Universidad
Inca Garcilaso de la Vega
Nuevos Tiempos. Nuevas Ideas
Facultad de Ingeniería de Sistemas, Cómputo y Telecomunicaciones

DISEÑO DE UNA RED PRIVADA VIRTUAL PARA LA OPTIMIZACIÓN DE LAS COMUNICACIÓNES EN LA EMPRESA COMUNICACIONES E INFORMÁTICA SAC

CASO: REDES DE DATOS

Tesis para optar el Título de Ingeniero de Sistemas y Cómputo

Presentado por:

Torres Rodríguez Pool Jonathan

Asesor

Mg. Juan Carlos Rodríguez Sulca

Lima – Perú
Setiembre del 2016

DEDICATORIA

Quiero agradecer a toda mi familia que ha sido un apoyo incondicional en el Desarrollo de mi carrera y sobre todo en mi crecimiento personal.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La Empresa Comunicaciones e Informática dedicada a la venta de productos y servicios informáticos, luego de un estudio del mercado decidieron abrir una nueva sede en Trujillo por ello la empresa se ve en la necesidad de tener comunicación con la sede remota y viceversa, como principal requisito para la productividad empresarial en dicha sede. Por tal motivo es necesario la implementación de una VPN para la interconexión de dichas sedes, aplicando políticas de configuración como son: Calidad de servicio (QoS), Alta disponibilidad a nivel de default Gateway (HSRP), Protocolo de enrutamiento BGP, Segmentación de red en la LAN de la sede principal, Diseño jerárquico de la red LAN en la sede principal. Para ello es necesario hacer un estudio y seguir una metodología, el cual para el desarrollo de esta tesis se utilizó la metodología Cisco. La describo a continuación en el desarrollo de mi tesis.

La presente tesis consistió en el desarrollo de la metodología Cisco que consta de las siguientes fases desarrolladas: Planificación, Diseño, Implementación, Operación y Optimización, el cual me sirvió de guía y base para el diseño de la red teniendo en cuenta los requerimientos de la empresa.

Palabras clave: VPN, QoS, Gateway, HSRP, BGP, LAN.

ABSTRACT

The Communications and Information company dedicated to selling products and services, after a market survey decided to open a new headquarters in Trujillo why the company is in the need for communication with the remote site and vice versa, as the main requirement for business productivity in that place. Therefore implementing a VPN for the interconnection of these sites is necessary, applying configuration policies such as: Quality of Service (QoS), high availability level of default gateway (HSRP) routing protocol BGP, Network Segmentation on the LAN of the headquarters, hierarchical design LAN at headquarters. This requires a study and follows a methodology, which for the development of this thesis Cisco methodology was used. I describe below in the development of my thesis.

This thesis was the development of the Cisco methodology consists of the following developed phases: Planning, Design, Implementation, Operation and Optimization, which served as a guide and basis for the design of the network, taking into account the requirements of the company.

Keywords: VPN, QoS, Gateway, HSRP, BGP, LAN.

INTRODUCCIÓN

El presente trabajo de investigación lleva por título "Diseño de una Red Privada Virtual para la optimización de las comunicaciones en la empresa Comunicaciones e Informática SAC", para optar el Título de Ingeniero de Sistemas, presentado por el alumno Torres Rodríguez, Pool Jonathan.

El desarrollo de las Redes es hoy en día uno de los temas de mayor importancia en el área de las Telecomunicaciones, tanto las Redes LAN como en las Redes WAN, vitales en la comunicación actual de las personas y empresas que deseen tener un mayor campo de alcance a sus clientes. Las empresas y las personas están en constante comunicación, ya que en la actualidad mantenerse informado del acontecer del día a día es necesario para su toma de decisiones, logrando así la optimización de productividad empresarial y personal.

La presente tesis está centrado en el diseño e implementación de una Red privada virtual (VPN) que permite la comunicación en tiempo real e información de todos los procesos, tanto de la sede principal como remota, es decir provee interconexión de sede a sede estableciendo niveles de calidad de servicio (QOS) y alta disponibilidad (HSRP) a nivel de default Gateway en la sede Principal; el cual se desarrolló mediante un protocolo de enrutamiento dinámico conocido especialmente por los proveedores de servicio como BGP (Protocol Gateway Border).

El propósito de este diseño se llevaría a cabo utilizando parte de la infraestructura del proveedor de servicios CLARO, pero para nuestro caso de estudio debido a no contar con los equipos físicos se implementó en un simulador de redes muy importante llamado GNS3 que es el más robusto y de mayor utilidad que el simulador de Redes creado por Cisco (Packet Tracer).

Capítulo 1: Planteamiento del Problema

1.1. Situación Problemática

La Empresa Comunicaciones e Informática SAC es una organización empresarial constituida en Lima – Perú el 25 de marzo del 2014, tiene como sede principal en la Av. Circunvalación Golf Los Incas 154 Of. 1501 Edificio Capital El Golf Piso 15 en la ciudad de Lima distrito de Santiago de Surco.

La actividad comercial se centra en la venta de productos informáticos y servicios como: mantenimiento, instalación y reparación de PC's.

La empresa se encuentra en crecimiento acelerado en el mercado de las comunicaciones por lo que se apertura una nueva sede en Trujillo. Este rápido crecimiento conlleva a una centralización en la producción de la empresa y a la vez una falta de planificación estratégica por su rápido crecimiento. Esta situación origina o causa que no existan especialistas en diseño de su Red.

La empresa no disponía con sucursales remotas en provincias es por eso que no contaba con especialistas del tema de interconexión para sus sedes ni monitoreo de sus redes. Solo contaba con personal de soporte para su sede principal en Lima. Esta falta especialistas no permitió el diseño de una Red.

Métodos empíricos y con tecnología desactualizada hacían que los productos y servicios que ofrecía Comunicaciones e Informática se desarrollen de manera lenta e ineficiente con esto la productividad y la eficiencia se vio afectada por la lentitud en sus procesos de negocio. Por lo tanto la empresa se encontró con la necesidad de contar con una Red Privada Virtual, previo diseño, que le permitió tener la disponibilidad de información de primera mano es decir en tiempo real. A causa de esta falta de diseño, no existía comunicación entre sus sedes.

Basándonos en la realidad del mundo en que vivimos las empresas tienden siempre a optimizar las maneras de llegar a cumplir sus objetivos de negocio. Una de las maneras es la reducción de los costos y del tiempo, es por ello que la comunicación en tiempo real entre las sedes es de vital importancia.

En la actualidad la empresa Comunicaciones e Informática SAC cuenta con una sede principal en Lima y sede remota en Trujillo, debido al crecimiento en la demanda de los productos y servicios que oferta, la empresa se vió con la necesidad contar con un sistema de datos y disponibilidad de la información de manera rápida y eficiente de manera que pueda satisfacer la demanda de sus clientes y lograr sus objetivos trazados.

1.2. Problema de la investigación

- Problema General:

  ¿En qué medida el diseño de una Red Privada Virtual influirá en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC?

- Problemas Específicos:

  ¿En qué medida el nivel de funcionalidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC?

  ¿En qué medida el nivel de confiabilidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC?

¿En qué medida el nivel de seguridad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC?

1.3. Objetivos

- Objetivo General:

  Determinar la influencia del diseño de una Red Privada Virtual en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.

- Objetivos Específicos:

  - Determinar el nivel de funcionalidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.

  - Determinar el nivel de confiabilidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.

  - Determinar el nivel de seguridad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.

1.4. Justificación

La Empresa Comunicaciones e Informática SAC no contaba con una red de datos para manejar su información, esto hacia que sus procesos se desarrollen de forma incorrecta y en un tiempo muy extenso por lo que esto ocasionaba malestar entre los trabajadores y los clientes que necesitaban de sus bienes y servicios ofertados.

Es por esta razón que este diseño de red toma importancia porque se dio solución al problema que existía en el manejo de la información, por medio del diseño de una red de datos RPV por fibra óptica para interconectar su sede principal y remota con alta disponibilidad a nivel de default Gateway en su sede principal; siguiendo algunos de los requerimientos, los cuales se ajustó a la necesidad de Comunicaciones e Informática SAC y la benefició, con lo que permitió interconectar las diversas áreas que existen, además de interconectar sus sedes y de esta forma compartir información en tiempo real, agilizar procesos y hacer eficiente sus servicios y productos que ofrecen a sus clientes.

1.5. Alcance

El diseño de red es una herramienta útil en la implementación de una Red Privada Virtual, es decir: con esta solución dada, el administrador de Red o personal encargado de la configuración de sus Routers y demás equipos de Red podrá usar esta misma configuración en la implementación real a su servicio de Datos, el cual se tiene proyectado en conjunto con el proveedor de servicios en este caso es la empresa CLARO.

El diseño de la Red abarcó cinco fases como son: planeación, análisis, diseño, implementación y pruebas, según la metodología Cisco, que es capaz de lograr la interconexión entre dos sedes separadas por una amplia área geográfica (Lima – Trujillo), mediante un RPV que es una plataforma de Red convergente para lograr la transmisión de voz, datos y video sobre el protocolo IP.

El diseño de la red cuenta con alta de disponibilidad a nivel de default Gateway, ya que se utilizó el protocolo HSRP, el cual si un enlace falla por algún motivo rápidamente se utiliza otro enlace backup para continuidad de las comunicaciones en la empresa. Estos enlaces tanto el principal como el de contingencia establecen políticas de calidad de servicios (QoS) para el adecuado uso de los datos transmitidos clasificados en: voz y video, datos críticos y no críticos. Así como también se empleó para su comunicación y enrutamiento entre los routers, el protocolo BGP para el enrutamiento de sus paquetes de datos entre dichas sedes.

Capítulo 2: Marco Teórico

2.1. Antecedentes de la investigación

- GUSTAVO ARRIAGA MENDEZ, GUSTAVO LAREDO ZAMORANO, ITZA BELBETH MORALES HERNANDEZ (2009); Con su trabajo de investigación "Diseño de la infraestructura de una red de comunicaciones en la zona minera de Compañía Minera San Miguel del Cantil S.A. de C.V." donde se trata de que este Proyecto reúne las condiciones necesarias a cubrir para ofrecer de una manera totalmente factible la creación de una Red en la zona minera haciendo llegar los servicios mediante la alternativa seleccionada (Radioenlace) .

- NUTTSY AURORA, LAZO GARCIA (2012); Con su trabajo de investigación "Diseño e implementación de una Red Lan y Wlan con sistema de control de acceso mediante servidores AAA" donde se trata de que este proyecto comprobó que los protocolos AAA RADIUS y TACACS+ tienen diferentes características en el manejo de la autenticación y autorización así como también se demostró que con ayuda de adecuados protocolos y técnicas de red se puede optimizar el uso de recursos de la misma y hacer que esta sea más robusta frente a averías que pueda sufrir.

- LOPEZ ANDRADE XAVIER FRANCISCO (2008); Con su trabajo de investigación "Rediseño de la Red con calidad de servicios para datos y tecnología de voz sobre IP en el ilustre Municipio de Ambato" donde se trata de una Red de la Ilustre Municipalidad de Ambato que es una red que está trabajando en buena forma pero fue diseñada y construida para dar servicio en un periodo aproximado de 5 años, este periodo está a punto de fenecer y esta Red se ve enfrentada a los nuevos retos , nuevas tecnologías y aplicaciones de hoy en día, por lo que el rediseño completo planteado satisficiera tales demandas.

- GLADYS YANINA CUBAS DIAZ, MICHEL HERBERT PERALES FABIAN (2011); Con su trabajo de investigación "Rediseño de la Red Wan de la Empresa Epsel S.A." donde se concluyó que la empresa prestadora de servicios EPSEL S.A. en su conjunto, puede brindar mejores servicios y elevar el nivel de eficiencia y calidad en los diversos procesos que ofrecen, a través del uso de Tecnologías de Información.

2.2. Bases teóricas

2.2.1 Redes de comunicaciones

Una Red es un conjunto de ordenadores conectados entre sí logrando así comunicación entre ellos con esto comparten datos y recursos sin importar la ubicación física que separen estos equipos. A través de una red se pueden ejecutar procesos en otro ordenador o acceder a sus ficheros, enviar mensajes, compartir programas, etc.

Los ordenadores suelen estar conectados entre sí por cables. Pero si la red abarca una región extensa, las conexiones pueden realizarse a través de líneas telefónicas, microondas, líneas de fibra óptica e incluso satélites.

2.2.1.1 Clasificación de una Red:

Se clasifican de 2 formas dependiendo del territorio:

2.2.1.1.1 Redes LAN: Local Area Network. Está constituida por un conjunto de ordenadores independientes interconectados entre sí, pueden comunicarse y compartir recursos. Abarcan una zona no demasiado grande, un edificio o un campus.

Las redes de área local (LAN), se caracterizan principalmente por compartir recursos o distribuir servicios en un área relativamente pequeña, generalmente, en entornos de oficina.

Existen estándares y metodologías para implementar infraestructuras de este tipo, por ejemplo, para que circule la información por un medio físico (cable UTP), no se debe exceder la distancia de 100 metros hasta el medio de difusión (servidor o switch). (Arias Sanchez, 2011)

2.2.1.1.1.1 Aspectos de planeación de una Red LAN (Zuñiga Lopez, 2005)

La buena planeación de una LAN es definitiva para conseguir que atienda satisfactoriamente las necesidades por las cuales se crea. Cuatro aspectos son de importancia para la planeación de redes.

• Determinar las necesidades de la red.

• Decidir sobre una red de punto a punto o basada en servidor.

• Establecer la disposición física de las computadoras en la red e identificar las estaciones de trabajo y los servidores.

• Seleccionar el estándar de red por utilizar y la disposición del cable de red (topología) para conectar los nodos.

2.2.1.1.1.2 Dispositivos de una Red LAN (Principales)

- Switch.- Se puede decir que un switch es un puente multipuerto. Poseen tablas de envío para acordar la entrega de la información. Estos dispositivos trabajan a una velocidad más elevada que un puente. Actualmente, la utilización de switches en un entorno LAN es muy conveniente porque permiten la utilización de segmentos dedicados en un entorno virtual libre de colisiones, lo que maximiza el ancho de banda. Según CISCO un switch es "un dispositivo de red de capa 2 que actúa como punto de concentración para la conexión de estaciones de trabajo, servidores, hubs y otros switches".

También se puede decir que es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network– Red de Área Local).

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo vaya desde el puerto origen al puerto de destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por lo tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

Figura 2.1 Switch Cisco 48 puertos

[Fuente: Cisco Systems, Inc. Academia de Networking. Guía del primer año. CCNA® 1 y 2. Madrid, Pearson Educación S.A., 3ra edición, 2004, página 78.

- Host (NIC).- Toda red LAN la conforman computadoras (hosts), tarjetas de interfaz de red (NIC / Network Interface Card), dispositivos periféricos, medios de red y dispositivos de red.

Una NIC "Es un circuito impreso que proporciona capacidad de comunicación entre computadoras" (System, 2010); sirve de enlace entre un medio físico (cable) y un dispositivo (host). Tiene un número expresado en hexadecimal único llamado dirección MAC que sirve de identificador. La tecnología Ethernet utiliza conectores RJ45. Las tarjetas de red son consideradas dispositivos de capa 2 del modelo OSI (modelo de referencia para una red).

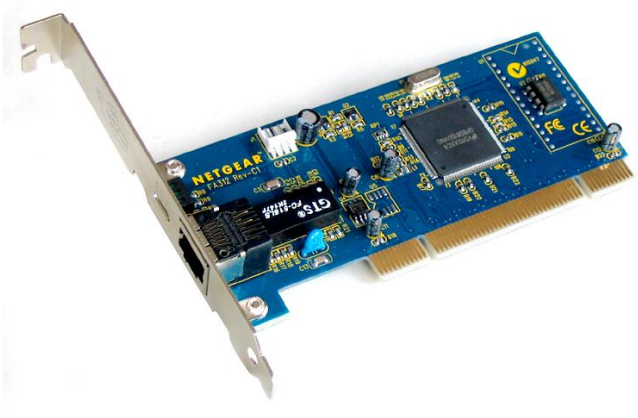


Figura 2.2 Tarjeta de Red

[Fuente: http://www.informaticamoderna.com/Tarjetas_de_red.htm].

- Servidores.- Un servidor es aquel o aquellas computadoras que van a compartir sus recursos hardware y software con los demás equipos de la red. Sus características son potencia de cálculo, importancia de la información que almacena y conexión con recursos que se desean compartir.

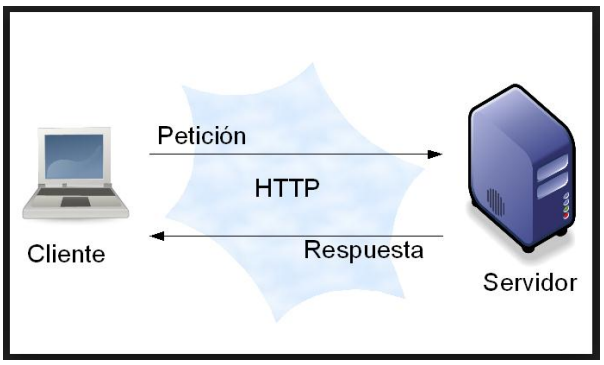


Figura 2.3 Servidores (Sanchez Galiano, 2015)

2.2.1.1.1.3 Topologías de una Red LAN (Garcia Higuera, 2007)

Estas son las topologías más comúnmente usadas:

- Una **topología de bus** usa solo un cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este *backbone*. Su funcionamiento es simple y es muy fácil de instalar, pero es muy sensible a problemas de tráfico, y un fallo o una rotura en el cable interrumpe todas las transmisiones.
- La **topología de anillo** conecta los nodos punto a punto, formando un anillo físico y consiste en conectar varios nodos a una red que tiene una serie de repetidores. Cuando un nodo transmite información a otro la información pasa por cada repetidor hasta llegar al nodo deseado. El problema principal de esta topología es que los repetidores son unidireccionales (siempre van en el mismo sentido). Después de pasar los datos enviados a otro nodo por dicho nodo, continua circulando por la red hasta llegar de nuevo al nodo de origen, donde es eliminado. Esta topología no tiene problemas por la congestión de tráfico, pero si hay una rotura de un enlace, se produciría un fallo general en la red.
- La **topología en estrella** conecta todos los nodos con un nodo central. El nodo central conecta directamente con los nodos, enviándoles la información del nodo de origen, constituyendo una red punto a punto. Si falla un nodo, la red sigue funcionando, excepto si falla el nodo central, que las transmisiones quedan interrumpidas.
- Una **topología en estrella extendida** conecta estrellas individuales entre sí mediante la conexión de concentradores (hubs) o switches. Esta topología puede extender el alcance y la cobertura de la red.
- Una **topología jerárquica** es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.
- La **topología de malla** se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. En esta topología, cada host tiene sus propias conexiones con los demás hosts. Aunque Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.
- La **topología de árbol** tiene varias terminales conectadas de forma que la red se ramifica desde un servidor base. Un fallo o rotura en el cable interrumpe las transmisiones.
- La **topología de doble anillo** es una de las tres principales topologías. Las estaciones están unidas una con otra formando un círculo por medio de un cable común. Las señales circulan en un solo sentido alrededor del círculo, regresándose en cada nodo. El doble anillo es una variación del anillo que se utiliza principalmente en redes de fibra como FDDI es el doble anillo.
- La **topología mixta** es aquella en la que se aplica una mezcla entre alguna de las otras topologías: bus, estrella o anillo. Principalmente las podemos encontrar dos topologías mixtas: Estrella-Bus y

Estrella-Anillo. Los cables más utilizados son el cable de par trenzado, el cable coaxial y la fibra óptica.

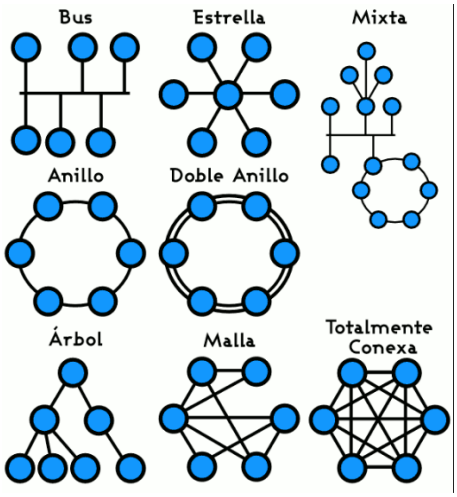


Figura 2.4 Topologías de Red LAN (Garcia Higuera, 2007)

2.2.1.1.1.4 Diseño Jerárquico de una Red LAN

El diseño jerárquico de la red comprende tres capas: (Diane, 2006)

• **Capa de acceso** provee al usuario y a los grupos de trabajo el acceso a los recursos de la red.

• **Capa de distribución** implementa las políticas de la organización y provee las conexiones entre grupos de trabajo y entre los grupos de trabajo y el núcleo.

• **Capa de Núcleo** provee el transporte de alta velocidad entre los dispositivos de la capa de distribución y los recursos del núcleo.

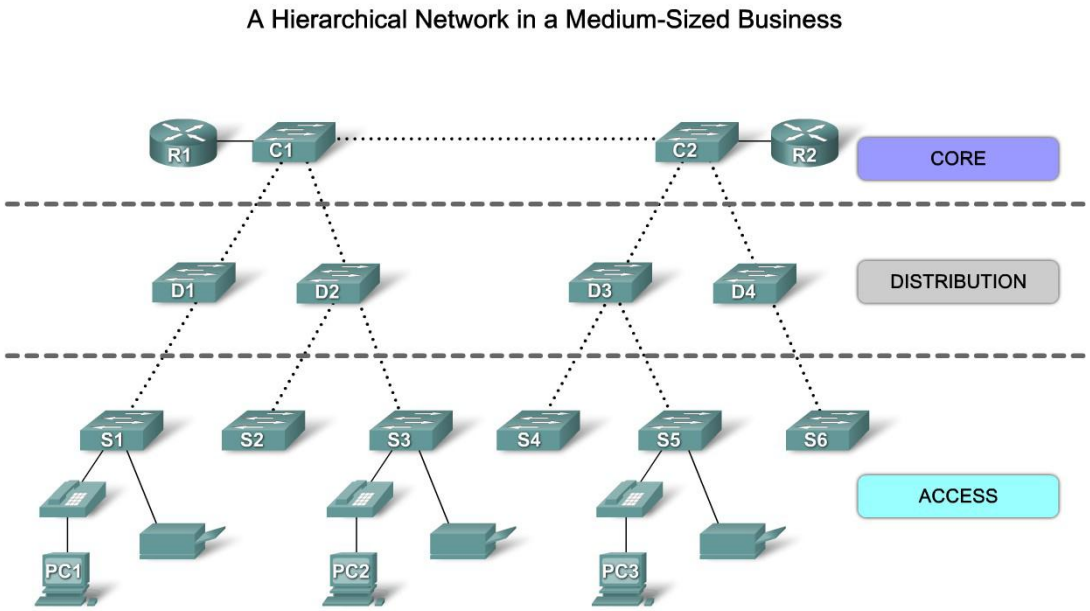


Figura 2.5 Diseño Jerárquico de una Red LAN (Diane, Campus Network Design Fundamentals, 2006)

2.2.1.1.2 Redes WAN: Wide Area Network, comprenden regiones más extensas que las LAN e incluso pueden abarcar varios países.

Se denomina también a las redes de área extensa (WAN), a las LAN separadas por una amplia distancia geográfica conectadas entre sí.

Las redes WAN permiten que las computadoras, impresoras y otros dispositivos de una red LAN compartan y sean compartidas por redes en sitios distantes. Las redes WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. La tecnología de red de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

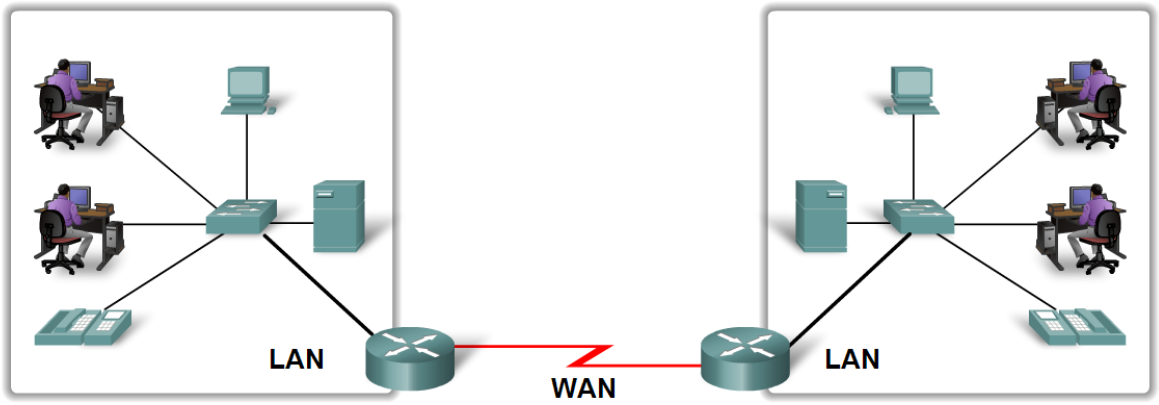


Figura 2.6 Topologías de Red WAN (Garcia Higuera, 2007)

2.2.1.1.2.1 Tipos de Redes WAN

Líneas Dedicadas: Una línea arrendada (leased line), también llamada comúnmente línea privada o dedicada, se obtiene de una compañía de comunicaciones para proveer un medio de comunicación entre dos instalaciones que pueden estar en edificios separados en una misma ciudad o en ciudades distantes. Aparte de un cobro por la instalación o contratación [pago único], la compañía proveedora de servicios le cobrará al usuario un pago mensual por uso de la línea, el cual se basará en la distancia entre las localidades conectadas.

Conmutadas por Circuitos: Redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.

Conmutadas por Mensaje: En este tipo de redes el conmutador suele ser un computador que se encarga de aceptar tráfico de los computadores y terminales conectados a él. El computador examina la dirección que aparece en la cabecera del mensaje hacia el DTE que debe recibirlo. Esta tecnología permite grabar la información para atenderla después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.

Conmutadas por Paquetes: En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, estás insertados dentro de informaciones del protocolo y recorren la red como entidades independientes.

Redes Orientadas a Conexión: En estas redes existe el concepto de multiplexión de canales y puertos conocido como circuito o canal virtual, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.

Redes no orientadas a conexión: Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es INTERNET.

Red Pública de Conmutación Telefónica (PSTN): Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino.

Opción:	Descripción	Ventajas	Desventajas	Rango de ancho de banda	Protocolos muestra utilizada
Línea dedicada	Punto-a-Punto de conexión entre dos ordenadores o redes de área local (LAN)	Lo más seguro	Caro		PPP , HDLC , SDLC , HNAS
La conmutación de circuitos	Un camino circuito dedicado se crea entre los puntos finales. Mejor ejemplo es de acceso telefónico conexiones	Menos Caro	Configuración de llamadas	28-144 kbit /s	PPP , RDSI
La conmutación de paquetes (Conexión orientado)	Dispositivos de paquetes de transporte a través de una compartida única de punto a punto de enlace punto a multipunto o a través de una red interna de soporte. Antes se puede intercambiar información entre dos puntos finales, primero establecer un circuito virtual. Paquetes de longitud variable se transmiten a través de los circuitos virtuales permanentes (PVC) o circuitos virtuales conmutados (SVC)		Los medios compartidos a través de enlace		X.25 , Frame-Relay
La conmutación de paquetes (sin conexión)	Dispositivo de paquetes de transporte a través de una compartida única de punto a punto de enlace punto a multipunto o a través de una red interna de soporte. Paquetes de longitud variable se transmiten. Entre los puntos finales sin conexión es la acumulación; puntos finales sólo pueden ofrecer paquetes a la red, dirigirse a cualquier otro punto final y la red intentará entregar el paquete. A modo de ejemplo: el Internet funciona de esta manera.	Muy robusto y bajo costo operativo	Los medios compartidos a través de enlace		IPv4 , IPv6
Relé celular	Al igual que en la conmutación de paquetes, pero utiliza células de longitud fija en lugar de paquetes de longitud variable. Los datos se divide en celdas de longitud fija y luego transportado a través de circuitos virtuales	Antes de 2000 esto fue visto como la mejor opción para el uso simultáneo de voz y datos. Con las mucho más altas velocidades de enlace en las redes modernas, esta ventaja es efectivamente sin sentido.	*Overhead* puede ser considerable		Cajero automático

Figura 2.7 Tipos de Red LAN (Garcia Higuera, 2007)

2.2.2 Diseño de una Redes de comunicaciones

Debido al reciente surgimiento de la conectividad de redes, es posible creer que se puede instalar una red tan solo adquiriendo sus partes y siguiendo algunas instrucciones que expliquen cómo insertar un conector A en la ranura B y así sucesivamente. En la actualidad es posible comprar las partes y con la ayuda de un manual formar una red.

Sin embargo si está trabajando en una red empresarial o de negocios y si desea empezar adecuadamente es necesario de una planificación, una visión a futuro, aplicar los estándares y pasos básicos fundamentales de la conectividad de redes para construir una red WAN.

En la siguiente Metodología presentada a continuación para el diseño de redes WAN servirá como una guía para remediar la falta de experiencia de un principiante y como una base para los expertos en redes, basada en sus necesidades y expectativas.

La Metodología ha sido desarrollada partiendo de que ya existen redes LAN funcionando correctamente; el proceso para diseñar una Red WAN comprende las siguientes Fases:

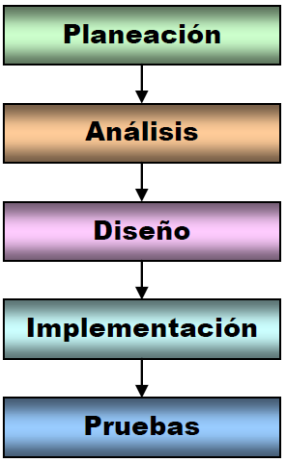


Figura 2.8 Fases para el desarrollo de una red [Fuente: http://repositorio.utn.edu.ec/bitstream/123456789/1095/8/04%20ISC%20005%20RESUMEN%20EJECUTIVO.pdf]

2.2.3 Red Privada Virtual VPN (Virtual Private Network)

Una VPN es una estructura de red que emula una red privada sobre infraestructura pública existente. Brinda comunicación a nivel de las capas 2 ó 3 del modelo OSI. La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a través de la infraestructura de un proveedor de servicios. Esto es posible ya que la tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles sólo en redes privadas.

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

En una VPN de acceso remoto típica gran escala, diferentes usuarios remotos pueden tener diferentes derechos de acceso en la red corporativa privada. (Bidgoli, 2006)

Los paquetes de datos de una VPN viajan por medio de un túnel definido en la red pública. El túnel es la conexión definida entre dos puntos en modo similar a como lo hacen los circuitos en una topología WAN basada en paquetes. A diferencia de lo protocolos orientados a paquetes, capaces de enviar los datos a través de una variedad de rutas antes de alcanzar el destino final, un túnel representa un circuito virtual dedicado entre dos puntos. Para crear el túnel es preciso que un protocolo especial encapsule cada paquete origen a uno nuevo que incluya los campos de control necesario para crear, gestionar y deshacer el túnel. (Velasquez Zeballos & Padilla Diaz, 2006)

Una VPN (Virtual Private Network) es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de encriptación y/o autentificación criptográfica. Una VPN es virtual porque no es físicamente una red distinta, es privada porque la información que transita por los túneles es encriptada para brindar confidencialidad, y es una red porque consiste de computadoras y enlaces de comunicación, pudiendo incluir enrutadores, switches y gateways de seguridad. (Mendoza, 2002)

VPN es una tecnología punto a punto, ampliamente adoptada en ambientes de transacciones corporativas, financieras, y/o redes que requieren confidencialidad permanente, tanto en redes privadas como entre proveedores de Servicio de Internet y sus clientes. En el mercado existe una gran variedad de soluciones

VPN, la Ilustración muestra un ejemplo de interconexión de oficinas sucursales de una corporación, interconectadas vía VPN usando Internet como medio. Cada oficina tiene un Firewall o dispositivo de seguridad que provee una interfaz con Internet y la red interna de la sucursal. Los Firewalls se configuran para definir las políticas de control de acceso para cada oficina. El protocolo de seguridad IPSec es ampliamente utilizado para la implementación de VPN con Firewalls. Más adelante se explicará detalladamente acerca del uso y funcionamiento de los Firewalls y los protocolos de seguridad.

En la figura siguiente se muestra una conexión de la red corporativa a través de una VPN.

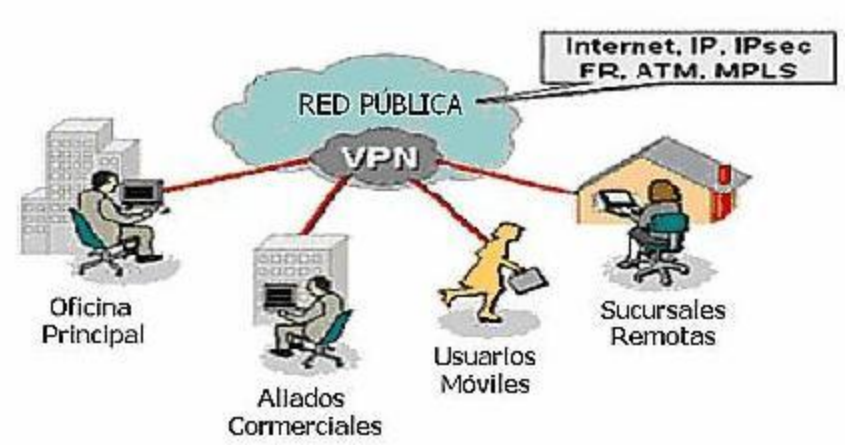


Figura 2.9 Conexión de la Red Corporativa a Través de una VPN (Cisco System, 2001)

Una VPN o Red Privada Virtual es una estructura de red corporativa implantada sobre una red de recursos de transmisión y conmutación públicos, que utiliza la misma gestión y políticas de acceso que se utilizan en las redes privadas. En la mayoría de los casos la red pública es Internet, pero también puede ser una red ATM o Frame Relay. Adicionalmente, puede definirse como una red privada que se extiende, mediante procesos de encapsulamiento y cifrado, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte, la Internet.

Las Redes VPN constituyen una excelente combinación entre seguridad y garantía, y a diferencia de las costosas redes privadas de tipo Frame Relay o X.25 poseen gran alcance, son asequibles y escalables debido a su acceso a través de Internet. Esta combinación hace de las Redes Privadas Virtuales una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier organización.

Las VPN utilizan protocolos especiales de seguridad que permiten, únicamente al personal autorizado, obtener acceso a servicios privados de una organización: cuando un empleado se conecta a Internet, la configuración VPN le permite conectarse a la red privada de la compañía y navegar en la red como si estuvieran localmente en la oficina.

Una de las necesidades vitales de la empresa moderna es la posibilidad de compartir información, particularmente para aquellas empresas que se encuentran dispersas, con sedes en diferentes zonas y unidades de negocio que no se encuentran en el mismo entorno físico.

Hasta el momento, las grandes corporaciones habían solucionado el problema mediante sistemas de comunicación como líneas punto a punto y sofisticadas instalaciones de interconexión. Aunque efectivas, estas soluciones quedaban fuera del alcance de empresas de menor tamaño y con recursos económicos y técnicos más escasos.

La funcionalidad de una VPN está definida más que por el protocolo de transporte, por los dispositivos instalados en sus extremos, encargados de realizar la conexión con los elementos de la red de área local, en los puntos remotos a través de la WAN. Las VPN pueden enlazar las oficinas corporativas con aliados comerciales o asociados de negocio, usuarios móviles y sucursales remotas, mediante canales de comunicación seguros utilizando protocolos como el IPSec (IP Secure).

Los paquetes de datos de una VPN viajan por medio de un "túnel" definido en la red pública. El túnel es la conexión definida entre dos puntos en modo similar a como lo hacen los circuitos en una topología

WAN basada en paquetes. A diferencia de los protocolos orientados a paquetes, capaces de enviar los datos a través de una variedad de rutas antes de alcanzar el destino final, un túnel representa un circuito virtual dedicado entre dos puntos. Para crear el túnel es preciso que un protocolo especial encapsule cada paquete origen en uno nuevo que incluya los campos de control necesarios para crear, gestionar y deshacer el túnel, tal como se muestra en la Figura.

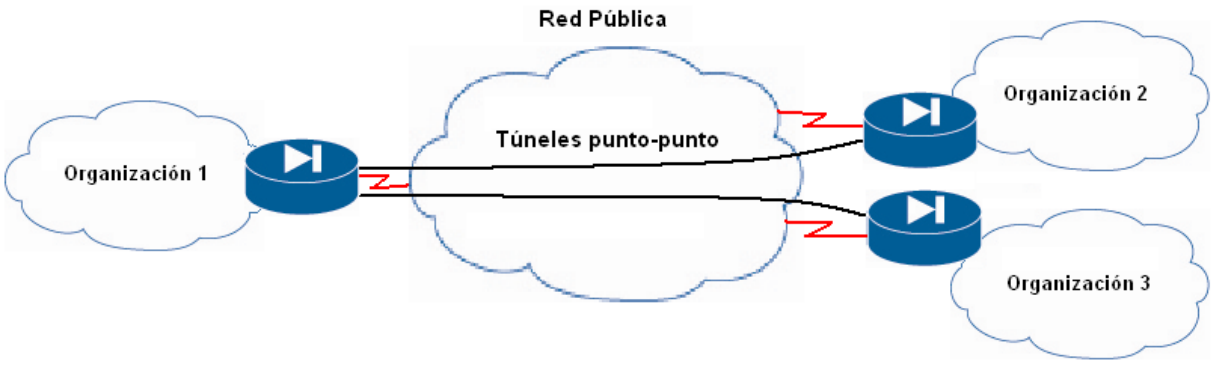


Figura 2.10 Túnel de una VPN (Pepelnjak & Guichard, 2002)

Adicionalmente las VPN emplean el túnel con propósitos de seguridad. Los paquetes utilizan inicialmente funciones de cifrado, autenticación o integridad de datos, y después se encapsulan en paquetes IP (Internet Protocol). Posteriormente los paquetes son descifrados en su destino.

2.2.3.1 Categorías de Redes VPN

Las VPN pueden dividirse en las siguientes categorías:

2.2.3.1.1 VPN de Acceso Remoto

Las VPN de Acceso Remoto permiten conectar a la red corporativa usuarios móviles desde cualquier ubicación, de este modo, el empleado pudiera trabajar desde su casa, desde otra oficina sucursal o desde cualquier otra parte del mundo. El usuario móvil sólo requiere conectarse a Internet, y a través de esta red pública acceder a la red de la empresa, disfrutando de las mismas políticas de seguridad que en la red privada. Las VPN de Acceso Remoto o llamadas también Virtual Private Dial-up Network proporcionan un reducido ancho de banda al usuario y por lo tanto un mínimo tráfico de data, siendo este proporcional al tipo de conexión al medio público los cuales pueden ser sobre líneas analógicas, digitales, RDSI o xDSL.

2.2.3.1.2 VPN de Intranet

Las VPN de Intranet permiten conectar localidades o sucursales fijas de la empresa a la red corporativa usando conexiones dedicadas (Internet de alto rendimiento). Las VPN de Intranet sustituyen la utilización de las WAN en la interconexión de las redes LANs. Empresas trasnacionales que tienen oficinas esparcidas al rededor del mundo, generalmente utilizaban tecnologías costosas de línea alquilada como Frame Relay, T1 o T3. Las VPN de Intranet evitan esto, estableciendo túneles seguros entre cada una de estas ubicaciones. Estos túneles atraviesan realmente la Internet pública de forma transparente a través de los ISP locales.

Nuevas tecnologías como DSL, cable e inalámbrica pueden proporcionar ahora un acceso de alta velocidad con tarifas extremadamente bajas.

2.2.3.1.3 VPN de Extranet

Las VPN de Extranet proporcionan acceso limitado a los recursos de la corporación a sus aliados comerciales externos como proveedores y clientes, facilitando el acceso a la información de uso común

para todos a través de una estructura de comunicación pública, esa es la principal diferencia con las VPN de Intranet que sólo interconectan redes de la misma corporación. Las VPN de Extranet utilizan las mismas tecnologías de las VPN de Intranet enlazando parte de la red local corporativa con sus socios, clientes, y suministradores utilizando una infraestructura compartida a través de conexiones dedicadas. Otra forma de visualizarlo sería en imaginar que las Extranets son Intranets que proporcionan un acceso limitado a sus clientes, y socios. También las VPN de Extranet permiten el acceso autorizado de usuarios móviles constituyendo una herramienta que fortalece la comunicación de la empresa y que brinda muchas ventajas.

En la figura podemos observar las diferentes categorías de redes VPN. El usuario móvil y la oficina en casa representan la VPN de acceso remoto. La interconexión de la oficina principal con la secundaria representa a una VPN de Intranet y si a esta interconexión le sumamos el socio comercial entonces claramente se representa la VPN de Extranet.

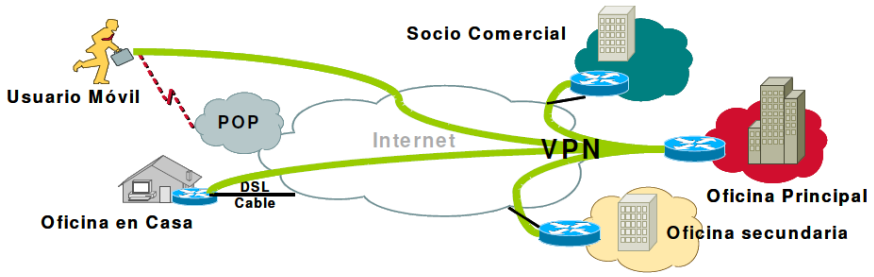


Figura 2.11. Categoría de Redes VPN (Pepelnjak & Guichard, 2002)

2.2.3.2 Tipos de VPN según su Implementación

Las VPN se pueden implementar de diferentes y variadas formas. Mediante Hardware especializados, Software que emulen dichos Hardware, modernos Firewall que poseen como función intrínseca la de establecer enlaces de túneles VPN. Cada una tiene sus ventajas y desventajas dependiendo de su utilización.

2.2.3.2.1 VPN mediante Software

Este tipo de VPN se implementa mediante la ejecución de un Software sobre una plataforma PC, Servidor o Workstation. Estos Software son desarrollados para correr sobre diferentes Sistemas Operativos, ya sea Windows 9x, ME, NT, 2000, XP Unix, o Linux, y desempeñan todas las funciones y manejo de protocolos de una VPN de Hardware especializado: la autentificación, encriptación, enlace y manejo de la data.

Una VPN mediante Software es adecuada para establecer un enlace VPN a un usuario móvil que desee conectarse a la red corporativa para consultar una base de datos utilizando su computadora personal desde un lugar remoto utilizando una conexión lenta dial up; en la oficina principal pudiera preferiblemente atender el llamado a conexión VPN un Hardware especializado para el manejo de redes VPN, así como también lo pudiera atender un Software corriendo en el servidor, todo depende del rendimiento que se desee.

Los PCs, servidores o workstations no son Hardware diseñado específicamente para el manejo de VPN, además pudieran encontrarse corriendo otras aplicaciones que utilicen sus recursos de procesamiento limitando su rendimiento, por esta razón su desempeño sería proporcional a varios factores tales como la velocidad de procesador, dedicación de sus recursos a los procesos de enlace de la VPN vs. los demás procesos, y el número de aplicaciones corriendo en el computador. Por esta razón la implementación de VPN mediante Software es ideal para enlaces móviles en donde no se requiera manejos de grandes cantidades de data y no en oficinas principales donde se adecua la utilización de un Hardware especializado.

2.2.3.2.2 VPN mediante Hardware

Los sistemas basados en hardware son routers que encriptan. Son seguros y fáciles de usar, simplemente hay que conectarlos. Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido, y de fácil instalación.

2.2.4 Calidad de Servicio (Robles, 2008)

Hace un tiempo atrás, los usuarios no encontraban muchos servicios disponibles en las redes de datos. Con el transcurso de los años, la oferta de servicios por parte de las redes se ha ido incrementando. Hoy en día, las redes de datos son usadas para acceder a información estática y/o dinámica, transmitir voz y video, realizar compras, etc. Obviamente, estas acciones generan diferente tipo de tráfico que debe recibir distinto tratamiento por parte de la red.

Calidad de Servicio (QoS, Quality of Service) es un término usado para definir la capacidad de una red para proveer diferentes niveles de servicio a los distintos tipos de tráfico. Permite que los administradores de una red puedan asignarle a un determinado tráfico prioridad sobre otro y, de esta forma, garantizar que un mínimo nivel de servicio le será provisto. Debido al desarrollo de estos nuevos tipos de aplicaciones (streaming, Voz sobre IP, videoconferencia, etc.), la necesidad de implementar técnicas de calidad de servicio se ha vuelto más evidente.

En los últimos tiempos, la capacidad de las redes se ha incrementado considerablemente, a tal punto que en la actualidad la velocidad de muchas redes se llega a medir en gigabit, lo que permite, que si una red presenta problemas de congestión sea muy posible aumentar su ancho de banda. Ésta es una solución simple que, además de ser costosa, puede introducirnos en un círculo vicioso. Podría suceder que después de incrementar el ancho de banda de la red los protocolos que causaron la congestión original, o nuevos tipos de tráficos, consuman el ancho de banda adquirido lo que nos ubica nuevamente en la misma situación experimentada antes del incremento. Una mejor solución sería analizar los distintos flujos de tráficos de la red con el fin de determinar la importancia de cada protocolo y/o aplicación, y así, poder implementar una estrategia para priorizar la utilización del ancho de banda de acuerdo a las necesidades de cada tráfico y/o aplicación.

Dependiendo del tipo de aplicación son los requerimientos que se precisan. Por ejemplo, FTP no es un protocolo críticamente sensitivo a la congestión de la red. Simplemente, la operación tardará un tiempo mayor en realizarse pero no impide que se ejecute correctamente (salvo que la congestión sea tan grande que la conexión de timeout y se aborte). En cambio, las aplicaciones de voz o video son particularmente sensitivas a retardos de la red. Si a los paquetes que componen una comunicación de voz les toma demasiado tiempo en llegar al destino, el sonido o el video resultante estarán distorsionados. Aplicando técnicas de Calidad de Servicio se puede proveer un servicio más acorde al tipo de tráfico.

A continuación se indican algunas de las situaciones en las cuales sería conveniente dar Calidad de Servicio:

• Para dar prioridad a ciertas aplicaciones de nivel crítico en la red

• Para maximizar el uso de la infraestructura de la red

• Para proveer una mejor performance a aplicaciones sensitivas al retardo como son las de voz y video

• Para responder a cambios en los flujos del tráfico de red.

Al aplicar técnicas de Calidad de Servicio, el administrador de la red puede tener control sobre los diferentes parámetros que definen las características de un tráfico en particular, entre los que se encuentran el delay (latencia), jitter (variación en el retardo), packet loss (pérdida de paquetes) y bandwidth (ancho de banda). A continuación se definen cada uno de ellos:

• Delay: es la cantidad de tiempo que tarda un paquete en alcanzar el destino después de ser transmitido desde el emisor. Este periodo de tiempo es conocido como "retardo de fin a fin" (end-to-end delay).

• Jitter: es el cambio de la latencia durante un periodo de tiempo. Indica la variación de tiempo en el arribo entre paquetes debido a las condiciones variables de la red. Por ejemplo, si un paquete tiene 100

milisegundos de latencia y el siguiente paquete tiene una latencia de 130 milisegundos, entonces el jitter es de 30 milisegundos.

• Packet Loss: indica la cantidad máxima de paquetes que puede perder una red. Ésta no puede garantizar que todos los paquetes alcanzarán su destino. En determinados picos de carga, los paquetes serán eliminados por los routers.

• Bandwidth: los distintos tipos de aplicaciones compiten por el limitado ancho de banda. La falta de ancho de banda puede causar retardo, pérdida de paquetes y pobre performance para las aplicaciones.

Si una red estuviese vacía el tráfico de una aplicación debería conseguir cumplir con todos los parámetros anteriores, obtendría el bandwidth necesario, no perdería paquetes y tampoco sufriría delay ni jitter. Pero la realidad es diferente. Existen varias aplicaciones usando la red al mismo tiempo y, por lo tanto, compitiendo por los recursos disponibles.

De los anteriores términos el más difícil de comprender es el Jitter, es por esto que a continuación se muestra un gráfico para ayudar a entender su significado. Los paquetes A y B llegan al destino cada 50 milisegundos pero el paquete C tarda 90 milisegundos, 40 milisegundos más de retardo que los dos paquetes anteriores lo que provoca un jitter de 40 milisegundos.

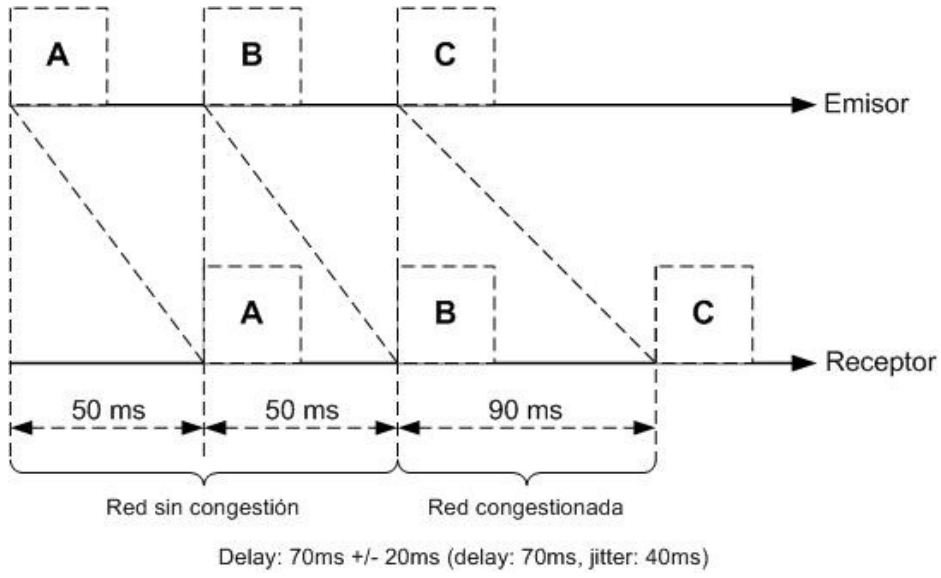


Figura 2.12 Jitter (Robles, 2008)

2.2.4.1 - Modelos de servicios

Las técnicas de Calidad de Servicio pueden ser divididas en tres niveles o modelos de servicios. Estos modelos describen un conjunto de capacidades que provee la red a determinados tráficos desde su origen hasta su destino. Estos niveles son: servicio de mejor esfuerzo, servicios integrados y servicios diferenciados.

2.2.4.1.1 - Servicio de mejor esfuerzo

Éste es el nivel que proveen las redes IP y, por consiguiente, es el modelo que se utiliza en Internet. La red hará todo lo posible por enviar cada paquete hasta su destino, pero no da ninguna garantía de que eso suceda. Una aplicación puede enviar todos los datos que desee en cualquier momento sin solicitar permiso o notificar a la red. Determinadas aplicaciones, como FTP o HTTP, pueden utilizar este modelo sin mayores inconvenientes, pero no es un modelo óptimo para otro tipo de aplicaciones.

2.2.4.1.2 - Servicios integrados

En este modelo se provee, a cada flujo, un nivel garantizado de servicio mediante la negociación de distintos parámetros de red desde el origen al destino. Para esto, la aplicación debe indicar las características del flujo que inyectará en la red y especificar los requerimientos de recursos para el flujo. Los routers que se encuentran a lo largo del camino, entre el origen y el destino, reservan los recursos de

red solicitados antes de que la aplicación empiece a transmitir. Ésta no enviará tráfico hasta que reciba una señal de la red indicándole que puede manejar la carga y proveer la calidad de servicio requerida.

Cuando recibe una solicitud de recursos, la red ejecuta un proceso de control de admisión. Mediante este mecanismo, la red comprueba que está en condiciones de satisfacer los requerimientos solicitados. Si es así, se realiza la reserva de recursos en los routers, que se mantiene hasta que la aplicación termine la transmisión. En caso contrario, la reserva no se puede hacer y se rechaza la conexión.

RSVP (Resource Reservation Protocol) es el protocolo que se encarga de realizar la reserva de los recursos solicitados por la aplicación en forma dinámica. Éste es un protocolo que se desarrolla entre los usuarios y la red, y entre los routers de la red que soportan este protocolo. Tanto la solicitud de reserva de recursos en los routers, como su mantenimiento y cancelación, se hace mediante el intercambio de mensajes de señalización RSVP. En grande entornos esto representaría un considerable tráfico adicional.

Este método tiene la desventaja de que para cada flujo de información que lo requiera es necesario hacer una reserva de recursos en los routers, lo que puede producir que, ante una gran demanda de servicios, un router no pueda satisfacer todos los pedidos. No es una solución escalable, por lo cual no es adecuada para grandes entornos como Internet.

2.2.4.1.3 - Servicios diferenciados

Este método fue concebido para superar los problemas de escalabilidad de Servicios Integrados. Los tráficos ya no se tratan individualmente, sino que se agrupan en diferentes clases que reciben distinto tratamiento por parte de los routers. Los routers de borde son los encargados de marcar los paquetes que entran a la red. El procesamiento que reciban los paquetes dentro de la red depende de la clase en la que fueron ubicados.

El marcado consiste en modificar los primeros 6 bits del campo DS (DiffServ) llamado DSCP (DiffServ Code Point). DS suplanta las definiciones de los campos Type of Service de la cabecera IP y Traffic Class de IPv6. Cada uno de los posibles valores de DSCP puede significar una forma diferente de tratar los paquetes por parte de los routers. A cada una de las formas de tratar los paquetes se lo conoce como Per Hop Behavior (PHB).

Ésta es una solución escalable. El router sólo debe mirar el valor del campo DSCP para decidir como procesar cada paquete. No es necesario mantener un estado por flujo en cada router ni intercambiar tráfico de señalización. La desventaja de este método es que si se agrega una nueva conexión, todos las demás conexiones serán afectadas. Por ejemplo, si hay 10 conexiones atravesando un router y se genera una nueva conexión, el router la aceptará, incluso si sus recursos están saturados, los que, a partir de ahora serán compartidos por las 11 conexiones, introduciendo una posible degradación en la calidad recibida en todas las conexiones. En Servicios Integrados esto no sucede. Una nueva conexión no afecta el rendimiento de las demás conexiones ya establecidas y, si un router no tiene suficientes recursos para satisfacer los requerimientos de aplicación, la conexión se rechaza.

2.2.4.2 - Herramientas de Calidad de Servicio

Las herramientas de Calidad de Servicio que tienen disponibles los administradores de redes se encuentran dentro de las siguientes:

• Marcado y clasificación

• Policing y Shaping

• Control de congestión

• Evitar la congestión

2.2.4.2.1 - Marcado y clasificación

Un paquete que entra en un router primero debe pasar por los procesos de marcado y clasificación. Esto permite diferenciar entre los distintos tráficos y así poder tratarlos de acuerdo a la clase de tráfico a la que pertenecen. Aunque se suelen usar en forma intercambiable, su función es diferente.

Marcado: este paso se encarga de escribir un campo en un paquete con el propósito de distinguir un tipo de paquete de otro. Modifica el campo DiffServ (DS) que ocupa los primeros 6 bits del campo Type of Service en IPv4 y Traffic Class en IPv6. Este paso se realiza en los routers de borde de la red.

Clasificación: el grupo o clase al que pertenecen cada uno de los paquetes depende del valor con el que fueron marcados. Cada uno de esos agrupamientos recibirá un tratamiento diferente, de acuerdo a las políticas que se hayan especificado para cada de una de las clases.

2.2.4.2.2 - Policing and shaping

Estas son dos de las primeras técnicas utilizadas para brindar Calidad de Servicio. El objetivo de estas herramientas es similar, controlar la velocidad a la cual es admitido el tráfico en la red. Aunque la forma de identificar las violaciones de tráfico es similar, la forma en que las resuelven es donde difieren.

Policing: esta técnica, al detectar tráfico excesivo, elimina los paquetes con el fin de mantener los flujos de datos dentro de los límites definidos o los remarca para que tengan menor prioridad. No introduce ningún retardo a los flujos que cumplen con las reglas de policing pero puede provocar más retransmisiones por parte de TCP.

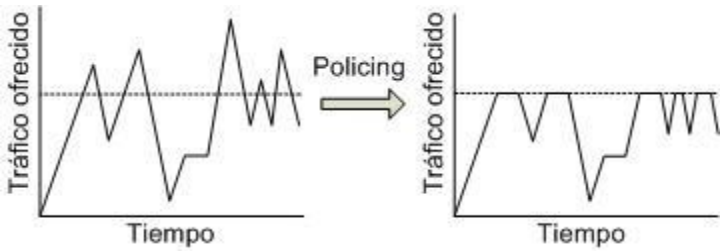


Figura 2.13 Policing (Robles, 2008)

Shaping: esta técnica, a diferencia del policing, no elimina el tráfico excesivo sino que lo aplaza, intentando que no se sobrepase el límite establecido. Lo que hace es poner en un buffer el tráfico excesivo e intenta transmitirlo más tarde cuando su transmisión no exceda el límite acordado. Implica la existencia de colas y suficiente espacio de memoria para mantener los paquetes pendientes.

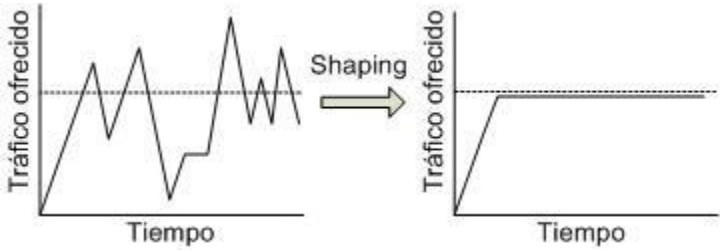


Figura 2.14 Shaping (Robles, 2008)

2.2.4.2.3 - Control de congestión

Existen distintas estrategias de encolado para solucionar el problema que se presenta cuando las aplicaciones, en su conjunto, requieren más ancho de banda del total disponible. Estas estrategias no evitan la congestión pero si permiten que cierto tráfico de red tenga prioridad sobre otro.
Los routers mantienen los paquetes en las colas hasta que tengan suficientes recursos para reenviarlos por el puerto correspondiente, lo que harían inmediatamente si no hubiese congestión. Las colas son usadas para manejar las ráfagas de tráfico que llegan al router más rápido de lo que la interface de salida puede reenviarlas. En un router, las colas son espacio de memoria física lo que implica que su tamaño no es infinito. Sólo pueden contener una cantidad limitada de información (por lo general, el tamaño de las colas es un valor configurable). Los paquetes son ubicados en la cola en el mismo orden en el que arriban.

Si la cantidad de paquetes que se reciben sobrepasan la capacidad de la cola, ésta se desborda y los paquetes no se pueden encolar. Se los descarta. Esto se conoce como tail-drop. Obviamente, los protocolos de las capas superiores lo detectarán y retransmitirán los paquetes eliminados. En un entorno TCP/IP corriendo varias aplicaciones esto puede introducir un problema conocido como "TCP global synchronization" que se muestra en la figura 3.4. Si una cola se llena, los paquetes de las distintas conexiones TCP, que arriben a esa cola, serán descartados. TCP interpretará esto como un error de transmisión y disminuirá el tamaño de su "ventana deslizante" para reducir su velocidad de transmisión. A medida que las próximas trasmisiones sean exitosas irá agrandando esa ventana. Si varias conversaciones TCP acontecen simultáneamente, todas sufrirán el mismo problema e intentarán solucionarlo de igual manera, decrementando su correspondiente ventana y luego incrementándola paulatinamente mientras transmiten exitosamente. Esto podría causar que la interface se vuelva a congestionar y comience a eliminar paquetes de nuevo. Esto será interpretado como un error de transmisión por parte de TCP. Nuevamente, las conversaciones TCP reducirán su ventana de transmisión para disminuir su tasa de transferencia causando una fluctuación en el uso de la red.

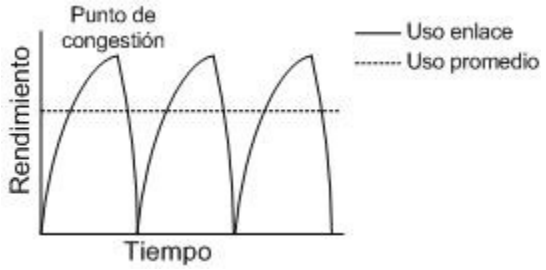


Figura 2.15 TCP Global Synchronization (Robles, 2008)

Además del encolado es importante entender el término *scheduling (planificación)*. Éste es el proceso encargado de determinar cuál es el próximo paquete a transmitirse. Si se tienen varias colas con distintas prioridades el scheduler se encarga de seleccionar de qué cola se enviará el siguiente paquete. Hay varios algoritmos que permiten realizar esta decisión:
• Strict Priority (Prioridad estricta): siempre sirve primero las colas con mayor prioridad. Sólo si éstas están vacías atiende a una de menor prioridad, lo que puede producir inanición.
• Round Robin: las colas son servidas en secuencia. No produce inanición pero puede introducir delay en los tráficos sensitivos al tiempo.
• Weighted Fair: las colas son servidas según su importancia. Los paquetes en las colas son "pesados" (weighted), por ejemplo, por el campo IP Precedence, y las colas con mayor importancia son servidas más frecuentemente. No puede garantizar el ancho de banda que algunos tráficos necesitan pero soluciona los problemas de los dos algoritmos anteriores.

Entre las técnicas de encolado más conocidas se encuentran las siguientes:

• First In First Out (FIFO)
• Priority Queuing (PQ)
• Custom Queuing (CQ)
• Fair Queuing (FQ) / Weighted Fair Queuing (WFQ)

2.2.4.2.3.1 - First In First Out (FIFO)
Éste es el tipo de encolado más simple. Simplemente, el primer paquete que entre en la cola será el primero en ser reenviado. Ninguna clasificación se realiza con los paquetes. El principal propósito es manejar los paquetes entrantes en una interface, ubicarlos en la cola en el mismo orden en el que fueron recibidos, y alimentar la interface saliente a la velocidad constante que la interface puede manejar. No existen las clases de tráficos, todos los paquetes pertenecen a la misma clase. Si se llenan, los buffers empiezan a descartar paquetes (tail-drop). Y esto lo hace con todos los paquetes sin importar la prioridad de los mismos. Además, un flujo muy agresivo puede provocar inanición al transmitir una cantidad de

paquetes que mantenga siempre llena la cola y provoque que los paquetes de las demás flujos sean descartados. Al arribar los paquetes de un flujo en particular, la cola puede estar vacía, con lo cual se reenviarán rápidamente, prácticamente sin delay, o puede estar casi llena lo que provocará que tengan que esperar un tiempo mayor para ser retransmitidos. Esto puede introducir variación en el jitter de la conexión.

2.2.4.2.3.2 - Priority Queuing

Este método, muy fácil de implementar, es una manera estricta de manejar la congestión. Permite definir varias colas y asignarle a cada una un nivel distinto de prioridad. Estas colas son del tipo FIFO y, si se llenan, utilizan el método tail-drop para descartar paquetes. Son procesadas estrictamente por orden de prioridad. Si una cola de mayor prioridad tiene paquetes encolados será procesada hasta que esté vacía, independientemente del estado de las demás colas. Cuando el router termina de procesar una cola de mayor prioridad pasa a la siguiente cola basándose en el nivel de prioridad. Cada vez que se envía un paquete de una cola, el router chequea las colas de mayor prioridad para asegurarse que siguen vacías. Si no es así, el router enviará los paquetes de la cola de mayor prioridad. Este algoritmo es muy bueno en el manejo del tráfico de tiempo real y permite que los tráficos más importantes sean reenviados más rápido. El problema que presenta es que puede producir inanición. Si las colas de mayor prioridad tienen mucho tráfico, los paquetes encolados en las de menor prioridad nunca serán enviados.

2.2.4.2.3.3- Custom Queuing

Para solucionar el problema de inanición presente en el método anterior se introdujo Custom Queuing o Class-Based Queuing. Este método permite definir varias colas, tipo drop-tail, que son atendidas en forma round-robin, asegurándose que todas las colas tengan su oportunidad de transmitir. Cada cola sólo puede enviar una cantidad máxima de bytes, no paquetes, por turno. La prioridad de una cola está dada por la cantidad de bytes que es capaz de enviar por turno. El último paquete siempre es enviado en su totalidad aun si la cantidad total de bytes enviados en el turno supera el máximo permitido para la cola. Aunque no es posible la inanición, sí puede suceder que se le asigne un ancho de banda tan grande a una cola (o más de una) que implique que las colas de menor prioridad no puedan obtener el ancho de banda necesario. Cuando esto sucede, las aplicaciones con datos en estas colas (las de menor prioridad) pueden dar timeout. Esto provoca que las aplicaciones no puedan funcionar en forma apropiada y tiene los mismos efectos que la inanición.

2.2.4.2.3.4- Fair Queuing (FQ) / Weighted Fair Queuing (WFQ)

El método Fair Queuing es otro método para crear distintas clases de tráficos. También se lo conoce como encolado por flujo o basado en flujo. Los paquetes entrantes son clasificados en N colas y, a cada cola, se le asigna 1/N del ancho de banda de la interface de salida. El scheduler visita las colas en forma round-robin, salteando las que están vacías. Es simple de implementar, no requiere un mecanismo especial de asignación de ancho de banda. Si se agrega una nueva cola, para crear un nuevo tráfico, el scheduler, automáticamente, ajusta el ancha de banda de las colas de salida a 1/(N + 1).

El problema que presenta esta solución es que si algún tráfico necesita mayor ancho de banda no tiene forma de poder cumplir con ese requerimiento. Otro problema que presenta es que un paquete entero es transmitido por cada ciclo y el tamaño de los paquetes impactará la distribución del ancho de banda. Una cola con paquetes de mayor tamaño conseguirá más ancho de banda que otra con paquetes de menor tamaño aunque las dos envíen la misma cantidad de paquetes.

Con la idea de solucionar este problema surge Weighted Fair Queuing. Ésta es una generalización del método Fair Queuing. En vez de asignar el ancho de banda de salida en forma proporcional a cada clase, lo hace de acuerdo a sus requerimientos de ancho de banda. Para poder diferenciar los distintos requerimientos de cada flujo (o cola) se les asigna un peso (weight). Este peso controla el porcentaje de ancho de banda que recibirá cada flujo. Usando el campo ToS (Type of Service), de la cabecera IP, podemos indicar el peso.

2.2.4.2.4 - Evitar la congestión

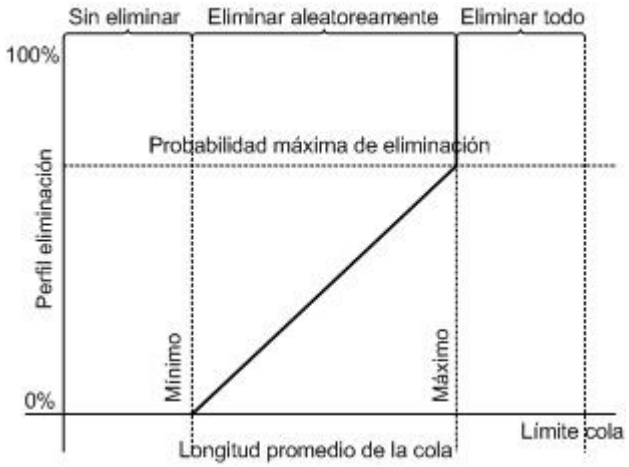
Los métodos anteriores no intentan evitar la congestión sino que mediante la definición de distintas reglas, priorizan un tráfico sobre otro, es decir, administran la congestión una vez que se produjo. Existen otras técnicas que intenta evitar que se produzca una congestión en la red eliminando paquetes de flujos TCP cuando detecta que se está alcanzando un estado de congestión. El propósito de estos métodos es indicarle a los protocolos end-toend, como TCP, que en algún punto, la red se está empezando a congestionar. Se busca que TCP disminuya la velocidad de transmisión en un conjunto random de flujos antes de que la congestión se torne severa y se eliminen paquetes de todos los flujos, como lo haría tail-drop. Entre esas técnicas se encuentran:

• Random Early Detection (RED)
• Weighted Random Early Detection (WRED)

2.2.4.2.4.1 - Random Early Detection (RED)

Este mecanismo descarta paquetes, en forma aleatoria, antes de que se produzca la congestión. No espera a que se llenen los buffers para empezar a descartar, como hace tail-drop, con lo cual evita problemas presentes en este método como "TCP global synchronization". Debe medir constantemente la ocupación de los buffers para empezar a descartar una vez que se superó un umbral predeterminado. El umbral, en el cual RED empieza a descartar paquetes, es un valor configurable. Si el buffer está casi vacío, todos los paquetes entrantes son aceptados y reenviados normalmente. Pero si el tamaño de la cola crece, la probabilidad de eliminar los paquetes entrantes también crece.

A continuación se muestra un gráfico donde se detalla el funcionamiento de este método.



Figurax.2.16 – Funcionamiento del método RED (Robles, 2008)

Cuando la longitud de una cola excede el umbral mínimo el router empieza a descartar paquetes en forma aleatoria. Si se alcanza el máximo tamaño de la cola, se descartan todos los paquetes.

2.2.4.2.4.2- Weighted Random Early Detection (WRED)

Ésta es una mejora al método RED. La selección de los paquetes a ser eliminados no es tan aleatoria como en RED, sino que se introduce un grado de influencia en esa selección. Se utiliza un peso, el campo IP Precedence, para determinar que paquetes descartar. En general, WRED descarta primero los paquetes con un valor menor en ese campo. De esta forma, los tráficos con prioridad superior son enviados con una mayor probabilidad que los tráficos menos prioritarios.

A simple vista, las técnicas de evitación de congestión parecen ser la solución a todos los problemas de congestión de una red. Sin embargo, presentan algunas desventajas. En primer lugar, sólo trabajan con

conexiones TCP. Por ejemplo, IPX no trabaja con el concepto de "ventana deslizante", por lo tanto, si se descartan paquetes pertenecientes a este protocolo la retransmisión será a la misma velocidad que antes del descarte. Tanto RED como WRED son ineficientes en una red con protocolos distintos a TCP. Otra desventaja es que los paquetes son eliminados directamente, no los encola.

2.2.5 Protocolo BGP

2.2.5.1 Definición

El protocolo Border Gateway Protocol (BGP) se estableció como un estándar de Internet en 1989 y fue definido originalmente en la RFC_1105, adoptándose como un protocolo para la comunicación entre dominios dentro de la comunicación EGP. La versión actual es la BGP-4, que se adoptó en 1995 y ha sido definida en la RFC 1771. BGP-4 soporta CIDR (Classless Inter Domain Routing) y es el protocolo de enrutamiento que actualmente se usa de forma mayoritaria para encaminar la información entre sistemas autónomos, ya que ha demostrado ser fácilmente escalable, estable y dotado de los mecanismos necesarios para soportar políticas de encaminamiento complicadas. A partir de ahora cuando se nombre al protocolo BGP, se está haciendo mención de la versión BGP-4.
BGP continúa desarrollándose a través del trabajo del proceso de los estándares de Internet en el IETF. Como los requisitos del encaminamiento de Internet cambian, el protocolo BGP se extiende para continuar proporcionando mecanismos que controlen la información de encaminamiento y soporten los nuevos requisitos. Por eso, la RFC básica ha sido extendida por varias RFCs posteriores. (Teldat, 2008).

2.2.5.2 Mecanismos del Protocolo

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

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

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

2.2.5.3 Criterio de Selección de Rutas

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

a) Preferencia (Distancia administrativa)

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

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

Tabla 2.1 *"Distancia administrativo"* (Teldat, 2008)

b) Preferencia (tie-breaker)
   El parámetro Preferencia2, también llamado tie-breaker, sirve para resolver casos de conflicto entre dos rutas de la misma Preferencia.
c) Métrica (MULTI_EXIT_DISC)
   La Métrica indica el coste de la ruta, y sólo es comparable entre rutas de un mismo protocolo o. El significado de la métrica se define para cada protocolo. Por ejemplo, en RIP indica el número de saltos hasta el destino. La Métrica en BGP hereda el valor del atributo MULTI_EXIT_DISC.
d) Métrica2 (LOCAL_PREF)
   Este parámetro en BGP hereda el valor del atributo LOCAL_PREF. Si no se ha asignado ningún valor (se muestra -1) se considera de máxima preferencia.
e) AS-path
   En una ruta aprendida por BGP el AS-path indica a través de qué Sistemas Autónomos se ha aprendido dicha ruta.
f) Eligiendo una ruta
   El protocolo BGP utiliza las siguientes reglas para elegir la mejor ruta o salto a un determinado destino.
   La ruta con la menor Preferencia (Distancia Administrativa) es la elegida. Si dos rutas tienen la misma Preferencia, se elige la ruta con la menor Preferencia2.
   Si las dos rutas se han aprendido por BGP se aplican los siguientes criterios:

   - Se prefiere la ruta con mayor Métrica2 (LOCAL_PREF). Si no se ha asignado valor de Métrica2 (aparece –1) se considera el valor máximo.
   - Una ruta con información de AS-path es preferida frente a otra sin AS-path.
   - Entre dos rutas con AS-path, provenientes del mismo AS, y con información de Métrica, se prefiere aquella que tiene menor valor de Métrica (MULTI_EXIT_DISC).
   - Entre dos rutas con AS-path distintos, se prefiere la de origen IGP, y si no la de origen EGP.
   - Entre dos rutas con AS-path distinto y con mismo origen, se prefiere la de AS-path de menor longitud.

- Una ruta aprendida desde IGP es preferida a una aprendida desde EGP. La ruta menos preferida es la que se obtiene indirectamente de un IGP que la ha obtenido de un EGP.
- Si ambas rutas se aprendieron del mismo protocolo y el mismo AS, se usa la que tenga la menor Métrica.
- Se prefieren las rutas instalables en la tabla de rutas activas del equipo frente a las rutas no instalables.
- Se prefiere la ruta que tenga siguiente salto con el valor de dirección IP más bajo.

En la Figura siguiente muestra este proceso de forma esquemática.

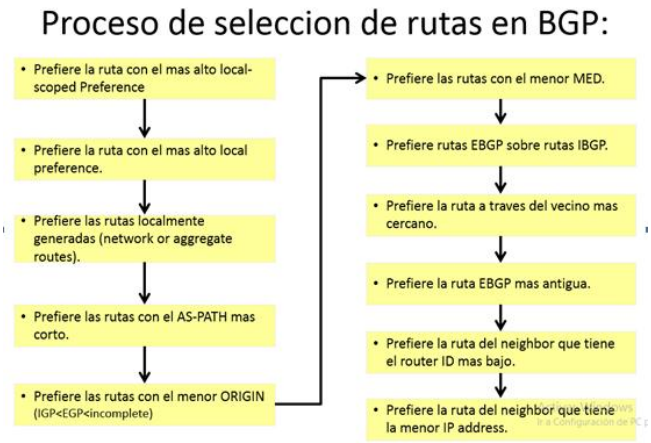


Figura 2.17 Selección de rutas, Fuente "Capacitación CLARO"

2.2.6 Protocolos de redundancia de primer salto.

2.2.6.1 Definición

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

2.2.6.2 HSRP (protocolo de router de respaldo de salto)

Cuando se usa HSRP y STP a la vez, hay que tener en cuenta que el switch activo de HSRP sea el mismo que el switch root Bridge de STP, así nos evitamos problemas de bucles. Esto lo logramos poniendo a ese switch una prioridad HSRP mayor que la de los demás switchs del grupo (Dan, 2016). La figura siguiente muestra un escenario con HSRP:

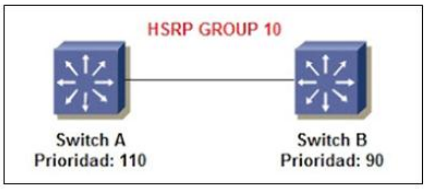


Figura 2 18 Escenario HSRP
Fuente "CCNP SWITCH" (Pérez, D. 2013)

2.2.6.3 VRRP (Protocolo de redundancia de router virtual)

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

- HSRP es propietario de Cisco, VRRP es un IEEE estándar.
- En HSRP se pueden configurar 16 grupos como máximo, en VRRP 255.
- HSRP usa un switch como activo y otro como standby, VRRP usa un switch como master, y todos los demás como backups.
- Los tiempos de hello y holdtime son más cortos en VRRP.
- VRRP soporta encriptación en la autenticación (HMAC/MD5)

Cuando el switch que esta como master cae, uno de los que está en backup toma el rol de master, para determinar que switch toma el control, se lleva a cabo un cálculo entre todos ellos en los que entran en juego diferentes intervalos de tiempo. En definitiva, todos los switchs hacen un cálculo, y a el que menos tiempo le dé, es el primero en enviar paquetes al resto de switchs, por lo cual se convierte en master,
Los intervalos de tiempo de hello también se pueden configurar en VRRP, a diferencia de HSRP, en VRRP se configuran en el master y los backups aprenden esos intervalos del master. (Pérez, D. 2013). La figura siguiente muestra un escenario con VRRP.

.

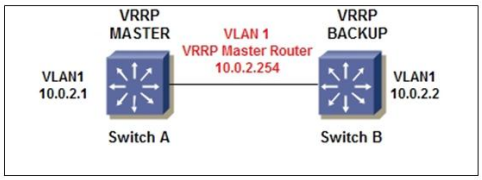


Figura 2 19 Escenario VRRP
Fuente "CCNP SWITCH" (Pérez, D. 2013)

2.2.6.4 GLBP (protocolo de balanceo de carga de salida) (Pérez, D. 2013)

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

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

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

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

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

Si algún switch cae, su MAC virtual es asignado a otro switch, de tal forma que algún switch tendría más de una MAC virtual, de esta manera no hay equipos que se queden sin red.

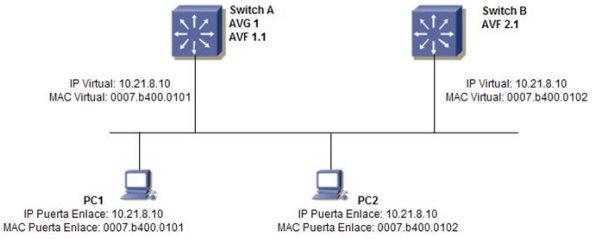


Figura 2.20 Escenario GLBP.
Fuente "CCNP SWITCH" (Pérez, D. 2013)

2.3. Glosario de términos

Ancho de banda La capacidad de información de un sistema de telecomunicaciones hace referencia a la cantidad de información generada en la fuente que pede pasar al sumidero por unidad de tiempo. Precisamente la capacidad de información de un sistema de telecomunicaciones está dada por el ancho de banda en el canal. (Castro Lechtaler & Fusario, 2010)

QoS (Quality of Service) Es definida como "Si determinadas aplicaciones no son sensibles al retardo o fluctuaciones de retardo (correo electrónico, web o transferencia de archivos), mientras que otra si lo son (voz y video), si se diferenciara el trafico da cada una de ellas, la red podría ofrecerles un tratamiento distinto, satisfaciendo de esa forma las distintas necesidades sin aumentar cosiderablemente el costo de la red." (Carballar Falcón, 2007)

Broadcast La dirección de broadcast (la que hace referencia a todos los nodos de la red) se obtiene tomando los bits de la dirección IP que están a 1 en la máscara y dando valor 1 al resto, es decir, a los bits del identificador de host. (Barbancho Concejero & Benjumea Mondejar, 2014)

Cable de fibra óptica Medio físico capaz de conducir una transmisión de luz modulada. Comparado con otros medios de transmisión, el cable de fibra óptica es más costoso, pero no es susceptible a la interferencia electromagnética y es capaz de mayores velocidades de datos. Llamado a veces fibra óptica. "La fibra Óptica (F.O.) es el medio de transmisión del presente y del futuro. Sustituye muy ventajosamente a los cables (de pares, coaxiales, etc.). Tiene como ventajas: Mucho menor peso, gran ancho de banda, Atenuación muy pequeña, inmune a las interferencias electromagnéticas, diafonía y otros fenómenos electromagnéticos." (Carmelo Fernandez Garcia & Barbado Santana, 2008)

Ethernet Especificación de LAN de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y corren por una variedad de tipos de cable a 10 Mbps. Ethernet es similar a la serie de normas IEEE 802.3.
"Protocolo de comunicación por el que se rigen los equipos que trabajan en redes cableadas, también conocido como estándar IEEE 802.3." (Bermudez Luque & Bermudez Luque, 2016)

CSMA/CD Se focaliza en tres funciones transmitir-recibir, decodificar y detectar paquetes de datos. Es un método de difusión de medio compartido, es decir, antes de transmitir primero detecta un flujo

portador, si dos host transmiten al mismo tiempo, se produce una colisión que se manifiesta por el aumento de la amplitud de la señal, una vez que toda la red a detectado la colisión, cada host ejecuta un algoritmo de retardo que permite intentar la transmisión nuevamente; si persiste la colisión se aborta la transmisión. (Arias Sanchez, 2011)

Fast Ethernet Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de Frame, mecanismos MAC y MTU.
"Un desarrollo posterior de Ethernet (10 Mbits/s) se denomina Fast Ethernet y está diseñado para transmitir 100 Mbits/s. La ultima variante de Ethernet es Gigabit-Ethernet, que puede proporcionar un máximo de 1000 Mbits/s. Todas las variantes de Ethernet se basan en el procedimiento CSMA/CD por lo que pueden ser compatibles entre sí" (Dembowski, 2033)

Internet Internet hace referencia a un sistema global de información que está relacionado lógicamente por un único espacio de direcciones global basados en el protocolo de Internet o en sus extensiones, es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles con IP, y emplea, provee o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas aquí descritas. (Holgado Saez, 2016)

IP "El IP, protocolo de Internet, provee los procedimientos y reglas que definen la transmisión de paquetes dados, es decir, la fragmentación y el ruteo (medio de encaminar paquetes) de los datos a través de la red. La versión actual es IPv4 mientras que en Internet2 se intenta implementar la versión 6 (IPv6). Que permitirá mejores prestaciones dentro del concepto QoS (Quality of Service). Frecuentemente se usan las siglas IP para referirse al número o la dirección IP" (Redón Gómez, 2007)

IPsec Trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme. IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP). Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión. Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación. Por autenticidad se entiende por la validación de remitente de los datos. Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo. (Cubas Diaz & Perales Fabian, 2011)

Router Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red. Los router envían paquetes de una red a otra en base a la información de capa de red. (Vaucamps, 2011)

Capítulo 3: Variables e Hipótesis

3.1. Variables e Indicadores

a. Identificación de Variables

- Variable Independiente:

  Diseño de una Red Privada Virtual VPN.

- Variable Dependiente:

  Optimización de la comunicación.

b. Operacionalización de Variables

- Indicadores Variable Independiente

  - Funcionalidad.- Cumplir con la finalidad de compartir información.
  - Confiabilidad.- Es una medida de la probabilidad de falla.
  - Seguridad.- Indica el grado de seguridad de la red incluyendo los datos transmitidos.

- Indicadores Variable Dependiente:

  - Evaluaciones o pruebas
  - Inspecciones en cableado
  - Equipos de Red
  - Infraestructura de Red (medios)

3.2. Hipótesis

- Hipótesis General:

  El diseño de una Red privada virtual influirá en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.

- Hipótesis Específicas:

  - El nivel de funcionalidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.

  - El nivel de confiabilidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.

  - El nivel de seguridad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.

Capítulo 4: Metodología de Desarrollo

A continuación se muestra lo que es la metodología Cisco desarrollado en este proyecto:

4.1. Metodología CISCO

Nuestra realidad ha cambiado. Hoy la red pasa a ser un componente esencial y estratégico, lo que hace indispensable el asegurar una alta disponibilidad, así como también las mejores condiciones de seguridad y confiabilidad. Para llevar la red a este nivel se requiere conocimiento especializado y experiencia, específicamente para las nuevas tecnologías que incluyen seguridad, voz, redes inalámbricas y almacenamiento.

Para asegurar el aprovechamiento óptimo de la red, es esencial que esté funcionando a su máximo desempeño y que esté ciento por ciento disponible para entregar el más alto nivel de calidad de servicios. Para hacer crecer el negocio y entregar la siguiente generación de servicios, la red debe evolucionar hacia nuevos servicios IP, los cuales crean una plataforma de red convergente para soportar comunicaciones de datos, voz y video.

La Metodología CISCO soporta la evolución de la red hacia sistemas de negocios y ayuda a las empresas a incrementar el retorno de inversión en estas tecnologías.

Esta Metodología se define el conjunto mínimo de actividades necesarias, por tecnología y por nivel de complejidad de la red, para ayudar a los clientes a instalar y operar exitosamente tecnologías de Cisco, y optimizar su desempeño a través del ciclo de vida de la red.

4.1.1 Beneficios de la Metodología CISCO

- Incrementa el valor de la red en la gestión de negocios y el retorno de inversión y coloca al cliente en una posición ventajosa al disminuir el costo total de propiedad de la red, mejorando ambos: la agilidad del negocio y la disponibilidad de la red.
- Acelera la estrategia de penetración del mercado (go-to-market) al entregar soluciones a tiempo, dentro del presupuesto, y a un precio competitivo a través de una metodología comprobada y consistente que enfatiza la coordinación entre Cisco, sus socios de negocios y las capacidades de los clientes.
- Mejora la disponibilidad, estabilidad, seguridad y escalabilidad de la red a través del sistema de planeación, diseño, mantenimiento y optimización.
- Maneja la complejidad creciente de la red al proveer consistencia en los procesos para instalar y mantener la tecnología de Cisco Systems.

4.1.2 Fases

4.1.2.1 Fase de Planificación

En este punto se presenta una descripción detallada de las problemáticas y la propuesta del grupo de proyecto sobre cómo pueden trabajar contra dicha problemática.

En esta fase se recopila información necesaria para el diseño de una Red Wan:

- Propósito Organizacional
- Necesidades de la Organización
- Ubicación Geográfica (Sucursales y oficinas)
- Tipos de Redes existentes en la Organización, etc.

4.1.2.2 Fase de Diseño

Se desarrolla lo siguiente:

- Diseño Lógico de la Red Wan
- Elabore un diagrama lógico de la red y bosquejo general del diseño.
- Primera Alternativa de Diseño
- El diagrama físico de la red no es muy complicado, por lo que se opta por realizar las alternativas de diseño físico factibles, en donde se especifica: protocolos, medios de comunicación, equipos de comunicación y el grado de centralización de la red WAN. Para el diseño de la red WAN se debe generar una tabla de información detallada con nombre del nodo, medio de comunicación, protocolo, equipos de comunicación y proveedores.
- Análisis Costo / Beneficio
- Se debe generar una tabla de costos de los medios y equipos de comunicación que se utilizara en el diseño o seleccionar la mejor alternativa. Aquí se deberá evaluar mediante un cuadro comparativo de todas las alternativas generadas anteriormente.

4.1.2.3 Fase de Implementación

La Red es construida de acuerdo al diseño aprobado.
Se hace el desarrollo del diseño físico y lógico de la red completa, permite la integración de los equipos sin interrumpir la red existente, sin crear puntos de vulnerabilidad en el proceso.

4.1.2.4 Fase de Operación

La Red es puesta en operación y es monitoreada. Esta fase es la prueba máxima del diseño.

Esta fase mantiene el estado de la red día a día. Esto incluye administración y monitoreo de los componentes de la red, mantenimiento de ruteo, administración de actualizaciones, administración de performance, e identificación y corrección de errores de red.

4.1.2.5 Fase de Optimización

Esta fase envuelve una administración pro-activa, identificando y resolviendo errores antes que afecten a la red. Esta fase puede crear una modificación al diseño si demasiados problemas aparecen, para mejorar cuestiones de performance de nuestra Red.

Capítulo 5: Solución Tecnológica

Para el desarrollo de este proyecto se utilizó la metodología CISCO ya que cuando se trabaja en una Red empresarial o de Negocios es necesario empezar adecuadamente utilizando metodologías actuales y de uso continuo que muestren resultados óptimos. Para ello fue necesario: una buena planificación, una visión a futuro, aplicar los estándares y pasos básicos fundamentales de la conectividad de redes para construir una red WAN.

5.1. Fase de Planificación

En este punto se presentó una descripción de las problemáticas y de cómo se puede trabajar contra dicha problemática.
En esta fase se recopiló información necesaria para el diseño de una Red WAN:

5.1.1 Propósito Organizacional

La Organización tiene como propósito consolidarse en su nueva sede de Trujillo como la mejor alternativa en la compra de productos y de servicios informáticos para todos sus clientes en esta nueva sede.

5.1.2 Necesidades de la Organización

La principal necesidad de la Organización fue la comunicación con esta nueva sede, es decir comunicación informática en tiempo real entre la sede principal (Lima) y su sede remota (Trujillo) a través de una VPN la que será solicitada al proveedor de servicios Claro.

5.1.3 Ubicación Geográfica (sucursales, oficinas)

La Empresa Comunicaciones e Informática SAC es una organización empresarial constituida en Lima – Perú el 25 de marzo del 2014, tiene como sede principal en la Av. Circunvalación Golf Los Incas 154 Of. 1501 Edificio Capital El Golf Piso 15 en la ciudad de Lima distrito de Santiago de Surco y una nueva sede en Jr. Independencia 475, Plaza de Armas, Trujillo.

5.1.4 Tipos de Redes existentes en la organización

La Empresa Comunicaciones e Informática SAC no contaba con sedes remotas (WAN) por lo que en la sede principal solo contaba con una red LAN dividida en 2 segmentos de red es decir 2 Vlan una Red 192.168.20.0 mascara 24 para los datos y la Red 192.168.21.0 mascara 24 para Voz y video. Cuenta con el servicio de Internet brindado por Claro.

5.1.5 Requerimientos de ancho de banda para las clases de servicio

Los datos de requerimientos de ancho de banda para la VPN y la cantidad de espacio distribuida para cada clase de servicio, fueron proporcionadas por los ingenieros residentes de "Comunicaciones e Informática SAC" quienes dan soporte a su red, estos datos se describen en la tabla 5.1 y 5.2 para la VPN implementada y fueron solicitados de acuerdo a la sección 2.2.3 CALIDAD DE SERVICIO donde especifica cómo deben venir marcados los paquete (valor de DSCP en el campo de servicio diferenciado del encabezado IP) y que redes o IPs deben pertenecer a qué clase de servicio para que sean marcados y aplicar las políticas a realizar frente a una congestión de tráfico.

ITEM	COS5(clase de servicio)	COS2(clase de servicio)	COS1(clase de servicio)	Total ancho de banda
TIPO DE TRÁFICO	voz	Datos críticos	Datos transacciones	
PRIORIDAD	Máxima	Máxima	Normal	
IP DSCP	Cs5	Cs2	Cs1	
ANCHO DE BANDA	128kbps	384kbps	512kbps	1024kbps
POLITICA APLICABLE AL TRAFICO EXC	Se descarta	Se remarca como P1	No aplica	
APLICACIONES	Telefonía IP	Aplicaciones de Datos críticas para el negocio como el tráfico generado por la caja registradora	Datos de aplicaciones de negocio, intranet.	
Al tráfico de que red es aplicado.	192.168.21.254 hacia el destino 192.168.100.254	Desde cualquier origen a los servidores.	Trafico restante.	

Tabla 5.1 Requerimiento de ancho de banda la para red en la sede principal de "Comunicaciones e Informática". Fuente: Creación propia

ITEM	COS5(clase de servicio)	COS2(clase de servicio)	COS1(clase de servicio)	Total ancho de banda
TIPO DE TRÁFICO	voz	Datos críticos	Datos transacciones	
PRIORIDAD	Máxima	Máxima	Normal	
IP DSCP	Cs5	Cs2	Cs1	
ANCHO DE BANDA	64kbps	96kbps	128kbps	288kbps
POLITICA APLICABLE AL TRAFICO EXC	Se descarta	Se remarca como P1	No aplica	
APLICACIONES	Telefonía IP	Aplicaciones de Datos críticas para el negocio como el tráfico generado por la caja registradora	Datos de aplicaciones de negocio, intranet.	

Al tráfico de que red es aplicado.	192.168.100.254 hacia el destino 192.168.21.254	Desde cualquier origen a los servidores.	Trafico restante.	

Tabla 5.2 Requerimiento de ancho de banda la para red en la sede remota de "Comunicaciones e Informática". Fuente: Creación propia

5.1.6 Análisis de recursos y protocolos a utilizar.

Como se mencionó en el transcurso de este proyecto se diseñó e implemento una red privada virtual entre la sede principal y la sede remota para que pueda tener acceso una con la otra. Para ello primero se realizó la planificación, diseño, implementación, operación, optimización según la metodología que se está siguiendo.

5.1.6.1 Análisis del simulador GNS3

Para la simulación se dispuso de esta herramienta GNS3 que fue sumamente eficaz ya que se puede realizar una simulación casi real porque se utilizan los mismos IOS de los router Cisco y no están limitados en comando como lo son con el simulador Packet Tracert de propiedad de Cisco. Los IOS que se seleccionaron son los que soportan los protocolos a utilizar como son BGP, HSRP, TACACS, Q&S, SNMP Y NETFLOW, Etc.

5.1.6.2 Análisis del HSRP

Este protocolo se utilizó para lograr que el tiempo de actividad, es decir, de conectividad (en capa 3) de la red este cerca del 100%. Esto nos fue brindado al utilizar este protocolo HSRP ofreciéndonos así redundancia de red para nuestras redes ip.

A continuación mostramos una configuración con una breve descripción de cada línea de comando:

interface Ethernet0
 ip address 171.16.6.5 255.255.255.0

!--- Asigna una dirección IP a la interfaz.

standby 1 ip 171.16.6.100

!--- Asigna un grupo de reserva y una dirección IP de reserva

standby 1 priority 105

!--- Asigna una prioridad (en este caso 105) a la interfaz del router (e0)
!--- para un número de grupo determinado (1). El valor predeterminado es 100.

standby 1 preempt

!--- Permite que el router se convierta en el router activo cuando la prioridad
!--- sea superior a los routers configurados con HSRP restantes del grupo de reserva activo.
!--- Si no usa el comando standby preempt en la configuración de
!--- un router, dicho router no se convertirá en el router activo, incluso aunque
!--- su prioridad sea superior a la de los routers restantes.

standby 1 track Serial0

!--- Indica que HSRP realiza un seguimiento de la interfaz Serial0.
!--- La prioridad de la interfaz también se puede configurar e indicar la
!--- cantidad en que se reducirá la prioridad del router cuando
!--- la interfaz se desactive. El valor predeterminado es 10.

5.1.6.3 Análisis del protocolo de enrutamiento BGP

El enrutamiento estuvo a cargo de BGP, se utiliza este protocolo para intercambiar prefijos tanto con los vecinos EBGP y con los vecinos IBGP, IBGP es necesario debido a que se necesita un respaldo a nivel de red para cualquiera de nuestros CPE en caso ocurra problemas en la detección por parte de HSRP, se utiliza este protocolo por las siguientes razones.

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

5.1.6.4 Análisis de Implementación de políticas de ancho de banda

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

5.2 Fase de Diseño

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

5.2.1 Diseño Lógico de la Red Wan-Lan (Topología Lógica)

La figura muestra la topología lógica implementada, el cual refleja la sede remota que está compuesta por red de Comunicaciones e Informática y la nube de Claro que es nuestro proveedor de servicios los que tienen comunicación mediante dos routers; donde el tráfico de cada red de la sede principal pasa a través de su respectivo router teniendo así una segmentación de carga entre cada de red, es decir, una red para cada router y a la vez también actuando cada router como el respaldo o contingencia del otro, esto gracias a HSRP. Cada enlace de los router principal y secundarios son independientes y están dirigidos hacia el proveedor mediante fibra independiente al igual que en la sede remota, siendo esto un objetivo.

La red MPLS de Claro simulada en GNS3 no se detalló en este diseño, solo se utilizó como medio demostrativo y tratar de asemejar la simulación a un escenario real, siendo solo materia de estudio los CPE del lado principal y remoto.

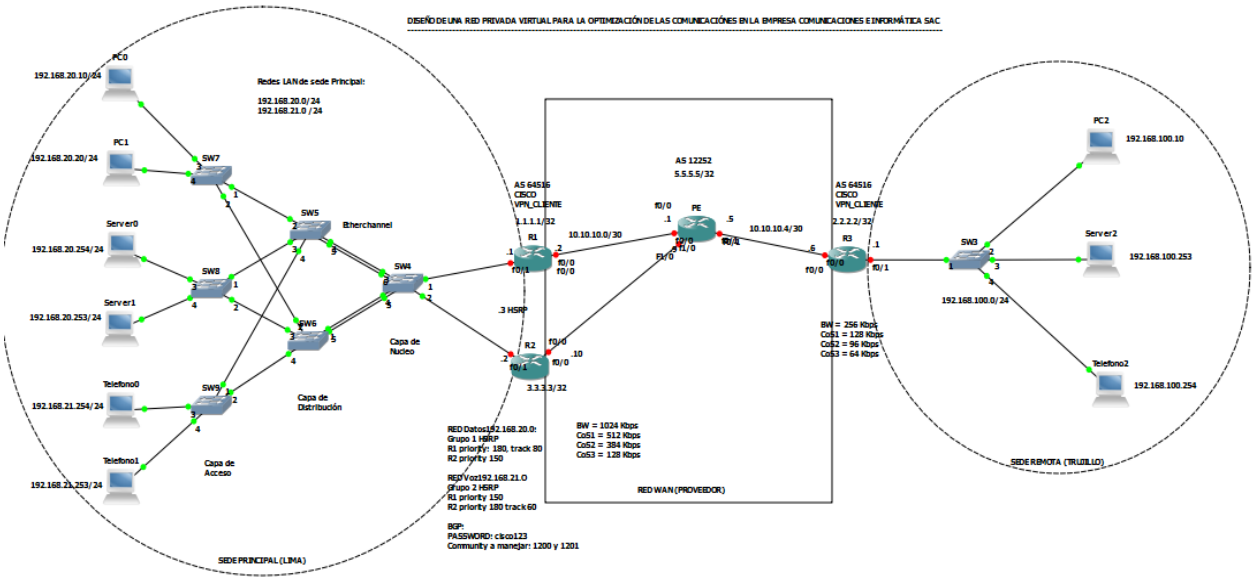


Figura 5.1 Diagrama de topología Lógica (Topología simulada)
Fuente: Creación propia

5.2.2 Diseño Físico de la Red Wan-Lan (Topología Física)

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

A nivel WAN se dispone de una topología point-to-point hacia la principal, que es donde se concentra todos los servidores y por ende solo se necesitó un enlace hacia dicha sede por lo que la topología fue como se muestra en la figura.

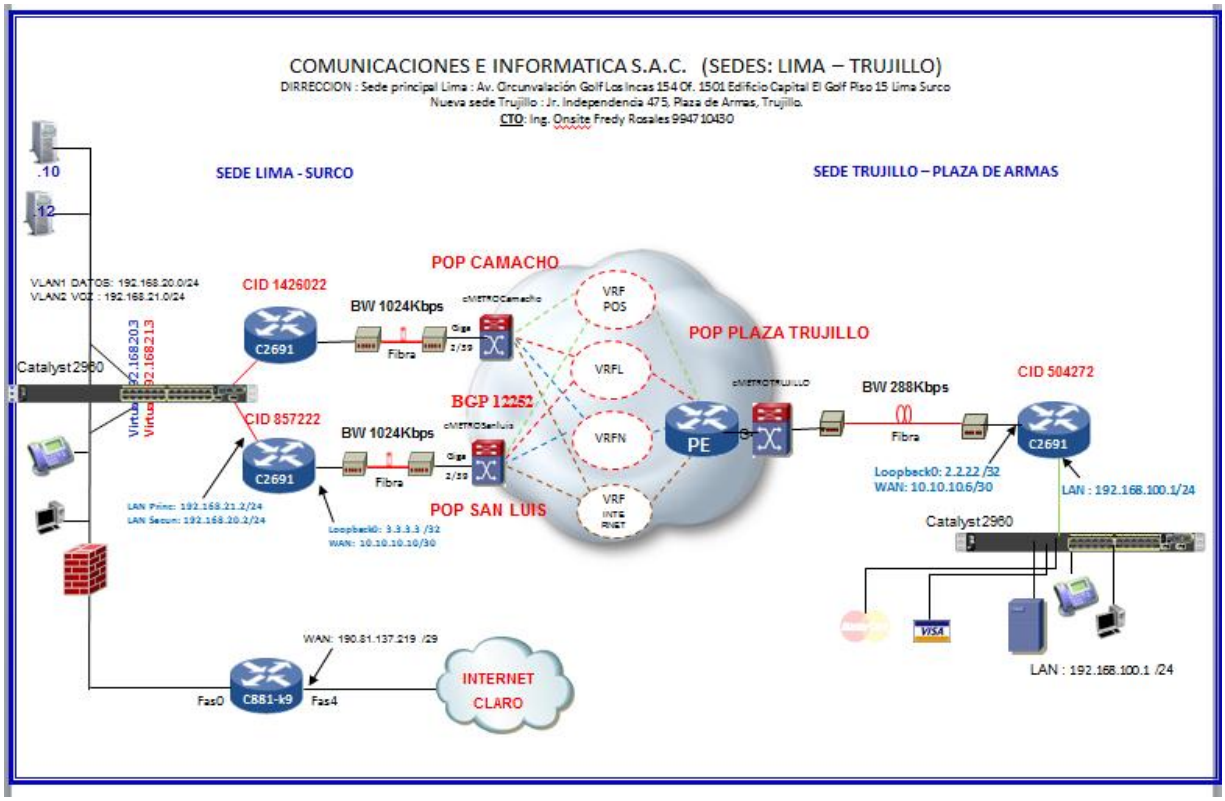


Figura 5.2 Diagrama de topología Física
Fuente: Creación propia

A nivel LAN se utilizó una topología en capas de núcleo contraído, donde la capa de núcleo está formada por los router CPE y la capa de acceso solo por un switch, pero cabe recalcar que solo se utilizó un switch porque solo fue usado de manera demostrativa y la compañía "Comunicaciones e Informática" podría realizar unas mejoras en cuanto a la disponibilidad en la capa de conmutación por parte de los switch, la figura nos muestra la topología según el modelo jerárquico.

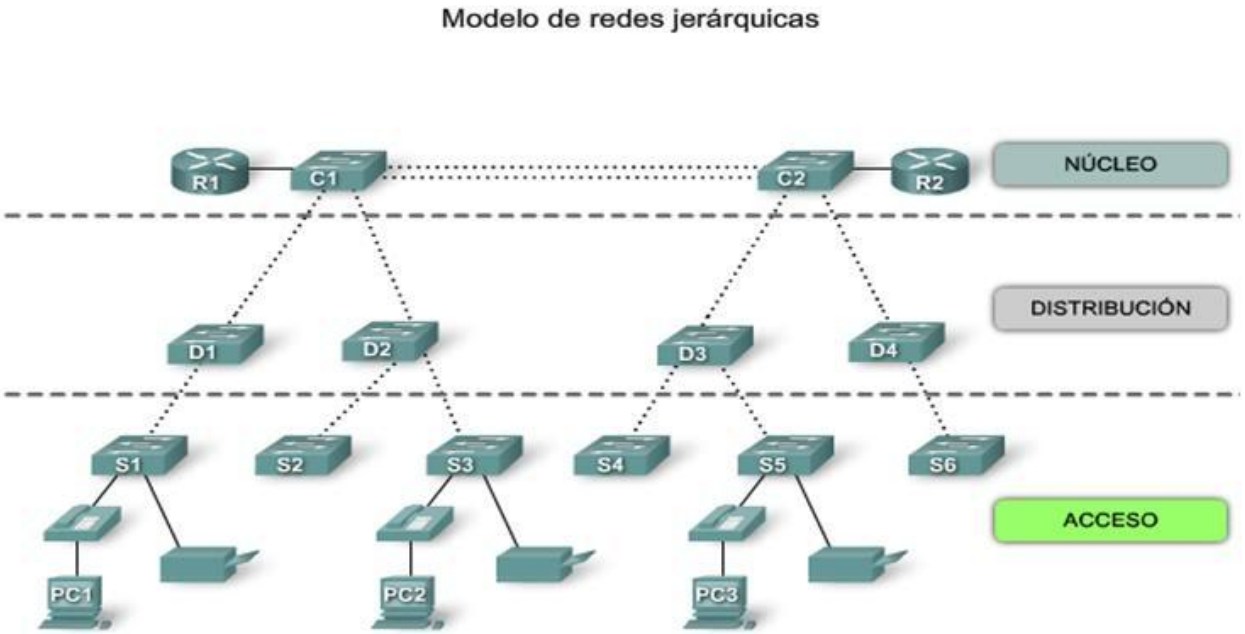


Figura 5.3 Modelo Jerárquico de Red **(System, 2010)**

5.2.3 Plan de Direccionamiento

Primero se realizó el direccionamiento concerniente a nuestra topología. Para ello se tuvo la siguiente tabla de direccionamiento.

DISPOSITIVO	INTERFACE	DIRECCION	DEFAULT
ROUTER CPE1 (R1-Principal)	FastEthernet 0/1.1	192.168.20.1/24	N/A
	FastEthernet 0/1.2	192.168.21.1/24	N/A
	FasEthernet 0/0	10.10.10.2/30	N/A
	FasEthernet 0/1	N/A	N/A
	Loopback 0	1.1.1.1/32	N/A
ROUTER	FasEthernet 0/1.1	192.168.20.2/24	N/A
	FasEthernet 0/1.2	192.168.21.2/24	N/A
	FasEthernet 0/0	10.10.10.10/30	N/A

CPE2 (R2-Secundario)	FastEthernet0/1	N/A	N/A
	Loopback0	3.3.3.3/32	N/A
ROUTER PE (Proveedor)	FastEthernet0/0	10.10.10.1/30	N/A
	FastEthernet0/1	10.10.10.5/30	N/A
	FastEthernet1/0	10.10.10.9/30	N/A
	Loopback0	5.5.5.5/32	N/A
	Loopback1	7.7.7.7/32	N/A
HOST1 (PC1)	Vlan 1	192.168.20.10/24	192.168.20.3
HOST2 (PC2)	Vlan 1	192.168.100.10/24	192.168.100.1
HOST3 (SERVER1)	Vlan 1	192.168.20.254/24	192.168.20.3
HOST4 (SERVER2)	Vlan 1	192.168.100.253/24	192.168.100.1
HOST5 (TELEFONO1)	Vlan 2	192.168.21.254/24	192.168.21.3
HOST6 (TELEFONO2)	Vlan 1	192.168.100.254/24	192.168.100.1

Tabla 5.3 Plan de direccionamiento. Fuente: Creación propia

5.2.4 Análisis Costo-Beneficio

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

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

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

Las tablas siguientes describen la comparación de costos entre LPL y RPV para los ancho de banda empleados en este proyecto.

Para la RPV de “Comunicaciones e Informática“ los precios se obtuvieron por clase de servicio: para un ancho de banda de 128kbps en Cos5 es $217.98, para CoS2 con 384kbps es $ 237.48, para CoS1 con 512kbps es $166.11 dando $621.57 para el ancho de banda total. Se tomó en cuenta un horizonte de tres años en base al tiempo de contrato. Tanto los costos de instalación como los de acceso son pagos que se hacen una sola vez.

LPL para Red Comunicaciones e Informática			
AÑO	**2016**	**2017**	**2018**
DETALLE DE EGRESOS			
COSTO DE B/W 2048kbps anual	**$14352**	**$14353**	**$14354**
COSTO DE ACCESO	**-**	**-**	**-**
COSTO DE INSTALACIÓN	**$991.6**	**-**	**-**
TOTAL EGRESOS ANUAL	**$15343.6**	**$14353**	**$14353**

Tabla 5.4 Costos de servicios LPL para red "Comunicaciones e Informática" Fuente: Creación propia

TOTAL 1= 15343.6 + 14353 + 14353 = 44049.6

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

Tabla 5.5 Costos de servicios RPV para RED "Comunicaciones e Informática" (RPVL) Fuente: Creación propia

TOTAL 2= 9136.53 + 7458.85 + 7458.85 = 24054.23
TOTAL 1 - TOTAL 2=19995.37

Como se puede notar hay una diferencia significativa respecto a los servicios de LPL y RPV esto debido a que los pagos mensuales son menores en la RPV, esto optimizo los recursos asignados a los servicios contratados por "Comunicaciones e Informática", lo que fue así una alternativa rentable.

5.2.5 Equipos de Comunicación

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

Listado de Equipos utilizados:

- Routers (Cisco 2691 con IOS de Cisco C2691-ADcompleto.BIN o similar).
- Routers (Cisco7200 con IOS c7200-p-mz.124-8a.image o similar).
- Switches (Cisco 2960 con IOS de Cisco versión 15.0 (2), imagen lanbasek9 o similar).
- Computadoras

Producto	**Descripción**	**Cantidad**	**Costos por unidad ($)**	**Costos Total ($)**
Router	Cisco 881 k9	4	3044.91	12179.64
Switch	Catalyst 2960 48 Port	2	2237.72	4475.44
PC Core I5	PC – Core I5	3	870.50	2611.5
Cd de Configuración	Cisco Config Professional on CD, CCP-Express on Router Flash	2	0.00	0.00

Tabla 5.6 Equipos utilizados para RED “Comunicaciones e Informática” (RPVL) Fuente: Creación propia

5.3 Fase de Implementación

Se llevó a cabo un conjunto de actividades coordinadas y controladas, con fechas de inicio y final, llevadas a cabo para conseguir el objetivo, que es la simulación e implementación de una VPN de acuerdo con requerimientos especificados por "Comunicaciones e Informática", incluyendo restricciones de tiempo, costo y recursos.

5.3.1 Desarrollo del Diseño Físico

Las actividades realizadas fueron las siguientes:

- Estudio de campo en cliente: Se realizó una visita a las instalaciones de "Comunicaciones e Informática" para dimensionar el cableado, verificar la disponibilidad de tomas de corriente, determinación de instalación de gabinetes si no hay espacio en rack existente.

- Dimensionamiento y solicitud de equipos: Esta etapa constó en determinar los equipos a instalar de acuerdo a los estudios de campo, que incluyó el modelo de router, tipo de convertidores de medio, medida de jumper y cable patch corp, tipo de gabinete. Luego se realizó la solicitud de equipos a CLARO y la solicitud de materiales a almacén de la contrata que ejecutara la instalación.

- Preparación de configuración: Mediante el requerimiento descritos en la sección "Requerimientos de ancho de banda" y el plan de direccionamiento descrito en la sección "Plan de direccionamiento" se realizó la plantilla de configuración.

- Instalación de equipos en POP (punto de presencia): Se instaló el jumper de fibra óptica, tarjetas conversoras (de fibra a cobre) y cable UTP desde los recursos asignados hacia los ODF.

- Configuración de equipos: Se realizó la configuración a los dos routers de la sede principal y al router de la sede remota, verificando que no se borre de la memoria.

- Validación de equipos en POP: Se simuló un escenario cliente en POP para validar recursos asignados en switch de agregación y router PE, también de los convertidores de medios y jumper llevados a la empresa, que luego fueron instalados en las sedes de "Comunicaciones e Informática".

- Instalación de equipos en cliente: Se realizó el montaje del gabinete y estabilizadores, para posteriormente montar sobre ello los media converter (conversores) y router.

- Medición de eventos con OTDR: Para validar un óptimo desempeño de infraestructura de cableado de fibra óptica externo (es decir tendido de fibra desde el POP hacia el cliente) se determinó la atenuación en los empalmes, conectores; y la potencia de recepción y transmisión para verificar que este dentro de los márgenes o rangos establecidos, utilizando equipo llamado Power Meter.

- Pruebas de conectividad, saturación, contingencia, calidad de servicio y elaboración de check-list: Se validó que el ancho de banda de las clases de servicio (QoS) sean los solicitados, y exista conectividad hacia la sede remota y viceversa, realizando a su vez captura de pantalla de pruebas (ping continuos) de las mismas para la elaboración de check-list.

- Validación del servicio, Se firmó actas de servicio, instalación y Liquidación de trabajo.

La figura a continuación refleja lo descrito mediante un diagrama de Gantt:

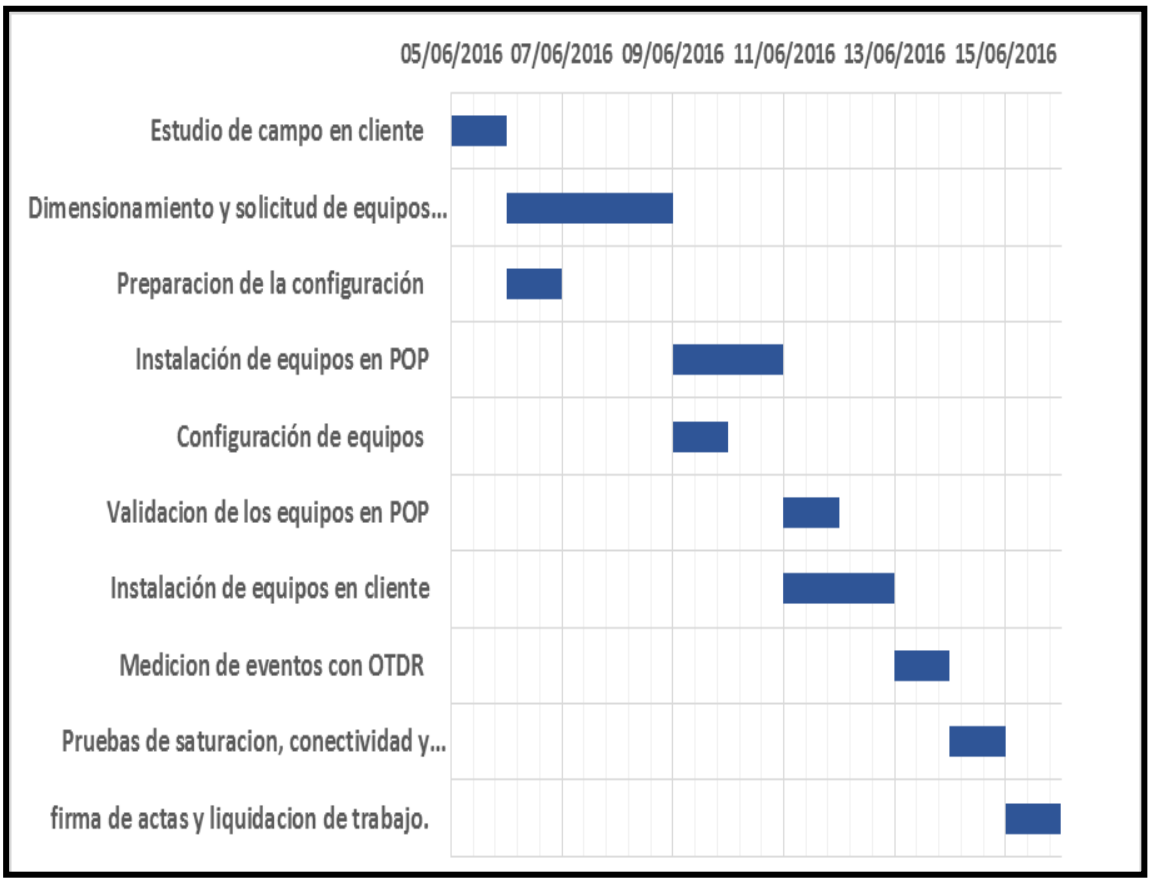


Figura 5.4 Diagrama de Gantt del desarrollo del diseño Físico. Fuente: Creación propia

En la imagen mostrada se detalla las actividades realizadas con sus respectivos periodos de duración, como podrá notarse no existe simultaneidad pero si continuidad en la elaboración de ciertas actividades y otras son dependientes de otras en su proceso de ejecución.

5.3.2 Desarrollo del Diseño Lógico

Se realizó la simulación de la VPN para la empresa Comunicaciones e Informática utilizando el simulador grafico de Red GNS3 ya anteriormente mencionado desarrollando así la topología de red compleja para la empresa en estudio.

5.3.2.1 Configuración en la sede Principal "R1 – Router Principal"

Se procedió a conectar los enlaces Ethernet entre equipos siguiendo el diagrama de topología físico para luego establecer una conexión de consola hacia el router para su configuración, utilizando un software de emulación de terminal; para nuestro proyecto se utilizó el SecureCRT

5.3.2.1.1 Configuración básica del Router

Se realizó la configuración de estos comandos en todos los routers:

Paso 1: Ingresar al modo privilegiado

```
Router>enable
Router#
```

Paso 2: Borrar configuración si es que lo tenga

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Paso 3: Reiniciar equipo router

```
Router#reload
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]:
Press Enter to accept default.
Press RETURN to get started!
```

Paso 4: Configurar un nombre al router

```
Router(config)#hostname R1
R1(config)#
```

Paso 5: Configurar una contraseña de modo EXEC

```
R1(config)#enable secret cisco
R1(config)#
```

Paso 6: Configurar un mensaje de titulo

```
R1(config)#banner motd &
Enter TEXT message. End with the character '&'.
**********************************
!!!AUTHORIZED ACCESS ONLY!!!
**********************************
&
R1(config)#
```

Paso 7: Configurar contraseña de consola en el router

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Paso 8: Configurar contraseña para las líneas de terminal virtual (TELNET)

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
```

```
R1(config-line)#exit
R1(config)#
```

```
enable secret 5 $1$/rrI$.U/NJcRzzQHZthJDN.h3S.
!
banner motd ^C **********SOLO ACCESO AUTORIZADO**********   ^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 login
!
```

Figura 5.5: Configuración básica de seguridad del router. Fuente: Creación propia

5.3.2.1.2 Configuración de interfaz del Router

Paso 1: Configuración interface WAN

```
interface FastEthernet0/0
 description Interface WAN Sede RPVL 1024 Kbps - CID 1426022
 ip address 10.10.10.2 255.255.255.252
 load-interval 30
 speed 100
 full-duplex
 service-policy output Shape1024
```

Figura 5.6: Configuración interface WAN. Fuente: Creación propia

Podemos apreciar en la figura lo siguiente:

- Que la interface WAN es la fastethernet 0/0
- Se proporciona una pequeña descripción a la interfaz con el comando "**description"**
- Se configuró la interfaz con la dirección asignada según nuestro diagrama de topología Lógico
- Se creo un intervalo de carga de 30 segundos ya que promediara en este tiempo la carga que pasa por la interfaz para ser mostrada en cualquier momento. Realizado con el comando "**load-interval 30".**
- Se configuró la interfaz o el puerto a 100 Mbps de velocidad.
- Se configuró la interfaz o el puerto con una negociación en "**full-duplex"** es decir que va a poder enviar y recibir datos a la vez.
- El comando: "**service.policy output Shape1024**". Política del marcado por servicio para el ancho de banda. Sera definido mas adelante.

Paso 2: Configuración interface LAN

```
interface FastEthernet0/1
 description Interface LAN
 no ip address
 load-interval 30
 speed 100
 full-duplex
 service-policy input SetDscpLan
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 192.168.20.1 255.255.255.0
 standby 1 ip 192.168.20.3
 standby 1 priority 180
 standby 1 preempt
 standby 1 track FastEthernet0/0 80
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.21.1 255.255.255.0
 standby 2 ip 192.168.21.3
 standby 2 priority 150
 standby 2 preempt
!
```

Figura 5.7: Configuración interface LAN. Fuente: Creación propia

Podemos apreciar en la figura lo siguiente:

- Que la interface LAN es la fastethernet 0/1 y tiene los mismos comandos ya antes mencionados salvo el comando "**service.policy input SetDscpLan**" que es una política para el marcado de paquetes según el servicio.
- Se aprecia que la interfaz fastethernet 0/1 fue dividido en 2 subinterfaces ya que la sede principal cuenta con 2 segmento de Red en su red lan ya definindas anteriormente. Esta división de la interfaz es gracias al comando "**encapsulation dot1Q Vlan"** que es un protocolo estándar de interconexión multiple.
- Cada subinterface contó con una ip definida para cada Vlan.
- Comando "**standby**" será definido más adelante.

Paso 3: Configuración interface Loopback

```
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
```

Figura 5.8: Configuración interface Loopback. Fuente: Creación propia

Podemos apreciar en la figura lo siguiente: que la loopback utilizada es la loopback0 a la cual fue asignada una dirección ip.

5.3.2.1.3 Configuración del BGP

Paso 1: Configuración del filtrado de prefijos

En esta parte se realizó la selección de rutas que se ingresó en la tabla bgp y las rutas que se envió al vecino BGP que este caso es el PE todo esto para evitar loops de datos y destinos que innecesariamente se instalarían en la tabla BGP y posteriormente en la tabla de enrutamiento, por lo que se hace uso de los

Prefix Lists que son introducidos en BGP ya que son una forma eficiente de filtrado muy rápido porque buscan el prefijo de las direcciones dadas por el administrador y la búsqueda es muy rápida. Los Prefix Lists se pueden editar. La modificación de ACLs es bastante compleja. A demás son fáciles de configurar y usar, pero antes de aplicarlos es necesario definir el criterio del Prefix List. A continuación se muestra la configuración de IP PREFIX-LIST una herramienta de coincidencia más versátil que las listas de acceso, las direcciones ip que aparecen son las redes nuestra LAN de la sede principal.

```
ip prefix-list Red_Lan seq 5 permit 0.0.0.0/0
ip prefix-list Red_Lan seq 10 permit 1.1.1.1/32
ip prefix-list Red_Lan seq 20 permit 192.168.20.0/24
!
ip prefix-list Red_Voz seq 10 permit 192.168.21.0/24
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
```

Figura 5.9: Configuración del filtrado de prefijos. Fuente: Creación propia

Paso 2: Configuración para aplicación de políticas y creación de coincidencia

Para ello se utilizó el comando route-map que tiene muchas aplicaciones ya sea para ajustar los atributos sobre los prefijos que coinciden en este contexto, la siguiente figura muestra cómo se aplicó los criterios de coincidencia y que política se aplicó para esa coincidencia, en el paso 3 se verá como estos route-map son invocados dentro de la configuración de BGP.

```
route-map SET_TELMEX_COMM permit 10
 description Envio de Redes Lan Seteados COMUNIDAD 1200
 match ip address prefix-list Red_Lan
 set community 12252:1200
!
route-map SET_TELMEX_COMM permit 15
 description Envio de Redes Voz Seteados COMUNIDAD 1201
 match ip address prefix-list Red_Voz
 set community 12252:1201
!
route-map From_VPN_Telmex deny 10
 description Denegacion de Redes LAN Internas
 match ip address prefix-list Red_Lan
!
route-map From_VPN_Telmex permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
```

Figura 5.10: Configuración para aplicación de políticas y creación de coincidencia. Fuente: Creación propia

Paso 3: Configuración de BGP para el servicio de RPVL (VPN-Local)

El protocolo de Gateway de frontera BGP, permite la comunicación entre dominios por lo que su implementación debe ser únicamente en las fronteras de una Red. Para la conexión de sitios locales con sitios remotos mediante VPNs, este protocolo es muy usual ya que además permite ser trabajado como protocolo de interiores y se utiliza para la comunicación específica entre dispositivos de frontera.
En esta parte se configuró EBGP entre el PE con el sistema autónomo 12252 y CPE (R1) con el sistema autónomo 64516 para que las rutas de la redes LAN de “Comunicaciones e Informática” sean publicadas hacia la sede remota y a su vez recibir prefijos de red de la sede remota, claro utilizando políticas basadas en atributos. Se configuró dos contextos de enrutamiento BGP una para la red RPVL y otra para el router

backup. Las FIGURAS 3.18 y 3.19 muestran el contexto de enrutamiento para la tabla de enrutamiento tradicional allí está incluida dos vecindades BGP una con el PE y otra con el CPE(R2) de backup, esta sesión adicional es para asegurar que cuando ocurra un problema a nivel de capa 3 en el enlace WAN hacia el proveedor los paquetes que están destinados hacia CPE(R1) desde la red LAN sean redireccionados hacia CPE(R2) y puedan salir hacia la Sede Remota (Trujillo) y como se mencionó en el paso 1, las políticas de filtrado son invocados en esta sección mediante el comando route-map From_VPN_DATOS en la dirección entrante para que tenga efecto sobre los prefijos que son publicados por el PE.

```
router bgp 64516
 no synchronization
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 network 1.1.1.1 mask 255.255.255.255
 network 192.168.20.0
 network 192.168.21.0
 neighbor SEDE_PRINCIPAL1 peer-group
 neighbor SEDE_PRINCIPAL1 remote-as 12252
 neighbor SEDE_PRINCIPAL1 password cisco123
 neighbor SEDE_PRINCIPAL1 timers 10 30
 neighbor SEDE_PRINCIPAL1 send-community both
 neighbor SEDE_PRINCIPAL1 soft-reconfiguration inbound
 neighbor SEDE_PRINCIPAL1 route-map From_VPN_Telmex in
 neighbor SEDE_PRINCIPAL1 route-map SET_TELMEX_COMM out
 neighbor LAN_PRINCIPAL1 peer-group
 neighbor LAN_PRINCIPAL1 remote-as 64516
 neighbor LAN_PRINCIPAL1 password cisco123
 neighbor LAN_PRINCIPAL1 timers 10 30
 neighbor LAN_PRINCIPAL1 next-hop-self
 neighbor LAN_PRINCIPAL1 soft-reconfiguration inbound
 neighbor 10.10.10.1 peer-group SEDE_PRINCIPAL1
 neighbor 10.10.10.1 description enlace WAN Sede Principal 1
 neighbor 192.168.20.2 peer-group LAN_PRINCIPAL1
 neighbor 192.168.20.2 description enlace LAN Principal 1 de Contingencia
 no auto-summary
!
```

Figura 5.11: Configuración del BGP. Fuente: Creación propia

5.3.2.1.4 Configuración del Protocolo de redundancia HSRP

Hot Standby Routing Protocol (HSRP) es un protocolo propietario de Cisco que, al igual que Virtual Route Redundancy Protocol (VRRP), permite disponer de lo que llamamos High Availabilty (Alta Disponibilidad) a nivel de Default Gateway en una red LAN. Alta disponibilidad significa que, en caso de existir una falla en un equipo, otro equipo estará inmediatamente disponible de forma automática para sustituir el averiado.

La alta disponibilidad en HSRP se logra compartiendo una misma dirección IP virtual entre dos o más Router. En nuestro caso fue definida la .3 como último octeto en cada ip virtual para cada segmento de Red. Mayor detalle en el diagrama de topología Lógico.

En la configuración del protocolo HSRP tuvimos dos tipos de Routers: el Router Activo “R1” y el Router Pasivo “R2” para la red de Datos en nuestro caso la Red 192.168.20.0 /24. De manera inversa fue definida para la Red de Voz en nuestro caso la Red 192.168.21.0 /24.

El Router Activo es aquel que atiende permanentemente las peticiones que se realizan a la dirección IP Virtual. En caso que el Router Activo (R1) falle, entonces el Router Pasivo (R2) adquiere el rol del Router Activo y comienza atender las peticiones enviadas a la dirección IP Virtual.

En términos prácticos, el objetivo de HSRP es permitir que nuestros paquetes IP sigan encaminándose a través de la red WAN, aun cuando el Default Gateway haya sufrido un problema, sea de hardware o software.

El procedimiento para configurar HSRP en Cisco IOS fue el siguiente:

Paso 1: Configuración en el router Principal o Activo:

```
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 192.168.20.1 255.255.255.0
 standby 1 ip 192.168.20.3
 standby 1 priority 180
 standby 1 preempt
 standby 1 track FastEthernet0/0 80
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.21.1 255.255.255.0
 standby 2 ip 192.168.21.3
 standby 2 priority 150
 standby 2 preempt
!
```

Figura 5.12: Configuración HSRP en el router Principal. Fuente: Creación propia

Paso 2: Configuración en el router Backup o Pasivo:

```
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 192.168.20.2 255.255.255.0
 standby 1 ip 192.168.20.3
 standby 1 priority 150
 standby 1 preempt
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.21.2 255.255.255.0
 standby 2 ip 192.168.21.3
 standby 2 priority 180
 standby 2 preempt
 standby 2 track FastEthernet0/0 60
!
```

Figura 5.12: Configuración HSRP en el router Backup. Fuente: Creación propia

5.3.2.1.5 Configuración de la calidad de servicio QoS

Paso 1: Configuración de las listas de acceso en la sede Principal:

```
ip access-list extended qos2
 permit ip host 192.168.20.254 any
ip access-list extended qos5
 permit ip host 192.168.21.254 host 192.168.100.254
!
```

Figura 5.13: Configuración de las listas de acceso - Sede Principal. Fuente: Creación propia

Podemos apreciar según muestra nuestra figura que fueron creadas listas de acceso para el marcado de paquetes en qos 2 y qos5.

La lista de acceso extendida de qos2 (que es trafico crítico del cliente es decir aplicaciones sensibles al retardo como son: SAP, Oracle, etc) nos permitió que la ip de nuestra red 192.168.20.254 llegue a cualquier destino y viceversa, es decir que a nuestro servidor (Server1) de la sede principal pueda acceder a ella de cualquier destino de la sede remota (Trujillo).

La lista de acceso extendida de qos5 (que es tráfico en la que trabajan aplicaciones en tiempo real como son VoIP, Multimedia, Telefonía IP, Video conferencia) nos permitió la ip de nuestra red 192.168.21.254 (Telefono1) llegara a cualquier destino 192.168.100.254 (Telefono2 de la sede remota) y viceversa.

Paso 2: Configuración de las políticas de calidad en la sede Principal:

```
class-map match-any qos5
 match ip dscp cs5
class-map match-any qos1
 match ip dscp cs1
class-map match-any qos2
 match ip dscp cs2
class-map match-any P2
 match ip dscp cs2
 match access-group name qos2
class-map match-any P5
 match ip dscp cs5
 match access-group name qos5
!
```

Figura 5.13: Configuración de las políticas de calidad en la sede Principal. Fuente: Creación propia

- Se realizó el marcado de paquetes en la Red del cliente utilizando el comando "**class-map match-any qos5**" el cual identifica el tipo de trafico ya sea qos5, qos2, qos1.
- Se utilizó también el comando "**match ip dscp cs5**" el cual realizó un marcado de paquetes general en la red del cliente por lo que ya no es necesario hacer referencia a redes en lista de acceso, sino solamente a la precedencia de paquetes.
- Este comando: "**match access-group name qos5**"se utilizó para la identificación del tipo de QoS que necesitan reservación de BW. Se debe de definir la lista de acceso dependiendo del qos en las redes asociadas a este tipo de QoS.

Paso 3: Configuración del policy-map para el marcado de paquetes en la LAN de la sede Principal:

```
policy-map SetDscpLan
 class P5
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1
```

Figura 5.14: Configuración del policy-map para el marcado de paquetes en la LAN de la sede Principal. Fuente: Creación propia

- Como apreciamos en la figura el comando "**policy-map SetDscpLan**" es una política del marcado de paquetes.
- El comando "**class P5**" define la clase P5, identifica al tráfico tipo QoS5 en este caso.
- El comando "**set ip dscp cs5**" especifica el BW a priorizar trafico Qos5 para este caso.

Paso 4: Configuración del policy-map para el tipo de trafico Qos5, Qos2, Qos1

```
policy-map wan
 class qos5
  priority 128
    police 128000 24000 48000 conform-action transmit  exceed-action drop  violate-action drop
 class qos2
  bandwidth 384
    police 384000 72000 144000 conform-action transmit  exceed-action set-dscp-transmit cs1 violate-action set-dscp-transmit 8
 class qos1
  bandwidth 512
 class class-default
  fair-queue
policy-map Shape1024
 class class-default
  shape average 1025000
  service-policy wan
!
```

Figura 5.15: Configuración del policy-map para el tipo de trafico Qos5, Qos2, Qos1. Fuente: Creación propia

- Como apreciamos en la figura el comando "**policy-map wan**" es una política del marcado de paquetes que hace referencia al tráfico Qos5, Qos2, Qos1.
- El comando "**class qos5**" identificó al trafico Qos5.
- El comando "**priority 128**" identificó al BW a priorizar trafico Qos5.
- El comando "**pólice 128000 24000 48000 confort-action trnasmit drop violate-action drop**" marcó los paquetes que ingresaron a la red MPLS. Luego si desborda el BW asignado puede tomar varias acciones como son: el drop (descartar paquetes), transmitir por qos1. Para este caso como es qos5 es decir tráfico en tiempo real no se puede pasar a otro qos ni transmitirlo a otro ya que la voz no puede retrasarse ni ponerlo es espera es por eso que en este caso como es qos5 se dropea los excedentes. Si fuera el caso de qos2 si se podría pasar o utilizar el BW brindado a qos1.

Paso 5: Definición de la Política que garantizó el QoS desde la sede principal a la sede remota

```
policy-map Shape1024
 class class-default
  shape average 1025000
  service-policy wan
!
```

Figura 5.16: Definición de la Política. Fuente: Creación propia

- El comando "**policy-map Shape1024**" hizo referencia al tráfico de salida desde la sede principal hacia la sede remota.
- El comando "**class class-default**" identificó al tráfico nombrado como class-default en este caso.
- El comando "**shape average 1025000**" aseguró el ancho de banda hacia la sede remota.
- El comando "**service-policy wan**" la política "wan" definió el tratamiento de tráfico hacia le sede remota, las reservas del BW se realizó tomando en cuenta el ancho de banda máximo.

Paso 6: Aplicación de Políticas

En la WAN:

```
interface FastEthernet0/0
 description Interface WAN Sede RPVL 1024 Kbps - CID 1426022
 ip address 10.10.10.2 255.255.255.252
 load-interval 30
 speed 100
 full-duplex
 service-policy output Shape1024
!
```

Figura 5.17: Aplicación de Políticas en la WAN. Fuente: Creación propia

Como vemos en la última línea de comando aplicada a la interface fastethernet 0/0 que es nuestra interface WAN, se aplicó la política de Qos al tráfico de salida de la interface.

En la LAN:

```
interface FastEthernet0/1
 description Interface LAN
 no ip address
 load-interval 30
 speed 100
 full-duplex
 service-policy input SetDscpLan
!
```

Figura 5.18: Aplicación de Políticas en la LAN. Fuente: Creación propia

Como vemos en la última línea de comando aplicada a la interface fastethernet 0/1 que es nuestra interface LAN, se aplicó la política de Qos al tráfico de entrada de la interface.

5.3.2.1.6 Configuración Final al router

Luego de configurado nuestro router (R1) de la sede Principal se procedió al guardado de la configuración, existiendo 2 formas veamos los comandos:

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#wr
Building configuration...
[OK]
R1#
```

Figura 5.19: Configuración Final al router. Fuente: Creación propia

5.3.2.1.7 Muestra total de nuestra configuración realizada al router Principal

```
R1#sh run
Building configuration...

Current configuration : 4515 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$/rrI$.U/NJcRzzQHZthJDN.h3S.
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
class-map match-any qos5
 match ip dscp cs5
class-map match-any qos1
 match ip dscp cs1
class-map match-any qos2
 match ip dscp cs2
class-map match-any P2
 match ip dscp cs2
 match access-group name qos2
class-map match-any P5
 match ip dscp cs5
 match access-group name qos5
!
!
policy-map SetDscpLan
 class P5
  set ip dscp cs5
 class P2
```

```
  set ip dscp cs2
 class class-default
  set ip dscp cs1
policy-map wan
 class qos5
  priority 128
    police 128000 24000 48000 conform-action transmit  exceed-action drop  violate-action drop
 class qos2
  bandwidth 384
    police 384000 72000 144000 conform-action transmit  exceed-action set-dscp-transmit cs1 violate-
action set-dscp-transmit 8
 class qos1
  bandwidth 512
 class class-default
  fair-queue
policy-map Shape1024
 class class-default
  shape average 1025000
  service-policy wan
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 description Interface WAN Sede RPVL 1024 Kbps - CID 1426022
 ip address 10.10.10.2 255.255.255.252
 load-interval 30
 speed 100
 full-duplex
 service-policy output Shape1024
!
interface FastEthernet0/1
 description Interface LAN
 no ip address
 load-interval 30
 speed 100
 full-duplex
 service-policy input SetDscpLan
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 192.168.20.1 255.255.255.0
 standby 1 ip 192.168.20.3
 standby 1 priority 180
 standby 1 preempt
 standby 1 track FastEthernet0/0 80
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.21.1 255.255.255.0
 standby 2 ip 192.168.21.3
 standby 2 priority 150
 standby 2 preempt
!
router bgp 64516
 no synchronization
```

```
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 network 1.1.1.1 mask 255.255.255.255
 network 192.168.20.0
 network 192.168.21.0
 neighbor SEDE_PRINCIPAL1 peer-group
 neighbor SEDE_PRINCIPAL1 remote-as 12252
 neighbor SEDE_PRINCIPAL1 password cisco123
 neighbor SEDE_PRINCIPAL1 timers 10 30
 neighbor SEDE_PRINCIPAL1 send-community both
 neighbor SEDE_PRINCIPAL1 soft-reconfiguration inbound
 neighbor SEDE_PRINCIPAL1 route-map From_VPN_Telmex in
 neighbor SEDE_PRINCIPAL1 route-map SET_TELMEX_COMM out
 neighbor LAN_PRINCIPAL1 peer-group
 neighbor LAN_PRINCIPAL1 remote-as 64516
 neighbor LAN_PRINCIPAL1 password cisco123
 neighbor LAN_PRINCIPAL1 timers 10 30
 neighbor LAN_PRINCIPAL1 next-hop-self
 neighbor LAN_PRINCIPAL1 soft-reconfiguration inbound
 neighbor 10.10.10.1 peer-group SEDE_PRINCIPAL1
 neighbor 10.10.10.1 description enlace WAN Sede Principal 1
 neighbor 192.168.20.2 peer-group LAN_PRINCIPAL1
 neighbor 192.168.20.2 description enlace LAN Principal 1 de Contingencia
 no auto-summary
!
!
ip bgp-community new-format
!
no ip http server
no ip http secure-server
!
ip access-list extended qos2
 permit ip host 192.168.20.254 any
ip access-list extended qos5
 permit ip host 192.168.21.254 host 192.168.100.254
!
!
ip prefix-list Red_Lan seq 5 permit 0.0.0.0/0
ip prefix-list Red_Lan seq 10 permit 1.1.1.1/32
ip prefix-list Red_Lan seq 20 permit 192.168.20.0/24
!
ip prefix-list Red_Voz seq 10 permit 192.168.21.0/24
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
!
route-map SET_TELMEX_COMM permit 10
 description Envio de Redes Lan Seteados COMUNIDAD 1200
 match ip address prefix-list Red_Lan
 set community 12252:1200
!
route-map SET_TELMEX_COMM permit 15
 description Envio de Redes Voz Seteados COMUNIDAD 1201
 match ip address prefix-list Red_Voz
 set community 12252:1201
!
route-map From_VPN_Telmex deny 10
```

```
 description Denegacion de Redes LAN Internas
 match ip address prefix-list Red_Lan
!
route-map From_VPN_Telmex permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
!
control-plane
!
!
banner motd ^C **********SOLO ACCESO AUTORIZADO**********  ^C
!
line con 0
 exec-timeout 0 0
 privilege level 15
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 password cisco
 login
!
!
end

R1#
```

5.3.2.2 Configuración en la sede Principal "R2 – Router Backup"

Se procedió a conectar los enlaces Ethernet entre equipos siguiendo el diagrama de topología físico para luego establecer una conexión de consola hacia el router para su configuración, se utilizó un software de emulación de terminal; para nuestro proyecto se utilizó el SecureCRT

5.3.2.2.1 Configuración básica del Router Backup

```
enable secret 5 $1$O69X$ikrNcLY2Yv2SF.jMnnF/w0
!
banner motd ^C ********** SOLO ACCESO AUTORIZADO AL R2 ********** ^C
!
line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
```

Figura 5.20: Configuración básica del Router Backup. Fuente: Creación propia

Se configuró la contraseña "cisco" para todos los password en todos los router

5.3.2.2.2 Configuración de interfaz del Router Backup

Paso 1: Configuración interface WAN

```
interface FastEthernet0/0
 description Interface WAN Sede RPVL 1024 Kbps - CID XXXXXX
 ip address 10.10.10.10 255.255.255.252
 speed 100
 full-duplex
 service-policy output Shape1024
!
```

Figura 5.21: Configuración interface WAN del Router Backup. Fuente: Creación propia

Paso 2: Configuración interface LAN

```
interface FastEthernet0/1
 description Interface LAN
 no ip address
 speed 100
 full-duplex
 service-policy input SetDscpLan
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 192.168.20.2 255.255.255.0
 standby 1 ip 192.168.20.3
 standby 1 priority 150
 standby 1 preempt
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.21.2 255.255.255.0
 standby 2 ip 192.168.21.3
 standby 2 priority 180
 standby 2 preempt
 standby 2 track FastEthernet0/0 60
!
```

Figura 5.22: Configuración interface LAN del Router Backup. Fuente: Creación propia

Paso 3: Configuración interface Loopback

```
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
```

Figura 5.23: Configuración interface Loopback del Router Backup. Fuente: Creación propia

Podemos apreciar en la figura lo siguiente: que la loopback utilizada es la loopback0 la cual fue asignada una dirección ip según nuestro diagrama de diseño lógico.

5.3.2.2.3 Configuración del BGP

Paso 1: Configuración del filtrado de prefijos

```
ip prefix-list Red_Lan seq 5 permit 0.0.0.0/0
ip prefix-list Red_Lan seq 10 permit 3.3.3.3/32
ip prefix-list Red_Lan seq 20 permit 192.168.20.0/24
!
ip prefix-list Red_Voz seq 10 permit 192.168.21.0/24
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
```

Figura 5.24: Configuración del filtrado de prefijos del Router Backup. Fuente: Creación propia

Paso 2: Configuración para aplicación de políticas y creación de coincidencia

```
route-map SET_TELMEX_COMM permit 10
 description Envio de Redes Lan Seteados COMUNIDAD 1200
 match ip address prefix-list Red_Lan
 set community 12252:1200
!
route-map SET_TELMEX_COMM permit 15
 description Envio de Redes Voz Seteados COMUNIDAD 1201
 match ip address prefix-list Red_Voz
 set community 12252:1201
!
route-map From_VPN_Telmex deny 10
 description Denegacion de Redes LAN Internas
 match ip address prefix-list Red_Lan
!
route-map From_VPN_Telmex permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
```

Figura 5.25: Configuración para aplicación de políticas y creación de coincidencia del Router Backup. Fuente: Creación propia

Paso 3: Configuración de BGP para el servicio de RPVL (VPN-Local)

```
router bgp 64516
 no synchronization
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 network 3.3.3.3 mask 255.255.255.255
 network 192.168.20.0
 network 192.168.21.0
 neighbor SEDE_PRINCIPAL2 peer-group
 neighbor SEDE_PRINCIPAL2 remote-as 12252
 neighbor SEDE_PRINCIPAL2 password cisco123
 neighbor SEDE_PRINCIPAL2 timers 10 30
 neighbor SEDE_PRINCIPAL2 send-community both
 neighbor SEDE_PRINCIPAL2 soft-reconfiguration inbound
 neighbor SEDE_PRINCIPAL2 route-map From_VPN_Telmex in
 neighbor SEDE_PRINCIPAL2 route-map SET_TELMEX_COMM out
 neighbor LAN_PRINCIPAL2 peer-group
 neighbor LAN_PRINCIPAL2 remote-as 64516
 neighbor LAN_PRINCIPAL2 password cisco123
 neighbor LAN_PRINCIPAL2 timers 10 30
 neighbor LAN_PRINCIPAL2 next-hop-self
 neighbor LAN_PRINCIPAL2 soft-reconfiguration inbound
 neighbor 10.10.10.9 peer-group SEDE_PRINCIPAL2
 neighbor 10.10.10.9 description enlace WAN Sede Principal 2
 neighbor 192.168.20.1 peer-group LAN_PRINCIPAL2
 neighbor 192.168.20.1 description enlace LAN Principal 2 de Contingencia
 no auto-summary
!
```

Figura 5.26: Configuración de BGP del Router Backup. Fuente: Creación propia

5.3.2.2.4 Configuración del Protocolo de redundancia HSRP

Paso 1: Configuración en el router Backup:

```
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 192.168.20.2 255.255.255.0
 standby 1 ip 192.168.20.3
 standby 1 priority 150
 standby 1 preempt
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.21.2 255.255.255.0
 standby 2 ip 192.168.21.3
 standby 2 priority 180
 standby 2 preempt
 standby 2 track FastEthernet0/0 60
!
```

Figura 5.27: Configuración de HSRP del Router Backup. Fuente: Creación propia

5.3.2.2.5 Configuración de la calidad de servicio QoS

Paso 1: Configuración de las listas de acceso en la sede Principal (Router Backup):

```
ip access-list extended qos2
 permit ip host 192.168.20.254 any
ip access-list extended qos5
 permit ip host 192.168.21.254 host 192.168.100.254
!
```

Figura 5.28: Configuración de las listas de acceso del Router Backup. Fuente: Creación propia

Paso 2: Configuración de las políticas de calidad en la sede Principal (Router Backup):

```
class-map match-any qos5
 match ip dscp cs5
class-map match-any qos1
 match ip dscp cs1
class-map match-any qos2
 match ip dscp cs2
class-map match-any P2
 match ip dscp cs2
 match access-group name qos2
class-map match-any P5
 match ip dscp cs5
 match access-group name qos5
!
```

Figura 5.29: Configuración de las políticas de calidad del Router Backup. Fuente: Creación propia

Paso 3: Configuración del policy-map para el marcado de paquetes en la LAN de la sede Principal (Router Backup):

```
policy-map SetDscpLan
 class P5
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1
```

Figura 5.30: Configuración del policy-map del Router Backup. Fuente: Creación propia

Paso 4: Configuración del policy-map para el tipo de trafico Qos5, Qos2, Qos1

```
policy-map wan
 class qos5
  priority 128
    police 128000 24000 48000 conform-action transmit  exceed-action drop  violate-action drop
 class qos2
  bandwidth 384
    police 384000 72000 144000 conform-action transmit  exceed-action set-dscp-transmit cs1 violate-action set-dscp-transmit 8
 class qos1
  bandwidth 512
 class class-default
  fair-queue
policy-map Shape1024
 class class-default
  shape average 1025000
  service-policy wan
!
```

Figura 5.31: Configuración del policy-map para el tipo de trafico Qos5, Qos2, Qos1
. Fuente: Creación propia

Paso 5: Definición de la Política que garantiza el QoS desde la sede principal (Router Backup) a la sede remota

```
policy-map Shape1024
 class class-default
  shape average 1025000
  service-policy wan
!
```

Figura 5.32: Definición de la Política del Router Backup. Fuente: Creación propia

Paso 6: Aplicación de Políticas

En la WAN:

```
interface FastEthernet0/0
 description Interface WAN Sede RPVL 1024 Kbps - CID XXXXXX
 ip address 10.10.10.10 255.255.255.252
 speed 100
 full-duplex
 service-policy output Shape1024
!
```

Figura 5.33: Aplicación de Políticas en la WAN del Router Backup. Fuente: Creación propia

Como vemos en la última línea de comando aplicada a la interface fastethernet 0/0 que es nuestra interface WAN, se aplicó la política de Qos al tráfico de salida de la interface.

En la LAN:

```
interface FastEthernet0/1
 description Interface LAN
 no ip address
 speed 100
 full-duplex
 service-policy input SetDscpLan
!
```

Figura 5.34: Aplicación de Políticas en la LAN del Router Backup. Fuente: Creación propia

5.3.2.2.6 Configuración Final al router

Luego de configurado nuestro router (R2) de la sede Principal procedemos al guardado:

```
R2#copy running-config startup-config
R2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R2#wr
Building configuration...
[OK]
R2#
```

Figura 5.35: Guardando configuracion del Router Backup. Fuente: Creación propia

5.3.2.2.7 Muestra total de nuestra configuración realizada al router Backup de la sede Principal:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
```

```
!
!
!
class-map match-any qos5
 match ip dscp cs5
class-map match-any qos1
 match ip dscp cs1
class-map match-any qos2
 match ip dscp cs2
class-map match-any P2
 match ip dscp cs2
 match access-group name qos2
class-map match-any P5
 match ip dscp cs5
 match access-group name qos5
!
!
policy-map SetDscpLan
 class P5
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1
policy-map wan
 class qos5
  priority 128
    police 128000 24000 48000 conform-action transmit  exceed-action drop  violate-action drop
 class qos2
  bandwidth 384
    police 384000 72000 144000 conform-action transmit  exceed-action set-dscp-transmit cs1 violate-
action set-dscp-transmit 8
 class qos1
  bandwidth 512
 class class-default
  fair-queue
policy-map Shape1024
 class class-default
  shape average 1025000
  service-policy wan
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
 description Interface WAN Sede RPVL 1024 Kbps - CID XXXXXX
 ip address 10.10.10.10 255.255.255.252
 speed 100
 full-duplex
 service-policy output Shape1024
!
interface FastEthernet0/1
 description Interface LAN
 no ip address
 speed 100
 full-duplex
```

```
 service-policy input SetDscpLan
!
interface FastEthernet0/1.1
 encapsulation dot1Q 1 native
 ip address 192.168.20.2 255.255.255.0
 standby 1 ip 192.168.20.3
 standby 1 priority 150
 standby 1 preempt
!
interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.21.2 255.255.255.0
 standby 2 ip 192.168.21.3
 standby 2 priority 180
 standby 2 preempt
 standby 2 track FastEthernet0/0 60
!
router bgp 64516
 no synchronization
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 network 3.3.3.3 mask 255.255.255.255
 network 192.168.20.0
 network 192.168.21.0
 neighbor SEDE_PRINCIPAL2 peer-group
 neighbor SEDE_PRINCIPAL2 remote-as 12252
 neighbor SEDE_PRINCIPAL2 password cisco123
 neighbor SEDE_PRINCIPAL2 timers 10 30
 neighbor SEDE_PRINCIPAL2 send-community both
 neighbor SEDE_PRINCIPAL2 soft-reconfiguration inbound
 neighbor SEDE_PRINCIPAL2 route-map From_VPN_Telmex in
 neighbor SEDE_PRINCIPAL2 route-map SET_TELMEX_COMM out
 neighbor LAN_PRINCIPAL2 peer-group
 neighbor LAN_PRINCIPAL2 remote-as 64516
 neighbor LAN_PRINCIPAL2 password cisco123
 neighbor LAN_PRINCIPAL2 timers 10 30
 neighbor LAN_PRINCIPAL2 next-hop-self
 neighbor LAN_PRINCIPAL2 soft-reconfiguration inbound
 neighbor 10.10.10.9 peer-group SEDE_PRINCIPAL2
 neighbor 10.10.10.9 description enlace WAN Sede Principal 2
 neighbor 192.168.20.1 peer-group LAN_PRINCIPAL2
 neighbor 192.168.20.1 description enlace LAN Principal 2 de Contingencia
 no auto-summary
!
!
ip bgp-community new-format
!
no ip http server
no ip http secure-server
!
ip access-list extended qos2
 permit ip host 192.168.20.254 any
ip access-list extended qos5
 permit ip host 192.168.21.254 host 192.168.100.254
!
!
ip prefix-list Red_Lan seq 5 permit 0.0.0.0/0
```

```
ip prefix-list Red_Lan seq 10 permit 3.3.3.3/32
ip prefix-list Red_Lan seq 20 permit 192.168.20.0/24
!
ip prefix-list Red_Voz seq 10 permit 192.168.21.0/24
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
!
route-map SET_TELMEX_COMM permit 10
 description Envio de Redes Lan Seteados COMUNIDAD 1201
 match ip address prefix-list Red_Lan
 set community 12252:1201
!
route-map SET_TELMEX_COMM permit 15
 description Envio de Redes Voz Seteados COMUNIDAD 1200
 match ip address prefix-list Red_Voz
 set community 12252:1200
!
route-map From_VPN_Telmex deny 10
 description Denegacion de Redes LAN Internas
 match ip address prefix-list Red_Lan
!
route-map From_VPN_Telmex permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
End
```

5.3.2.3 Configuración en la sede Remota "R3 – Router Sede Trujillo"

Se realizó una configuración similar a las otras configuraciones anteriores solo que con otras ips y algunos otros parámetros:

```
R3#sh running-config
Building configuration...

Current configuration : 3137 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
```

```
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
ip cef
!
!
!
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
!
!
class-map match-any qos5
 match ip dscp cs5
class-map match-any qos1
 match ip dscp cs1
class-map match-any qos2
 match ip dscp cs2
class-map match-any P2
 match ip dscp cs2
 match access-group name qos2
class-map match-any P5
 match ip dscp cs5
 match access-group name qos5
!
!
policy-map SetDscpLan
 class P5
  set ip dscp cs5
 class P2
  set ip dscp cs2
 class class-default
  set ip dscp cs1
policy-map wan
 class qos5
  priority 64
    police 64000 12000 24000 conform-action transmit  exceed-action drop  violate-action drop
 class qos2
  bandwidth 96
    police 96000 18000 36000 conform-action transmit  exceed-action set-dscp-transmit cs1 violate-action
set-d                                                  scp-transmit 8
 class qos1
  bandwidth 128
 class class-default
  fair-queue
policy-map Shape288
 class class-default
  shape average 289000
```

```
 service-policy wan
!
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.252
!
interface FastEthernet0/0
 description Interface WAN Sede RPVL 384 Kbps - CID XXXXXX
 ip address 10.10.10.6 255.255.255.252
 speed 100
 full-duplex
 service-policy output Shape288
!
interface FastEthernet0/1
 description Interface LAN
 ip address 192.168.100.1 255.255.255.0
 speed 100
 full-duplex
 service-policy input SetDscpLan
!
router bgp 64516
 no synchronization
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 network 2.2.2.2 mask 255.255.255.255
 network 192.168.100.0
 neighbor SEDE_REMOTA peer-group
 neighbor SEDE_REMOTA remote-as 12252
 neighbor SEDE_REMOTA password cisco123
 neighbor SEDE_REMOTA timers 10 30
 neighbor SEDE_REMOTA send-community both
 neighbor SEDE_REMOTA soft-reconfiguration inbound
 neighbor SEDE_REMOTA route-map From_VPN_Telmex in
 neighbor SEDE_REMOTA route-map SET_TELMEX_COMM out
 neighbor 10.10.10.5 peer-group SEDE_REMOTA
 neighbor 10.10.10.5 description enlace WAN Sede Remota
 no auto-summary
!
!
ip bgp-community new-format
!
no ip http server
no ip http secure-server
!
ip access-list extended qos2
 permit ip any host 192.168.20.254
ip access-list extended qos5
 permit ip host 192.168.100.254 host 192.168.21.254
!
!
ip prefix-list Red_Lan seq 5 permit 0.0.0.0/0
ip prefix-list Red_Lan seq 10 permit 2.2.2.2/32
ip prefix-list Red_Lan seq 20 permit 192.168.100.0/24
!
ip prefix-list Redes_All seq 10 permit 0.0.0.0/0 le 32
!
```

```
!
!
route-map SET_TELMEX_COMM permit 10
 description Envio de Redes Lan Seteados COMUNIDAD 1200
 match ip address prefix-list Red_Lan
 set community 12252:1200
!
route-map From_VPN_Telmex deny 10
 description Denegacion de Redes LAN Internas
 match ip address prefix-list Red_Lan
!
route-map From_VPN_Telmex permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end
```

Capítulo 6: Resultados

Como resultado final se tuvo la siguiente topología simulada en el GNS3, esta simulación se asemeja a un ámbito real, donde dos redes físicamente muy distantes pueden comportarse como una sola red sin importar las limitaciones geográficas, esto gracias a las bondades de MPLS en la nube de red de nuestro proveedor Claro en donde se ejecuta ingeniería de tráfico, calidad de servicio. Esto permitió ofrecer a Comunicaciones e Informática conexión a su sede remota y viceversa. A todo esto se añadió la gestión de tráfico por medio de clases políticas y clases de tráfico para manejar por prioridad el tráfico en momentos de congestión y también políticas de prevención de congestión.

La alta disponibilidad a nivel de default gateway en la sede principal no se pudo dejar de lado por lo que se añadió un enlace redundante para cada segmento de Red ya que consta de 2 redes nuestra sede principal, una de datos y otra de voz segmentando el tráfico para que la red de datos pase por un router y la red de voz pase por nuestro otro router llamado router backup (R2) a la vez también cada uno funciona como contingencia del otro en caso suceda algún problema con alguno de los router.

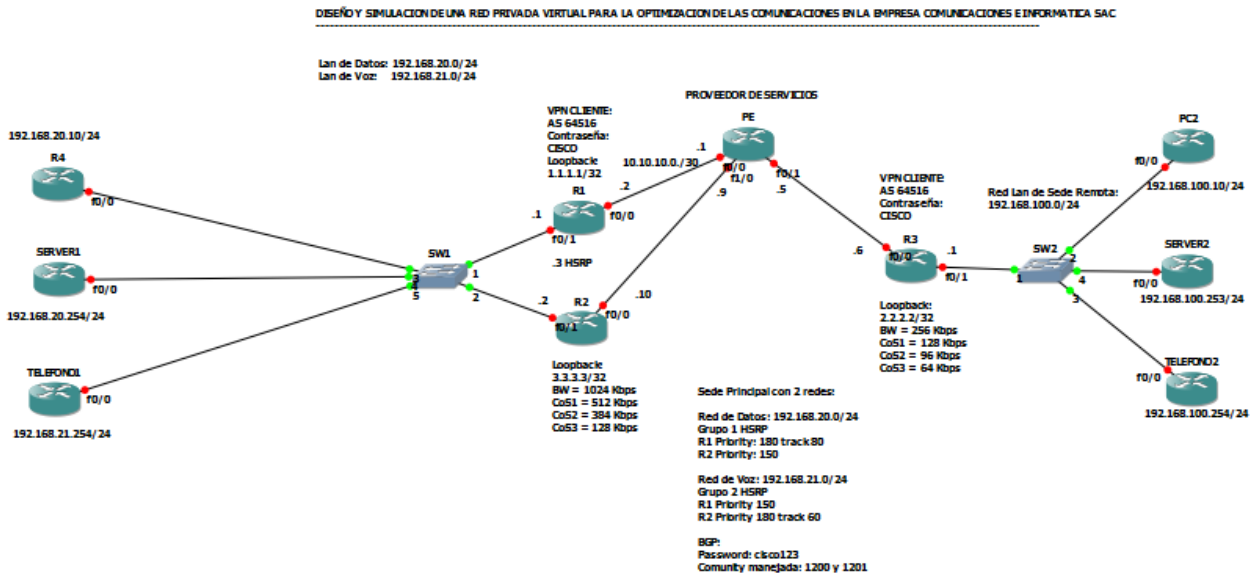


Figura 6.1: Topología Simulada. Fuente: Creación propia

Según nuestro grafico vemos que como terminales o pc tenemos configurados routers; ya que por motivos de capacidad de RAM de mi pc, en donde se realiza la simulación no me fue posible la colocación de equipos de virtual pc. Estos router-terminales cumplieron la misma función de una pc logrando hacer ping, alcanzando los quipos remotos de la otra sede.

6.1 Comandos básicos de muestra:

Show versión:

Nos mostró algunos parámetros importantes como la versión del IOS, tiempo prendido, puertos, espacios de memoria, configuración de registro.

```
R1#sh ver
Cisco IOS Software, 2600 Software (C2691-ADVENTERPRISEK9-M), Version 12.4(15)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Mon 25-Jun-07 21:33 by prod_rel_team

ROM: ROMMON Emulation Microcode
ROM: 2600 Software (C2691-ADVENTERPRISEK9-M), Version 12.4(15)T, RELEASE SOFTWARE (fc3)

R1 uptime is 33 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 2691 (R7000) processor (revision 0.1) with 187392K/9216K bytes of memory.
Processor board ID XXXXXXXXXX
R7000 CPU at 160MHz, Implementation 39, Rev 2.1, 256KB L2, 512KB L3 Cache
2 FastEthernet interfaces
DRAM configuration is 64 bits wide with parity enabled.
55K bytes of NVRAM.

Configuration register is 0x2102

R1#
```

Figura 6.2: Show Version. Fuente: Creación propia

Show inventory:

Nos mostró la serie y modelo de nuestro router.

```
R1#sh inventory
NAME: "2691 chassis", DESCR: "2691 chassis"
PID:                   , VID: 0.1, SN: XXXXXXXXXXX


R1#
```

Figura 6.3: Show Inventory. Fuente: Creación propia

Show cdp neighbors:

Nos mostró información sobre los equipos vecinos del router.

```
R1#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
PE               Fas 0/0            157         R S I     2691      Fas 0/0
TELEFONO1        Fas 0/1.2          151         R S I     2691      Fas 0/0
PC1              Fas 0/1.1          160         R S I     2691      Fas 0/0
SERVER1          Fas 0/1.1          106         R S I     2691      Fas 0/0
R2               Fas 0/1.1          153         R S I     2691      Fas 0/1.1
R1#
```

Figura 6.4: Show cdp Neighbors. Fuente: Creación propia

Show ip route:

Nos mostró la tabla de enrutamiento aprendida por nuestro router.

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     3.0.0.0/32 is subnetted, 1 subnets
B       3.3.3.3 [200/0] via 192.168.20.2, 00:38:37
     7.0.0.0/32 is subnetted, 1 subnets
B       7.7.7.7 [20/0] via 10.10.10.1, 00:36:10
C    192.168.21.0/24 is directly connected, FastEthernet0/1.2
C    192.168.20.0/24 is directly connected, FastEthernet0/1.1
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/0
B    192.168.100.0/24 [20/0] via 10.10.10.1, 00:34:42
R1#
```

Figura 6.5: Show ip route. Fuente: Creación propia

Ping a la WAN:

```
R1# ping 10.10.10.2 repeat 500 size 1500

Type escape sequence to abort.
Sending 500, 1500-byte ICMP Echos to 10.10.10.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 1/1/4 ms
R1#
```

Figura 6.6: Ping a la WAN de R1. Fuente: Creación propia

Vemos que si contó con salida (ping) hacia el siguiente salto (PE). Prueba común de conectividad.

6.2 Revisión de BGP en los routers :

6.2.1 Revisión de BGP en router principal (R1) de la sede principal:

Este protocolo fue el responsable de importar y exportar rutas en nuestro router CPE (R1) a su vez que provee respaldo al sistema de redundancia a la red de Voz de nuestra sede principal. También fue utilizado en el router PE para el intercambio de etiquetas VPN mediante MP-BGP y IBGP para el intercambio de rutas entre PE. Se utilizó el comando show ip bgp summary y show ip bgp:

Show ip bgp summary:

```
R1#sh ip bgp summary
BGP router identifier 1.1.1.1, local AS number 64516
BGP table version is 7, main routing table version 7
6 network entries using 720 bytes of memory
12 path entries using 624 bytes of memory
7/4 BGP path/bestpath attribute entries using 868 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 2 (at peak 2) using 64 bytes of memory
BGP using 2324 total bytes of memory
BGP activity 6/0 prefixes, 12/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.1      4 12252     319     317        7    0    0 00:51:53        4
192.168.20.2    4 64516     332     332        7    0    0 00:54:21        5
```

Figura 6.7: Show ip bgp summary de R1. Fuente: Creación propia

Show ip bgp :

```
R1#sh ip bgp
BGP table version is 7, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.1.1.1/32       0.0.0.0                  0         32768 i
*  3.3.3.3/32       10.10.10.1                             0 12252 12252 i
*>i                 192.168.20.2             0    100      0 i
* i7.7.7.7/32       192.168.20.2             0    100      0 12252 i
*>                  10.10.10.1               0             0 12252 i
* i192.168.20.0     192.168.20.2             0    100      0 i
*>                  0.0.0.0                  0         32768 i
*  192.168.21.0     10.10.10.1                             0 12252 12252 i
* i                 192.168.20.2             0    100      0 i
*>                  0.0.0.0                  0         32768 i
* i192.168.100.0    192.168.20.2             0    100      0 12252 12252 i
*>                  10.10.10.1                             0 12252 12252 i
R1#
```

Figura 6.8: Show ip bgp de R1. Fuente: Creación propia

6.2.2 Revisión de BGP en el router backup (R2) de la sede principal:

Show ip bgp summary:

```
R2#sh ip bgp summary
BGP router identifier 3.3.3.3, local AS number 64516
BGP table version is 7, main routing table version 7
6 network entries using 720 bytes of memory
12 path entries using 624 bytes of memory
7/4 BGP path/bestpath attribute entries using 868 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 2 (at peak 2) using 64 bytes of memory
BGP using 2324 total bytes of memory
1 received paths for inbound soft reconfiguration
BGP activity 6/0 prefixes, 12/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.9      4 12252     788     787        7    0    0 02:10:14        3
192.168.20.1    4 64516     802     802        7    0    0 02:12:46        5
```

Figura 6.9: Show ip bgp sumamry de R2. Fuente: Creación propia

Show ip bgp :

```
R2#sh ip bgp
BGP table version is 7, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  1.1.1.1/32       10.10.10.9                             0 12252 12252 i
*>i                 192.168.20.1             0    100      0 i
*> 3.3.3.3/32       0.0.0.0                  0         32768 i
* i7.7.7.7/32       192.168.20.1             0    100      0 12252 i
*>                  10.10.10.9               0             0 12252 i
* i192.168.20.0     192.168.20.1             0    100      0 i
*>                  0.0.0.0                  0         32768 i
* i192.168.21.0     192.168.20.1             0    100      0 i
*>                  0.0.0.0                  0         32768 i
* i192.168.100.0    192.168.20.1             0    100      0 12252 12252 i
*>                  10.10.10.9                             0 12252 12252 i
R2#
```

Figura 6.10: Show ip bgp de R2. Fuente: Creación propia

6.2.3 Revisión de BGP en el router Remoto (R3) de la sede de Trujillo:

Show ip bgp summary:

```
R3#sh ip bgp summary
BGP router identifier 2.2.2.2, local AS number 64516
BGP table version is 7, main routing table version 7
6 network entries using 720 bytes of memory
6 path entries using 312 bytes of memory
4/3 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1608 total bytes of memory
BGP activity 6/0 prefixes, 6/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.5      4 12252     799     797        7    0    0 02:12:09        5
R3#
```

Figura 6.11: Show ip bgp sumamry de R3. Fuente: Creación propia

Show ip bgp :

```
R3#sh ip bgp
BGP table version is 7, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.1.1.1/32       10.10.10.5                             0 12252 12252 i
*> 3.3.3.3/32       10.10.10.5                             0 12252 12252 i
*> 7.7.7.7/32       10.10.10.5               0             0 12252 i
*> 192.168.20.0     10.10.10.5                             0 12252 12252 i
*> 192.168.21.0     10.10.10.5                             0 12252 12252 i
*> 192.168.100.0    0.0.0.0                  0         32768 i
R3#
```

Figura 6.12: Show ip bgp de R3. Fuente: Creación propia

6.3 Revisión de Tablas de enrutamiento en los routers:

Veamos las rutas aprendidas y por donde estas van dirigidas según el destino:

6.3.1 Revisión de la tabla de enrutamiento en router principal (R1) de la sede principal:

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     3.0.0.0/32 is subnetted, 1 subnets
B       3.3.3.3 [200/0] via 192.168.20.2, 02:21:12
     7.0.0.0/32 is subnetted, 1 subnets
B       7.7.7.7 [20/0] via 10.10.10.1, 02:18:46
C    192.168.21.0/24 is directly connected, FastEthernet0/1.2
C    192.168.20.0/24 is directly connected, FastEthernet0/1.1
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/0
B    192.168.100.0/24 [20/0] via 10.10.10.1, 02:17:17
R1#
```

Figura 6.13: Show ip route de R1. Fuente: Creación propia

6.3.2 Revisión de la tabla de enrutamiento en router secundario (R2) de la sede principal:

```
R2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
B       1.1.1.1 [200/0] via 192.168.20.1, 02:22:28
     3.0.0.0/32 is subnetted, 1 subnets
C       3.3.3.3 is directly connected, Loopback0
     7.0.0.0/32 is subnetted, 1 subnets
B       7.7.7.7 [20/0] via 10.10.10.9, 02:20:01
C    192.168.21.0/24 is directly connected, FastEthernet0/1.2
C    192.168.20.0/24 is directly connected, FastEthernet0/1.1
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.8 is directly connected, FastEthernet0/0
B    192.168.100.0/24 [20/0] via 10.10.10.9, 02:18:32
R2#
```

Figura 6.14: Show ip route de R2. Fuente: Creación propia

6.3.3 Revisión de la tabla de enrutamiento en router remoto (R3) de la sede de Trujillo:

```
R3# sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/32 is subnetted, 1 subnets
B       1.1.1.1 [20/0] via 10.10.10.5, 02:13:57
     2.0.0.0/30 is subnetted, 1 subnets
C       2.2.2.0 is directly connected, Loopback0
     3.0.0.0/32 is subnetted, 1 subnets
B       3.3.3.3 [20/0] via 10.10.10.5, 02:13:57
     7.0.0.0/32 is subnetted, 1 subnets
B       7.7.7.7 [20/0] via 10.10.10.5, 02:13:57
B    192.168.21.0/24 [20/0] via 10.10.10.5, 02:13:57
B    192.168.20.0/24 [20/0] via 10.10.10.5, 02:13:57
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.4 is directly connected, FastEthernet0/0
C    192.168.100.0/24 is directly connected, FastEthernet0/1
R3#
```

Figura 6.15: Show ip route de R3. Fuente: Creación propia

6.4 Revisión de Listas de Acceso en los routers:

6.4.1 Revisión de las listas de acceso en el router principal (R1) de la sede principal:

```
R1#  sh access-lists
Extended IP access list qos2
    10 permit ip host 192.168.20.254 any (20 matches)
Extended IP access list qos5
    10 permit ip host 192.168.21.254 host 192.168.100.254
R1#
```

Figura 6.16: Listas de acceso de R1. Fuente: Creación propia

6.4.2 Revisión de las listas de acceso en el router secundario (R2) de la sede principal:

```
R2#sh access-lists
Extended IP access list qos2
    10 permit ip host 192.168.20.254 any (4 matches)
Extended IP access list qos5
    10 permit ip host 192.168.21.254 host 192.168.100.254 (10 matches)
R2#
```

Figura 6.17: Listas de acceso de R2. Fuente: Creación propia

6.4.3 Revisión de las listas de acceso en el router backup (R3) de la sede remota (Trujillo):

```
R3#sh access-lists
Extended IP access list qos2
    10 permit ip any host 192.168.20.254 (30 matches)
Extended IP access list qos5
    10 permit ip host 192.168.100.254 host 192.168.21.254 (14 matches)
R3#
```

Figura 6.18: Listas de acceso de R3. Fuente: Creación propia

6.5 Revisión del HSRP en los routers:

6.5.1 Revisión de los estados HSRP en el router principal (R1) de la sede principal:

```
R1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/1.1     1    180 P Active  local           192.168.20.2    192.168.20.3
Fa0/1.2     2    150 P Standby 192.168.21.2    local           192.168.21.3
R1#
```

Figura 6.19 Revisión de los estados HSRP de R1. Fuente: Creación propia

6.5.2 Revisión de los estados HSRP en el router secundario (R2) de la sede principal:

```
R2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/1.1     1    150 P Standby 192.168.20.1    local           192.168.20.3
Fa0/1.2     2    180 P Active  local           192.168.21.1    192.168.21.3
R2#
```

Figura 6.20 Revisión de los estados HSRP de R2. Fuente: Creación propia

6.6 Pruebas

6.6.1 Pruebas de conectividad entre sede y sede (Lima - Trujillo) para el caso de QOS1 es decir PC1 – PC2

```
PC1#ping
Protocol [ip]: ip
Target IP address: 192.168.100.10
Repeat count [5]: 400
Datagram size [100]: 1000
Timeout in seconds [2]: 1
Extended commands [n]: yes
Source address or interface: 192.168.20.10
Type of service [0]: 32
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 400, 1000-byte ICMP Echos to 192.168.100.10, timeout is 1 seconds:
Packet sent with a source address of 192.168.20.10
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (400/400), round-trip min/avg/max = 48/105/200 ms
PC1#
```

Figura 6.21 Pruebas de conectividad entre sede y sede (PC1 – PC2). Fuente: Creación propia

6.6.2 Pruebas de conectividad entre sede y sede (Lima - Trujillo) para el caso de QOS2 es decir SERVER1 – SERVER2

```
SERVER1#ping
Protocol [ip]: ip
Target IP address: 192.168.100.253
Repeat count [5]: 400
Datagram size [100]: 1000
Timeout in seconds [2]: 1
Extended commands [n]: yes
Source address or interface: 192.168.20.254
Type of service [0]: 64
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 400, 1000-byte ICMP Echos to 192.168.100.253, timeout is 1 seconds:
Packet sent with a source address of 192.168.20.254
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (400/400), round-trip min/avg/max = 48/106/212 ms
SERVER1#
```

Figura 6.22 Pruebas de conectividad entre sede y sede (SERVER1 – SERVER2). Fuente: Creación propia

6.6.3 Pruebas de conectividad entre sede y sede (Lima - Trujillo) para el caso de QOS3 es decir TELEFONO1 – TELEFONO2

```
TELEFONO1#ping
Protocol [ip]: ip
Target IP address: 192.168.100.254
Repeat count [5]: 400
Datagram size [100]: 200
Timeout in seconds [2]: 1
Extended commands [n]: yes
Source address or interface: 192.168.21.254
Type of service [0]: 160
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 400, 200-byte ICMP Echos to 192.168.100.254, timeout is 1 seconds:
Packet sent with a source address of 192.168.21.254
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (400/400), round-trip min/avg/max = 32/107/200 ms
TELEFONO1#
```

Figura 6.23 Pruebas de conectividad entre sede y sede (TELEFONO1 – TELEFONO2). Fuente: Creación propia

6.6.2 Pruebas de alta disponibilidad a nivel de default Gateway en la sede Principal (HSRP)

Mediante un ping continuo fue demostrado la continuidad y el tiempo que demora el router en conmutar para el cambio de ruta ya que de manera de prueba fue realizado un corte o se provocó una falla en el router principal para que conmute al router secundario o backup.

Ruta Inicial:

```
PC1#traceroute 192.168.100.10

Type escape sequence to abort.
Tracing the route to 192.168.100.10

  1 192.168.20.1 28 msec 8 msec 32 msec
  2 10.10.10.1 28 msec 52 msec 36 msec
  3 10.10.10.6 100 msec 116 msec 72 msec
  4 192.168.100.10 80 msec 116 msec 72 msec
PC1#
```

Figura 6.24 Traceroute (PC1 – PC2). Fuente: Creación propia

Estado Inicial del Router principal (R1):

```
R1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/1.1     1    180 P Active  local           192.168.20.2    192.168.20.3
Fa0/1.2     2    150 P Standby 192.168.21.2    local           192.168.21.3
R1#
```

Figura 6.25 Estado Inicial del Router principal (R1) Fuente: Creación propia

Se demostró la caída del servicio por: (12 segundos), mientras el router conmutó y levantó el servicio utilizando el protocolo HSRP:

```
PC1#ping 192.168.100.10 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.100.10, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.............!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 98 percent (987/1000), round-trip min/avg/max = 32/104/252 ms
PC1#
```

Figura 6.26 Caída del servicio por segundos Fuente: Creación propia

Ruta Final:

```
PC1#traceroute 192.168.100.10

Type escape sequence to abort.
Tracing the route to 192.168.100.10

  1 192.168.20.2 96 msec 28 msec 32 msec
  2 10.10.10.9 28 msec 76 msec 44 msec
  3 10.10.10.6 76 msec 96 msec 68 msec
  4 192.168.100.10 80 msec 128 msec 88 msec
PC1#
```

Figura 6.27 Nuevo Traceroute (PC1 – PC2).Fuente: Creación propia

Estado Final del Router principal (R1):

```
R1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/1.1     1    100 P Standby 192.168.20.2    local           192.168.20.3
Fa0/1.2     2    150 P Standby 192.168.21.2    local           192.168.21.3
R1#
```

Figura 6.28 Estado Final del Router principal (R1) Fuente: Creación propia

6.6.3 Pruebas de saturación en la sede Remota

6.6.3.1 Pruebas de saturación en QOS1

Ping de PC2 a PC1:

```
PC2#ping 192.168.20.10 repeat 1000000 size 18000

Type escape sequence to abort.
Sending 1000000, 18000-byte ICMP Echos to 192.168.20.10, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Figura 6.29 Ping de PC2 a PC1 Fuente: Creación propia

Ancho de Banda:

```
R3#sh interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c004.1af0.0000 (bia c004.1af0.0000)
  Description: Interface WAN Sede RPVL 384 Kbps - CID XXXXXX
  Internet address is 10.10.10.6/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:05, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 204000 bits/sec, 18 packets/sec
  30 second output rate 206000 bits/sec, 18 packets/sec
     22189 packets input, 29505220 bytes
     Received 70 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     22238 packets output, 29535173 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#
```

Figura 6.30 Ancho de banda. Fuente: Creación propia

Como vemos se llegó casi al ancho de banda total.

Ancho de banda por qos1:

```
        Class-map: qos1 (match-any)
          25768 packets, 35987448 bytes
          30 second offered rate 205000 bps, drop rate 0 bps
          Match: ip dscp cs1 (8)
            25768 packets, 35987448 bytes
            30 second rate 205000 bps
          Queueing
            Output Queue: Conversation 42
            Bandwidth 128 (kbps)Max Threshold 64 (packets)
            (pkts matched/bytes matched) 21511/29987013
        (depth/total drops/no-buffer drops) 2/0/0
```

Figura 6.31 Ancho de banda por qos1. Fuente: Creación propia

Vemos según nuestra figura que nuestro ancho de banda respectivo para qos1 es 128 kbps pero se llegó a 205 kbps dado que qos1 puede disponer del total del enlace mientras no estén ocupados los demás.

6.6.3.2 Pruebas de saturación en QOS2

Ping de SERVER2 a SERVER1:

```
SERVER2#ping 192.168.20.254 repeat 10000000 size 18000

Type escape sequence to abort.
Sending 10000000, 18000-byte ICMP Echos to 192.168.20.254, timeout is 2 seconds:
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Figura 6.32 Ping (Server1 – Server2). Fuente: Creación propia

Ancho de Banda:

```
R3#sh inter fastEthernet
% Incomplete command.

R3#sh inter fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c004.1af0.0000 (bia c004.1af0.0000)
  Description: Interface WAN Sede RPVL 384 Kbps - CID XXXXXX
  Internet address is 10.10.10.6/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 205000 bits/sec, 18 packets/sec
  30 second output rate 206000 bits/sec, 18 packets/sec
     41941 packets input, 57181243 bytes
     Received 87 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     41989 packets output, 57202503 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#
```

Figura 6.33 Ancho de banda. Fuente: Creación propia

De la misma manera se llegó casi al ancho de banda total del enlace.

Ancho de banda por qos2

```
Class-map: qos2 (match-any)
  7597 packets, 10640438 bytes
  30 second offered rate 201000 bps, drop rate 0 bps
  Match: ip dscp cs2 (16)
    7597 packets, 10640438 bytes
    30 second rate 201000 bps
  Queueing
    Output Queue: Conversation 41
    Bandwidth 96 (kbps)Max Threshold 64 (packets)
    (pkts matched/bytes matched) 6409/8932079
(depth/total drops/no-buffer drops) 4/0/0
  police:
      cir 96000 bps, bc 18000 bytes, be 36000 bytes
    conformed 4063 packets, 5374382 bytes; actions:
      transmit
    exceeded 27 packets, 35838 bytes; actions:
      set-dscp-transmit cs1
    violated 3507 packets, 5230218 bytes; actions:
      set-dscp-transmit cs1
    conformed 95000 bps, exceed 0 bps, violate 105000 bps
```

Figura 6.34 Ancho de banda por qos2. Fuente: Creación propia

Vemos en nuestra figura que el ancho de banda llegó a 201 kbps, pero porque si nuestro ancho de banda para QOS2 es 96 kbps. Esta situación se debió a que la política de QOS2 es que cuando sobrepase los 96 kbsp disponga del ancho de banda destinado para QOS1 y como sabemos qos1 puede tomar todo el ancho de banda del enlace. En la parte final de la figura vemos (violate 105000 bps) que es el ancho de banda que sobrepasó para qos2 y que está siendo pasado para el espacio de qos1.

6.6.3.3 Pruebas de saturación en QOS3

Ping de TELEFONO2 a TELEFONO1:

```
TELEFONO2#ping 192.168.21.254 repeat 10000000 size 800

Type escape sequence to abort.
Sending 10000000, 800-byte ICMP Echos to 192.168.21.254, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Figura 6.35 Ping de Telefono2 a Telefono1. Fuente: Creación propia

Ancho de Banda:

```
R3#sh inter fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c004.1af0.0000 (bia c004.1af0.0000)
  Description: Interface WAN Sede RPVL 384 Kbps - CID XXXXXX
  Internet address is 10.10.10.6/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:04, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:06:53
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 5
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 58000 bits/sec, 11 packets/sec
  30 second output rate 57000 bits/sec, 11 packets/sec
     3512 packets input, 2794879 bytes
     Received 7 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     3519 packets output, 2799268 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#
```

Figura 6.36 Ancho de banda. Fuente: Creación propia

De la misma manera se llegó casi al ancho de banda de qos3 pero no al total del enlace como casos anteriores. Ya que qos3 solo dispone de su ancho de banda asignado y este no puede disponer de los anchos de banda de los otros qos.

Ancho de banda por qos3

```
        Class-map: qos5 (match-any)
          4471 packets, 3639394 bytes
          30 second offered rate 61000 bps, drop rate 0 bps
          Match: ip dscp cs5 (40)
            4471 packets, 3639394 bytes
            30 second rate 61000 bps
          Queueing
            Strict Priority
            Output Queue: Conversation 40
            Bandwidth 64 (kbps) Burst 1600 (Bytes)
            (pkts matched/bytes matched) 0/0
            (total drops/bytes drops) 0/0
          police:
              cir 64000 bps, bc 12000 bytes, be 24000 bytes
            conformed 4462 packets, 3632068 bytes; actions:
              transmit
            exceeded 10 packets, 8140 bytes; actions:
              drop
            violated 0 packets, 0 bytes; actions:
              drop
            conformed 61000 bps, exceed 0 bps, violate 0 bps
```

Figura 6.37 Ancho de banda por qos3. Fuente: Creación propia

En la siguiente figura apreciamos que ya hubo pérdida de paquetes ya que se saturó el enlace de 64 kbps para lo que es qos3.

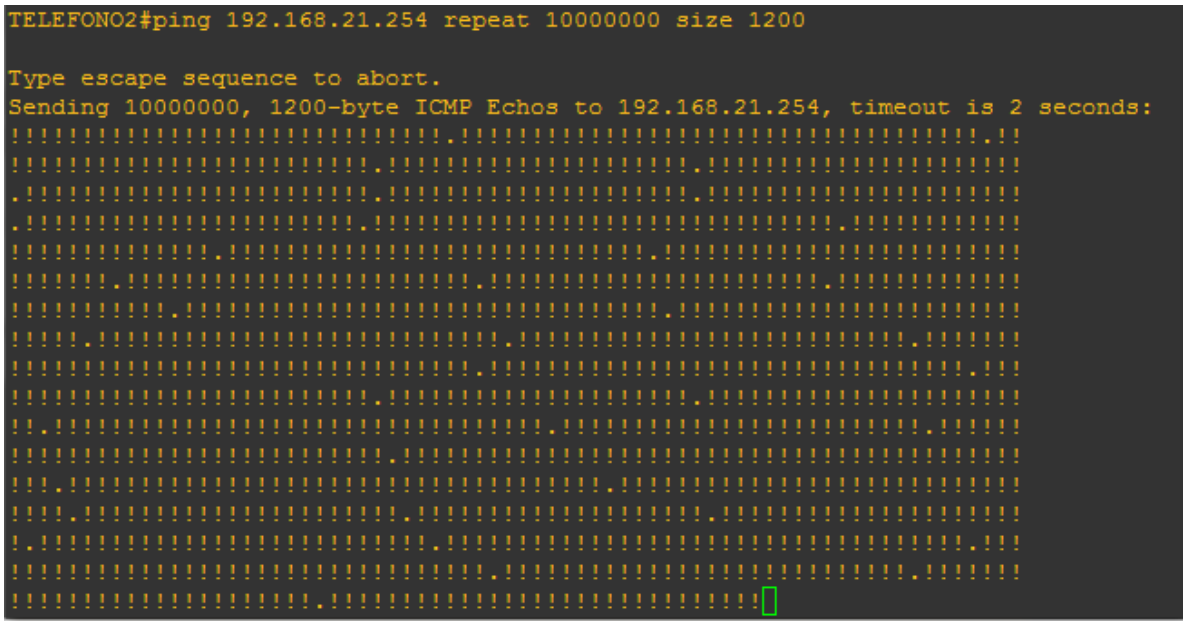


Figura 6.38 Perdida de paquetes. Fuente: Creación propia

Y en la muestra de la interface vemos que ya está dropeó, es decir, descartó paquetes a pesar de que no está llegando al ancho de banda total como en los casos anteriores de qos1 y qos2. Esto es debido a políticas ya configuradas que solo permiten para el tráfico de qos3 que es de Voz y video, permitirle lo fijado y dropear (descartar) si es que sobrepasa este límite.

```
R3#sh inter fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c004.1af0.0000 (bia c004.1af0.0000)
  Description: Interface WAN Sede RPVL 384 Kbps - CID XXXXXX
  Internet address is 10.10.10.6/30
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:07, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:21:06
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 96
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 54000 bits/sec, 5 packets/sec
  30 second output rate 54000 bits/sec, 5 packets/sec
     8038 packets input, 7262362 bytes
     Received 21 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     8057 packets output, 7279515 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#
```

Figura 6.39 Dropeando. Fuente: Creación propia

Dropeó o descarte de paquetes, como vemos en la imagen fueron 96 paquetes descartados.

```
        Class-map: qos5 (match-any)
          6287 packets, 5436418 bytes
          30 second offered rate 57000 bps, drop rate 1000 bps
          Match: ip dscp cs5 (40)
            6287 packets, 5436418 bytes
            30 second rate 57000 bps
          Queueing
            Strict Priority
            Output Queue: Conversation 40
            Bandwidth 64 (kbps) Burst 1600 (Bytes)
            (pkts matched/bytes matched) 0/0
            (total drops/bytes drops) 0/0
          police:
              cir 64000 bps, bc 12000 bytes, be 24000 bytes
            conformed 6247 packets, 5392658 bytes; actions:
              transmit
            exceeded 40 packets, 43760 bytes; actions:
              drop
            violated 0 packets, 0 bytes; actions:
              drop
            conformed 55000 bps, exceed 1000 bps, violate 0 bps
```

Figura 6.40 Dropeando a 1000 bps. Fuente: Creación propia

En esta figura apreciamos que dropeó o descartó paquetes a un promedio de 1000 bps promediado en 30 segundos. Y no consume ancho de banda de los otros qos como apreciamos en la última línea (violate 0 bps).

Conclusiones

- Se presentó una solución Red WAN para la empresa Comunicaciones e Informática para que pueda ser implementada o dirigida hacia una red MPLS de un proveedor de servicios (Claro) donde pueden converger todos sus servicios en una misma plataforma.

- La comunicación otorgada por la VPN fue transparente porque permitió establecer un enlace de comunicación directa entre dos computadoras, sin preocupación de la infraestructura física de la red existente y de los equipos que la conformaban.

- El protocolo BGP presentó muchas opciones para forzar medidas administrativas de rutas, lo que garantizó una tabla de enrutamiento eficiente.

- El protocolo HSRP provee alta disponibilidad a nivel de default Gateway en la red LAN de la sede Principal; además de segmentar la carga en los routers administrando números de grupos y utilizando solo una dirección ip virtual.

- La gestión de tráfico para afrontar momentos de congestión provee una solución a los cuellos de botella en la salida de tráfico y a la fácil solución de aumentar el ancho de banda.

Recomendaciones

- Si por algún motivo la empresa Comunicaciones e Informática desea incrementar la capacidad de sus enlaces, deberá considerar cambiar el router CPE, debido a que cada modelo posee limitaciones en cuanto a procesamiento, se sabe además que a mayor comando ejecutado mayor es el procesamiento.

- En la implementación del BGP se deberá tener en cuenta que por cada red añadida no solo se tiene que realizar la configuración de la interfaces sino que también conllevan a la agregación de la misma en la lista de prefijos y en el protocolo de enrutamiento BGP con el comando network.

- Con respecto al HSRP, se deberá considerar las capacidades del router debido a que esto aumenta la carga sobre él, en caso se esté utilizando diferentes modelos o marcas.

- Tener en cuenta que no se deberá saturar el ancho de banda máximo sumado a los picos de ancho de banda configurado para el cos5 de lo contrario descartara paquetes y se perderá información.

Referencias Bibliográficas

Arias Sanchez, P. X. (2011). *Diseño de una red Lan/Wan segura para el Tribunal Constitucional aplicando la metodologia de 3 capas de Cisco.* Pontifia Universidad Catolica del Ecuador, Quito.

Barbancho Concejero, J., & Benjumea Mondejar, O. (2014). *Redes locales.* Paraninfo S.A.

Bermudez Luque, J. J., & Bermudez Luque, D. (2016). *Montaje de infraestructuras de redes locales de datos. ELES0209.* Malaga: IC Editorial.

Bidgoli, H. (2006). *Handbook of Information Security* (Vol. 3). (Editor-in-Chief, Ed.) Bakersfield, California, EEUU: John Wiley & Sons.

Carballar Falcón, J. A. (2007). *VoIP : la telefonia de Internet.* Madrid, España: Paraninfo.

Carmelo Fernandez Garcia, J., & Barbado Santana, A. (2008). *Instalaciones de telefonia. Practicas.* Madrid, España: Paraninfo.

Castro Lechtaler, A. R., & Fusario, R. J. (2010). *Teleinformatica* (2 ed.). Barcelona, España: Reverte.

Cubas Diaz, G. Y., & Perales Fabian, M. H. (2011). *Rediseño de la Red Wan de la Empresa EPSEL S.A.* Universidad Señor de Sipan, Pimentel.

Dembowski, K. (2033). *Gran libro del hardware.* Zaragoza, España: Marcombo.

Diane, P. C. (2006). *Campus Network Design Fundamentals.* Indianapolis, USA: Cisco Press.

Diane, P. C. (2006). *Campus Network Design Fundamentals.* Indianapolis USA: Cisco Press.

Garcia, G. (2009). Propuesta de Migración de la Red NGN de una Operadora Implementada en IP hacia MPLS. Pontificia Universidad Católica del Perú, Lima, Peru.

Gil Vazquez, P., Pomares Baeza, J., & Candelas Herias, F. (2010). *Redes y transmksion de datos.* Alicante, España: Publicaciones Universidad de Alicante.

Holgado Saez, C. (2016). *Nuevos Tiempos Universidad y Tic's.* Area de Innovacion y desarrollo.

Lavado, G. (2010). MPLS-Multiprotocol Label Switching. Versión 1.0

Limari, R. V. (2004). Protocolos de Seguridad para Redes Privadas Virtuales (VPN). Universidad Austral de Chile Valdivia, Chile.

Mahmoud, M. (2008). Inter - AS MPLS VPN – The Whole Story. USA.

Morales, B. (2006) Investigación de Redes VPN con Tecnología MPLS. Universidad de las Américas Puebla, México

Netacad, Cisco System (2016). Infraestructura WAN privada

Pepelnjak, I. & Guichard, J. (2002). *MPLS and VPN Architectures.* Indianapolis, USA: Cisco Press.

Perez, D. (2013). CCNP SWITCH- Alta disponibilidad y redundancia, HSRP, VRRP Y GLBP.

Redón Gómez, H. R. (2007). *El periodista digital mexicano: Hacia su definición.* Universidad Nacional Autonoma de Mexico, Mexico.

Robles, M. (2008). *QoS en redes Wireless con IPv6.* Universidad Nacional de la Plata.

System, C. (2010). *Guia de primer año CCNA* (4ta Edicion ed.). Pearson Education S.A.

Teldat, (2008). Protocolo BGP. Indianapolis, USA.

Vaucamps, A. (2011). *CISCO. INSTALAR Y CONFIGURAR UN ROUTER.* Eni Ediciones.

Velasquez Zeballos, J. V., & Padilla Diaz, L. H. (2006). *Rediseño de la Red de Datos (WAN) de Banpro incorporando nuevas tecnologias de telecomunicaciones.* Universidad Simon Bolivar.

Zuñiga Lopez, V. (2005). *Redes transmisionde datos.* Universidad autonoma del estado de Hidalgo.

ANEXO
MATRIZ DE COHERENCIA INTERNA

	PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES
GENERAL	¿En qué medida el diseño de una Red Privada Virtual influirá en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC?	Determinar la influencia del diseño de una Red Privada Virtual en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.	El diseño de una Red privada virtual influirá en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.	Independiente: Diseño de una Red Privada Virtual VPN.	• Funcionabilidad • Confiabilidad • Seguridad
ESPECÍFICO	¿En qué medida el nivel de funcionalidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC?	Determinar el nivel de funcionalidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.	El nivel de funcionalidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.	Dependiente: Optimización de las comunicaciones	• Evaluaciones o pruebas. • Inspecciones en cableado. • Equipos de Red. • Infraestructura de Red (medios).
	¿En qué medida el nivel de confiabilidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC?	Determinar el nivel de confiabilidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.	El nivel de confiabilidad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.		
	¿En qué medida el nivel de seguridad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC?	Determinar el nivel de seguridad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.	El nivel de seguridad del diseño de una Red Privada Virtual influye en la optimización de las comunicaciones para la empresa Comunicaciones e Informática SAC.		