UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"PROPUESTA DE IMPLEMENTACIÓN DEL PROTOCOLO NETFLOW Y LA CALIDAD DE SERVICIO PARA MEJORAR EL RENDIMIENTO DE LA RED LAN EN UNA SEDE DE LA SUNARP"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

SOTELO PALACIOS, ALDO ANTONIO

Villa El Salvador
2019

DEDICATORIA

Este proyecto de investigación se lo dedico a mis padres, a quienes les debo mi vida por ser las personas que a pesar de las dificultades han sabido sacarme adelante con mucho amor, empeño y sacrificio.

AGRADECIMIENTO

Mi sincero agradecimiento a mi asesor el Dr. La Rosa Longobardi Carlos Jacinto por su sabia orientación y al Ing. José Palacios Torres por compartir sus conocimientos a la hora de la elaboración del proyecto.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

Hoy en día con el gran avance de la tecnología y los riesgos que surgen en la red de datos, las diferentes empresas e instituciones están en busca de las mejores soluciones que permitan un mayor control y un mejor rendimiento de su red LAN, debido a los diversos problemas que estas redes presentan rutinariamente, como el gran consumo de ancho de banda.

En el área de redes hay un protocolo que se está volviendo de suma importancia para el análisis del tráfico y el monitoreo de los enlaces; a este protocolo se le conoce como Netflow, el cuál a través de la herramienta Netflow Traffic Analyzer nos brinda acceso a toda la información del tráfico de nuestra red, permitiéndonos así monitorear todo lo que ocurre dentro de ella, asimismo nos ayuda a prevenir el alto consumo de ancho de banda identificando el dispositivo de mayor consumo, el cual puede llegar a afectar el rendimiento de nuestra red.

Respecto a la Superintendencia Nacional de Registros Públicos, el problema radica en que la institución no hace uso del protocolo Netflow para el análisis del tráfico IP, ni tampoco hacen referencia a la calidad de servicio como una solución para mejorar el rendimiento de la red; a pesar de ser una institución que presenta un alto consumo de ancho de banda y un tiempo de respuesta muy elevado.Para ello se establece una propuesta para mejorar el rendimiento de la red mediante el protocolo Netflow y la calidad de servicio.

La estructura que se ha seguido para elaborar este proyecto se compone de tres capítulos:

El primer capítulo comprende el planteamiento del problema, donde se habla de la realidad problemática que afecta a la Superintendencia Nacional de Registros Públicos, motivo por el cual se desarrolla el presente proyecto.

El segundo capítulo comprende el marco teórico, donde se describe los antecedentes de la investigación, así como también las bases teóricas y la definición

de términos los cuáles nos permitirán comprender el tema y los términos usados en este proyecto

El tercer capítulo comprende el desarrollo del proyecto donde se realizará una simulación en Packet Tracer que permita comprobar que la propuesta brindada esta apta para ser configurada en el Router de la Superintendencia Nacional de Registros Públicos, una vez hecha esta simulación se procederá a solicitar un acta de permiso para configurar el protocolo Netflow y la priorización del tráfico en el router de SUNARP, realizado esto se le mostrará al cliente que una vez configurado el protocolo Netflow se podrá saber que usuarios o dispositivos afectan al rendimiento de la red, además se le mostrará mediante la herramienta Netflow Traffic Analyzer la latencia y las pérdidas de paquetes que puede llegar a sufrir la red, los cuales permitirán verificar si la configuración de políticas de calidad de servicio ayudaron a mejorar el rendimiento de la red.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Hoy en día, las entidades que cuentan con un diseño de red WAN y una gran cartera de clientes requieren nuevos avances tecnológicos con el fin de mejorar su rendimiento de su red.

La Superintendencia Nacional de Registros Públicos - SUNARP, se fundó en el año 1997 a través de la ley 26366, es una institución que tiene como principal función supervisar las inscripciones de actos en los registros públicos. Si bien podemos destacar que SUNARP es una de las instituciones más grandes del Perú y unas de las instituciones que más movimiento tienen en el día, es necesario que su estructura tenga un protocolo que solucione los problemas que se presentan cada día en la red de SUNARP; cómo la alta latencia y el alto consumo de ancho de banda que llega en promedio a los 2.79 megas diario de los 3 megas contratado, provocado muchas veces por los equipos y usuarios dentro de la sede, dado que no se cuenta con ningún protocolo o herramienta que permita la identificación de los dispositivos que provocan el saturamiento de la red; afectando así su rendimiento.

Al no tener un correcto control del consumo de ancho de banda ni mucho menos una herramienta o protocolo que ayude a prevenir la saturación de la red que en muchas ocasiones son producidas por los mismos trabajadores al momento de descargar videos, el rendimiento de la red LAN de SUNARP se ve afectada, provocando que los clientes lleguen a tener inconvenientes al momento de realizar algún trámite o inscripción en los registros públicos.

Por ello se realizará una propuesta para mejorar el rendimiento de la red, haciendo uso del protocolo Netflow para prevenir el alto consumo de ancho de banda y también de la calidad de servicio con el fin de priorizar el tráfico de los servicios.

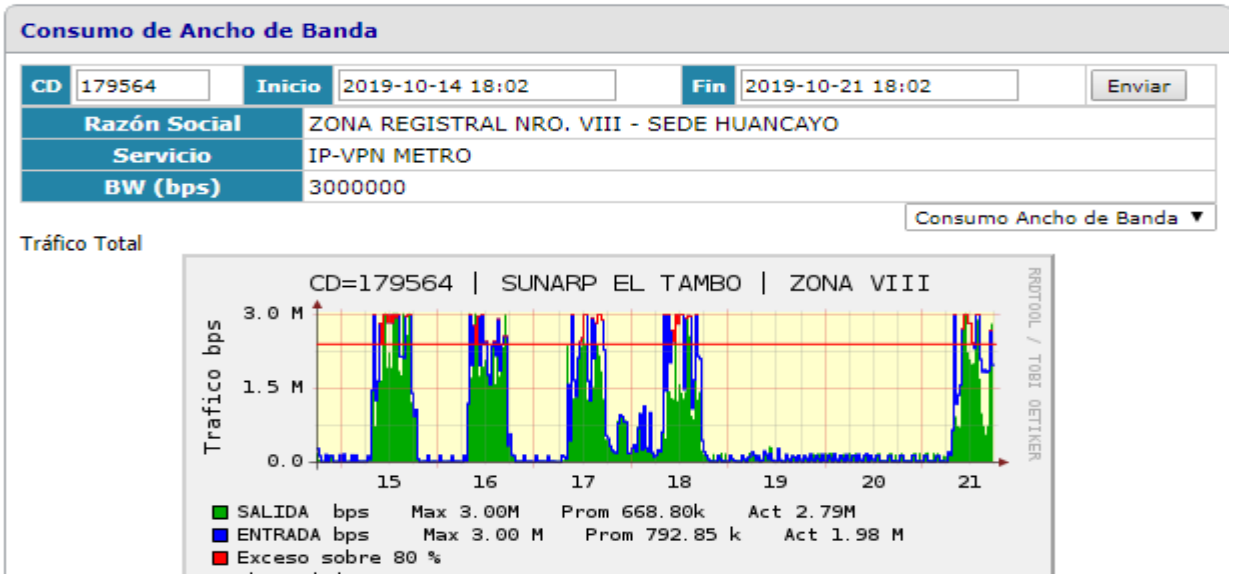


Figura 1: Reporte del consumo de ancho de banda promedio
Fuente: SIGMARS

1.2. JUSTIFICACIÓN DEL PROBLEMA

Visto la problemática mencionada anteriormente, la propuesta para mejorar el rendimiento de la red LAN de la Superintendencia Nacional de Registros Públicos a través del protocolo Netflow y la Calidad de servicio, es de suma importancia ya que permitirá tener un mejor monitoreo del tráfico IP y una mejor priorización del tráfico de los distintos servicios, además ayudará a identificar que dispositivo es el que consumo el mayor ancho de banda permitiendo de esta manera prevenir las altas latencias que pueden llegar a afectar el rendimiento de la red. Asimismo, esta propuesta ayuda a mejorar la toma de decisiones las cuales dependen de la velocidad de la red, debido a que muchas empresas e instituciones como SUNARP al sentir un bajo rendimiento de su red optan en comprar un mayor ancho de banda o en peores casos optan por la compra innecesaria de equipos muy costosos.

1.3 DELIMITACIÓN DEL PROYECTO

1.3.1. Teórica

Netflow es un protocolo que se encarga de brindar estadísticas respecto al tráfico de paquetes IP que fluye a través de todos los dispositivos de red.

La calidad de servicio (Qos) es una expresión que se usa para explicar la ideonidad de una red para organizar el tráfico y evitar que este se congestione.

1.3.2. Temporal

Se desarrolló entre el 12 de Octubre hasta el 22 de Noviembre del 2019

1.3.3. Espacial

La propuesta para mejorar el rendimiento de la red LAN de SUNARP se realizó en la sede Huancayo, ubicada en Jr. Arequipa N° 240 - El Tambo, en el departamento de Junín.

1.4 FORMULACIÓN DEL PROBLEMA

1.4.1. Problema General

¿Cuál es el nivel de la calidad de servicio y la influencia del protocolo Netflow en la propuesta de mejora del rendimiento de la red LAN en una sede de la Superintendencia Nacional de Registros Públicos?

1.4.2. Problemas Específicos

- ¿Cuál es el nivel de QoS en la red LAN de la Superintendencia Nacional de Registros Públicos?
- ¿Cuál es la influencia del protocolo Netflow en la red LAN de la Superintendencia Nacional de Registros Públicos?
- ¿De qué forma la herramienta Netflow Traffic Analyzer resultará util para el monitoreo del tráfico de la Red LAN de la SUNARP?

- ¿Qué usuarios consumen un mayor consumo de ancho de banda en la red LAN de la Superintendencia Nacional de Registros Públicos?
- ¿En qué horario se presenta un mayor consumo de ancho de banda en la red LAN de la Superintendencia Nacional de Registros Públicos?
- ¿Cómo podríamos verificar que la propuesta de configuración del protocolo Netflow y la calidad de servicio mediante la priorización de tráfico no sufrirá complicaciones al momento de ser configurado en router principal de SUNARP?

1.5. OBJETIVOS

1.5.1. Objetivo General

Determinar la calidad de servicio y la implementación del protocolo Netflow para mejorar el rendimiento de la red LAN de la Superintendencia Nacional de Registros Públicos.

1.5.2. Objetivos Específicos

- Determinar el nivel de QoS en la red LAN de la Superintendencia Nacional de Registros Públicos.
- Determinar la influencia de la implementación del protocolo Netflow en la red LAN de la Superintendencia Nacional de Registros Públicos.
- Explicar cómo la utilización de la herramienta Netflow Traffic Analyzer ayudará a obtener mayor información de la Red LAN de la Superintendencia Nacional de Registros Públicos.
- Determinar los usuarios que realizan un mayor consumo de ancho banda en la red LAN de la Superintendencia Nacional de Registros Públicos.
- Determinar el horario donde se consume un mayor ancho de banda en la red LAN de la Superintendencia Nacional de Registros Públicos.
- Realizar una simulación que permita comprobar que la propuesta brindada es apta para ser aplicada en la vida real.

CAPÍTULO II
MARCO TEÓRICO

2.1. ANTECEDENTES

2.1.1 Antecedentes Internaciones

Cristian, Villadiego (2003). “Técnicas de optimización del ancho de banda en las redes LAN-PARTE II”. El autor de esta tesis llegó a las siguientes conclusiones:

La latencia y la granularidad en las redes LAN s son los principales problemas que reducen el ancho de banda en una red.

Con el proyecto realizado se minimizarán los costos de la optimización del ancho de banda para las empresas e universidades que deseen tener un mejor rendimiento de su red; evitando así la compra innecesaria de equipos costosos para desempeñar las mismas funciones que los equipos anteriores.

El uso inadecuado del ancho de banda en los diferentes equipos de la red LAN como los routers y switches afectan al rendimiento de la red.

La calidad de servicio (QoS) facilitara la asignación del ancho de banda y hará que el trabajo de los administradores de red al implementar la solución propuesta, sea más sencillo y ventajoso.

La referida tesis hace alusión a la optimización del ancho de banda a través de la calidad de servicio, enfocándose en la granularidad y latencia debido a que para los autores estos dos factores son los que más influyen en el rendimiento de la red, ocasionando un 100% de pérdida de paquetes. Los resultados del estudio de este trabajo permitieron comprender los diferentes problemas que afectan al ancho de banda en una red LAN así como también las políticas y configuraciones que brindan para optimizarla. Por este antecedente se busca agregar como técnica el protocolo Netflow, el cual permitirá identificar el dispositivo que consume un mayor ancho de banda en la red LAN de la SUNARP. (Cristian Villadiego Angulo, 2003).

Edgar, Morales (2013). “Análisis del protocolo Netflow y su aplicación en la determinación del nivel de uso de la red de datos de la Facultad de Mecánica”. El autor de esta tesis llegó a las siguientes conclusiones:

> Gracias a la implementación del protocolo Netflow y la herramienta Netflow Analyzer, se pudo observar luego del análisis de flujos que el periodo de mayor consumo es el de la mañana.
>
> Se determinó gracias a la implementación del protocolo Netflow que las computadoras con las direcciones IP 172.30.102.50 y 172.30.102.78 generan en total un tráfico de 176420.33 Megabytes que corresponde al 37% del tráfico total de la red.
>
> Con los resultados obtenidos se desprende que el porcentaje proyectado de crecimiento del número de paquetes sobre la red de datos de la Facultad de Mecánica para el próximo mes será del 59.07% con relación al mes anterior; lo que significa que para diciembre del año 2012 el uso de la tasa de reenvio de paquetes del switch Cisco 3560G será del 0.18%.

La referida tesis hace alusión al análisis del protocolo Netflow y a la herramienta Netflow Traffic Analyzer para determinar el periodo de tiempo donde más se consume el ancho de banda y para saber que dispositivos son los que generan un mayor tráfico en la red de la Escuela Superior Politécnica de Chimborazo – Ecuador. Los resultados de este análisis permitieron verificar que los dispositivos con IP 172.30.12.50 y 172.30.102.78 eran los que consumían más de 37% del tráfico total de la red, además permitieron un correcto monitoreo del tráfico de su intranet. Por este antecedente nació la idea de la propuesta de aplicar el protocolo Netflow y la herramienta Netflow Traffic Analyzer en la red LAN de SUNARP. (Edgar Morales Muchagalo, 2013).

2.1.2. Antecedentes Nacionales

Julio, Molina (2012). *"*Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la Empresa Editora El Comercio – Planta Norte". El autor de esta tesis llegó a las siguientes conclusiones:

> La proyección de crecimiento de la Planta Norte es de 16% anual, donde actualmente se cuenta con 50 terminales. Se implementó y configuró la red para soportar este promedio de crecimiento sin afectar el rendimiento de la LAN, gracias a los lineamientos de la metodología adoptada. Con lo que es posible conectar otros switch Cisco de 48 puertos hacia el switch Core y responder a la tasa de crecimiento con una velocidad de 100/1000 Gbps en cada troncal. Con ello se concluyó que el objetivo de la escabilidad fue posible.

La velocidad o tasa de transferencia de datos está operando dentro de los rangos esperados, gracias a la implementación de técnicas de balanceo y priorización de tráfico con QoS, el cual se configuró en los dispositivos que consumen mayor ancho de banda (Teléfonos IP, PC´s periodistas y Preprensa), identificándose tipos de paquetes (Voz, Datos y Video) para reservar un ancho de banda de origen a destino donde los equipos detectan el tráfico de datos relevantes y lo gestionan con mayor prioridad (Video y Voz).

El tráfico de voz también se optimiza debido a la configuración de priorización en el tráfico con el estándar IEEE 802.1p, lo cual indica a los switches jerarquizar la transmisión de la data mediante la gestión de las colas de estas tramas.

Se ha implementado mecanismos para autenticación de los accesos a servicios y recursos de red a través de roles y perfiles de usuario, como RADIUS que trabaja con Active Directory, lográndose un mejor nivel de seguridad, dado que los filtros son más rigurosos gracias a las capas de seguridad que brinda Radius. Asimismo, se modificaron privilegios de usuarios en el Active Directory, para estar alineados al nuevo esquema de trabajo en red y uso de recursos.

La referida tesis plantea un rediseño de la configuración de la red haciendo uso de la calidad de servicio (QoS) y la segmentación por VLAN´s dado que el diseño inicial no cuenta con todas las políticas y configuraciones necesarias para un correcto rendimiento de la red provocando de este modo la existencia de latencia y degradación de servicio en horas pico en la Empresa Editora El Comercio, llegando a alcanzar un pico máximo de latencia de 1300 ms. Los resultados de esta tesis demostraron una vez más que la Calidad de Servicio (QoS) nos ayuda a mejorar el rendimiento de la red debido a la buena priorización del tráfico IP que se realizó en esta tesis, en donde se verifica que se priorizo el tráfico de Prensa ya que esta

presenta un mayor número de empleados; resolviendo de esta manera la latencia y el bajo rendimiento que presentaba inicialmente la red, por otro lado también se demostró que la implementación de VLAN´s brinda varios beneficios el cual entre los más importantes tenemos a la segmentación de la red y la seguridad en la capa de Red. La importancia de este antecedente es que aporta la implementación de VLAN´s como una técnica para optimizar el ancho de banda de SUNARP, además del uso de Calidad de Servicio (Qos) donde explica más a fondo la priorización del tráfico IP para un mejor rendimiento de la red. (Julio Molina Ruiz, 2012).

2.2. BASES TEÓRICAS

2.2.1 Protocolo de Red

El protocolo de red es un término que se emplea para nombrar a las normativas y los criterios que fijan cómo deben comunicarse los diversos componentes de un cierto sistema de interconexión. Esto quiere decir que, a través de este protocolo, los dispositivos que se conectan en red pueden intercambiar datos. Es así que se entiende que un protocolo es un sistema de reglas que hacen posible la comunicación entre dos o más equipos que manejan un diferente lenguaje (Perez y Merino, 2015).

2.2.2. Modelo TCP/IP

El modelo TCP es un protocolo que usa en las comunicaciones en redes con el fin de que un equipo pueda lograr comunicarse dentro de una red. Este modelo en 1983 se convirtió en el modelo estándar para la comunicación en redes. El modelo TCP/IP hace posible el intercambio de datos siguiendo un sistema jerárquico de 4 capas (Robledano, 2019). En la tabla 1.1 podemos observar las 4 capas del modelo TCP/IP y los protocolos con el que se identifican.

Tabla 1: Capas TCP/IP

CAPA	NOMBRE	PROTOCOLOS
4	Aplicación	HTTP - SSH
3	Transporte	UDP - TCP
2	Red	IP-ICMP
1	Físico	MEDIO FÍSICO

Fuente: Elaboración Propia

2.2.2.1. Capa de Aplicación

Esta capa hace referencia a las aplicaciones y servicios que pueden ser utilizados por un usuario. Estos servicios de internet hacen uso de la capa de transporte para poder enviar y recibir datos (Echeverria, 2008).

2.2.2.2. Capa de Transporte

Esta capa se encarga de ver que los paquetes sean enviados sin errores y en un debido orden para no producir alguna colisión (Juncosa, 2018)

2.2.2.3. Capa de Red

Esta capa se encarga de proporcionar los paquetes datos a la red. El protocolo IP es el protocolo más importante de esta capa ya que se encarga de declarar la dirección IP para determinar la ruta que debe seguir el paquete, el cual va ser fragmentado para que pueda ser transmitido sin ninguna pérdida de información (Juncosa, 2018).

2.2.2.4. Capa Física

La capa física hace referencia a las características físicas del medio de comunicaciones (Llamas, 2016).

2.2.3. Router

El Router es un hardware que hace posible la interconexión de computadoras dentro de una red. Su principal función es determinar la mejor ruta de los paquetes al momento de ser enviados a través de la red de datos". Existen varios tipos de routers, los routers básicos no aguantan ciertos protocolos por ser de muy bajos costos, usualmente estos tipos de routers son de uso doméstico; sin embargo los routers sofisticados suelen ser usados por grandes empresas ya que estas necesitan usar los diferentes protocolos que ayudan a la optimización de la red (Merino, 2010).

2.2.4. Switch

Un dispositivo Switch es un hardware que permite la conexión de varios elementos como las PC, las impresoras, los Access Point dentro de una red. Existen switches de gama alta más conocidos como Switches de capa 3 que además de ser administrables permiten la utilización de VLAN`s, la utilización de funciones de enrutamiento IP, el control de bucles, la monitorización de puertos y seguridad IEEE 802.1X. (Gonzales, 2013).

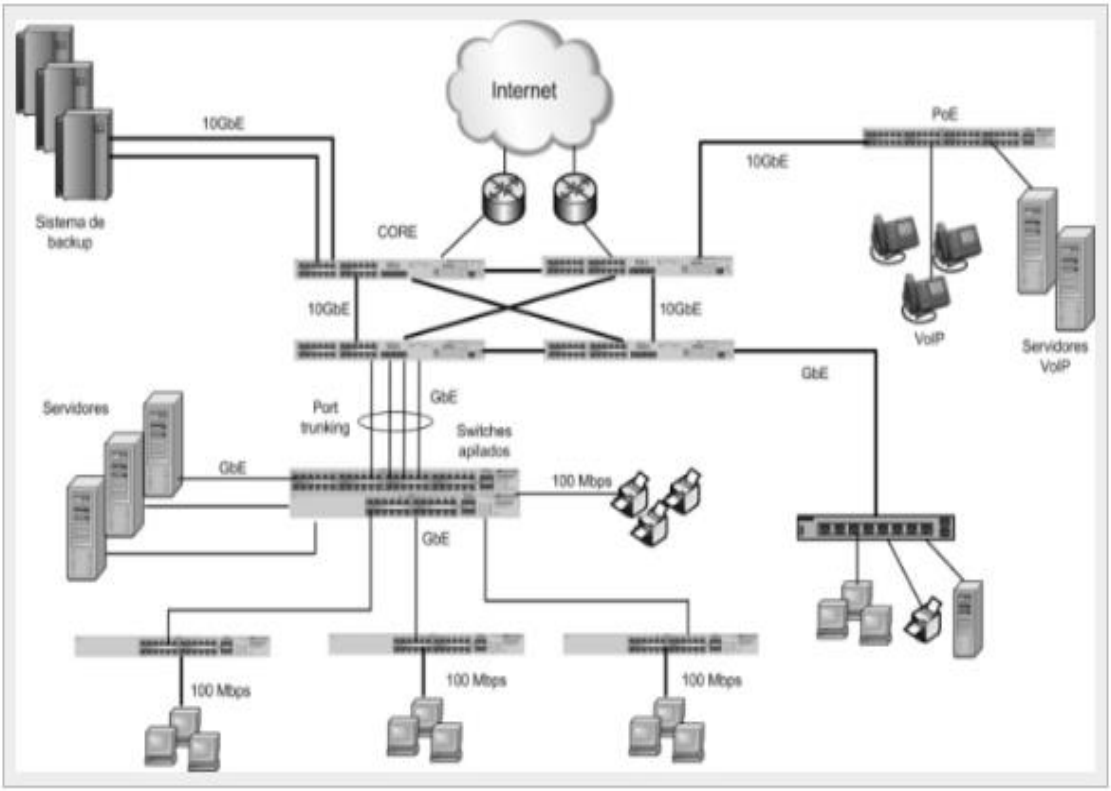


Figura 2: Estructura Jerárquica de Switch capa 3
Fuente: Ms. Gonzales

2.2.5. Protocolo Netflow

Netflow es un protocolo que fue desarrollado por CISCO SYSTEM en el año 1990, su principal función es recolectar la información del tráfico IP que fluye a través de nuestra red para posteriormente enviarlos mediante datagramas UDP o SCTP hacia algún colector NETFLOW. Asimismo el protocolo Netflow permite obtener información del consumo del ancho de banda y cuellos de botella convirtiéndolo así uno de los mejores protocolos para el monitoreo del tráfico de red (Morales,2017).

2.2.5.1 Caché de Netflow

En redes, el termino caché hace referencia a una memoria que se encarga de almacenar datos. Netflow trabaja con la información de flujos los cuales están dentro de una caché. Estos caché son enviados a un servidor de colector de flujos mediante dispositivos como routers y switches con la finalidad de recopilados posteriormente por un software(Rodríguez, 2015).

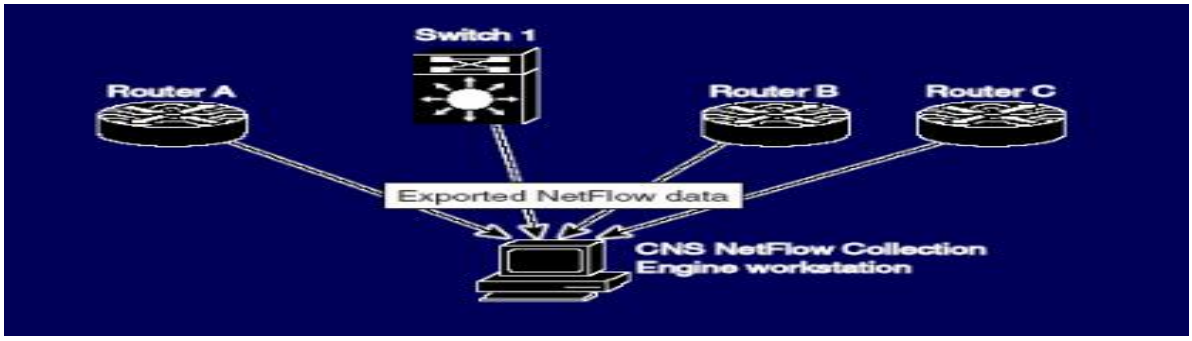


Figura 3: Diseño de exportación del Caché
Fuente: Humberto Rodríguez Jorge

2.2.5.2 Flujo de Netflow

Según Rodríguez (2015) se puede definir flujo como “Una cadena unidireccional de paquetes entre una determinada fuente y un destino, ambos definidos por una dirección IP de la capa de red y también por números de puertos origen y destino en la capa de transporte”(p.7).Un flujo está definido por 7 campos:

- Dirección IP de origen
- Dirección IP de destino
- Número de puerto de origen
- Número de puerto de destino
- Tipo de protocolo de capa 3
- Marca de tipo de servicio (ToS)
- Interfaz Lógica de entrada

  Referente a estos 7 campos, Walton (2018) afirma:

  Para NetFlow, que se basa en TCP/IP, las direcciones IP de capa de red y los números de puerto de origen y destino de capa de transporte definen el origen y el destino. Los primeros cuatro campos que usa NetFlow para identificar un flujo se deberían conocer. El tipo de protocolo de capa 3 identifica el tipo de encabezado que sigue al encabezado IP (generalmente TCP o UDP). El byte ToS en el encabezado de IPv4 contiene información sobre cómo los dispositivos deben aplicar las reglas de calidad de servicio (QoS) a los paquetes en ese flujo. (p.4)

2.2.5.3 Arquitectura Netflow

Para el correcto funcionamiento del protocolo Netflow se requiere una arquitectura muy específica, dicha arquitectura debe contar con los siguientes elementos: El primer elemento que conforma esta estructura es un router, el cual se encargará de informar de todo tráfico que pasa a través del mismo. El segundo elemento que conforma esta estructura es el colector, el cual tendrá como principal función la recopilación de información que ha fluido a través del router. El tercer elemento que conforma esta estructura es un software, el cual tiene como principal función organizar y elaborar un informe de toda la información que ha recopilado el colector Netflow, para que posteriormente sea brindado a todos los administradores o usuarios de la red (Espinal, 2016).

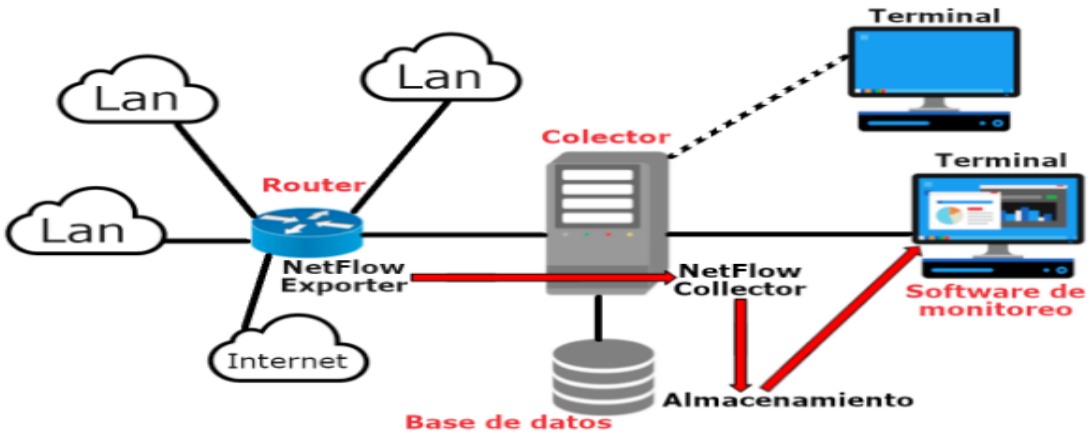


Figura 4: Arquitectura Netflow
Fuente: Juan. M Espinal

2.2.5.4 Hardware que soporta Netflow

Los routers CISCO son dispositivos que soportan el protocolo Netflow. Cabe recalcar que los routers CISCO no son las únicas marcas de routers que soportan este protocolo, también se encuentran las marcas: Alcatel, Huawei, Enterasys, Foundry y Juniper. En la figura 5 se mostrará los modelos de los routers CISCO los cuales son una de las marcas más usadas por las compañías.

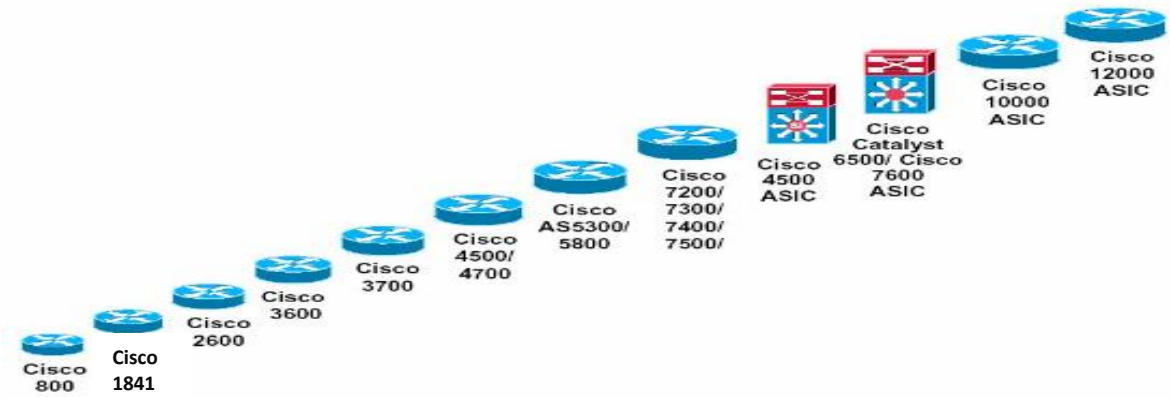


Figura 5: Hardware que soportan Netflow
Fuente: Humberto Rodríguez Jorge

2.2.5.5 Configuración Netflow

Para que el protocolo Netflow funcione correctamente, en primer lugar se debe entrar al router Cisco y estar en modo privilegiado, en segundo lugar se debe entrar en modo configuración y poner la interfaz que se desea configurar para que fluya todo el tráfico, en tercer lugar se debe habilitar el flow y se debe elegir la versión del protocolo con el que se trabajara. Por último se debe configurar el lugar a donde se dirigirán todos los paquetes, en este caso al colector Netflow, así como también la interfaz de entrada por donde entra todo el tráfico(Leopoldo,2009). En la figura 6 se muestra el modelo de configuración más detallado

.

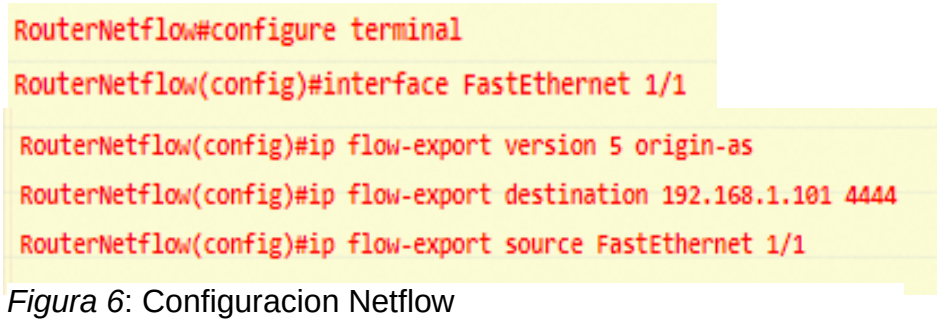


Figura 6: Configuracion Netflow
Fuente: José Leopoldo(2009)

2.2.5.6 Configuración Netflow Top Talkers

La configuracion del Netflow Top Talkers forma parte de la configuracion del Netflow, esta configuracion permite identificar los usuarios que consume un mayor ancho de banda. En la figura 7 se muestran los pasos para configurar Netflow Top Talkers el cual varia según la interfaz por entra el tráfico y de la cantidad usuarios que se desea visualizar en el listado(Rodriguez,2016).

Configuración de Netflow

```
Router(config)# interface GigabitEthernet1/0
Router(config-if)# ip flow ingress
Router(config-if)# ip flow egress
```

Configuración de Netflow Top Talkers

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 50
Router(config-flow-top-talkers)# sort-by [packets|bytes]
```

Figura 7: Configuración de Netflow Top Talkers

Fuente: Rolando Rodriguez (2016)

2.2.5.7 Versiones de Netflow

En la actualidad existen 10 versiones del protocolo Netflow: La versión 5 es la versión estándar, las versiones comprendidas entre el 1 y el 4 son exclusividad de cisco y la versión 9 es la que brinda mayor compatibilidad con diferentes dispositivos permitiendo de esta manera la transmisión en distintos formatos de Netflow (Morales, 2013). En la tabla 1.1 se muestra las características respecto a las versiones más utilizadas.

Tabla 2: Características de las versiones Netflow

VERSIONES	COMENTARIO
1	VERSIÓN ORIGINAL, ESTA VERSIÓN SOLO SOPORTA ROUTER CISCO
5	VERSIÓN ESTANDARIZADA, ESTA VERSIÓN SOLO SOPORTA IPV4
7	VERSIÓN EXLUSIVA PARA SWITCH CISCO 6500 Y 7600
8	ESTA VERSIÓN PERMITE COMPATIBILIDAD ENTRE SWITCH
9	VERSIÓN MÁS UTILIZADA DEBIDO A SU MÚLTIPLE COMPATIBILIDAD

Fuente: Elaboración propia

2.2.6. Monitoreo de red

Es una técnica que se usa para visualizar todo el tráfico que fluye a través de una red, esta técnica sirve de apoyo para los administradores ya que reporta enlaces caídos y detecta anomalías dentro de una red. En la actualidad existen programas de monitoreo como el Netflow y el Nagius que apoyan con la detección de enlaces caídos y en el monitoreo del tráfico IP. Para monitorear una red existen dos puntos de enfoques: activo y pasivo (Morales, 2013, p.13).

2.2.6.1. Monitoreo Activo

El monitoreo activo se realiza con la inyección de paquetes a la red o realizando un envío de paquetes de prueba a distintas aplicaciones midiendo el tiempo de respuesta. Este enfoque es usualmente utilizado con la finalidad de saber cuál es el rendimiento de la red. Las técnicas utilizadas para el monitoreo activo son 3: La primera se basa en ICMP, con este técnica se podrá detectar las pérdidas de paquetes. La segunda se basa en TCP, con esta técnica se podrá verificar la tasa de transferencia y la tercera técnica se basa en el protocolo UDP, con esta técnica visualizaremos el traceroute (Morales, 2013).

2.2.6.2. Monitoreo Pasivo

El monitoreo pasivo se basa en recopilar los datos del tráfico que fluyen a través de la red mediante dispositivos con soporte netflow. A comparación del trafico activo este tipo de monitoreo se usa para registrar el tráfico de la red. Las técnicas utilizadas para el monitoreo pasivo son 2: La primera se da mediante solicitudes remotas, la cual a través de SNMP permite tener estadísticas del consumo de ancho de banda y reportes de un evento inusual. La segunda técnica se da mediante captura de tráfico, en donde el dispositivo de red mediante previa configuración de un puerto va a enviar todo el tráfico hacia un software que realizara la captura y la recopilación de información (Morales, 2013).

2.2.6.3 Netflow Traffic Analyzer

Netflow Traffic Analyzer es una herramienta de monitoreo de redes que se basa en el protocolo Netflow de Cisco, el cual ofrece una visión en tiempo real del tráfico, además de esto también permite verificar el rendimiento, la latencia, la disponibilidad y la pérdida de paquetes de la red LAN. Entre las características más importantes tenemos: Alertas personalizables, informes de utilización de ancho de banda, informes de tráfico e informaciones a medida (Morales, 2013).

2.2.7 Calidad de Servicio (QoS)

La calidad de servicio (Qos) es una expresión que se usa para explicar la ideonidad de una red al momento de priorizar el tráfico con el fin de evitar que este se congestione (Brent,2002). Para Martínez (2017) Calidad de Servicio se define como: “Un conjunto de requisitos de servicio que la red debe cumplir para asegurar un nivel de servicio adecuado para la transmisión de los datos” (p.5). En la figura 8 visualizamos un claro ejemplo de la importancia de QoS.

Figura 8: Calidad de Servicio
Fuente: Mac Josán(2018)

2.2.7.1 QoS y sus ventajas

Las principales ventajas que QoS puede brindar a una red son: La capacidad de priorización del tráfico y la mayor fiabilidad en la red, ya que QoS permite dar

prioridad a los flujos más importantes, así como también permite tener un mayor control de la cantidad de ancho de banda que una aplicación puede utilizar (Martínez, 2017).

2.2.7.2 Congestión

La congestión es un fenómeno que se provoca cuando una interfaz recibe más tráfico del que puede soportar, debido a esto se generan los retrasos en la red; a estos retrasos se le conoce como latencia (Colomés, 2017).

2.2.7.3 Latencia

La latencia es el tiempo que demora un paquete en trasmitirse dentro de una red (Soto, 2018).

2.2.8 Modelos de Calidad de Servicio

Martínez (2017) afirma que existen 3 mecanismos básicos para mejorar el rendimiento de la red: Best-effort, IntServ y DiffServ.

2.2.8.1 Best-effort

Para este mecanismo no es necesario algún cambio en la red ya que su solución para mejorar el rendimiento de la red es en optar un mayor ancho de banda de modo que sea suficiente para la carga del tráfico (Martínez, 2017). Este mecanismo no es muy recomendado ya que frente a los protocolos codiciosos es muy limitado debido a que estos aumentan la cantidad de datos hasta que todo el ancho de banda se consuma y pierda los paquetes de los diferentes servicios (Yuksel,Ramakrishnan,Houle,Sadhvani, 2007).

2.2.8.2 Servicios Integrados (IntServ)

Es una arquitectura que tiene como objetivo brindar garantías QoS a los flujos. En este modelo de arquitectura las aplicaciones utilizan el protocolo RSVP para

reservar recursos mediante la red. InstServ para poder gestionar el tráfico y poder brindar transporte con QoS emplea 3 funciones:

- Control de Admisión: Determina si existe recursos suficientes para el flujo.
- Atención en cola: Determina el paquete siguiente que va ser enviado.
- Política de descarte: Se usa para gestionar el paso del tráfico.

IntServ consta de 2 clases de servicio: Servicio garantizado y Servicio de carga Controlada (Matango, 2016).

2.2.8.2.1 Servicios garantizados

Este servicio se caracteriza por no presentar perdidas en la colas es decir te garantiza que los datos lleguen a su destino, el problema de este servicio es que pueden presentar grandes retardos (Matango,2016).

2.2.8.2.2 Carga controlada

Este servicio se caracteriza por brindar varios paquetes hacia su destino con un retardo bajo, sin embargo no te garantiza del todo ya que puedes tener pérdidas de paquetes (Matango, 2016).

2.2.8.2.3 RSVP

El protocolo de reserva de recursos es el protocolo usado en los servicios integrados para que las aplicaciones puedan determinar y liberar ancho de banda. RSVP lo pueden usar los routers y los host con el fin de pedir y brindar niveles determinados de QoS para los flujos de datos de las aplicaciones. El problema con este protocolo es que es muy poco eficiente si se tiene un alto número de flujos (Martínez, 2017).

2.2.8.3 Servicios Diferenciados (DiffServ)

Esta arquitectura clasifica los paquetes en distintas clases, cada paquete que pasa es marcado por una clase, estos mismos tendrán una prioridad al momento de

pasar de un router a otro. DiffServ contiene una tabla de prioridades dependiendo a qué clase de paquete recibe el router este recibirá una mayor prioridad (Matango, 2016).

2.2.9. Tipos y Perfiles de tráfico

2.2.9.1 Tráfico Elástico

El tráfico Elástico se puede adaptar a la variación del rendimiento y el retardo de una red basada en TCP/IP. Entre los tipos de tráfico elástico se encuentran: Transferencia de archivos, correo electrónico, conexión remota y acceso a la web (Martínez, 2017). En la tabla 3.1 se verifica la sensibilidad de los tipos de tráfico elástico.

Tabla 3 : Tipos de Tráfico

Tipo de Tráfico	Comentario
Transferencia de archivos	Dependiendo al tamaño sera sensible a retardos
Correo Electrónico	Insensible al momento de variaciones de retardo
Conexión Remota	Sensible a retardos
Acceso a la Web	Sensible a retardos

Fuente: Elaboración propia

2.2.9.2 Tráfico no Elástico

El tráfico de Voz y Audio es un tráfico no elástico que no se adapta a la alteración del rendimiento y el retardo de una red; por ende es necesario un mecanismo que otorgue prioridad a las aplicaciones que son más importantes. Estas aplicaciones no elásticas no pueden reducir su ancho de banda para enfrentar la congestión ya que tienen un tráfico en tiempo real, por ende se recomienda usar las políticas de Control de Calidad de Servicio (Martínez, 2017). En la figura 9 se verifica la comparación de la sensibilidad frente a retardos, donde se hace referencia a los perfiles de tráfico:

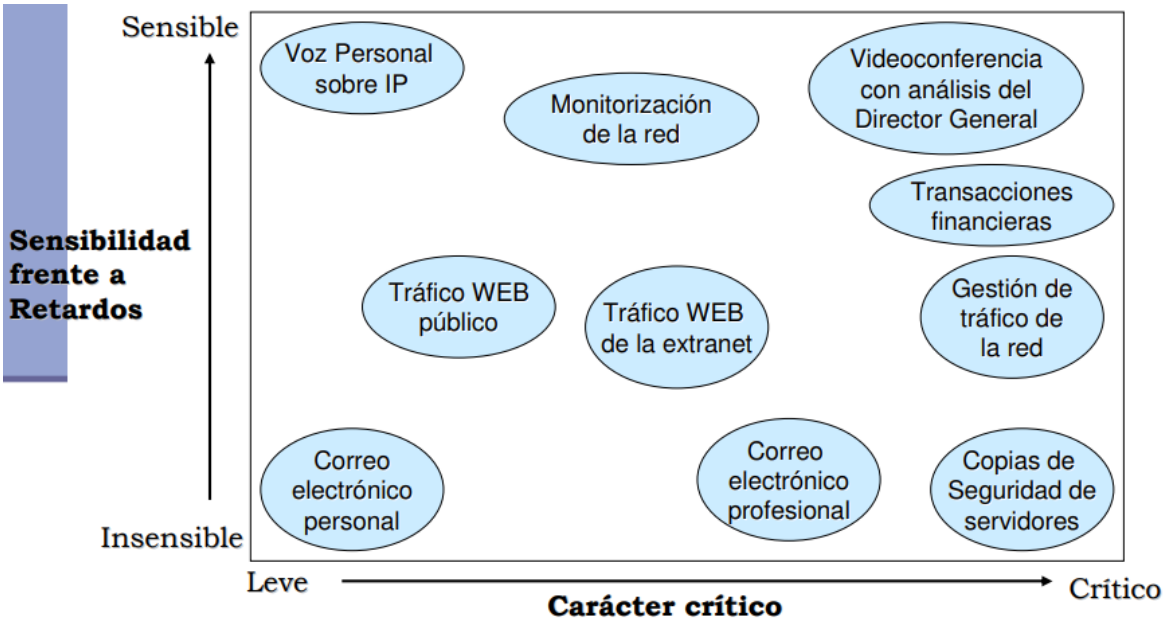


Figura 9: Sensibilidad frente a retardos
Fuente: Juan Martínez (2017)

2.2.9.3 Voz sobre IP

La voz sobre IP es un tráfico que relativamente es predecible ya que una llamada telefonica consume de 30 a 100 Kbps, la voz sobre IP trabaja con el protocolo UDP ya que se requiere un rápido procesamiento de información (Colomés, 2017).

2.2.9.4 Video sobre IP

El tráfico Video sobre IP es impredecible ya que se genera un aumento de ancho de banda por la funcionalidad del infrarrojo que tienen instalado. Este tipo de tráfico es sensible a la latencia y puede consumir entre 20 a 30 Mbps (Colomés, 2017).

2.2.9.5. Tráfico de Datos

Este tipo de tráfico trabaja con TCP ya que se requiere que la información llegue a su destino sin pérdidas. Este tráfico es insensible a la latencia ya que no le afecta que la entrega de datos se demore unos segundos más con tal que se la información llegue completa (Colomés, 2017).

2.2.10. Políticas de Calidad de Servicio: Encolamiento

La calidad de servicio se basa en el concepto de encolamiento, hay distintos tipos de encolamiento, entre los principales tenemos: FIFO, WFQ, CBWFQ, LLQ, CBWFQ/LLQ.

2.2.10.1 FIFO

Las colas de tipo FIFO(First In, First Out), son las colas que se caracterizan por la orden de llegada esto quiere decir que el paquete que llegue primero es el primero que sale. FIFO es ideal en una red de mínima congestión y un gran ancho de banda. En la figura 10 se muestra cómo funciona este tipo de cola (Colomés, 2017).

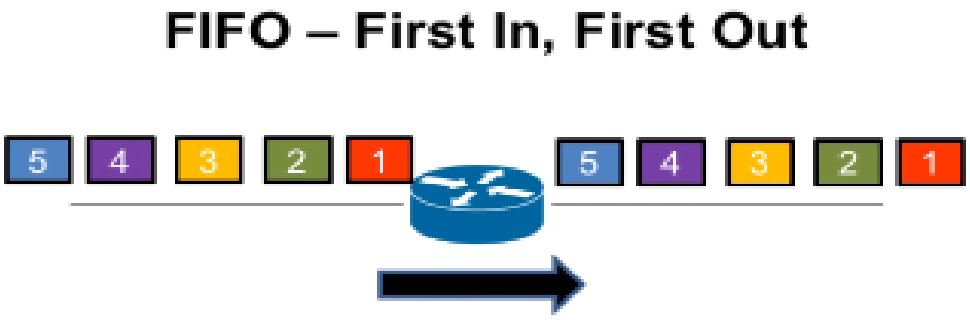


Figura 10 : FIFO
Fuente: Paulo Colomés(2017)

2.2.10.2 WFQ

Las colas de tipo Weighted Fair Queuing son un método de priorización automática que se encargan de clasificar el tráfico en forma dinámica, la idea de este método es evitar que un flujo consuma todo el ancho de banda. El problema de este método es que no funciona con tráfico encriptado ya que WFQ necesita ver el contenido del paquete y su peso para la toma de decisión al momento de clasificarlo. En la figura 11 se muestra cómo funciona este tipo de cola (Colomés, 2017).

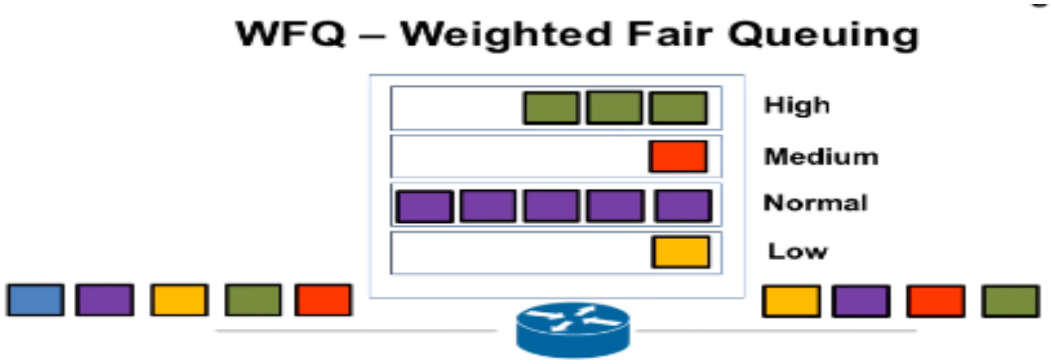


Figura 11: WFQ
Fuente: Paulo Colomés (2017)

2.2.10.3 CBWFQ

Este método se basa en WFQ sin embargo, este método utiliza los Access List para definir manualmente las clases de tráfico que van a tener prioridad. Estas clases de tráfico van a tener un ancho de banda garantizado al momento de periodos de congestión. En la figura 12 se muestra cómo funciona este tipo de cola (Colomés, 2017).

Figura 12 : CBWFQ
Fuente: Paulo Colomés (2017)

2.2.10.4 LLQ

Low Latency Queuing es un método que brinda mecanismos de prioridad para paquetes sensibles a la latencia como VoIP, haciendo posible que estos paquetes sean enviados antes que otras colas. En la figura 13 se muestra cómo funciona este tipo de cola (Colomés, 2017).

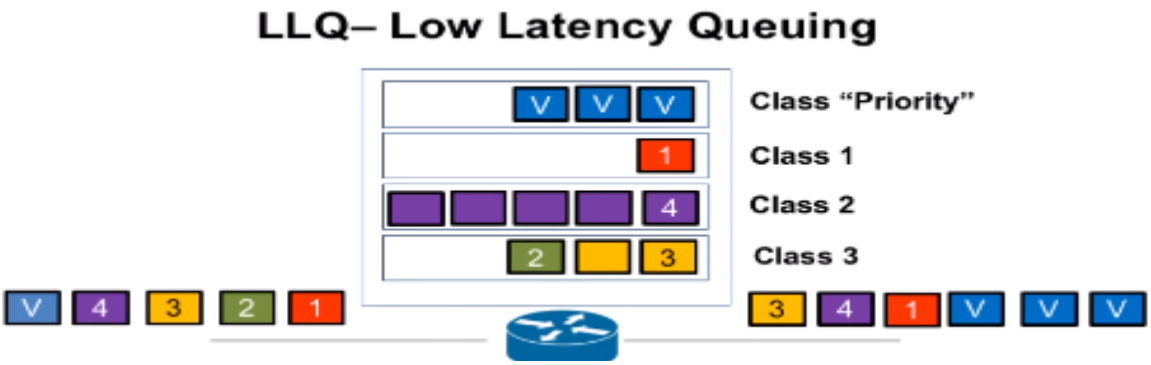
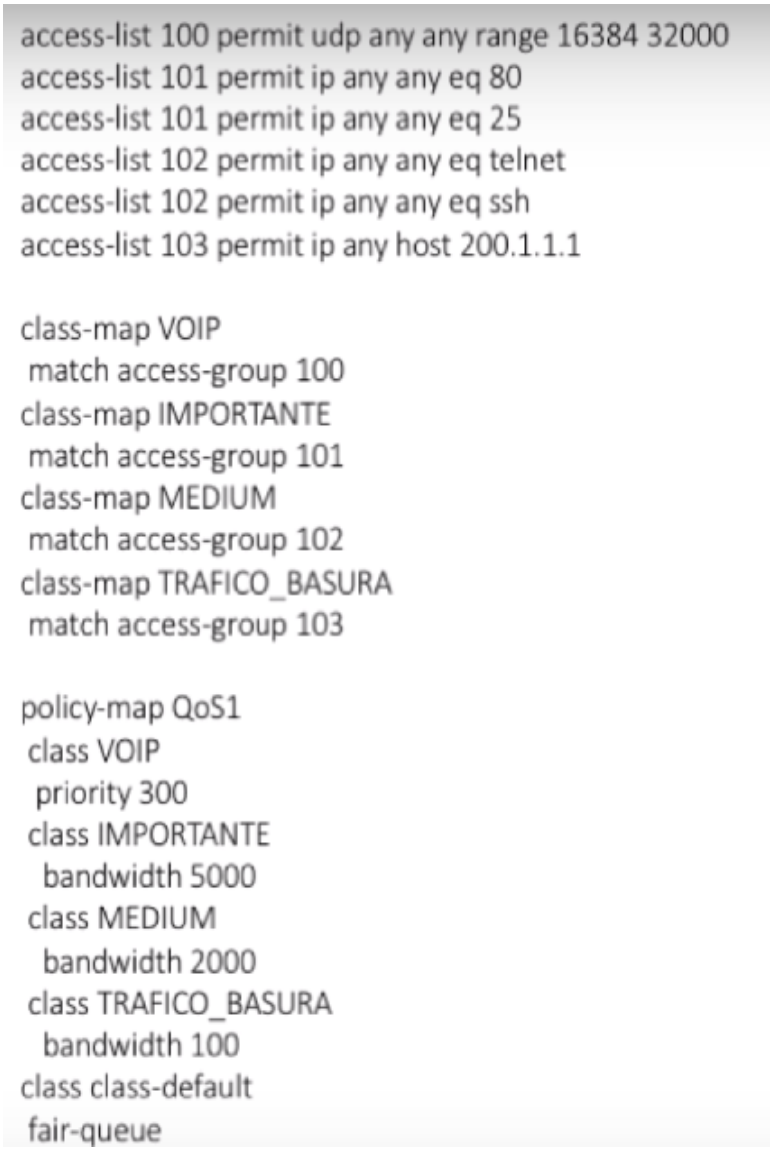


Figura 13: LLQ
Fuente: Paulo Colomés (2017)

2.2.10.5 CBWFQ con LLQ

Este método involucra tanto a CBWFQ y LLQ, el cual permite brindar un ancho de banda garantizado a ciertos tipos de tráficos y a la vez brindar una prioridad de ancho de banda a un tráfico sensible a la latencia (Colomés, 2017).En la

figura 14 se muestra un ejemplo de la configuración del método CBWFQ con LLQ haciendo referencia a la clasificación de las políticas.



```
access-list 100 permit udp any any range 16384 32000
access-list 101 permit ip any any eq 80
access-list 101 permit ip any any eq 25
access-list 102 permit ip any any eq telnet
access-list 102 permit ip any any eq ssh
access-list 103 permit ip any host 200.1.1.1

class-map VOIP
 match access-group 100
class-map IMPORTANTE
 match access-group 101
class-map MEDIUM
 match access-group 102
class-map TRAFICO_BASURA
 match access-group 103

policy-map QoS1
 class VOIP
  priority 300
 class IMPORTANTE
   bandwidth 5000
 class MEDIUM
   bandwidth 2000
 class TRAFICO_BASURA
   bandwidth 100
class class-default
 fair-queue
```

Figura 14: CBWFQ con LLQ
Fuente: Paulo Colomés (2017)

2.3. Definición de términos básicos

1) Ancho de banda: Es la cantidad de datos que pueden ser enviados a través de la red en un periodo de tiempo determinado (Quiñones, 2016).

2) Rendimiento: Son las medidas que permiten saber si la red está operando en forma óptima (Alegsa, 2018)

3) Retardos: Mide el tiempo entre el envió de un mensaje por el usuario de origen y su recepción por el usuario destino (Martínez, 2017)

4) Paquetes: Son los datos enviados por los dispositivos durante una conexión (Stopford, 2009).

5) Red LAN: Una Red LAN permite la conexión de varios dispositivos para enviar, recibir y compartir archivos en un área pequeña (Estela, 2018).

6) PING: Es una prueba de diagnóstico que ayuda a comprobar el estado de comunicación del emisor con los diferentes equipos de la red (Muus, 2012).

7) Disponibilidad: Hace referencia al servicio operativo con absoluta continuidad operacional en un periodo de tiempo (Piedras, 2015).

8) Pérdida de Paquetes: Es la cantidad de paquetes que son descartados en la red producto a una alta congestión (Pandora, 2019).

9) ICMP: Protocolo de control de mensajes de Internet el cual es utilizado con el fin de enviar mensajes de información indicando que un host o servicio no está siendo localizado. (Villagomez, 2018).

10) TCP: Es el protocolo de control de transmisión que brinda un servicio fiable ya que permite que los mensajes lleguen sin inconvenientes a su destino; además este protocolo permite un control de congestión con el fin de no colapsar la red (De Luz, 2011).

11) UDP : Es el protocolo de datagramas de usuario, el cual brinda un servicio no fiable, debido a que intentará que los datos lleguen a su destino por todos los medios posibles; pero no lo garantiza al 100% ya que se recibirá ninguna confirmación de recepción. A diferencia del TCP este protocolo no brinda un control de congestión del tal manera enviará los datos a cualquier velocidad provocando una posible saturación. Este protocolo se utiliza más para la transmisión de voz y video ya que en estos casos es más importante transmitir con mayor velocidad que esperar que todos los bytes lleguen al destino (De Luz,2011).

12) Packet Tracer: Es un software que permite la simulación de redes con el fin de experimentar el comportamiento de la red (Torres,2015).

CAPÍTULO III
DESARROLLO DEL TRABAJO DE SUFICIENCIA PROFESIONAL

3.1 Modelo de Solución Propuesto

La solución que se propone para mejorar el rendimiento de la red LAN de SUNARP se basa en la implementación del protocolo Netflow y en la priorización del tráfico gracias a la calidad de servicio.

En primer lugar se simulará en Packet Tracer un diseño modelo de la red LAN de SUNARP-Junín, el cual contará con una PC y un teléfono IP de prueba para cada área. Una vez elaborado el modelo se procederá con la configuración de las políticas de priorización y el protocolo Netflow con el objetivo de verificar si esta configuración afecta de alguna manera a la conectividad entre equipos.

Realizando esta simulación se podrá verificar si nuestra propuesta respecto a la configuración de políticas de priorización y la configuración del protocolo Netflow es apta, por ende no surgirá ninguna complicación al momento de ser configuradas en el router de SUNARP- JUNIN.

En segundo lugar, con la evidencia obtenida de la simulación se presentará una petición formal al cliente para que nos autorice la configuración del protocolo Netflow y la configuración para la priorización del tráfico en su router principal.

En tercer lugar, una vez obtenido el permiso se procederá con la configuración del protocolo Netflow, el cual permitirá monitorear todo el tráfico de la red e identificar los dispositivos que consumen un mayor ancho de banda; asimismo con la configuración para la priorización del tráfico para mejorar el rendimiento de la red.

Por último, gracias a la herramienta Netflow Traffic Analyzer obtendremos información de la disponibilidad, latencia y pérdidas de paquetes; recopilando así datos entre los días 28 y 31 de Octubre con el fin de comparar los datos obtenidos después del día en que se proceda con la configuración.

3.2 Simulación de la red LAN de SUNARP

Como ya se hizo mención en los párrafos anteriores, se realizará una simulación con el fin de verificar que la propuesta de configuración de la priorización de políticas y el protocolo Netflow son aptas para ser configuradas en el Router de SUNARP-JUNÍN. Para empezar en la figura 15 se muestra un modelo de diseño de la red LAN de SUNARP el cual consta de 3 routers, 2 switch de distribución, 5 switch de acceso y un servidor de internet. En el modelo podemos observar 4 áreas, las cuales corresponden al área de finanzas, ventas, TI y alta gerencia. Cabe recalcar que para este diseño se trabajó con una PC y un teléfono IP por área, además se hizo uso de servidores DHCP, DNS y CORREO para una simulación más acertada. Actualmente la red LAN de SUNARP utiliza el método FIFO, es decir el tráfico sale según la orden de llegada; el problema de este método aplicado es que esta sede cuenta con un pequeño ancho de banda, el cual hace al método FIFO un método no recomendable para ser aplicado.

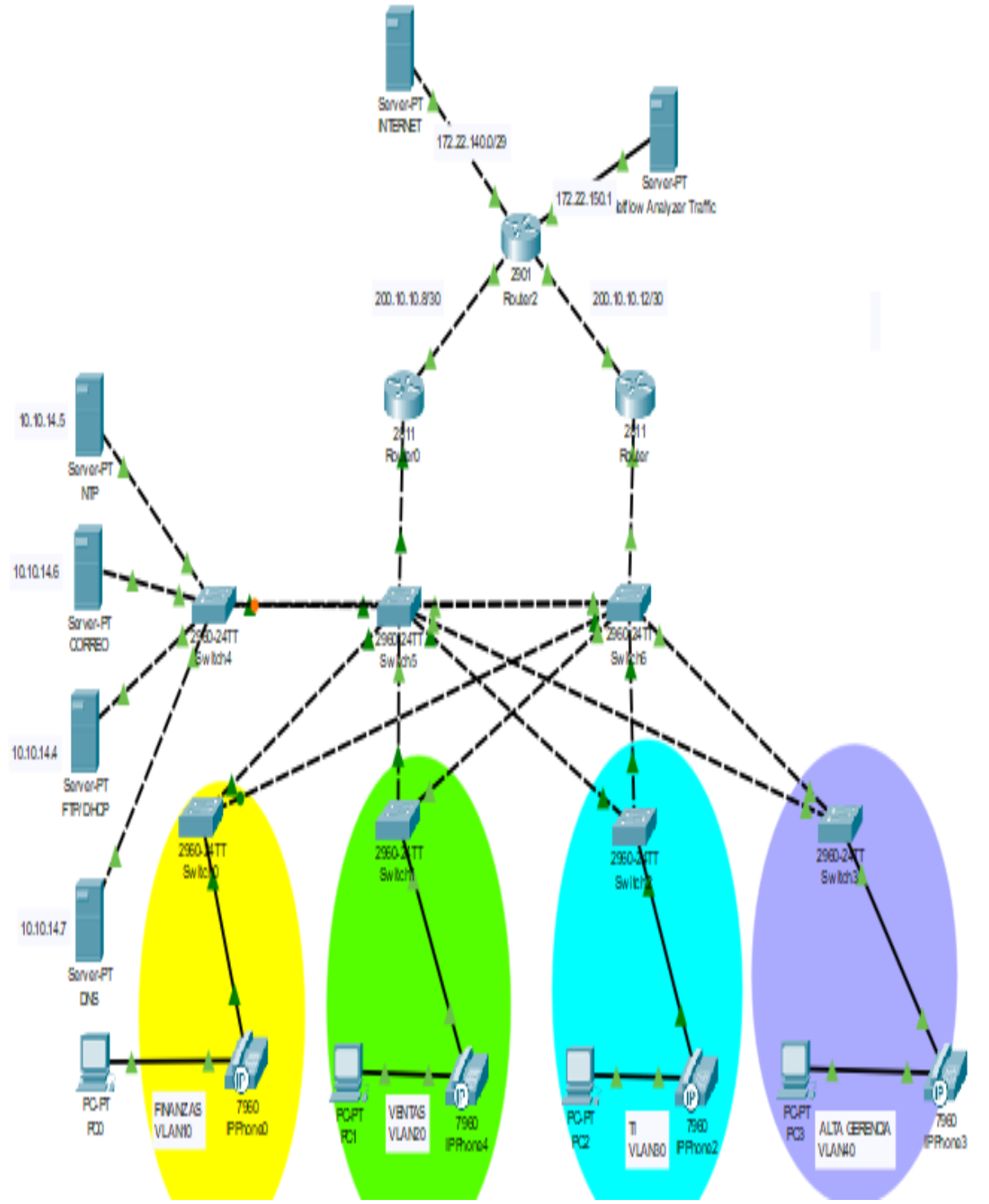


Figura 15: Diseño de la red LAN de SUNARP
Fuente: Elaboración propia

3.2.1 Configuración del Router 0

Como se observa en la figura 16, el Router 0 tiene configurado el protocolo DHCP para brindar direccionamiento IP automático a los dispositivos de telefonía IP, los anexos de los teléfonos y las subinterfaces e interfaces con sus respectivos gateways.

‘

Router0

Physical Config CLI Attributes

IOS Command Line Interface

```
Router>en
Router#sh run
Building configuration...

Current configuration : 3739 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
!
ip dhcp excluded-address 10.10.9.1 10.10.9.10
!
ip dhcp pool Voz
 network 10.10.9.0 255.255.255.0
 default-router 10.10.9.2
 option 150 ip 10.10.9.1
!
interface FastEthernet0/0
 ip address 200.10.10.9 255.255.255.252
 ip access-group 100 out
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.10.14.1 255.255.255.0
 duplex auto
 speed auto
 standby 5 ip 10.10.14.3
 standby 5 priority 120
 standby 5 preempt
 standby 5 track FastEthernet0/0
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
 ip helper-address 10.10.14.4
 standby 1 ip 10.10.10.2
 standby 1 priority 120
 standby 1 preempt
 standby 1 track FastEthernet0/0
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 10.10.11.1 255.255.255.0
 ip helper-address 10.10.14.4
 standby 2 ip 10.10.11.2
 standby 2 priority 120
 standby 2 preempt
 standby 2 track FastEthernet0/0
!
```

```
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 10.10.12.1 255.255.255.0
 ip helper-address 10.10.14.4
 standby 3 ip 10.10.12.2
 standby 3 priority 120
 standby 3 preempt
 standby 3 track FastEthernet0/0
!
interface FastEthernet0/1.40
 encapsulation dot1Q 40
 ip address 10.10.13.1 255.255.255.0
 ip helper-address 10.10.14.4
 standby 4 ip 10.10.13.2
 standby 4 priority 120
 standby 4 preempt
 standby 4 track FastEthernet0/0
!
interface FastEthernet0/1.500
 encapsulation dot1Q 500
 ip address 10.10.9.1 255.255.255.0
 standby 6 ip 10.10.9.2
 standby 6 priority 120
 standby 6 preempt
 standby 6 track FastEthernet0/0
!
telephony-service
 max-ephones 20
 max-dn 20
 ip source-address 10.10.9.3 port 2000
 auto assign 1 to 20
!
ephone-dn 1
 number 241
!
ephone-dn 2
 number 242
!
ephone-dn 3
 number 243
!
ephone-dn 4
 number 244
!
ephone-dn 5
 number 245
!
ephone-dn 6
 number 246
!
ephone-dn 7
 number 247
!
ephone-dn 8
 number 248
!
ephone-dn 9
 number 249
!
```

Figura 16: Configuración Router 0

Fuente: Packet Tracer

3.2.1.1 Prioridad del Router 0

En la figura 17 podemos observar la prioridad y el estado del router, en este caso el Router 0 se encuentra en modo activo con una prioridad de 120, esto quiere decir que este equipo es el router principal por el cual va a pasar todo el tráfico.

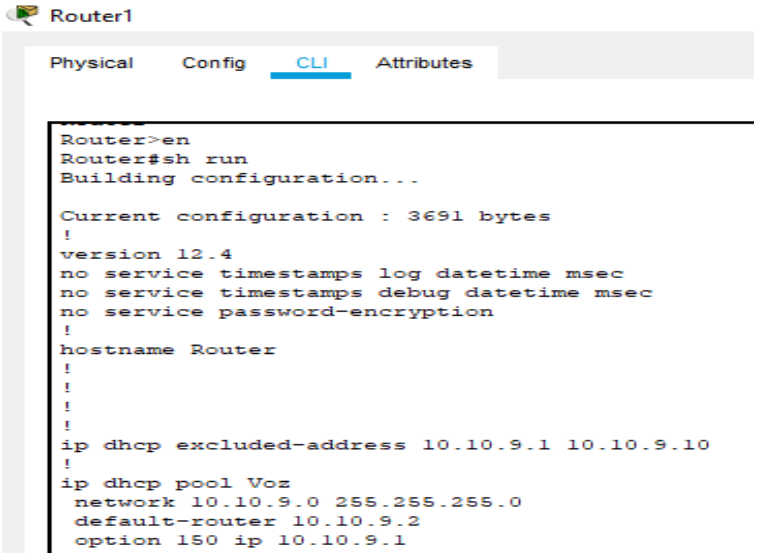
```
Router#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Fa0/1       5    120 P Active   local           10.10.14.2      10.10.14.3
Fa          1    120 P Active   local           10.10.10.3      10.10.10.2
Fa          2    120 P Active   local           10.10.11.3      10.10.11.2
Fa          3    120 P Active   local           10.10.12.3      10.10.12.2
Fa          4    120 P Active   local           10.10.13.3      10.10.13.2
Fa          6    120 P Active   local           10.10.9.1       10.10.9.2
```

Figura 17: Prioridad del Router 0

Fuente: Packet Tracer

3.2.2 Configuración del Router 1

Como se observa en la figura 18, el Router 1 al igual que el Router 0 tiene una configuración similar esto es debido a que el Router 1 funciona como Router Backup. Por ende, este router también tiene configurado el protocolo DHCP para brindar direccionamiento IP automático a los dispositivos de telefonía IP, los anexos de los teléfonos y las subinterfaces e interfaces con sus respectivos gateways.



```
interface FastEthernet0/0
 ip address 10.10.14.2 255.255.255.0
 duplex auto
 speed auto
 standby 5 ip 10.10.14.3
 standby 5 priority 115
 standby 5 preempt
!
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.10.10.3 255.255.255.0
 ip helper-address 10.10.14.4
 standby 1 ip 10.10.10.2
 standby 1 priority 115
 standby 1 preempt
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.10.11.3 255.255.255.0
 ip helper-address 10.10.14.4
 standby 2 ip 10.10.11.2
 standby 2 priority 115
 standby 2 preempt
!
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.10.12.3 255.255.255.0
 ip helper-address 10.10.14.4
 standby 3 ip 10.10.12.2
 standby 3 priority 115
 standby 3 preempt
```

```
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 10.10.13.3 255.255.255.0
 ip helper-address 10.10.14.4
 standby 4 ip 10.10.13.2
 standby 4 priority 115
 standby 4 preempt
!
interface FastEthernet0/0.500
 encapsulation dot1Q 500
 ip address 10.10.9.1 255.255.255.0
 standby 6 ip 10.10.9.2
 standby 6 priority 115
 standby 6 preempt

 telephony-service
  max-ephones 20
  max-dn 20
  ip source-address 10.10.9.3 port 2000
  auto assign 1 to 20
 !
 ephone-dn 1
  number 241
 !
 ephone-dn 2
  number 242
 !
 ephone-dn 3
  number 243
 !
 ephone-dn 4
  number 244
 !
 ephone-dn 5
  number 245
 !
 ephone-dn 6
  number 246
 !
 ephone-dn 7
  number 247
 !
 ephone-dn 8
  number 248
 !
 ephone-dn 9
  number 249
```

Figura 18: Configuración del Router 1
Fuente: Packet Tracer

3.2.2.1 Prioridad del Router 1

En la figura 19 podemos observar la prioridad y el estado del router, en este caso el Router 1 se encuentra en modo Standby con una prioridad de 115, esto quiere decir que el Router 1 es el router backup, el cual ante cualquier inconveniente con el Router principal este pasaría al estado Activo.

```
Router#sh stan
Router#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Fa0/0       5    115 P Standby 10.10.14.1      local           10.10.14.3
Fa          1    115 P Standby 10.10.10.1      local           10.10.10.2
Fa          2    115 P Standby 10.10.11.1      local           10.10.11.2
Fa          3    115 P Standby 10.10.12.1      local           10.10.12.2
Fa          4    115 P Standby 10.10.13.1      local           10.10.13.2
Fa          6    115 P Standby 10.10.9.1       local           10.10.9.2
Router#
```

Figura 19: Prioridad del Router 1
Fuente: Packet Tracer

3.2.3 Configuración del Router 2

Como se observa en la figura 20, el Router 2 tiene configurado el protocolo NAT para que las direcciones privadas salgan a internet con direcciones públicas, las interfaces a las que se conecta y las redes que conoce. Además, cuenta con la configuración de los Access List, Class Map y Policy Map para la priorización del tráfico de datos y voz; por último, también se puede observar la configuración del protocolo Netflow para monitorear e identificar el dispositivo de mayor consumo de ancho de banda. Cabe recalcar que se dio prioridad al tráfico de voz por ser un tipo de tráfico sensible a la latencia.

Router2

Physical Config CLI Attributes

```
!
class-map match-all VOICE
 match access-group 100
class-map match-all DATOS
 match access-group 104
!
policy-map IPVPN
 class VOICE
  priority 512
 class DATOS
  bandwidth 2048
 class class-default
  fair-queue
!
!
!
!
!
interface GigabitEthernet0/0
 ip flow egress
 ip flow ingress
 ip address 200.10.10.10 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 200.10.10.14 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
 switchport mode trunk
```

```
interface FastEthernet0/0/1
 switchport access vlan 900
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/0/2
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/0/3
 switchport mode access
 switchport nonegotiate
!
interface GigabitEthernet0/1/0
 no ip address
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan900
 mac-address 0007.ece2.db01
 ip address 172.22.140.1 255.255.255.248
 ip nat outside
!
router ospf 100
 router-id 3.3.3.3
 log-adjacency-changes
 network 200.10.10.8 0.0.0.3 area 0
 network 200.10.10.12 0.0.0.3 area 0
 network 172.22.140.0 0.0.0.7 area 0
ip nat pool INTERNET 172.22.140.3 172.22.140.6 netmask 255.255.255.248
ip nat inside source list vlan10 pool INTERNET overload
ip nat inside source list vlan20 pool INTERNET overload
ip nat inside source list vlan30 pool INTERNET overload
ip nat inside source list vlan40 pool INTERNET overload
ip classless
!
ip flow-export destination 172.22.150.0 4444
ip flow-export destination 172.22.150.1 4444
ip flow-export version 9
ip flow-export source GigabitEthernet0/0
!
!
ip access-list standard vlan10
 permit 10.10.10.0 0.0.0.255
ip access-list standard vlan20
 permit 10.10.11.0 0.0.0.255
ip access-list standard vlan30
 permit 10.10.12.0 0.0.0.255
ip access-list standard vlan40
 permit 10.10.13.0 0.0.0.255
access-list 100 permit udp any any range 10000 65535
access-list 100 permit tcp any any eq 1720
access-list 100 permit ip 10.10.9.0 0.0.0.255 any
access-list 104 permit ip any any
```

Figura 20: Configuración del Router 2

Fuente: Packet Tracer

3.2.3.1 Configuración de Netflow

Como se observa en figura 21, se configura el protocolo Netflow en la interfaz Gi0/0 para capturar todo el tráfico entrante y saliente de este puerto. La explicación de los pasos para configurar el protocolo Netflow se puede visualizar en la página 29.

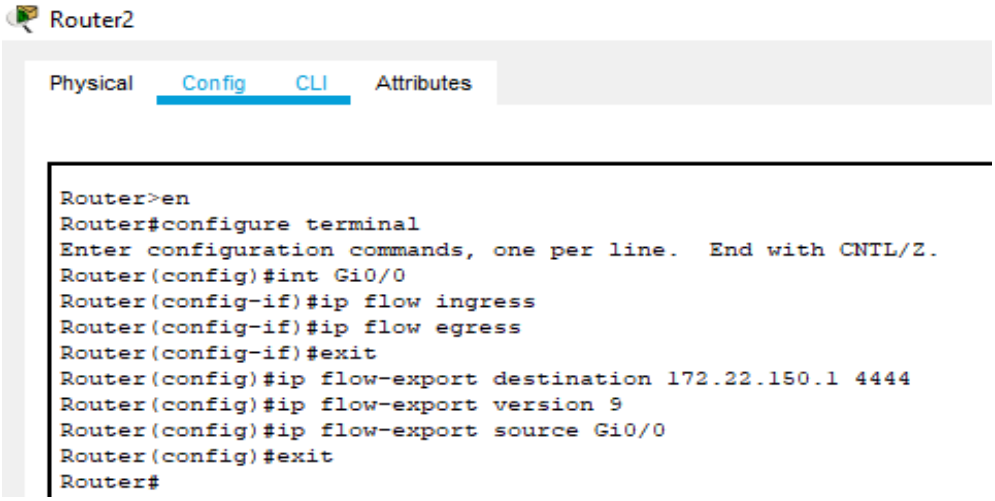


Figura 21: Configuración de Netflow
Fuente: Packet Tracer

3.2.3.2 Prueba de Configuración de Netflow

En la figura 22 se puede verificar la configuración del protocolo Netflow usando el comando sh run | i flow

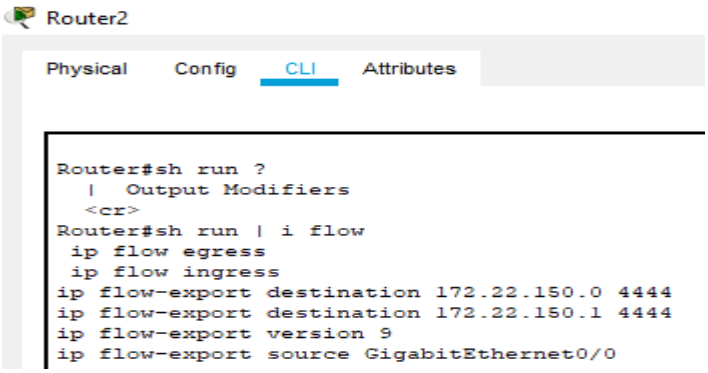


Figura 22: Prueba de Configuración de Netflow
Fuente: Packet Tracer

3.2.3.3 Configuración de QoS

Como se observa en la figura 23, se configura la priorización de tráfico para prevenir la congestión en la red haciendo uso del método CBWFQ con LLQ. Cabe recalcar que se brindó prioridad al tráfico de voz por ser un tráfico sensible a la latencia.

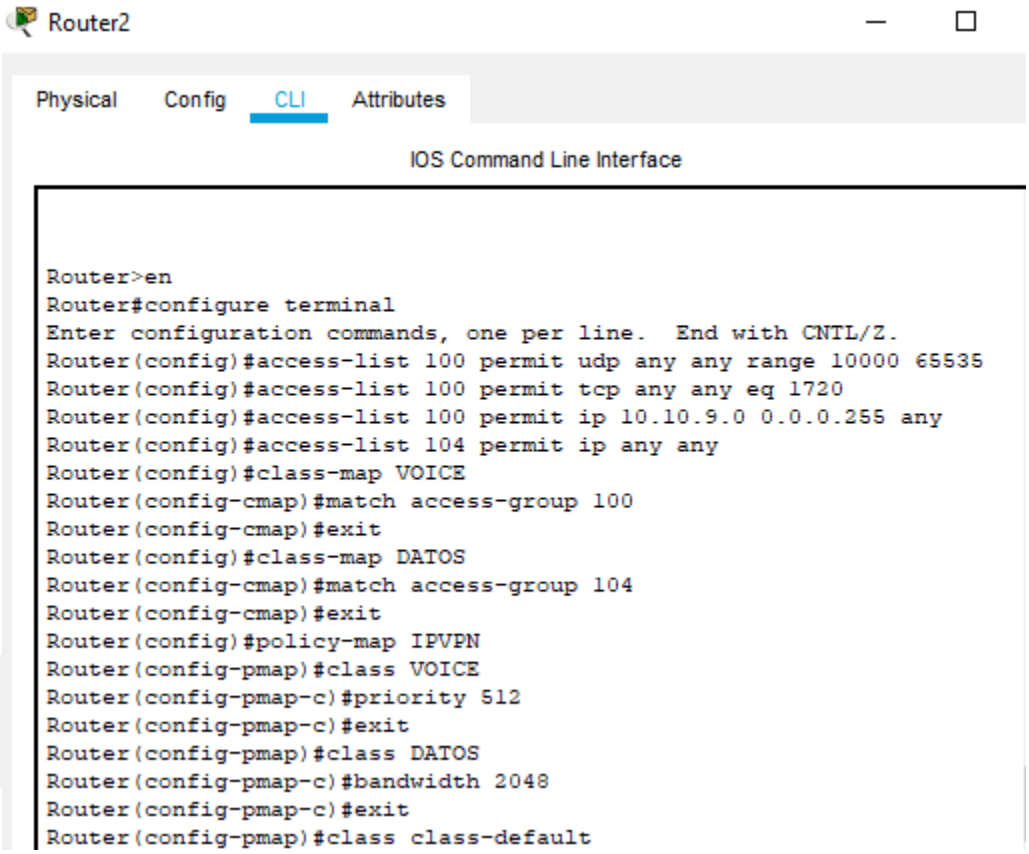


Figura 23: Configuración de QoS

Fuente: Packet Tracer

3.2.3.4 Prueba de configuración de QoS

En la figura 24 se puede verificar la configuración de las clases de priorización del tráfico, usando el comando sh run | i class.

```
Router#sh run | i class
class-map match-all VOICE
class-map match-all DATOS
 class VOICE
 class DATOS
 class class-default
```

Figura 24: Prueba de Configuración de QoS
Fuente:Packet Tracer

3.2.4 Switches de Acceso

Los switches de acceso que se observan en la parte inferior de la figura 25 poseen una similar configuración, solo tienen como diferencia la asignación de las Vlan's por cada área, debido a que estas se usan para segmentar las áreas de la empresa con el objetivo de tener una mejor administración de red. En la figura 25 se observa las Vlan`s asignadas para cada red.

```
RED INTERNA
10.10.09.0/24 vlan 500 VOZ
10.10.10.0/24 vlan10 FINANZAS -SWITCH 0
10.10.11.0/24 vlan20 VENTAS -SWITCH 1
10.10.12.0/24 vlan30 RRHH -SWITCH 2
10.10.13.0/24 vlan40 ALTA GERENCIA -SWITCH 3
```

Figura 25: Vlan`s asignadas
Fuente: Packet Tracer

3.2.4.1 Switch 0

En la figura 26 se observa la configuración del Switch 0, el cual consta del comando switchport mode Access en la interface Fa/01 y Fa/02 para permitir que muchas VLANS pasen por un solo link. Además de la asignación de la Vlan 1 como default en el interface Fa/03 y la asignación de la Vlan 10 así como también la Vlan 500 en cada puerto restante.

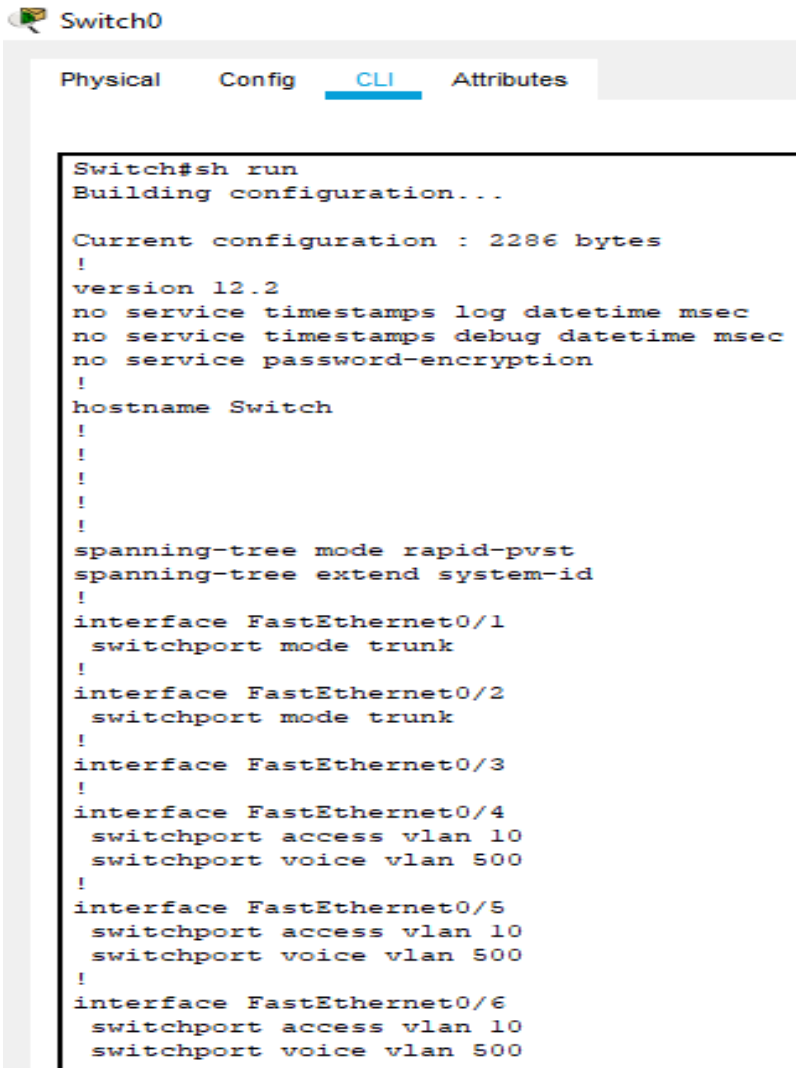


Figura 26: Configuración del Switch 0

Fuente: Packet Tracer

3.2.4.2 Switch 1

En la figura 27 se observa la configuración del Switch 1, el cual consta del comando switchport mode Access en la interface Fa/01 y Fa/02 para permitir que muchas VLANS pasen por un solo link. Además de la asignación de la Vlan 1 como default en el interface Fa/03 y la asignación de la Vlan 10 así como también la Vlan 500 en cada puerto restante.

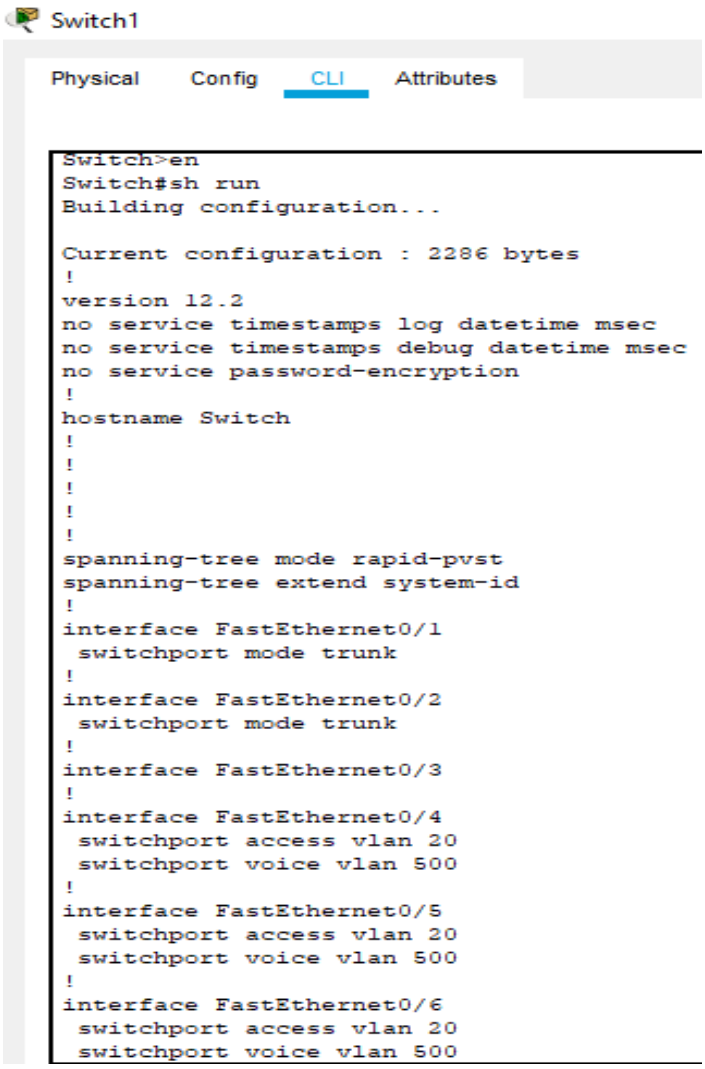


Figura 27: Configuración del Switch 1

Fuente: Packet Tracer

3.2.4.3 Switch 2

En la figura 28 se observa la configuración del Switch 2, el cual consta del comando switchport mode Access en la interface Fa/01 y Fa/02 para permitir que muchas VLANS pasen por un solo link. Además de la asignación de la Vlan 1 como default en el interface Fa/03 y la asignación de la Vlan 10 así como también la Vlan 500 en cada puerto restante.

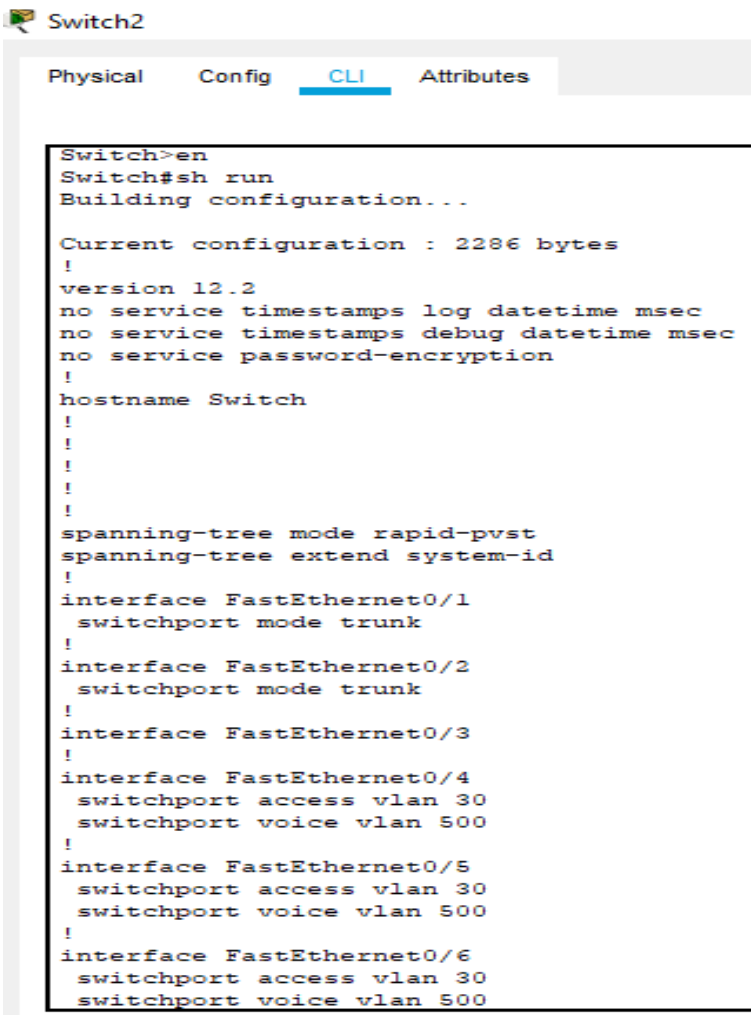


Figura 28: Configuración del Switch 2

Fuente: Packet Tracer

3.2.4.4 Switch 3

En la figura 29 se observa la configuración del Switch 3, el cual consta del comando switchport mode Access en la interface Fa/01 y Fa/02 para permitir que muchas VLANS pasen por un solo link. Además de la asignación de la Vlan 1 como default en el interface Fa/03 y la asignación de la Vlan 10 así como también la Vlan 500 en cada puerto restante.

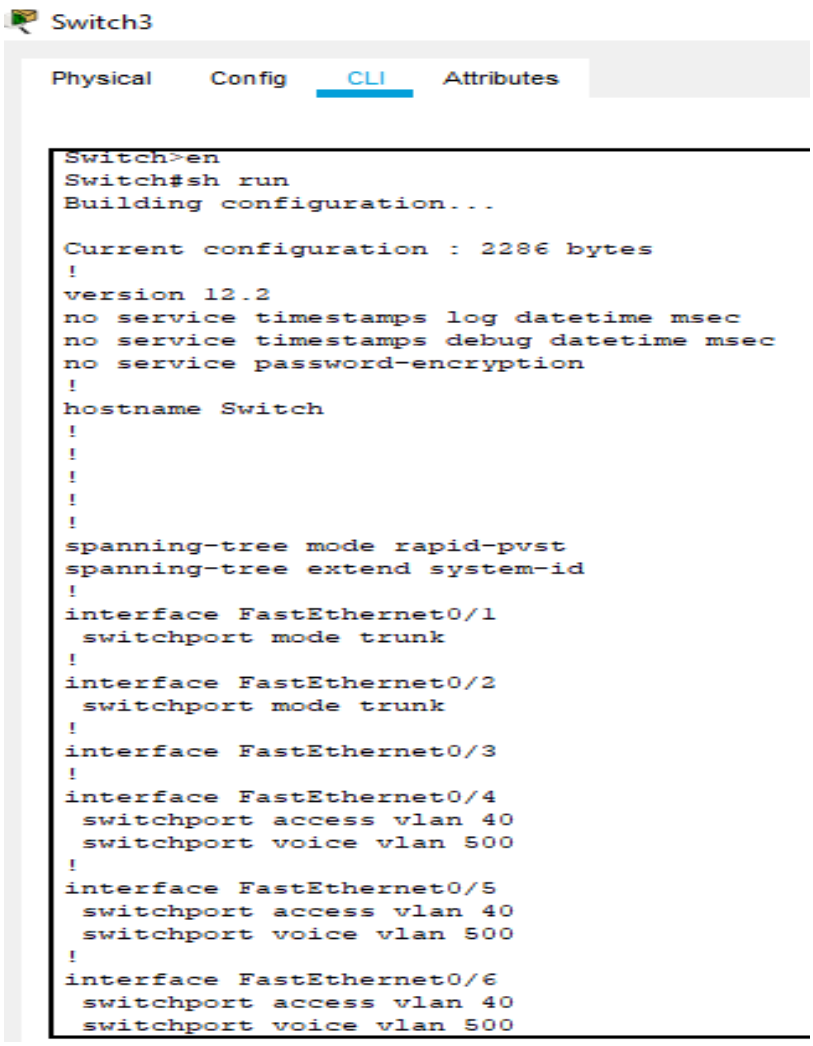


Figura 29: Configuración del Switch 3
Fuente: Packet Tracer

3.2.5 Servidor de Internet

Como se observa en la figura 30, el servidor de internet fue configurado con la dirección IP 172.22.140.1, con el fin de realizar las pruebas de salida de cada PC hacia internet.

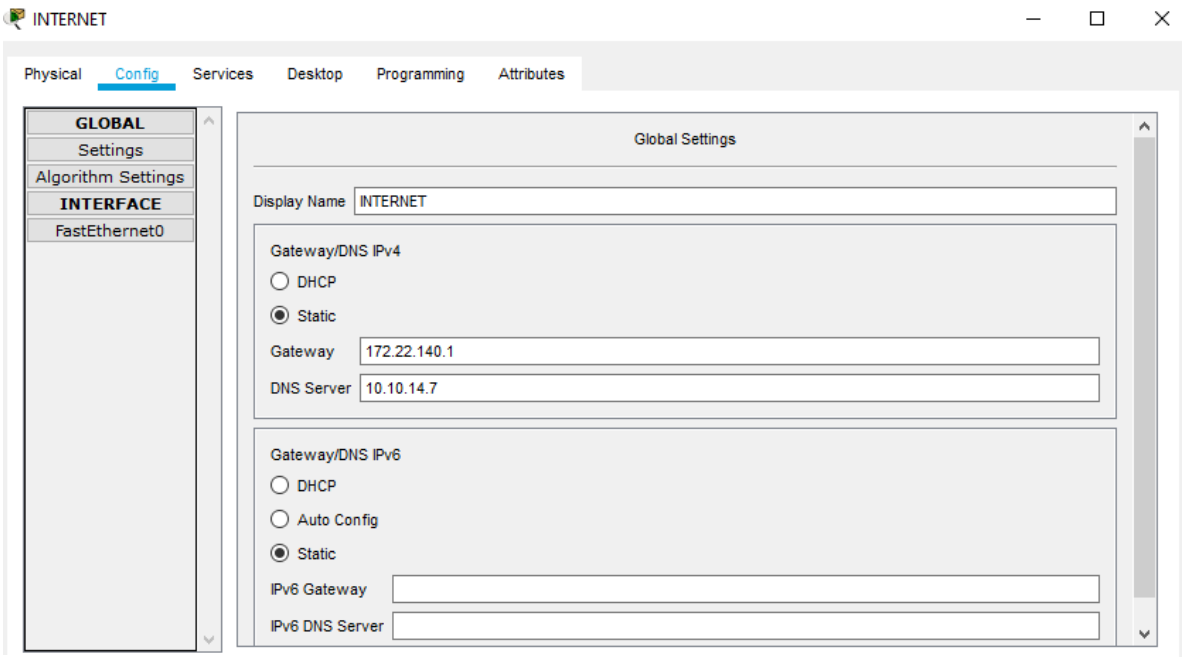


Figura 30: Servidor de Internet

Fuente: Packet Tracer

3.2.6 Área de Finanzas

3.2.6.1 PC 0

La PC 0 hace referencia a uno de los dispositivos que se encuentran en el área de finanzas, esta PC mediante el Servidor DHCP se le asignó la IP 10.10.10.10. En la figura 31 se puede observar la asignación de la IP 10.10.10.10 por DHCP.

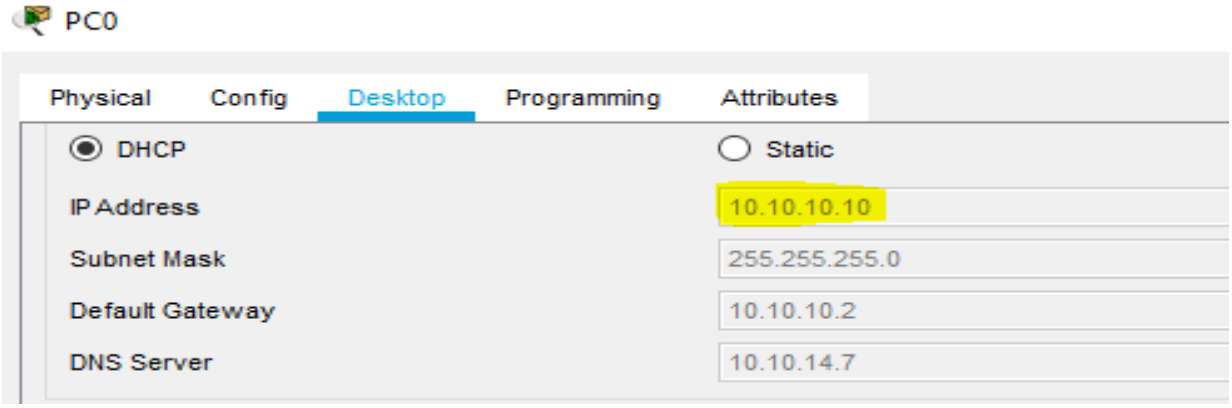


Figura 31: IP Address PC 0
Fuente: Elaboración Propia

3.2.6.2 Teléfono IP 0

El teléfono IP 0 hace referencia a uno de los dispositivos que se encuentran en el área de finanzas, este equipo se encargará de simular el tráfico VoIP que pasara por la red de SUNARP. En la figura 32 se muestra el teléfono IP 0 y el número de línea 244 que fue configurado.

Figura 32 Teléfono IP 0

Fuente: Software Packet Tracer

3.2.7 Área de Ventas

3.2.7.1 PC 1

La PC 1 hace referencia a uno de los dispositivos que se encuentran en el área de Ventas, esta PC mediante el Servidor DHCP se le asignó la IP 10.10.11.10. En la figura 33 se puede observar la asignación de la IP 10.10.11.10 por DHCP.

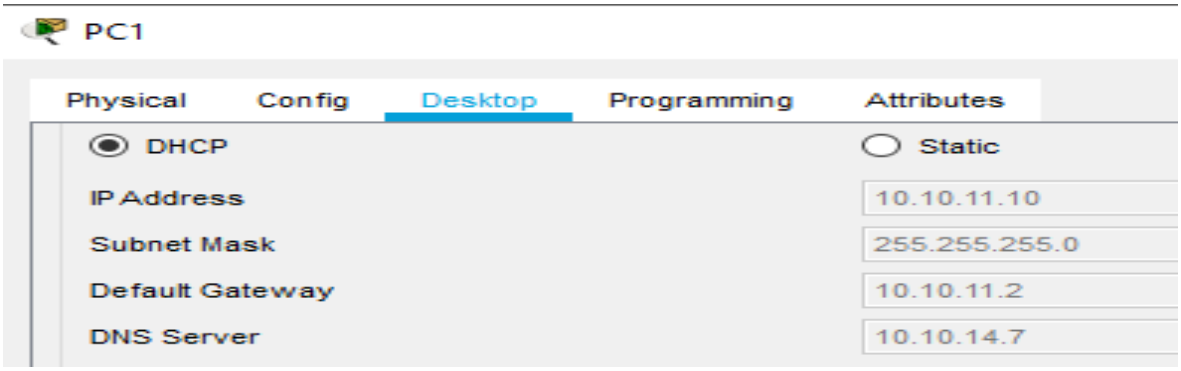


Figura 33 : IP Address PC 1
Fuente: Elaboración Propia

3.2.7.2 Teléfono IP 1

El teléfono IP 1 hace referencia a uno de los dispositivos que se encuentran en el área de ventas, este equipo se encargará de simular el tráfico VoIP que pasara por la red de SUNARP. En la figura 34 se muestra el teléfono IP 01 y el número de línea 246 que fue configurado.

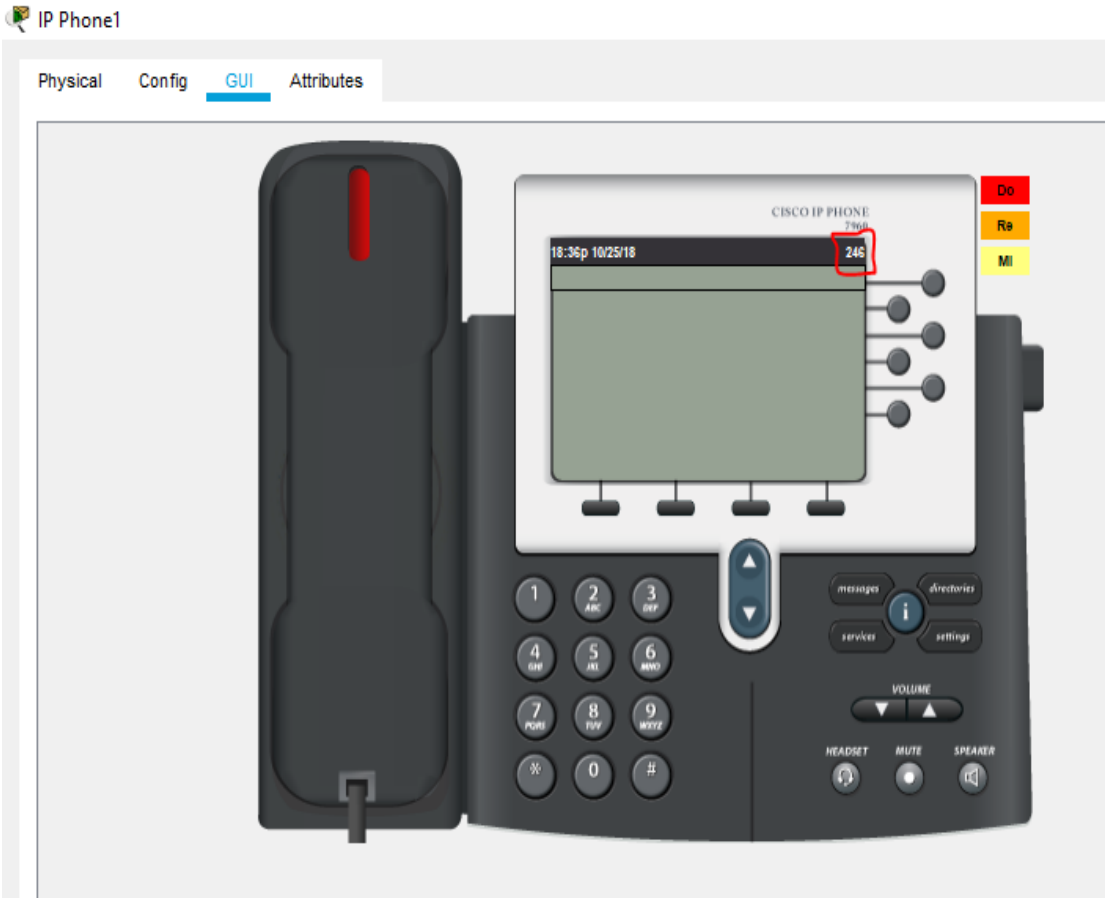


Figura 34: Teléfono IP 1
Fuente: Packet Tracer

3.2.8 Área TI

3.2.8.1 PC 2

La PC 2 hace referencia a uno de los dispositivos que se encuentran en el área de TI, esta PC mediante el Servidor DHCP se le asignó la IP 10.10.12.10. En la figura 35 se puede observar la asignación de la IP 10.10.12.10 por DHCP.

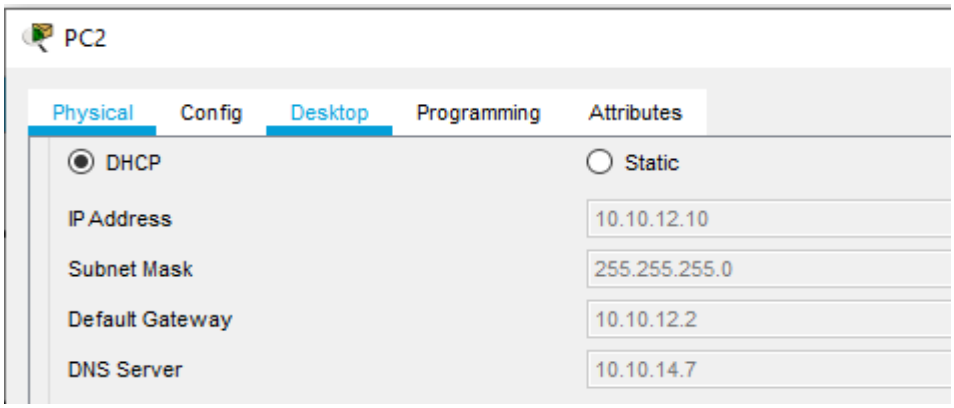


Figura 35: IP Address PC2
Fuente: Packet Tracer

3.2.8.2 Teléfono IP 2

El teléfono IP 2 hace referencia a uno de los dispositivos que se encuentran en el área de TI, este equipo se encargará de simular el tráfico VoIP que pasara por la red de SUNARP. En la figura 36 se muestra el teléfono IP 2 y el número de línea 243 que fue configurado.

*Figura 36 :*Teléfono IP 2
Fuente: Packet Tracer

3.2.9 Área de Alta Gerencia

3.2.9.1 PC 3

La PC 3 hace referencia a uno de los dispositivos que se encuentran en el área de TI, esta PC mediante el Servidor DHCP se le asignó la IP 10.10.13.10. En la figura 37 se puede observar la asignación de la IP 10.10.13.10 por DHCP.

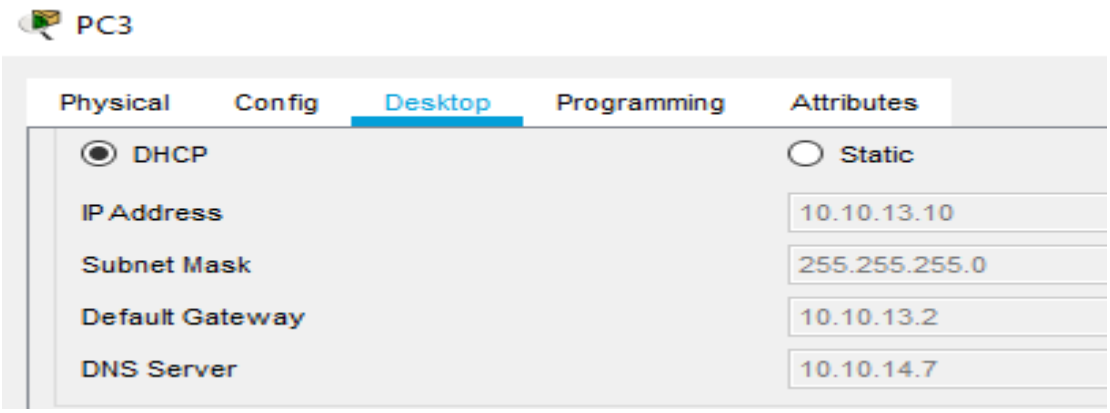


Figura 37: IP Address PC 3
Fuente:Packet Tracer

3.2.9.2 Teléfono IP 3

El teléfono IP 3 hace referencia a uno de los dispositivos que se encuentran en el área de TI, este equipo se encargará de simular el tráfico VoIP que pasará por la red de SUNARP. En la figura 38 se muestra el teléfono IP 3 y el número de línea 242 que fue configurado.

Figura 38: Teléfono IP 3
Fuente: Packet Tracer

3.2.10 Pruebas de Ping

La tabla 4 muestra las pruebas de PING que se va a realizar para verificar si hay conectividad hacia la IP destino, además se verificará el tiempo de respuesta más conocido como latencia y los posibles errores en la red cuando las PC y los teléfonos IP intercambian información.

Tabla 4: Pruebas de Ping

Pc Origen	PC Destino	IP Origen	IP Destino
PC 3	Servidor Internet	10.10.13.10	172.22.140.1
PC 2	Servidor Internet	10.10.12.10	172.22.140.1
PC 1	Servidor Internet	10.10.11.10	172.22.140.1
PC 0	Servidor Internet	10.10.10.10	172.22.140.1
Pc 3	Pc 0	10.10.13.10	10.10.10.10
Pc 2	Pc 0	10.10.12.10	10.10.10.10
Pc 1	Pc 0	10.10.11.10	10.10.10.10
Pc 0	Pc 3	10.10.10.10	10.10.13.10

Fuente: Elaboración propia

3.2.10.1 Ping PC3 – Servidor de Internet

En la figura 39 se puede observar que se envió 23 paquetes hacia la dirección IP del Servidor de Internet con un tiempo promedio de 1ms, a pesar de que hubo un paquete que su tiempo máximo de viaje fue de 10 ms no se tuvo ninguna pérdida de paquetes. Al realizar esta prueba con el comando PING se pudo verificar conectividad hacia el servidor de Internet.

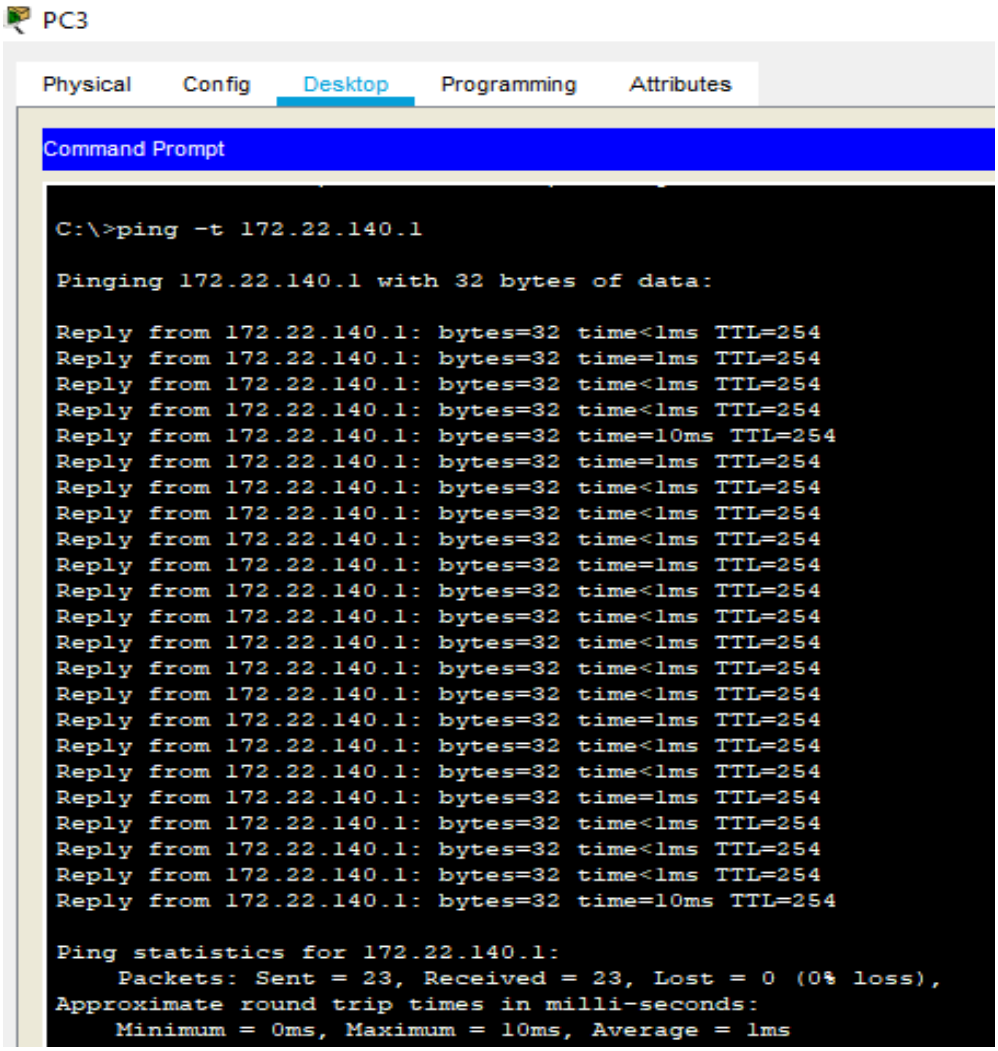


Figura 39: Ping PC3–Servidor de Internet
Fuente: Packet Tracer

3.2.10.2 Ping PC2 – Servidor de Internet

En la figura 40 se puede observar que se envió 27 paquetes hacia la dirección IP del Servidor de Internet con un tiempo promedio de 1ms, a pesar de que hubo un paquete que su tiempo máximo de viaje fue de 11 ms no se tuvo ninguna pérdida de paquetes. Al realizar esta prueba con el comando PING se pudo verificar conectividad hacia el servidor de Internet.

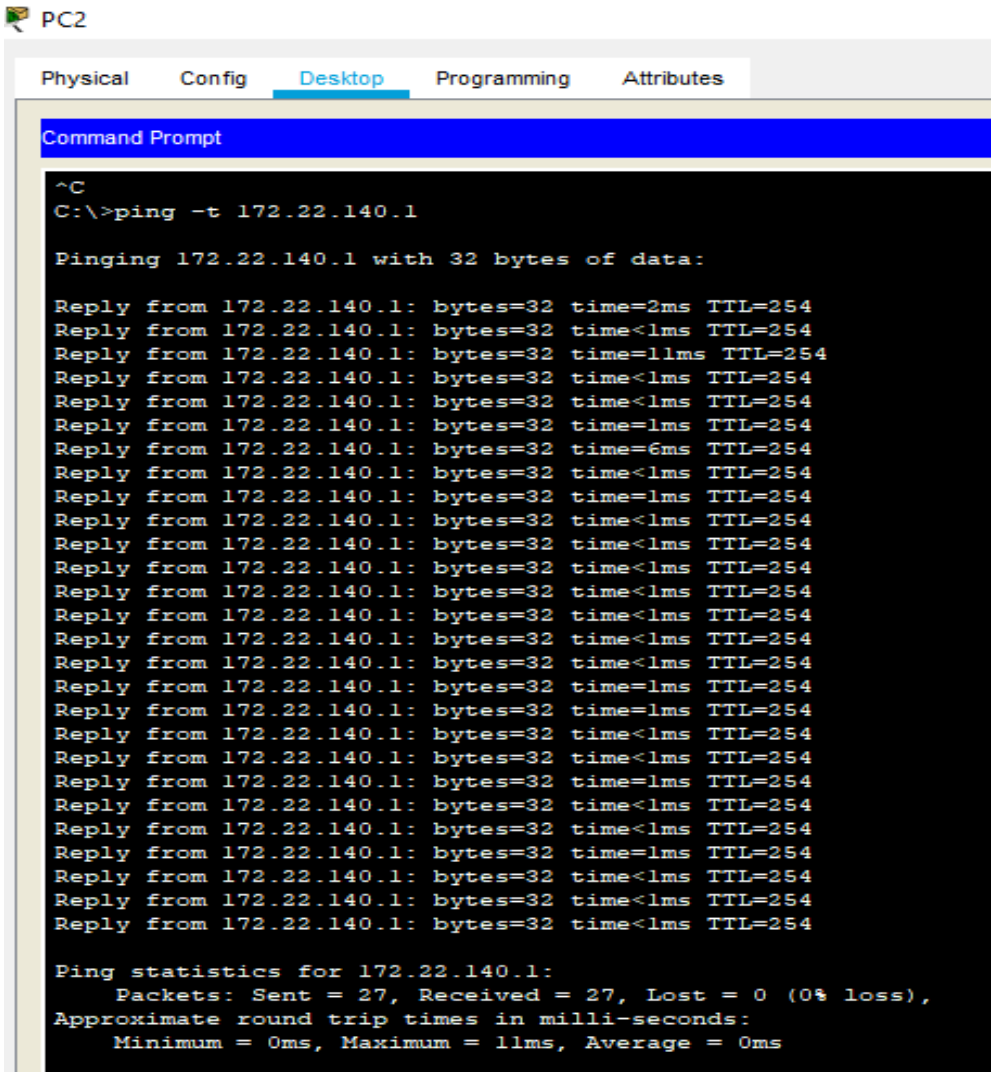


Figura 40: Ping PC2 – Servidor de Internet

Fuente: Packet Tracer

3.2.10.3 Ping PC1 – Servidor de Internet

En la figura 41 se puede observar que se envió 27 paquetes hacia la dirección IP del Servidor de Internet con un tiempo promedio de 2ms, a pesar de que hubo un paquete que su tiempo máximo de viaje fue de 26 ms no se tuvo ninguna pérdida de paquetes. Al realizar esta prueba con el comando PING se pudo verificar conectividad hacia el servidor de Internet.

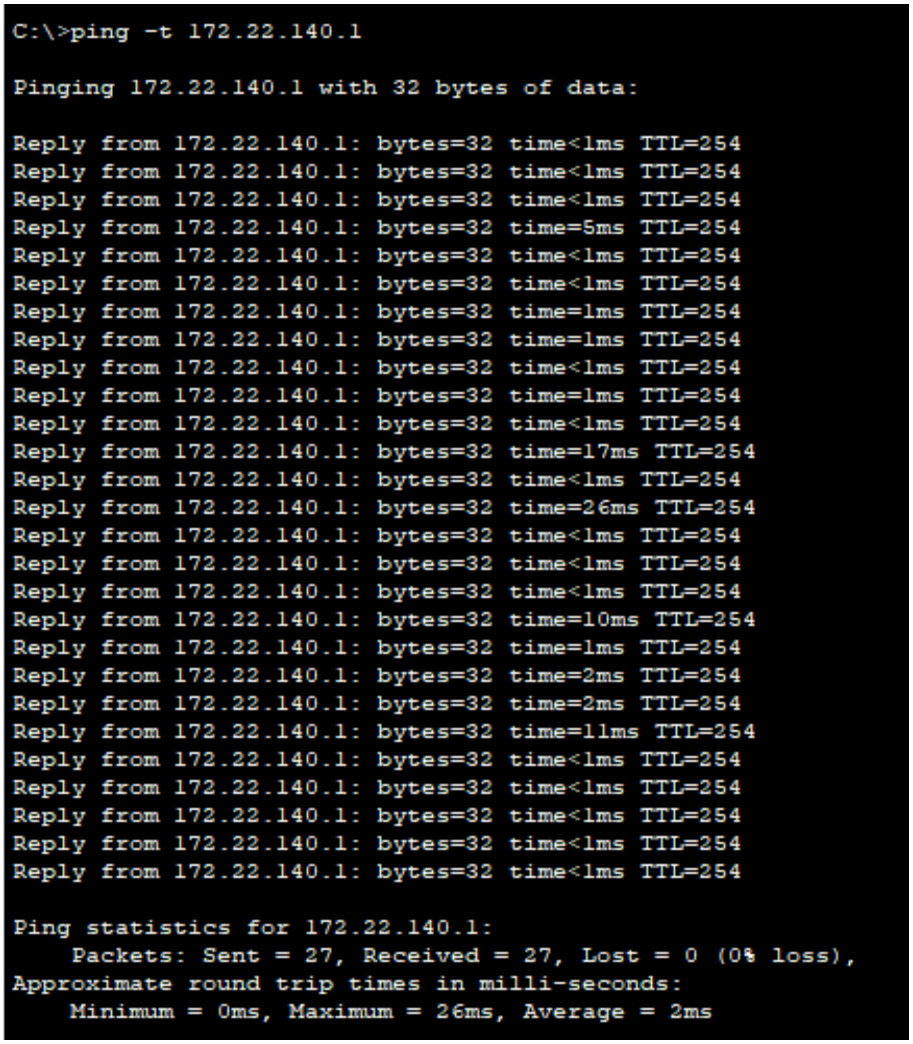


Figura 41: Ping PC1 – Servidor de Internet

Fuente: Packet Tracer

3.2.10.4 Ping PC0 – Servidor de Internet

En la figura 42 se puede observar que se envió 27 paquetes hacia la dirección IP del Servidor de Internet con un tiempo promedio de 5ms, a pesar de que hubo un paquete que su tiempo máximo de viaje fue de 18 ms no se tuvo ninguna pérdida de paquetes. Al realizar esta prueba con el comando PING se pudo verificar conectividad hacia el servidor de Internet.

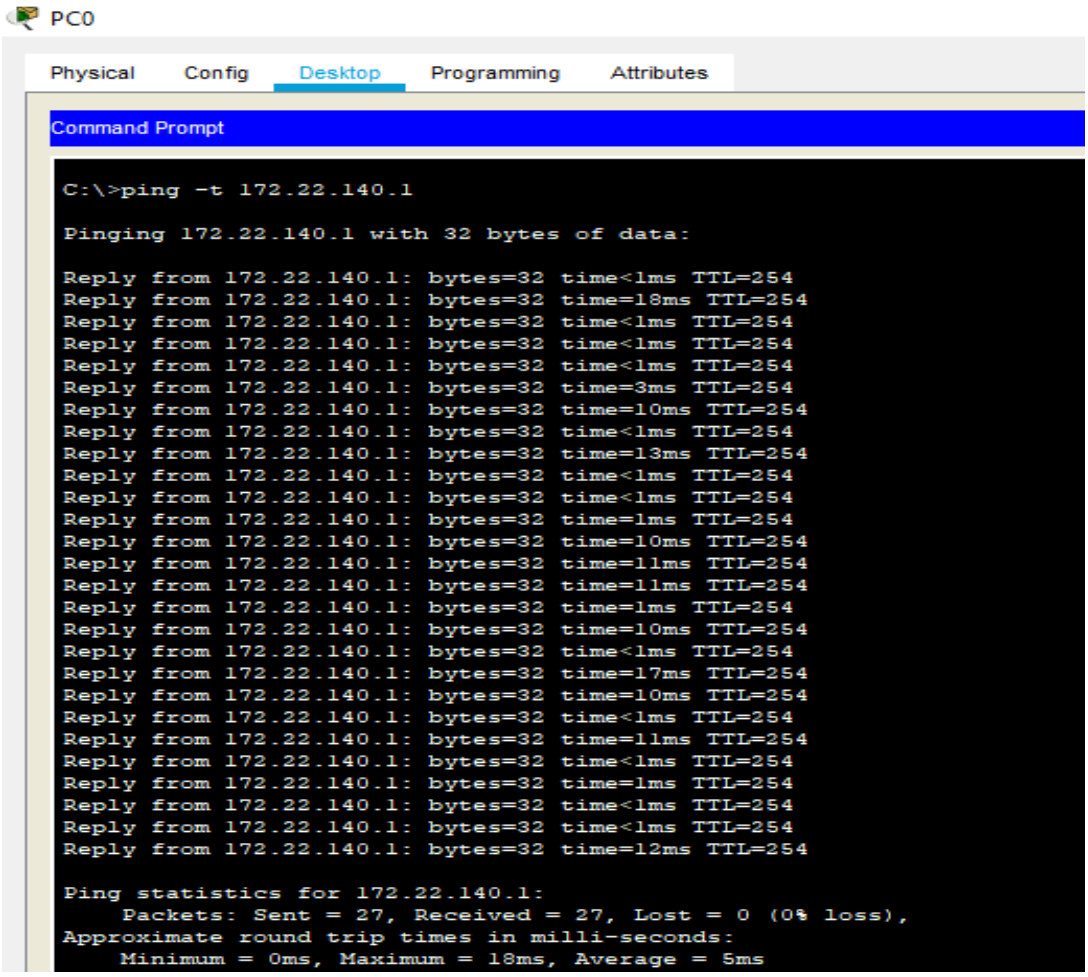


Figura 42: Ping PC0 – Servidor de Internet
Fuente: Packet Tracer

3.2.10.5 Ping PC0 – PC3

En la figura 43 se puede observar que se envió 29 paquetes hacia la dirección IP de la PC 3 con un tiempo promedio de 6ms, a pesar de que hubo un paquete que su tiempo máximo de viaje fue de 29 ms no se tuvo ninguna pérdida de paquetes. Al realizar esta prueba con el comando PING se pudo verificar conectividad hacia el servidor de Internet.

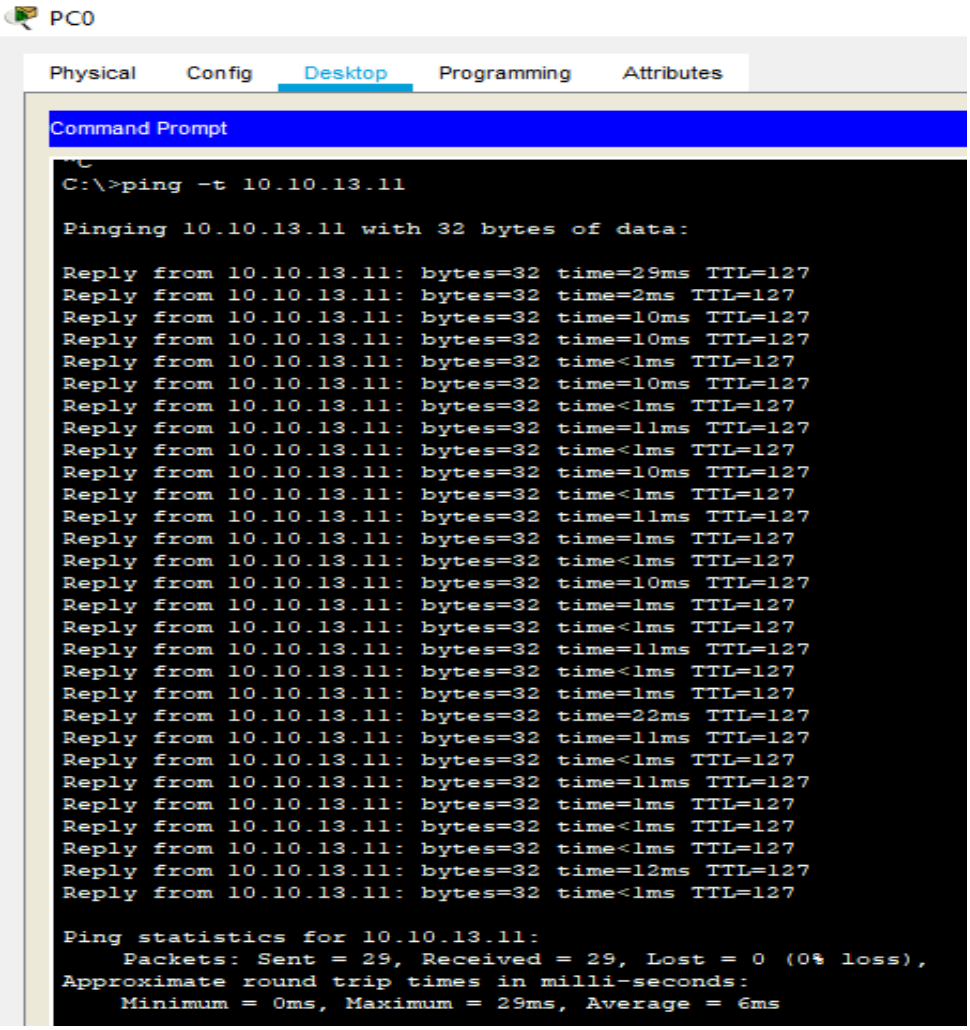


Figura 43: Ping PC0 – PC3
Fuente: Packet Tracer

3.2.10.6 Ping PC1 – PC0

En la figura 44 se puede observar que se envió 29 paquetes hacia la dirección IP de la PC0 con un tiempo promedio de 4ms, a pesar de que hubo un paquete que su tiempo máximo de viaje fue de 18 ms no se tuvo ninguna pérdida de paquetes. Al realizar esta prueba con el comando PING se pudo verificar conectividad hacia el servidor de Internet.

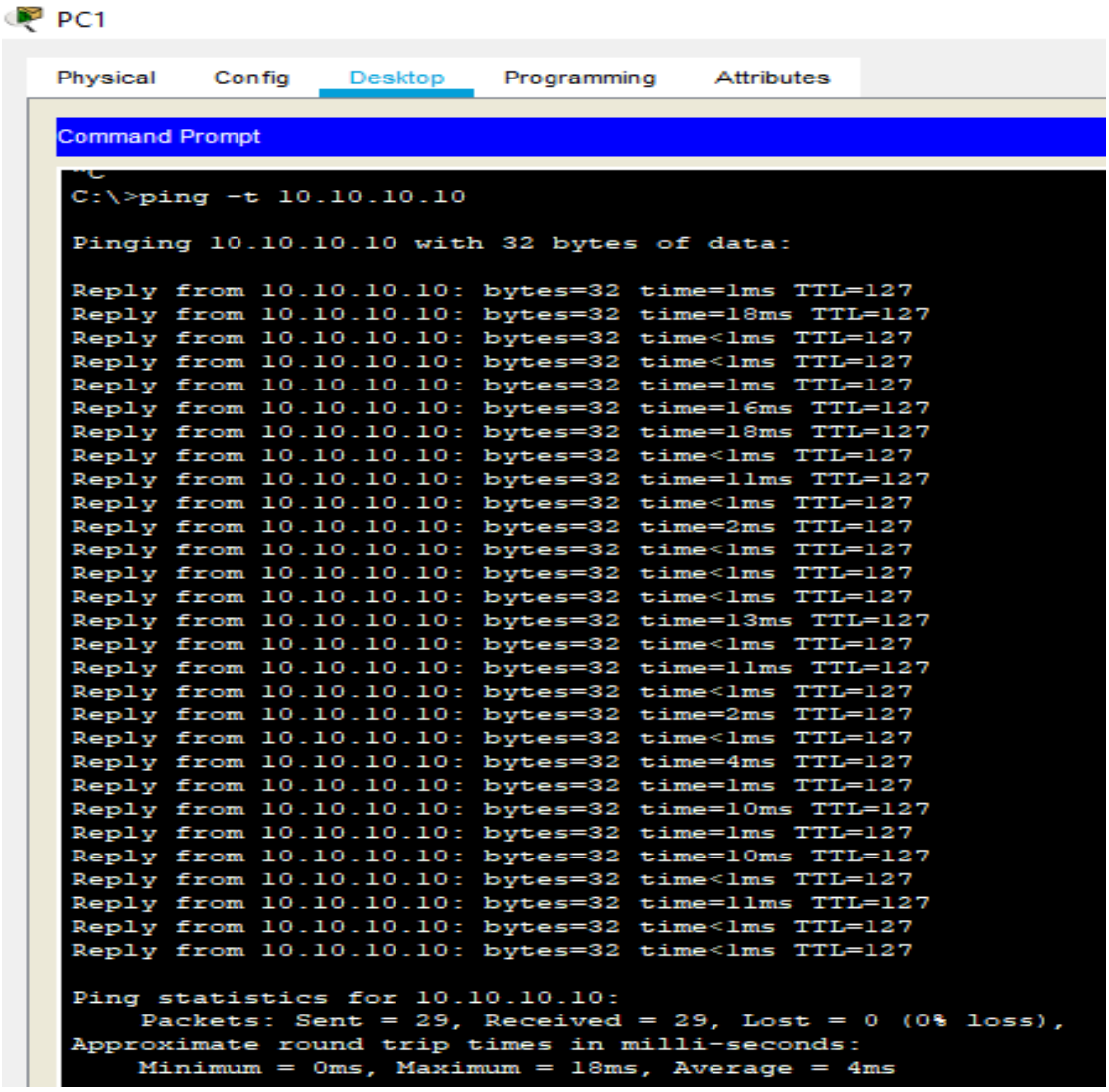


Figura 44: Ping PC1 – PC0
Fuente: Packet Tracer

3.2.10.7 Ping PC2 – PC0

En la figura 45 se puede observar que se envió 30 paquetes hacia la dirección IP de la PC 0 con un tiempo promedio de 6ms, a pesar de que hubo un paquete que su tiempo máximo de viaje fue de 43 ms no se tuvo ninguna pérdida de paquetes. Al realizar esta prueba con el comando PING se pudo verificar conectividad hacia el servidor de Internet.

.

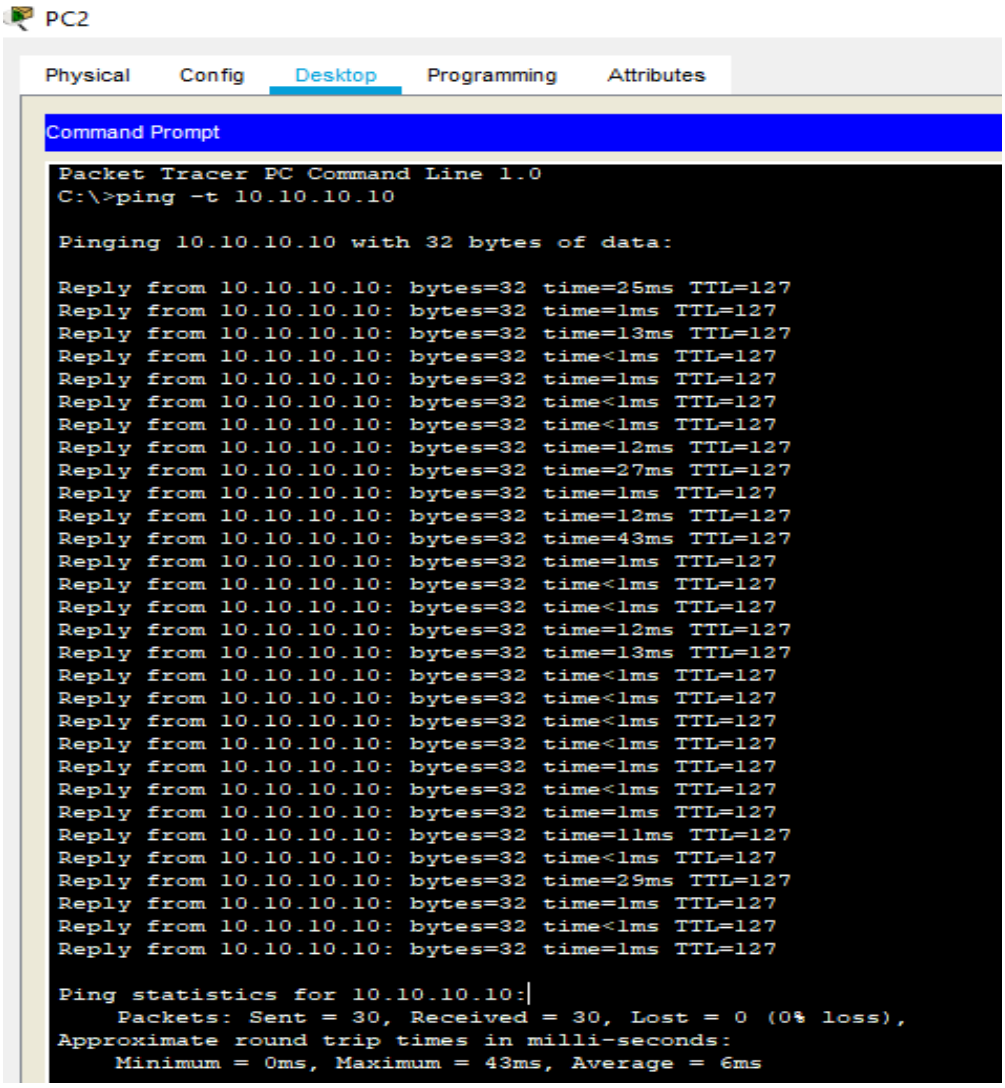


Figura 45: Ping PC2 – PC0
Fuente: Packet Tracer

3.2.10.8 Ping PC3 – PC0

En la figura 46 se puede observar que se envió 29 paquetes hacia la dirección IP de la PC 0 con un tiempo promedio de 8ms, a pesar de que hubo un paquete que su tiempo máximo de viaje fue de 47 ms no se tuvo ninguna pérdida de paquetes. Al realizar esta prueba con el comando PING se pudo verificar conectividad hacia el servidor de Internet

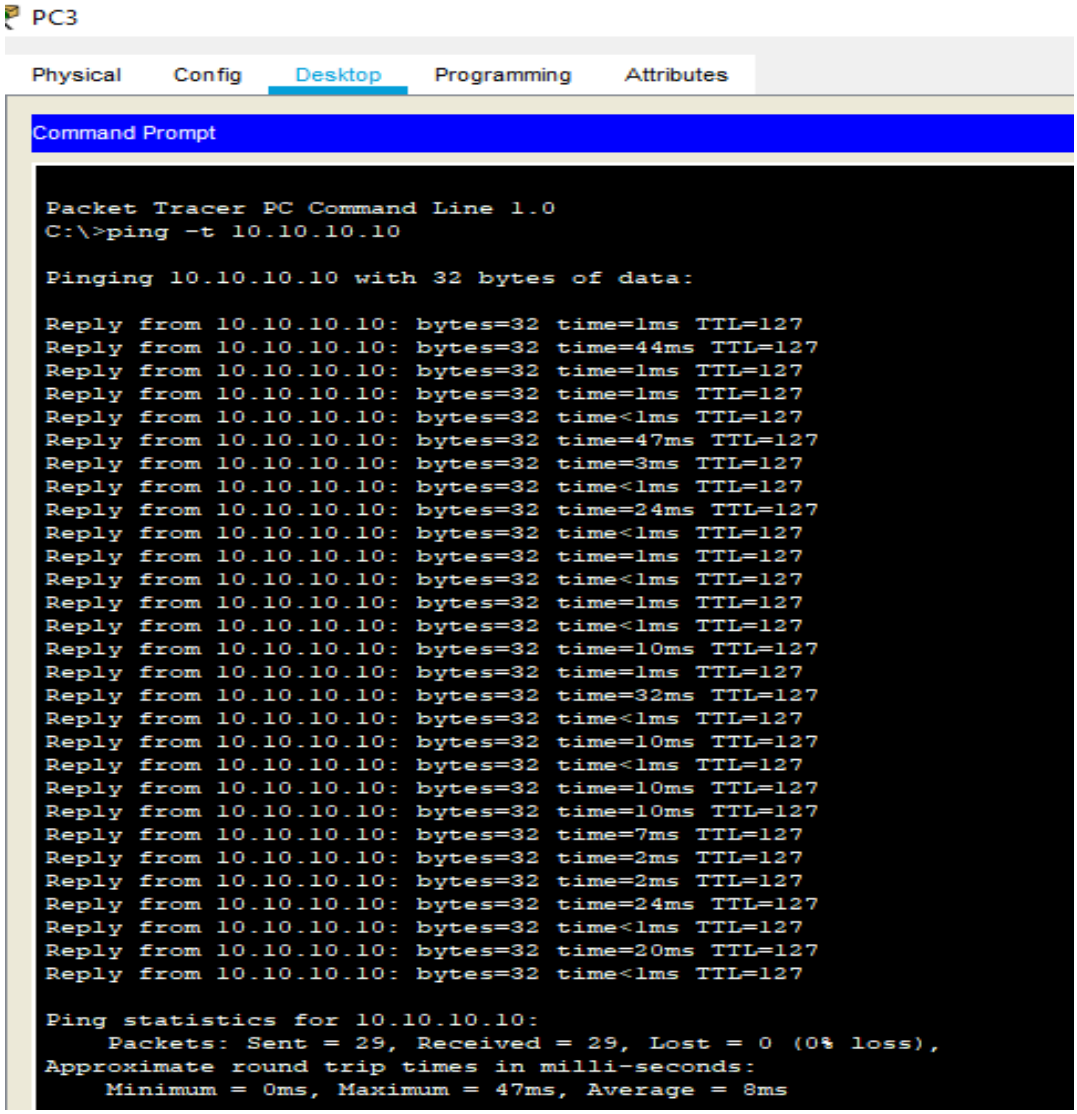


Figura 46: Ping PC3 – PC0

Fuente: Packet Tracer

3.2.11 Acta de solicitud y conformidad

Se realizó un acta de solicitud a los Ingenieros Residentes de la Superintendencia Nacional de Registros Públicos para la autorización de los cambios propuestos en el router principal de SUNARP-JUNIN, estos cambios implican agregar la configuración del protocolo Netflow y la configuración de las políticas de priorización. En el anexo 1 se podrá observar el acta de solicitud dirigido a los ingenieros residentes. En el anexo 2 se podrá observar el acta de conformidad emitido por el ingeniero residente de SUNARP.

3.2.12 Configuración del Protocolo Netflow

En la figura 47 se puede verificar el preciso momento donde se está configurando el protocolo Netflow. Como ya se hizo mención anteriormente primero se debe entrar al router Cisco y estar en modo privilegiado; en segundo lugar se debe entrar en modo configuración y poner la interfaz que se desea configurar para que fluya todo el tráfico; en tercer lugar se debe habilitar el flow y elegir la versión del protocolo con el que se trabajara y por último se debe configurar el lugar a donde se dirigirán todos los paquetes, en este caso al colector Netflow, así como también la interfaz de entrada del router(Leopoldo,2009).

Ahora para saber que IP está saturando la red se debe proceder con la configuración del comando ip flow top talkers, el cual su configuración consta en especificar la interfaz por donde entra todo el tráfico, el número máximo de dispositivos que se desea visualizar en la lista top y la unidad de información digital del tráfico.

```
username: asotelo
password:

SUNARP-CD179564_EL_TAMBO>en
SUNARP-CD179564_EL_TAMBO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SUNARP-CD179564_EL_T(config)#interface fastEthernet 0/0
SUNARP-CD179564_EL_T(config-if)#ip flow-export version 5 origin-as
SUNARP-CD179564_EL_T(config)#ip flow-export destination 10.28.128.130 4444
SUNARP-CD179564_EL_T(config)#ip flow-export source fastEthernet 0/0
SUNARP-CD179564_EL_T(config)#interface fastEthernet 0/0
SUNARP-CD179564_EL_T(config-if)#ip flow ingress
SUNARP-CD179564_EL_T(config-if)#ip flow egress
SUNARP-CD179564_EL_T(config-if)#ip flow-top-talkers
SUNARP-CD179564_EL_T(config-flow-top-talkers)#top 20
SUNARP-CD179564_EL_T(config-flow-top-talkers)#sort-by bytes
SUNARP-CD179564_EL_T(config-flow-top-talkers)#exit
SUNARP-CD179564_EL_T(config)#
```

Figura 47: Configuración del Protocolo Netflow
Fuente: Elaboración Propia

3.2.12.1 Prueba de la configuración realizada

En la figura 48 se puede visualizar mediante el comando show “running-config | i flow” la configuración ya realizada y guardada en el Router.

```
SUNARP-CD179564_EL_TAMBO#sh running-config | i flow
 ip flow ingress
 ip flow egress
ip flow-export source FastEthernet0/0
ip flow-export version 5 origin-as
ip flow-export destination 10.28.128.130 4444
ip flow-top-talkers
```

Figura 48: Prueba de la configuración realizada
Fuente: Elaboración Propia

3.2.12.2 Pruebas del funcionamiento del Netflow

Para verificar el funcionamiento del protocolo Netflow se usa el comando show ip flow top-talkers, con el fin de descubrir que dispositivo es el que consume un mayor ancho de banda. Las pruebas tuvieron una duración de 5 días, en los cuales se procedió a tomar una captura de pantalla diaria en el horario de 7:00 am y 15:00 pm para determinar el dispositivo que mayor ancho de banda consume. En la figura 49 se visualiza el comando a utilizar.

```
SUNARP-CD179564_EL_TAMBO#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/1         172.20.89.86    Fa0/0*        172.20.210.207  11 FAC3 00A1    74K
Fa0/0         172.20.211.254  Fa0/1         172.20.89.86    01 0000 0301    69K
Fa0/0         172.18.1.110    Null          172.20.89.63    11 D2B7 00A1  8221
Fa0/0         172.20.2.197    Fa0/1         172.20.89.120   11 13C4 13C4  3441
Fa0/0         172.20.2.197    Fa0/1         172.20.89.29    11 13C4 13C4  3380
Fa0/0         172.20.2.197    Fa0/1         172.20.89.28    11 13C4 13C4  3372
Fa0/0         172.20.2.197    Fa0/1         172.20.89.25    11 13C4 13C4  3303
Fa0/0         172.20.2.197    Fa0/1         172.20.89.18    11 13C4 13C4  3302
Fa0/0         172.20.2.197    Fa0/1         172.20.89.78    11 13C4 13C4  3302
Fa0/1         172.20.89.28    Fa0/0*        172.20.2.197    11 13C4 13C4  2431
Fa0/1         172.20.89.25    Fa0/0*        172.20.2.197    11 13C4 13C4  2362
Fa0/1         172.20.89.18    Fa0/0*        172.20.2.197    11 13C4 13C4  2361
Fa0/1         172.20.89.120   Fa0/0*        172.20.2.197    11 13C4 13C4  2228
Fa0/1         172.20.89.29    Fa0/0*        172.20.2.197    11 13C4 13C4  2164
Fa0/1         172.20.89.78    Fa0/0*        172.20.2.197    11 13C4 13C4  1314
Fa0/0         10.125.25.92    Local         10.132.236.234  06 EC3C 0017  1297
Fa0/0         172.20.2.197    Fa0/1         172.20.89.120   11 0000 0000  1097
Fa0/1         172.20.89.78    Fa0/0*        172.20.2.197    11 13C4 13C5  1047
Fa0/1         172.20.89.11    Fa0/0*        172.20.91.3     32 0101 55BD   432
Fa0/0         172.20.91.3     Fa0/1         172.20.89.11    32 0000 1D0C   432
20 of 20 top talkers shown. 40 flows processed.
```

Figura 49: Pruebas del funcionamiento del Netflow

Fuente: Servidor Trollin

3.2.13 Configuración de Calidad de Servicio (QoS)

En la figura 50 se puede observar el preciso momento donde se está configurando la priorización del tráfico, el cual tendrá un encolamiento de tipo CBWFQ + LLQ debido a que se hizo uso del comando Access List para definir manualmente el ancho de banda de los distintos tipos de tráfico y del método de prioridad para paquetes sensibles a la latencia como VoIP. Cabe recalcar que se determinó según el ingeniero residente el ancho de banda determinado de 2048 kbps equivalente a 2 megas al tráfico de datos(Plata) y un ancho de banda de 512 kbps equivalente a la mitad de un mega para el tráfico de voz, el cual es el tráfico de prioridad.

```
[gromero@trolin]/export/home/gromero: telnet 10.132.236.234
Trying 10.132.236.234...
Connected to 10.132.236.234.
Escape character is '^]'.

username: asotelo
password:

SUNARP-CD179564_EL_TAMBO>en
SUNARP-CD179564_EL_TAMBO#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SUNARP-CD179564_EL_T(config)#access-list 100 permit udp any any range 10000 65535
SUNARP-CD179564_EL_T(config)#access-list 100 permit udp any range 10000 65535 any
SUNARP-CD179564_EL_T(config)#access-list 100 permit tcp any any eq 1720
SUNARP-CD179564_EL_T(config)#access-list 100 permit tcp any eq 1720 any
SUNARP-CD179564_EL_T(config)#access-list 100 permit ip 172.20.2.128 0.0.0.63 any
SUNARP-CD179564_EL_T(config)#access-list 100 permit ip any 172.20.2.128 0.0.0.63
SUNARP-CD179564_EL_T(config)#access-list 100 permit ip 172.20.2.192 0.0.0.63 any
SUNARP-CD179564_EL_T(config)#access-list 100 permit ip any 172.20.2.192 0.0.0.63
SUNARP-CD179564_EL_T(config)#access-list 104 permit ip any any
SUNARP-CD179564_EL_T(config)#class-map VOICE
SUNARP-CD179564_EL_T(config-cmap)#match access-group 100
SUNARP-CD179564_EL_T(config-cmap)#exit
SUNARP-CD179564_EL_T(config)#class-map PLATA
SUNARP-CD179564_EL_T(config-cmap)#match access-group 104
SUNARP-CD179564_EL_T(config-cmap)#exit
SUNARP-CD179564_EL_T(config)#policy-map IPVPN
SUNARP-CD179564_EL_T(config-pmap)#class VOICE
SUNARP-CD179564_EL_T(config-pmap-c)#priority 512
SUNARP-CD179564_EL_T(config-pmap-c)#set ip precedence 5
SUNARP-CD179564_EL_T(config-pmap-c)#exit
SUNARP-CD179564_EL_T(config-pmap)#class PLATA
SUNARP-CD179564_EL_T(config-pmap-c)#bandwidth 2048
SUNARP-CD179564_EL_T(config-pmap-c)#set ip precedence 1
SUNARP-CD179564_EL_T(config-pmap-c)#exit
SUNARP-CD179564_EL_T(config-pmap)#class class-default
SUNARP-CD179564_EL_T(config-pmap-c)#fair-queue
SUNARP-CD179564_EL_T(config-pmap-c)#exit
SUNARP-CD179564_EL_T(config-pmap)#exit
SUNARP-CD179564_EL_T(config)#exit
SUNARP-CD179564_EL_TAMBO#
```

Figura 50: Configuración de Calidad de Servicio (QoS)
Fuente: Servidor Trollin

3.2.13.1 Prueba de configuración realizada QoS

En la imagen 51 se puede visualizar mediante el comando “show running-config | i class” la configuración ya realizada y guardada de las clases de tráfico en el router.

```
SUNARP-CD179564_EL_TAMBO#sh running-config | i class
class-map match-all PLATA
class-map match-all VOICE
 class VOICE
 class PLATA
 class class-default
```

Figura 51: Prueba de configuración realizada QoS

Fuente: Servidor Trollin

Asimismo en las figura 52 se puede verificar que la configuración propuesta ya se visualiza cuando se ejecuta el comando sh running-config. Cabe recalcar que no se muestra la imagen de los Access List debido a que están junto a otras configuraciones confidenciales de la empresa.

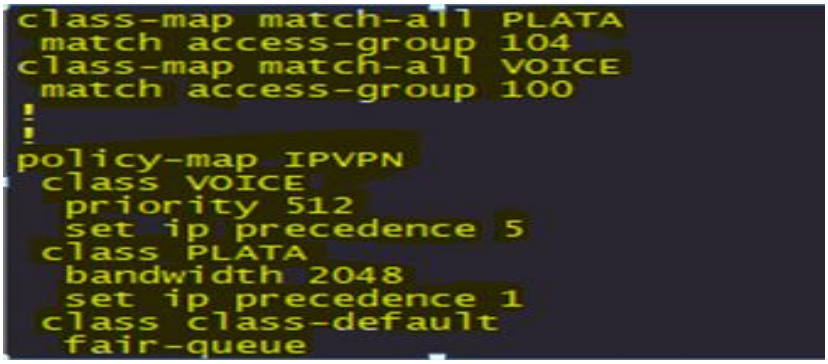


Figura 52: Configuración de Priorización de Tráfico
Fuente: Servidor Trollin

3.2.14 Diagrama de Gantt

En la figura 53 se observa el Diagrama de Gantt, el cual especifica la secuencia que se siguió para elaborar el presente trabajo.

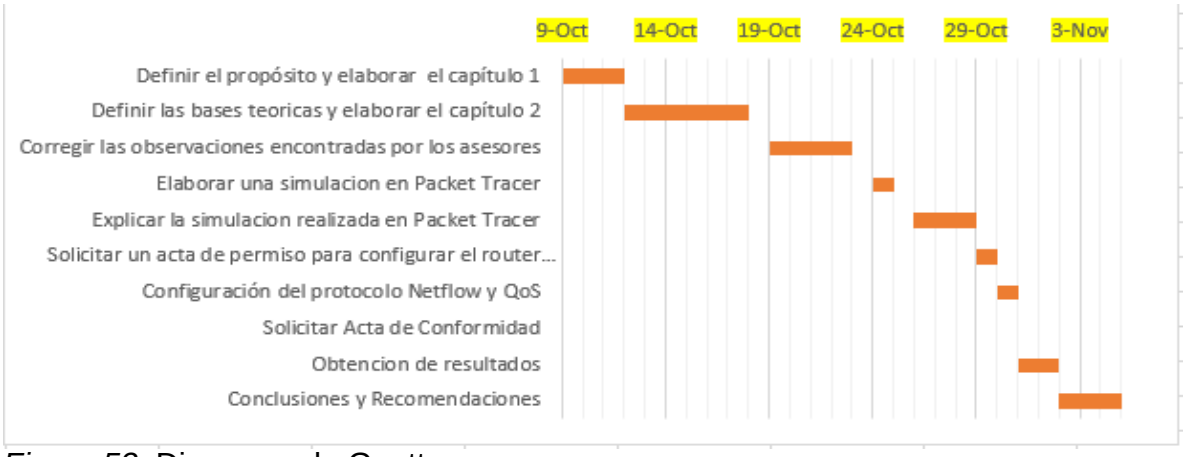


Figura 53: Diagrama de Gantt
Fuente: Elaboración Propia

3.2.15 Diagrama de Bloques

En la figura 54 se observa el Diagrama de bloques, el cual específica la secuencia que se siguió para la configuración del protocolo Netflow.

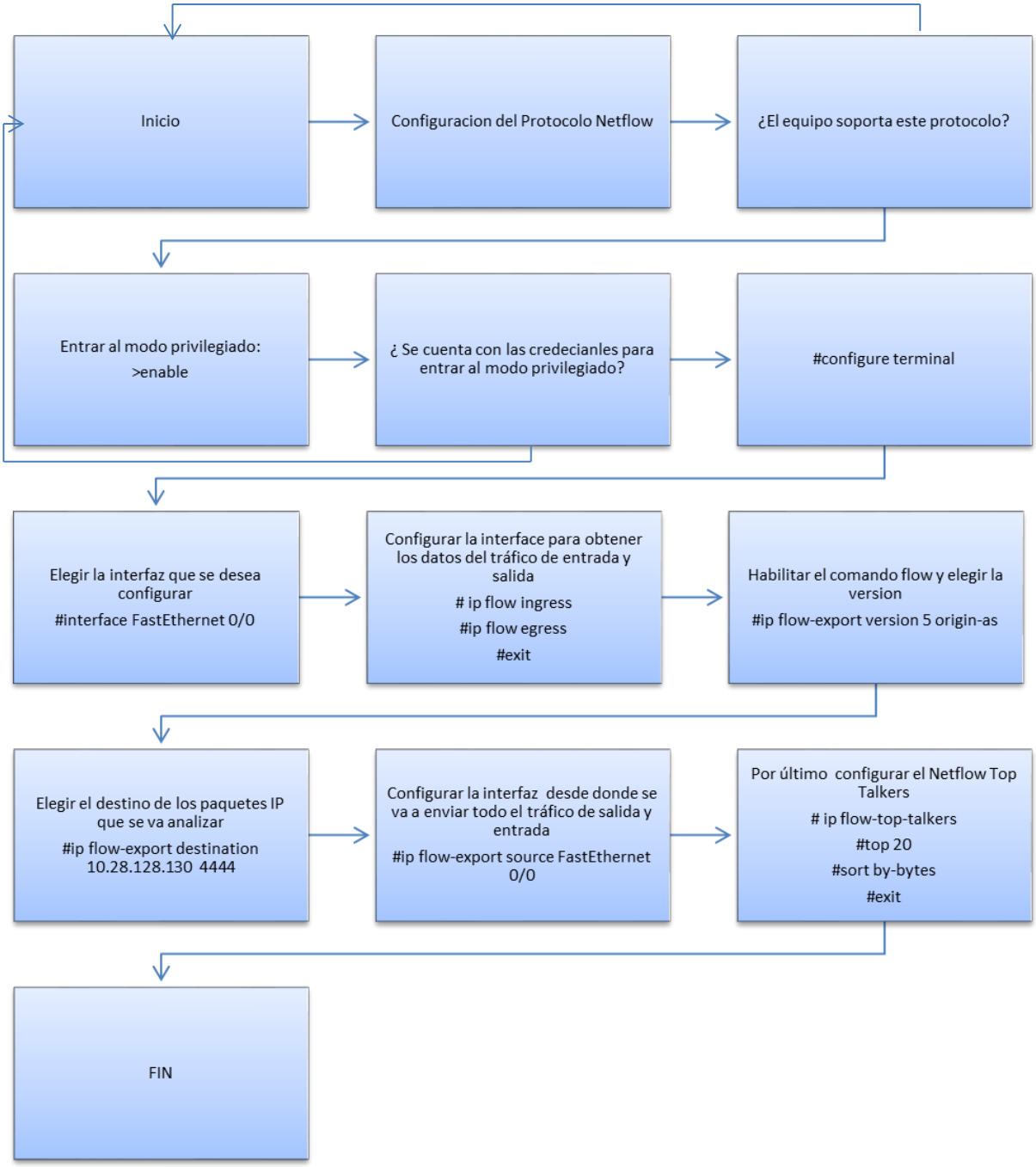


Figura 54: Diagrama de Bloques del protocolo Netflow
Fuente: Elaboración Propia

3.3 RESULTADOS

3.3.1 Tráfico de la red LAN de SUNARP

En la imagen 55 se puede observar que gracias a la implementación del protocolo Netflow y a la herramienta Netflow Traffic Analyzer se puede visualizar el tráfico en tiempo real; en este caso se puede verificar que a las 12:00 pm se obtuvo un promedio de tráfico transmitido de 28,0 kbps y un promedio de tráfico recibido de 492,5 kbps; obteniendo así un mejor monitoreo el cual ayudará a evitar un posible saturamiento que afecte el rendimiento de la red.

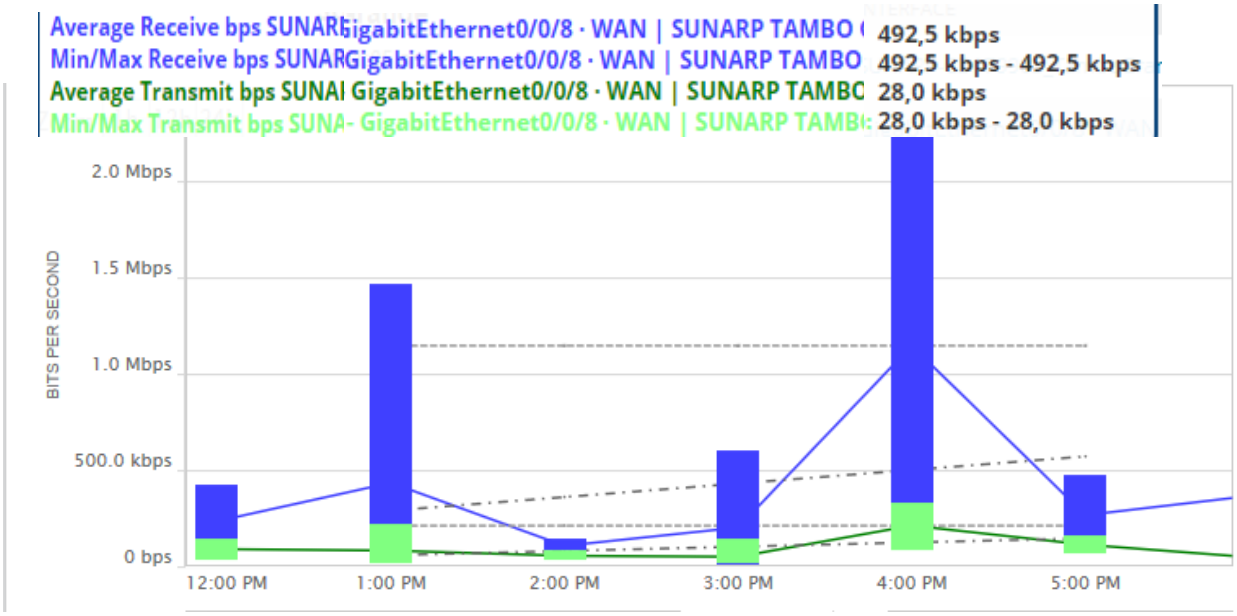


Figura 55: Tráfico de la red LAN de SUNARP
Fuente: Netflow Analyzer Traffic

3.3.2 Latencia y Perdida de paquetes antes de la implementación

La información respecto a la latencia y la pérdida de paquetes se dará gracias a la herramienta Netflow Analyzer Traffic (SolarWinds). Para saber los resultados se tomarán como prueba la información registrada desde el 28 de Octubre hasta el 30 de Octubre.

3.3.2.1 Dia 28 de Octubre

En la figura 56 se puede visualizar el tiempo de latencia desde las 2:49 am hasta las 8:16p m del día 28 de Octubre, siendo el horario de la mañana donde se alcanzó el mayor pico de latencia (80.29 ms). Por otro lado, la imagen muestra que no se presentó pérdida de paquetes en este lapso de tiempo.

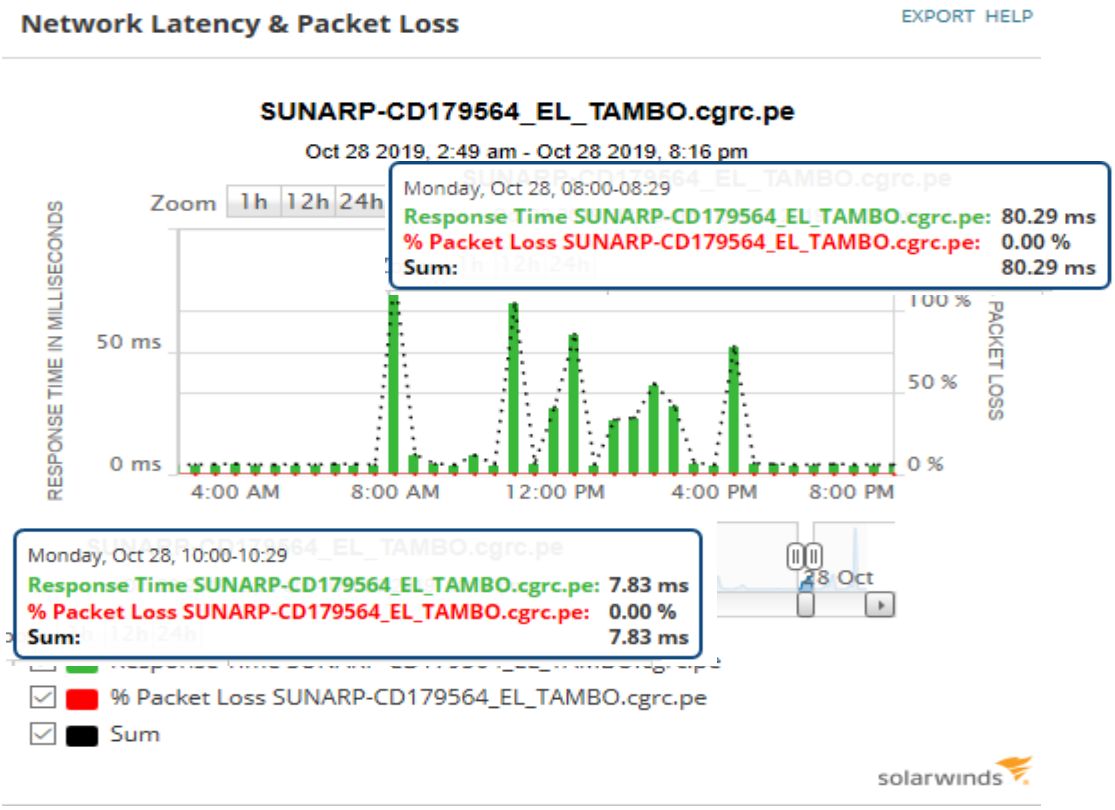


Figura 56 : Latencia del día 28 de Octubre
Fuente: Netflow Analyzer Traffic

3.3.2.2 Dia 29 de Octubre

En la figura 57 se puede visualizar el tiempo de latencia desde las 1:38 am hasta las 11:27pm del día 29 de Octubre, siendo el horario de la tarde donde se alcanzó el mayor pico de latencia (148.13 ms). Por otro lado la figura muestra que aproximadamente a las 6:00 am se presentó un 10% de pérdida de paquetes afectando así el rendimiento de la red.

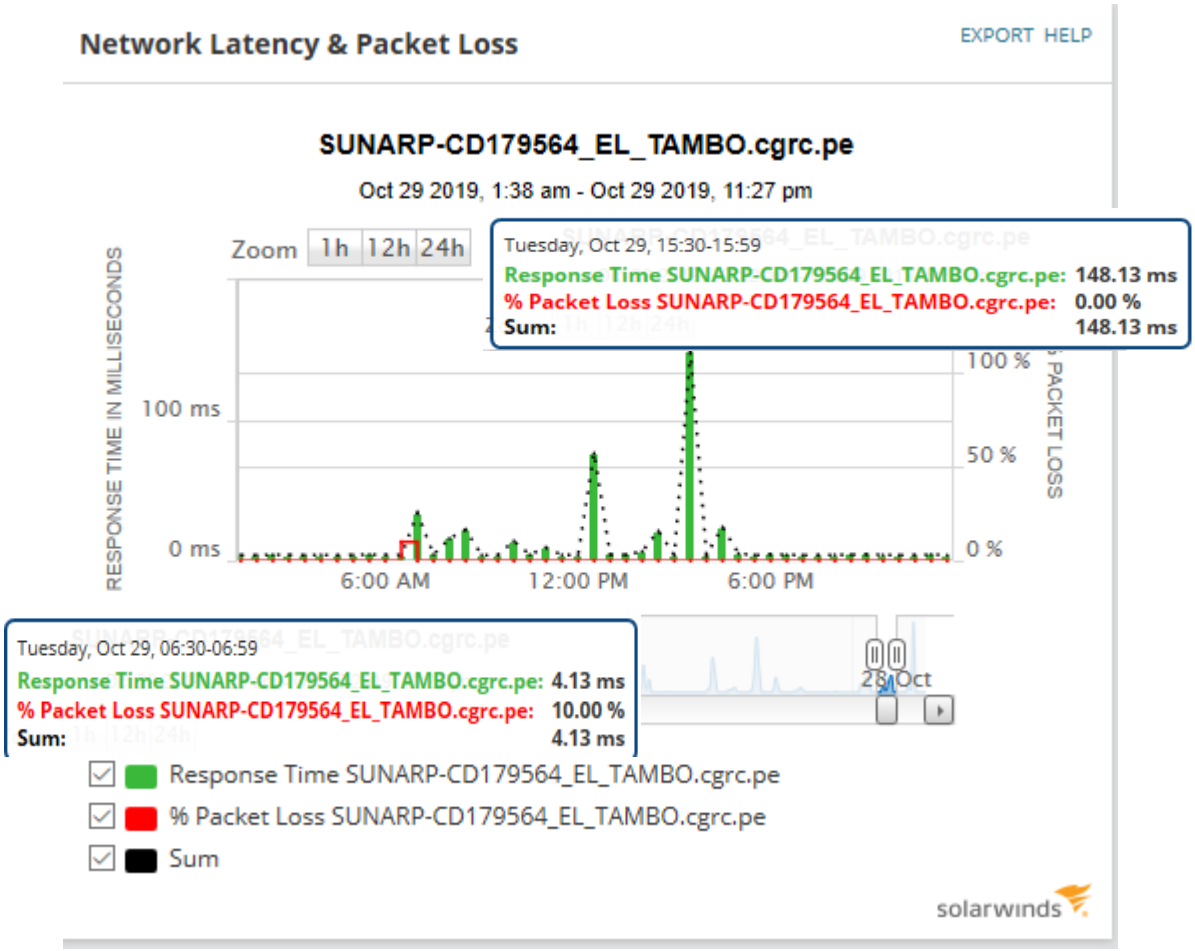


Figura 57: Latencia del día 29 de Octubre
Fuente: Netflow Analyzer Traffic

3.3.2.3 Dia 30 de Octubre

En la figura 58 se puede visualizar el tiempo de latencia desde las 1:53 am hasta las 9:31pm del día 30 de Octubre, siendo el horario de la tarde donde se alcanzó el mayor pico de latencia (427.75ms). Por otro lado, la figura muestra que aproximadamente a las 5:00 am se presentó un 5% de pérdida de paquetes.

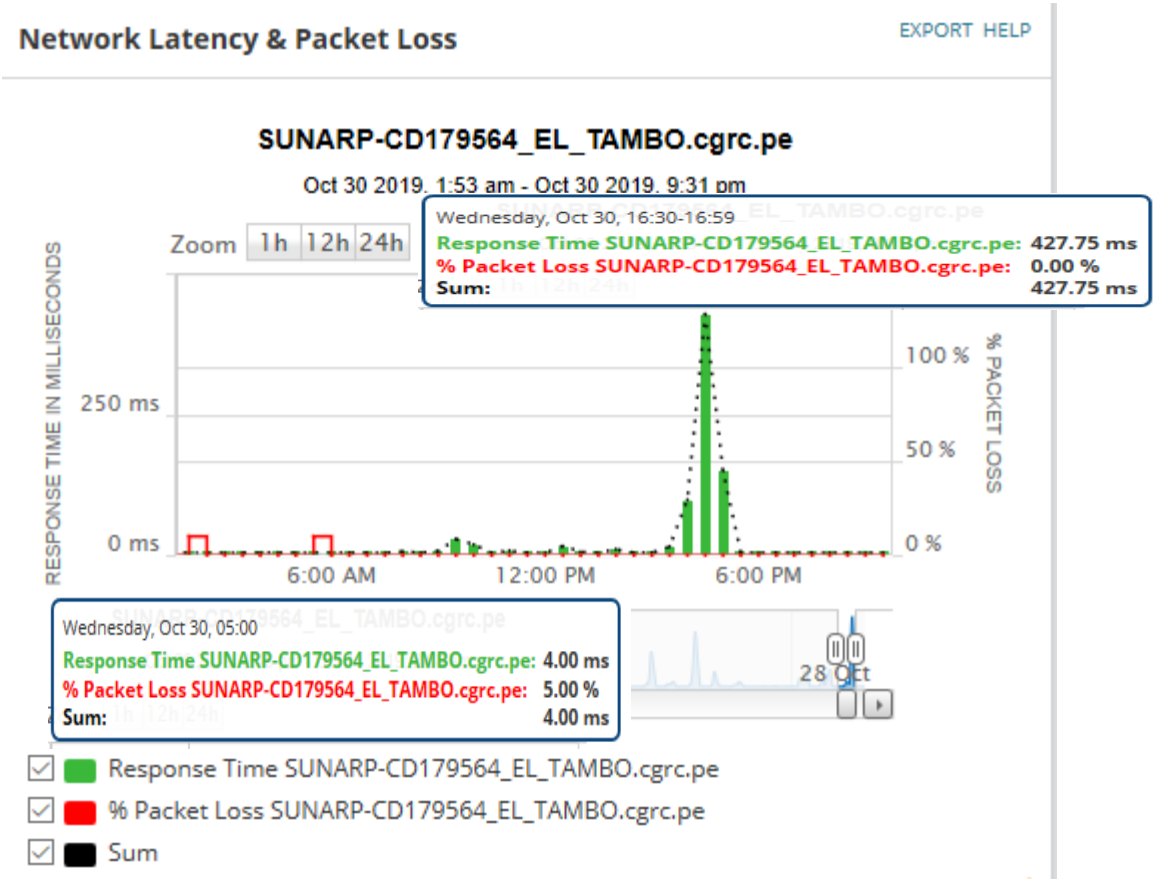


Figura 58: Latencia del día 30 de Octubre
Fuente: Netflow Analyzer Traffic

3.3.3 Latencia y Pérdida de paquetes después de la implementación

La información respecto a la latencia y la pérdida de paquetes se dará gracias a la herramienta Netflow Analyzer Traffic (SolarWinds). Para saber los resultados de la implementación de la propuesta se tomará como prueba la información registrada desde el 31 de Octubre hasta el 2 de Noviembre.

3.3.3.1 Día 31 de Octubre

En la figura 59 se puede visualizar el tiempo de latencia desde las 3:00 am hasta las 10:28pm del día 31 de Octubre, siendo el horario de la tarde donde se

alcanzó el mayor pico de latencia (4.63 ms). Por otro lado la figura muestra que aproximadamente que no se presentó perdida de paquetes en este lapso de tiempo.

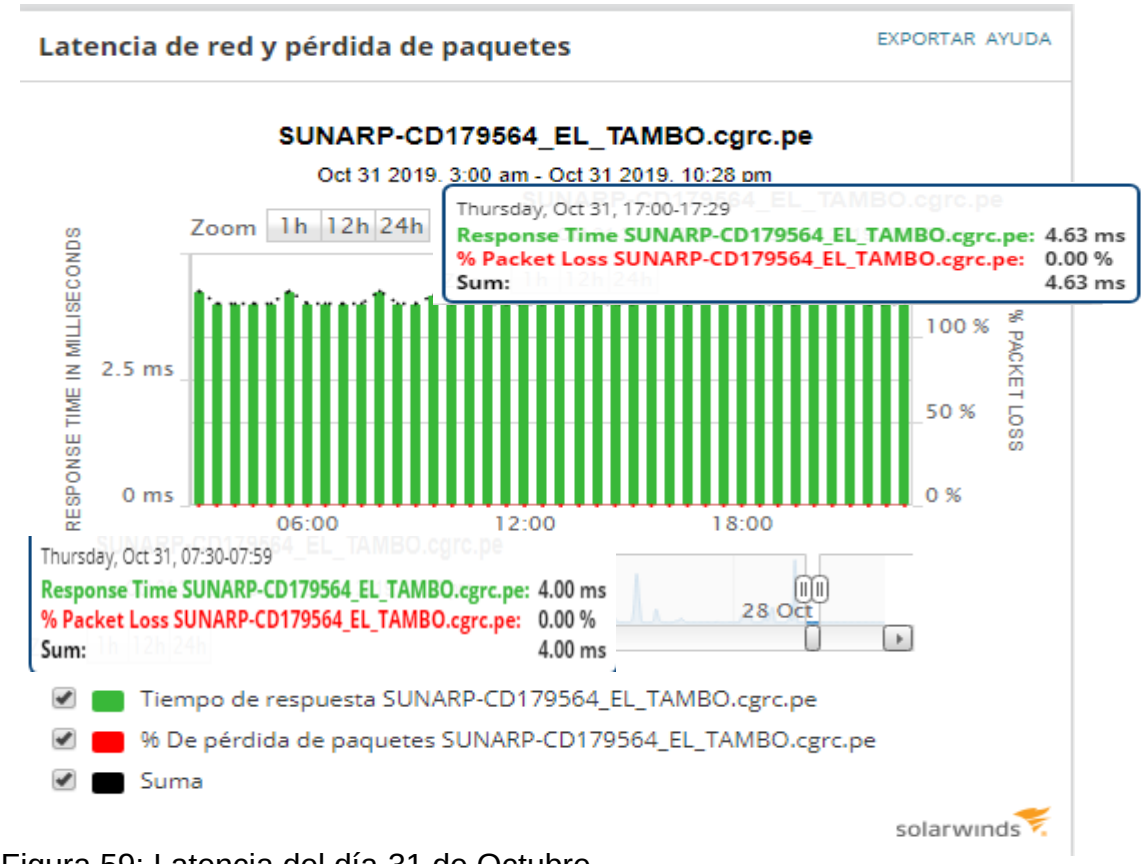


Figura 59: Latencia del día 31 de Octubre

Fuente: Netflow Analyzer Traffic

3.3.3.2 Día 1 de Noviembre

En la figura 60 se puede visualizar el tiempo de latencia desde las 3:18 am hasta las 10:46 pm del día 1 de Noviembre, siendo el horario de la mañana donde se alcanzó el mayor pico de latencia (4.50 ms). Por otro lado se verifica que no se obtuvo ninguna pérdida de paquetes y el tiempo promedio de latencia no sube de los 5 ms a comparación de los anteriores días que superaban los 427 ms.

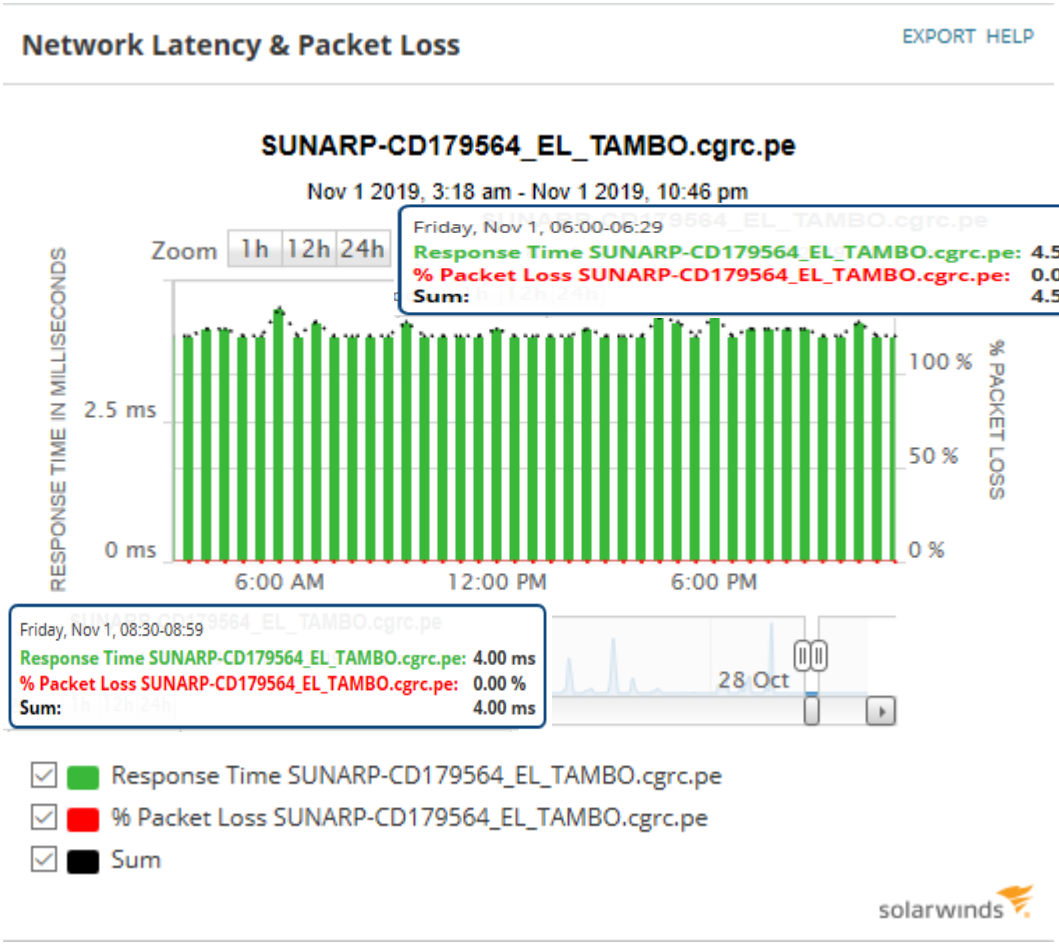


Figura 60: Latencia del día 1 de Noviembre
Fuente: Netflow Analyzer Traffic

3.3.3.3 Día 2 de Noviembre

En la figura 61 se puede visualizar el tiempo de latencia desde las 1:40 am hasta las 11:18 pm del día 1 de Noviembre, siendo el horario de la tarde donde se alcanzó el mayor pico de latencia (5.38 ms). Por otro lado, se verifica que no se obtuvo ninguna pérdida de paquetes y el tiempo promedio de latencia no sube de los 6 ms a comparación de los anteriores días que superaban los 427 ms.

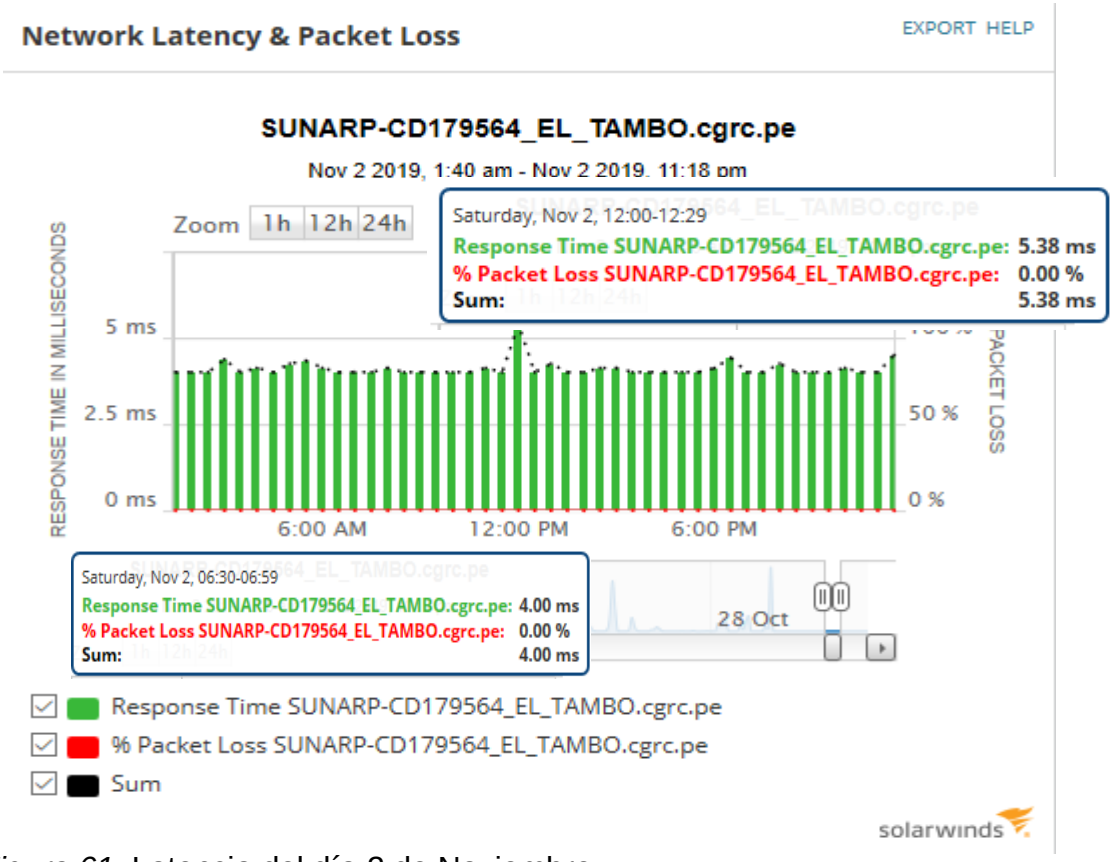


Figura 61: Latencia del día 2 de Noviembre

Fuente: Netflow Analyzer Traffic

3.3.4 Cálculo promedio de la latencia

3.3.4.1 Latencia promedio del 28 Octubre hasta el 30 de Octubre

Tabla 5: Latencia Promedio

Día	Latencia
28 de Octubre	80.29ms
29 de Octubre	148.13ms
30 de Octubre	427.13ms

Fuente: Elaboración propia

$$\frac{80.29 + 148.13 + 427.75}{3} = \mathbf{218.72\ ms}$$

3.3.4.2 Latencia promedio del 31 Octubre hasta el 2 de Noviembre

Tabla 6: Latencia después de la implementación

Día	Latencia
31 de Octubre	4.63ms
1 de Noviembre	4.50ms
2 de Noviembre	5.38ms

Fuente: Elaboración propia

$$\frac{4.63 + 4.50 + 5.38}{3} = \mathbf{4.8366\ ms}$$

3.3.4.3 Cálculo del porcentaje de latencia después de la implementación

$$218.72 = 100\ \%$$

$$4.8366 = \mathbf{x}$$

$$\frac{4.8366\ \times 100}{218.72} = \mathbf{2.2113}\ \%$$

3.3.4.4 Cálculo del porcentaje de mejora de la latencia

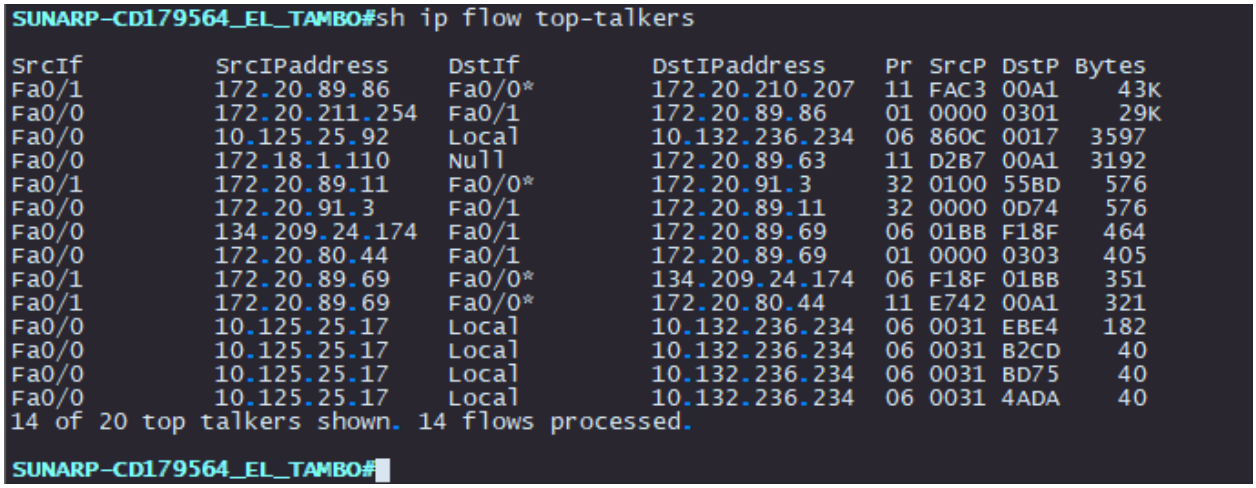
$$100\% - 2.2113\ \% = \mathbf{97.78}\ \%$$

3.3.5 Consumo de Ancho de Banda

La información respecto al consumo de ancho de banda se dará gracias al protocolo Netflow previamente configurado en el Router. Para saber los resultados de la aplicación de la propuesta se tomará como prueba la información registrada desde el 31 de Octubre hasta el 2 de Noviembre.

3.3.5.1 Día 31 de Octubre (Turno Mañana)

Como se observa en la figura 62, se verifica que la dirección IP 172.20.89.86 y la dirección IP 172.20.211.254 son las direcciones que mayor ancho de banda han consumido en el turno de 7:00 – 12:00am, sumando un total de 72 KB de los 3MB de ancho de banda contratado.



```
SUNARP-CD179564_EL_TAMBO#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/1         172.20.89.86    Fa0/0*        172.20.210.207  11 FAC3 00A1   43K
Fa0/0         172.20.211.254  Fa0/1         172.20.89.86    01 0000 0301   29K
Fa0/0         10.125.25.92    Local         10.132.236.234  06 860C 0017  3597
Fa0/0         172.18.1.110    Null          172.20.89.63    11 D2B7 00A1  3192
Fa0/1         172.20.89.11    Fa0/0*        172.20.91.3     32 0100 55BD   576
Fa0/0         172.20.91.3     Fa0/1         172.20.89.11    32 0000 0D74   576
Fa0/0         134.209.24.174  Fa0/1         172.20.89.69    06 01BB F18F   464
Fa0/0         172.20.80.44    Fa0/1         172.20.89.69    01 0000 0303   405
Fa0/1         172.20.89.69    Fa0/0*        134.209.24.174  06 F18F 01BB   351
Fa0/1         172.20.89.69    Fa0/0*        172.20.80.44    11 E742 00A1   321
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 EBE4   182
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 B2CD    40
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 BD75    40
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 4ADA    40
14 of 20 top talkers shown. 14 flows processed.

SUNARP-CD179564_EL_TAMBO#
```

Figura 62: Consumo del ancho de banda en el turno mañana del 31/10
Fuente: Servidor Trollin

3.3.5.2 Día 31 de Octubre (Turno Tarde)

Como se observa en la figura 63, se verifica que las direcciones IP: 172.20.89.86 – 172.20.72.10 son las direcciones que mayor ancho de banda han consumido en el turno de 12:00 – 18:00pm, sumando un total de 4237 KB de los 3MB de ancho de banda contratado.

```
SUNARP-CD179564_EL_TAMBO#show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/1         172.20.89.86    Fa0/0*        172.20.210.9    06 170C DC33  2180K
Fa0/0         172.20.72.10    Fa0/1         172.20.89.83    06 01BD C289  2057K
Fa0/1         172.20.89.83    Fa0/0*        172.20.72.10    06 C289 01BD  1165K
Fa0/0         168.61.52.70    Fa0/1         172.20.89.111   06 01BB FD6E   327K
Fa0/0         168.61.52.70    Fa0/1         172.20.89.111   06 01BB FD70   314K
Fa0/0         168.61.52.70    Fa0/1         172.20.89.111   06 01BB FD71   112K
Fa0/0         172.20.210.9    Fa0/1         172.20.89.86    06 DC33 170C    23K
Fa0/1         172.20.89.111   Fa0/0*        168.61.52.70    06 FD71 01BB    10K
Fa0/1         172.20.89.111   Fa0/0*        168.61.52.70    06 FD70 01BB    10K
Fa0/1         172.20.89.111   Fa0/0*        168.61.52.70    06 FD72 01BB    10K
Fa0/1         172.20.89.111   Fa0/0*        168.61.52.70    06 FD6D 01BB  9176
Fa0/1         172.20.89.111   Fa0/0*        168.61.52.70    06 FD6F 01BB  8737
Fa0/1         172.20.89.98    Fa0/0*        172.20.80.242   01 0000 0800  7612
Fa0/0         172.20.80.242   Fa0/1         172.20.89.98    01 0000 0000  7612
Fa0/1         172.20.89.125   Fa0/0*        172.20.80.242   01 0000 0800  7568
Fa0/1         172.20.89.111   Fa0/0*        168.61.52.70    06 FD6E 01BB  7438
Fa0/1         172.20.89.115   Fa0/0*        172.20.80.242   01 0000 0800  7216
Fa0/0         172.20.80.242   Fa0/1         172.20.89.115   01 0000 0000  7216
Fa0/1         172.20.89.107   Fa0/0*        172.217.204.189 11 DBEA 01BB  6190
Fa0/1         172.20.89.117   Fa0/0*        108.177.11.189  11 F9DE 01BB  5960
20 of 20 top talkers shown. 216 flows processed.
```

Figura 63: Consumo del ancho de banda en el turno tarde del 31/10
Fuente: Servidor Trollin

3.3.5.3 Día 1 de Noviembre (Turno Mañana)

Como se observa en la figura 64, se verifica que la dirección IP 172.18.1.110 ha consumido 25 KB de los 3MB de ancho de banda contratado siendo así la dirección IP que mayor ancho de banda ha consumido en el turno de 7:00 – 12:00am.

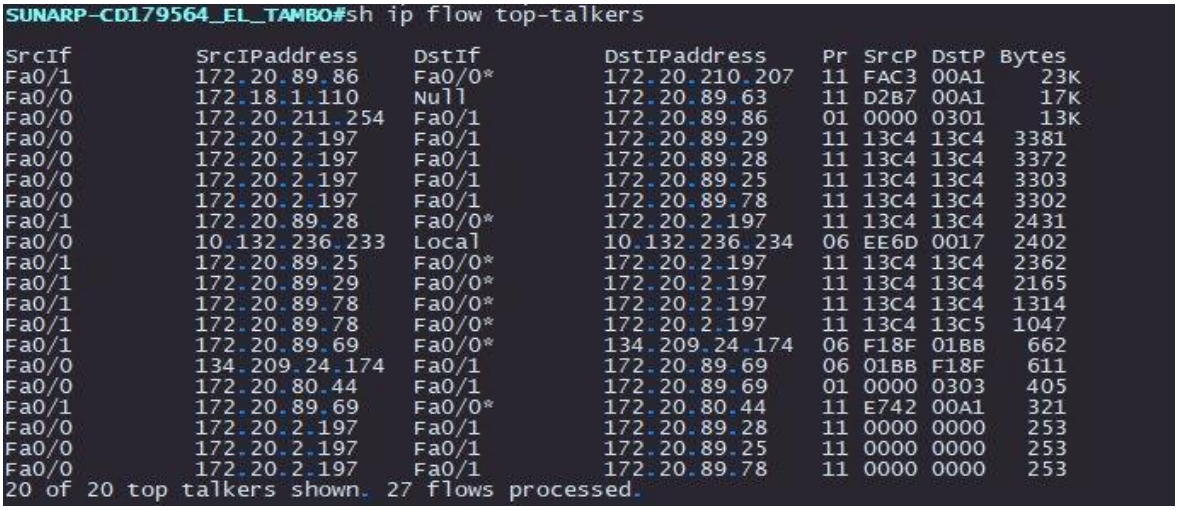
```
SUNARP-CD179564_EL_TAMBO#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/0         172.18.1.110    Null          172.20.89.63    11 D2B7 00A1   25K
Fa0/0         172.20.211.254  Fa0/1         172.20.89.69    01 0000 0301  5500
Fa0/0         172.20.2.197    Fa0/1         172.20.89.17    11 13C4 13C4  5209
Fa0/1         172.20.89.86    Fa0/0*        172.20.210.207  11 FAC3 00A1  4182
Fa0/1         172.20.89.17    Fa0/0*        172.20.2.197    11 13C4 13C4  3709
Fa0/0         172.20.2.197    Fa0/1         172.20.89.120   11 13C4 13C4  2023
Fa0/1         172.20.89.120   Fa0/0*        172.20.2.197    11 13C4 13C4  1695
Fa0/0         172.20.211.254  Fa0/1         172.20.89.86    01 0000 0301  1044
Fa0/0         178.128.235.246 Fa0/1         172.20.89.69    06 01BB F145   948
Fa0/1         172.20.89.69    Fa0/0*        178.128.235.246 06 F145 01BB   722
Fa0/1         172.20.89.11    Fa0/0*        172.20.91.3     32 0101 55BD   432
Fa0/0         172.20.91.3     Fa0/1         172.20.89.11    32 0000 1D0C   432
Fa0/0         172.20.2.197    Fa0/1         172.20.89.17    11 0000 0000   253
Fa0/0         10.125.25.92    Local         10.132.236.234  06 EC3C 0017   248
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 70B8   182
Fa0/1         172.20.89.69    Fa0/0*        172.20.80.242   06 C239 DEFC   152
Fa0/1         172.20.89.69    Fa0/0*        172.20.80.248   06 C23F 01BD   152
Fa0/1         172.20.89.69    Fa0/0*        172.20.80.247   06 C23E 01BD   152
Fa0/1         172.20.89.69    Fa0/0*        172.20.80.240   06 C236 01BD   152
Fa0/1         172.20.89.69    Fa0/0*        172.20.80.241   06 C237 01BD   152
20 of 20 top talkers shown. 31 flows processed.
```

Figura 64: Consumo del ancho de banda en el turno mañana del 01/11
Fuente: Servidor Trollin

3.3.5.4 Día 1 de Noviembre (Turno Tarde)

Como se observa en la figura 65 se verifica que las direcciones IP: 172.20.89.86 - 172.18.1.110 - 172.20.211.254 son las direcciones que mayor ancho de banda han consumido en el turno de 12:00 – 18.00 pm, sumando un total de 53 KB de los 3 MB de ancho de banda contratado.



```
SUNARP-CD179564_EL_TAMBO#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/1         172.20.89.86    Fa0/0*        172.20.210.207  11 FAC3 00A1    23K
Fa0/0         172.18.1.110    Null          172.20.89.63    11 D2B7 00A1    17K
Fa0/0         172.20.211.254  Fa0/1         172.20.89.86    01 0000 0301    13K
Fa0/0         172.20.2.197    Fa0/1         172.20.89.29    11 13C4 13C4  3381
Fa0/0         172.20.2.197    Fa0/1         172.20.89.28    11 13C4 13C4  3372
Fa0/0         172.20.2.197    Fa0/1         172.20.89.25    11 13C4 13C4  3303
Fa0/0         172.20.2.197    Fa0/1         172.20.89.78    11 13C4 13C4  3302
Fa0/1         172.20.89.28    Fa0/0*        172.20.2.197    11 13C4 13C4  2431
Fa0/0         10.132.236.233  Local         10.132.236.234  06 EE6D 0017  2402
Fa0/1         172.20.89.25    Fa0/0*        172.20.2.197    11 13C4 13C4  2362
Fa0/1         172.20.89.29    Fa0/0*        172.20.2.197    11 13C4 13C4  2165
Fa0/1         172.20.89.78    Fa0/0*        172.20.2.197    11 13C4 13C4  1314
Fa0/1         172.20.89.78    Fa0/0*        172.20.2.197    11 13C4 13C5  1047
Fa0/1         172.20.89.69    Fa0/0*        134.209.24.174  06 F18F 01BB   662
Fa0/0         134.209.24.174  Fa0/1         172.20.89.69    06 01BB F18F   611
Fa0/0         172.20.80.44    Fa0/1         172.20.89.69    01 0000 0303   405
Fa0/1         172.20.89.69    Fa0/0*        172.20.80.44    11 E742 00A1   321
Fa0/0         172.20.2.197    Fa0/1         172.20.89.28    11 0000 0000   253
Fa0/0         172.20.2.197    Fa0/1         172.20.89.25    11 0000 0000   253
Fa0/0         172.20.2.197    Fa0/1         172.20.89.78    11 0000 0000   253
20 of 20 top talkers shown. 27 flows processed.
```

Figura 65: Consumo del ancho de banda en el turno tarde del 01/11

Fuente: Servidor Trollin

3.3.5.5 Día 2 de Noviembre (Turno Mañana)

Como se observa en la figura 66, se verifica que la direcciones IP: 172.20.89.86 – 172.20.211.254 – 172.18.1.110 son las direcciones que mayor ancho de banda han consumido en el turno de 7:00 – 12:00am, sumando un total de 105 KB de los 3 MB de ancho de banda contratado.

```
SUNARP-CD179564_EL_TAMBO#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/1         172.20.89.86    Fa0/0*        172.20.210.207  11 FAC3 00A1   53K
Fa0/0         172.20.211.254  Fa0/1         172.20.89.86    01 0000 0301   41K
Fa0/0         172.18.1.110    Null          172.20.89.63    11 D2B7 00A1   11K
Fa0/0         10.125.25.92    Local         10.132.236.234  06 860C 0017   327
Fa0/0         134.209.24.174  Fa0/1         172.20.89.69    06 01BB F18F   317
Fa0/1         172.20.89.11    Fa0/0*        172.20.91.3     32 0100 55BD   216
Fa0/0         172.20.91.3     Fa0/1         172.20.89.11    32 0000 0D74   216
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 8F05   182
Fa0/1         172.20.89.69    Fa0/0*        172.20.72.10    11 007B 007B    96
Fa0/0         172.20.72.10    Fa0/1         172.20.89.69    11 007B 007B    96
Fa0/0         172.19.14.180   Local         10.132.236.234  01 0000 0800    75
Fa0/1         172.20.89.11    Fa0/0*        172.20.91.3     11 0400 01F4    72
Fa0/1         172.20.89.11    Fa0/0*        172.19.12.5     11 0400 01F4    72
Fa0/1         172.20.89.69    Fa0/0*        134.209.24.174  06 F18F 01BB    40
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 8F05    40
15 of 20 top talkers shown. 15 flows processed.
```

Figura 66: Consumo del ancho de banda en el turno mañana del 02/11

Fuente: Servidor Trollin

3.3.5.6 Día 2 de Noviembre (Turno Tarde)

Como se observa en la figura 67, se verifica que la direcciones IP: 172.20.89.86 – 172.20.211.254 – 172.18.1.110 son las direcciones que mayor ancho de banda han consumido en el turno de 12:00 – 18:00am, sumando un total de 186KB de los 3MB de ancho de banda contratado.

```
SUNARP-CD179564_EL_TAMBO#sh ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Fa0/1         172.20.89.86    Fa0/0*        172.20.210.207  11 EE88 00A1   82K
Fa0/0         172.20.211.254  Fa0/1         172.20.89.86    01 0000 0301   76K
Fa0/0         172.18.1.110    Null          172.20.89.63    11 D2B7 00A1   28K
Fa0/1         172.20.89.26    Fa0/0*        172.20.80.242   06 F1B6 01BD 4450
Fa0/0         172.20.80.242   Fa0/1         172.20.89.26    06 01BD F1B6 1983
Fa0/0         10.125.25.92    Local         10.132.236.234  06 D27D 0017 1025
Fa0/1         172.20.89.11    Fa0/0*        172.20.91.3     32 0101 55BD  216
Fa0/0         172.20.91.3     Fa0/1         172.20.89.11    32 0000 38B6  216
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 D68A  182
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 787A  182
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 8EE8  181
Fa0/1         172.20.89.26    Fa0/0*        172.20.80.242   06 F1B6 01BD   80
Fa0/0         172.20.80.242   Fa0/1         172.20.89.26    06 01BD F1B6   80
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 A285   40
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 C1D1   40
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 8EE8   40
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 5A28   40
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 5ACF   40
Fa0/0         10.125.25.17    Local         10.132.236.234  06 0031 787A   40
19 of 20 top talkers shown. 19 flows processed.
```

Figura 67 : Consumo del ancho de banda en el turno tarde del 02/11

Fuente: Servidor Trollin

CONCLUSIONES

- Se logró aplicar la propuesta en la red LAN de SUNARP, recibiendo la conformidad por parte del cliente y de los ingenieros residentes.

- Se determinó que el nivel de la calidad de servicio en primera instancia fue baja, debido a que la red utilizaba un encolamiento tipo FIFO; provocando de esta manera que la red alcance picos de latencia de 427.75ms.

- A comparación del resultado obtenido por el Sr. Villadiego Angulo en su tesis titulada: “Técnicas de optimización del ancho de banda en las redes LAN-PARTE II”, se verificó en los 3 días de prueba que la implementación del protocolo Netflow logró reducir la perdida de paquetes en un 99.9%, convirtiéndolo en una técnica importante junto a la calidad de servicio para la optimización de ancho de banda.

- A través de la implementación del protocolo Netflow y la herramienta Netflow Traffic Analyzer se determinó que el turno tarde es el horario donde la red LAN de SUNARP presenta un mayor consumo de ancho de banda.

- Gracias a la implementación del protocolo Netflow se determinó que los dispositivos con las direcciones IP 172.20.89.86 y 172.20.211.254 generan un tráfico promedio por día de 846.6 KB que corresponde al 27.55% del tráfico total de la red.

- Netflow Traffic Analyzer resultó ser una herramienta muy útil para el usuario ya que proporciona información relevante como las pérdidas de paquetes, las latencias y el tráfico en tiempo real que pueden ocurrir dentro de una red LAN.

- A comparación del resultado obtenido por el Sr. Julio Molina en su tesis titulada: “Propuesta de segmentación con red virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la Empresa Editora El Comercio – Planta Norte”, se logró reducir el tiempo de respuesta en hora pico de 427.75ms a 4.63ms; logrando una reducción de un 97.78% de la latencia gracias a la implementación del protocolo Netflow, convirtiéndolo así en un protocolo demasiado útil junto a la calidad de servicio para mejorar el rendimiento de la red

RECOMENDACIONES

- Implementar el protocolo Netflow en todas las sedes de SUNARP, con el fin de que todos los administradores de red puedan diagnosticar las direcciones IP que están saturando la red.

- Priorizar el tráfico de voz por ser un tráfico sensible a los altos picos de latencia, debido a que se corre el riesgo de tener pérdidas de paquetes en momentos de congestión de la red.

- Realizar futuras investigaciones respecto al tráfico IP en las redes LAN, con el propósito de identificar comportamientos anómalos en el tráfico como la presencia de un malware, el cual provoque un riesgo de seguridad en la red.

- Realizar restricciones de acceso al equipo con la dirección IP 172.20.89.86 con el fin de tener más espacio para el consumo de ancho de banda y así evitar las altas latencias que puede llegar a presentar la red.

BIBLIOGRAFÍA

- Alegsa, Leandro (2018). *Definición de Rendimiento de Redes*. Obtenido de http://www.alegsa.com.ar/Dic/rendimiento_en_redes.php

- Echeverria Sierralta, Francisco (2008). *Implementación y Evaluación de Sistema de Monitoreo de Seguridad basado en flujos de paquetes IP*. Universidad de chile facultad de ciencias físicas y matemáticas departamento de ciencias de la computación.

- Estela, Maria (2018). *Red Lan*. Consultado el 22 de Octubre de 2019. Obtenido de https://concepto.de/red-lan/

- Juncosa, Martin (2018). *El modelo TCP/IP capa a capa*. Recuperado de https://aprendederedes.com/redes/introduccion/modelo-tcp-ip/

- Leopoldo (2009). *Activar Netflow en dispositivos Cisco para recolectar información de tráfico IP.* Recuperado de http://www.leopoldomaestro.com/activar-netflow-en-dispositivos-cisco-para-recolectar-informacion-de-trafico-ip/

- Mac, Josan (2018). *Configuración y optimización de un Router para gaming*. Obtenido de https://naseros.com/2018/03/24/cconfiguracion-y-optimizacion-de-un-router-para-gaming-1a-parte/

- Martinez, Juan (2017). *Calidad de servicio.* Recuperado de http://cic.puj.edu.co/wiki/lib/exe/fetch.php?media=materias:daysenr:daysenr_-_calidad_de_servicio_qos_.pdf

- Matango(2016). *Protocolo de reservación de recursos*. Obtenido de http://www.servervoip.com/blog/protocolo-de-reservacion-de-recursos-rsvp/

- Molina Ruiz, Julio (2012). *Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la Empresa Editora El Comercio – Planta Norte.* Universidad Católica Santo Toribio de Mogrovejo.

- Muuss, Michael John (2010). The Story of the PING Program. Consultado el 21 de marzo de 2012.Obtenido de https://www.webcitation.org/5saCKBpgH?url=http://ftp.arl.mil/~mike/ping.html

- Morales Muchagalo, Edgar (2013). *Análisis del protocolo Netflow y su aplicación en la determinación del nivel de uso de la red de datos de la Facultad de Mecánica*. Escuela Superior Politécnica de Chimborazo.

- PANDORA (2017). *Pérdida de paquetes.* Recuperado de https://www.sarenet.es/ayuda/glosario/perdida-paquetes.htmvillagl

- Perez y Merino (2015). *Definición de Router*. Recuperado de https://definicion.de/router/

- Piedras (2015). *Definición de Disponibilidad*. Obtenido de https://prezi.com/mnhhfkzvxioo/disponibilidad-de-redes/

- Quiñones, Francisco (2016). *Estudio de la red telefónica IP banda en Elastix instalada en la comunidad salesiana Maria Auxiliadora*. Pontificia Universidad Católica del Ecuador.

- Robedlano, Angel (2019). *Qué es TCP/IP*. Obtenido de https://openwebinars.net/blog/que-es-tcpip/

- Rodrigues, Rolando (2016). Netflow cisco ios - top-talkers. Recuperado de https://networkfaculty.com/es/video/detail/2533-netflow-cisco-ios---top-talkers

- Rodríguez, Jorge Humberto (2015). *Herramientas de análisis de tráfico*. Recuperado de https://docplayer.es/1444933-Netflow-herramientas-de-analisis-de-trafico.html

- Soto, Juan (2018). ¿Qué es la latencia y cómo se puede mejorar? Obtenido de https://www.inchosting.pe/blog/sitio-web/que-es-la-latencia-y-como-se-puede-mejorar

- Stopford, M. (2009). Maritime economy, tercera edición, Routledge.

- Torres (2015). *Para que sirve Packet Tracer*. Obtenido de https://prezi.com/pn_yxlnmcjot/para-que-sirve/

- Villadiego Angulo, Cristian (2003). *Técnicas de optimización del ancho de banda en las redes LAN-PARTE II.* Corporación Universitaria Tecnológica de Bolivar.

- Villagomez Carlos (2018). *El protocolo ICMP*. Obtenido de https://es.ccm.net/contents/265-el-protocolo-icmp

- Walton, Alex (2018). *Netflow Funcionamiento y configuración*. Recuperado de https://ccnadesdecero.es/netflow-funcionamiento-configuracion/

ANEXOS

Carta de solicitud

CARTA DE SOLICITUD PARA REALIZAR CONFIGURACIONES EN EL ROUTER "EL TAMBO "SUNARP

30 de Octubre del 2019

SOLICITO:

Permiso para realizar configuraciones en el router "EL TAMBO"

DIRIGIDO A:

INGENIERO RESIDENTE DE SUNARP

ING. JOSE PALACIOS TORRES

Estimado Sr. José Palacios Torres:

Me place extenderle un cordial saludo, mi nombre es Aldo Antonio Sotelo Palacios, bachiller de la carrera de Ingeniería Electrónica de la Universidad Nacional Tecnológica de Lima Sur. Ante Ud. Respetuosamente me presento y expongo:

Que pueda apoyarme en su función de Ing. Residente para poder tener el permiso de llevar a cabo una propuesta de configuración del protocolo Netflow y Calidad de servicio mediante la configuración de políticas, con el fin de mejorar el rendimiento de la red LAN de SUNARP-EL TAMBO (Junín).

Dado que actualmente la sede de Junín no cuenta estos protocolos para tener un mejor control del consumo de ancho de banda.

Por otro lado me comprometo como persona formada con valores éticos a manejar de manera correcta y con mucha confidencialidad la información obtenida.

Con saludos cordiales, agradeceré su atención a esta solicitud.

Agradezco de antemano su apoyo.

ING. JOSÉ PALACIOS TORRES

Carta de solicitud enviada

CARTA DE SOLICITUD PARA REALIZAR CONFIGURACIONES EN EL ROUTER "EL TAMBO "SUNARP

30 de Octubre del 2019

SOLICITO:

Permiso para realizar configuraciones en el router "EL TAMBO"

DIRIGIDO A:

INGENIERO RESIDENTE DE SUNARP

ING. JOSE PALACIOS TORRES

Estimado Sr. José Palacios Torres:

Me place extenderle un cordial saludo, mi nombre es Aldo Antonio Sotelo Palacios, bachiller de la carrera de Ingeniería Electrónica de la Universidad Nacional Tecnológica de Lima Sur. Ante Ud. Respetuosamente me presento y expongo:

Que pueda apoyarme en su función de Ing. Residente para poder tener el permiso de llevar a cabo una propuesta de configuración del protocolo Netflow y Calidad de servicio mediante la configuración de políticas, con el fin de mejorar el rendimiento de la red LAN de SUNARP-EL TAMBO (Junín).

Dado que actualmente la sede de Junín no cuenta estos protocolos para tener un mejor control del consumo de ancho de banda.

Por otro lado me comprometo como persona formada con valores éticos a manejar de manera correcta y con mucha confidencialidad la información obtenida.

Con saludos cordiales, agradeceré su atención a esta solicitud.

Agradezco de antemano su apoyo.

Aldo Antonio Sotelo Palacios

Acta de conformidad

	PROTOCOLO DE CONFORMIDAD		
	PRUEEBA DE FUNCIONAMIENTO		
	1. DATOS GENERALES		
NOMBRE	SOTELO PALACIOS ALDO ANTONIO		
TRABAJO	CONFIGURACIÓN DEL PROTOCOLO NETFLOW Y POLÍTICAS DE TRÁFICO		
CLIENTE	SUPERINTENDENCIA NACIONAL DE REGISTROS PÚBLICOS		
	2. DATOS DE PRUEBAS		
EQUIPO	ROUTER		
MARCA	CISCO		
MODELO	CISCO 1841		
SERIE	FTX1226W0A2		
UBICACIÓN	JR. AREQUIPA N° 240 - EL TAMBO		
3. FECHA DE INICIO:	**FECHA DE FINALIZACION:**		
	4.DESARROLLO DE PRUEBA		
N°	DESCRIPCION DE PRUEBA	CONFORME	
		SI	NO
1	Verificación del funcionamiento del equipo		
2	Verificacion de llegada a la direccion IP LAN		
3	Verificacion de llegada hacia el nodo PE		
4	Verificacion de la configuración del protocolo Netflow		
5	Verificación de la configuración de Politicas de Servicio		
6	Prueba de Conectividad		
7	Prueba de identificacion del dispositivo que consume un mayor ancho de banda		
8	Verificación del tráfico a traves de la herramienta Netflow Analyzer Traffic		
	OBSERVACIONES		
FIRMA			
NOMBRE	ING. JOSE PALACIOS TORRES		
CARGO	REDIDENTE DE LA SUPERINTENDENCIA NACIONAL DE REGISTROS PÚBLICOS		

Acta de conformidad completada

PROTOCOLO DE CONFORMIDAD			
PRUEEBA DE FUNCIONAMIENTO			
1. DATOS GENERALES			
NOMBRE	SOTELO PALACIOS ALDO ANTONIO		
TRABAJO	CONFIGURACIÓN DEL PROTOCOLO NETFLOW Y POLÍTICAS DE TRÁFICO		
CLIENTE	SUPERINTENDENCIA NACIONAL DE REGISTROS PÚBLICOS		
2. DATOS DE PRUEBAS			
EQUIPO	ROUTER		
MARCA	CISCO		
MODELO	CISCO 1841		
SERIE	FTX1226W0A2		
UBICACIÓN	JR. AREQUIPA N° 240 - EL TAMBO		
3. FECHA DE INICIO:	FECHA DE FINALIZACION:		
4.DESARROLLO DE PRUEBA			
N°	DESCRIPCION DE PRUEBA	CONFORME	
		SI	NO
1	Verificación del funcionamiento del equipo	X	
2	Verificacion de llegada a la direccion IP LAN	X	
3	Verificacion de llegada hacia el nodo PE	X	
4	Verificacion de la configuración del protocolo Netflow	X	
5	Verificación de la configuración de Politicas de Servicio	X	
6	Prueba de Conectividad	X	
7	Prueba de identificacion del dispositivo que consume un mayor ancho de banda	X	
8	Verificación del tráfico a traves de la herramienta Netflow Analyzer Traffic	X	
OBSERVACIONES			
Todo trabajo realizado bajo supervisión de mi persona.			
FIRMA	CIP 188112		
NOMBRE	ING. JOSE PALACIOS TORRES		
CARGO	REDIDENTE DE LA SUPERINTENDENCIA NACIONAL DE REGISTROS PÚBLICOS		