class CS1
LPZ(config-pmap-c)#  bandwidth percent 2
LPZ(config-pmap-c)# class class-default
LPZ(config-pmap-c)#  bandwidth percent 25
LPZ(config-pmap-c)#  exit
```

```
LPZ(config)#!
LPZ(config)#interface GigabitEthernet0/0
LPZ(config-if)# service-policy output QoS_LPZ
LPZ(config)#interface GigabitEthernet1/0
LPZ(config-if)# service-policy output QoS_LPZ
LPZ(config)#interface GigabitEthernet2/0
LPZ(config-if)# service-policy output QoS_LPZ
LPZ(config)#interface GigabitEthernet3/0
LPZ(config-if)# service-policy output QoS_LPZ
LPZ(config)#interface GigabitEthernet4/0
LPZ(config-if)# service-policy output QoS_LPZ
LPZ(config)#interface GigabitEthernet5/0
LPZ(config-if)# service-policy output QoS_LPZ
LPZ(config)#interface GigabitEthernet6/0
LPZ(config-if)# service-policy output QoS_LPZ
```

```
CBBA(config)#!policy-map QoS_CBBA
CBBA(config)#interface GigabitEthernet0/0
CBBA(config-if)# service-policy output QoS_CBBA
CBBA(config)#interface GigabitEthernet2/0
CBBA(config-if)# service-policy output QoS_CBBA
CBBA(config)#interface GigabitEthernet3/0
CBBA(config-if)# service-policy output QoS_CBBA
```

```
SCZ(config)#!policy-map QoS_SCZ
SCZ(config)#interface GigabitEthernet0/0
SCZ(config-if)# service-policy output QoS_SCZ
SCZ(config)#interface GigabitEthernet2/0
SCZ(config-if)# service-policy output QoS_SCZ
SCZ(config)#interface GigabitEthernet3/0
SCZ(config-if)# service-policy output QoS_SCZ
```

Anexo 6: Configuración para la conexión a la red de Internet y NAT para la traducción de direcciones IPv4

Rutas por defecto para la conexión a la red de Internet

```
LPZ(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet5/0 181.188.178.226
LPZ(config)#!
LPZ(config)#ipv6 route ::/0 GigabitEthernet5/0 2001:DB8:ACEF:F000::2
```

Configuración de NAT para la traducción de direcciones IPv4

```
LPZ(config)#ip nat inside source list TRADUCCION interface GigabitEthernet5/0 overload
LPZ(config)#ip access-list standard TRADUCCION
LPZ(config-std-nacl)#permit 192.168.0.0 0.0.255.255
LPZ(config-std-nacl)#exit
LPZ(config)#interface GigabitEthernet0/0
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet1/0.10
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet1/0.20
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet1/0.30
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet1/0.40
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet1/0.80
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet1/0.200
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet2/0.50
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet2/0.60
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet2/0.70
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet2/0.90
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet3/0.100
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet3/0.200
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet4/0.110
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet4/0.200
LPZ(config-if)#ip nat inside
LPZ(config-if)#interface GigabitEthernet5/0
LPZ(config-if)#ip nat outside
LPZ(config-if)#interface GigabitEthernet6/0
LPZ(config-if)#ip nat inside
```

Anexo 7: Configuración de Listas de Acceso

Listas de Acceso para denegar conexiones procedentes de Internet, mediante el protocolo Telnet

```
LPZ(config)#ip access-list extended TELNET_INTERNET_IPv4
LPZ(config-ext-nacl)# deny tcp any any eq telnet
LPZ(config-ext-nacl)# permit ip any any
LPZ(config-ext-nacl)# exit
LPZ(config)#ipv6 access-list TELNET_INTERNET_IPv6
LPZ(config-ipv6-acl)# deny tcp any any eq telnet
LPZ(config-ipv6-acl)# permit ipv6 any any
LPZ(config-ipv6-acl)# exit
LPZ(config)#interface GigabitEthernet5/0
LPZ(config-if)#ip access-group TELNET_INTERNET_IPv4 in
LPZ(config-if)#ipv6 traffic-filter TELNET_INTERNET_IPv6 in
```

Listas de Acceso para denegar conexiones mediante los protocolos Telnet y SSH en las redes LAN - LPZ

```
LPZ(config)#ip access-list extended TELNET_SSH_LAN_IPv4
LPZ(config-ext-nacl)#deny tcp any any eq 22
LPZ(config-ext-nacl)#deny tcp any any eq 23
LPZ(config-ext-nacl)#permit ip any any
LPZ(config-ext-nacl)#exit
LPZ(config)#ipv6 access-list TELNET_SSH_LAN_IPv6
LPZ(config-ipv6-acl)#deny tcp any any eq 22
LPZ(config-ipv6-acl)#deny tcp any any eq 23
LPZ(config-ipv6-acl)#permit ipv6 any any
LPZ(config-ipv6-acl)#exit
LPZ(config)#!
LPZ(config)#ip access-list extended ADMINISTRACION_IPv4
LPZ(config-ext-nacl)#deny tcp any any eq 23
LPZ(config-ext-nacl)#permit ip any any
LPZ(config-ext-nacl)#exit
LPZ(config)#ipv6 access-list ADMINISTRACION_IPv6
LPZ(config-ext-nacl)#deny tcp any any eq 23
LPZ(config-ext-nacl)#permit ipv6 any any
LPZ(config-ext-nacl)#exit
LPZ(config)#!
LPZ(config)#interface GigabitEthernet1/0.10
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet1/0.20
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet1/0.30
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
```

```
LPZ(config-subif)# interface GigabitEthernet1/0.40
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet1/0.80
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet1/0.150
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet1/0.200
LPZ(config-subif)# ip access-group ADMINISTRACION_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter ADMINISTRACION_IPv6 in
LPZ(config-subif)# interface GigabitEthernet2/0.50
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet2/0.60
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet2/0.70
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet2/0.90
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet2/0.151
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet2/0.200
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)#interface GigabitEthernet3/0.100
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet3/0.200
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet2/0.200
LPZ(config-subif)# ip access-group ADMINISTRACION_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter ADMINISTRACION_IPv6 in
LPZ(config-subif)# interface GigabitEthernet3/0.100
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet3/0.200
LPZ(config-subif)# ip access-group ADMINISTRACION_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter ADMINISTRACION_IPv6 in
LPZ(config-subif)# interface GigabitEthernet4/0.110
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet4/0.152
LPZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
LPZ(config-subif)# interface GigabitEthernet4/0.200
LPZ(config-subif)# ip access-group ADMINISTRACION_IPv4 in
LPZ(config-subif)# ipv6 traffic-filter ADMINISTRACION_IPv6 in
```

Listas de Acceso en las redes LAN – CBBA

```
CBBA(config)#interface GigabitEthernet2/0.10
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet2/0.20
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet2/0.30
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet2/0.40
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet2/0.80
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet2/0.150
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet2/0.200
CBBA(config-subif)# ip access-group ADMINISTRACION_IPv4  in
CBBA(config-subif)# ipv6 traffic-filter ADMINISTRACION_IPv6 in
CBBA(config-subif)# interface GigabitEthernet3/0.50
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet3/0.60
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet3/0.70
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet3/0.90
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet3/0.110
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet3/0.151
CBBA(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
CBBA(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
CBBA(config-subif)# interface GigabitEthernet3/0.200
CBBA(config-subif)# ip access-group ADMINISTRACION_IPv4  in
CBBA(config-subif)# ipv6 traffic-filter ADMINISTRACION_IPv6 in
```

Listas de Acceso en las redes LAN – SCZ

```
SCZ(config)#interface GigabitEthernet2/0.10
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet2/0.20
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet2/0.30
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet2/0.40
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet2/0.80
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet2/0.150
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet2/0.200
SCZ(config-subif)# ip access-group ADMINISTRACION_IPv4  in
SCZ(config-subif)# ipv6 traffic-filter ADMINISTRACION_IPv6 in
SCZ(config-subif)#interface GigabitEthernet3/0.50
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet3/0.60
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet3/0.70
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet3/0.90
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet3/0.110
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet3/0.151
SCZ(config-subif)# ip access-group TELNET_SSH_LAN_IPv4 in
SCZ(config-subif)# ipv6 traffic-filter TELNET_SSH_LAN_IPv6 in
SCZ(config-subif)# interface GigabitEthernet3/0.200
SCZ(config-subif)# ip access-group ADMINISTRACION_IPv4  in
SCZ(config-subif)# ipv6 traffic-filter ADMINISTRACION_IPv6 in
```

Configuración de acceso remoto en el Router LPZ

Modo	Contraseña
Consola	LPZ_1111_c
Privilegiado	LPZ_1111_p
SSH	LPZ_1111

Username: router_LPZ

```
LPZ(config)#enable secret LPZ_1111_p
LPZ(config)#service password-encryption
LPZ(config)#line console 0
LPZ(config-line)#password LPZ_1111_c
LPZ(config-line)#login
LPZ(config-line)#exit
LPZ(config)#!
LPZ(config)#ip domain-name red_corporativa_dual_stack
LPZ(config)#crypto key generate rsa
The name for the keys will be: LPZ.red_corporativa_dual_stack
How many bits in the modulus [512]: 2048
LPZ(config)#username router_LPZ privilege 15 secret LPZ_1111
LPZ(config)#line vty 0 4
LPZ(config-line)#transport input ssh
LPZ(config-line)#login local
LPZ(config-line)#logging synchronous
LPZ(config-line)#exit
LPZ(config)#!
LPZ(config)#ip ssh version 2
LPZ(config)#ip ssh authentication-retries 3
```

Configuración de acceso remoto en el Router CBBA

Modo	Contraseña
Consola	CBBA_2222_c
Privilegiado	CBBA_2222_p
SSH	CBBA_2222

Username: router_CBBA

```
CBBA(config)#enable secret CBBA_2222_p
CBBA(config)#service password-encryption
CBBA(config)#line console 0
CBBA(config-line)#password CBBA_2222_c
CBBA(config-line)#login
CBBA(config-line)#exit
CBBA(config)#!
CBBA(config)#ip domain-name red_corporativa_dual_stack
CBBA(config)#crypto key generate rsa
The name for the keys will be: CBBA.red_corporativa_dual_stack
How many bits in the modulus [512]: 2048
CBBA(config)#username router_CBBA privilege 15 secret
CBBA_2222
CBBA(config)#line vty 0 4
CBBA(config-line)#transport input ssh
CBBA(config-line)#login local
CBBA(config-line)#logging synchronous
CBBA(config-line)#exit
CBBA(config)#!
CBBA(config)#ip ssh version 2
CBBA(config)#ip ssh authentication-retries 3
```

Configuración de acceso remoto en el Router SCZ

Modo	Contraseña
Consola	SCZ_3333_c
Privilegiado	SCZ_3333_p
SSH	SCZ_3333

Username: router_SCZ

```
SCZ(config)#enable secret SCZ_3333_p
SCZ(config)#service password-encryption
SCZ(config)#line console 0
SCZ(config-line)#password SCZ_3333_c
SCZ(config-line)#login
SCZ(config-line)#exit
SCZ(config)#!
SCZ(config)#ip domain-name red_corporativa_dual_stack
SCZ(config)#crypto key generate rsa
The name for the keys will be: SCZ.red_corporativa_dual_stack
How many bits in the modulus [512]: 2048
SCZ(config)#username router_SCZ privilege 15 secret SCZ_3333
SCZ(config)#line vty 0 4
SCZ(config-line)#transport input ssh
SCZ(config-line)#login local
SCZ(config-line)#logging synchronous
SCZ(config-line)#exit
SCZ(config)#!
SCZ(config)#ip ssh version 2
SCZ(config)#ip ssh authentication-retries 3
```

Correo Electrónico: ecristianguerra@gmail.com

Teléfono: 2-807215

Celular: 77284016