DISEÑO DE UNA RED BASADA EN MPLS PARA EL SISTEMA DE TELEMETRÍA DEL OBSERVATORIO VULCANOLÓGICO Y SISMOLÓGICO DE PASTO

RICHARD ANDRÉS MIER PORTILLA

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de I+D Nuevas Tecnologías en Telecomunicaciones
MAESTRÍA EN TELECOMUNICACIONES
Popayán, Cauca.
2019

DISEÑO DE UNA RED BASADA EN MPLS PARA EL SISTEMA DE TELEMETRÍA DEL OBSERVATORIO VULCANOLÓGICO Y SISMOLÓGICO DE PASTO

RICHARD ANDRÉS MIER PORTILLA

Trabajo de grado para optar al título de:

MAGISTER EN TELECOMUNICACIONES

Director:

Ing. Guefry Agredo Méndez, PhD.

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de I+D Nuevas Tecnologías en Telecomunicaciones
MAESTRÍA EN TELECOMUNICACIONES
Popayán, Cauca.
2019

Agradecimientos

Nuestro agradecimiento a la Universidad del Cauca, por permitirnos culminar con éxitos esta maestría y suministrarnos todas las herramientas y equipos necesarios para el desarrollo del presente trabajo de grado. El desarrollo de este trabajo no habría sido posible sin la disponibilidad del SERVICIO GEOLÓGICO COLOMBIANO por permitirnos desarrollar el trabajo en el Observatorio Pasto. También agradecer al director de trabajo de grado Ing. Guefry Agredo Méndez, PhD, por su colaboración y guía en este proceso.

Resumen estructurado

Antecedentes: el constante aumento de estaciones para el monitoreo volcánico y la demanda de alto desempeño de la red implican nuevos retos para el despliegue de los sistemas de Telemetría basados en comunicación inalámbrica, que pese a todas las limitaciones deben satisfacer los requerimientos propios del proceso de vigilancia volcánica. El control de tráfico y la calidad de servicio (QoS, *Quality of Service*) es particularmente importante para el transporte de datos con requerimientos especiales sobre todo en redes con bajas prestaciones; en el proceso de vigilancia y monitoreo volcánico existen varias técnicas y cada una genera tráfico específico el cual debe ser diferenciado y priorizado para responder a eventos que afecten el rendimiento y disponibilidad de la red.

El diseño de una red basada en la Conmutación de Etiquetas Multiprotocolo (MPLS, *Multiprotocol Label Switching*) aplicada a la telemetría en el Observatorio Pasto, es apto para la soportar la convergencia en de redes de altas prestaciones.

Objetivos:

- Caracterizar la red de telemetría del Observatorio Vulcanológico y Sismológico de Pasto (OVSP) del Servicio Geológico Colombiano (SGC)
- Estimar el porcentaje de disponibilidad y capacidad máxima de transmisión en tramos principales de la red actual de telemetría.
- Determinar los requerimientos de calidad de servicio, disponibilidad y rendimiento de la red de telemetría.
- Diseñar la red de telemetría en capa 3 de OSI.

Método: se tomó apartes de la metodología *Top Down* que permitió analizar el estado actual, se realizó visitas a la infraestructura del instituto, posteriormente se diseñó la red de telemetría basada en la tecnología MPLS, así como también se implementó un prototipo utilizando el sistema operativo *RouterOS* de Mikrotik en su versión virtual [1]

(CHR, *Cloud Hosted Router*) implementado en la herramienta de simulación GNS3 1.1.12 [2].

Resultados:

- El tráfico *Broadcast* del dominio perteneciente a las redes 10.0.1.0/24 y 10.0.1.10/24, se registra entre 10 y 12 Kbps de manera permanente.
- La capacidad de transmisión en los enlaces troncales está entre 40 Kbps para la repetidora Cráter y 24600 Kbps para la repetidora Cruz de Amarillo.
- La capacidad mínima requerida en los enlaces troncales está entre 125 y 480 Kbps.
- La capacidad mínima requerida en los enlaces secundarios está entre 30 y 200 Kbps.
- La capacidad requerida por cada sensor varía entre 2 y 128 Kbps. Una estación sísmica triaxial de banda ancha a 100 muestras por segundo, transmitiendo a 32 bits y datos continuos (enjambre de sismos) requiere mínimo 30 Kbps.
- La intensidad de señal recibida, la capacidad de los enlaces, la pérdida y retransmisión de paquetes están ligados con la distancia entre los nodos, así como también los obstáculos presentes, la variación del clima y también la cantidad de tráfico en los mismos.
- Los resultados obtenidos al implementar un prototipo en la plataforma GNS3, muestran que con la priorización de paquetes, se logran desempeños adecuados que a través de una arquitectura redundante permiten soportar fallos y permitir el tráfico de datos mínimo necesario para la evaluación del fenómeno volcánico.

Conclusiones:

1. En la red de Telemetría del Observatorio Pasto, los parámetros importantes a tener en cuenta para garantizar la capacidad de transmisión requerida en los enlaces inalámbricos son:
    - Nivel de señal a ruido (SNR, Signal to Noise Ratio) superior a 25 dBm
    - Entre 10 y 15 dBm de guarda en el nivel de señal para soportar condiciones anómalas que puedan degradar la conexión.
    - Frecuencia y potencia acorde a las normas actuales en relación a comunicaciones inalámbricas.

2. La arquitectura y diseño actual de la red de Telemetría del Observatorio Pasto en algunos tramos no cumple con el requerimiento mínimo en capacidad de

Transmisión de la red, sin embargo, con actividad volcánica baja, la red opera con normalidad.

3. Con la priorización de paquetes, se logran desempeños adecuados que, a través de una arquitectura redundante, permite soportar fallos y garantizar el tráfico mínimo de datos necesario para la evaluación del fenómeno volcánico.

4. Una red basada en la tecnología MPLS mejora considerablemente la calidad del dato con respecto a las técnicas tradicionales de transporte de datos y reduce la incertidumbre para la toma de decisiones.

5. El uso de equipos Mikrotik hace posible implementar arquitecturas como MPLS-TE que hace poco se limitaba a dispositivos de gama alta como Cisco, Juniper Networks, Arista Networks entre otros, adicionalmente con herramientas como GNS3 se puede utilizar en un entorno de desarrollo o pruebas pre-producción de manera virtual.

6. La participación de la red pública de internet en la red de Telemetría y monitoreo volcánico, puede considerarse positiva en relación al uso de infraestructura y servicios que pueden aportar a diseños de sistemas redundantes.

7. La implementación de sistemas de monitorización y gestión de la red de Telemetría en el Observatorio Pasto, permite una gestión oportuna de incidentes y posibilita mejorar la red continuamente.

Palabras Clave: Telemetría, Calidad de servicio, MPLS, Control de tráfico

Structured Abstract

Background: The constant increase of stations for volcanic monitoring and the high performance demand of the network imply new challenges for the deployment of telemetry systems based on wireless communication, which despite all the limitations must satisfy the requirements of the volcanic monitoring process. Traffic control and *Quality of Service* is particularly important for the transport of traffic with special requirements, especially in networks with low benefits; In the process of volcanic monitoring there are several techniques and each generates specific traffic which can be differentiated and prioritized to respond to events that affect the performance and availability of the network.

The design of a network based on MPLS applied to telemetry in the Pasto Observatory, is suitable to support the convergence of high-performance networks.

Aims:

- Characterize the OVSP telemetry network
- Estimate the percentage of availability and maximum transmission capacity in main links of the current telemetry network.
- Determine the service quality, availability and performance requirements of the telemetry network.
- Design the telemetry network in layer 3 of OSI.

Methods: In this master's thesis, a apart from the *Top-Down* methodology was taken that allowed analyzing, designing the telemetry network based on MPLS technology, as well as implementing a prototype using MikroTik Cloud Hosted Router appliance implemented on GNS3 software.

Results:

- Broadcast traffic of the domain belonging to networks 10.0.1.0/24 and 10.0.1.10/24, is recorded between 10 and 12 Kbps permanently.
- The transmission capacity in the trunk links is between 40 Kbps for the Crater repeater and 24600 Kbps for the Cruz de Amarillo repeater.
- The minimum capacity required in the trunk links is between 125 and 480 Kbps.
- The minimum capacity required in secondary links is between 30 and 200 Kbps.
- The capacity required by each sensor varies between 2 and 128 Kbps. A broadband three-component digital seismometer station and 100 samples per second, transmitting at 32 bits and continuous data (earthquake swarm) requires a minimum of 30 Kbps.
- The received signal strength, the capacity of the links, the loss and retransmission of packets are linked to the distance between the nodes, as well as the obstacles present, the variation of the climate and also the amount of traffic in them.
- The results obtained by implementing a prototype on the GNS3 platform, show that with the prioritization of packets, adequate performance is achieved through a redundant architecture to support phalluses and provide a minimum of data for the evaluation of the volcanic phenomenon.

Conclusions:

1. The susceptible parameters to be taken into account were identified to guarantee the required transmission capacity in the wireless links, which were:

- Signal level noise greater than 25 dBm
- It should be considered 10 to 15 dBm of guard at the signal level to withstand anomalous conditions that may degrade the connection.
- Adjust the wireless parameters necessary to comply with the current regulations in relation to Radio Frequency communications.

2. The current architecture and design of the Telemetry network of the Pasto Observatory in some sections does not comply with the minimum requirement in transmission capacity of the network, however in idle conditions, the network operates normally.

3. With the prioritization of packages, adequate performance is achieved through a redundant architecture to support phalluses and provide a minimum of data for the evaluation of the volcanic phenomenon.

4. An MPLS network was designed to significantly improve data quality with respect to traditional data transport techniques.

5. The use of Mikrotik equipment makes it possible to implement architectures such as MPLS-TE that was recently limited to devices of the range of Cisco, Juniper Networks, Arista Networks among others, additionally with tools such as GNS3 can be used in a development environment or pre-testing virtually.

6. The participation of the public internet network in the Telemetry and volcanic monitoring network can be considered positive in relation to the use of infrastructure and services that can contribute to redundant system designs.

7. The implementation of monitoring and management systems for the Telemetry network at the Pasto Observatory, allows for timely management of incidents and makes it possible to continuously improve the network.

Keywords: Telemetry, Quality of service, MPLS, Traffic control

Contenido

Lista de figuras

Lista de tablas

Lista de anexos

Lista de acrónimos

ATM	*Asynchronous Transfer Mode,* Modo de transferencia asíncrona
BGP	*Border Gateway Protocol,* Protocolo de puerta de enlace de frontera
CR-LDP	*Constraint-Based Label Distribution Protocol,* Protocolo de distribución de etiquetas basado en restricciones
DSSS	*Direct Sequence Spread Spectrum,* Espectro ensanchado de secuencia directa
EIGRP	*Enhanced Interior Gateway Routing Protocol,* Protocolo mejorado de Enrutamiento de Puerta de enlace Interior
FHSS	*Frequency Hopping Spread Spectrum,* Espectro ensanchado por salto de frecuencia
IEEE	*Institute of Electrical and Electronics Engineers,* Instituto de Ingeniería Eléctrica y Electrónica
IETF	*Internet Engineering Task Force,* Grupo de Trabajo de Ingeniería de Internet
IGP	*Interior Gateway, Protocol* Protocolo de Pasarela Interna
IOS	*Internetwork Operating System,* Sistema operativo de interconexión de redes
IS-IS	*Intermediate System to Intermediate System,* Sistema intermedio a sistema intermedio
LDP	*Label Distribution Protocol,* Protocolo de distribución de etiquetas
LSDB	*Link-State Database,* Base de datos de estados de enlace
MAC	*Media Access Control,* Control de acceso al medio
MPLS	*Multiprotocol Label Switching,* Conmutación de etiquetas multiprotocolo
OFDM	*Orthogonal Frequency Division Multiplexing,* Multiplexación por división de frecuencias ortogonales
OSI	*Open System Interconnection,* Modelo de interconexión de sistemas abiertos
OSPF	*Open Shortest Path First,* Abrir primero la ruta más corta
OVSP	Observatorio Vulcanológico y Sismológico de Pasto
QoS	*Quality of Service,* Calidad de servicio
RIP	*Routing Information, Protocol* Protocolo de información de enrutamiento
RSVP	*Resource Reservation, Protocol* Protocolo de reserva de recursos
RSVP-TE	*Resource Reservation Protocol - Traffic Engineering,* Protocolo de reserva de recursos en ingeniería de tráfico
SGC	Servicio Geológico Colombiano
SLA	*Service Level Agreement,* Acuerdo de nivel de servicio
STP	*Spanning Tree, Protocol* Protocolo de árbol de expansión
TE	*Traffic Engineering,* Ingeniería de tráfico
VPN	*Virtual Private Network,* Red privada virtual
WWAN	*Wireless Wide Area Network,* Red inalámbrica de área amplia

Capítulo 1

1. INTRODUCCIÓN

El Servicio Geológico Colombiano (SGC), a través de los Observatorios Vulcanológicos y Sismológicos ubicados en las ciudades de Pasto, Popayán y Manizales, cumple con la actividad misional asociada al monitoreo de la actividad sísmica y volcánica del país. En el sur de Colombia, el Observatorio Vulcanológico y Sismológico Pasto (OVSP), cuenta con una red inalámbrica de cobertura amplia que transporta datos desde los sensores en campo hasta el sistema de adquisición y procesamiento en el Observatorio (Red de telemetría).

El constante aumento de estaciones para el monitoreo y la demanda de alto desempeño de la red implican nuevos retos para el despliegue de los sistemas de Telemetría basados en comunicación inalámbrica, que pese a todas las limitaciones deben satisfacer los requerimientos propios del proceso de vigilancia volcánica.

La red de telemetría del Observatorio Pasto [3],está basada en una red conmutada que se extiende a través de enlaces punto a punto y punto multipunto usando frecuencias en bandas libres de 900 MHz y 5 GHz, la mayoría de los equipos tienen un diseño industrial que soportan condiciones atmosféricas adversas cuyo resultado es una conectividad con bajas prestaciones.

En la arquitectura actual, el tráfico concurrente en varios puntos de la red, debe competir por los recursos disponibles generando retransmisión, pérdida y rechazo de paquetes, adicionalmente el flujo permanente y en ráfagas de paquetes *Broadcast* reducen el porcentaje de utilidad de cada enlace, esto ocasiona una disminución de la capacidad de transmisión y tiene un impacto negativo en el proceso de adquisición y procesamiento de datos.

En este trabajo de grado se hizo un análisis de la red de Telemetría y se realizó el diseño de una red basada en tecnología MPLS para soportar eventos en los cuales múltiples aplicaciones deben competir por los recursos disponibles en la red, garantizando reserva de recursos para aplicaciones sensibles al retardo que en su aplicación puede mejorar el desempeño[1] de la red actual del Observatorio Vulcanológico y Sismológico de Pasto

Para Latinoamérica en los países de Ecuador, Chile y Costa Rica, como parte del presente trabajo se realizó una consulta general sobre las redes de Telemetría, que en su mayoría usan redes privadas para el transporte de datos sin implementar mecanismos de calidad de servicio. En Ecuador la mayor parte de la red de transporte es contratada a través de un prestador de servicios de internet.

Este trabajo de grado se presenta de la siguiente forma:

El capítulo 2, presenta los aspectos generales de las redes de telemetría en Ecuador, Chile, Costa Rica y Colombia, generalidades sobre la tecnología MPLS como sus componentes y capacidades, finalmente la generalidad del protocolo de enrutamiento del camino más corto (OSPF, *Open Shortest Path First*) e ingeniería de tráfico (TE, *Traffic Engineering*).

El capítulo 3, presenta la metodología empleada, la caracterización de la Red de Telemetría, análisis de algunos parámetros de comunicación para determinar el rendimiento y disponibilidad de los enlaces principales, determinar los requerimientos de calidad de servicio y diseño de una basada en MPLS.

El capítulo 4, a partir de un prototipo, presenta el plan de pruebas, la selección de dispositivos, configuración, los resultados y la evaluación de la red.

El capítulo 5, presenta las conclusiones y recomendaciones del trabajo de grado.

[1] Entiéndase como desempeño, el análisis de los parámetros de la red de datos a nivel de la capa de enlace tales como *Throughput, Latency, Frame loss* y *Burst* en concordancia con el RFC-2544.

Capítulo 2

2. GENERALIDADES

En este capítulo se muestra aspectos generales sobre el estado de las implementaciones de redes de telemetría realizadas a nivel institucional en los Observatorios de Popayán y Manizales, así como también en entidades pares en los países de Ecuador, Chile y Costa Rica (los datos se obtuvieron a través de una solicitud realizada desde el servicio SGC a los encargados en telemetría de cada entidad), también se presentan los aspectos generales sobre los protocolos IP versión 4 y OSPF, Calidad de servicio y de la tecnología MPLS.

2.1. Redes de Telemetría

Lo primero que se debe entender cuando se aborda la definición de red de telemetría es el concepto de red de telecomunicaciones, según el Ministerio de las Telecomunicaciones de Colombia una red de telecomunicaciones es un conjunto de nodos y enlaces alámbricos, inalámbricos, ópticos u otros sistemas electromagnéticos, incluidos todos sus componentes físicos y lógicos necesarios, que proveen conexiones entre dos o más puntos fijos o móviles, terrestres y/o espaciales [4].

Para el Servicio Geológico Colombiano, una red de telemetría es un conjunto de nodos y enlaces que proveen conexión entre dos o más puntos con el fin de hacer mediciones remotas de magnitudes físicas o químicas [3], por ejemplo, medir la inclinación de las capas tectónicas en el estudio sísmico, o el comportamiento de una tormenta en el campo de la climatología. En una red de sensores existen cuatro componentes

básicos: (1) un conjunto de sensores distribuidos o localizados; (2) una red de interconexión (generalmente, pero no siempre, basada en la conexión inalámbrica); (3) un punto central de agrupamiento de información; y (4) un conjunto de recursos informáticos en el punto central (o más allá) para manejar la correlación de datos, tendencias de eventos, consultas de estado y extracción de datos [3].

La importancia de las redes de telemetría se debe a la facilidad en la recolección de datos que brindan al investigador, lo cual permite una mayor precisión al momento de estudiar un fenómeno en cuestión, pues al transmitir los datos a un centro de control remoto reduce la incertidumbre en el proceso de monitoreo, logrando agilizar la capacidad de respuesta en la interpretación de la persona encargada del estudio, monitoreo o cualquiera que sea el fin de esta información.

En este trabajo se tomó como referencia las instituciones relacionadas con la vigilancia y monitoreo de volcanes en los países de Ecuador, Chile y Costa Rica, dado que cuentan con una infraestructura y esquema de operación equivalente al de Colombia.

2.1.1. Instituto Geofísico EPN (Escuela Politécnica Nacional) – Ecuador

Redes de transmisión [5]

Con la finalidad de tener todas las señales generadas en las estaciones de monitoreo sísmico y volcánico en tiempo real, el Instituto Geofísico diversifico los medios de transmisión de datos para garantizar confiabilidad y en casos de estaciones estratégicas, redundancia de información, El Instituto cuenta con las siguientes redes:

- Transmisión por fibra óptica
- Transmisión por la red central de microondas
- Transmisión por la red satelital
- Transmisión por tecnología *Spread Spectrum*
- Transmisión por WiFi de largo alcance
- Transmisión analógica en frecuencia ultra alta (UHF, *Ultra High Frequency*)
- Transmisión por *Internet*
- En conjunto la red de transporte de datos se basa en una red ruteada IP.
- Se ha implementado listas de control de acceso (ACL, *Access Control List*) necesarias que mejoran la seguridad tanto en la red privada como el acceso a la pública.
- Se implementa QoS básicamente a nivel de VLAN garantizando la capacidad de canal”

2.1.2. El Servicio Nacional de Geología y Minería (Sernageomin) – Chile

Observatorio Vulcanológico de Los Andes del Sur (OVDAS) [6]

Una de las áreas científico-técnicas del Servicio Nacional de Geología y Minería (Sernageomin) está compuesta por el OVDAS, centro de interpretación de datos de la Red Nacional de Vigilancia Volcánica de la institución. Este observatorio del Sernageomin está localizado en la ciudad de Temuco, región de la Araucanía.

Las estaciones de vigilancia y nodos de transmisión de datos, instalados en el perímetro de los volcanes activos más peligros del país, están conectados al observatorio, el cual es responsable de establecer sistemas tecnológicos para la vigilancia y monitoreo volcánico. Sobre esta base, el Sernageomin informa a la ciudadanía a través de reportes periódicos sobre seguimiento habitual y reportes extraordinarios referidos a anomalías.

La Red Nacional de Vigilancia Volcánica del Sernageomin, está formada por varios equipos de diferentes sensores y áreas del monitoreo volcánico, como también equipos de redes y comunicaciones, en la figura 2.1 [7], se resume los equipos utilizados para transmisión de datos.

Figura 2.1. Red Nacional de Vigilancia Volcánica del Sernageomin

En conjunto la red de transporte de datos se basa en una red ruteada IP.

2.1.3. Observatorio Vulcanológico y Sismológico de Costa Rica (OVSICORI)

La red externa del OVSICORI [8], tiene las siguientes características:

- Transmisión por la red satelital
- Transmisión por tecnología *Spread Spectrum*
- Transmisión por WiFi de largo alcance
- Transmisión por la red móvil celular a través de módems
- Transmisión por internet, conexiones dedicadas contratadas con proveedores de servicios de *Internet* (ISP, *Internet Service Provider*)
- Uso de frecuencias libres en las bandas de 2.4 y 5.8 GHz
- Uso de redes ruteadas y conmutadas
- Uso a menor escala de una red privada virtual (VPN, *Internet Service Provider*) tipo *IPSec.*
- Se hace monitorización con herramientas libres usando el protocolo simple de administración de red (SNMP, *Simple Network Management Protocol*)
- No se tiene implementado mecanismos de QoS

2.2. A NIVEL INSTITUCIONAL

2.2.1. Observatorios de Popayán y Manizales

En los Observatorios de Popayán [9] y Manizales, se tiene redes de datos basadas en conexiones inalámbricas punto a punto, distribuidas en repetidoras principales, repetidoras secundarias y nodos finales. Los equipos de comunicación utilizados para telemetría operan en bandas libres en los segmentos de 900 MHz, 2.4 GHz y 5 GHz, con tecnologías como: espectro ensanchado por salto de frecuencia (FHSS, *Frequency Hopping Spread Spectrum*) y WiFi de largo alcance basado espectro ensanchado por secuencia directa (DSSS, *Direct Sequence Spread Spectrum*) y multiplexación por división de frecuencias ortogonales (OFDM, *Orthogonal Frequency Division Multiplexing*) [10].

La red de telemetría se unifica en una red Ethernet en dos o más dominios de *Broadcast* unidos a través de switches y enrutadores sin implementar mecanismos para calidad de servicio (QoS, *Quality of Service*).

2.2.2. Observatorio de Pasto

En el Observatorio de Pasto, no se ha implementado tecnologías relacionadas a la calidad de servicio, en su lugar, se ha avanzado en un proceso de migración de la red conmutada a la red enrutada, incorporando funcionalidades para tolerancia a fallos a través de enlaces inalámbricos redundantes, adicionalmente se tiene contratado para el respaldo de conectividad con un ISP un servicio de canal dedicado por fibra óptica en una repetidora principal.

2.3 Comparación de uso de tecnologías en Observatorios Vulcanológicos

En la tabla 2.1 se resume las tecnologías para el transporte de datos utilizadas por los diferentes observatorios vulcanológicos descritos anteriormente, se observa una tendencia marcada en el uso de redes públicas, y un uso reducido de mecanismos tendientes a mejorar la seguridad y disponibilidad de los datos.

Tecnología	Ecuador	Chile	Costa Rica	Colombia
Fibra óptica	x			
Microondas	x			
Satelital	x		x	x
FHSS	x	x	x	x
WiFi (largo alcance)	x	x	x	x
Internet (ISP)	x	x	x	x
Móvil celular			x	
Red conmutada			x	x
Red ruteada	x	x		x
ACLs	x			
VLAN	x			
VPN			x	x

Tabla 2.1. Comparación en el uso de tecnologías de comunicación

2.4 MPLS

La conmutación de etiquetas multiprotocolo (MPLS, *Multiprotocol Label Switching*) es una tecnología estándar creada por el grupo de trabajo de ingeniería de Internet (IETF, *Internet Engineering Task Force*) y definida en el RFC 3031. Ésta, se define como una tecnología de transporte de paquetes a través de una red de datos, usando información contenida en etiquetas añadidas a los paquetes IP. [11]

MPLS se propone como solución a los problemas de las redes actuales: velocidad, escalabilidad, gestión de QoS, e ingeniería de tráfico, MPLS es un protocolo diseñado para dar solución a la gran demanda de recursos y calidad de servicio que tienen las nuevas aplicaciones, éste funciona sobre diferentes tecnologías como ATM, *Ethernet, Frame Ralay*, PPP entre otras. Ya que MPLS puede existir con estas tecnologías, no busca reemplazarlas sino mejorar el transporte de datos a través de ellas.
MPLS requiere un conjunto de procedimientos para la distribución confiable de los enlaces de etiquetas. MPLS puede hacer uso de diferentes protocolos para la distribución de etiquetas, de los cuales el protocolo de distribución de etiquetas (LDP, *Label Distribution Protocol*) y el protocolo de reserva de recursos (RSVP-TE, *Resource Reservation Protocol - Traffic Engineering*) son los más populares.

Entre los beneficios que MPLS proporciona a las redes IP son: Realizar ingeniería del tráfico (TE, *Traffic Engineering*), cursar tráfico con diferentes calidades de clases de servicio (CoS, *Class of Service*) o grados de calidad de servicio (QoS, *Quality of Service*), y crear redes privadas virtuales (VPN, *Virtual Private Networks*) basadas en IP.

En este capítulo se describen las características básicas de la arquitectura MPLS, el protocolo de distribución de etiquetas LDP y sus extensiones CR-LDP y RSVP-TE. Adicionalmente se revisan algunos conceptos básicos de redes IP, enrutamiento OSFP y QoS.

2.4.1 Protocolo de Internet (IP)

IP es parte del conjunto de protocolos TCP/IP utilizados en internet. TCP corresponde a la capa de transporte del modelo OSI, mientras que IP corresponde a la capa de red. En esta sección se hace una breve descripción de la versión 4 de IP, conocido como IPV4.

IP proporciona un servicio no orientado a conexión, utilizando la conmutación de paquetes o datagramas, un Host IP puede transmitir paquetes a otro destino Host IP sin tener que establecer una conexión con el destino, como en el caso de *X25, Frame Relay* y las redes *ATM*. Datagramas IP, se encaminan a través de la red IP de forma independiente uno del otro y en teoría, pueden seguir diferentes caminos a través de la red. En la práctica, la red IP utiliza tablas de enrutamiento que se mantienen fijas durante un periodo de tiempo. En vista de esto, todos los paquetes IP desde un emisor a un receptor típicamente siguen el mismo camino.
IP no garantiza la entrega de datagramas y al igual que en las redes de modo de transferencia asíncrona (ATM, *Asynchronous Transfer Mode*), IP no comprueba errores sobre la carga útil de un datagrama, solo se hace del encabezado y al encontrar un error, el paquete se descarta [11].

2.4.1.1 Encabezado del protocolo IPv4

Un datagrama IP se compone de un encabezado y una carga útil, el encabezado IP se muestra en la figura 2.2 [11] y se compone de una parte fija de 20 *bytes* y una parte opcional que tiene longitud variable. Los campos del encabezado IP [11], se listan a continuación.

- *Versión*: un campo de 4 bits que se utiliza para indicar la versión del protocolo
- Longitud del encabezado Internet (IHL*, Internet Header Length*): este es un campo de 4 bits que da la longitud de la cabecera en palabras de 32 bits. La longitud mínima de cabecera es cinco palabras de 32 bits (o 20 bytes)
- *Type of service*: este campo se utiliza para indicar la calidad del servicio deseado. El tipo de servicio es un conjunto abstracto o generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet.

Esta indicación de tipo de servicio será usada por las pasarelas para seleccionar los parámetros de transmisión efectivos para una red en particular, la red que se utilizará para el siguiente salto, o la siguiente pasarela al encaminar un datagrama internet.

- *Total length*: un campo de 16 bits usado para indicar la longitud de todo el datagrama, es decir, el encabezado y la carga útil. El valor predeterminado para la longitud máxima es 65.535 bytes.
- *Identification*: un campo de 16 bits usado por el receptor para identificar a que fragmento pertenece el datagrama. Todos los fragmentos de un datagrama tienen el mismo valor en la identificación del campo.
- *Flags*: actualmente utilizado sólo para especificar valores relativos a la fragmentación de paquetes.
- *Fragment* offset: este campo de 13 bits, en paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0.
- *Time to live*: este campo es una indicación de un límite superior en la vida útil de un datagrama de Internet. El emisor del datagrama lo establece y se reduce en los puntos a lo largo de la ruta donde se procesa. Si el tiempo de vida llega a cero antes de que el datagrama de internet llegue a su destino, el datagrama de internet se destruye. El tiempo de vida puede considerarse como un límite de tiempo de autodestrucción.
- *Protocol*: este campo de 8 bits de longitud, especifica el siguiente protocolo de nivel superior (TCP o UDP).
- *Header checksum*: un campo de 16 bits utilizado para verificar si la cabecera IP se ha recibido correctamente.
- *Source address*: un campo de 32 bits que contiene dirección IP que origina el paquete.
- *Destination address*: un campo de 32 bits que contiene dirección IP de destino del paquete.
- *Options*: un campo de longitud variable que se utiliza para codificar las opciones solicitadas por el usuario.
- *Padding*: un campo de longitud variable utilizado para hacer el encabezado del datagrama un múltiplo entero de palabras de 32 bits.

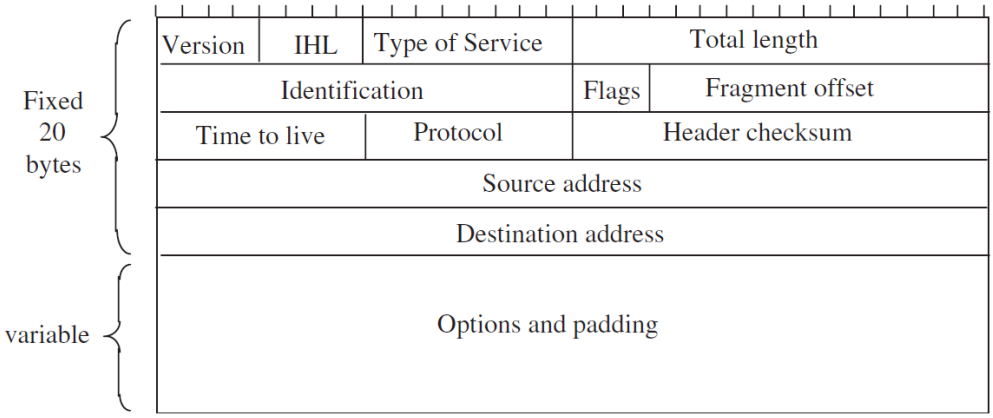

Figura 2.2. Encabezado IPv4

2.4.1.2 Direccionamiento IPv4

Las direcciones IPv4 son de 32 bits de longitud. Una dirección se divide en dos partes, una red y un sufijo. La red identifica la red física a la que el equipo host está conectado. El sufijo identifica el equipo host como tal. El tamaño de estos dos campos varía de acuerdo a la clase de la dirección IP. Específicamente hay cinco diferentes clases de direcciones (A, B, C, D y E). Véase la figura 2.3 [11]

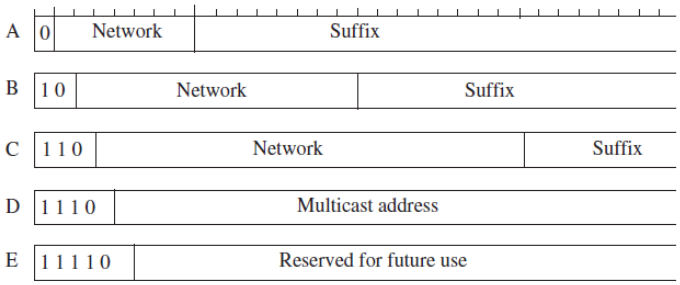

Figura 2.3. Clases de direcciones IP

Las clases A, B y C, se denominan clases primarias ya que se utilizan para las direcciones host. Clase D se utiliza para la multidifusión; clases E está reservada para uso futuro. El primer campo determina la clase de la dirección IP, y varía de 1 a 5 bits (A-E). El segundo campo hace referencia a la dirección de red y el tercer campo es el sufijo de la dirección de host.

En la clase A, hay una dirección de red de 7 bits y una dirección de host de 24 bits, el resultado es 128 direcciones de red y 16.777.246 direcciones de host. En la clase B, hay una dirección de red de 14 bits y una dirección de host de 16 bits, el resultado 16.384 direcciones de red y 65.536 direcciones de host. En la clase C, hay una dirección de red de 21 bits y una dirección de host de 8 bits, el resultado 2.097.152 direcciones de red y 256 direcciones de host.

Las direcciones de red se escriben normalmente en notación decimal con puntos, es decir, cada byte se escribe en decimal y que van de 0 a 265. De esta manera se tiene que el rango de direcciones de clase A es desde 10.0.0.0–127.255.255.255, para la clase B tenemos un rango de valores desde 128.0.0.0-191.255.255.255 y para la clase C que tiene una gama de 192.0.0.0 a 233.255.255.255.

2.4.2 OSPF

El protocolo de primero la ruta más corta abierto (OSFP, *Open Shortest Path First*), definido en RFC 2328, es un protocolo de red para enrutamiento jerárquico de pasarela interior (IGP, *Interior Gateway Protocol*) que se usa para distribuir la información para ruteo dentro de un solo sistema autónomo[2] (AS, *Autonomous System*).

El protocolo OSPF está basado en tecnología de estado de enlace [12], mediante el Algoritmo de SPF de Dijsktra “Primero la Ruta más Corta”. OSPF ha introducido conceptos nuevos, como la autenticación de actualizaciones de ruteo, Máscaras de subred de longitud variable (VLSM, *Variable Length Subnet Mask*), resumen de ruta, entre otras.

OSPF es un protocolo de estado de enlace, un enlace puede ser equivalente a una interfaz en el enrutador. El estado del enlace ofrece una descripción de esa interfaz y de su relación con los enrutadores vecinos. Una descripción de la interfaz incluiría, por ejemplo, la dirección IP de la interfaz, la máscara, el tipo de red a la que se conecta, los enrutadores conectados a esa red y así sucesivamente. La recolección de todos

[2] Un sistema autónomo se considera a cada red se opera de manera independiente a las demás [10]

estos estados de enlace formaría una base de datos de estados de enlace (LSDB, *Link-State Database*).

OSPF usa el algoritmo de *Disktra* para construir y calcular la trayectoria más corta a todos los destinos conocidos.

El algoritmo coloca cada enrutador en la raíz de un árbol y calcula la trayectoria más corta a cada destino basándose en el costo acumulativo necesario para alcanzar ese destino. Cada enrutador dispondrá de la topología, a pesar de que todos los enrutadores crearán un árbol de trayectoria más corta usando la misma base de datos de estados de enlace. El costo (también llamado métrica) de una interfaz en OSPF y el cálculo se realiza teniendo en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. El costo de una interfaz es un valor arbitrario asignado por el administrador de la red.

2.4.3 Calidad de servicio

Calidad de Servicio (QoS) [13] es una necesidad creciente en las redes actuales. La presencia de tráfico con características y requerimientos especiales en la misma infraestructura que se utiliza para el tráfico de datos requiere de la implementación de QoS a fin de asegurar una correcta prestación de cada uno de los servicios con diferentes prioridades, aplicaciones, usuarios, o flujos de datos.

Las diferentes aplicaciones tienen diferentes necesidades de retardo (*delay - latency*), variación de retardo (*jitter*), ancho de banda (*bandwidth*), tasa de pérdida de paquetes (*Packet loss rate*), tasa de errores y disponibilidad. Estos parámetros forman la base de la QoS. La red IP debe estar diseñada para proporcionar la calidad de servicio necesaria para las aplicaciones.

La implementación de políticas de calidad de servicio se puede enfocar en varios puntos según los requerimientos de la red, los principales son:

- Asignar ancho de banda en forma diferenciada.
- Evitar y/o administrar la congestión de la red.
- Manejar prioridades de acuerdo al tipo de tráfico.

- Modelar el tráfico de la red.

En el encabezado de IPv4 [14], el campo *Type of Service*, indica una serie de parámetros sobre la calidad de servicio deseada durante el tránsito por una red. Algunas redes ofrecen prioridades de servicios, considerando determinado tipo de paquetes más importantes que otros. Estos 8 bits se agrupan de la siguiente manera:

Los 3 primeros bits están relacionados con la precedencia de los mensajes, un indicador adjunto que indica el nivel de urgencia basado en el sistema militar de precedencia. La urgencia que estos estados representan aumenta a medida que el número formado por estos 3 bits lo hace, en la tabla 2.2 [14], se muestran los valores del campo precedencia.

Los 5 bits de menor peso son independientes e indican características del servicio. En la figura 2.4 [14] [15], se ilustra la ubicación y valor de cada bit.

Bit
(0-2) Precedencia: prioridad (ocho niveles). Mayor es mejor
(3-6) D,T,R,C: Banderas para indicar la ruta que se quiere utilizar
D: delay (mínimo retardo)
T: throughput (máximo rendimiento)
R: reliability (máxima fiabilidad)
C: cost (mínimo costo), RFC 1349
(7) X: bit reservado

Figura 2.4. Octeto Type of Service

Precedencia (decimal)	Precedencia (binario)	Nombre
7	111	Control de red
6	110	Control de interred
5	101	Crítico / ECP
4	100	Muy urgente
3	011	Urgente
2	010	Inmediato
1	001	Prioridad
0	000	Rutina

Reservados para tráfico de control

Disponibles para usuario

Tabla 2.2. Valores del campo precedencia

Para facilitar QoS de extremo a extremo sobre una red IP en la actualidad hay 3 modelos de aplicación de calidad de servicios para redes de datos: *Best-Effort, IntServ y DiffServ*. [16]

Sin un mecanismo de QoS, una red IP proporciona el servicio de mejor esfuerzo (*Best-Effort*), todos los paquetes son indistinguibles y reciben el mismo tratamiento de reenvío. Un mecanismo de QoS en la red IP proporciona un medio para distinguir los paquetes y tratarlos de manera diferente. Dos mecanismos principales de QoS disponibles para la red IP son los servicios integrados (*IntServ*) y los servicios diferenciados (*DiffServ*).

La figura 2.5 [16] ilustra los servicios de mejor esfuerzo, *IntServ* y *DiffServ*. En esta ilustración, el término "Traffic Flows" se utiliza en un sentido laxo y representa la fuente del tráfico. En el servicio de mejor esfuerzo, todos los paquetes se agrupan en una sola masa, independientemente de la fuente. En *IntServ*, los flujos individuales se distinguen de extremo a extremo. En *DiffServ*, los flujos individuales no se identifican de extremo a extremo. Por el contrario, se agregan en un número menor de clases. Además, estas clases de tráfico reciben un tratamiento diferencial por salto y no existe un tratamiento de extremo a extremo de estas clases de tráfico.

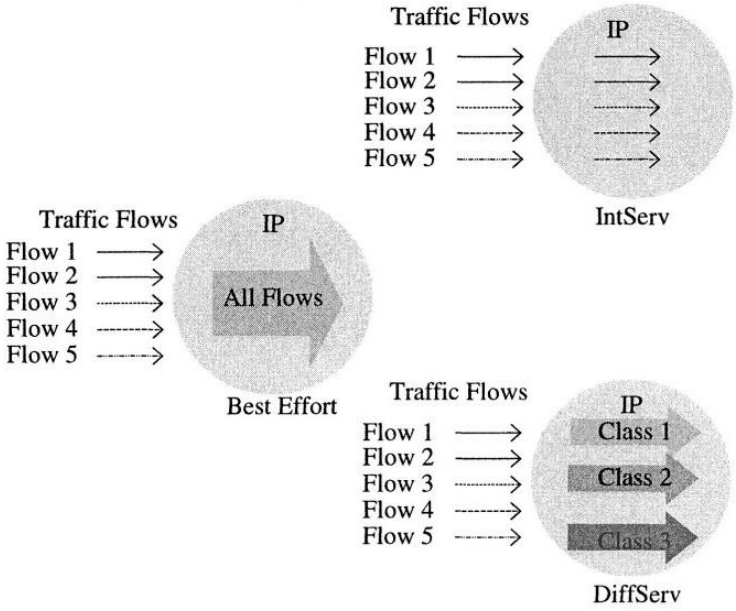

Figura 2.5. Best effort, IntServ y DiffServ

2.4.3.1 Best-Effort

Este modelo es el servicio más simple, en el cual, una aplicación envía información cuando ella lo desea, en cualquier cantidad, sin ningún permiso requerido y sin informar previamente a la red [17]. Es decir, simplemente no se aplica calidad en el servicio al tráfico. Además, no asegura tasa de transferencia, retraso o fiabilidad. Por último, utiliza el modelo de cola FIFO (*First In FirstOut*) para sus transmisiones.

Una red o un proveedor ofrecen calidad en el servicio cuando se garantiza el valor de uno o varios de los parámetros que definen esta calidad. Si el proveedor no se compromete en ningún parámetro se considera que lo que ofrece es un servicio "*best-effort*". TCP/IP fue diseñado para dar un servicio *best-effort* también. Existen aplicaciones que no pueden funcionan en redes congestionadas con *best-effort*, por ejemplo, la videoconferencia o VoIP [16].

2.4.3.2 IntServ – Integrated Services (RFC 1633)

El modelo *IntServ* adopta un enfoque por flujo, lo que significa que cada flujo de tráfico se maneja por separado en cada enrutador, por lo tanto, los recursos se pueden

asignar individualmente a cada flujo mediante el protocolo de reserva de recursos (RSVP, *Resource Reservation Protocol*) [18].

Es una arquitectura que tiene como objetivo dar garantías de QoS a sesiones de aplicación individuales (flujos), basados en servicio garantizado y servicio de carga controlada. En *IntServ* cada paquete IP puede asociarse a un flujo[3]. [11]

Servicio garantizado: este servicio proporciona límites firmes en el retraso de la cola de extremo a extremo sin pérdida de paquetes.

Servicio de carga controlada: este servicio proporciona al usuario una QoS que se aproxima mucho a la QoS del servicio de mejor esfuerzo, un usuario podría asumir lo siguiente a) La red entregará con éxito un porcentaje muy alto de paquetes transmitidos al receptor. El porcentaje de paquetes no entregados con éxito debe aproximarse estrechamente a la tasa de error de paquete básico de los enlaces de transmisión. b) El retraso de extremo a extremo experimentado por un porcentaje muy alto de los paquetes entregados no excederá en gran medida el retraso mínimo de extremo a extremo experimentado por cualquier paquete entregado con éxito.

El retraso de extremo a extremo experimentado por un porcentaje muy alto de los paquetes entregados no excederá en gran medida el retraso mínimo de extremo a extremo experimentado por cualquier paquete entregado con éxito.

En *IntServ*, el remitente especifica cuánto tráfico transmitirá a su (s) receptor (es), y un receptor especifica cuánto tráfico puede recibir y la QoS requerida, expresada en términos de pérdida de paquetes y retraso de extremo a extremo. Esta información permite que cada enrutador IP a lo largo de la ruta gestione la congestión y proporcione transporte con calidad de servicio realizando las siguientes funciones:

- Vigilancia: se utiliza para verificar que el tráfico transmitido por el remitente se ajuste a las especificaciones de tráfico (TSPEC, *Traffic Specification*), que son un conjunto de descriptores que caracterizan el tráfico transmitido.

[3] La RFC 1633 define flujo como una corriente discernible de paquetes IP relacionados, que resulta de la actividad única de un usuario y requiere una misma calidad de servicio.

- Control de admisión: se utiliza para decidir si un enrutador IP tiene los recursos adecuados para cumplir con la QoS solicitada.
- Clasificación: se utiliza para decidir qué paquetes IP se deben considerar como parte del tráfico del remitente y se les debe dar la QoS solicitada.
- Cola y programación: para que un enrutador IP proporcione diferentes QoS a diferentes receptores, debe poner los paquetes en diferentes colas y transmitirlos de acuerdo con un planificador.

La arquitectura *IntServ* requiere un protocolo de señalización para el establecimiento y mantenimiento confiables de reservas de recursos. Al igual que en MPLS, *IntServ* no requiere el uso de un protocolo de señalización específico, y puede acomodar una variedad de protocolos de señalización, de los cuales RSVP es el más popular. RSVP se desarrolló para admitir la arquitectura *IntServ*, pero se puede usar para transportar otros tipos de información de control. Esto se debe a que RSVP no conoce el contenido de los campos del protocolo RSVP que contienen información de control de políticas y tráfico utilizada por los enrutadores para reservar recursos. RSVP se puede usar para hacer reservas de recursos para aplicaciones de unidifusión y multidifusión.

La principal limitación de este modelo es la gran cantidad de información que debe almacenar cada nodo, provocando que la solución no sea aplicable en situaciones con gran cantidad de flujos entre usuarios finales, no es escalable en grandes redes o implementaciones muy complejas.

2.4.3.3 DiffServ – Differentiated Services (RFC 2474)

DiffServ es el segundo modelo y responde mejor al problema de QoS a través de redes IP. Su objetivo es proporcionar QoS por agregado. Ofrece mecanismos de diferenciación de servicios, que permiten la clasificación de paquetes. [18].

DiffServ utiliza los bits *DiffServ* en el encabezado IP para calificar el paquete IP para que sea de una determinada QoS. Los enrutadores observan estos bits para marcar, poner en cola, dar forma y establecer la prioridad de descarte del paquete. La gran ventaja de *DiffServ* sobre *IntServ* es que el modelo *DiffServ* no necesita ningún protocolo de señalización. El modelo *IntServ* utiliza un protocolo de señalización que debe ejecutarse en los hosts y enrutadores. Si la red tiene muchos miles de flujos, los

enrutadores deben mantener la información de estado para cada flujo que pasa a través de ella. Este es un problema grave de escalabilidad, por lo que *IntServ* no ha demostrado ser popular.

Un buen ejemplo donde se necesita QoS es el tráfico de VoIP. El tráfico de VoIP debe ser entregado dentro de un cierto tiempo al destino, o se vuelve obsoleto. Por lo tanto, QoS debe priorizar el tráfico de VoIP para garantizar que se entregue dentro de un cierto límite de tiempo. [19]

Se puede establecer la prioridad de un paquete IP en el campo Precedencia IP (tres bits) o en los seis bits del campo punto de código de servicios diferenciados (DSCP, *Differentiated Services Code Point*). Originalmente, solo tres bits del campo Tipo de servicio (TOS) en el encabezado IP estaban reservados para QoS. El número de bits en el encabezado de IP que podría usarse para QoS se aumentó luego a seis con la introducción de *DiffServ* QoS.

El uso de los bits de precedencia para QoS ahora se usa ampliamente en todo el mundo para muchas redes. Sin embargo, el inconveniente de los bits de precedencia es que solo existen tres, lo que significa que solo puede tener ocho niveles de servicio. Por lo tanto, la IETF decidió dedicar más bits para QoS. Los cuatro bits TOS quedaron en desuso, y tres de ellos fueron asignados a *DiffServ* QoS, además de los tres bits de precedencia. *DiffServ* terminó con seis bits, proporcionando niveles más que suficientes de QoS. La figura 2.6 [19] muestra qué bits del byte TOS se usan para *DiffServ*.

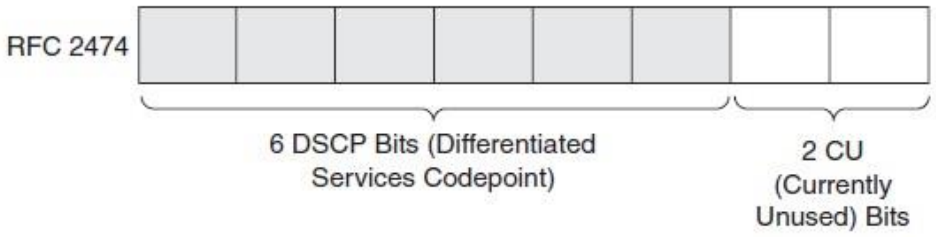

Figura 2.6. El byte TOS del encabezado IP que define el DSCP

Se definen dos tipos de clases de reenvío dentro del modelo *DiffServ*: reenvío acelerado (EF, *Expedited Forwarding*) y reenvío asegurado (AF, *Assured Forwarding*).

EF es una baja pérdida, baja latencia, baja fluctuación, ancho de banda garantizado, servicio de extremo a extremo a través de un dominio *DiffServ*. AF define diferentes servicios de garantías de reenvío a través de un dominio *DiffServ*. Se definen cuatro clases de AF, cada una con tres preferencias de caída. Las clases de AF se anotan como AFij, siendo i de 1 a 4 para la clase y j de 1 a 3 para la precedencia de caída.

Los primeros tres bits del campo DSCP de seis bits definen la clase, los siguientes dos bits definen la precedencia de descarte y el último bit está reservado. Cuanto mayor sea la precedencia de descarte dentro de una clase, más probable es que se descarte el paquete, en relación con los otros paquetes con menor precedencia de descarte cuando ocurre la congestión. Existen cuatro clases para el tráfico y existen tres niveles para la precedencia de caída. En la tabla 2.3 [19] se listan las cuatro clases de AF y tres precedentes de caída.

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low	001010	010010	011010	100010
Medium	001100	010100	011100	100100
High	001110	010110	011110	100110

Tabla 2.3. Cuatro clases de AF y tres precedentes de caída

El RFC 4594 proporciona pautas para los administradores de red al configurar el nivel de servicio para satisfacer sus necesidades de QoS. El operador de red debe configurar y proporcionar en sus redes un subconjunto de las clases de servicio definidas. Para esto se proporciona pautas para la configuración de servicios diferenciados a una amplia variedad de aplicaciones y servicios.

La tabla 2.4 [20] proporciona una vista de comportamiento para el tráfico atendido por cada clase de servicio. La columna de características de tráfico define las características y el perfil de los flujos atendidos, y las columnas de tolerancia a pérdida, retraso y fluctuación de fase definen el tratamiento que recibirán los flujos. Los requisitos de rendimiento cuantitativo de extremo a extremo se pueden obtener de las Recomendaciones UIT-T Y.1541 e Y.1540.

Un "*Yes*" en la columna tolerante *jitter* implica que los datos están almacenados temporalmente en el punto final y que un nivel moderado de la variación *network-*

induced en el retraso no afectará a la aplicación. Las aplicaciones que usan TCP como transporte son generalmente buenos ejemplos. Los protocolos de enrutamiento y la señalización punto a punto también se incluyen en esta clase.

La tabla 2.5 [20] define la relación recomendada entre clases de servicio y asignación de puntos de código DS con ejemplos de aplicación. Se debe propender en lo posible que esta relación se conserve de principio a fin. El reenvío predeterminado (DF) y el selector de clase 0 (CS0) proporcionan un comportamiento equivalente y usan el mismo punto de código DS, '000000'. Se espera que los administradores de red basen su elección de las clases de servicio que admitirán en sus necesidades, comenzando con tres o cuatro clases de servicio para el tráfico de usuarios y agregando otras según sea necesario.

Service Class Name	Traffic Characteristics	Tolerance to Loss	Tolerance to Delay	Tolerance to Jitter
Network Control	Variable size packets, mostly inelastic short messages, but traffic can also burst (BGP)	Low	Low	Yes
Telephony	Fixed-size small packets, constant emission rate, inelastic and low-rate flows	Very Low	Very Low	Very Low
Signaling	Variable size packets, some what bursty short-lived flows	Low	Low	Yes
Multimedia Conferencing	Variable size packets, constant transmit interval, rate adaptive, reacts to loss	Low - Medium	Very Low	Low
Real-Time Interactive	RTP/UDP streams, inelastic, mostly variable rate	Low	Very Low	Low
Multimedia Streaming	Variable size packets, elastic with variable rate	Low - Medium	Medium	Yes
Broadcast Video	Constant and variable rate, inelastic, non-bursty flows	Very Low	Medium	Low
Low-Latency Data	Variable rate, bursty short-lived elastic flows	Low	Low - Medium	Yes
OAM	Variable size packets, elastic & inelastic flows	Low	Medium	Yes
High-Throughput Data	Variable rate, bursty long-lived elastic flows	Low	Medium - High	Yes
Standard	A bit of everything	Not Specified		
Low-Priority Data	Non-real-time and elastic	High	High	Yes

Tabla 2.4. Características de clase de servicio

Service Class Name	DSCP Name	DSCP Value	Application Examples
Network Control	CS6	110000	Network routing
Telephony	EF	101110	IP Telephony bearer
Signaling	CS5	101000	IP Telephony signaling
Multimedia Conferencing	AF41,AF42 AF43	100010,100100 100110	H.323/V2 video conferencing (adaptive)
Real-Time Interactive	CS4	100000	Video conferencing and Interactive gaming
Multimedia Streaming	AF31,AF32 AF33	011010,011100 011110	Streaming video and audio on demand
Broadcast Video	CS3	011000	Broadcast TV & live events
Low-Latency Data	AF21,AF22 AF23	010010,010100 010110	Client/server transactions Web-based ordering
OAM	CS2	010000	OAM&P
High-Throughput Data	AF11,AF12 AF13	001010,001100 001110	Store and forward applications
Standard	DF (CS0)	000000	Undifferentiated applications
Low-Priority Data	CS1	001000	Any flow that has no BW assurance

Tabla 2.5. Mapeo de clase de servicio DSCP

La tabla 2.6 [20] proporciona un resumen de los mecanismos de QoS *DiffServ* que deberían utilizarse para las clases de servicio definidas de acuerdo con las aplicaciones o servicios que deben diferenciarse.

- La definición de *DS Edge* significa que la diferenciación del tráfico se realiza en el borde de la red *DiffServ* en donde se conectan dispositivos de usuario no confiables o entre dos redes diferentes.

- "sr + bs" representa un mecanismo de vigilancia que proporciona una tasa única con control de tamaño de ráfaga.

- El comportamiento de marcador de tres colores de una sola tasa (srTCM) debe ser equivalente a RFC 2697, y el comportamiento de marcador de tres colores de dos tasas (trTCM) debe ser equivalente a RFC 2698.

- El comportamiento por saltos (PHB, *Per-Hop Behaviors*) para la clase de servicio interactivo en tiempo real debe configurarse para proporcionar una garantía de alto ancho de banda. puede configurarse como un segundo *EF PHB* que utiliza parámetros de rendimiento relajados y un programador de velocidad.

- La clase de servicio PHB para *roadcast* Video debe configurarse para proporcionar una garantía de alto ancho de banda. puede configurarse como un tercer *EF PHB* que utiliza parámetros de rendimiento relajados y un programador de velocidad.

- En los segmentos de red que usan marcado de precedencia de IP, solo se admite una de las dos clases de servicio, Datos de alto rendimiento o Datos de baja prioridad. Se recomienda que los valores DSCP de la clase de servicio no admitida se cambien a 000xx1 al ingresar y se cambien nuevamente a los valores originales al salir del segmento de red que utiliza el marcado de precedencia. Por ejemplo, si los datos de baja prioridad se asignan a la clase de servicio estándar, entonces la marca DSCP 000001 puede usarse para distinguirlos de los paquetes marcados estándar al salir.

Service Class	DSCP	Conditioning at DS Edge	PHB Used	Queuing	AQM
Network Control	CS6	See Section 3.1	RFC2474	Rate	Yes
Telephony	EF	Police using sr+bs	RFC3246	Priority	No
Signaling	CS5	Police using sr+bs	RFC2474	Rate	No
Multimedia Conferencing	AF41 AF42 AF43	Using two-rate, three-color marker (such as RFC 2698)	RFC2597	Rate	Yes per DSCP
Real-Time Interactive	CS4	Police using sr+bs	RFC2474	Rate	No
Multimedia Streaming	AF31 AF32 AF33	Using two-rate, three-color marker (such as RFC 2698)	RFC2597	Rate	Yes per DSCP
Broadcast Video	CS3	Police using sr+bs	RFC2474	Rate	No
Low-Latency Data	AF21 AF22 AF23	Using single-rate, three-color marker (such as RFC 2697)	RFC2597	Rate	Yes per DSCP
OAM	CS2	Police using sr+bs	RFC2474	Rate	Yes
High-Throughput Data	AF11 AF12 AF13	Using two-rate, three-color marker (such as RFC 2698)	RFC2597	Rate	Yes per DSCP
Standard	DF	Not applicable	RFC2474	Rate	Yes
Low-Priority Data	CS1	Not applicable	RFC3662	Rate	Yes

Tabla 2.6. Resumen de los mecanismos de QoS utilizados para cada clase de servicio

La garantía de rendimiento en las redes de servicios diferenciados se proporciona mediante una combinación de aprovisionamiento de recursos, priorización de tráfico y control de admisión. Es importante que las redes se aprovisionen cuidadosamente para evitar desajustes entre los patrones de tráfico y el ancho de banda del cuello de botella, y pueden ser necesarios mecanismos adicionales para detectar el mal comportamiento y las fuentes de tráfico maliciosas. [21]

2.4.4 QoS en Redes de Área Local

En la capa de Control de Acceso al Medio (MAC, *Media Access Control*) del modelo de interconexión de sistemas abiertos (OSI, *Open System Interconnection*), se puede aplicar QoS de acuerdo al tipo de tecnología utilizada, para el nivel 2 de OSI, el uso de Ethernet se ha masificado. Esta tecnología define mecanismos QoS que operan en la capa de enlace. El primero se realiza a través de una red de área local virtual (VLAN, *Virtual Local Area Network*), definida en el estándar IEEE 802.1Q, en la cual el tráfico debe ser separado, aislado y priorizado por la identificación de la VLAN. El segundo se realiza a través del estándar IEEE 802.1p, que ofrece ocho clases diferentes de servicio [10].

En el encabezado del paquete IPv4, se utiliza un campo de tres bits para prioridad, obteniendo hasta ocho niveles o clases, bajo este modelo no se tiene información de estado, similar a *DiffServ*. La prioridad va asociada a la etiqueta de VLAN y como consecuencia solo se puede utilizar QoS en enlaces troncales. Normalmente QoS de LAN va asociada a la QoS a nivel de red, haciendo la equivalencia de prioridades 802.1p a tipos de servicio *IntServ* o *DiffServ*. En la figura 2.7 [22], se ilustra el contenido de una trama 802.3 y 802.1Q.

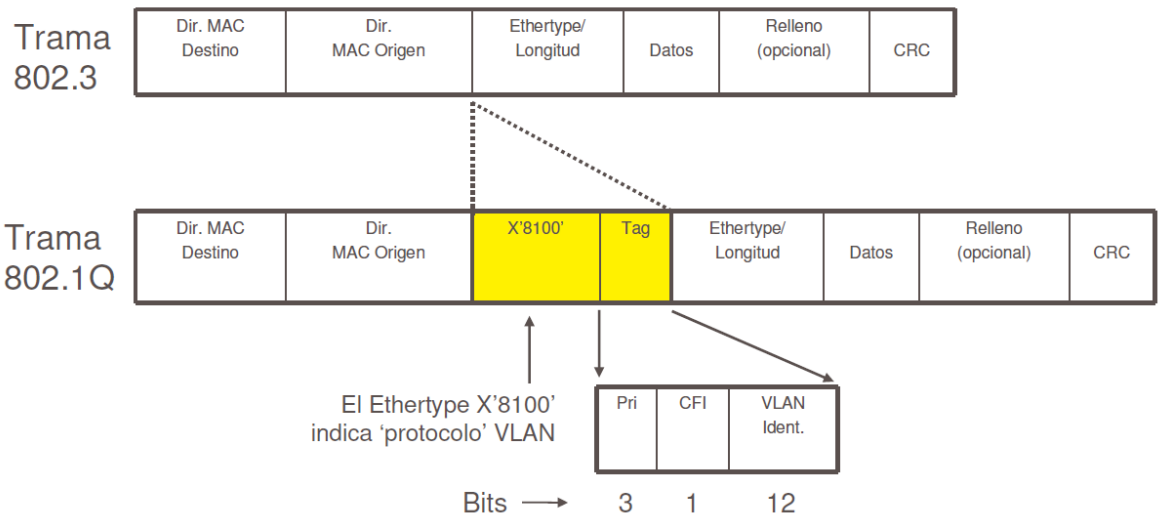

Figura 2.7. Etiquetado de trama según 802.1Q

2.4.4.1 IEEE 802.1Q

El estándar IEEE 802.1Q es un proyecto del grupo de trabajo 802 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, *Institute of Electrical and Electronics Engineers*) para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (*Trunking*).

Las VLAN permiten el agrupamiento lógico de usuarios o equipos que tengan requerimientos de QoS similares. Puede definir redes locales con equipos ubicados en diferentes redes locales físicas, es decir, aunque estas están basadas en dos capas los usuarios que pertenecen a la misma VLAN no necesitan estar conectados físicamente a la misma subred de *Ethernet*, permite la separación de dominios de difusión, además usa la regla de una VLAN por subred IP, es decir, usar un enrutador para enrutar paquetes entre diferentes VLAN. En general, las VLAN permiten la separación y priorización del tráfico basándose en el puerto del switch al cual el equipo está conectado.

En la figura 2.7 se muestra como el estándar de la IEEE 802.1q define el etiquetado para la trama *Ethernet*, como se observa introduce un encabezado de 4 bytes dentro del encabezado *Ethernet* después de la dirección MAC origen. Donde los primeros 12 bits del encabezado de etiqueta especifican el VLAN ID, permitiendo de esta manera 4095 VLAN individuales. El campo Indicador de Formato Canónico (CFI, *Canonical Format Indicator*) le corresponde 1 bit, este cuando está en OFF indica que el dispositivo debe leer la información de la trama en forma canónica (de derecha a izquierda), la razón de este bit es que 802.1q puede utilizar tramas *Token Ring* o *Ethernet*, un dispositivo siempre lee de forma canónica, pero los *Token Ring* no, por eso para una trama Ethernet este valor es "0". Para el campo *User Priority* se utiliza 3 Bits, y este se refiere a la prioridad de la trama por razón de calidad de servicio. Y por último el campo *Tag Protocol* ID (ID del protocolo de VLAN), a este campo se le asignan 2 bytes, especifica que es una trama etiquetada, señala el cambio en el formato de la trama.

2.4.4.2 IEEE 802.1P

IEEE 802.1p es un estándar que define niveles de prioridad diferentes para el campo *User Priority* de la figura 2.8 cuando se envían los paquetes clasificados por prioridad según este estándar a la red, los dispositivos preparados para IEEE 802.1p transfieren los paquetes con mayor prioridad, además cuando se produce congestión de la red, los paquetes que se consideren de mayor prioridad recibirán un trato preferencial, mientras que los paquetes de baja prioridad se mantendrán en cola [23].

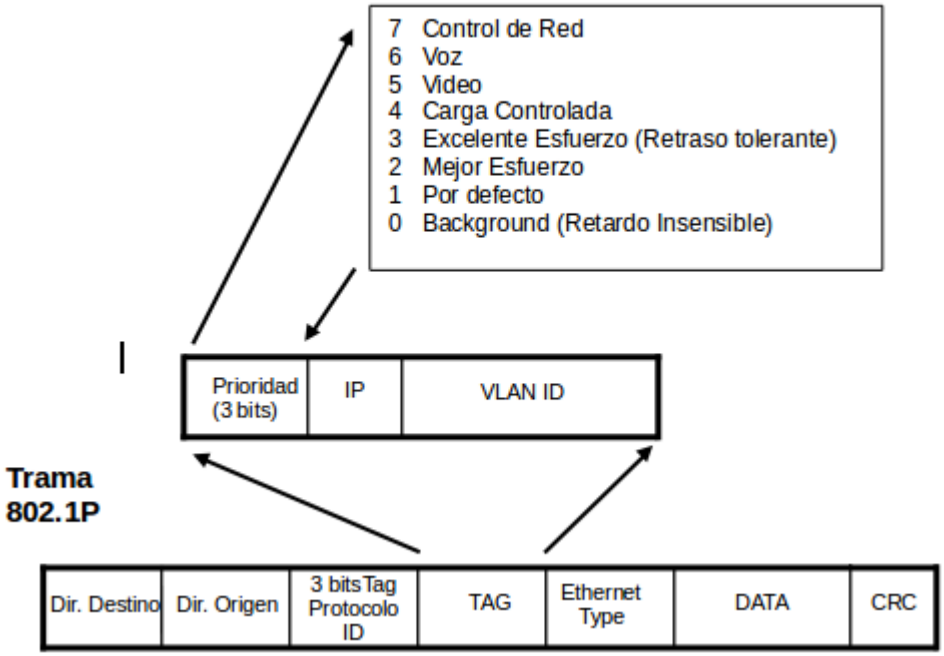

Figura 2.8. Etiquetado de trama según 802.1P

En la figura 2.8 muestra los primeros 2 bytes correspondientes al segmento de la trama *Ethernet* dedicado al estándar 802.1q, el estándar permite asignar 8 niveles de prioridad en VLAN, desde 0 (bajo) hasta 7 (elevado).

El etiquetado IEEE 802.1p aumenta el tamaño de los paquetes. Algunos concentradores y switches no reconocen los paquetes muy grandes debido a que exceden el tamaño máximo de la trama estándar de los paquetes *Ethernet* y los desactivan. Es importante señalar que solo este estándar será efectivo si los dispositivos que enrutan los paquetes son compatibles con 802.1p.

Este protocolo aplica prioridad por puerto, es decir, en caso de tener que elegir que paquete se envía primero el switch transmitirá el que tenga mayor prioridad. Esta prioridad se debe de configurar en cada puerto del switch y aplica a cualquier paquete que provenga de ese puerto.

2.4.4.3 Implementación de QoS en LAN

Para la implementación de calidad de servicio en una red LAN, se tiene:

- Los switches y enrutadores, que soportan QoS tienen varias colas de entrada y salida por interfaz en las que pueden usar diferentes algoritmos.
- Las colas pueden implementarse por software o por hardware. Cuando son por hardware el número suele estar entre dos y cinco.
- Los mecanismos hardware son los mismos para nivel 2 (802.1q) que para nivel 3 (*DiffServ*)
- No hay reservas estrictas sino asignaciones aproximadas.

En la tabla 2.7 [24], se presenta un ejemplo de configuración de un switch Catalyst 3560 para VoIP.

Tipo de tráfico	Etiqueta DSCP	Clase	Prior. 802.1p/Q	Cola salida	Caudal salida	Tamaño buffer
Datos VoIP	46 (EF)	5	5	1(Priority)	10%	10%
Control Voz y vídeo	26 (AF31)	3	3	2 (WRR)	10 %	10%
Prot. Routing	48	6	6			
Spanning Tree	56	7	7			
Vídeo t. real	34 (AF41)	4	4	3 (WRR)	60%	26%
Datos oro (1ª)	16	2	2			
Datos plata (2ª)	8	1	1	4 (WRR)	20%	54%
Datos resto (3ª)	0 (BE)	0	0			

WRR: Weighted Round Robin

Tabla 2.7. Configuración de QoS recomendada en switches Cisco Catalyst 3560 para el servicio de VoIP

2.4.5 Arquitectura de MPLS

MPLS es un estándar IETF basado en la conmutación de etiquetas de Cisco. La intención original era para ser utilizado en conjunto con diferentes protocolos de red, tales como IPv4, IPv6, IPX y *Apple Talk*, sin embargo, MPLS ha sido desarrollado exclusivamente para redes IP. [11]

Para entender el concepto básico detrás de MPLS [17], se debe revisar cómo funciona un enrutador IP. Un enrutador IP implementa dos componentes, uno de control y otro de reenvío. El componente de control consta de los protocolos de enrutamiento como OSFP, el protocolo de puerta de enlace de frontera (BGP, *Border Gateway Protocol*) y el protocolo de multidifusión independiente (PIM, *Protocol Independent Multicast*), usado para construir rutas y la información de enrutamiento entre enrutadores IP. Esta información es utilizada por los enrutadores IP para construir la tabla de reenvío de enrutamiento, referido como la base de información de reenvío (FIB, *Forwarding Information Base*), el componente de reenvío consta de procedimientos que usa un enrutador para crear decisiones de reenvío de un paquete IP. Por ejemplo, en reenvío de tráfico *Unicast* (información entre un único emisor y un único receptor) el enrutador utiliza la dirección IP de destino para encontrar la entrada en la FIB y el resultado de la consulta es el número de la interfaz, que es el número de puerto de salida que conecta el enrutador del siguiente salto al que el paquete IP debe ser enviado.

Un enrutador reenvía un paquete IP de acuerdo a su prefijo. Dentro de un enrutador, todas las direcciones que tienen el mismo prefijo, son referidas en la clase equivalente de reenvío (FEC, *Forwarding Equivalent Class*). Los paquetes IP que pertenecen a la misma FEC tienen la misma interfaz de salida. En MPLS, cada FEC está asociada con una etiqueta diferente. Esta etiqueta se utiliza para determinar la interfaz de salida del paquete IP sin tener que mirar la dirección en la FIB. Una etiqueta es una identificación corta de longitud fija que tiene un significado local, es decir, es válido en un solo salto que interconecta dos enrutadores.

En IPv6, la etiqueta se puede llevar en el campo de etiqueta de flujo. En IPv4, sin embargo, no hay espacio para una etiqueta de este tipo en la cabecera IP. Si la red IP se ejecuta en la parte superior de una red *ATM* (*Asynchronous Transfer Mode*), entonces la etiqueta es transportada en el campo VPI/VCI de la celda *ATM*. Si se está

ejecutando sobre *Frame Relay*, la etiqueta se transporta en el campo DLCI. Para *Ethernet*, *Token Riung* y las conexiones punto a punto (PPP, *Point-to-Point Protocol*) en las que se ejecuta un protocolo de capa de enlace, la etiqueta se encapsula y se inserta en el encabezado de la capa de Control de enlace lógico (LLC, *Logical Link Control*) y el encabezado de IP (véase en la figura 2.9 [11]). El primer campo de la encapsulación de la etiqueta, es un campo de 20 bits usado para llevar la etiqueta, el segundo campo contiene 3 bits utilizados para fines experimentales. Se puede por ejemplo realizar una indicación de clase de servicio (CoS, *Class of Service*), que puede ser utilizada para determinar el orden en que se transmitirán paquetes IP de una interfaz. El campo "S" se usa en unión con la pila de etiquetas y finalmente el tiempo de vida (TTL, *Time to Live*).

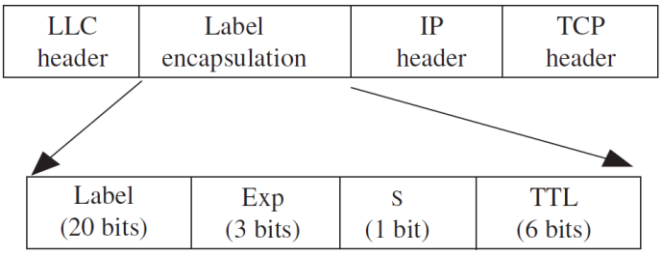

Figura 2.9. Encapsulación de la etiqueta

2.4.6 Componentes

- LSR: enrutador de conmutación de etiquetas: (*Label Switching Router*): Localizado en el núcleo de la red; está especializado en el enrutamiento de los paquetes.
- LSR de ingreso: inserta en los paquetes la etiqueta inicial
- LSR de tránsito: conmuta las etiquetas y reenvía los paquetes
- LSR de egreso: extrae la etiqueta final de los paquetes y los entrega a la red correspondiente
- LER: enrutador de etiquetas de borde (*Label Edge Router*): Localizado en el borde de la red, conecta distintas redes de acceso (FR, ATM, TCP/IP, etc.); está especializado en la inserción/extracción de etiquetas. Para un camino virtual dado también se denominan LSR de ingreso y de egreso LSP (*Label Switched Path* o intercambio de rutas por etiqueta) nombre genérico de un camino MPLS (para

cierto tráfico o FEC), es decir, del túnel MPLS establecido entre los extremos. En VPN el enrutador del cliente se denomina borde del cliente (*Customer Edge*, CE)

- LSP: camino conmutado de etiquetas (*Label Switched Path*), es el camino virtual que siguen los paquetes de una misma conexión. Tiene asignada una etiqueta en cada salto. Se establece mediante protocolos de enrutamiento o en forma manual
- FEC: clase de equivalencia de reenvío (*Forwarding Equivalence Class*), nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el switch.

En la figura 2.10 realizada con la herramienta *Edraw Max*[4], se ubican los componentes dentro de una red MPLS

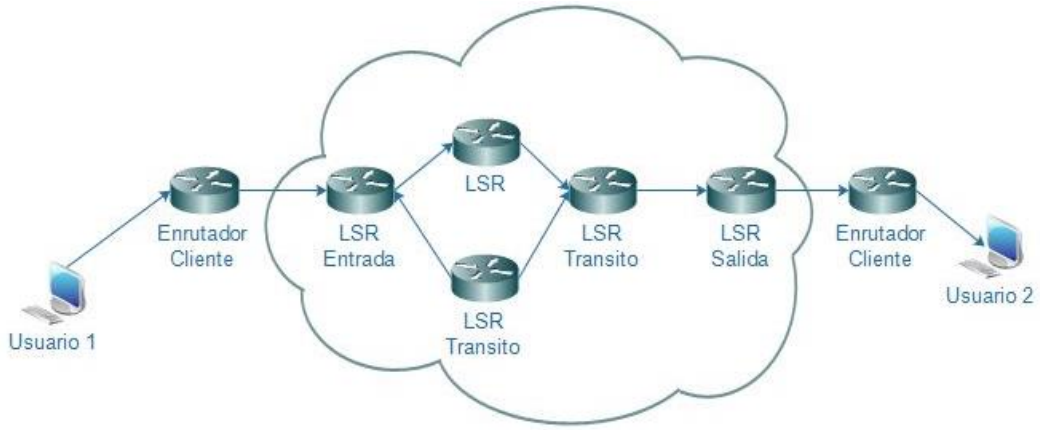

Figura 2.10. Componentes de MPLS

2.4.6 Protocolos en redes MPLS

Al igual que en la red IP tradicional, los protocolos de enrutamiento IP se utilizan para reenviar los paquetes pero, en la red MPLS, los LSR usan conmutación de etiquetas como el mecanismo de reenvío. Los LSP están configurados por distribución de etiquetas a lo largo de la red y los protocolos de distribución de etiquetas más comunes son: el protocolo de distribución de etiquetas (LDP, *Label Distribution Protocol*), El protocolo de reserva de recursos (RSVP, *The Resource Reservation Protocol*) y el protocolo de distribución de etiquetas basado en restricciones (CR-LDP, *Constraint-Based Label Distribution Protocol*).

[4] *Edraw Max*: es una herramienta para crea diagramas de flujo, mapas mentales, organigramas, diagramas de red y planos de planta, disponible en https://www.edrawsoft.com/es/edraw-max/

2.4.6.1 Protocolo de distribución de etiquetas (LDP)

En la red de MPLS, los paquetes se etiquetan y se conectan a través de los LSP, y LSR realizan la operación de intercambio para conmutar los paquetes. La etiqueta es necesita para distribuir a todos los enrutadores adyacentes. El protocolo de distribución de etiquetas (LDP, *Label Distribution Protocol*) fue desarrollado para distribuir las etiquetas en toda la red.

Se puede trabajar con los protocolos de pasarela interior (IGP, *Interior Gateway Protocols*) como OSPF, el Protocolo de enrutamiento de puerta de enlace Interior mejorado (EIGRP, *Enhanced Interior Gateway Routing Protocol*), sistema intermedio a sistema intermedio (IS-IS, *Intermediate System to Intermediate System*) y el protocolo de información de enrutamiento (RIP, *Routing Information Protocol*), aunque hay una excepción con el protocolo de puerta de enlace de frontera (BGP, *Border Gateway Protocol*), ya que lleva rutas exteriores y ya es un multiprotocolo.

Grupos de paquetes que tienen las características similares se consideran en la misma clase, conocida como FEC y la misma etiqueta se provee a estos paquetes. Un LSP específico se puede utilizar para las varias FEC. Grupos de paquetes conmutados a través de la misma ruta y con el mismo tratamiento que podría constituir la misma FEC.

El paquete, que se transmitirá en la red MPLS, se envía a través de la LSP. Los enrutadores LSR de ingreso reciben el paquete IP, inserta una o más etiquetas y busca la dirección de destino de acuerdo a la FEC específica, y reenvía el paquete.

Los LSR tienen un IGP internamente que se ejecuta a lo largo de la red. Los LSR intermedios intercambian las etiquetas con la etiqueta de salida y reenviarlos. Un LSR de egreso quita la etiqueta y reenvía el paquete.

Cuando un paquete entra en un dominio MPLS, el LER de entrada añade una etiqueta al paquete y conmuta el paquete etiquetado al LSR intermedio adyacente. Esta operación se conoce como *PUSH*. LER intermedios son responsables para intercambiar la etiqueta y conmutar los paquetes a LSR adyacente; esto se conoce

como operación *SWAP*. Finalmente, un paquete antes de salir de la red MPLS, la etiqueta se retira por el LER de salida o enrutador de tránsito, esto se llama operación *POP*.

2.4.6.2 Protocolo de reserva de recursos (RSVP)

El protocolo de reserva de recursos (RSVP, *The Resource Reservation Protocol*) [11], es un protocolo de señalización alternativa a la LDP y CR-LDP, a su vez RSVP-TE, es una extensión el cual fue diseñado para soportar la arquitectura de *IntServ*, esta arquitectura requiere un protocolo de señalización para el establecimiento fiable y mantenimiento de reservas de recursos. Como MPLS, *IntServ* no requiere el uso de protocolo de señalización específico y puede acomodar una variedad de protocolos de señalización, de los cuales RSVP es el más popular. RSVP fue desarrollado para apoyar la arquitectura *IntServ*, pero puede ser utilizado para transportar otros tipos de información de control. Esto se debe a que de RSVP no tiene conocimiento del contenido de los campos de protocolo RSVP que contienen el tráfico e información de control de políticas utilizadas por los enrutadores para reservar recursos. RSVP puede ser utilizado para hacer reservas de recursos, tanto para aplicaciones de con tráfico *Unicast* y *Multicast*. [11]

RSVP fue diseñado con el fin de apoyar conferencias de partes múltiples, es decir, muchos a muchos, con receptores heterogéneos. En RSVP, la reserva de recursos es decidida e iniciada por un receptor, ya que sólo el receptor sabe realmente cuánto ancho de banda necesita. Este enfoque también permite a un receptor unirse o dejar una conexión *Multicast* siempre que quiera.

Un problema con la reserva iniciada por el receptor es que el receptor no conoce la ruta de acceso desde el emisor hasta el mismo. Por lo tanto, no puede solicitar la asignación de recursos en cada enrutador a lo largo de la ruta, ya que no sabe cuáles son estos enrutadores. Este problema se resuelve mediante el *Path message* que se origina desde el emisor y viaja a lo largo de la ruta de *Unicast* o *Multicast* al receptor. El objetivo principal del *Path message* es almacenar la información del *Path state* en cada nodo a lo largo de la ruta y para llevar información sobre las características de tráfico del remitente y las propiedades de la ruta de extremo a extremo. Como parte de la información contenida en *Path message*, es la siguiente:

- *Phop*: esta es la dirección del salto previo del enrutador RSVP-compatible que reenvía el mensaje. Esta dirección se almacena en la información del *Path state* en cada nodo, y se utiliza para enviar el mensaje de reserva de *upstream* hacia el remitente.
- *Sender template*: este campo lleva la dirección IP del remitente y opcionalmente el puerto emisor UDP/TCP.
- *Sender TSpec*: esto campo define las características del tráfico de los flujos de datos que el emisor va a generar.
- *Adspec*: este campo transporta información de un paso con publicidad (OPWA, *One-Pass With Advertising*), esta es la información se reúne en cada nodo a lo largo del camino seguido por el *Path message*, los datos se envían al receptor, que luego se puede utilizar para construir una nueva solicitud de reserva o para modificar una reserva existente. Tras la recepción del *Path message*, el receptor envía una *Resv message* hacia el remitente lo largo de la trayectoria inversa que siguió el *Path message* (ver figura 2.11 [11]).
- *Flowspect*: este campo especifica la QoS deseada. Consta del receptor TSpec, la RSpec, y la clase de servicio. El receptor TSpec es un conjunto de descriptores de tráfico que utilizan los nodos a lo largo de la ruta para reservar recursos. El RSpec define el ancho de banda deseado y retrasar garantías. Cuando se utiliza RSVP en *IntServ*, la clase de servicio podría ser o bien el servicio garantizado o el servicio de carga controlada.
- *Filterspec*: define los paquetes que van a recibir la QoS solicitada que fue definida en el *flowspec*. Una especificación de filtro simple podría ser sólo la dirección IP del remitente y opcionalmente el puerto UDP o TCP.

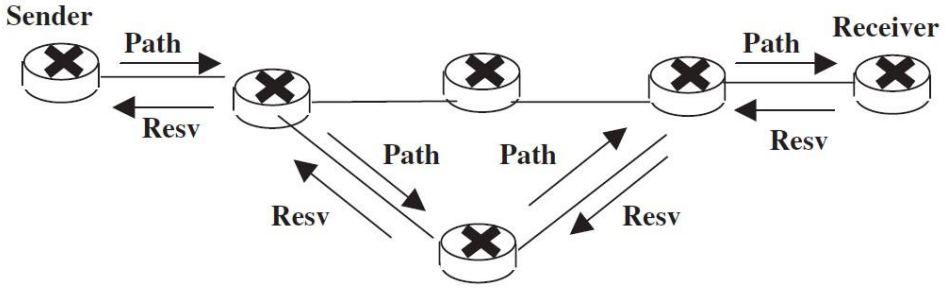

Figura 2.11. Ruta y mensaje de reserva

Cuando un enrutador recibe el mensaje Resv, se reserva recursos de acuerdo con las instrucciones del receptor y luego envía el mensaje de Resv al enrutador del anterior salto obtenido a partir de la información del estado de ruta. Mensajes RSVP se envían en datagramas IP sin procesar y sin encapsulación TCP o UDP. (Se permite la encapsulación UDP para los enrutadores que no soportan los datagramas IP en bruto).

RSVP hace uso de las nociones de datos de flujo y sesión. Una sesión es definida por los parámetros: dirección IP de destino, ID de protocolo y número de puerto de destino opcionalmente. Un flujo de datos es simplemente los paquetes transmitidos por un emisor en una sesión particular. RSVP es simplex; es decir, se hace reservaciones para los datos de flujos unidireccionales. Por lo tanto, a fin de que dos usuarios A y B para comunicarse en ambos sentidos, que se han establecido dos sesiones separadas; una sesión de A a B, y otra de B a A.

2.4.6.3 Protocolo de distribución de etiquetas basado en restricciones (CR-LDP)

El protocolo de distribución de etiquetas basado en restricciones (CR-LDP, *Constraint-Based Label Distribution Protocol*) es un protocolo de distribución de etiquetas basado en LDP. Como se describió anteriormente, LDP se puede utilizar para establecer una LSP asociada a un FEC en particular. CR-LDP se utiliza para configurar un LSP enrutado explícitamente punto a punto unidireccional, referido como la ruta conmutada de etiquetas con enrutado basado en restricciones (CR-LSP, *Constrained-Based Routed Label Switched Path*). [11]

Un LSP está configurado como resultado de la información de ruteo en una red IP utilizando el algoritmo del camino más corto. Una CR-LSP se calcula en la fuente LSR basado en criterios no limitado a la información de enrutamiento, tal como el enrutamiento explícito y basado en QoS. La ruta señalizada a los otros nodos a lo largo de la trayectoria que obedecen instrucciones de enrutamiento de origen. Esta técnica de enrutamiento, llamado enrutamiento de origen, también se utiliza en ATM.

Una CR-LSP en MPLS es análogo a una conexión en ATM, sólo que es unidireccional. Los procedimientos de señalización ATM configurar automáticamente una conexión bidireccional entre dos *host* ATM, donde cada dirección de la conexión puede estar asociado con diferentes parámetros de tráfico y de QoS. Una CR-LSP bidireccional

entre LSR 1 y 2 sólo puede ser creada mediante la configuración de una CR-LSP desde LSR 1 a LSR 2 y una separada de LSR 2 a LSR 1. Como en el caso de un LSP, una CR-LSP tiene un LSR de entrada y una salida.

CR-LSP se puede utilizar de diversas maneras. Por ejemplo, pueden ser utilizados en una red IP para hacer balance de carga. Es decir, el tráfico entre sus enlaces se puede distribuir de manera uniforme al forzar algo del tráfico sobre CR-LSP, que pasan a través de enlaces menos utilizados. Una CR-LSP también se puede utilizar para crear túneles en MPLS, e introducir rutas basadas en criterios de QoS, tales como la minimización del retardo total de extremo a extremo, y la maximización del *Throughput*. Por ejemplo, una la red MPLS distribuida como aparece en la en la figura 2.12 [11] y se considera que la trayectoria entre el LSR de entrada A y el LSR de salida G, calculado utilizando OSPF, pasa a través de E y F.

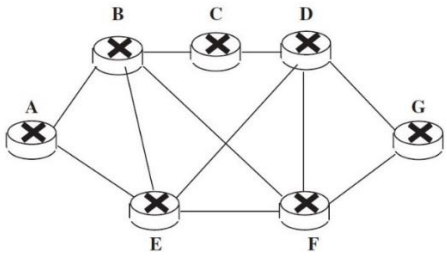

Figura 2.12. Ejemplo de un CR-LSP

Usando CR-LDP se puede configurar una CR-LSP que satisface un criterio de calidad de servicio, tales como minimizar el retardo de extremo a extremo. Por ejemplo, si los LSR B, C y D no se utilizan en gran medida, el enrutamiento de la CR-LSP a través de estos LSR reducirá el retardo de extremo a extremo, a pesar de que el número de saltos será más alto que el camino de E-a-F. Las siguientes son algunas de las características de la CR-LDP:

- CR-LDP se basa en LDP, y se ejecuta en la parte superior de TCP por fiabilidad.
- La máquina de estados CR-LDP no requiere actualización periódica.
- CR-LDP permite rutas explícitas estrictas y sueltas. Esto facilita que el LSR de entrada tenga un cierto grado de conocimiento imperfecto acerca de la topología de la red. El LSR fuente también podría solicitar la fijación de ruta, el cual corrige

el camino a través de una ruta definida vagamente para que no cambie cuando un mejor salto siguiente esté disponible.

- CR-LDP permite la preferencia de ruta mediante la asignación de configuración / mantenimiento de las prioridades a CR-LSPs. Si no se puede encontrar una ruta para una CR-LSP de alta prioridad, entonces existen CR-LSPs de menor prioridad y puede ser desviado para permitir CR-LSPs con prioridad más alta.
- El operador de red puede clasificar a los recursos de red de varias maneras. CR-LDP permite la indicación de las clases de recursos que se pueden utilizar cuando se está estableciendo un CR-LSP.
- Como en el caso de ATM, CR-LDP permite la especificación de los parámetros de tráfico en un CR-LSP y cómo deben ser vigilados estos parámetros.

CR-LDP depende de loa siguientes funcionalidades mínimas de LDP:

- Mecanismo básico descubrimiento extendido (y/o)
- Mensaje de petición de etiqueta para *downstream* por demanda con control ordenado
- Mensaje de asignación de etiquetas para *downstream* por demanda con control ordenado
- Mensajes de notificación
- Etiqueta de retirar y liberar mensajes
- Detección de bucle para los segmentos enrutados sueltos

2.4.7 Ingeniería de tráfico

La ingeniería de tráfico (TE, *Traffic Engineering*) [25] hace referencia al proceso de selección de las mejores rutas para el tráfico de datos con el fin de equilibrar la carga de tráfico en los diferentes enlaces. Por lo general, los algoritmos de enrutamiento (por ejemplo, OSPF) calcular el camino más corto disponible, y ponen todo el tráfico en esos enlaces. Sin embargo, la mayoría de las veces la red tiene caminos alternativos para enviar la información, y el tráfico se puede distribuir entre todos esos enlaces. La ingeniería de tráfico es muy importante en las redes donde múltiples caminos paralelos o alternativos disponibles. En la figura 2.13 [26], se

muestran los caminos posibles que un paquete tomaría desde un origen, hacia un destino.

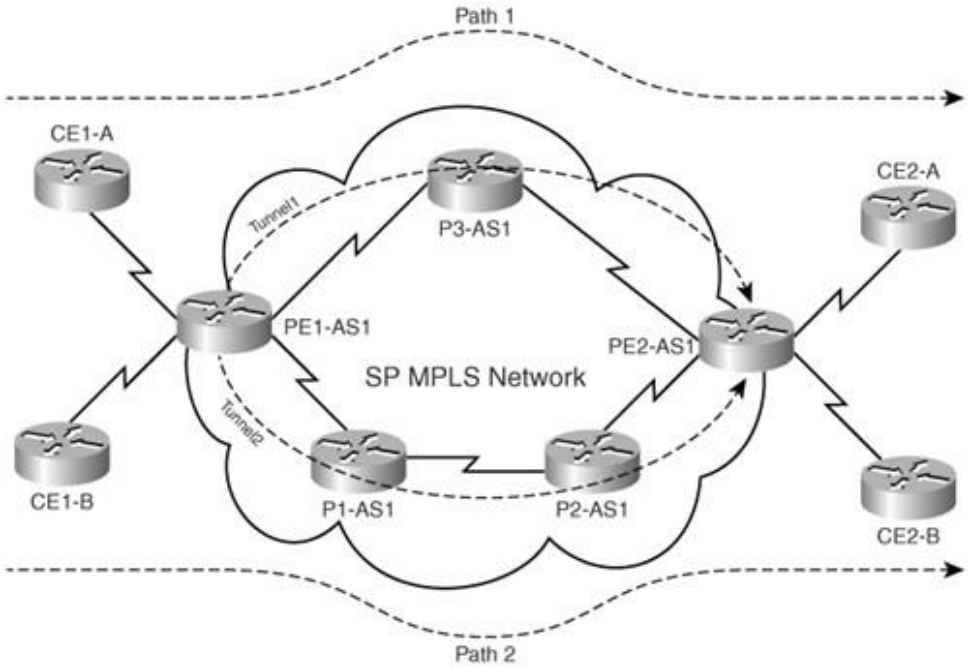

Figura 2.13. Dos caminos en una red

Antes de MPLS TE, la ingeniería de tráfico se llevó a cabo ya sea por IP o por ATM, dependiendo del protocolo en uso entre dos enrutadores de borde en una red. TE con IP se implementó en su mayoría por la manipulación de costo interfaz cuando múltiples caminos existían entre dos puntos extremos de la red. Además, permitieron a las rutas estáticas de dirección del tráfico a lo largo de un camino específico hacia un destino.

La principal ventaja de la implementación de MPLS TE es que proporciona una combinación de capacidades de TE de ATM, junto con CoS a diferencia de IP. En MPLS TE, el enrutador extremo de la cabeza en la red controla el camino tomado por el tráfico a cualquier destino en particular dentro de la red.

Con MPLS, no es necesario crear una malla completa de circuitos virtuales, y la red se transforma dentro del dominio de etiquetas conmutadas, en el que los LSP de TE o túneles TE definir rutas que se pueden utilizar por el tráfico.

2.4.8 MPLS TE para QoS

2.4.8.1 DiffServ MPLS TE

MPLS-TE y *DiffServ* se pueden implementar simultáneamente en una red troncal IP, con TE se determina la trayectoria del tráfico sobre la base de las limitaciones de ancho de banda total, y mecanismos *DiffServ* que se utilizan en cada enlace para la programación diferencial de paquetes por clase de servicio. TE y *DiffServ* son tecnologías ortogonales que pueden ser utilizados de manera simultánea para obtener beneficios combinados: TE permite la distribución de tráfico en rutas que no son las más cortas para el uso eficiente de ancho de banda disponible, mientras que *DiffServ* permite la diferenciación SLA por clase de servicio, sin embargo, de esta forma, MPLS TE solo conoce un conjunto agregado de ancho de banda disponible por enlace y no sabe qué recursos específicos de ancho de banda de enlace se asignan a qué colas y, por lo tanto, a qué clases.

DiffServ MPLS TE (DS-TE) se extiende las capacidades básicas de TE para permitir que el cálculo de ruta basado en restricciones, el enrutamiento explícito y el control de admisión se realicen por separado para diferentes clases de servicio. DS-TE proporciona la capacidad de imponer diferentes restricciones de ancho de banda para diferentes clases de tráfico mediante la adición de más grupos de ancho de banda disponible en cada enlace. [17]

Capítulo 3

3. DISEÑO DE LA RED DE TELEMETRÍA

El diseño de la red de telemetría se realizó con base en la Metodología *Top - Down Network Design*, en la cual se tienen cuatro fases, se inició por el análisis de requisitos, posteriormente se realizó el diseño lógico de la red, seguidamente se hizo el diseño físico, para finalmente realizar pruebas y documentar.

3.1 Análisis de requisitos

En esta fase se identificará los objetivos y restricciones del negocio, y los objetivos y restricciones técnicos del cliente.

3.1.1 Análisis de los Objetivos y Restricciones del Negocio

El Servicio Geológico Colombiano tiene la misión de contribuir al desarrollo económico y social del país, a través de la investigación en geociencias básicas y aplicadas del subsuelo, el potencial de sus recursos, la evaluación y monitoreo de amenazas de origen geológico, la gestión integral del conocimiento geocientífico, la investigación y el control nuclear y radiactivo, atendiendo las prioridades de las políticas del Gobierno Nacional.

El SGC, cuenta con una Dirección de Geoamenazas cuyo objetivo es realizar investigación, seguimiento y monitoreo de amenazas geológicas como base para la gestión integral del riesgo, ordenamiento territorial y planificación del desarrollo mediante investigación y zonificación de movimientos en masa; amenaza sísmica, amenaza volcánica, investigación y monitoreo de actividad volcánica e investigación

de deformación de la corteza terrestre. En la figura 3.1 [27], se ilustra el organigrama del Instituto.

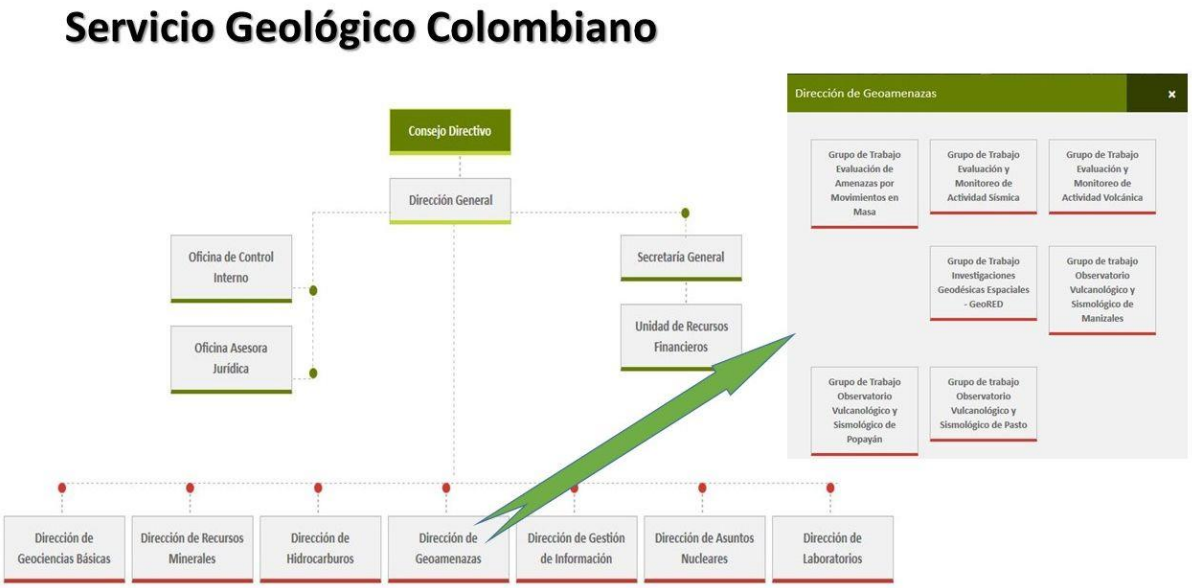

Figura 3.1. Organigrama Servicio Geológico Colombiano

En el Servicio Geológico Colombiano (SGC), la Dirección de Geoamenazas, cuenta con tres Observatorios Vulcanológicos, ubicados en las ciudades de Manizales, Popayán y Pasto, los cuales están liderados por un Coordinador de proyecto que sería el primer filtro para asignar recursos tanto en dinero como en personal a determinadas iniciativas, entre ellas, la renovación de equipos de telecomunicaciones.

El proyecto a desarrollar es una iniciativa de diseño que cambia de manera significativa la red de telemetría, es por eso que se debe exponer ante la Dirección Técnica y luego a la Dirección General para una asignación de recursos a futuro enmarcado en el plan estratégico de la institución.

El presente proyecto impacta de manera directa sobre el desempeño y administración de la red de telemetría, así como también sobre los costos de capital y operación.

Objetivos a considerar en el diseño del presente proyecto que son requerimientos del SGC:

- Diseño para toda la red de telemetría del SGC-OVSP.

- Soporte para ejecución de las aplicaciones actuales
- Servicios de red seguros, optimizados para reducir el impacto en el rendimiento.
- Solución de conectividad robusta y escalable.

Restricciones del Negocio

- Para la caracterización de la red, se presenta una dificultad al acceder a la totalidad de las repetidoras debido al trámite de permisos y logística necesaria, en la mayoría de las estaciones se puede ingresar únicamente para realizar mantenimiento.
- El alcance del presente proyecto se limita al diseño, es por eso que no es posible evidenciar una mejora en el desempeño con datos reales de la red, para ello se utiliza un escenario de conectividad similar y generadores de tráfico.
- En lo relacionado a presupuesto, el proyecto se enfoca en el diseño, es por eso que no hay impacto financiero en esta fase para el SGC.
- Tanto el recurso humano como el cronograma propuestos para este diseño son responsabilidad únicamente del autor, de tal manera que el SGC no tiene asignación de recursos en este proyecto.
- En el SGC, no se cuenta con políticas sobre la red de telemetría
- Las conexiones inalámbricas de largo alcance, se rigen por las normas establecidas por la Agencia Nacional del Espectro (ANE).

Aplicaciones a ejecutar en la red

En el SGC OVSP se realizó un levantamiento de información relacionada con las aplicaciones que utilizan la red de telemetría, en la tabla 3.1 se presenta un resumen. La capacidad requerida por estación se calculó a partir de datos registrados utilizando un equipo *Router Board Mikrotik* 2011 configurado con un puerto espejo en el que se conectó un equipo de cómputo con sistema operativo *Kali* Linux y el programa *ntopng*. En la figura 3.2 se ilustra el esquema de conexión.

Nombre	Descripción	Almacenamiento	Capacidad Requerida (kbps) por cada estación
NAM [5]	Unidad de adquisición de datos Digitalizador Guralp (Ocupación permanente) Nivel máximo de saturación del sensor, hasta 48 Kbps	Red LAN, Sistema Scream, Disco duro estación de trabajo	24
RTPD[6]	Sistema de adquisición de datos Digitalizador Reftek (Ocupación permanente)	Red LAN, sistema EarthWorm	24
NaqServer	Sistema de adquisición de datos Digitalizador Taurus (Ocupación permanente)	Red LAN, sistema EarthWorm	24
SeedLink Server	Sistema de adquisición de datos Digitalizador Centaurus (Ocupación permanente)	Red LAN, sistema EarthWorm	24
Advanced TCP/IP Data Logger	Sistema de adquisición de datos de digitalizadores a baja tasa de muestreo (Inclinómetros, Radón, Termocuplas, Anemómetros) (Ocupación de 1 segundo cada 5 minutos)	Disco duro unidad local (texto plano)	2
Geonica	Sistema de adquisición de datos de digitalizadores a baja tasa de muestreo (Climatológica)	Disco duro unidad local (SQL Server E)	10
Cliente FTP (Cámaras IP)	Aplicaciones para el envío de imágenes desde cámaras IP (ocupación 1 segundo para imágenes de 24 KB cámara AXIS, para cámaras Vivotek imágenes 1600x1200 pixels, 128 KB, ocupan 128 Kbps durante 8 segundos)	Disco duro unidad local (imágenes)	128
NovacProgram	Sistema de adquisición de datos de digitalizadores a baja tasa de muestreo (SO_2)	Disco duro unidad local (texto plano)	10
Trimble 4D Control	Sistema de adquisición de datos de estaciones GNSS[7]	Disco duro unidad local (binarios)	24

Tabla 3.1. Aplicaciones

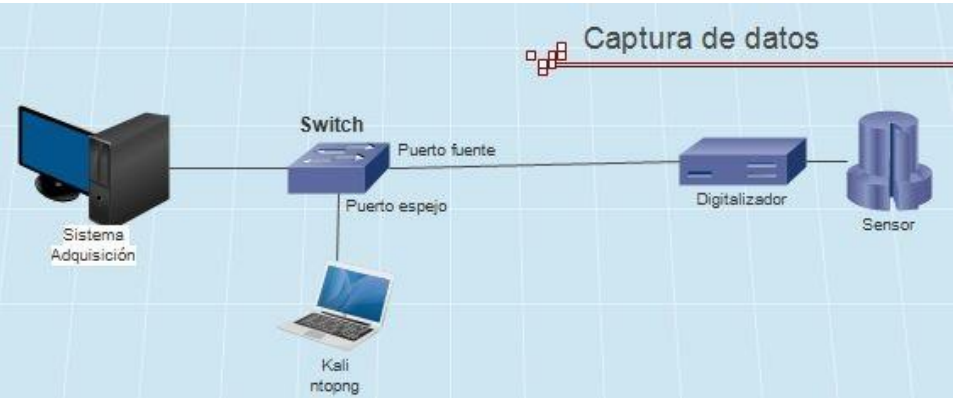

Figura 3.2. Esquema de conexión para la captura de datos

[5] NAM es un equipo servidor de señales sísmicas, diseñado para recibir, almacenar y transmitir flujos de datos en una red IP (http://www.guralp.com/products/data-acquisition/nam).

[6] RTPD Protocolo de corrección de errores, ha sido desarrollado para proporcionar la comunicación y la adquisición de datos en tiempo real desde las estaciones de red (http://www.reftek.com/ref-tek-protocol-daemon-rtpd/)

[7] GNSS Sistema global de navegación por satélite

3.1.2 Análisis de los Objetivos Técnicos y sus Restricciones

En este aparte, se trata de evaluar las metas técnicas planteadas por el Instituto para este proyecto con el objetivo de presentar una solución de diseño acorde a los requerimientos descritos en la tabla 3.2

Objetivo técnico	Requerimiento	Limitación
Escalabilidad	- Garantizar la capacidad de crecimiento horizontal y vertical de la red - Garantizar la incorporación de nuevas estaciones a la red	
Disponibilidad	- Incluir redundancia tanto en número de conexiones como en trayectoria. - Se requiere una disponibilidad mayor al 90 %	Consecución de permisos en predios para la ubicación de estaciones de comunicación.
Capacidad	Se hace necesario aumentar la capacidad de transmisión (Rx/Tx) para incrementar la periodicidad en el muestreo de algunas estaciones y uso de nuevas aplicaciones como: escritorio remoto, voz sobre IP (VoIP, Voiceover IP) y video.	
Resiliencia	Como el SGC soporta la información que se entrega a Instituciones afines, con los datos del mayor número de estaciones, la capacidad de recuperación ante desastres es altamente valorada	
Rendimiento	Es importante considerar los aspectos como exactitud, eficiencia, retraso y variación del retraso, en el diseño de la red	Baja capacidad de transmisión de equipos de comunicación de tipo industrial utilizados en zonas de condiciones climáticas adversas.
Seguridad	La seguridad para este proyecto, se enmarca en: Integridad, Confidencialidad y Disponibilidad	
Gestionabilidad	- Centralizada - Simplificada - Uso de tablero pizarra (Dashboard) - Mesa de ayuda para soporte	
Usabilidad	Acceso fácil a la red y los servicios	
Adaptabilidad	- Facilidad de implementar cambios - Escalable horizontalmente - Compatibilidad con diferentes fabricantes - Genera poco tráfico adicional	
Accesibilidad	Este requerimiento se asocia a la conectividad, visto como la posibilidad de conexión entre dos nodos, así como también el ingreso desde otras redes ya sean públicas o privadas tanto en estaciones portátiles o temporales como para ingreso permanente al sistema de procesamiento.	

Tabla 3.2. Requerimientos técnicos

3.1.3 Caracterización de la Red Existente

La red de telemetría tiene la función de interconectar los equipos sensores y el sistema de adquisición, la red está distribuida en una topología en estrella, se divide en dos dominios de *Broadcast*, uno basado en switches y otro una red ruteada con redundancia en capa 3 del modelo OSI. En la figura 3.3, se ilustra la conectividad de la red de telemetría a nivel de OSI en capa 2 y 3.

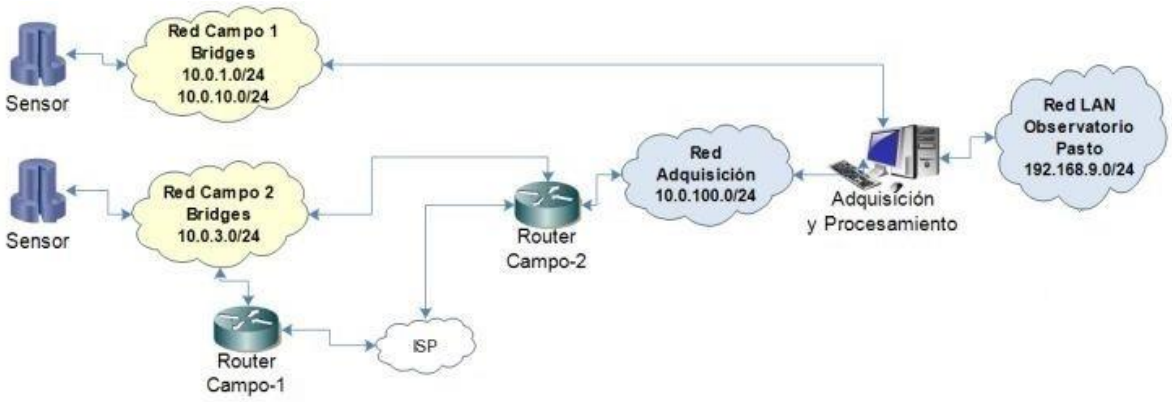

Figura 3.3. Esquema de conectividad en capa 2 y 3 de OSI de la red de Telemetría.

En cuanto a conectividad y transporte de datos, la red de telemetría del OVSP, se basa en equipos de comunicación inalámbrica enmarcados en el concepto de Redes Inalámbricas de área extensa (WWAN, *Wireless Wide Area Network*) que utilizan frecuencias de operación en las bandas libres (900 MHz y 5 GHz); la red de telemetría tiene tres componentes:

a) Troncal, son enlaces de radio desde el nodo central (Observatorio) hasta las repetidoras principales, esta conexión tiene capacidad de transporte entre 5 y 10 Mbps.
b) Sub troncal, son enlaces de radio desde las repetidoras principales hasta las repetidoras secundarias.
c) *End point*, es el enlace desde la repetidora secundaria hasta los equipos finales en los cuales se conectan sensores que registran varios parámetros geofísicos, estos equipos están ubicados en cercanías a los edificios volcánicos.

La recepción de los datos trasportados por la red de Telemetría se recibe en una torre de comunicaciones que por canaletas metálicas se conecta a un rack en el cual se disponen físicamente los equipos de comunicación.

En figura 3.4 [3], se ilustra el esquema físico de conectividad entre repetidoras principales y secundarias hasta el OVSP; en la tabla 3.3, se listan los equipos utilizados en cada componente y algunas de sus características.

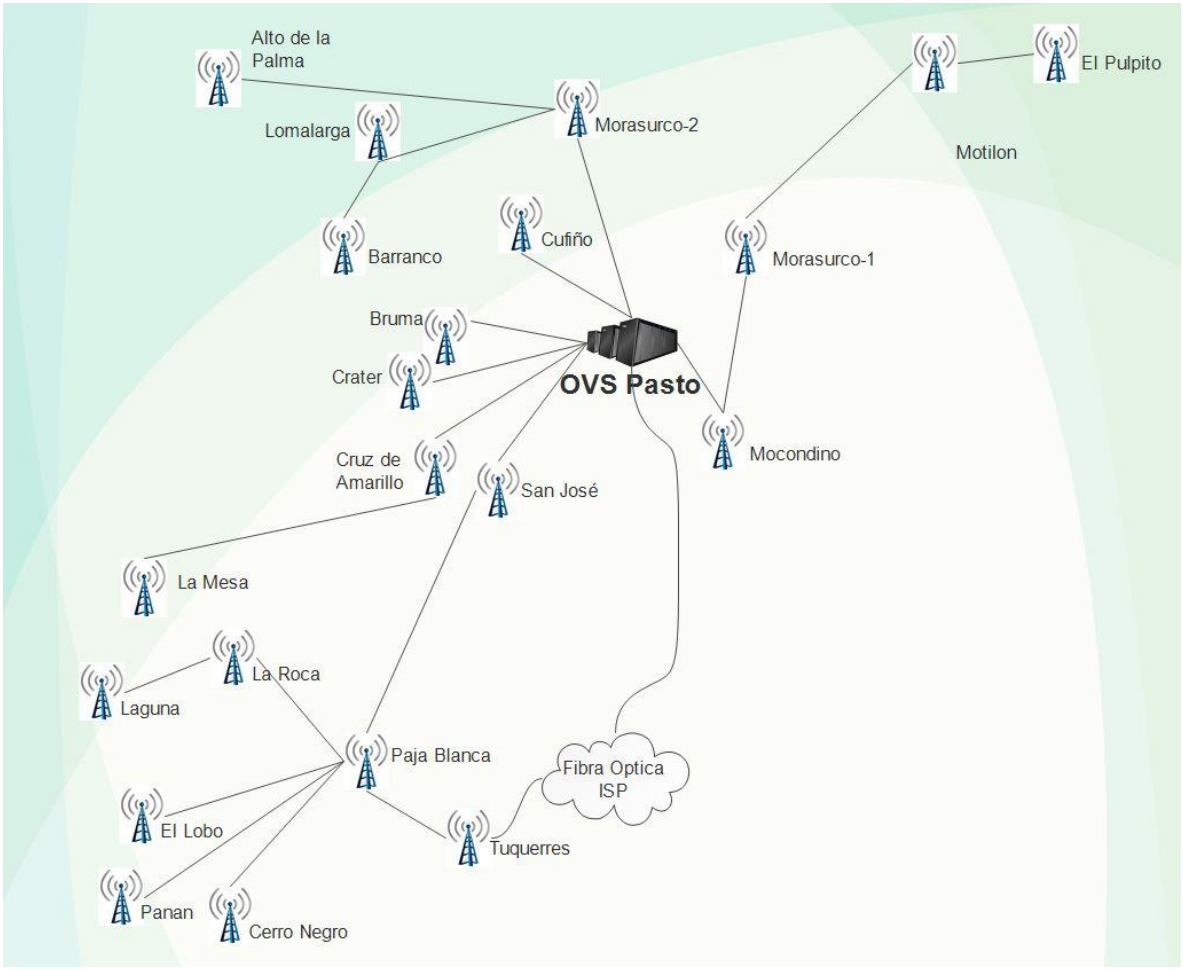

Figura 3.4. Distribución física de repetidoras en el OVSP

Componente	Equipo utilizado	Característica
Troncal	Radio antena Ubiquiti AirMax M/AC Frecuencia libre banda 5 GHz	IEEE 802.11 n 5 – 10 Mbps Ethernet
Sub troncal	Radio Freewave HTPlus Frecuencia libre banda 900 MHz	FHSS 128 – 400 Kbps Ethernet
Punto final	Radio Freewave FGR 2P	FHSS 8 – 128 Kbps Ethernet Serial (socket)

Tabla 3.3. Componentes de la red de telemetría

3.1.4 Caracterización del tráfico de la red

Para caracterizar el tráfico actual en la red de telemetría, se utilizó como base de recolección de datos, el equipo enrutador Campo-2, representado en la figura 3.3. Esquema de conectividad LAN en el OVSP; de marca Mikrotik modelo RB2011 UiAS-2HnD y sistema operativo *RouterOS mipsbe* 6.34.3, a través del módulo IP Firewall Mangle, se creó reglas para marcar o etiquetar conexiones y paquetes que atraviesan el enrutador correspondiente a equipos sensores de varios tipos. En la figura 3.5 se muestra una captura de pantalla de la herramienta *Winbox*[8] utilizada para gestionar dispositivos Mikrotik.

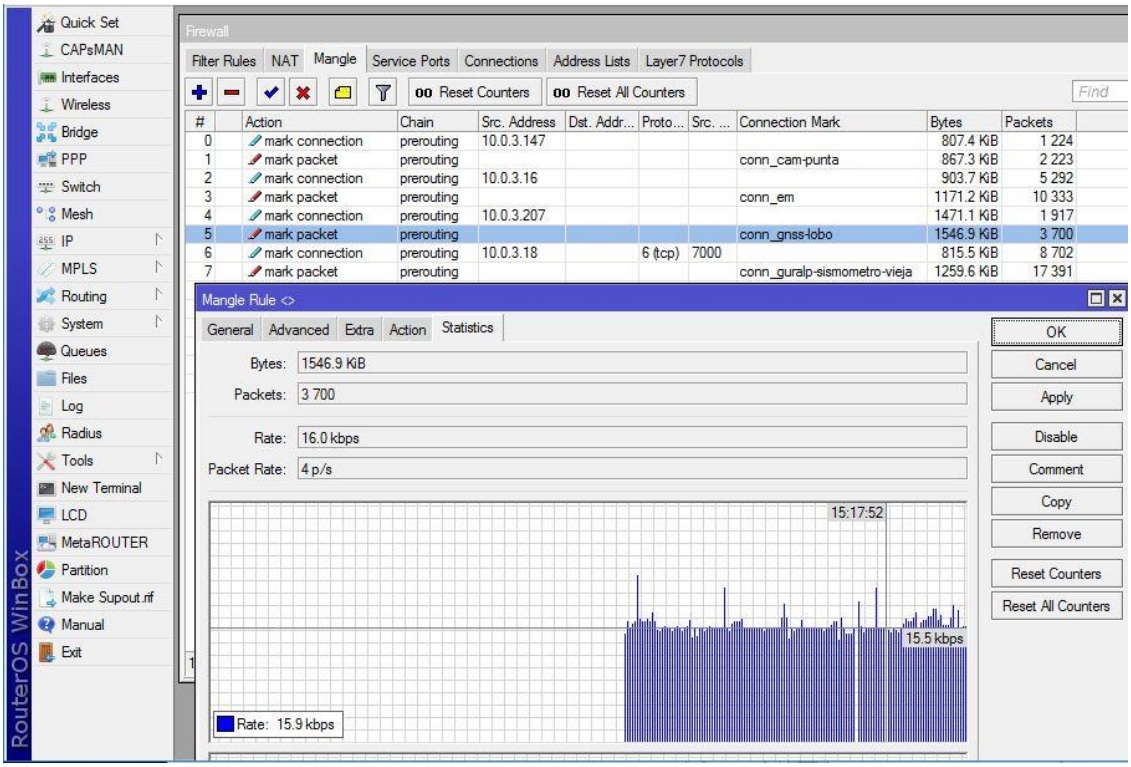

Figura 3.5. Reglas de etiquetado de tráfico en la interfaz Winbox, para equipos Mikrotik

Basados en el esquema de conexión para captura de datos representado anteriormente en la figura 3.2, con el uso de la herramienta *ntop-ng*[9] se realizó una

[8] Winbox: es una herramienta que permite la administración de *MikroTik RouterOS* usando una *GUI* rápida y simple que se describe en detalle en el anexo C, disponible en: https://mikrotik.com/download

[9] Ntop-ng: es una herramienta para el análisis de tráfico basado en web de alta velocidad y recopilación de flujo, disponible en: https://www.ntop.org/products/traffic-analysis/ntop.

captura del tráfico de las troncales principales y se evidencian varios aspectos relacionados al uso de protocolos, equipos, capacidad utilizada entre otros parámetros, en las figuras 3.6, 3.7 y 3.8, se puede observar los principales resultados en el sondeo realizado.

Application Protocol	Total (Since Startup)	Percentage
Unknown	18.63 MB	69.91 %
FTP_DATA	2.19 MB	8.22 %
SNMP	741.04 KB	2.72 %
ICMP	728.66 KB	2.67 %
FTP_CONTROL	63.96 KB	0.23 %
IGMP	30.7 KB	0.11 %
HTTP	27.86 KB	0.1 %
LLMNR	20.58 KB	0.08 %
DHCP	12.69 KB	0.05 %
sFlow	7.2 KB	0.03 %
NetBIOS	7.66 KB	0.03 %
SSDP	3.03 KB	0.01 %
ICMPV6	2.13 KB	0.01 %

Figura 3.6. Protocolos bien conocidos usados en la troncal Cruz de Amarillo

El tráfico identificado como *Unknown*, hace referencia al tráfico generado por los sistemas de adquisición de señales de diferentes áreas del monitoreo y se representan en la figura 3.7.

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	? Unknown	TCP	10.0.1.122:afs3-fileserver	10.0.1.247:44072	42 min, 52 sec	Client Server	35.48 Kbit	9.39 MB	
Info	? Unknown	TCP	10.0.1.247:40827	10.0.1.26:afs3-fileserver	26 min, 58 sec	Client Server	20.01 Kbit	2.63 MB	
Info	? Unknown	TCP	10.0.1.54:afs3-fileserver	10.0.1.247:40581	42 min, 52 sec	Client Server	18.72 Kbit	8.16 MB	
Info	? Unknown	TCP	10.0.1.204:5018	10.0.1.240:49289	42 min, 52 sec	Client	16.14 Kbit	4.98 MB	
Info	? Unknown	TCP	10.0.1.148:afs3-fileserver	10.0.1.247:39009	42 min, 51 sec	Client Serve	13.03 Kbit	4.08 MB	
Info	? Unknown	TCP	10.0.1.216:5017	10.0.1.240:58044	42 min, 51 sec	Client	11.87 Kbit	3.56 MB	
Info	? Unknown	TCP	10.0.1.247:47210	10.0.1.22:afs3-fileserver	34 min, 1 sec	Clien Server	11.74 Kbit	2.81 MB	
Info	? Unknown	TCP	10.0.1.52:afs3-fileserver	10.0.1.247:49200	42 min, 51 sec	Client	6.81 Kbit	1.77 MB	
Info	? Unknown	TCP	10.0.1.24:afs3-callback	10.0.1.3:51928	42 min, 51 sec	Client Server	2.12 Kbit	639.58 KB	
Info	? Unknown	TCP	10.0.1.208:5017	10.0.1.240:56813	42 min, 32 sec	Client Server	729.5 bps	569.2 KB	
Info	? Unknown	UDP	10.0.10.200:5678	Broadcast:5678	42 min	Client	278.36 bps	7.31 KB	
Info	? Unknown	UDP	10.0.1.200:5678	Broadcast:5678	42 min	Client	276.76 bps	7.26 KB	

Figura 3.7. Protocolos y puertos utilizados por los sistemas de adquisición de datos transportados en la troncal Cruz de Amarillo

En la figura 3.8, se presenta un estimativo de la ocupación del canal de comunicación por cada equipo, el tamaño del cuadro, es proporcional al porcentaje de uso del canal.

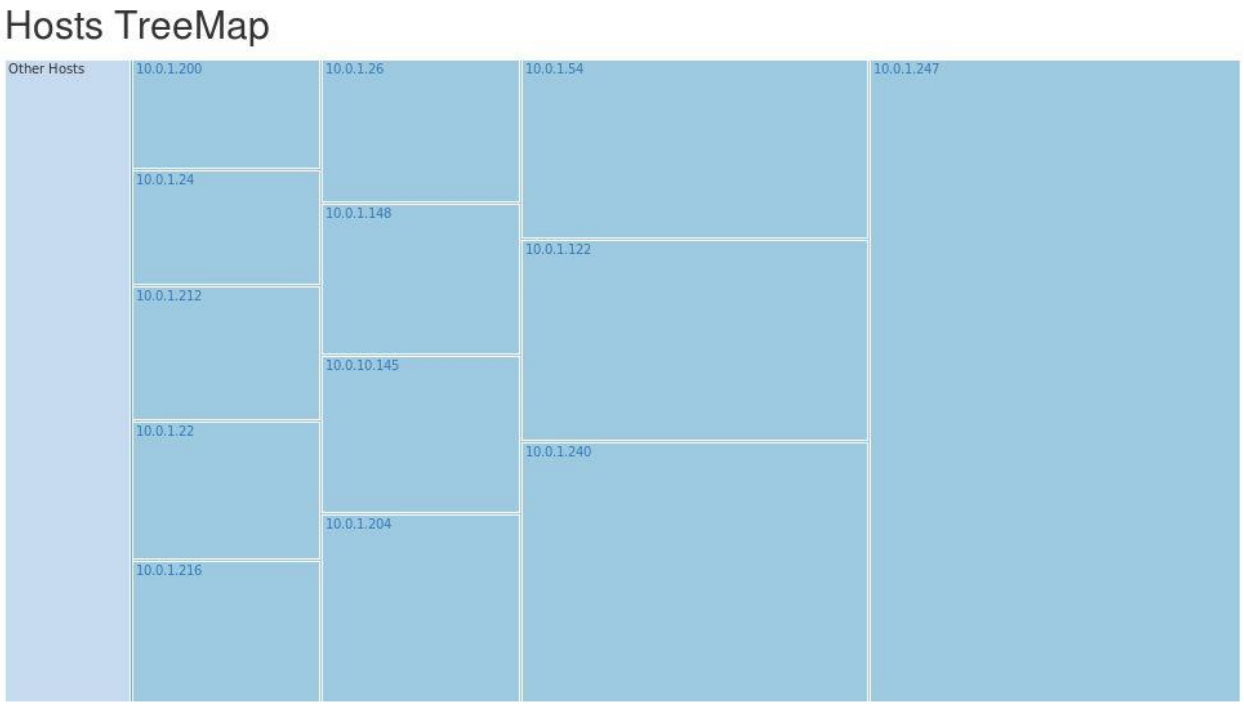

Figura 3.8. Esquema del porcentaje de utilización por equipo del canal de comunicación en la troncal de Cruz de Amarillo

En la tabla 3.4 se listan las aplicaciones o equipos y los protocolos que más tráfico generan a través de la red de telemetría.

Aplicación	**Protocolo**									
	ICMP	ARP/ RARP	TCP	UDP	RTP	SSH	HTTP/ HTTPS	SNMP	FTP	Otros
NAM		X	x	X						
RTPD		X	x	X	X					X
NaqServer		X	X				X			X
SeedLink Server		X	X	X			X			X
Advanced TCP/IP Data Logger		X	X							X
Geonica		X	X							X
Cliente FTP (cámaras IP)		X							X	
Novac		x				x		X	x	

Tabla 3.4. Protocolos más utilizados en la red de telemetría

Broadcast / Multicast

Con la aplicación *Ntop* (ntop-5.0-5.el6.x86_64) en Linux, se realizó la captura del tráfico *Broadcast* y *Multicast* de las redes 10.0.1.0/24 y 10.0.10.0/24, conectando directamente a un puerto del switch de la red de telemetría el servidor Linux. En las figuras 3.9 y 3.10 se ilustran los resultados obtenidos. Estas dos redes pertenecen al mismo dominio de *Broadcast*.

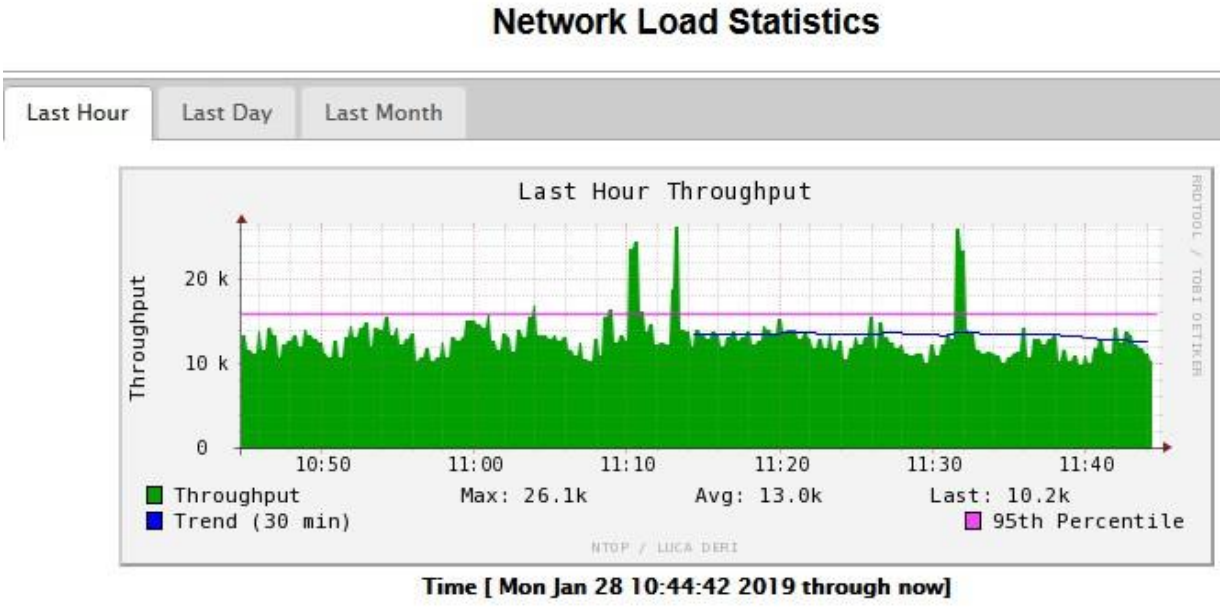

Figura 3.9. Tráfico Broadcast en las redes 10.0.1.0/24 y 10.0.10.1

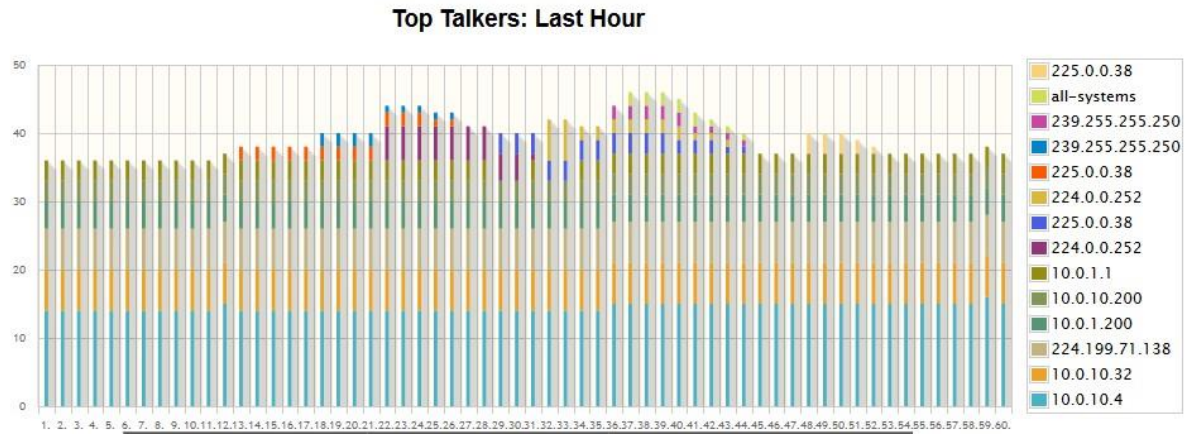

Figura 3.10. Protocolos bien conocidos usados en la troncal Cruz de Amarillo

Disponibilidad de la red

En el Observatorio Pasto, se cuenta con varias herramientas de uso libre, enfocadas a monitorizar varios parámetros de rendimiento de las redes de datos como son *Nagios*[10], *MRTG*[11], Cacti[12] y *The Dude*[13], para evaluar la disponibilidad se utiliza *Nagios* y la funcionalidad Reportes / Disponibilidad / Service / Ping – Troncal. En la figura 3.11 se muestra la disponibilidad de las troncales en el segundo semestre del año 2018, en promedio se obtuvo un valor del 99.2 % de disponibilidad de las 8 repetidoras principales.

Hostgroup 'repetidoras' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
bruma	98,456% (98,456%)	1,544% (1,544%)	0,000% (0,000%)	0,000%
crater	97,567% (97,567%)	2,433% (2,433%)	0,000% (0,000%)	0,000%
cruz-amarillo	99,997% (99,997%)	0,003% (0,003%)	0,000% (0,000%)	0,000%
cufino	99,434% (99,434%)	0,566% (0,566%)	0,000% (0,000%)	0,000%
incli-crater	99,906% (99,906%)	0,094% (0,094%)	0,000% (0,000%)	0,000%
mocondino	98,922% (98,922%)	1,078% (1,078%)	0,000% (0,000%)	0,000%
morasurco-2	99,359% (99,359%)	0,641% (0,641%)	0,000% (0,000%)	0,000%
paja-blanca	99,957% (99,957%)	0,043% (0,043%)	0,000% (0,000%)	0,000%
Average	99,200% (99,200%)	0,800% (0,800%)	0,000% (0,000%)	0,000%

Figura 3.11. Disponibilidad de troncales OVSP

Como parte del proceso de Operación de redes de vigilancia volcánica, los grupos de electrónica de cada Observatorio generan un informe de funcionamiento de la red, en este sentido para el caso del Observatorio Pasto, se tomó el resumen de los informes mensuales de funcionamiento desde enero de 2015 hasta diciembre de 2018 y están graficados en la figura 3.12 con un valor en promedio para los cuatro años del 88.1%

[10] Nagios. Software de monitoreo de servidores (https://www.nagios.org/)
[11] MRTG. Graficador de múltiple tráfico de red (MRTG, *Multi Router TrafficGrapher*)
[12] Cacti. Herramienta para generar gráficos de datos temporales (https://www.cacti.net/)
[13] TheDude. Software de monitoreo de redes, desarrollado por Mikrotik (https://mikrotik.com/thedude)

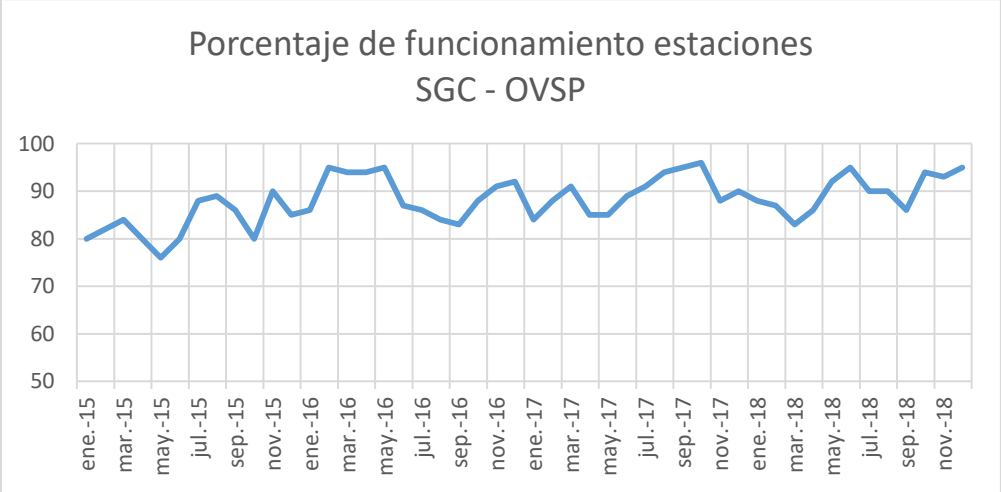

Figura 3.12. Porcentaje de funcionamiento red de telemetría OVSP

En el sistema *Nagios*, se tiene configurado la monitorización de las troncales principales, evaluando la conectividad por medio del protocolo ICMP, en la figura 3.13 se resume los valores registrados por el sistema para el periodo comprendido entre el mes de agosto y el mes de diciembre de 2018.

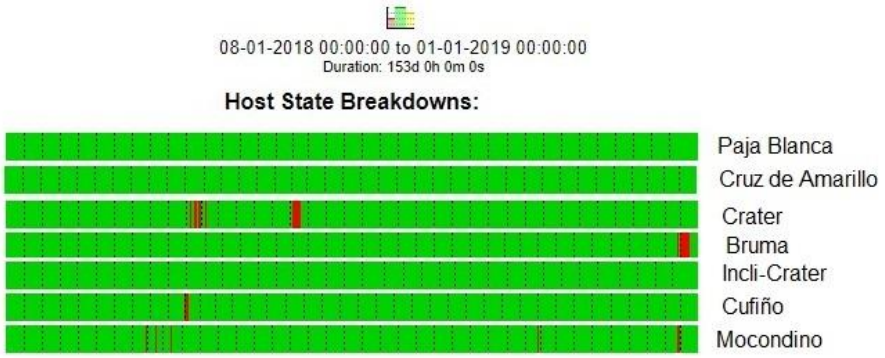

Figura 3.13. Porcentaje de disponibilidad troncales principales (agosto a diciembre de 2018)

En la tabla 3.5, se presentan los valores de tiempo medio entre fallas (MTBF, *Mean Time Between Failures*) y tiempo medio de reparación (MTTR, *Mean Time To Repair*) relacionados con las troncales principales en el periodo comprendido entre agosto y diciembre de 2018, los valores son los reportados por el sistema de monitorización *Nagios*.

Troncales	Equipo	MTBF	MTTR	Fecha y duración de la máxima indisponibilidad	Causa de la máxima indisponibilidad
Paja Blanca	Ubiquiti AirGrid27 + rocket-34	5 meses	61 minutos	09-28-2018 10:34:52 0d 1h 1m 41s	Mantenimiento del sistema eléctrico en la repetidora
Cruz de Amarillo	Ubiquiti AirGrid 27	2.5 meses	3.5 minutos	12-21-2018 09:50:24 0d 0h 6m 2s	Indeterminado
Crater	FW HTPlus	10.2 días	5.6 Horas	10-03-2018 14:24:05 1d 14h 14m	Descarga eléctrica
Bruma	FW HTPlus	7.1 días	2.5 Horas	2-28-2018 11:59:53 2d 01h 44m	Descarga eléctrica
Incli-Crater	FW HTPlus	5.55 días	7.8 Minutos	08-18-2018 17:05:46 0d 1h 15m 20s	Clima
Cufiño	FW HTPlus	5.53	44.3 Minutos	09-09-2018 18:31:27 0d 16h 36m	Clima
Morasurco-2	FW HTPlus	24.5 días	3.91 Horas	09-16-2018 11:47:42 0d 21h 20m	Desacomodo de la antena
Mocondino	Ubiquiti AirGrid 27	12.7 días	2.5 horas	11-26-2018 20:25:00 0d 11h 56m	Batería

Tabla 3.5. Caracterización de la disponibilidad de la red de Telemetría durante el año 2018

Capacidad de los enlaces troncales

La capacidad de transferencia de enlaces troncales se calculó a partir de la herramienta *Bandwidth Test* de Mikrotik, utilizando los parámetros tal como se observan en la figura 3.14. Las pruebas se realizaron con los enlaces libres de tráfico con el fin de garantizar toda la capacidad disponible. En la tabla 3.6, se consignan los resultados obtenidos para los enlaces troncales implementados con equipos *Freewave HTPlus*

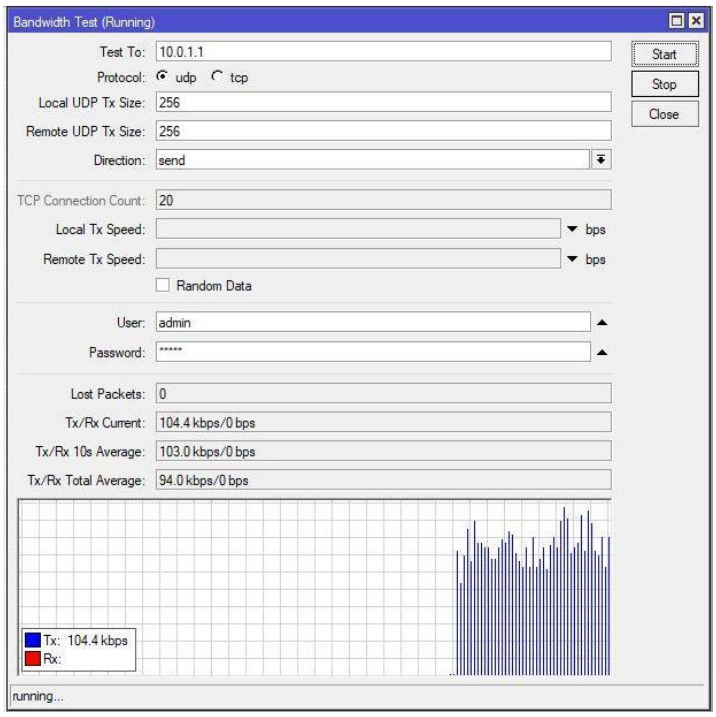

Figura 3.14. Herramienta Bandwidth Test de Mikrotik

			Destino		Protocolo		#	MTU (B)		Dirección			
Troncal	**Equipo**	**Origen**	**Equipo**	**IP**	**UDP**	**TCP**	**Con**	**Local**	**Remoto**	**Tx**	**Rx**	**Thrughput (Kbps)**	Distancia Km
Paja Blanca	Grid M5 Rocket Ti	Mtk	Mtk	10.0.3.1	x			1500			x	7700	48,2
					x			256	256		x	9700	
						x	5			x	x	5300 / 4100	
Cruz de Amarillo	Grid M5	Mtk	Mtk	10.0.1.1	x					x	X	4600 / 2750	11,1
Crater	HT Plus	Mtk	Mtk	10.0.1.1	x			256	256	x		75,5	11.3
						x	5			x		39,3	
Bruma					x			256	256	x		60.5	11,1
Incli Crater					x			256	256	x		66.3	10,6
										x			
Cufiño	HT Plus	Mtk	Mtk	10.0.1.1	x			256	256	X		99,2	10
						x	5			x		71,6	
Morasurco-2	HT Plus	Mtk	Mtk	10.0.1.1	x			256		x		145,1	3,9
						x				x		145,4	
Mocondino					x			1500	1500	x	x	2670 / 1540	1,7
San José					x			1500		x	x	3540 / 2850	7.9

Tabla 3.6. Resultados de pruebas de capacidad de transmisión en los enlaces troncales.

3.2 Diseño Lógico

3.2.1 Diseñar Direccionamiento y Nombramiento

Actualmente en el Observatorio de Pasto, se tiene configuradas varias redes pertenecientes al proceso de adquisición, transporte, proceso y almacenamiento de datos. Para la red de Telemetría se utilizan dos redes o dominios de *Broadcast* (10.0.1.0/24 y 10.0.3.0/24), para los equipos de adquisición se utiliza la red 10.0.100.0/24 y para los demás servicios de red del Observatorio, se usa la red 192.168.9.0/24 con acceso a la WAN institucional y a la red pública de internet.

En la figura 3.15, se ilustra el esquema de conectividad actual tanto a nivel físico como lógico en la red de telemetría y la red de datos del OVSP.

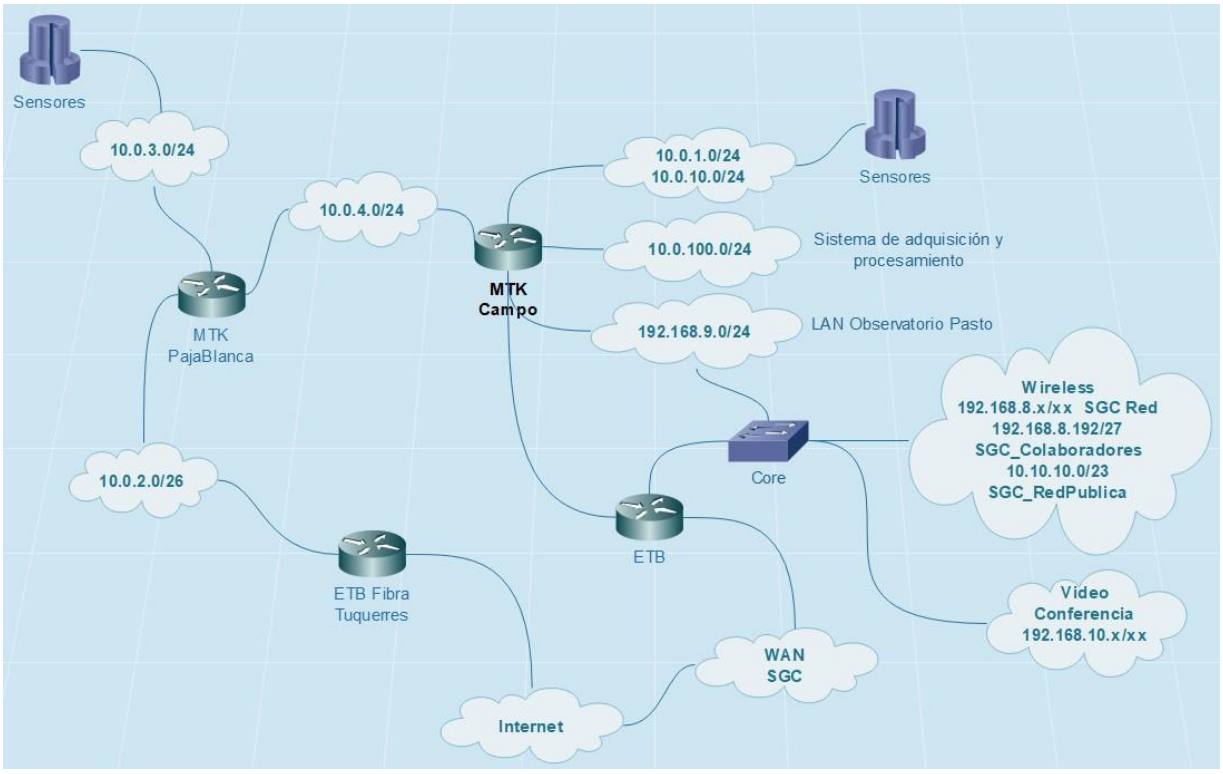

Figura 3.15. Esquema red actual LAN14, WWAN15 y WAN16 en el OVSP

[14] LAN (*Local Area Network*) Red de área local
[15] WWAN (*Wireless Wide Area Network*) Red inalámbrica de área amplia
[16] WAN (*Wide Area Network en inglés*) Red de área amplia

Direccionamiento de red

Basados en la topología de la red de telemetría, se cuenta con 8 troncales y conexiones de redes individuales, cada una con una red clase C independiente unidas a través del área núcleo en la cual están los enrutadores del área *backbone*, en la tabla 3.7, se lista el direccionamiento para cada troncal.

Troncal	Nombre	Direccionamiento IPv4
1	San José	192.168.1.0/27 192.168.1.32/27 192.168.1.64/27 192.168.1.96/27 192.168.1.128/27
2	Cruz de Amarillo	192.168.2.0/24
3	Crater	192.168.3.0/24
4	Bruma	192.168.4.0/24
5	Incli-Crater	192.168.5.0/24
6	Cufiño	192.168.6.0/24
7	Morasurco-2	192.168.7.0/24
8	Mocondino	192.168.8.0/24
9	Redes individuales	192.168.9.0/24

Tabla 3.7. Direccionamiento IPv4 troncales

Los enlaces troncales llegan al Observatorio y se conecta a una interfaz del núcleo que básicamente es el área *Backbone* de enrutamiento, para el caso de las redes individuales consideradas como no troncales, llegan primero a un switch y luego se conectan a una interfaz de un enrutador.

Diseño de la topología de red

En el presente proyecto, se parte de la topología de red actual y que se ilustra en la figura 3.4. Distribución física de repetidoras en el OVSP en donde se identifica redes y puntos de interconexión, tamaño y alcance.

Después de un análisis de los requerimientos y en base a la infraestructura actual se definió un sistema de red que hace uso principalmente de la red existente considerando cuatro áreas principales como son: Núcleo (*Backbone*), Transporte, Distribución y Acceso, enmarcados en los conceptos de seguridad y calidad de servicio.

El núcleo, corresponde a todos los equipos instalados en el Observatorio, tales como switches y un enrutador principal que conecta todas las redes, principalmente las troncales. Adicionalmente en esta área se conecta también la red LAN del Observatorio y los servicios asociados a la red WAN del instituto.

El nivel de transporte, hace referencia a las conexiones entre el núcleo y repetidoras y entre repetidoras, es decir una topología en malla con conexiones redundantes entre sí.

El nivel de distribución, saldría de la red troncal que para el presente diseño es el dominio MPLS y consta de repetidoras secundarias y equipos de conexión final a los sensores. Dependiendo de la importancia de los nodos que se ubiquen en este nivel, se considera tener un enlace de respaldo hacia el nivel de transporte.

Finalmente, el nivel de acceso, es el último elemento en la red en el cual se conectan directamente los sensores, usualmente el sitio en donde se ubica físicamente tienen condiciones adversas del clima, es de difícil acceso y más distante del Observatorio.

Desde el nivel de transporte hasta el nivel de acceso, se considera la posibilidad de tener un acceso redundante a través de un prestador de servicios de Internet (ISP, *Internet Service Provider*) con el objetivo de tener acceso remoto al sitio y transportar datos de sensores de ser necesario. Mantener acceso remoto a cada sitio, posibilita realizar reinicio de equipos y cambiar algunos parámetros de conectividad, así como también transportar datos de sensores que se consideren primarios para la vigilancia y monitoreo de volcanes.

En la figura 3.16, se ilustra el resumen de la distribución física de las repetidoras y equipos finales.

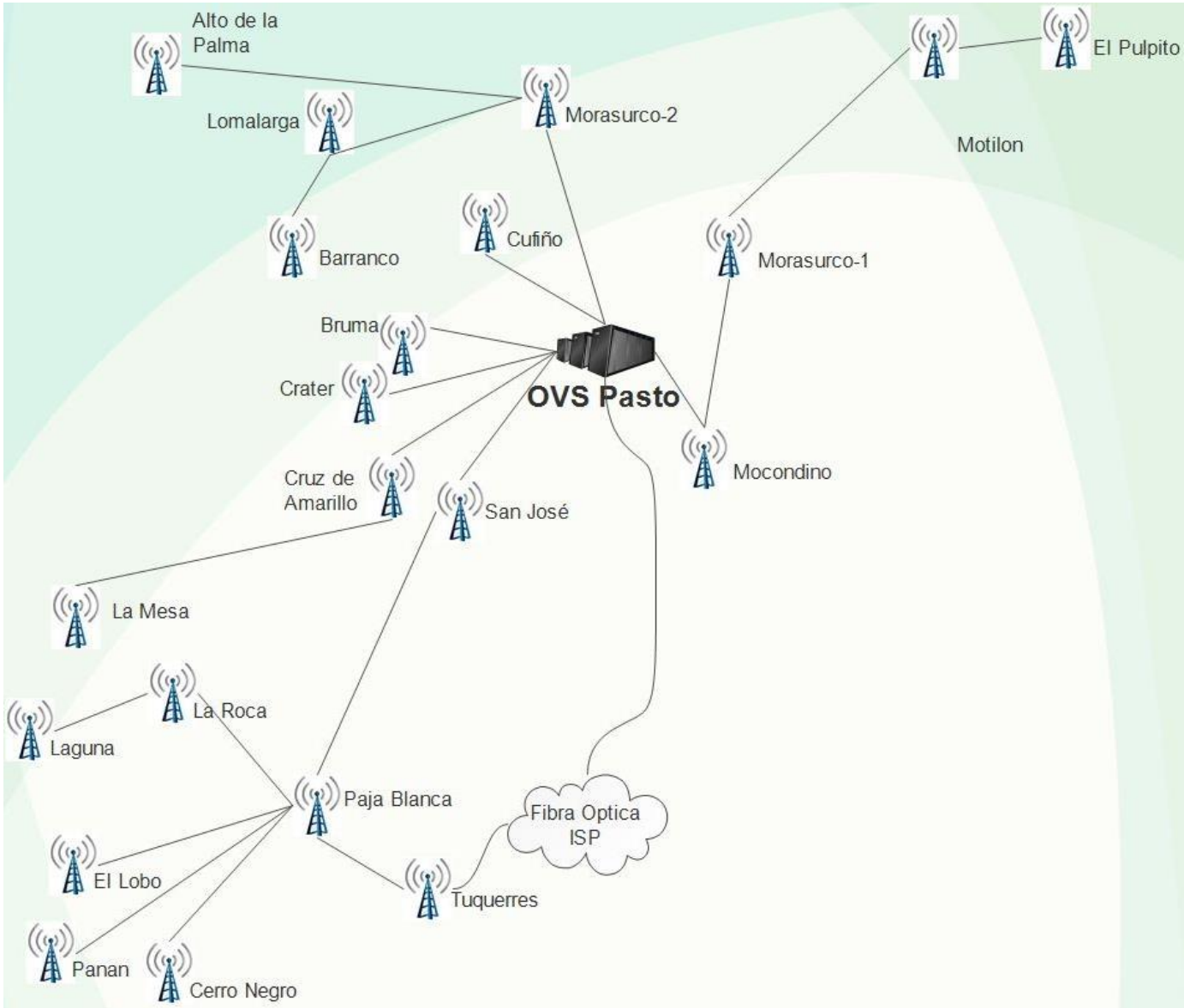

Figura 3.16. Distribución física de red

3.2.2 Seleccionar métodos *Switching* y Protocolos de Routing

En todos los niveles de la red de telemetría, se utiliza la tecnología *Ethernet*, los switches ubicados en las repetidoras principales y secundarias, tienen interfaces a 10/100/1000 así como también los equipos de conexión inalámbrica punto a punto en los que se tiene habilitado el sistema de distribución inalámbrico (WDS, *Wireless Distribution System*) en modo de puente transparente.

Considerando que el diseño de la red se basa en la tecnología MPLS, en todo el dominio (nivel núcleo y transporte) debe haber conectividad a nivel de IP, el proyecto se diseñó utilizando un protocolo de enrutamiento dinámico de estado de enlace OSPF con un área principal y varias áreas dependiendo del número de troncales (actualmente 10 áreas).

3.2.3 Requerimientos mínimos de seguridad y mecanismos de control

La seguridad es un proceso continuo y los administradores de red deben tener en cuenta muchos aspectos desde la capa física hasta la capa de aplicaciones. Teniendo como referencia el modelo OSI.

En el presente trabajo, se consideraron los requerimientos propios del proceso de monitoreo volcánico y funcionalidad de la red con el fin de no degradar el rendimiento de puntos críticos, inicialmente se consideró actualizar a la última versión estable del firmware de los equipos de comunicación y adicionalmente para la capa 2 se diseñó lo siguientes controles dependiendo del ataque, listados en la tabla 3.8:

Ataque	**Control**
CAM Table Overflow	En switches del nivel de core y distribución se debe configurar el bloqueo de puerto si supera un número finito de entradas en la tabla. No se tiene DHCP en ningún segmento de red Para equipos Mikrotik, se habilita la opción External FDB
ARP Spoofing	En switches del nivel de core y distribución se debe configurar se debe configurar el filtrado de paquetes, únicamente permitiendo paquetes IP de las redes conocidas. En equipos Mikrotik, se debe deshabilitar la opción MNDP Descartar tramas que no sean Ethernet
SYN *Flood*	En LANs, se podría instalar programas para la detección de este ataque, el programa puede ser SYN Cookies
ICMP *Flood*	Implementar ACL para controlar el ancho de banda
DHCP Starvation	DHCP con reservación, Considerar utilizar un servicio de *Radius*
VLAN Hopping Attack	En equipos Mikrotik, se debe bloquear el MAC Protocolo 8100 en todas las puertas de entrada de la red
STP Flooding	Para equipos Mikotik, se debe filtrar selectivamente los mensajes de STP por los clasificadores (BPDU o tcn BPDU)

Tabla 3.8. Ataques de seguridad y control asociado

La exposición de una red a ataques es muy grande y de difícil control, más aún cuando se tiene acceso físico a ella y los potenciales ataques de negación de servicio son en su mayoría afectando de manera directa la continuidad del servicio.

3.2.4 Proponer calidad de servicio y clase de servicio (QoS y CoS)

Antes de proceder a implementar medidas de QoS y CoS, se identificó el tráfico y los sistemas asociados a este, se definió 5 niveles de prioridad en donde 1 es el más importante y 7, no tiene prioridad. En la tabla 3.9 se determina el escenario para la prioridad y la precedencia asociada a los tipos de tráfico.

		Precedencia					
Nivel de Actividad volcán	Estación Sísmica base clasificación	Estación Sísmica base clasificación Alternativa	Estaciones Sísmicas	Acelerómetros	Acústicos	Inclinómetros	Baja tasa de muestreo
	Cámara seleccionada	GNSS	Navegación web				
Otros volcanes	Estaciones sísmicas principales otros volcanes	Baja tasa de muestreo	Otras estaciones Sísmicas	GNSS	Otras Cámaras	Sin prelación	

Tabla 3.9. Niveles de prioridad

Una vez definidos los dos escenarios que dependen del nivel de actividad de un volcán o volcanes, se determina la precedencia para el flujo de datos, resultando de esta manera 18 niveles de prioridad en la que el nivel 1 es el más importante y el nivel 18 sin prioridad.

3.2.5 Proponer mecanismos de Tolerancia a fallos (*Failover*)

Con base en la figura 3.15 (Esquema red actual LAN, WWAN y WAN en el OVSP), se determinó enlaces redundantes entre las repetidoras y el punto central de la red, estos enlaces se realizan en capa 2, utilizando el protocolo de árbol de expansión (STP, *Spanning Tree Protocol*) o el protocolo rápido (RSTP, *Rapid Spanning Tree Protocol*) y debidamente configurados en el switch correspondiente. De esta manera quedaría con un soporte de tolerancia de fallo entre el punto central de la red y cada repetidora.

Adicionalmente, en capa 3, a través del protocolo de enrutamiento OSPF, se determinan varios caminos desde cada repetidora hasta al punto central, trazando conexiones entre repetidoras creando una red tipo malla.

En los casos en los que esté disponible una conexión adicional contratada con un ISP, se tendría acceso a través de una VPN desde la estación hasta la red WAN del instituto. Tal como se ilustra en la figura 3.15.

3.2.6 Diseñar la Red

El dominio MPLS está dividido en 9 áreas de OSPF, en donde el área 0 pertenece al núcleo de la red, cada área desde A1 hasta A8 está asociada a una repetidora, el enrutador R9 concentra datos de las estaciones individuales.

Las áreas de A1 hasta A9, tienen enlaces redundantes en capa 2 hasta la repetidora secundaria, estos enlaces inician y terminan en switches en los que está configurado el protocolo RSTP en el cual el peso de cada puerto depende de la capacidad de cada enlace. En la figura 3.17, se muestra la distribución física, las áreas para OSPF y el diseño de la red de telemetría basada en MPLS. En el simulador GNS3 [28] se incluyó solo 4 de las 8 troncales existentes (figura 3.18) debido a que la herramienta demanda grandes prestaciones de cómputo y emular la totalidad de la red degrada el rendimiento del equipo.

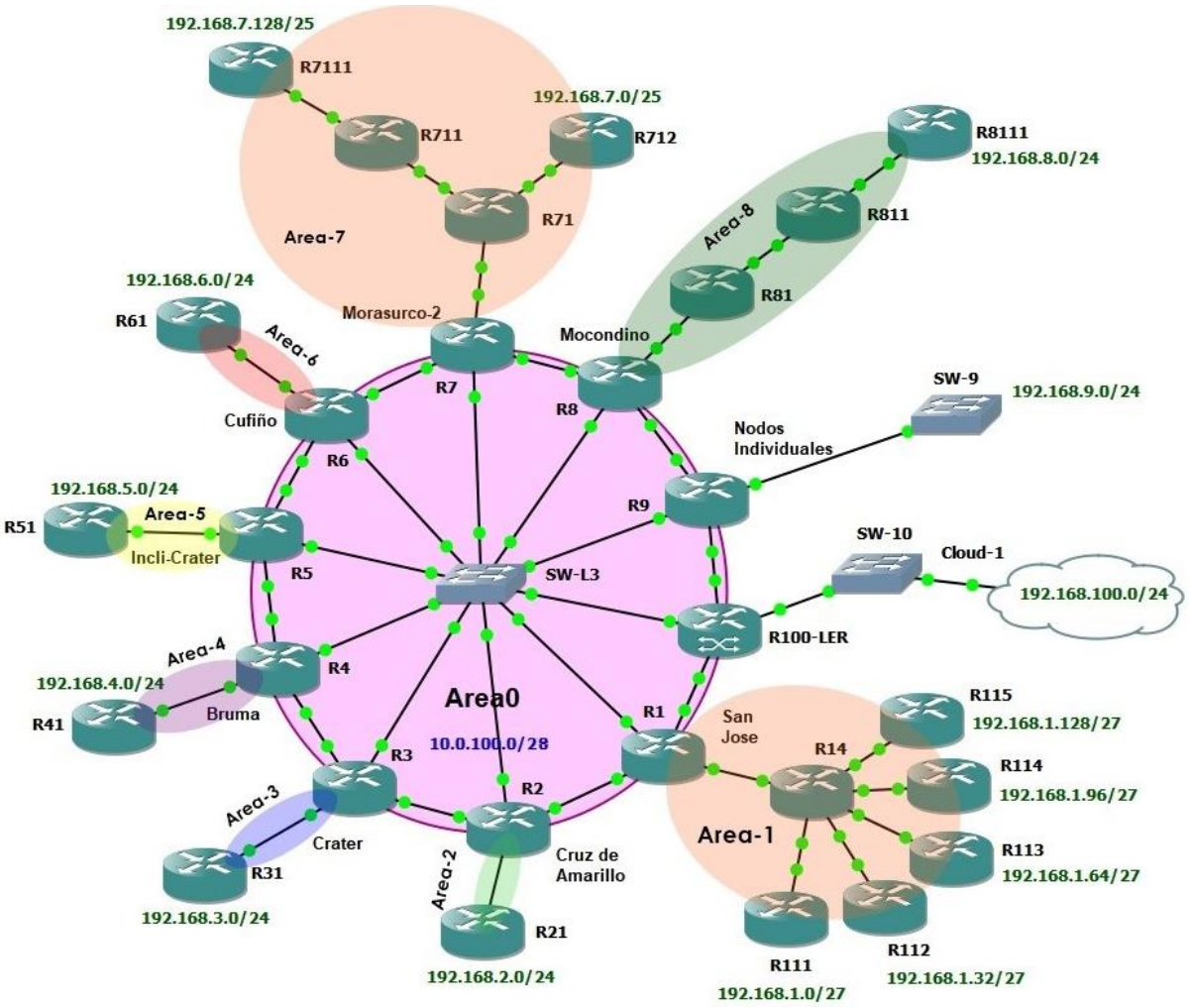

Figura 3.17. Diseño de red MPLS

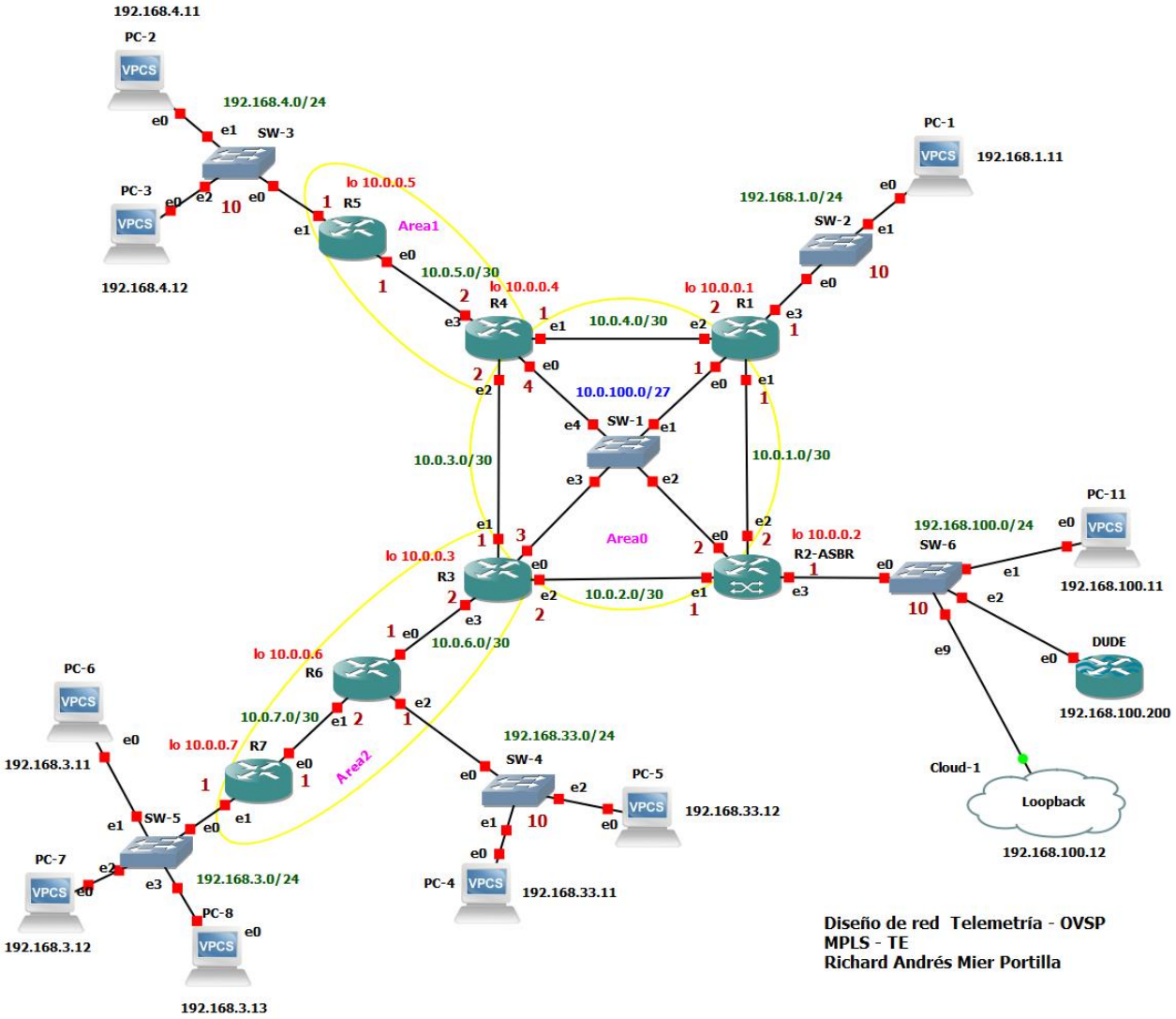

Figura 3.18. Diseño de red MPLS-TE para emulación con GNS3

3.3 Diseño de MPLS-TE

3.3.1 Definición de recursos en interfaces

La naturaleza heterogénea en los dispositivos de comunicación de las redes de telemetría del SGC, sumado a un contexto de transporte de datos inalámbrico, implica variación de las capacidades en cada tramo, esto dificulta la definición de un recurso por interfaz, en este caso y para efectos del diseño, se consideró una capacidad asociada a un mínimo calculado dependiendo de los equipos, las condiciones de instalación, clima y demás factores que afectan la comunicación.

El túnel TE se puede configurar para limitar la velocidad a la que el tráfico puede ingresar al túnel, esta configuración se realiza directamente en la interface asociada con la red MPLS. Para enlaces troncales, se estima velocidades entre 1 Mbps y 10 Mbps, con relación a enlaces de sub troncal, desde 128 hasta 512 Kbps y para enlaces de punto final desde 32 hasta 128 Kbps.

3.3.2 Definición de caminos (*Path*)

La red de Telemetría del Observatorio Pasto está conformada estructuralmente por repetidoras troncales, repetidoras secundarias y puntos finales, tal como se detalla en la tabla 3.3, para el caso práctico de la simulación del diseño implementado en GNS3, se definieron únicamente 4 de las 10 repetidoras troncales, la arquitectura es equivalente para cada troncal independiente del número. A continuación, se listan las recomendaciones para la asignación de caminos del dominio MPLS-TE desde y hacia cada punto final.

- Camino primario, es el enlace de mayor estabilidad, así como también el de mayores prestaciones en comunicación tanto en capacidad como en latencia. Para el Observatorio Pasto, se definió los enlaces con equipos Ubiquiti de preferencia con la tecnología *AirMax AC*. Por otra parte, se debe elegir el enlace que vaya de manera directa al LER, es decir el equipo enrutador que está conectado a la red LAN del sistema de adquisición y procesamiento.
- Camino secundario 1: se asigna al enlace que va desde el punto hasta el enrutador LER pasando por el switch del área 0.

- Camino secundario 2: se asigna al enlace que va desde el punto hasta el enrutador LER pasando por el lado derecho del anillo de repetidoras sin pasar por el switch del área 0.
- Camino secundario 3: se asigna al enlace que va desde el punto hasta el enrutador LER pasando por el lado izquierdo del anillo de repetidoras sin pasar por el switch del área 0.

En la figura 3.19, se indica la ruta principal y las rutas secundaria para el envío de datos desde un punto final de MPLS (LER de entrada) y el LER de salida que tiene acceso a la LAN de adquisición de datos; con respecto al camino de retorno, el principal cubre la misma ruta de envío principal y el camino o caminos secundarios se deja el control al protocolo OSFP.

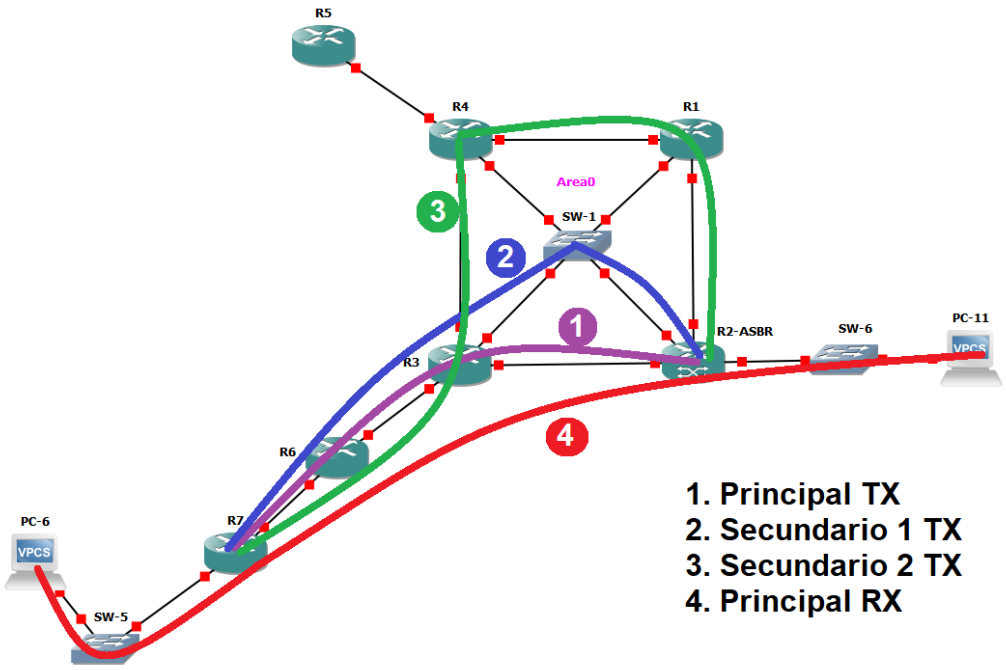

Figura 3.19. Diseño de caminos principal y secundarios

3.3.3 Definición de recursos en el túnel (reserva)

La red de telemetría del Observatorio Pasto, como es común en una red de sensores utilizados para la vigilancia y monitoreo volcánico, el tráfico en la red no es constante y varía en cada tramo, esto dependiendo de la actividad en la zona de influencia volcánica, sin embargo, de acuerdo a los datos consignados en la tabla 3.1 Aplicaciones, se define la capacidad mínima requerida por cada estación y se hace la

reserva adecuada según la prioridad de los datos definida también en la Tabla 3.9. Niveles de prioridad.

Adicionalmente si se considera un entorno de conectividad inalámbrico, para definir la capacidad total del túnel, se debe cumplir con las recomendaciones dadas en el capítulo 5, numeral 5.1 Conclusiones.

La repetidora secundaria El Pulpito, ubicada al norte del departamento de Nariño concentra señales de 5 estaciones pertenecientes a los volcanes Las Animas y Doña Juana, en la figura 3.20, se ilustra la distribución de los equipos pertenecientes a la repetidora troncal Mocondino cuyo punto final es la repetidora secundaria El Pulpito.

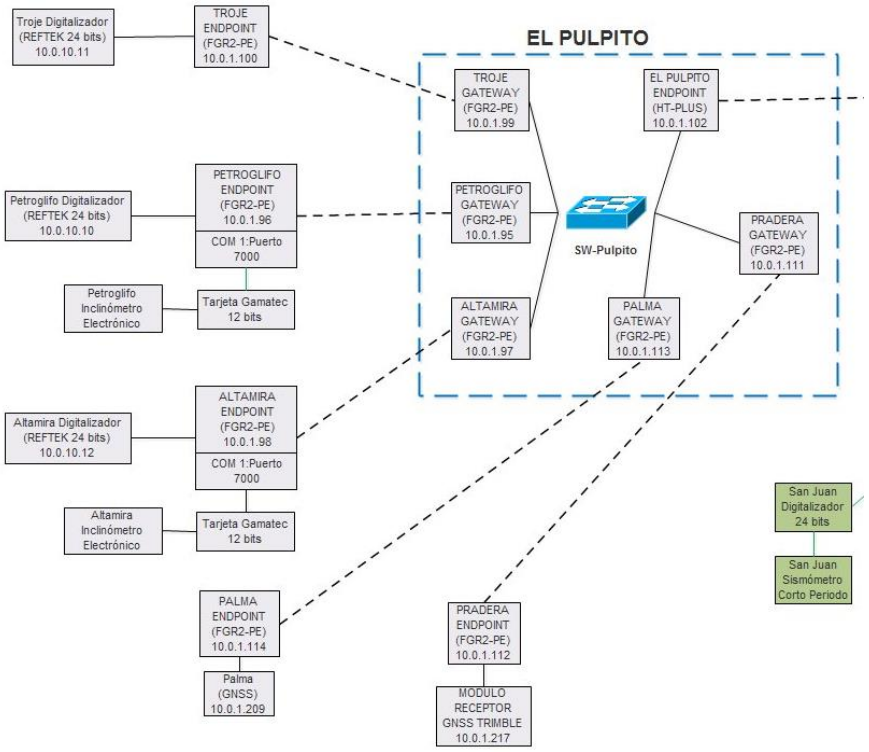

Figura 3.20. Equipos de comunicación y sensores en la repetidora secundaria El Pulpito

Los recursos en conectividad para las estaciones de la repetidora secundaria El Pulpito, dependen de la prioridad en la actividad del volcán, como ejemplo se reserva capacidad de transmisión para las estaciones asociadas el volcán Las Ánimas, en la tabla 3.10, se consignan los valores en Kbps para cada estación y se organizan de acuerdo a la precedencia. El valor total necesario calculado para esta repetidora es de 132 Kbps.

Prioridad	Reserva en Kbps	Descripción
1	24	Estación sísmica base clasificación – Petroglifo
2	24	Estación sísmica base clasificación alternativa – Altamira
3	24	Estaciones sísmicas volcán - Troje
4		
5		
6	2	Inclinómetros volcán - Petroglifo
	2	Inclinómetros volcán - Altamira
7		
8		
9	24	GNSS volcán - Pradera
10	8	Navegación web volcán 10
11		
12		
13		
14	24	GNSS – La Palma
15		
16		Sin prelación

Tabla 3.10. Reserva de recursos para el volcán Las Ánimas

3.3.4 Definición de ruteo

En *MPLS-TE* al definir un túnel y sus recursos, de manera intrínseca se crea una interfaz virtual, a la cual se puede asignar una dirección IP y reglas de enrutamiento estático. En este sentido podemos direccionar el tráfico de toda una red, una dirección IP o puerto específico a una interfaz de *TE* con un destino en particular. Como en el presente trabajo se consideran varias rutas para dar soporte de *Failover*, fue necesario crear una regla de enrutamiento por cada *Path*, adicionalmente optimizar el intervalo de muestreo para reducir el tiempo de cambio entre una ruta y otra (En equipos Mikrotik: `reoptimize-interval=5s`).

En la repetidora secundaria El Pulpito, se debe crear 8 túneles por cada *Path* para el envío de datos y desde el Observatorio Pasto, un túnel de regreso hacia la repetidora, cada túnel deber tener una dirección IP, un *Gateway* y una regla de ruteo.

3.4 Diseño Físico

3.4.1 Diseñar enlaces inalámbricos de largo alcance (WWAN, *Wireless Wide Area Network*)

Para el diseño de enlaces inalámbricos, se tuvo en cuenta el requerimiento mínimo de capacidad de transferencia de cada enlace asociado con la cantidad y tipo de estaciones que van a generar tráfico. En la tabla 3.11, se especifica la capacidad requerida por cada enlace troncal y repetidoras secundarias calculada a partir de los equipos sensores instalados.

Troncal / Repetidora secundaria	Nombre	Capacidad mínima requerida (Kbps) Actividad normal	Capacidad diseñada (Kbps 50 % +)
1	**Paja Blanca**	**475**	**720**
2	**Cruz de Amarillo**	**480**	**720**
3	**Crater**	**125**	**190**
4	**Bruma**	**200**	**300**
5	**Incli-Crater**	**120**	**180**
6	**Cufiño**	**144**	**220**
7	**Morasurco-2**	**235**	**350**
8	**Mocondino**	**320**	**480**
9	Morasurco 1	200	300
10	Motilon	145	220
11	El Pulpito	145	220
12	El Lobo	85	130
13	Cerro Negro	165	250
14	Calera	30	45
15	La Roca	170	255
16	Laguna	100	150
17	Mesa	105	155
18	Loma Larga	145	220
19	Alto de la Palma	30	45
20	Redes individuales	200	300

Tabla 3.11. Requerimiento de capacidad de transmisión

En la figura 3.21 se observa la capacidad de transmisión en Mbps utilizada en la repetidora Cruz de Amarillo durante un evento sísmico relativamente pequeño, en el gráfico se observan valores que equivalen al promedio de la capacidad utilizada en Mbps (Rx/Tx) cada 5 segundos.

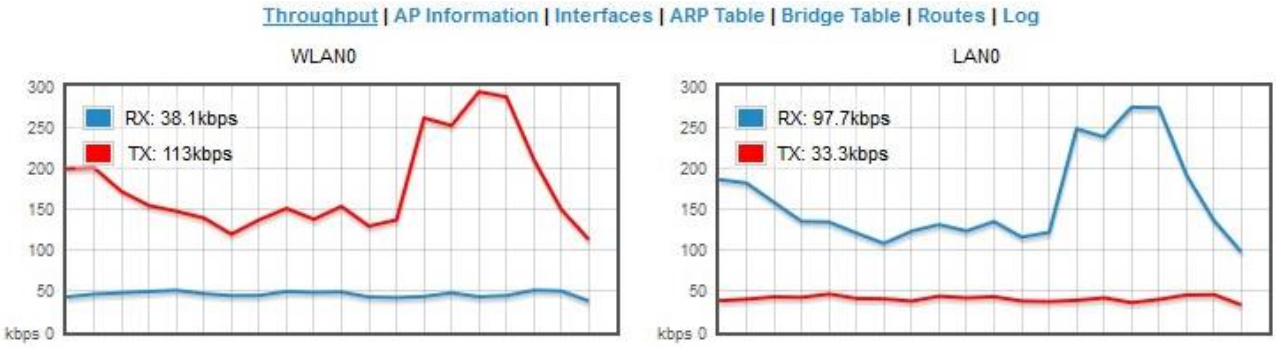

Figura 3.21. Capacidad utilizada en la repetidora Cruz de Amarillo durante un evento sísmico

Adicionalmente para garantizar la capacidad de transmisión diseñada en los enlaces inalámbricos debe considerar:

- Nivel de señal ruido superior a 25 dBm
- Se debe dejar de 10 a 15 dBm de guarda en el nivel de señal para soportar condiciones anómalas que puedan degradar la conexión.
- Ajustar los parámetros inalámbricos necesarios para cumplir con las normas actuales en relación a comunicaciones de Radio Frecuencia.
- En los casos en los que no se requiere una capacidad mayor a 1 Mbps y haciendo uso de comunicaciones basadas en IEEE 802.11b, se recomienda usar espectro ensanchado por secuencia directa (DSSS, *Direct Sequence Spread Spectrum*), para lograr mayor alcance y estabilidad del enlace.

3.4.2 Tecnologías utilizadas en WWAN

La red de área extensa (WWAN, *Wireless Wide Area Network*) se considera como los enlaces inalámbricos de troncales, repetidoras principales y secundarias, que van desde 7 a 45 Km, estos enlaces se diseñaron con equipos que utilizan frecuencias en bandas libres como la de 2.4 y 5 GHz, utilizando protocolos:

- IEEE 802.11 b, especialmente DSSS
- IEEE 802.11 n
- IEEE 802.11 AC

Los enlaces inalámbricos que llegan a los equipos finales, se diseñaron con equipos de menor capacidad de transmisión, aunque con mayor protección para soportar condiciones climáticas adversas, se utiliza la banda libre de 900 MHz y la tecnología FHSS.

3.4.3 Dispositivos de interconexión

Selección de Tecnologías

En este aparte, adicionalmente a las tecnologías WWAN listadas anteriormente, se hace referencia a los dispositivos utilizados para la interconexión en capa 2 y 3. En capa dos, una vez resuelto el enlace WWAN, se usa el protocolo STP y RSTP para dar redundancia a la conexión y soportar un fallo. En el sitio de las repetidoras principales y algunas secundarias, adicionalmente se instala un acceso a la red móvil celular 3G a través de un Modem conectado a través del puerto USB de un enrutador.

Para la capa 3, el principal componente es el enrutador, éste dispositivo debe tener la capacidad de utilizar el protocolo de enrutamiento OSFP, soportar la tecnología MPLS. En el área A0 (núcleo de la red), los enrutadores deben tener como mínimo 12 interfaces Ethernet.

Dispositivos

En la tabla 3.12, se listan los dispositivos utilizados en el diseño, adicionalmente después de realizar una consulta al área encargada en el Observatorio Pasto sobre la disponibilidad de los equipos se presenta la disponibilidad o no del equipo y un valor aproximado en dólares.

Dispositivo	Marca - Modelo	Capacidad - Detalle	Disponibilidad almacén SGC	Costo aproximado (Dólares - U$)
Radio antena	Ubiquiti [29] PBE-5AC-ISO-Gen2	5 GHz 450+ Mbps 25+ km	No	200
Radio	Ubiquiti RP-5AC-Gen2	Full-Band 5 GHz 500+ Mbps (Max. 80 MHz) (1) 10/100/1000 Ethernet Port	No	500
Antena	Ubiquiti airMAX ac 2x2 PtP Bridge Dish Antenna	30 Dbi	No	175
Radio antena	Ubiquiti PBE-5AC-500-ISO	5 GHz 450+ Mbps 25+ km	No	150
Switch	Sixnet® SLX Managed Ethernet Switches	5 y 8 puertos	No	500
Switch	HP	48 puertos administrable	Si	3000
Enrutador	Mikrotik RB2011UiAS-IN	Desktop metal case, 5xEthernet, 5xGigabit Ethernet, USB, LCD, PoE	No	170

		out on port 10, 600MHz CPU, 128MB RAM, RouterOS L5		
Enrutador	Mikrotik RB1100AHx4	Powerful 1U rackmount router with 13x Gigabit Ethernet ports	No	350
Enrutador	Mikrotik RB1100AHx4 Dude Edition	Powerful 1U rackmount router with 13x Gigabit Ethernet ports, 60GB M.2 drive for Dude database	No	400
Enrutador	Mikrotik hEXPoE	5x Gigabit Ethernet with PoE output for four ports, SFP, USB, 800MHz CPU, 128MB RAM, RouterOS L4	Si	100
Modem	huawei e303	USB 3G	Si	20

Tabla 3.12. Dispositivos utilizados en el diseño

Seguridad Física

La seguridad física, tiene dos elementos, el primero es la protección contra intrusiones o vulneración de puertas, cerrojos entre otros elementos necesarios para mantener aislado los equipos electrónicos, en este caso, el Observatorio Pasto, tiene un estándar para la construcción de sistemas de protección, en la figura 3.22, se muestra un ejemplo de una de las estaciones en intemperie y en la figura 3.23, una imagen de una repetidora.

Figura 3.22. Sistema de protección de una estación en intemperie

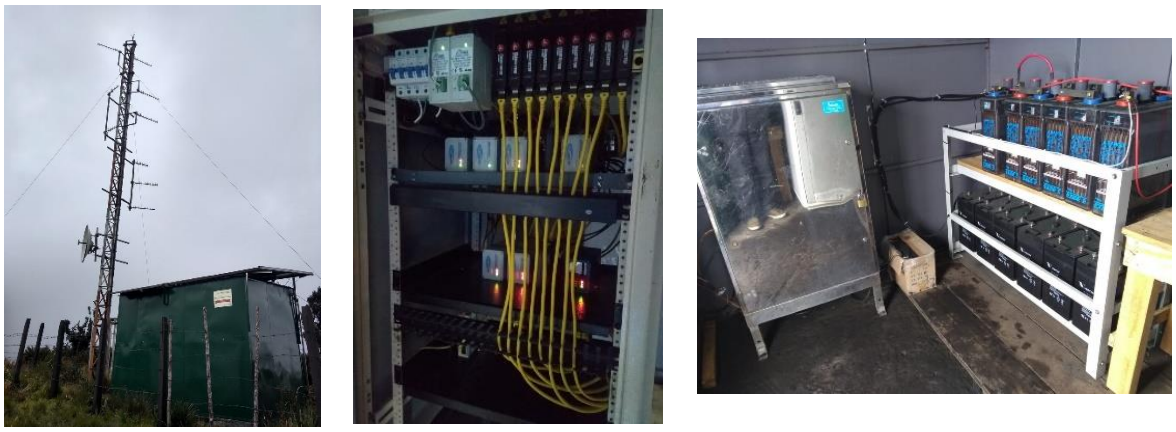

Figura 3.23. Caseta o cuarto de equipos en repetidoras

El segundo elemento en los sistemas de seguridad física es la monitorización y notificación de intrusiones, para el presente proyecto, se diseñó un sistema de notificación basado en elementos de Internet de las cosas (IoT, *Internet of Things*) el cual envía un mensaje al presentarse una novedad con la apertura de puertas. El sistema tiene tres componentes, el primero es el sensor, el cual se compone de dos contactares magnéticos, normalmente abiertos o normalmente cerrados según sea el caso y las baterías junto con la electrónica administradora del sensor. El segundo componente es la red de transmisión de datos, en este caso se utilizó la red de IoT con más despliegue en el mundo que es *SIGFOX*. El tercer componente es el sistema computacional encargado de recibir, procesar y notificar al usuario, en el proyecto se utilizó la plataforma de *Ubidots*[17] para recibir los datos y programar las notificaciones. En la figura 3.24, se ilustra el sistema diseñado.

[17] Ubidots: sistema integrador equipos y aplicaciones para Internet de las cosas, desplegando una serie de herramientas de recolección, análisis, despliegue de datos y ejecución de acciones, sistema disponible en https://ubidots.com

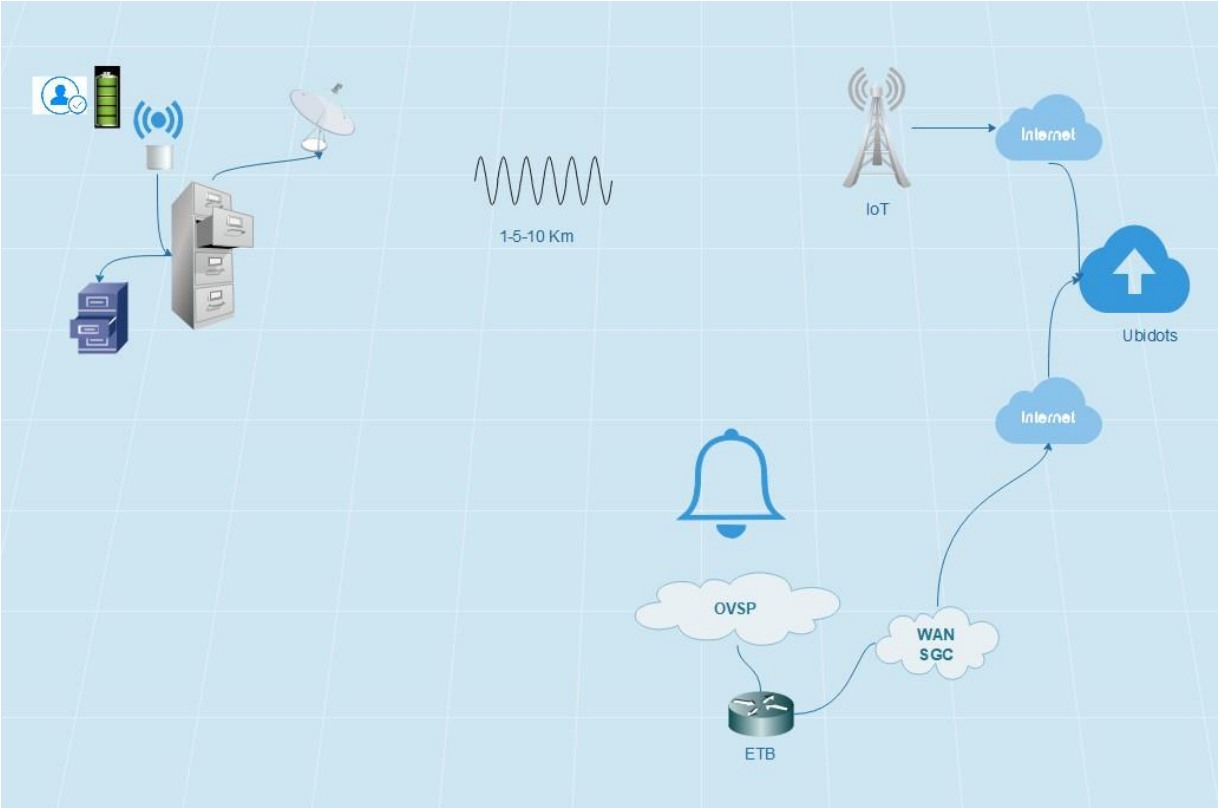

Figura 3.24. Sistema de alerta de Intrusiones físicas a estaciones

Capítulo 4

4. PRUEBAS Y DOCUMENTACIÓN

Pruebas e implementación virtual de la red MPLS-TE

Este capítulo desarrolla la definición del plan de pruebas, la selección de dispositivos, la configuración de equipos y la obtención de resultados a partir de la simulación de la red en la aplicación GNS3.

4.1 Definición del plan de pruebas

Teniendo en cuenta el diseño realizado, se presenta el plan de pruebas que permitió verificar el cumplimiento de los requerimientos del trabajo de grado, con el fin de garantizar la correcta implementación para mejorar la disponibilidad del servicio de comunicación de la red de Telemetría, los datos que serán suministrados al personal encargado del área de Telemetría del SGC.

El diseño de la red de Telemetría se validó mediante la evaluación de varios parámetros de conectividad definidos por el Protocolo de control de mensajes de Internet (ICMP, *Internet Control Message Protocol*), utilizando la aplicación PING desde varios equipos en los extremos hasta un equipo definido como servidor de adquisición y con los parámetros del comando *ping* como: número de intentos *–n <300>*, es decir, una prueba durante 5 minutos y tamaño del búfer definido en *bytes –l <1-1000>*, por limitación de la licencia usada de GNS3, este parámetro tiene un límite de 1000, que representa un *Throughput* de 8 Kbps para cada flujo. Al final se evalúa la disponibilidad dependiendo de los valores relacionados con el porcentaje de paquetes perdidos y la latencia.

Este plan se realizará a través de cuatro pruebas desde distintos puntos de vista, que generarán información de validación de la red; las pruebas se realizarán sobre la arquitectura montada en el emulador que se muestra en la figura 3.17, y a la integración de todos los dispositivos al tiempo. A continuación, se listan los cuatro escenarios:

a) Pruebas de dispositivos
b) Pruebas de conectividad
c) Pruebas de *Failover*
d) Pruebas de saturación de tráfico

4.1.1 Ambiente de pruebas

Se creó un ambiente que permite realizar pruebas a los diferentes componentes del sistema establecidos en el diseño, el espacio es un laboratorio virtual para probar enlaces, dispositivos y su integración.

4.1.2 Recursos

Para el presente proyecto, se utilizó el programa GNS3 [28] en la versión 2.1.12, equipos Mikrotik con *RouterOS* versión 6.43.8 para desarrollar un ambiente de pruebas, un equipo portátil con sistema operativo Windows 10, procesador Intel Core i5 y 8 GB de memoria RAM.

GNS3

GNS3 es utilizado por ingenieros de redes en todo el mundo para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar desde una pequeña topología en un equipo portátil, hasta aquellas que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube.

GNS3 ha permitido a los ingenieros de redes virtualizar dispositivos de hardware reales. Originalmente solo emulando dispositivos Cisco utilizando un software llamado *Dynamips*, GNS3 ahora ha evolucionado y es compatible con muchos dispositivos de

múltiples proveedores de red, incluidos los switches virtuales de Cisco, los ASA de Cisco, los vRouters de Brocade, los switches Cumulus Linux, las instancias de Docker, los VSR de HPE, los múltiples dispositivos Linux, equipos Mikrotik y muchos otros los cuales se pueden descargar desde el sitio web [2].

Recursos computacionales recomendados

En la tabla 4.1 se listan los recursos mínimos necesarios para que la aplicación GNS3 opere de manera adecuada, si el diseño incorpora muchos elementos, las prestaciones deben ser proporcionales a la cantidad de equipos tanto en memoria RAM como en procesador. Para esto se debe tener en cuenta la hoja de datos del equipo Emulado.

Procesador	2 o más núcleos lógicos
Virtualización	Extensiones de virtualización requeridas. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	4 GB de RAM
Almacenamiento	1 GB de espacio disponible (la instalación de Windows es <200MB).
Notas adicionales	Es posible que necesite almacenamiento adicional para su sistema operativo y las imágenes del dispositivo.

Tabla 4.1. Recursos computacionales recomendados

Recomendaciones iniciales

El equipo en el cual se vaya a instalar GNS3, se recomienda:

a) Ejecutarlo con privilegios de administración
b) Desactivar Firewall del sistema operativo
c) Desactivar Antivirus
d) El equipo no debe pertenecer a un dominio de *Directorio Activo*

Configuración básica

En este proyecto se utilizó equipos Mikrotik para el desarrollo de pruebas, fue necesario descargar e incluir en GNS3 el componente *MikroTik CHR appliance*, que es una versión de *RouterOS* diseñada para ejecutarse como una máquina virtual. Es compatible con la arquitectura x86 de 64 bits y se puede usar en la mayoría de los hipervisores populares como VMWare, Hyper-V, VirtualBox, KVM y otros. El enrutador

virtual (CHR, *Cloud Hosted Router*) tiene características completas de *RouterOS* habilitadas de manera predeterminada, pero tiene un modelo de licencia diferente al de otras versiones de *RouterOS*. (Tráfico por interfaz limitado a 1 Mbps), de manera práctica en GNS3 se ingresa al menú *Edit*, se selecciona *Preferences*, del menú izquierdo *QEMU* (*Quick EMUlator*), se selecciona *QemuVMs, New* y finalmente se ingresa la ruta del archivo con extensión de tipo img (chr-6.43.8.img [2]).

Para los equipos Mikrotik en GNS3, es necesario adicionarles interfaces, por defecto solo tiene habilitado una, para ello se requiere seleccionar el dispositivo, menú *Node,* opción *Configure*, luego en la pestaña *Network*, el atributo *Adapters*, se ingresa el número de interfaces que se requiera, para el proyecto, se definió 5 interfaces para todos los enrutadores.

4.2 Plan de pruebas

El plan de pruebas se realiza conforme a los requerimientos establecidos previamente en el numeral 4.1.

4.2.1 Pruebas de dispositivos

- Se realiza un encendido y apagado de cada enrutador, se verifica interfaces y configuración básica a través de la herramienta Winbox.
- Se realiza un encendido y apagado de cada equipo de cómputo virtual simulado (VPCS, *Virtual PC Simulator*)

En GNS3, se indica a través de un círculo de color verde o rojo en la salida de cada interfaz de los dispositivos, indicando que el equipo está disponible.

Con esta prueba se verificará que es posible obtener de los dispositivos datos consistentes, disponibilidad de acceso, y que el registro de tiempo está acorde con el tiempo real.

4.2.2 Pruebas de conectividad

En estas pruebas se verificó la conexión entre equipos y la transmisión de la información hacia el equipo designado como servidor de adquisición (PC11). El

proceso se realizará utilizando el comando PING con la herramienta *Console* del menú *Node* en GNS3.

Para lo anterior se realizará una red con una muestra de la red y de sensores representados por VPCS y se verificará que la capacidad de transmisión cumpla con el requisito previo, para ello se valida lo siguiente:

- Dirección IP en cada dispositivo
- Conectividad entre enrutadores
- Conectividad entre equipos finales (*VPCS*)

Adicionalmente se implementó en la misma arquitectura un sistema de monitorización de equipos en red a través del protocolo SNMP llamado *DUDE*[18] desarrollada por Mikrotik. En el proyecto se implementó un servidor virtual sobre la arquitectura y un sistema cliente en el equipo de cómputo, en la figura 4.1, se puede observar la interfaz de *DUDE* representando varios elementos, algunos parámetros de estado y cantidad de tráfico en cada enlace.

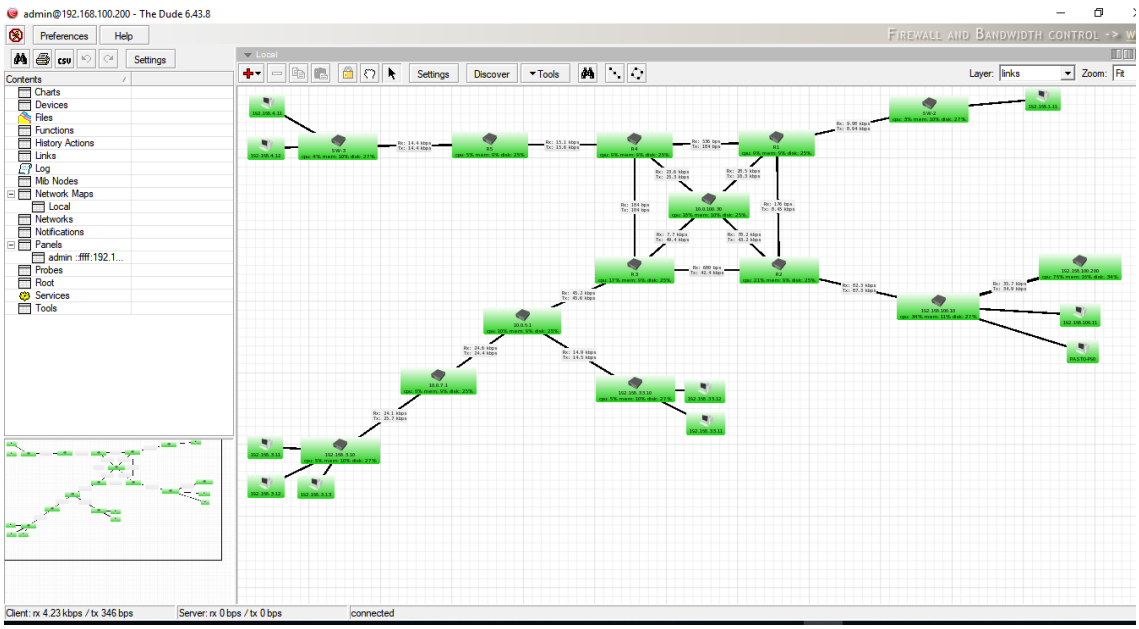

Figura 4.1. Sistema DUDE

[18] *DUDE:* monitor de red Dude es una nueva aplicación de MikroTik que puede mejorar drásticamente la forma en que administra su entorno de red [33]

4.2.3 Pruebas de *Failover*

En esta prueba de tolerancia frente a fallos, se verifica que la red de Telemetría continúe en operación al ocurrir un fallo en un componente del sistema de comunicación, en esta prueba definimos dos escenarios:

a) Fallo de un enlace de conexión: para la prueba se generará un error en enlace entre R2 y R3, que para el diseño corresponde al enlace entre el enrutador que conecta la red LAN de adquisición y el enrutador que permite el acceso al área 2 correspondiente a la repetidora troncal 2.
b) Fallo del switch SW-1 quién recibe todos los enlaces de las repetidoras troncales.

Fallo del enlace de conexión

Una manera de realizar esta prueba, es deshabilitando una de las interfaces asociadas a este enlace, este procedimiento se puede realizar tanto en R2 como en R3. En la prueba realizada, se deshabilitó la interfaz eth-1 del enrutador R2 utilizando la herramienta *Winbox*.

Fallo del switch SW-1

Para la realización de esta prueba, se utilizó las herramientas del programa GNS3 en el menú `Node`, la opción `Stop`.

4.2.4 Pruebas de saturación de tráfico

En esta prueba se verificará el correcto desempeño de las reglas asociadas a la reserva de recursos de red, acorde con prioridad definida para cada estación, para lo cual se simulará una disminución de la capacidad de transmisión en el enlace entre R3 y R6; adicionalmente se permite comprobar las reglas definidas de calidad de servicio para datos generados desde la estación principal (PC8 - 192.168.3.13) y el equipo servidor (PC11 – 192.168.100.11).

La arquitectura montada en GNS3 para la simulación de una muestra de la red, se contempla un total de 8 equipos que se pueden asociar con una estación y un equipo que se lo puede considerar como el sistema de adquisición. Dada las limitaciones

asociadas a la licencia de las herramientas utilizadas, se puede generar un tráfico máximo de 8 Kbps en Rx y 8 Kbps en Tx por cada estación, teniendo un tope máximo de flujo de tráfico hacia el servidor de adquisición de 64 Kbps en un modo full dúplex.

Para reducir la capacidad del enlace entre R2 y PC-11, se configuró R2 con la herramienta *Winbox*, una regla de cola simple (*Simple Queues*) en el interfaz Eth-3 que limita el tráfico a un máximo de 32 Kbps en Rx y 32 Kbps en Tx a todo el tráfico con origen y destino el PC-11 (192.168.100.11).

4.3 Ejecución del plan de pruebas

Pruebas de dispositivos

De acuerdo con el plan de pruebas, se ejecutó paso a paso el procedimiento y los equipos operan con normalidad, esto se puede observar en la figura 4.2 en donde todos los enlaces están de color verde (círculos en cada interfaz), así como también los objetos de un color sólido.

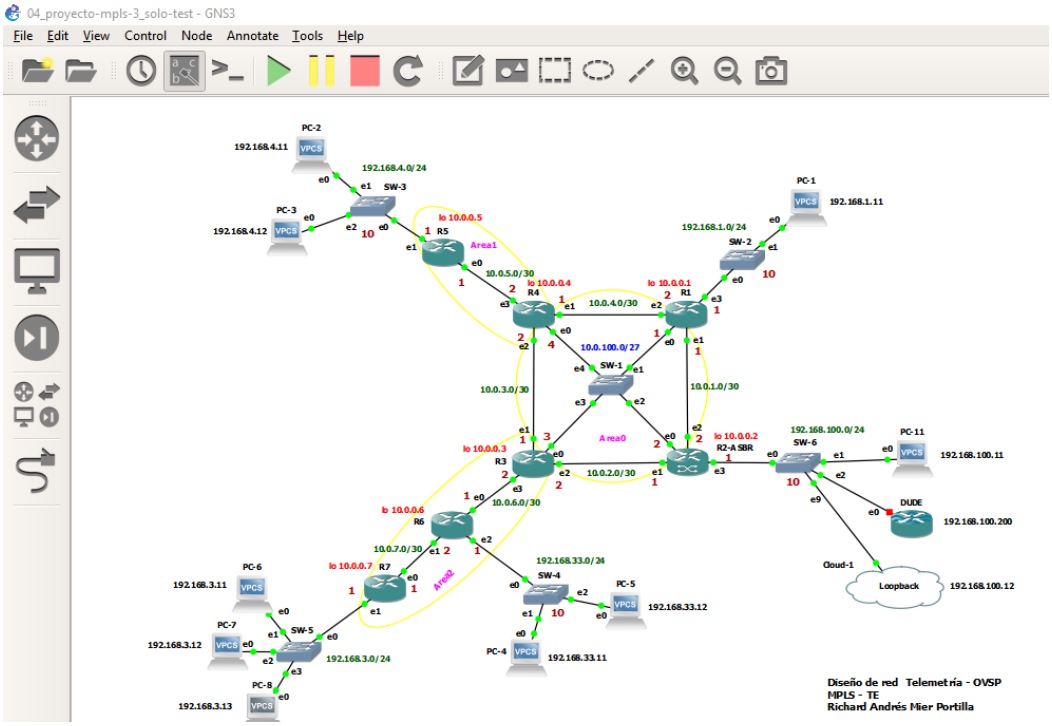

Figura 4.2. Dispositivos en GNS3

Por otro lado, en la figura 4.1, de acuerdo con el sistema *DUDE*, se puede observar que todos los elementos se encuentran de color verde.

Pruebas de conectividad

Inicialmente se procede a verificar la dirección IP de cada equipo VPCS, para ello se usa la herramienta *Console* en GNS3 y se ejecuta el comando: *show ip* cuya salida es la configuración de red del dispositivo.

Posteriormente, se verifica la dirección IP de cada enrutador, para esta tarea se utiliza la herramienta Winbox, y de manera gráfica en el menú izquierdo IP, en la opción *Address*, se despliega una ventana *Address List* que contiene todas las interfaces a las que se le ha asignado una dirección IP.

Una vez verificada la configuración, se procede a verificar conectividad entre enrutadores y puntos finales, para el caso de enrutadores se utiliza la herramienta *Winbox* y una de las opciones para hacerlo es utilizando la aplicación del menú izquierdo llamada *New Terminal*, esta despliega una ventana con una interfaz de línea de comando y a través de la aplicación ping, se verifica conectividad con cada enrutador.

En la figura 4.3, se muestra las direcciones IP del enrutador R2 como también las rutas a los diferentes enrutadores.

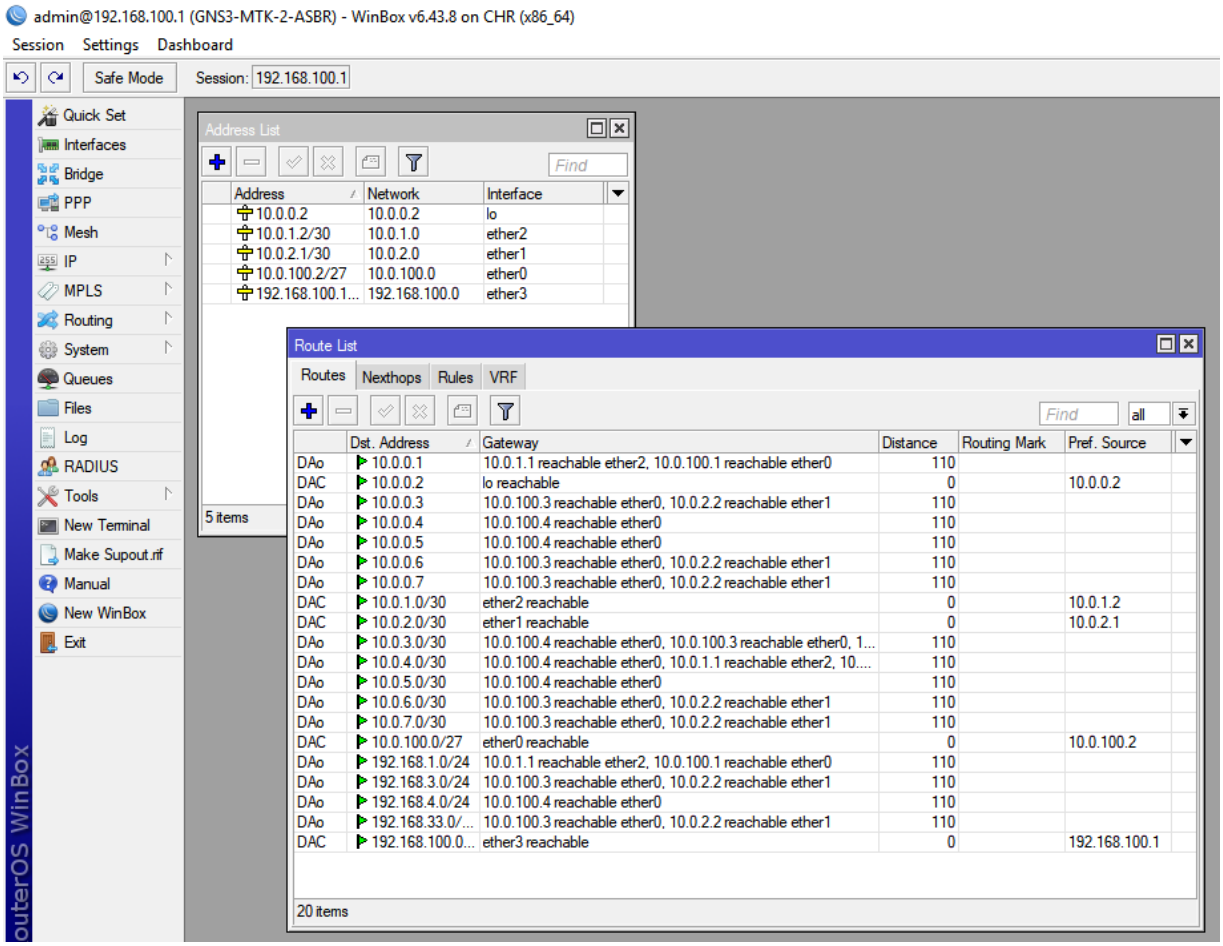

Figura 4.3. Direcciones IP y rutas en R2

Adicionalmente a la conectividad, se envió datos de manera permanente desde cada uno de los 8 VPCS hasta el equipo designado como servidor de adquisición, observando de manera práctica que al enviar el tamaño máximo del paquete permitido en GNS3 en un `ping`, utilizando la directiva `-l =1000`, en el último tramo (SW6-PC11) se obtiene un valor de 66.6 Kbps tanto en Rx como en Tx tomado en la interfaz Eth-1 de SW-6. En la figura 4.4 en la parte izquierda, la arquitectura en GNS3, al centro, 8 ventanas de ping correspondiente a cada VPCS y a la derecha, una imagen de Winbox con el valor registrado de Rx/Tx en la interfaz Eth-1 de SW-6. Como dato adicional, con la arquitectura montada en GNS3, el procesador del equipo host, oscila entre 60 y 80 % de ocupación.

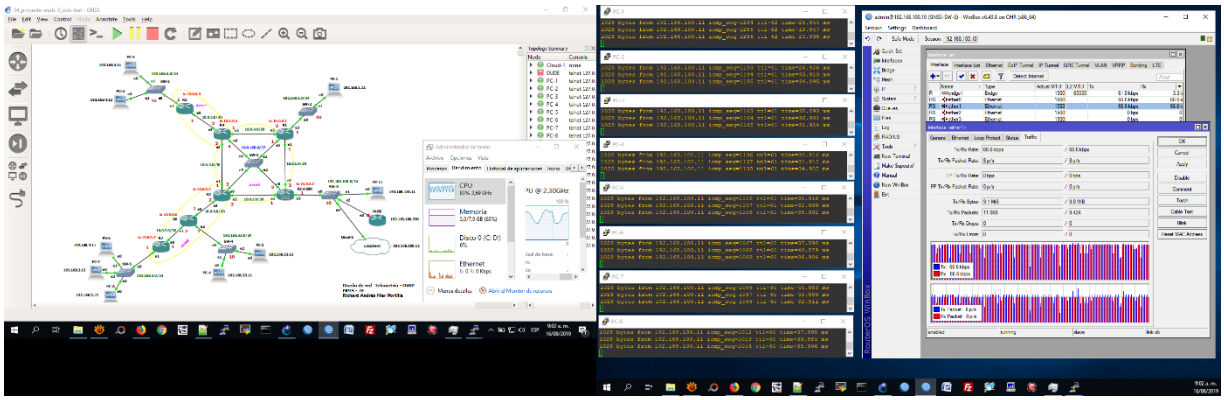

Figura 4.4. Tráfico total desde y hacia PC11

Pruebas de Failover

En la figura 4.5, se puede observar la ruta que un paquete entre PC8 y R3, considerando que no existe fallo alguno en la red, adicionalmente en la parte inferior derecha, se puede observar las etiquetas MPLS utilizadas para el enrutamiento.

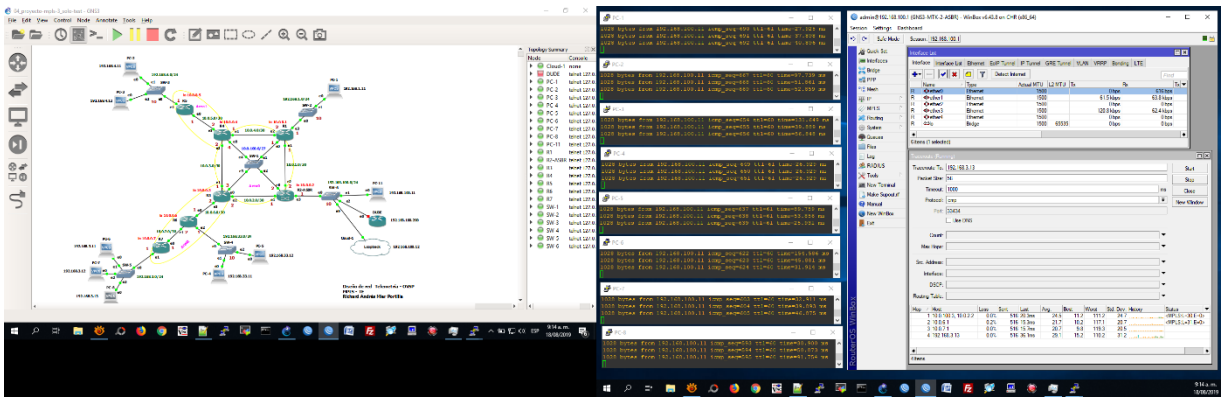

Figura 4.5. Rutas entre PC8 y R2

Para el escenario a) Fallo de un enlace de conexión, con la herramienta Winbox, ingresamos al enrutador R2 se ingresa a la opción Interfaces del menú izquierdo, se selecciona la interfaz que conecta a R2 con R3 y se hace clic en el botón deshabilitar. En la figura 4.6, se puede observar en la parte central, que al bloquear la interfaz Eth-1 de R2, no se pierde conectividad alguna con el servidor.

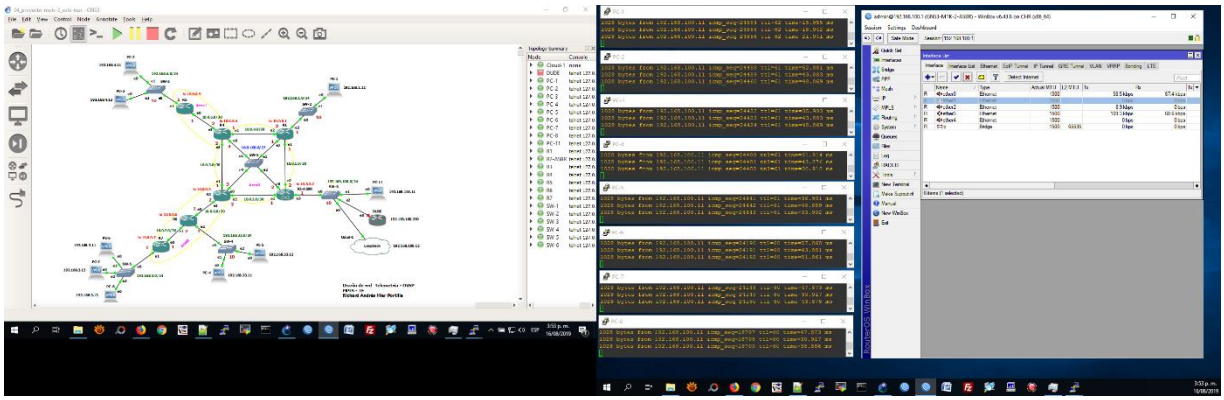

Figura 4.6. Bloqueo del enlace R2-R3

Con respecto al escenario b) Fallo del switch SW-1, en la herramienta GNS3, se selecciona el dispositivo, del menú `Node`, se selecciona la opción `Stop`. En la figura 4.7, se evidencia que se mantiene conectividad, aunque es necesario esperar alrededor de 30 segundos mientras se re enruta el tráfico.

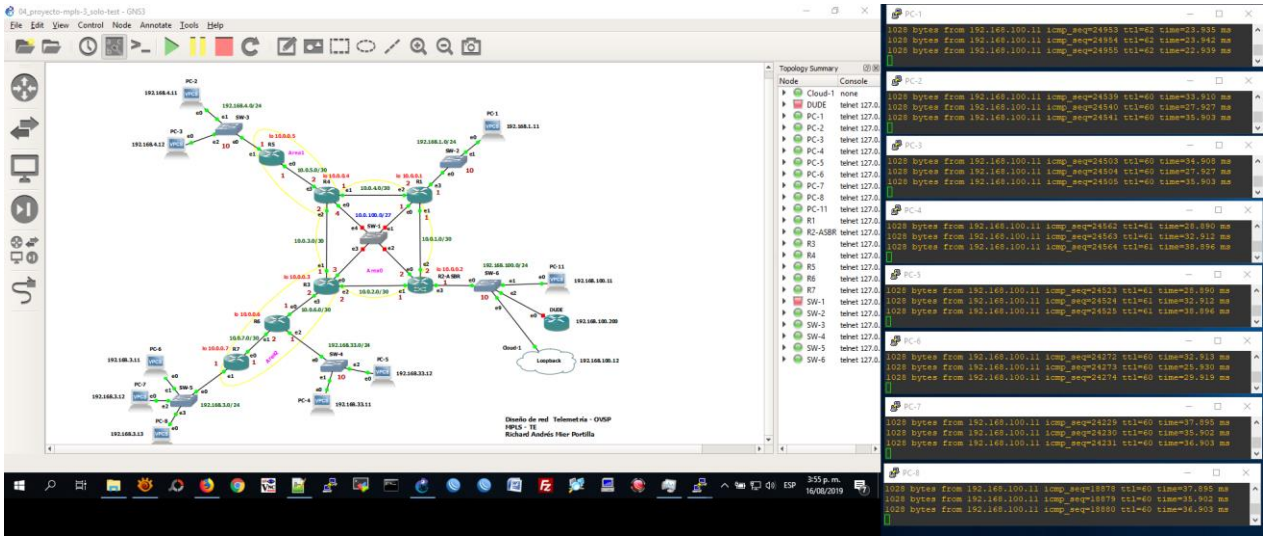

Figura 4.7. Fallo de SW-6

Pruebas de saturación de tráfico

Con la herramienta Winbox, se ingresa al equipo R2, en el menú izquierdo, se selecciona la opción `Queues`, posteriormente se despliega una pestaña `Queue List` en la que se debe hacer clic en la opción `New` (botón “+”), finalmente se agrega una regla que limita la capacidad de comunicación para el equipo PC-11 con un máximo

de 32 Kbps en Rx y 32 Kbps en Tx; de esta manera se simula un fallo que deriva una reducción significativa en un enlace inalámbrico y se evalúan las reglas de ingeniería de tráfico basadas en prioridad. En la figura 4.8, en la parte izquierda se puede observar que tres estaciones pierden conectividad, mientras que las cuatro últimas mantienen activa la conexión sin pérdida de paquetes y una latencia promedio de 38.8 ms, en la parte derecha, se tiene una captura de la interfaz de *Winbox* en la que se visualiza la regla de cola simple utilizada; la prueba se realizó durante 5 minutos.

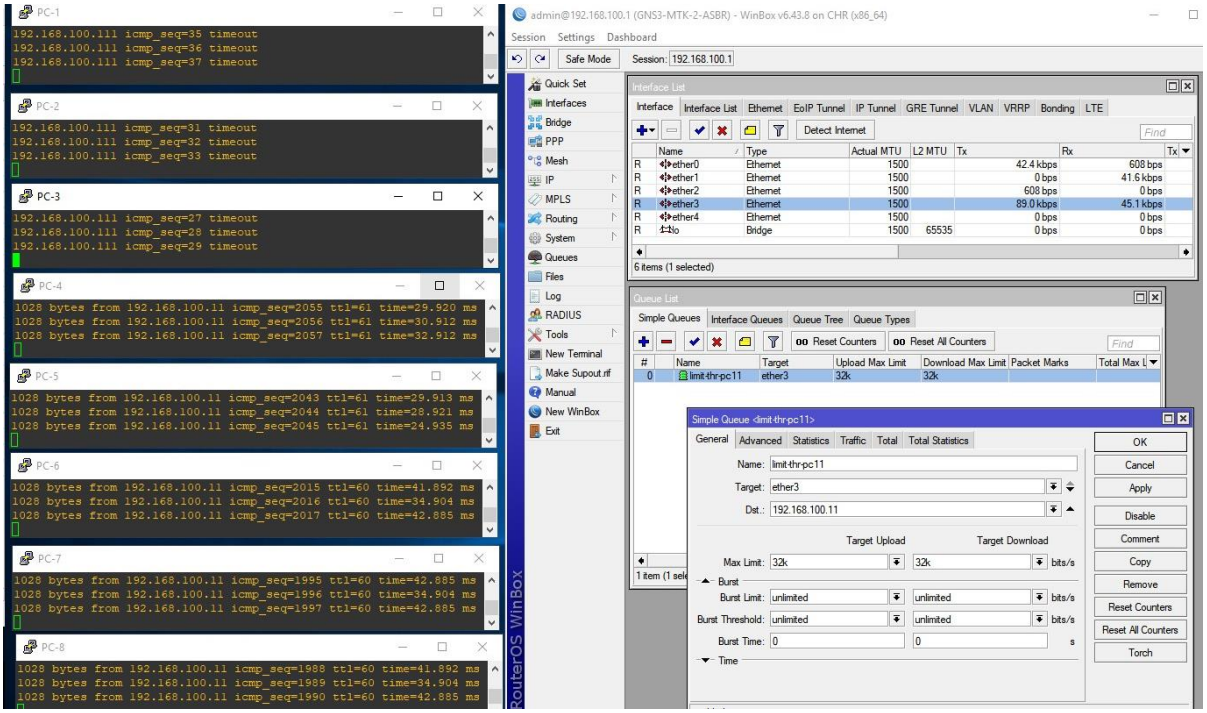

Figura 4.8. Saturación del enlace entre R2 y PC-11 con MPLS-TE

4.4 Evaluación de resultados obtenidos en la simulación

De acuerdo con los resultados derivados del plan de pruebas y su ejecución, utilizando las herramientas de monitorización propuestas, se puede evidenciar que los objetivos del diseño se cumplen, al obtener un porcentaje superior al 95 % de disponibilidad de la red de Telemetría en un escenario tolerante a fallos con reservación de recursos para el tráfico prioritario definido por el Instituto.

Adicionalmente, durante el mismo tiempo y sobre la arquitectura implementada, se realizó la prueba de saturación, en la cual se deshabilito las reglas de MPLS-TE, obteniendo como resultado un incremento significativo de la latencia, pasando de un promedio de 35.8 a 696 ms, y pérdida de paquetes de 0 al 28.1 %. En la figura 4.9, se puede observar el resultado de la prueba.

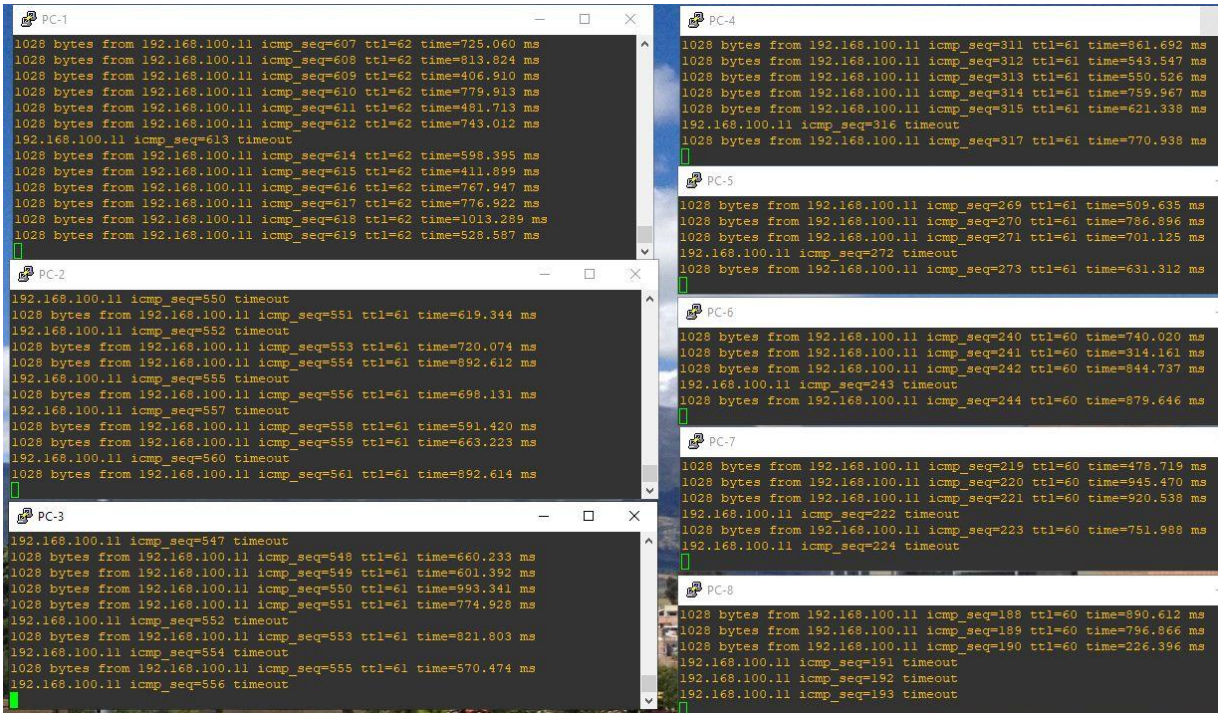

Figura 4.9. Saturación del enlace entre R2 y PC-11 sin MPLS-TE

Capítulo 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones.

1. En la red de Telemetría del Observatorio Pasto, los parámetros importantes a tener en cuenta para garantizar la capacidad de transmisión requerida en los enlaces inalámbricos son:

   - Nivel de señal a ruido (SNR, *Signal to Noise Ratio*) superior a 25 dBm
   - Entre 10 y 15 dBm de guarda en el nivel de señal para soportar condiciones anómalas que puedan degradar la conexión.
   - Frecuencia y potencia acorde a las normas actuales en relación a comunicaciones inalámbricas.

2. Como resultado del análisis del estado actual de la red, en contraste con los sensores instalados, la arquitectura y diseño de la red de Telemetría del Observatorio Pasto, en algunos tramos no cumple con el requerimiento mínimo en capacidad de Transmisión, sin embargo, con actividad volcánica baja, la red opera con normalidad.

3. Con la priorización de paquetes, se logran desempeños adecuados que, a través de una arquitectura redundante, permite soportar fallos y garantizar el tráfico mínimo de datos necesario para la evaluación del fenómeno volcánico.

4. Una red basada en la tecnología MPLS mejora considerablemente la calidad del dato con respecto a las técnicas tradicionales de transporte de datos y reduce la incertidumbre para la toma de decisiones.

5. El uso de equipos Mikrotik hace posible implementar arquitecturas como MPLS-TE que hace poco se limitaba a dispositivos de gama alta como Cisco, Juniper Networks, Arista Networks entre otros, adicionalmente con herramientas como GNS3 se puede utilizar en un entorno de desarrollo o pruebas pre-producción de manera virtual.

6. La participación de la red pública de internet en la red de Telemetría y monitoreo volcánico, puede considerarse positiva en relación al uso de infraestructura y servicios que pueden aportar a diseños de sistemas redundantes.

7. La implementación de sistemas de monitorización y gestión de la red de Telemetría en el Observatorio Pasto, permite una gestión oportuna de incidentes y posibilita mejorar la red continuamente.

5.2. Recomendaciones.

Los trabajos realizados consideraron redes privadas y enlaces dedicados entre la sede central y repetidoras principales y secundarias, trabajos futuros deben tener en cuenta apoyarse en las redes públicas de *Internet* como respaldo tanto para verificar estados de salud de los equipos como para realizar reinicios y cambios de configuración en equipos de red.

Para trabajos futuros se sugiere integrar un sistema de monitorización desarrollado a la medida que permita no solo el sondeo periódico de conectividad sino también una interfaz de consulta y despliegue de datos de variables de comunicación, un sistema de notificación y un desarrollo en hardware y software para realizar cambios de parámetros en equipos de comunicación.

La implementación del presente diseño se debe realizar de manera gradual tal y como se describe en la metodología.

En el Observatorio Pasto, se debe implementar y mantener un sistema de documentación de la red de telemetría enfocado a gestión de equipos de comunicación.

Bibliografía

[1] SIA Mikrotīkls, «MikroTik Routers and Wireless - Software,» [En línea]. Available: https://mikrotik.com/download. [Último acceso: 25 julio 2019].

[2] GNS3, «MikroTik CHR appliance - GNS3,» 2019. [En línea]. Available: https://docs.gns3.com/appliances/mikrotik-chr.html. [Último acceso: julio 2019].

[3] Servicio Geológico Colombiano, «Distribución física de repetidoras y equipos de comunicación Observatorio Pasto,» Pasto, 2017.

[4] Ministerio de Tecnologías de la información y las Comunicaciones, «Ministerio de Tecnologías de la información y las Comunicaciones,» 2010. [En línea]. Available: https://www.mintic.gov.co/portal/inicio/3762:Resolucion-202-de-2010. [Último acceso: 3 Octubre 2019].

[5] Instituto Geofísico EPN, «Escuaela Politéncica Nacional,» Quito, 2016.

[6] El Servicio Nacional de Geología y Minería (Sernageomin), «Observatorio Volcanológico de Los Andes del Sur (OVDAS),» Providencia, 2016.

[7] SERNAGEOMIN, «SERNAGEOMIN - Servicio Nacional de Geología y Minería,» [En línea]. Available: https://www.sernageomin.cl/red-nacional-de-vigilancia-volcanica/. [Último acceso: diciembre 2017].

[8] Observatorio Vulcanológico y Sismológico de Costa Rica (OVSICORI), «Red de datos,» Heredia.

[9] Servicio Geológico Colombiano, «Nuevos Conceptos de Telemetría del Observatorio Vulcanológico y Sismológico de Popayán,» Popayan, 2013.

[10] T. A. S., Redes de computadoras, Naucalpan de Juárez - México: Pearson - Pentice Hall, 2003.

[11] H. G. Perros, Connection-Oriented Networks: SONET/SDH, ATM, MPLS and Optical Networks, Chichester, England., 2005.

[12] Cisco Systems, Inc., «Guía de diseño de OSPF,» [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html. [Último acceso: Octubre 2019].

[13] Huston, Geoff, «Quality of Service-Fact or Fiction?,» 2000. [En línea]. Available: http://www.potaroo.net/papers/ipj/2000-v3-n1-qos/qos.html. [Último acceso: octubre 2019].

[14] Internet Engineering Task Force, «RFC 791 - Internet Protocol,» Septiembre 1981. [En línea]. Available: https://tools.ietf.org/html/rfc791. [Último acceso: octubre 2019].

[15] Internet Engineering Task Force, «RFC 1349 - Type of Service in the Internet Protocol Suite,» Julio 1992. [En línea]. Available: https://tools.ietf.org/html/rfc1349. [Último acceso: octubre 2019].

[16] K. I. Park, QoS in packet networks, Springer Science + Business Media, Inc., 2005.

[17] B. D. -. A. Farrel, MPLS: Next Steps, Burlington, Massachusetts, USA: Morgan Kaufmann, 2008.

[18] S. G. R. P. Dominique Gaïti, Network control and Engineering for QoS, Security and Mobility - III, Boston: Springer Science + Business Media, Inc., 2005.

[19] Cisco Systems, Inc., MPLS Fundamentals, 800 East 96th Street Indianapolis, IN 46240 USA: Cisco Press, 2007.

[20] Internet Engineering Task Force, «RFC 4594 - Configuration Guidelines for DiffServ Service Classes,» agosto 2006. [En línea]. Available: https://tools.ietf.org/html/rfc4594. [Último acceso: octubre 2019].

[21] Z. Wang, Internet Qos - Architectures and Mechanism for Quality of Service, The Morgan Kaufmann Series in Networking.

[22] Cisco Systems, Inc., «Inter-Switch Link and IEEE 802.1Q Frame Format,» [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html. [Último acceso: octubre 2019].

[23] S. B. Morris, Network Management, MIBs and MPLS: Principles, Design and Implementation, Addison Wesley, 2003.

[24] Cisco Systems, Inc., «Catalyst 3560 Software Configuration Guide QoS,» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swqos.html. [Último acceso: octubre 2019].

[25] G. R. Ash, Traffic Engineering and QoS Optimization of MPLS-Based Integrated Voice/Data Dynamic Routing Networks, San Francisco, CA: Morgan Kaufmann Publishers, 2007.

[26] PTG Media, 2007. [En línea]. Available: http://ptgmedia.pearsoncmg.com/images/chap9_1587051990/elementLinks/09fig01.gif. [Último acceso: 21 Diciembre 2018].

[27] Servicio Geológico Colombiano, «Organigrama,» 26 nov 2019. [En línea]. Available: https://www2.sgc.gov.co/Nosotros/Organigrama/Paginas/organigrama.aspx.

[28] «Software | GNS3,» Agosto 2019. [En línea]. Available: https://gns3.com/software. [Último acceso: Agosto 2019].

[29] Ubiquiti Networks, «Ubiquiti Networks - Products,» [En línea]. Available: https://www.ui.com/products.

[30] D. M. y. T. Z. K. Sohraby, Wireless Sensor Network Technology, New Jersey: Jhon Wiley & Sons, 2007, p. 307.

[31] L. D. Ghein, MPLS Fundamentals, Indianapolis, IN 46240 USA: Cisco Press, 2007.

[32] Internet Engineering Task Force, «RFC-2474,» Diciembre 1998. [En línea]. Available: https://tools.ietf.org/html/rfc2474.

[33] «MIkroTik Routers and Wireless - DUDE,» SIA MikroTikls, [En línea]. Available: https://mikrotik.com/thedude.

[34] Servicio Geológico Colombiano, «www.sgc.gov.co,» [En línea]. Available: www.sgc.gov.co.

[35] R. J. (. Bates, Broadband Telecommunications Handbook, United States of America: McGraw Hill, 2002.

[36] MPLS Resource Center, «The MPLS-VPLS Resource Center,» 2007. [En línea]. Available: http://www.mplsrc.com/faq2.shtml#MPLS%20Traffic%20Engineering. [Último acceso: 21 Diciembre 2018].

[37] Mikrotik Wiki, «Manual: TOC Mikrotik Wiki,» 2019. [En línea]. Available: https://wiki.mikrotik.com/wiki/Manual:TOC. [Último acceso: 2019].

[38] ACGIH, TLVs and BEIs Threshold Limit Values, for chemical substances and Physical Agents. Biological Exposure Indices, Cincinnati: Signature Publications, 2009.

[39] Internet Engineering Task Force, «RFC 1633 - Integrated Services in the Internet Architecture and Overview,» junio 1994. [En línea]. Available: https://tools.ietf.org/html/rfc1633. [Último acceso: octubre 2019].

[40] Internet Engineering Task Force, «RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers,» diciembre 1998. [En línea]. Available: https://tools.ietf.org/html/rfc2474. [Último acceso: octubre 2019].

[41] Internet Engineering Task Force, «RFC 2205 - Resourse ReSerVation Protocol (RSVP) -- Version 1 Functional Specification,» septiembre 1997. [En línea]. Available: https://tools.ietf.org/html/rfc2205. [Último acceso: octubre 2019].

[42] Internet Engineering Task Force, «RFC 3209 - RSVP-TE: Extensions to RSVP for LSP Tunnels,» diciembre 2001. [En línea]. Available: https://tools.ietf.org/html/rfc3209. [Último acceso: octubre 2019].

[43] Internet Engineering Task Force, «RFC 3031 - Multiprotocol Label Switching Architecture,» Diciembre 2009. [En línea]. Available: https://www.ietf.org/rfc/rfc3031.txt.

[44] Cisco Systems, Inc., «Implementación de políticas de calidad del servicio (QoS) con DSCP,» [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.pdf. [Último acceso: octubre 2019].

Anexo A

Configuración de GNS3

Una vez instalada la herramienta GNS3, en el equipo de cómputo es necesario tener activa y conectada la interfaz de red *Ethernet*, adicionalmente configurar el servidor en la interfaz de Loopback de sistema con la dirección IP 127.0.0.1.

Para acceder desde el sistema operativo del equipo de cómputo hacia los equipos virtuales en GNS3, se debe realizar la siguiente configuración.

a) Agregar un interfaz virtual de red
   Inicio – Ejecutar
   hdwwiz
   Siguiente, instalar manualmente
   Adaptadores de red
   Microsoft - Adaptador de bucle invertido KM-Test de Microsoft
   Cambiar nombre de la interfaz por Loopback

b) Seleccionar el adaptador creado (Adaptador de bucle invertido)
   Cambiar nombre (Loopback-GNS3)
   *Si se requiere acceso a internet (Seleccionar la interfaz con acceso a internet)
   Propiedades
   Uso compartido
   Permitir que los usuarios de otras redes se conecten
   Conexión de red doméstica

c) En GNS3
   Agregar el objeto Cloud
   Configure
   En la pestaña Ethernet interfaces
   Eliminar todas las conexiones que aparecen
   Habilitar: Show special Ethernet interfaces
   Seleccionar: Loopback y add
   Apply
   Conectar el objeto

Anexo B

Descripción de los equipos Mikrotik

SIA Mikrotīkls, conocida internacionalmente como MikroTik, es una compañía letona proveedora de tecnología disruptiva de hardware y software para la creación de redes. Mikrotik RouterOS es un software que funciona como un Sistema Operativo para convertir un PC o una placa Mikrotik Router BOARD en un router dedicado.

MikroTik se dedica principalmente a la venta de productos de hardware de red como routers denominados Routerboards y switches también conocidos por el software que lo integra, denominado RouterOS y Sw OS. La compañía fue fundada en el 1995, aprovechando el emergente mercado de la tecnología inalámbrica. En 2007, contaba con más de 70 empleados.

RouterOS

Mikrotik RouterOS [1] es el Sistema Operativo y software que puede convertir un PC o un Routerboard en un enrutador dedicado. Es un sistema operativo basado en el núcleo Linux, el cual implementa varias funcionalidades como por ejemplo BGP, IPv6, OSPF o MPLS. Proporciona una gran estabilidad, controles y flexibilidad para todo tipo de interfaces de datos y enrutamiento.

Routerboard

La división de hardware de la marca MikroTik es caracterizada por incluir su sistema operativo RouterOS por defecto y actualizaciones de por vida. Estos dispositivos tienen la ventaja de tener una excelente relación precio/calidad.

Certificaciones Oficiales

Desde Mikrotik se lanzaron una serie de certificaciones oficiales para los usuarios de sus dispositivos. Estas certificaciones acreditan que el usuario está cualificado por parte del fabricante para gestionar y administrar sus dispositivos. Tienen certificaciones para enrutamiento, enrutamiento avanzado, WiFi, gestión de usuarios entre otras.

Anexo C

Descripción de herramienta Winbox

Existen varias aplicaciones para acceder a la configuración de los equipos Mikrotik, entre ellos el más usado es Winbox, esta aplicación es una interfaz gráfica del sistema operativo instalado en el Hardware.

Winbox es una pequeña utilidad que permite la administración de Mikrotik RouterOS usando una guía rápida y simple. Es un Win32 binary nativo, pero se puede ejecutar en Linux y MacOS (OSX) usando Wine. Se puede descargar desde la web oficina de Mikrotik. En la figura C.1., se puede observar el entorno de administración del sistema.

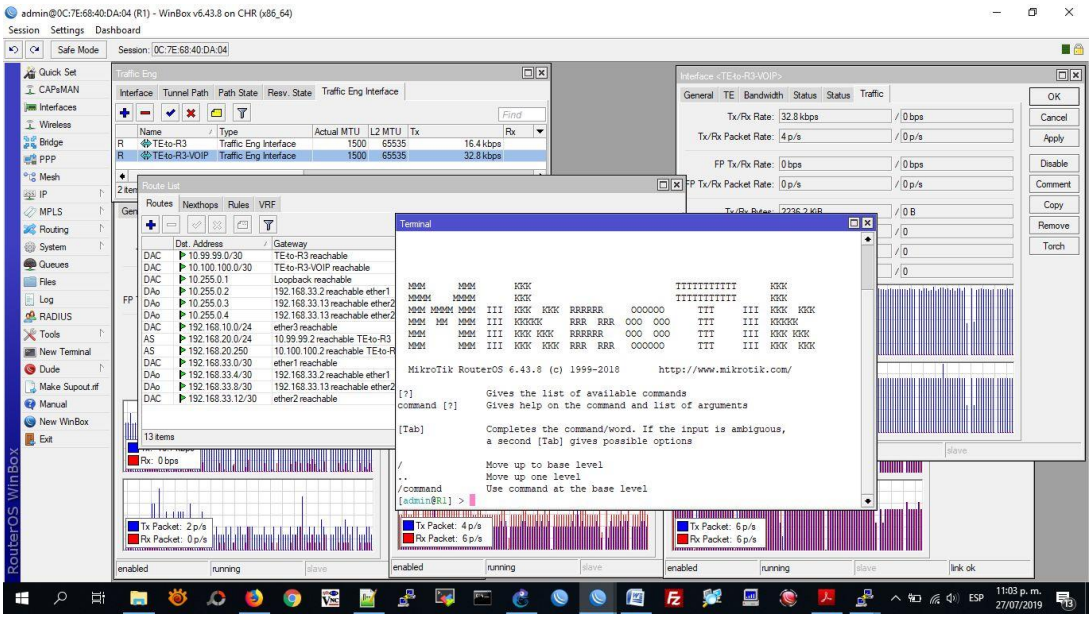

Figura C.1. Interfaz visual de la herramienta Winbox

Anexo D

Configuración de equipos Mikrotik

La configuración de RouterOS, se puede realizar de varias maneras, una de ellas es a través de una terminal dentro de una sesión de SSH o utilizando la herramienta Terminal de Winbox, como caso de uso, el código documentado simula un equipo de adquisición y varios clientes, se generan tres túneles de MPLS-TE en los cuales se hace reserva de recursos y se da prioridad para un tráfico específico. Adicionalmente se utiliza un modelo de *Failover* utilizando también el enrutamiento dinámico por OSFP. En la figura D.1., se ilustra la arquitectura básica de MPLS-TE como guía inicial de configuración.

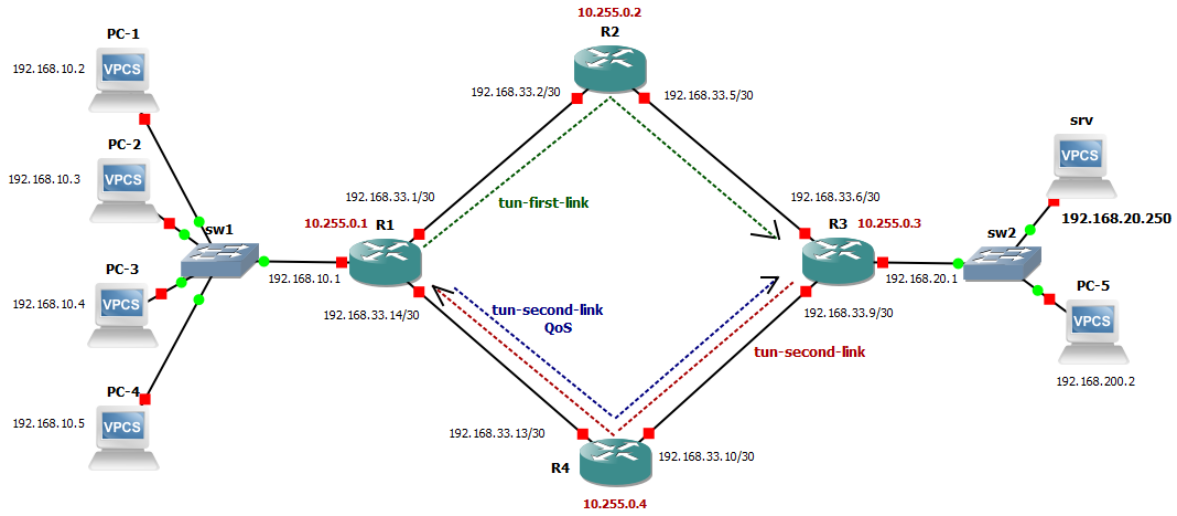

Figura D.1. Diagrama guía de diseño de MPLS-TE

A continuación, se muestra el código para cada enrutador del sistema básico de MPLS-TE en GNS3.

```
------------------------------------------------------------------------
RUTEO
------------------------------------------------------------------------
R1
------------------------------------------------------------------------
/system identity set name=R1
/interface bridge add name=Loopback
/ip address
add address=192.168.33.1/30 interface=ether1
add address=192.168.33.14/30 interface=ether2
add address=192.168.10.1/24 interface=ether3
add address=10.255.0.1/32 interface=Loopback
------------------------------------------------------------------------
R2
------------------------------------------------------------------------
/system identity set name=R2
/interface bridge add name=Loopback
/ip address
add address=192.168.33.2/30 interface=ether1
add address=192.168.33.5/30 interface=ether2
add address=10.255.0.2/32 interface=Loopback
------------------------------------------------------------------------
R3
------------------------------------------------------------------------
/system identity set name=R3
/interface bridge add name=Loopback
/ip address
add address=192.168.33.6/30 interface=ether1
add address=192.168.33.9/30 interface=ether2
add address=192.168.20.1/24 interface=ether3
add address=10.255.0.3/32 interface=Loopback
------------------------------------------------------------------------
R4
------------------------------------------------------------------------
/system identity set name=R4
/interface bridge add name=Loopback
/ip address
add address=192.168.33.10/30 interface=ether1
add address=192.168.33.13/30 interface=ether2
add address=10.255.0.4/32 interface=Loopback
------------------------------------------------------------------------
```

```
------------------------------------------------------------------------
OSPF
------------------------------------------------------------------------
R1
------------------------------------------------------------------------
/routing ospf instance
set default router-id=10.255.0.1 mpls-te-area=backbone mpls-te-router-id=Loopback

(/routing ospf instance
set default router-id=10.255.0.4 mpls-te-area=backbone mpls-te-router-id=Loopback
redistribute-connected=as-type-1)

/routing ospf network
add network=192.168.33.0/24 area=backbone
add network=10.255.0.1/32 area=backbone
------------------------------------------------------------------------
R2
------------------------------------------------------------------------
/routing ospf instance
set default router-id=10.255.0.2 mpls-te-area=backbone mpls-te-router-id=Loopback
/routing ospf network
add network=192.168.33.0/24 area=backbone
add network=10.255.0.2/32 area=backbone
------------------------------------------------------------------------
R3
------------------------------------------------------------------------
/routing ospf instance
set default router-id=10.255.0.3 mpls-te-area=backbone mpls-te-router-id=Loopback
/routing ospf network
add network=192.168.33.0/24 area=backbone
add network=10.255.0.3/32 area=backbone
------------------------------------------------------------------------
R4
------------------------------------------------------------------------
/routing ospf instance
set default router-id=10.255.0.4 mpls-te-area=backbone mpls-te-router-id=Loopback
/routing ospf network
add network=192.168.33.0/24 area=backbone
add network=10.255.0.4/32 area=backbone
------------------------------------------------------------------------
```

```
------------------------------------------------------------------------
TE-Tunnel
------------------------------------------------------------------------
1. Define recursos R1-R2-R3-R4 BW interface

/mpls traffic-eng interface
add interface=ether1 bandwidth=128kbps
add interface=ether2 bandwidth=128Kbps

2. Crear Path // Origen y destino (IP hops) desde R1-R3 // definir primero el dinámico
por OSPF

------------------------------------------------------------------------
R1
------------------------------------------------------------------------
/mpls traffic-eng tunnel-path
add name=dyn use-cspf=yes
add name=tun-first-link use-cspf=no
hops=192.168.33.2:strict,192.168.33.5:strict,192.168.33.6:strict
------------------------------------------------------------------------

------------------------------------------------------------------------
R3
------------------------------------------------------------------------
/mpls traffic-eng tunnel-path
add name=dyn use-cspf=yes
add name=tun-second-link use-cspf=no
hops=192.168.33.10:strict,192.168.33.13:strict,192.168.33.14:strict

------------------------------------------------------------------------

------------------------------------------------------------------------
3. Define recursos TE-Tunnel BW 32Kbps (IP Loopback)
------------------------------------------------------------------------
R1
------------------------------------------------------------------------
/interface traffic-eng
add bandwidth=32Kbps name=TE-to-R3 to-address=10.255.0.3 primary-path=tun-first-link
secondary-paths=dyn record-route=yes from-address=10.255.0.1
------------------------------------------------------------------------
R3
------------------------------------------------------------------------
/interface traffic-eng
add bandwidth=16Kbps name=TE-to-R1 to-address=10.255.0.1 primary-path=tun-second-link
secondary-paths=dyn record-route=yes from-address=10.255.0.3
------------------------------------------------------------------------
RUTEO - TE
------------------------------------------------------------------------
R1
------------------------------------------------------------------------
/ip address add address=10.99.99.1/30 interface=TE-to-R3
/ip route add dst-address=192.168.20.0/24 gateway=10.99.99.2
------------------------------------------------------------------------
R3
------------------------------------------------------------------------
/ip address add address=10.99.99.2/30 interface=TE-to-R1
/ip route add dst-address=192.168.10.0/24 gateway=10.99.99.1
------------------------------------------------------------------------
```

```
------------------------------------------------------------------------
FAILOVER (optimizaciónpor automatically - at specific interval) de vacio a 5s
------------------------------------------------------------------------
R1
/interface trafic-eng set TE-to-R3 reoptimize-interval=5s
([admin@R1] /interface> traffic-eng set TE-to-R3 reoptimize-interval=5s)
R3
/interface trafic-eng set TE-to-R1 reoptimize-interval=5s
/interfacetrafic-eng set TE-to-R1 reoptimize-interval=5s
------------------------------------------------------------------------

------------------------------------------------------------------------
VoIP
------------------------------------------------------------------------
Crea path
Define recursos TE
------------------------------------------------------------------------
R1
------------------------------------------------------------------------
/mpls traffic-eng tunnel-path
add name=tun-second-link use-cspf=no
hops=192.168.33.13:strict,192.168.33.10:strict,192.168.33.9:strict

/interface traffic-eng
add name=TE-to-R3-VOIP to-address=10.255.0.3 bandwidth=8Kbps record-route=yes primary-
path=tun-second-link secondary-paths=dynreoptimize-interval=5s
------------------------------------------------------------------------
RUTEO TE
------------------------------------------------------------------------
R1
------------------------------------------------------------------------
/ip address add address=10.100.100.1/30 interface=TE-to-R3-VOIP
/ip route add dst-address=192.168.20.250/32 gateway=10.100.100.2
------------------------------------------------------------------------
R3
------------------------------------------------------------------------
/ip address add address=10.100.100.2/30 interface=TE-to-R1
------------------------------------------------------------------------

------------------------------------------------------------------------
```