DISEÑO DE RED PARA LA MEJORA DE LA DISPONIBILIDAD Y CALIDAD DEL SERVICIO DE DATOS E INTERNET EN ENTIDAD DEL SECTOR SALUD

PRESENTADO POR:
MALDONADO JONATHAN
MELENDEZ MARGARITA
VICTORIA EFRAIN

ASESOR TÉCNICO DE PROYECTO:
Carlos René Suárez

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN DISEÑO DE REDES TELEMATICAS
BOGOTÁ, COLOMBIA
2019

DEDICATORIA

El presente proyecto de grado es el resultado del esfuerzo conjunto de los que formamos el grupo de trabajo.

Este proyecto lo dedicamos a nuestras familias por habernos brindado su apoyo incondicional a lo largo de nuestras vidas.

AGRADECIMIENTOS

Agradecemos a Dios por guiarnos en este camino y por permitirnos culminar con éxito el objetivo de obtener la especialización.

Agradecemos a nuestros docentes de la Universidad El Bosque, por haber compartido sus conocimientos a lo largo de la preparación de esta especialización.

RESUMEN

El presente caso de estudio tiene como finalidad validar el funcionamiento de la entidad del sector salud, que actualmente está experimentando inconvenientes de comunicaciones entre sus sedes Principal y Remotas, este proyecto estará enfocada en hallar las causas raíz de las anomalías presentadas en el servicio de comunicación.

Así mismo, se planteará desde el punto de vista consultivo, las mejores prácticas de comunicación de acuerdo con los estándares de industria que apliquen de acuerdo con las tecnologías en uso.

PALABRAS CLAVE

Redes, Servicio, Tecnologías, Comunicación, QoS, Optimización de redes

ABSTRACT

The purpose of this case study is to validate the functioning of the health sector entity, which is currently experiencing communication problems between its headquarters and remote, this project will be focused on finding the root causes of the anomalies presented in the communication service.

Likewise, the best communication practices in accordance with the industry standards that apply according to the technologies in use will be considered from the consultative point of view.

KEYWORDS

Networks, Service, Technologies, Communication, QoS, Network optimization.

Tabla de contenido

Índice de Figuras

1. Título

Diseño de red para la mejora de la disponibilidad y calidad del servicio de datos e internet de entidad del sector salud.

2. Introducción

Las empresas cada día requieren de actualizaciones tanto a nivel tecnológico como a nivel estructural para el correcto funcionamiento de sus diversas áreas, ya que estas utilizan las telecomunicaciones hoy en día para todo lo que concierne al funcionamiento de las organizaciones, en este caso a una organización prestadora de servicios de salud. Por esta razón la necesidad de tener tecnología crece juntamente con la habilidad para recolectar, procesar y distribuir información, en búsqueda de mejorar el desempeño de las áreas internas de la organización. De ahí la importancia de contar con las mejores herramientas de conectividad, lo cual implica que haya un acondicionamiento de dichas organizaciones desde sus redes eléctricas hasta sus redes de comunicaciones cumpliendo una serie de normas que garanticen el buen funcionamiento.

La propuesta del proyecto se fundamentará en el de diseño de la configuración e infraestructura de la red de una entidad del sector salud para la mejora de la disponibilidad y calidad de servicio con sus respectivas sucursales.

Este diseño permitirá a la entidad del sector salud operar según sus requerimientos, se requerirá tener una red de internet dedicado como actualmente se encuentra implementado y se necesitará poder prestar un servicio con una disponibilidad según requerimientos y funcionamiento de este dónde se deberá garantizar un óptimo funcionamiento de los servicios que allí se demanden.

3. Descripción general del proyecto

3.1. Definición del problema

Para la entidad de salud constituido por una sede principal ubicada en Sopo y tres sucursales ubicada, una en La Calera y dos en Tocancipá, en las cuales se prestan servicios de chequeos médicos, laboratorio clínico, etc.; donde los empleados requieren el uso de las plataformas para el agendamiento, consultas y facturación hacia los usuarios finales. En ocasiones los empleados reportan que se presenta lentitud y caídas en la red bloqueando las acciones anteriormente mencionadas en la plataforma al subir o consultar registros de pacientes, esto se genera por tráfico y tiempos altos entre las diferentes sedes, ya que todas las consultas y cargue de información llegan directamente al servidor quien almacena todo sobre su base de datos el cual está ubicado en su sede principal, un canal de Datos de 8Mbps; acá empieza a observarse uno de los problemas debido a que de sus tres sedes remotas, 2 son también de 8Mbps y que además de ir a la sede principal hacia el servidor, también se usan para la salida a internet generando un "cuello de botella"; los empleados también presentan inconformidad al momento de caída de su canal principal ya que toda la empresa queda incomunicada y por lo general tarda más de una hora en volver a la normalidad, esto se presenta cuando su canal principal presenta una falla de fibra, equipos físicos de última milla o cualquier anomalía que genere caída de su canal de Datos, todas sus sucursales se verán afectadas por el tiempo que tarde en volver a subir el servicio.

Las causas de estos inconvenientes son:

- Bajo ancho de banda en el canal de Datos principal.
- No hay control sobre el tráfico hacia la sede principal desde sus sedes remotas.
- No hay un canal de respaldo en la sede principal que tome su rol de maestro al momento de afectación del canal de datos principal.
- No hay prioridad al servidor ubicado en la sede principal.

Para demostrar los tres primeros puntos anteriormente mencionados se explicarán las figuras a continuación.

Como se observa en la figura 1, el canal de la sede principal presenta saturación sobre su servicio (8Mbps), ya que las demás sedes están realizando petición al servidor y hacia Internet.

```
HOSPITAL_SOPO_DX#   sh int sum
 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD       RXBS       RXPS       TXBS       TXPS       TRTL
------------------------------------------------------------------------------------------------------------------------
  Em0/0                         0         0         0         0          0          0          0          0          0
* GigabitEthernet0/0            0         0         0         8    7587000        988    8206000        931          0
* Gi0/0.1120                    -         -         -         -          -          -          -          -          -
* GigabitEthernet0/1            0         0         0         0     934000        271     313000        256          0
* Loopback500                   0         0         0         0          0          0          0          0          0
NOTE:No separate counters are maintained for subinterfaces

  Interface                   IHQ       IQD       OHQ       OQD       RXBS       RXPS       TXBS       TXPS       TRTL
------------------------------------------------------------------------------------------------------------------------
     Hence Details of subinterface are not shown
```

Figura 1. Trafico en sede Principal 8Mbps (saturado)

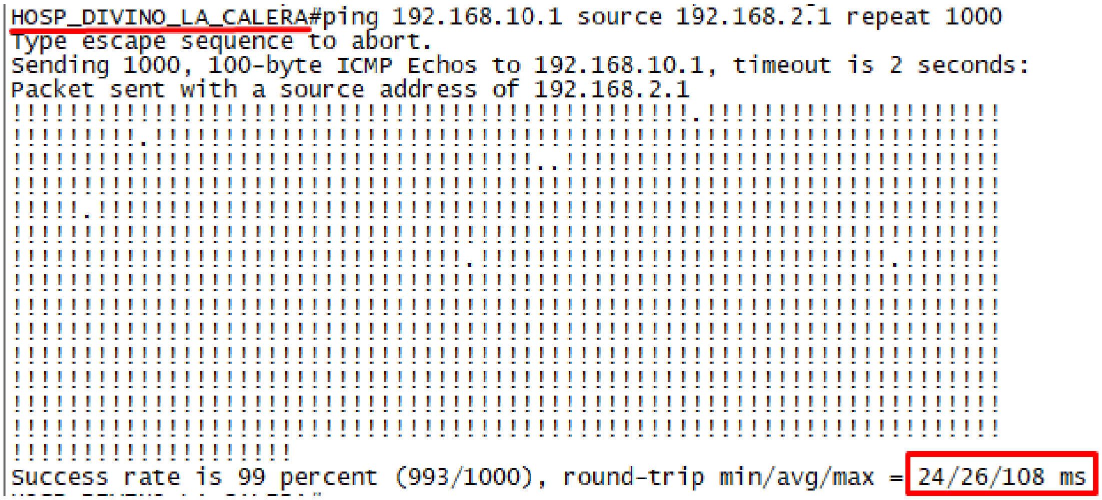
En las figuras 2, figura 4 y figura 6 se observa sobre cada canal de las sedes remotas el tráfico de cada una las cuales no llegan a su ancho de banda total, pero como el canal principal no tiene más capacidad para recibir todas las peticiones empieza a generar pérdidas hacia todas las sedes como se observa en los pings realizados desde cada Router al enlace principal sobre las figuras 3, figura 5 y figura 7.

El tráfico de la sede La Calera se encuentra a 3.5 Mbps, su capacidad total es de 8Mbps, pero no es aprovechada debido a la saturación del canal principal, el ping de la figura 3 demuestra la perdida de paquetes y tiempos de respuesta con la mitad de tráfico.

```
HOSP_DIVINO_LA_CALERA#sh int sum
 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD       RXBS       RXPS       TXBS       TXPS       TRTL
------------------------------------------------------------------------------------------------------------------------
  Em0/0                         0         0         0         0          0          0          0          0          0
* GigabitEthernet0/0            0         0         0       139    3566000        383    3582000        385          0
* Gi0/0.3510                    -         -         -         -          -          -          -          -          -
* GigabitEthernet0/1            0         0         0         0     234000         76     210000         71          0
* Loopback500                   0         0         0         0          0          0          0          0          0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
```

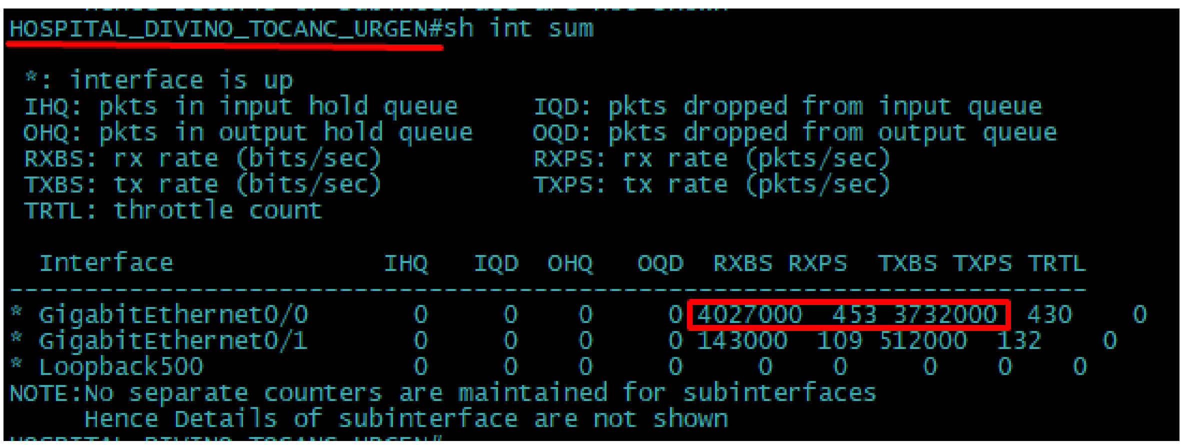
Figura 2. Trafico en sede Calera



```
HOSP_DIVINO_LA_CALERA#ping 192.168.10.1 source 192.168.2.1 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!..!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (993/1000), round-trip min/avg/max = 24/26/108 ms
```

Figura 3. Ping a sede Principal desde la Calera

El tráfico de la sede Tocancipá Urgencias se encuentra a 4 Mbps, su capacidad total es de 4Mbps, este canal si se encuentra saturado ocasionando perdida de paquetes y aumentando las peticiones al canal principal, el ping de la figura 5 demuestra la perdida de paquetes y tiempos de respuesta.



```
HOSPITAL_DIVINO_TOCANC_URGEN#sh int sum

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface              IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
-------------------------------------------------------------------------
* GigabitEthernet0/0       0     0    0     0 4027000  453 3732000  430    0
* GigabitEthernet0/1       0     0    0     0 143000  109 512000  132    0
* Loopback500              0     0    0     0      0     0      0    0    0
NOTE:No separate counters are maintained for subinterfaces
     Hence Details of subinterface are not shown
```

Figura 4. Trafico en sede Tocancipá Urgencias

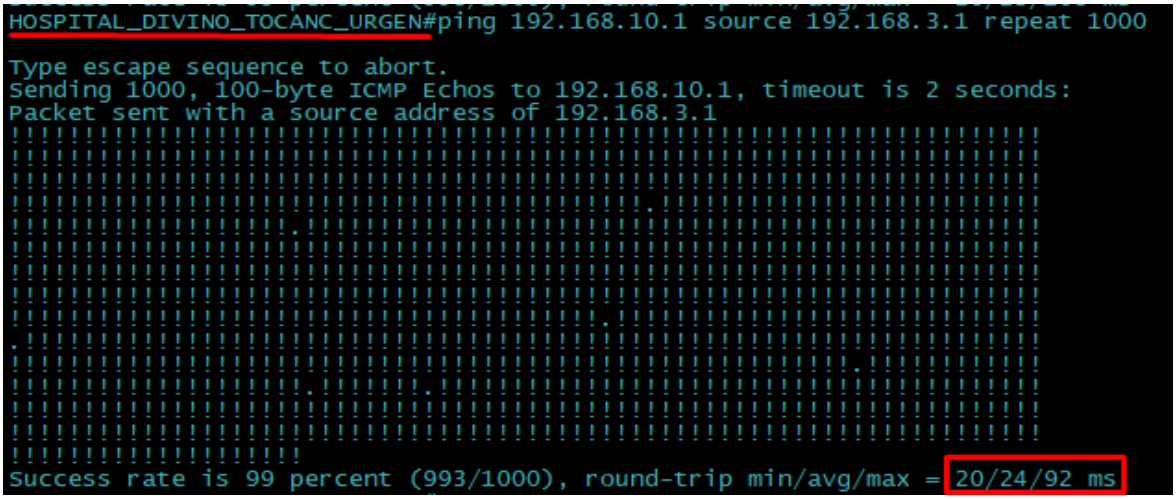


Figura 5. Ping a sede Principal desde Tocancipá Urgencias

El tráfico de la sede Tocancipá se encuentra a 4.1 Mbps, su capacidad total es de 8Mbps, pero no es aprovechada debido a la saturación del canal principal, el ping de la figura 7 demuestra la perdida de paquetes y tiempos de respuesta con la mitad de tráfico.

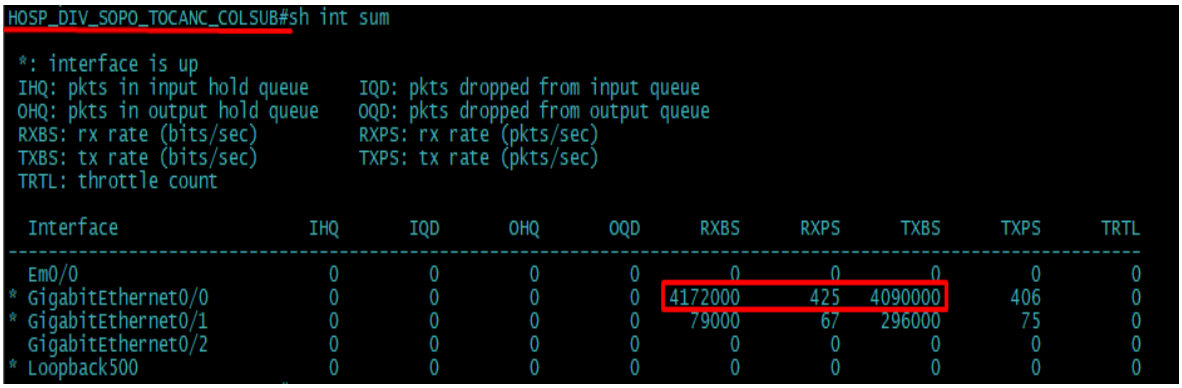


Figura 6. Trafico en sede Tocancipá

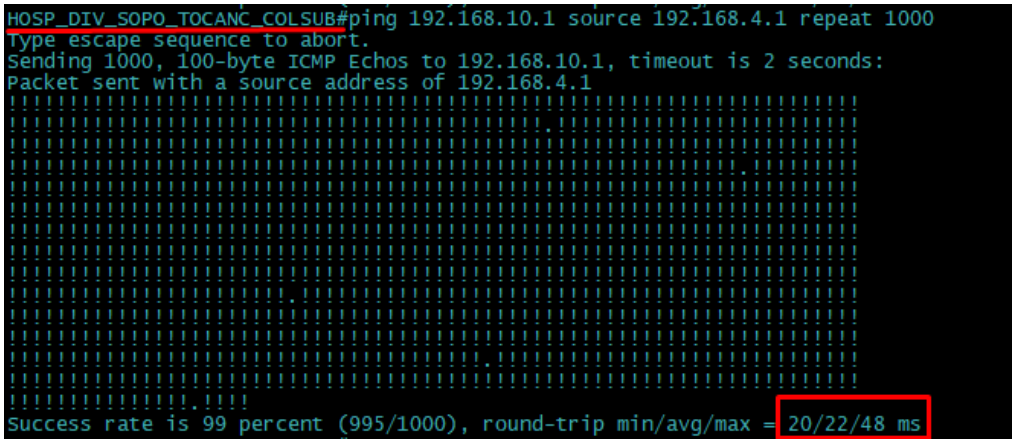


Figura 7. Ping a sede Principal desde Tocancipá

3.2. Aspectos a solucionar

Se presentan principalmente cuatro problemáticas sobre la red de la entidad de salud, las cuales son:

- Bajo ancho de banda en el canal de Datos principal.
- No hay control sobre el tráfico hacia la sede principal desde sus sedes remotas.
- No hay un canal de respaldo en la sede principal que tome su rol de maestro al momento de afectación del canal de datos principal.
- No hay prioridad al servidor ubicado en la sede principal.

3.3. Solución propuesta

- Se propone realizar la ampliación de ancho de banda de la sede principal para que pueda soportar el tráfico de entrada y salida de las sedes remotas, con el fin de evitar "cuellos de botella".
- Mejorar el servicio para cada sede configurando unas políticas de calidad (QoS) apuntando a la IP del servidor, con esto se da prioridad a los paquetes y la información que llega y sale de este.
- Realizar una configuración sobre el Router principal diferente a los QoS para restringir y permitir cierto ancho de banda sobre los canales de datos, en este caso permitiendo al servidor usar todo el ancho de banda y no al Internet, dando aún más prioridad al tráfico del servidor.[1]

[1] Ra-Ma, "Sistemas de Telecomunicaciones e informáticos: Redes telemáticas", Editorial Paraninfo, España, 2015.

- Se diseñará y simulará el funcionamiento de un canal de Backup en la sede principal con las mismas características de canal principal para asegurar servicio en caso de falla, este servicio Backup debe ir por otra ruta diferente a principal en MPLS o por otro proveedor.

4. Estado del arte

4.1. Marco de referencia Teórico

A continuación, se referenciará las tecnologías que serán aplicadas en este proyecto.

4.1.1 MPLS

Conmutación de etiquetas multiprotocolo o MPLS (Multiprotocol Label Switching), está definido para funcionar sobre múltiples protocolos unificando los niveles 2 (enlace de datos) y 3 (red) del modelo OSI, las principales motivaciones para su desarrollo son la ingeniería de tráfico, la diferenciación de clases de servicio, y las redes privadas virtuales (VPN). MPLS hace más viable la ingeniería de tráfico, permite que se pueda ejecutar enrutamiento rápido y también permite que los equipos de reenvío sean más baratos si sólo deben entender paquetes etiquetados, permite ofrecer QoS basándose en diferentes CoS (clases de servicio) y optimiza el establecimiento de túneles en las VPN.[2]

La estructura del encabezado MPLS es el siguiente:

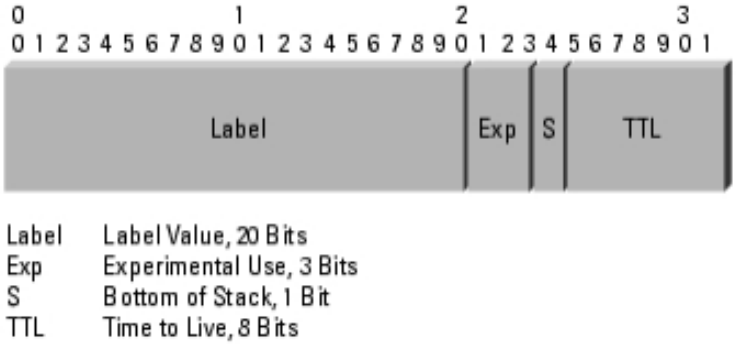


Figura 8. Estructura del encabezado MPLS

[2]https://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html

Los puntos de entrada en la red MPLS son llamados Enrutadores de borde de Etiqueta (LER), es decir enrutadores que son interfaces entre la red MPLS y otras redes. Los enrutadores que generan la conmutación basados únicamente en etiquetas se llaman Enrutadores Conmutadores de Etiqueta (LSR). Hay que aclarar que un LER es simplemente un LSR que cuenta con la habilidad de dirigir paquetes en redes externas a MPLS. Las etiquetas son distribuidas usando el Protocolo de Distribución de Etiquetas (LDP). Es precisamente mediante el protocolo LDP que los enrutadores de etiquetas intercambian información acerca de la posibilidad de alcanzar otros enrutadores, y las etiquetas que son necesarias para ello.

4.1.2 QoS

QoS refiere a la capacidad de una red de proporcionar un mejor estándar de prestación del servicio, el tráfico de la red seleccionada sobre las diversas tecnologías subyacentes incluyendo el Frame Relay, Asynchronous Transfer Mode (ATM), los Ethernetes y 802.1 redes, SONET, y las redes ruteadas por IP. Calidad de servicio (QoS) es un conjunto de tecnologías que permite que las aplicaciones soliciten y reciban niveles de servicio predecibles en términos de la capacidad de rendimiento de datos (ancho de banda), variaciones de latencia (fluctuación) y retraso. En particular, las funciones de QoS ofrecen lo mencionado en la parte superior de este texto, a través de los siguientes métodos:[3]

- Soportar el Ancho de banda dedicado.
- Mejora de las características de pérdida.
- Cómo evitar y administrar la congestión de la red.
- Formar el tráfico de la red.
- Configuración de prioridades de tráfico en la red

[3]https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/22833-qos-faq.html

En la siguiente figura se ve una pirámide con la prioridad para cada cola y la marcación que necesita cada una de ellas:

EN MPLS	EN EL ROUTER	TIPO DE TRAFICO
COLA 6	marcación ef	VOZ
COLA 5	marcación af41	VIDEO
COLA 4	marcación af31	PLATINO
COLA 3	marcación af 21	ORO
COLA 2	marcación af11	PLATA
COLA 1	marcación default	BRONCE O POR DEFECTO

Figura 9. Información de las políticas de calidad QoS.[4]

4.1.3 PROTOCOLO HSRP

Existe un protocolo capaz de lograr que el tiempo de actividad de la red esté cerca del 100% y es el HSRP propiedad de CISCO, este ofrece una redundancia asegurado que el tráfico de los usuarios se recupere casi de forma inmediata cuando se presenta una caída de su Router principal. Su funcionamiento se va dando una ilusión de un solo Router (virtual) al host de la red LAN, se genera un grupo entre los Router configurados y solo uno de ellos va a ser el activo, encargado del reenvío de los paquetes de los hosts hacia el Router virtual, mientras tanto hay otro dispositivo en forma de espera. En caso de que falle el Router activo, el Router inactivo asume las tareas de reenvío de paquetes de éste.[5]

[4] Ernesto Ariganello, "Redes Cisco CCNP Routing & Switching", Editorial Ra-Ma – Ediciones de la U, España, 2016.
[5]https://www.cisco.com/c/es_mx/support/docs/ip/hot-standby-router-protocol-hsrp/10583-62.html

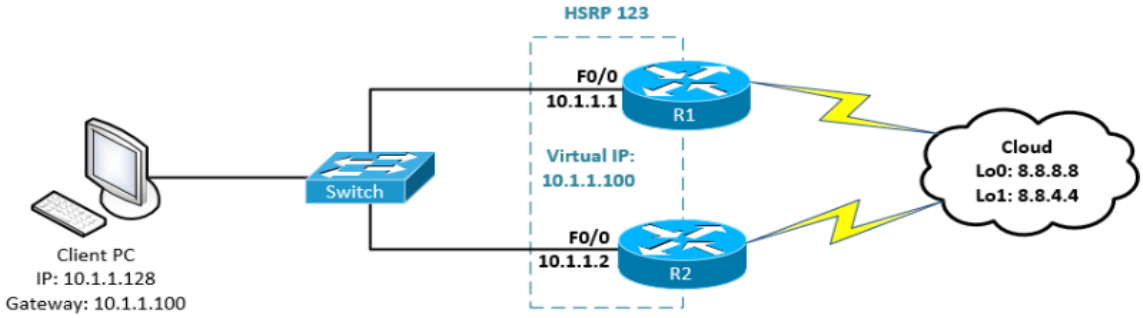


Figura 10. Topología configuración de HSRP

4.1.4 PRUEBAS RFC 2544

La recomendación RFC-2544[6] corresponde a un método de evaluación comparativa para elementos de interconexión de redes elaborado por la IETF. Está diseñada para probar enlaces de Ethernet. La RFC 2544 discute y define un número de pruebas que son utilizadas para describir y comparar las características de performance de dispositivos de interconexión de redes, tales como:

- Throughput
- Latencia
- Tasa de perdida de tramas

La manera ideal de implementar las pruebas es usar un equipo de prueba (tester) con puertos de transmisión y recepción, así el equipo de prueba puede determinar si todos los paquetes transmitidos fueron recibidos y verificar que los paquetes correctos sean recibidos.

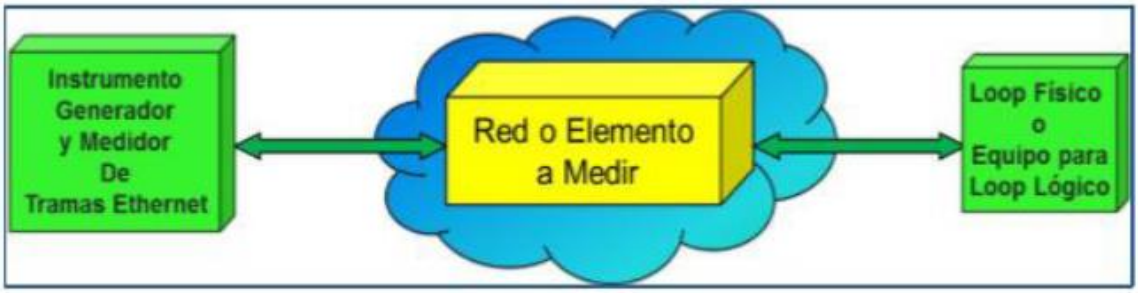


Figura 11. Topología RFC 2544

[6] Pablo Scaniello y Gonzalo Sosa, "Curso de Evaluación de performance de Redes", Uruguay

4.2. Marco de referencia Tecnológico

4.2.1 Equipo Cisco 1941

La serie 1900 de Cisco ofrece ahorros de costos totales de propiedad y agilidad en la red a través de la integración inteligente de seguridad líder en el mercado, comunicaciones unificadas y servicios de aplicaciones, soportando una capacidad de throughput de hasta 25 Mbps.

4.2.1 Equipo Cisco 2900

La serie 2900 de Cisco están diseñados para satisfacer las demandas de aplicaciones de las sucursales medianas de hoy y evolucionan a servicios basados en la nube. Ofrecen aplicaciones vitalizadas y una colaboración altamente segura a través de la gama más amplia de conectividad WAN con un alto rendimiento que ofrece servicios simultáneos de hasta 75 Mbps.[7]

4.2.2 Equipo Cisco 2800

La serie 2800 de Cisco, son equipos ideales para pequeñas y medianas empresas. Están diseñados para ofrecer servicios concurrentes de alta velocidad a través de una conexión por cable y pueden acomodar múltiples conexiones para servicios que incluyen, Datos, Vídeo, Seguridad, Inalámbrico y Voz.

4.2.3 Firewall Fortinet 60D

El FortiGate 60D ofrece una excelente solución de seguridad de red en una forma compacta de escritorio sin ventilador Factor para sucursales de empresas y medianas empresas. Protege contra las amenazas cibernéticas con SD-WAN segura líder en la industria en una solución simple, asequible y fácil de implementar.[8]

[7]Ernesto Ariganello, "Técnicas de configuración de Router Cisco", Alfaomega Grupo Editor, SA., México, Abril 2008.
[8]https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60D_Series.pdf

4.2.4 Servidor SO Windows server 2016

Windows Server 2016 Standard Edition. Soporta hasta 64 sockets y hasta 4 TB de RAM, incluyendo licencias para 2 máquinas virtuales.

Windows Server 2016 Datacenter Edition. Soporta hasta 64 sockets, 640 Cores y 4 TB de RAM, incluyendo licencias ilimitadas para máquinas virtuales.

Windows Server 2016 Foundation Edition. Para pequeñas empresas, tiene un límite de hasta 15 usuarios. Soporta un número limitado de roles, un Core y hasta 32 GB de RAM.[9]

5. Glosario de términos

C

Conmutada: La Conmutación se considera como la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión.[10]

Cuello de Botella: Este término hace referencia al cuello de una botella, donde la velocidad del flujo de un líquido es limitado por este cuello angosto. Este punto es donde el rendimiento o capacidad de un sistema completo es severamente limitado.

L

LAN:(Red de área Local). Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña. Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográfica limitada.

M

MPLS: (Switching de etiquetas multiprotocolo). Es un estándar de la industria sobre el cual se basa la conmutación (Switching) de etiquetas, las cuales identifican los diferentes tipos de información sobre la red. La tecnología MPLS le permite a un proveedor de servicios montar sobre su red Red servicios diferenciados a los cuales se tiene acceso a través del protocolo IP.[11]

[9] https://www.internetya.co/servidores-windows-server-2016-caracteristicas-y-versiones/

[10] Ernesto Ariganello, "Redes Cisco CCNP Routing & Switching", Editorial Ra-Ma – Ediciones de la U, España, 2016.

[11] https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/22833-qos-faq.html

Q

QoS: Calidad de servicio es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red.[12]

W

WAN: (Red de Área Amplia). Red de conmutación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrado por carriers comunes.[13]

6. Justificación

El presente proyecto se enfocará el diseño de una red para un Hospital, mejorando así el rendimiento del grupo médico y la eficiencia para atender a los pacientes; ya que en la actualidad la red está presentado continuas intermitencias y caídas del sistema, ocasionando así lentitud en la atención, malestar en los usuarios finales y grandes pérdidas económicas por el retiro de los usuarios que prefieren ser atendidos en otro lugar.

Actualmente el Hospital cuenta con 3 sucursales (1 Calera y 2 Tocancipá) y su sede central en Sopo, las 4 sedes están presentado los mismos problemas mencionados anteriormente. De acuerdo con las necesidades expuestas por el Hospital se sugerirá una solución a estos inconvenientes ofreciendo así una disponibilidad para toda la red de 99,9%. La infraestructura actual de la red para el hospital está conmutada desde la sede principal (Sopo) hacia las tres sucursales (1 Calera y 2 Tocancipá), enlazados por medio de la conmutación de etiquetas multiprotocolo (MPLS) y con última milla en fibra óptica, donde cada sede cuenta con un Router y su respectivo Switch para suministrar red. La sede principal (Sopo) es la encargada de suministrar el tráfico de internet hacia las demás sedes y donde está ubicado el servidor, este tiene la función de guardar toda la información suministrada por los pacientes y consultar en el momento que sea necesario, allí se ubica o se crea el historial de cada uno, este tráfico no maneja Internet, pero si pasa por los canales de datos los cuales deben dar una alta disponibilidad a la información. Al presentar lentitud se tarda la consulta por paciente generando encolamiento de usuarios, pérdida de información vital y un decremento económico debido al retiro de los pacientes por demoras en la atención.

[12] Ernesto Ariganello, "Redes Cisco CCNP Routing & Switching", Editorial Ra-Ma – Ediciones de la U, España, 2016.
[13]Ernesto Ariganello, "Redes Cisco: Guía de estudio para la certificación CCNA 640-802", Alfaomega Grupo Editor, SA., México, Enero 2009.

A continuación, la infraestructura representada en la figura 12:

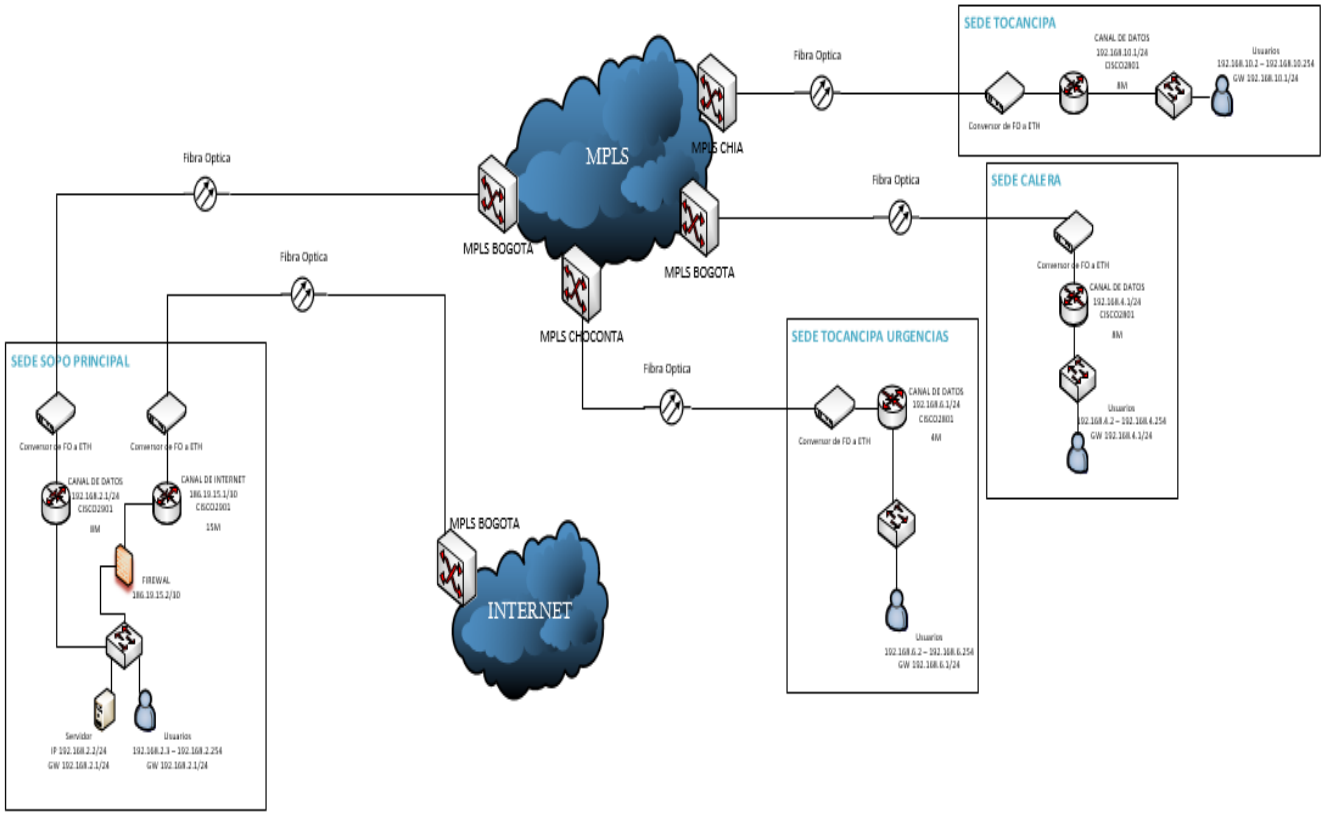


Figura 12. Topología Red Actual

Partiendo de ese criterio al momento de diseñar una red, donde su principal objetivo es evitar la pérdida de paquetes producto de una lentitud, y para ello se deberá tener en cuenta que esta debe ser sencilla, confiable, funcional, integra y segura, se deberá tener siempre un punto de transición y dicho diseño debe evolucionar dependiendo la demanda presentada para la organización donde esta fue implementada. Es por esta razón que el caso de esta entidad del sector salud llego al borde de la capacidad por la demanda y crecimiento del negocio para sus sedes, donde sus transacciones han aumentado por el uso del personal médico en las plataformas sobre la red, realizando las mismas acciones en paralelo para todas sus sedes.[14]

El Objetivo de este diseño es proponer una solución a cada una de las problemáticas generadas dentro de la entidad, las cuales mejorarán el servicio si se implementa y se toma en cuenta cada una de ellas por el cliente, ya que algunas generaran un costo extra como el canal

[14] Ricardo Jorge Rodríguez, "Desarrollo del proyecto de la red telemática", IC Editorial, Antequera Málaga, 2014.

de respaldo, pero esto repercutirá en la facilidad del trabajo del personal médico y administrativo dentro de la organización, permitiendo realizar sus labores sin pensar ni interrumpir sus actividades con la lentitud del sistema, además y más importante en la satisfacción al cliente quien será bien atendido, en la hora programada de su cita; incrementando el ingreso de pacientes diario a la entidad del sector salud y paralelamente sus ingresos.

7. Objetivos

7.1. General.

Proponer un diseño de red que mejore la disponibilidad y calidad del servicio de datos e internet en una entidad del sector salud.

7.2. Específicos

- Diseñar una red que mejora la disponibilidad y calidad del servicio de datos e internet en entidad del sector salud.
- Simular una red que mejora la disponibilidad y calidad del servicio de datos e internet en entidad del sector salud.
- Analizar los resultados obtenidos para demostrar que los cambios realizados mejoran la eficiencia de la red.

8. Requerimientos

El diseño de la red que mejora la disponibilidad y calidad del servicio de datos e internet en entidad del sector salud deberá:

- Funcionar con un Ancho de Banda de 20Mbps para el canal principal sede Sopo.
- Disminuir los tiempos de respuesta hacia el servidor de la sede principal desde sus sedes remotas.
- Disminuir las pérdidas de paquetes hacia el servidor de la sede principal desde sus sedes remotas.
- Tener un enlace Backup con las mismas características de físicas y recursos de red del enlace principal.
- Aumentar la disponibilidad del servicio con el enlace Backup.
- Priorizar el tráfico desde y hacia el servidor ubicado en la sede principal.

9. Metodología

Con los datos obtenidos sobre el tráfico del cliente en sus diferentes sucursales, se realizará un diseño de la red para evitar encolamiento de tráfico, saturaciones y caídas que indispongan la funcionalidad de toda la red.

- Se realizará una emulación de toda la red sobre GNS3 aprovechando que este emulador maneja imágenes (IOS) iguales a los que usan los Router Cisco reales.
- Con las pruebas tomadas en la red real y la emulación, se determina que tráfico sería el óptimo para evitar el cuello de botella sobre la red.
- Con la topología realizada sobre el emulador se va a realizar las diferentes configuraciones que permitan optimizar la red, se analizaran los resultados de cada una de ellas para comprobar su funcionamiento.
- Cuando se comprueba funcionamiento del rate-limit, configuración de QoS y se ha establecido un ancho de banda para controlar el tráfico de la red, se emulará el funcionamiento de un router backup en la sede principal para mejorar la disponibilidad.
- Si se comprueba funcionamiento de todo lo anterior se harán pruebas sobre la red real, observando el comportamiento de tráfico, que tantos paquetes son rechazados en el rate-limit, cuantos paquetes son marcados en los QoS y que tráfico promedio se manejaría sobre la red.

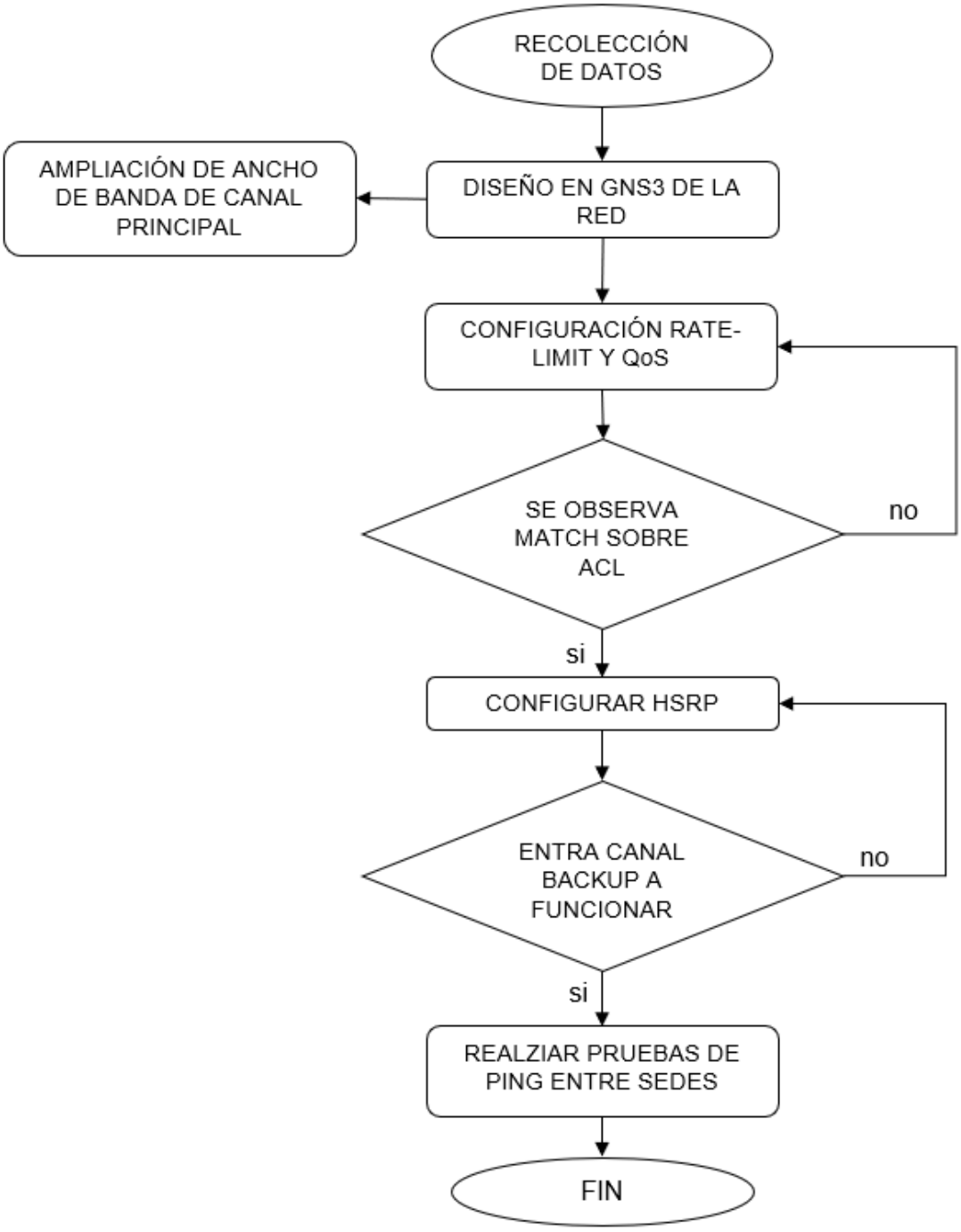


Figura 13. Diagrama de Flujo del Proceso

10. Pruebas de desarrollo de proyecto

10.1. Análisis de la ampliación del Ancho de Banda del enlace Principal Sopo

Para establecer el incremento que se debe realizar en el enlace principal Sopo se debe tener en cuenta que este enlace debe soportar las peticiones realizadas por las otras tres sedes (Tocancipá, Tocancipá Urgencias y Calera) hacia el Servidor alojado en la sede Principal.

Actualmente los Anchos de Banda de los enlaces están distribuidos de la siguiente manera:

- SOPO: 8Mbps
- TOCANCIPA: 8Mbps
- TOCANCIPA URGENCIAS: 4Mbps
- LA CALERA: 8Mbps

Esta distribución de BW no es la apropiada ya que todas las sedes realizan peticiones a la sede SOPO la cual solo cuenta con 8Mbps al igual que las otras sedes lo que está ocasionando un "cuello de botella", generando así lentitud en las aplicaciones utilizadas en el Centro médico.

La ampliación que se debe realizar en la sede Principal SOPO debe poder soportar a las otras sedes por lo tanto la ampliación del enlace debe ser mínimo de 20Mbps, que es la sumatoria de los BW de los enlaces Tocancipá, Tocancipá Urgencias y La Calera.

Además, para realizar la ampliación requerida se requiere realizar una actualización tecnológica en el Router instalado en la sede SOPO; actualmente se encuentra instalado un Router Cisco 1921, este equipo solo soporta un ancho de Banda de 15Mbps. Para poder llevar a cabo la ampliación a 20Mbps se debe realizar cambio de Router como mínimo a un Cisco 1941 el cual soporta 25Mbps (Figura 14).

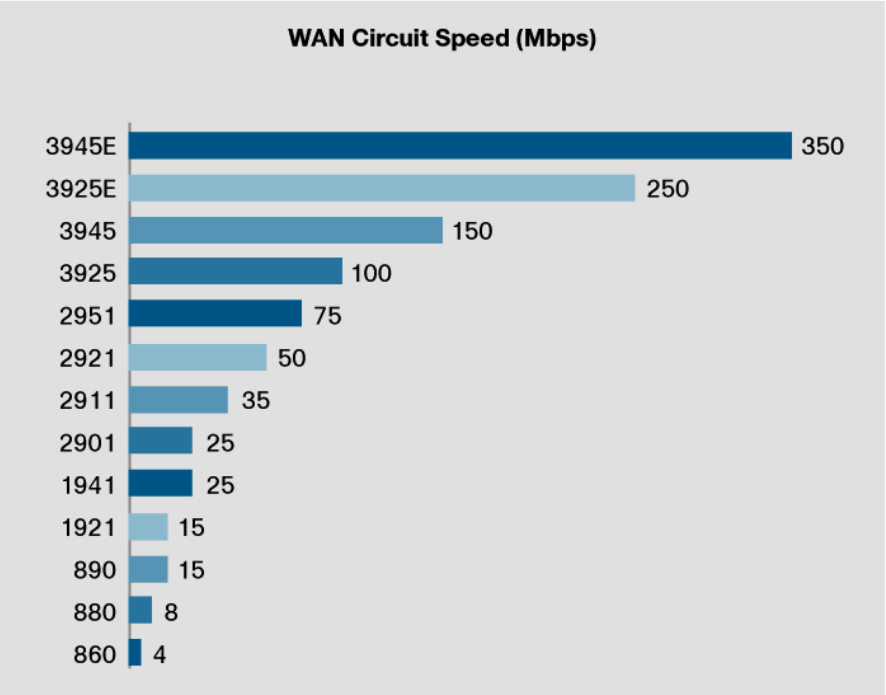


Figura 14. Posicionamiento del rendimiento por plataforma con servicios (Cisco)[15]

10.2. Prueba de conmutación protocolo HSRP

Para esta prueba se requiere tener otro servicio de Datos, preferiblemente con la misma capacidad del principal para que la afectación al subir sea mínima y no genere intermitencias o lentitud si es de menor ancho de banda; luego de tener el otro servicio no importa el proveedor se realiza la configuración en ambos equipos, para la prueba se realizó una simulación en el software GNS3 el cual usa imágenes sobre las que se mueven los Router en físico.[16]

[15] https://community.cisco.com/legacyfs/online/legacy/7/1/5/15373517-white_paper_c11_595485.pdf
[16] https://www.gns3.com/

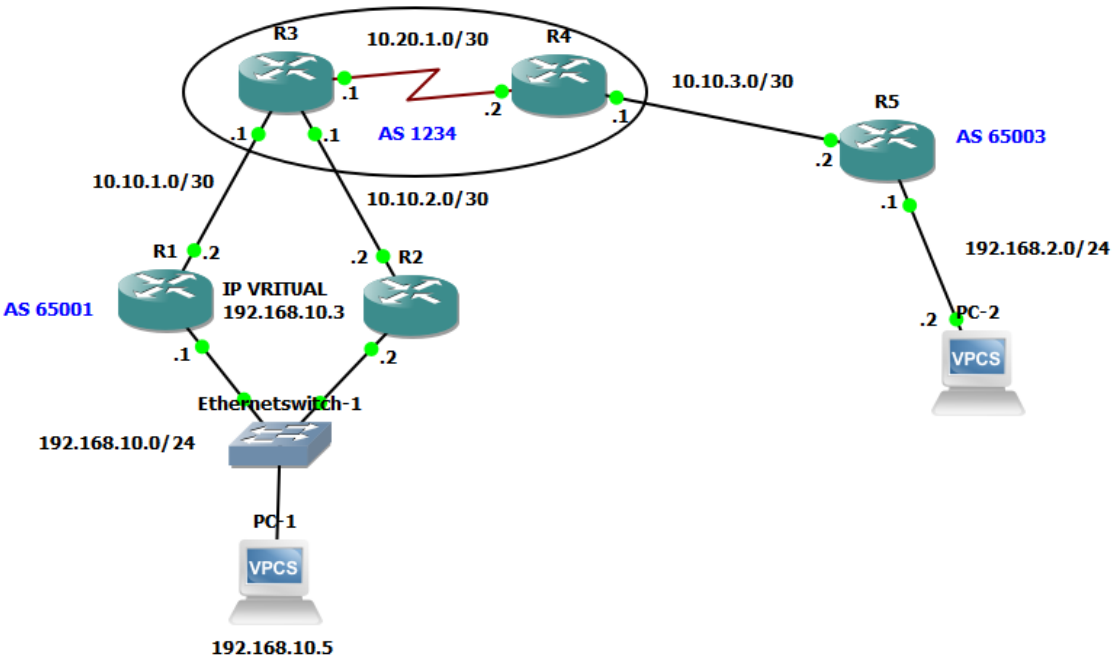


Figura 15. Topología de simulación protocolo HSRP

R1 Y R2 emulan los dos Router de la sede principal los cuales van a conmutar, la IP virtual será 192.168.10.3 la cual debe ser común en ambos equipos y será el Gateway de toda la LAN de esta sede. R3 y R4 será la MPLS por donde pasan los paquetes hacia las demás sedes y finalmente R5 será una sede remota la cual deberá llegar a la LAN de la sede principal donde se encuentra el servidor.

La configuración empezará en R1 donde se creará un IP SLA que será el encargado de testear la conectividad entre la interfaz WAN del Router y el PE, es decir las IP 10.10.1.0/30, con una frecuencia de 10 segundos, figura 16.

```
!
ip sla monitor 10
 type echo protocol ipIcmpEcho 10.10.1.1 source-ipaddr 10.10.1.2
 frequency 10
ip sla monitor schedule 10 life forever start-time now
!
```

Figura 16. Configuración IP SLA

Luego de tener esto se crea el TRACK, el cual es el que contiene toda la información del IP SLA y es quien será llamado en la interfaz del Router, en este caso por ser una versión 12.4 de la

imagen se usa el RTR en vez del IP SLA, pero la configuración es la misma que la versión 15.2.

Figura 17. Configuración Track

En la interfaz LAN del Router se aplicará el TRACK con un decremento a la prioridad cuando el IP SLA detecte que la conectividad cayo, esto se hace inicialmente creando un grupo HSRP y sobre este se asigna prioridad, se configura IP virtual y preempt, figura 18.

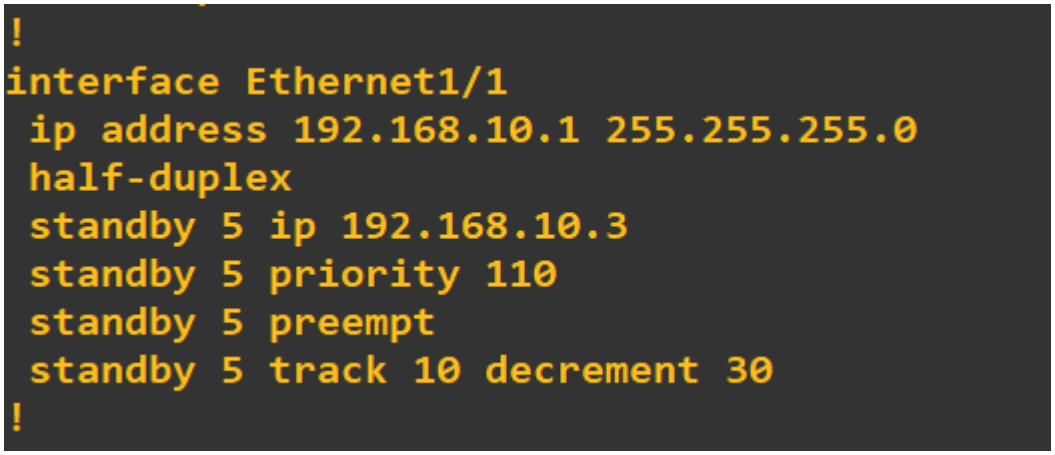


Figura 18. Configuración HSRP en interfaz del Router

Hasta aquí se finaliza la configuración en el canal principal o el que queramos como principal por capacidad de procesamiento, ancho de banda, esto ya se determina según lo queramos.

Finalmente, sobre Router backup se deberá crear en la interfaz LAN el mismo grupo HSRP y sobre este el preempt y la IP virtual que debe ser la misma, no se configura prioridad ya que por defecto en 100, figura 19.

```
!
interface Ethernet1/1
 ip address 192.168.10.2 255.255.255.0
 half-duplex
 standby 5 ip 192.168.10.3
 standby 5 preempt
!
```

Figura 19. Configuración HSRP en Router backup

La conmutación estaría funcionando, pero los paquetes provenientes de R5 deben saber una ruta la cual sea más rápida que la otra para que así no se generen loops, por lo que se crea un router-map para aumentar la cantidad de saltos del AS que tiene en común el Router principal y el Router backup y se aplica sobre el BGP, figura 20.

```
!
router bgp 65001
 no synchronization
 bgp log-neighbor-changes
 network 192.168.10.0
 neighbor 10.10.2.1 remote-as 1234
 neighbor 10.10.2.1 version 4
 neighbor 10.10.2.1 route-map BK out
 no auto-summary
!
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
route-map BK permit 10
 set as-path prepend 65001 65001 65001
```

Figura 20. Configuración Route-map aplicado a BGP canal backup

Para comprobarlo revisamos sobre el Router R3 quien sería la MPLS, vemos que la 10.10.2.2 tiene 4 saltos del AS 65001 por lo que sería ruta secundaria como lo identifica el símbolo **>** que indica mejor ruta y esta no la tiene, pero si la 10.10.1.2, figura 21.

```
R3#sh ip bgp
BGP table version is 17, local router ID is 10.20.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.1.0/30     0.0.0.0                  0         32768 i
*> 10.10.2.0/30     0.0.0.0                  0         32768 i
*>i10.10.3.0/30     10.20.1.2                0    100      0 i
r>i10.20.1.0/30     10.20.1.2                0    100      0 i
*>i192.168.2.0      10.10.3.2                0    100      0 65003 i
*> 192.168.10.0     10.10.1.2                0             0 65001 i
*                   10.10.2.2                0             0 65001 65001 65001 65001 i
R3#
```

Figura 21. Verificación de rutas.

Funcionamiento:

Vemos en figura 24 que la traza desde R5 va a la sede principal por el canal con mejor ruta 10.10.1.2, en las figuras 22 y 23 se observa que router es Master y cual Standby (backup).

```
R1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Et1/1       5   110  P Active   local           192.168.10.2    192.168.10.3
```

Figura 22. Show de HSRP en Router principal

```
R2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Et1/1       5   100  P Standby  192.168.10.1    local           192.168.10.3
```

Figura 23. Show de HSRP en Router backup

```
R5#ping  192.168.10.5 source 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.5, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/62/108 ms
R5#traceroute 192.168.10.5 source 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.10.5

  1 10.10.3.1 8 msec 24 msec 36 msec
  2 10.20.1.1 [AS 1234] 64 msec 64 msec 20 msec
  3 10.10.1.2 [AS 1234] 68 msec 40 msec 40 msec
  4 192.168.10.5 [AS 65001] 80 msec 56 msec 80 msec
```

Figura 24. Ping y traza desde Router remoto a principal

Para la prueba se puso shutdown la interfaz WAN y se ve la conmutación en la figura 25, donde R1 ahora queda standby y backup R2 como master, figura 26.

```
R1(config)#interface e1/0
R1(config-if)#sh
R1(config-if)#shutdown
R1(config-if)#
R1(config-if)#
*Mar  1 01:09:38.043: %BGP-5-ADJCHANGE: neighbor 10.10.1.1 Down Interface flap
R1(config-if)#
*Mar  1 01:09:40.027: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
*Mar  1 01:09:41.027: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
R1(config-if)#
*Mar  1 01:09:46.551: %HSRP-5-STATECHANGE: Ethernet1/1 Grp 5 state Active -> Speak
R1(config-if)#
R1(config-if)#
R1(config-if)#
R1(config-if)#
*Mar  1 01:09:56.551: %HSRP-5-STATECHANGE: Ethernet1/1 Grp 5 state Speak -> Standby
R1(config-if)#^Z
R1#sh
*Mar  1 01:10:15.519: %SYS-5-CONFIG_I: Configured from console by console
R1#sh stan
R1#sh standby bri
R1#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Et1/1       5   80   P Standby  192.168.10.2    local           192.168.10.3
```

Figura 25. Shutdown interfaz WAN de Router principal

```
R2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Et1/1       5   100  P Active   local           192.168.10.1    192.168.10.3
```

Figura 26. Verificación HSRP después de conmutar en Router backup

En R3 se ve que desaparece la ruta 10.10.1.2 y queda la 10.10.2.2 como principal indicada por **>**, en la traza de R5 se ve que llega por el canal backup, figura 27.

```
R3#sh ip bgp
BGP table version is 18, local router ID is 10.20.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.1.0/30     0.0.0.0                  0         32768 i
*> 10.10.2.0/30     0.0.0.0                  0         32768 i
*>i10.10.3.0/30     10.20.1.2                0    100      0 i
r>i10.20.1.0/30     10.20.1.2                0    100      0 i
*>i192.168.2.0      10.10.3.2                0    100      0 65003 i
*> 192.168.10.0     10.10.2.2                0             0 65001 65001 65001 65001 i
```

Figura 27. Verificación de rutas.

```
R5#ping  192.168.10.5 source 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.5, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/56/76 ms
R5#traceroute 192.168.10.5 source 192.168.2.1

Type escape sequence to abort.
Tracing the route to 192.168.10.5

  1 10.10.3.1 16 msec 20 msec 12 msec
  2 10.20.1.1 [AS 1234] 44 msec 20 msec 68 msec
  3 10.10.2.2 [AS 1234] 68 msec 20 msec 64 msec
  4 192.168.10.5 [AS 65001] 88 msec 40 msec 112 msec
```

Figura 28. Ping y traza desde Router remoto a principal

10.3. Prueba de rate-limit

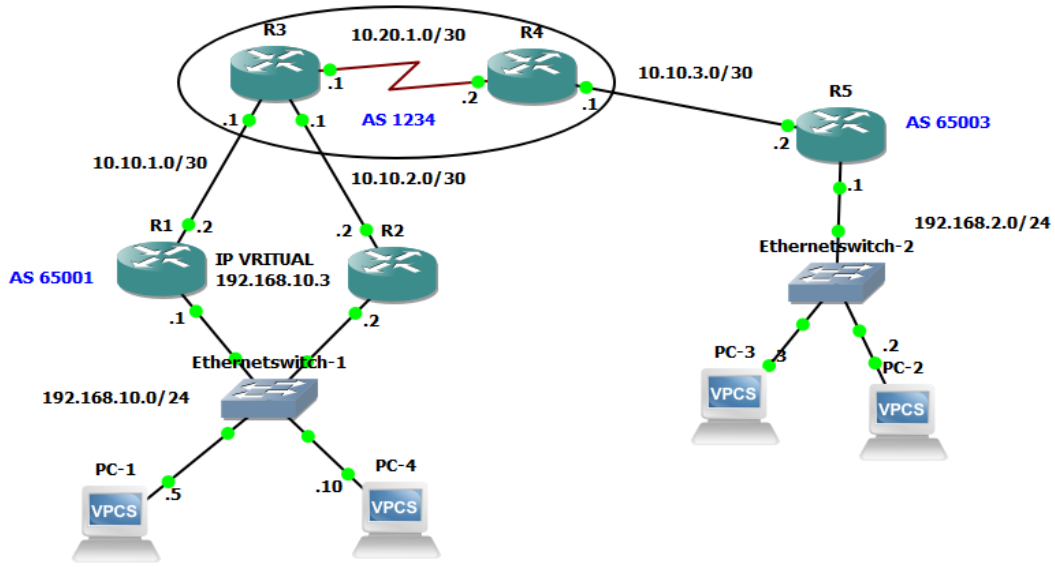


Figura 29. Topología para simulación de rate-limit

Para asegurar una mejor disponibilidad al servicio del servidor, se configura un rate-limit el cual será el encargado de asegurar que el servidor tenga todo el ancho de banda del servicio para su uso y no se vea afectado por posibles saturaciones del enlace, en caso de que el canal se sature todos los demás servicios llegaran hasta cierto porcentaje del ancho de banda y no ocupara todo el canal, esta es la funcionalidad del rate-limit en esta configuración.

Para su funcionamiento se deberá configurar en el Router principal y backup; inicialmente se configura una lista de acceso con la IP del servidor, figura 30.

```
!
access-list 100 permit ip host 192.168.10.5 any
```

Figura 30. Lista de acceso con IP de servidor

Luego se configura sobre la interfaz WAN el rate-limit indicando cuanto ancho de banda pueden usar todos los demás servicios.

En esta primera línea indica que la IP de la lista de acceso 100 puede usar más de 4 Mbps, figura 31.

```
rate-limit output access-group 100 4096000 768000 1536000 conform-action transmit exceed-action continue
```

Figura 31. Configuración rate-limit continue

En esta línea indica que cualquier otro servicio que use más de 4 Mbps sea rechazado, limitando así el tráfico de todos los servicios hasta 4 Mbps y en caso de que el canal sea de 8Mbps, el servidor tendrá 4 Mbps extra a todos los demás servicios, figura 32.

```
rate-limit output 4096000 768000 1536000 conform-action transmit exceed-action drop
```

Figura 32. Configuración rate-limit drop

Para comprobarlos se verifica el match en la lista de acceso con el comando "show access-lists *numero access-list*" como se ve en la figura 33, se puede ver cuando se realiza ping desde la sede remota a la Ip que está dentro de la lista de acceso, el match aumenta.

```
PC-3> ping 192.168.10.5
84 bytes from 192.168.10.5 icmp_seq=1 ttl=60 time=101.722 ms
84 bytes from 192.168.10.5 icmp_seq=2 ttl=60 time=51.863 ms
84 bytes from 192.168.10.5 icmp_seq=3 ttl=60 time=97.761 ms
84 bytes from 192.168.10.5 icmp_seq=4 ttl=60 time=89.761 ms
84 bytes from 192.168.10.5 icmp_seq=5 ttl=60 time=88.772 ms
```

Figura 33. Ping de sede remota a servidor

```
R1#sh access-lists 100
Extended IP access list 100
    10 permit ip host 192.168.10.5 any (156 matches)
```

Figura 34. Verificación de lista de acceso, match.

Para ver la funcionalidad del rate-imit se aplica el siguiente comando "show interface *interfaz donde se configuro rate-limit* rate-limit" como se ve en la figura 36, allí está el match para la lista de acceso y el match para todo el resto de tráfico, en el de la lista de acceso el tráfico es permitido (action: transmit y action: continue) y en el de todo el tráfico los paquetes que pasaron las 4Mbps son rechazados (action: drop), igualmente se ve tiempo entre paquetes y el tiempo que está establecido el rate-limit.

Para aumentar los paquetes del match de todo el tráfico se realiza un ping a una IP de la red LAN que no sea la que está en la lista de acceso, si aumentan los paquetes se comprueba su funcionamiento.

```
PC-2> ping 192.168.10.10
84 bytes from 192.168.10.10 icmp_seq=1 ttl=60 time=131.644 ms
84 bytes from 192.168.10.10 icmp_seq=2 ttl=60 time=65.823 ms
84 bytes from 192.168.10.10 icmp_seq=3 ttl=60 time=116.688 ms
84 bytes from 192.168.10.10 icmp_seq=4 ttl=60 time=99.720 ms
84 bytes from 192.168.10.10 icmp_seq=5 ttl=60 time=93.774 ms
```

Figura 35. Ping de sede remota a PC en principal

```
R1#sh int e1/0 rate-limit
Ethernet1/0
  Output
    matches: access-group 100
      params:  4096000 bps, 768000 limit, 1536000 extended limit
      conformed 194 packets, 51404 bytes; action: transmit
      exceeded 0 packets, 0 bytes; action: continue
      last packet: 784252ms ago, current burst: 0 bytes
      last cleared 00:39:48 ago, conformed 0 bps, exceeded 0 bps
    matches: all traffic
      params:  4096000 bps, 768000 limit, 1536000 extended limit
      conformed 1967 packets, 746075 bytes; action: transmit
      exceeded 0 packets, 0 bytes; action: drop
      last packet: 20ms ago, current burst: 0 bytes
      last cleared 00:39:46 ago, conformed 2000 bps, exceeded 0 bps
```

Figura 36. Verificación de rate-limit en canal principal

En la siguiente figura 37 se puede ver un caso práctico donde se ven paquetes rechazados (action: drop) por superar los 4 Mbps.

```
HOSPITAL_SOPO_DX#sh interfaces gigabitEthernet 0/0.3523 rate-limit
GigabitEthernet0/0.3523 WAN
  Output
    matches: access-group 100
       params:  4096000 bps, 768000 limit, 1536000 extended limit
       conformed 11678 packets, 4689911 bytes; action: transmit
       exceeded 0 packets, 0 bytes; action: continue
       last packet: 344ms ago, current burst: 0 bytes
       last cleared 00:02:23 ago, conformed 261662 bps, exceeded 0 bps
    matches: all traffic
       params:  4096000 bps, 768000 limit, 1536000 extended limit
       conformed 41704 packets, 27953281 bytes; action: transmit
       exceeded 2035 packets, 2476295 bytes; action: drop
       last packet: 344ms ago, current burst: 289466 bytes
       last cleared 00:02:21 ago, conformed 1575542 bps, exceeded 139572 bps
```

Figura 37. Verificación de rate-limit en caso real.

10.4. Prueba de QoS

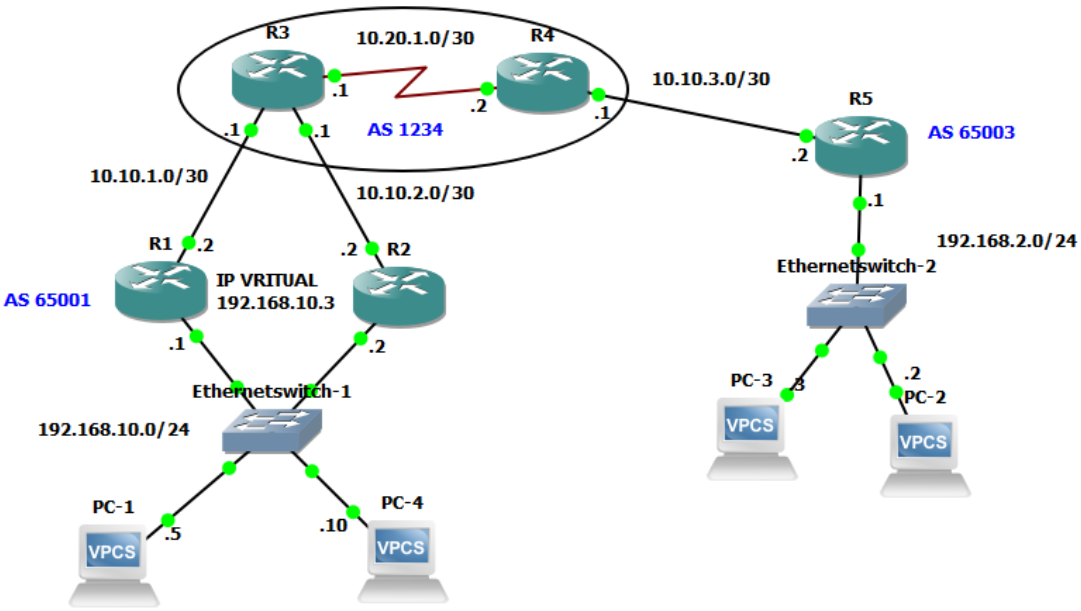


Figura 38. Topología para simulación QoS.

Para dar prioridad a los paquetes que salen y van hacia del servidor existen los QoS, por lo cual sobre el caudal Platino que después de Voz y Video es el de mayor rango, se asigna una lista de acceso la cual permite el tráfico hacia y desde el Router principal, en las siguientes figuras se observa el funcionamiento donde se realiza un ping al servidor desde una sede remota y tanto

la lista de acceso como los QoS configurados, tienen match que confirman la transmisión de paquetes por el caudal platino.

Para empezar sobre la sede remota se crea la lista de acceso, esta deberá permitir cualquier host de esta sede al destino 192.168.10.5 el cual es el servidor ubicado en la sede principal, figura 39.

Figura 39. Lista de acceso en sede remota

En la figura 40 se ve que al realizar ping desde un PC de la sede remota al servidor 192.168.10.5 si se ve coincidencia, en la lista de acceso se verá reflejada con un match.

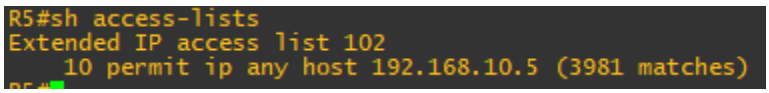


Figura 40. Match sobre lista de acceso en sede remota.

Al igual que la lista de acceso, cuando se aplican los QoS sobre las interfaces de entrada y salida, se observan el match generado confirmando que los paquetes al destino 192.168.10.5 en este caso por ser sede remota, están siendo etiquetados sobre la cola platino, esto se ve sobre la figura 43; en las figuras 41 y 42 se ven las configuraciones sobre el Router.

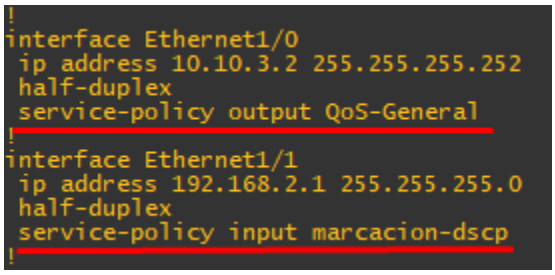


Figura 41. Configuración de QoS sobre interfaces sede remota.

```
!
class-map match-all Class-Platino
 match  dscp af31
class-map match-all MARC-Platino
 match access-group 102
!
!
policy-map QoS-Clases
 class Class-Platino
  bandwidth 5120
 class class-default
  bandwidth 15360
policy-map QoS-General
 class class-default
  shape peak 20480000 204800 0
  service-policy QoS-Clases
policy-map marcacion-dscp
 class MARC-Platino
  set dscp af31
 class class-default
  set dscp default
```

Figura 42. Configuración de QoS sobre rotuer sede remota.

```
R5#sh policy-map interface
 Ethernet1/0

  Service-policy output: QoS-General

    Class-map: class-default (match-any)
      2196 packets, 213401 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
        20480000/20480000   25600  204800    0         10        25600

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         2196      213401    0         0         no

      Service-policy : QoS-Clases

        Class-map: Class-Platino (match-all)
          1875 packets, 183750 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match:  dscp af31 (26)
          Queueing
            Output Queue: Conversation 265
            Bandwidth 5120 (kbps)Max Threshold 64 (packets)
            (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

        Class-map: class-default (match-any)
          321 packets, 29651 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any
          Queueing
            Output Queue: Conversation 266
            Bandwidth 15360 (kbps)Max Threshold 64 (packets)
            (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
 Ethernet1/1

  Service-policy input: marcacion-dscp

    Class-map: MARC-Platino (match-all)
      1876 packets, 183848 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 102
      QoS Set
        dscp af31
          Packets marked 1876

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

Figura 43. Match sobre interfaces de Router principal.

Como se realizó en la sede remota se debe realizar en la sede principal, el único cambio que va a haber es la dirección de la lista de acceso, ya que en esta sede es donde se encuentra el servidor, es decir, el destino son las sedes remotas, figura 44.

```
!
access-list 100 permit ip host 192.168.10.5 any
```

Figura 44. Lista de acceso en sede principal

En la figura 45 se ve que al realizar ping desde un PC de la sede remota al servidor 192.168.10.5 si se ve coincidencia, en la lista de acceso se verá reflejada con un match.

```
R1#sh access-lists
Extended IP access list 100
    10 permit ip host 192.168.10.5 any (3892 matches)
```

Figura 45. Match sobre lista de acceso en sede principal.

Al igual que la sede remota, cuando se aplican los QoS sobre las interfaces de entrada y salida se observan el match generado confirmando que los paquetes desde la IP 192.168.10.5 que es el servidor, tanto de entrada como salida están siendo etiquetados sobre la cola platino, esto se ve sobre la figura 48; en las figuras 46 y 47 se ven las configuraciones sobre el Router, como se tiene Router backup la configuraciones deben ser exactamente las mismas.

```
!
interface Ethernet1/0
 ip address 10.10.1.2 255.255.255.252
 rate-limit output access-group 100 4096000 768000 1536000 conform-action transmit exceed-action continue
 rate-limit output 4096000 768000 1536000 conform-action transmit exceed-action drop
 load-interval 30
 half-duplex
 service-policy output QoS-General
!
interface Ethernet1/1
 ip address 192.168.10.1 255.255.255.0
 half-duplex
 standby 5 ip 192.168.10.3
 standby 5 priority 110
 standby 5 preempt
 standby 5 track 10 decrement 30
 service-policy input marcacion-dscp
```

Figura 46. Configuración de QoS sobre interfaces sede principal.

```
!
class-map match-all Class-Platino
 match  dscp af31
class-map match-all MARC-Platino
 match access-group 100
!
!
policy-map QoS-Clases
 class Class-Platino
  bandwidth 5120
 class class-default
  bandwidth 15360
policy-map QoS-General
 class class-default
  shape peak 20480000 204800 0
  service-policy QoS-Clases
policy-map marcacion-dscp
 class MARC-Platino
  set dscp af31
 class class-default
  set dscp default
```

Figura 47. Configuración de QoS sobre rotuer sede principal.

```
R1#sh policy-map interface
 Ethernet1/0

  Service-policy output: QoS-General

    Class-map: class-default (match-any)
      5531 packets, 527743 bytes
      30 second offered rate 1000 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
         20480000/20480000  25600  204800    0         10        25600

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         5531      527743    0         0         no

      Service-policy : QoS-Clases

        Class-map: Class-Platino (match-all)
          4263 packets, 417774 bytes
          30 second offered rate 1000 bps, drop rate 0 bps
          Match:  dscp af31 (26)
          Queueing
            Output Queue: Conversation 265
            Bandwidth 5120 (kbps)Max Threshold 64 (packets)
            (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

        Class-map: class-default (match-any)
          1268 packets, 109969 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: any
          Queueing
            Output Queue: Conversation 266
            Bandwidth 15360 (kbps)Max Threshold 64 (packets)
            (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
 Ethernet1/1

  Service-policy input: marcacion-dscp

    Class-map: MARC-Platino (match-all)
      4265 packets, 417970 bytes
      5 minute offered rate 1000 bps, drop rate 0 bps
      Match: access-group 100
      QoS Set
        dscp af31
          Packets marked 4265

    Class-map: class-default (match-any)
      1843 packets, 114484 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        dscp default
          Packets marked 1843
```

Figura 48. Match sobre interfaces de Router principal.

11. Resultados

Ejecutando la ampliación del ancho de banda del canal principal, la configuración de QoS y la configuración de rate-limit, se evidencia que la saturación no se presenta por lo cual tampoco se evidencias latencias sobre las demás sedes hacia el servidor.

Para confirmar que el enlace está operando correctamente se realiza una prueba RFC 2544 con los respectivos equipos de medición; en esta prueba se revisa Latencia, Perdida de Tramas, Jitter y Throughput.

Las siguientes figuras sobre los Router del cliente muestra los tiempos de respuesta y tráfico que cursa sobre cada uno de ellos, en el Router principal sobrepasa notablemente las 8 Megas originales y no se presentan intermitencias.[17]

En las figuras 49 y 50, se observa el tráfico sobre canal principal donde se evidencia que tiene una ocupación de 12.8 Megas superando las 8 Megas que tenía inicialmente, comprobando que por el canal principal se tienen muchos más requerimientos de tráfico de las demás sedes y con el ancho de banda inicial no daba abasto.

```
HOSPITAL_SOPO_DX#sh int sum

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                IHQ       IQD       OHQ       OQD      RXBS      RXPS      TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------------------------
  Em0/0                      0         0         0         0         0         0         0         0         0
* GigabitEthernet0/0         0         0         0        42   1394000      1210  12896000      1382         0
* Gi0/0.3523                 -         -         -         -         -         -         -         -         -
* GigabitEthernet0/1         0         0         0       564  12772000      1332   1311000      1164         0
* Loopback500                0         0         0         0         0         0         0         0         0
NOTE:No separate counters are maintained for subinterfaces
```

Figura 49. Trafico sobre Router principal Sopo.

[17] [15] Ricardo Jorge Rodríguez, "Resolución de Incidencias de redes telemáticas", IC Editorial, Antequera Málaga, 2014.

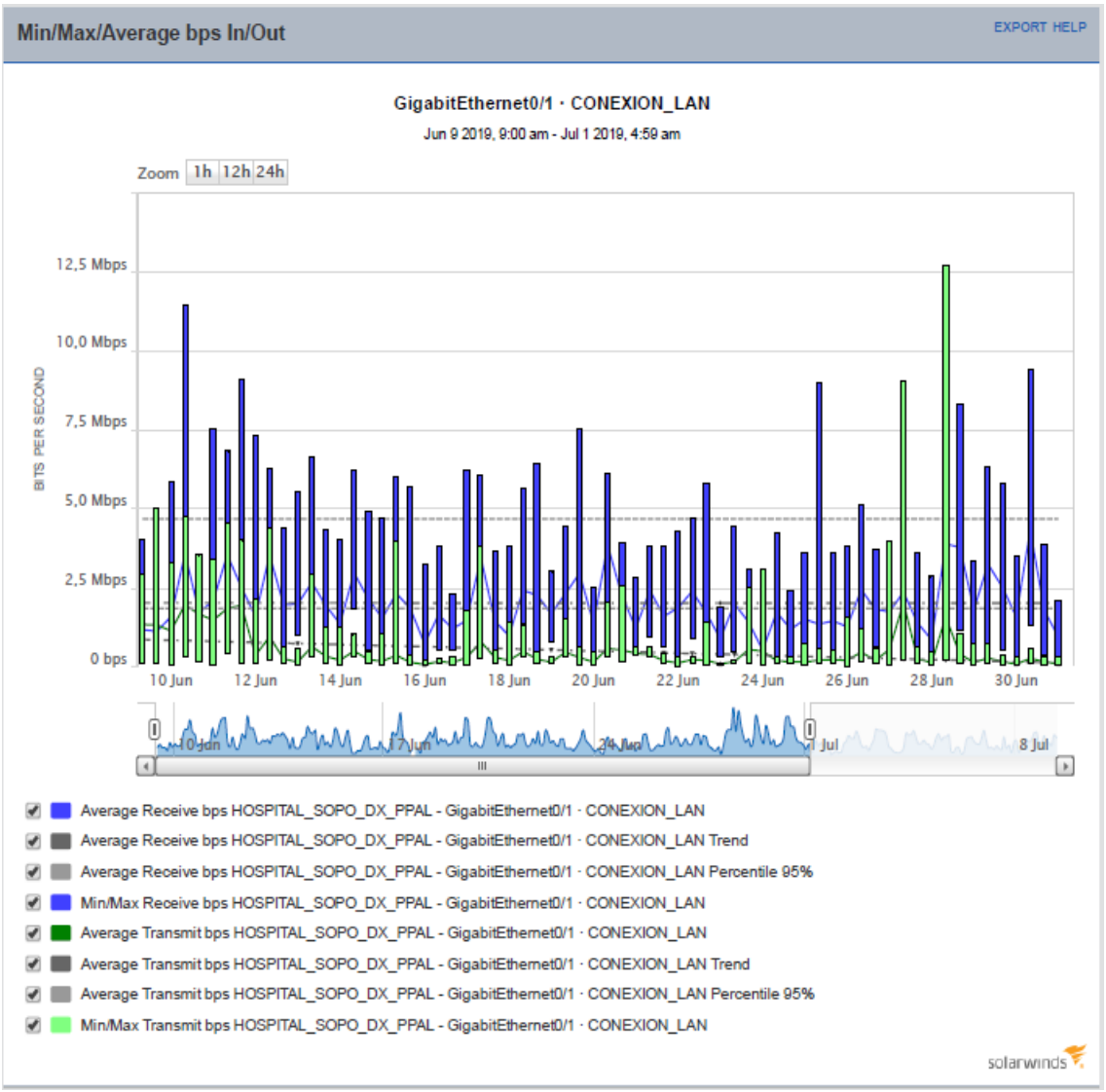


Figura 50. Trafico sede Principal Sopo (Herramienta monitoreo MOVISTAR MAS)[18]

Las siguientes figuras 51, 52 y 53 muestra la marcación de paquetes sobre el QoS y ACL configurado sobre el canal principal, muestra el ancho de banda manejado por cada cola al igual que en la emulación hecha, se comprueba correcto funcionamiento separando el tráfico marcado sobre la ACL 101.

```
HOSPITAL_SOPO_DX#sh access-lists 101
Extended IP access list 101
    10 permit ip host 192.168.1.40 any (167106 matches)
```

Figura 51. ACL 101 marcación de paquetes IP servidor.

[18] http://movistarmas.telefonica.com.co:8787/Orion - Herramienta Monitoreo Movistar Mas – SolarWinds

```
class-map match-all PLATINO
 match dscp af31
class-map match-all marc-PLATINO
 match access-group 101
!
policy-map ip-wan-qos
 class PLATINO
  bandwidth 16384
 class class-default
  bandwidth 4096
policy-map shape-20Mbps
 class class-default
  shape peak 20480000
   service-policy ip-wan-qos
policy-map marcacion-ip
 class marc-PLATINO
  set dscp af31
 class class-default
  set dscp default
```

Figura 52. Configuración de QOS sobre router sede principal.

```
HOSPITAL_SOPO_DX#sh policy-map interface gigabitEthernet 0/0
 GigabitEthernet0/0

  Service-policy output: shape-20Mbps

    Class-map: class-default (match-any)
      432748 packets, 368347348 bytes
      30 second offered rate 1236000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/35/0
      (pkts output/bytes output) 435604/372661554
      shape (peak) cir 20480000, bc 81920, be 81920
      target shape rate 40960000

      Service-policy : ip-wan-qos

        Class-map: PLATINO (match-all)
          131042 packets, 49245861 bytes
          30 second offered rate 135000 bps, drop rate 0000 bps
          Match:  dscp af31 (26)
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/35/0
          (pkts output/bytes output) 131007/49194999
          bandwidth 16384 kbps

        Class-map: class-default (match-any)
          301706 packets, 319101487 bytes
          30 second offered rate 1101000 bps, drop rate 0000 bps
          Match: any
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 304594/323462367
          bandwidth 4096 kbps
```

Figura 53. Marcación de paquetes sobre QoS en sede principal.

Las figuras 54 y 55 muestran al igual que con la configuración de QoS, configuración y marcación de paquetes, pero en este caso para la ACL 100 la cual está configurada para permitir el tráfico del servidor por encima de 16M, todo el resto será rechazado por el rate-limit, se observa que sobre la interfaz WAN del router la ACL 100 que tiene la IP del servidor como "permit" al sobrepasar las 16M continuara hasta las 20M de capacidad del enlace y la siguiente línea dice que todo demás tráfico que pase las 16M será rechazado.

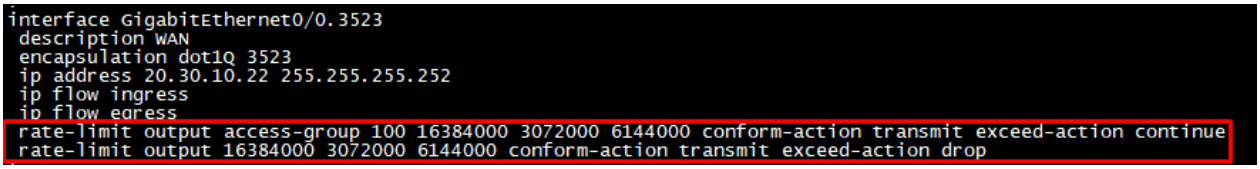


Figura 54. Configuración rate-limit en router principal

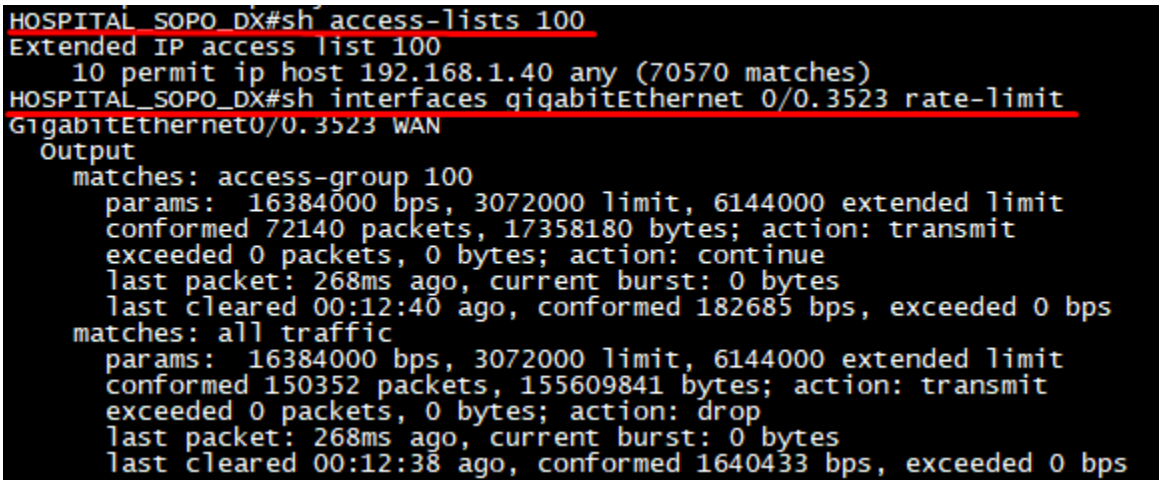


Figura 55. Marcación de paquetes sobre rate-limit en sede principal.

Las siguientes figuras 56, 57 y 58 respectivamente muestran configuración de QoS, ping a la sede principal Sopo desde Tocancipá y trafico sobre el mismo, debido que se amplía el ancho de banda del canal principal, se configuro QoS y rate-limit, las sedes remotas no se observa saturación en el canal. Se tendrá bajos tiempos de respuesta, no perciben pedidas de paquetes y tendrán ancho de banda para poder consultar sin problemas el servidor, se observa que los tiempos de respuesta bajaron de 22ms a 4ms en promedio para esta sede; en las sedes remotas no se configura rate-limit sin embargo QoS sí, ya que se debe dar prioridad al tráfico de entrada y salida al servidor desde las diferentes sedes.

```
class-map match-all PLATINO
 match dscp af31
class-map match-all marc-PLATINO
 match access-group 103
!
policy-map ip-wan-qos
 class PLATINO
  bandwidth 4096
 class class-default
  bandwidth 4096
policy-map shape-8Mbps
 class class-default
  shape peak 8192000
   service-policy ip-wan-qos
policy-map marcacion-ip
 class marc-PLATINO
  set dscp af31
 class class-default
  set dscp default
```

Figura 56. Configuración QoS en router Tocancipa

```
HOSP_DIV_SOPO_TOCANC_COLSUB#ping 192.168.10.1 source 192.168.4.1 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/4/20 ms
```

Figura 57. Ping a sede principal desde Tocancipá.

```
HOSP_DIV_SOPO_TOCANC_COLSUB#sh int sum

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD      RXBS      RXPS      TXBS      TXPS      TRTL
-----------------------------------------------------------------------------------------------------------------
  Em0/0                         0         0         0         0         0         0         0         0         0
* GigabitEthernet0/0            0         0         0         0   5707000       571    610000       561         0
* GigabitEthernet0/1            0         0         0         0   1573000       839   8208000       861         0
  GigabitEthernet0/2            0         0         0         0         0         0         0         0         0
* Loopback500                   0         0         0         0         0         0         0         0         0
```

Figura 58. Trafico de sede Tocancipá.

Las siguientes figuras 59, 60 y 61 respectivamente muestran configuración de QoS, ping a la sede principal Sopo desde Tocancipá Urgencias y tráfico sobre el mismo, se observa que no presenta perdida de paquetes, los tiempos bajaron de 24ms a un promedio de 4ms. Igualmente, en la sede se configura QoS para dar prioridad al tráfico del servidor.

```
class-map match-all PLATINO
 match dscp af31
class-map match-all marc-PLATINO
 match access-group 103
!
policy-map ip-wan-qos
 class PLATINO
  bandwidth 4096
 class class-default
  bandwidth 4096
policy-map shape-8Mbps
 class class-default
  shape peak 8192000
   service-policy ip-wan-qos
policy-map marcacion-ip
 class marc-PLATINO
  set dscp af31
 class class-default
  set dscp default
```

Figura 59. Configuración QoS en router Tocancipá Urgencias

```
HOSPITAL_DIVINO_TOCANC_URGEN#ping 192.168.10.1 source 192.168.3.1 repeat 1000

Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/4/16 ms
```

Figura 60. Ping a sede principal desde Tocancipá Urgencias.

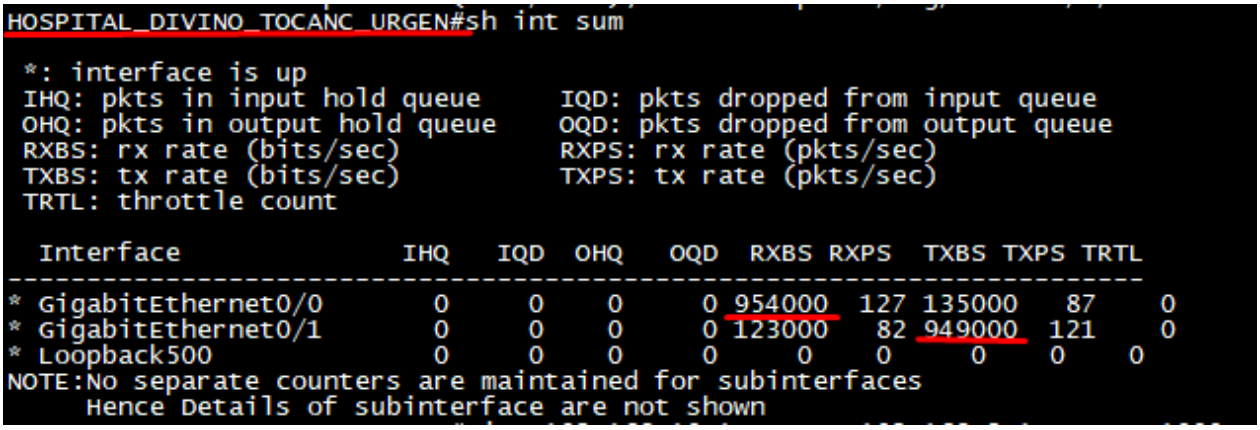


Figura 61. Trafico de sede Tocancipá Urgencias.

Las siguientes figuras 62, 63 y 64 respectivamente muestran configuración de QoS, ping a la sede principal Sopo desde Tocancipá Urgencias y trafico sobre el mismo, se observa que ya no presenta perdida de paquetes, los tiempos bajaron de 26ms a un promedio de 6ms de respuesta. Se configura QoS para dar prioridad al tráfico del servidor.

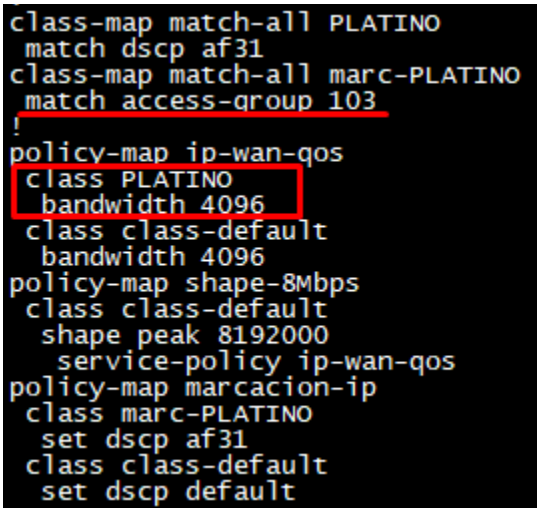


Figura 62. Configuración QoS en router La Calera.

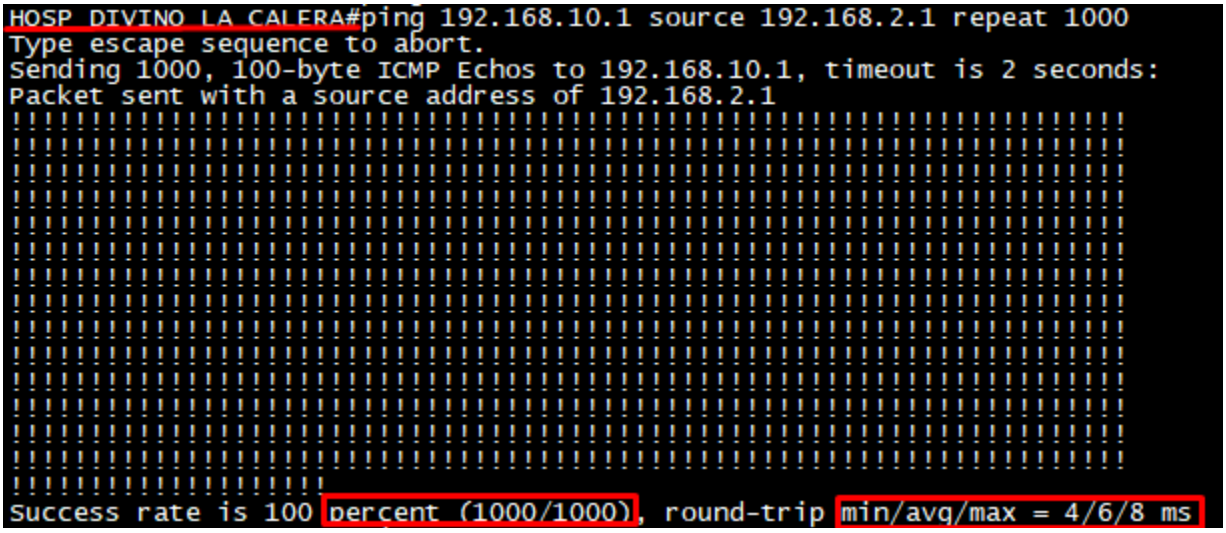


Figura 63. Ping a sede principal desde La Calera.

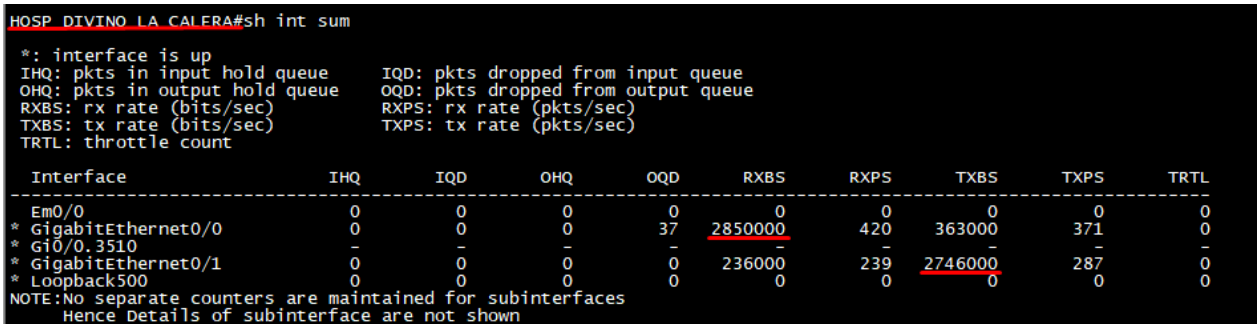


Figura 64. Trafico sobre sede La Calera.

Durante el proceso de implementación del proyecto también se recopilaron pruebas en el Router de la sede Sopo con el comando *show ip accounting.*
Con este comando se puede ver el número de paquetes y de bytes que se envían, evidenciando la mejora en la red.

La Figura 65 es una prueba tomada en agosto del 2018 cuando se inició con la implementación, aquí se observa que las 2 primeras IP son públicas (Internet) y saturan la red bloqueando el servicio del servidor.

HOSPITAL_SOPO_DX#show ip accounting

SrcIP	DstIP	Protocol	Pkts	Bytes
13.107.4.50	192.168.4.25	TCP	11306	16835887
173.194.186.202	192.168.2.10	TCP	8554	12597291
192.168.1.40	192.168.4.70	TCP	3117	2564272
192.168.1.40	192.168.3.10	TCP	2799	2535383
209.85.231.232	192.168.3.7	UDP	1715	2356598
192.168.1.43	192.168.2.26	TCP	2236	1917055
67.24.75.254	192.168.2.30	TCP	1311	1877593
10.25.30.185	172.22.65.52	UDP	466	503032
192.168.1.40	192.168.2.17	TCP	2888	487206
172.217.28.99	192.168.2.18	UDP	433	471965
192.168.1.40	192.168.2.38	TCP	1246	204827
192.168.1.40	192.168.3.19	TCP	1055	177076

Figura 65. show ip accounting (agosto 2018)

Una vez se realizó la implementación, nuevamente se toma la prueba con el comando *show ip accounting* donde se observa la mejora de la red, además ya no se está saturando el enlace (Figura 66).

HOSPITAL_SOPO_DX#show ip accounting

Source	Destination	Packets	Bytes
35.168.187.203	192.168.2.145	24	12570
172.217.8.134	192.168.2.145	129	163864
209.126.107.215	192.168.3.120	391	16684
192.168.10.2	192.168.3.10	917	154379
147.135.10.119	192.168.4.4	703	29920
192.168.1.40	192.168.3.40	57322	11505381
192.168.1.40	192.168.2.40	21021	4638106
172.106.3.170	192.168.3.7	549	29111
72.247.3.67	192.168.2.145	598	713302
104.16.130.5	192.168.2.145	26	4371
52.242.211.89	192.168.3.35	181	35380
173.194.217.125	192.168.4.163	274	19154
104.37.178.1	192.168.2.145	27	20943
152.204.131.190	192.168.2.5	40898	7372258
192.168.1.93	192.168.3.89	53	2343
192.168.1.98	192.168.2.102	186	8016
52.109.76.30	192.168.2.102	9	6554
8.8.8.8	192.168.2.98	148	19750
8.8.4.4	192.168.2.98	63	8052

Figura 66, show ip accounting (julio 2019)

Anteriormente la red funcionaba entre el 80% y 100% de la capacidad, con las mejoras realizadas bajaron los tiempos y ahora trabaja en un promedio del 15% y 30% teniendo opción de aumentar su personal o incluir más dispositivos a la red

12. Discusión

Según las pruebas realizadas al principio sobre la red se comprobó que los tiempos de respuesta entre las sedes no eran óptimos para el correcto funcionamiento del aplicativo del centro médico, generando un "Cuello de Botella", esto debido a que todas las sedes llegaban a consultar a la sede principal.

Con el análisis del tráfico se recomendó realizar una ampliación del ancho de banda de la sede principal que resolvió el tema de saturación, en este punto se tuvo que tener en cuenta el throughput del router para que este pudiera soportar el tráfico entrante y saliente de todas las sedes; además se realiza configuración de QoS y rate-limit para controlar el tráfico evitando una futura saturación por aumento de personal administrativo, además de dar prioridad al tráfico de entrada y salida del servidor para las diferentes sedes.

Para el respaldo de un canal de datos para la sede principal, el cliente no opto por implementar un nuevo servicio debido a los costos que le podían generar, pero se emulo el funcionamiento comprobando que el tráfico iría por el canal backup con normalidad, configuración de HSRP.

13. Conclusiones

- Con diseño de la red propuesta se logra mejorar la disponibilidad y calidad de servicio de acuerdo con las pruebas realizadas para la justificación del proyecto, con la ampliación del canal principal y cambio de Router se optimiza el throughput, eliminando la lentitud y perdidas de paquetes percibidas. Este nuevo diseño permite soportar el tráfico entrante y saliente.
- Las configuraciones de QoS ejecutadas en los routers de cada sede prioriza el tráfico hacia el servidor. Dicha configuración permite que los paquetes marcados sobre la ACL configurada pasen primero al router por encima de todo el tráfico restante.
- La configuración de rate-limit en el router principal confirma que cualquier otro tráfico diferente al del servidor pueda saturar la red y por ende afectar el aplicativo.
- Con la configuración del QoS y rate-limit, así como la ampliación del ancho de banda permiten que el tráfico sea controlado y también mejoren los tiempos de respuesta desde las sedes remotas hacia el servidor.
- Se emula la topología de la red con las configuraciones necesarias para controlar el tráfico y tener un correcto funcionamiento, con estos datos concluimos que las configuraciones planteadas funcionarán y tendrán una correcta aplicación.

14. Documentación de Referencia

[1] Cisco. (1984, Dic). [Online]. Disponible en: https://www.cisco.com}

[2] https://www.cisco.com/c/en/us/products/ios-nx-os-software/multiprotocol-label-switching-mpls/index.html

[3] https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/22833-qos-faq.html

[4] https://www.cisco.com/c/es_mx/support/docs/ip/hot-standby-router-protocol-hsrp/10583-62.html

[5] http://www.mustbegeek.com/configure-hsrp-in-cisco-ios-router/

[6] https://www.gns3.com/

[7] https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/command/reference/fqos_r

[8] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60D_Series.pdf

[9] Ernesto Ariganello, "Redes Cisco: Guía de estudio para la certificación CCNA 640-802", Alfaomega Grupo Editor, SA., México, Enero 2009.

[10] Ernesto Ariganello, "Técnicas de configuración de Router Cisco", Alfaomega Grupo Editor, SA., México, Abril 2008.

[11] Ernesto Ariganello, "Redes Cisco CCNP Routing & Switching", Editorial Ra-Ma – Ediciones de la U, España, 2016.

[12] Ra-Ma, "Sistemas de Telecomunicaciones e informáticos: Redes telemáticas", Editorial Paraninfo, España, 2015.

[13] Ángel Luis Calvo García, "Gestión de Redes telemáticas", IC Editorial, España, 2014.

[14] Ricardo Jorge Rodríguez, "Desarrollo del proyecto de la red telemática", IC Editorial, Antequera Málaga, 2014.

[15] Ricardo Jorge Rodríguez, "Resolución de Incidencias de redes telemáticas", IC Editorial, Antequera Málaga, 2014.

[16]https://community.cisco.com/legacyfs/online/legacy/7/1/5/15373517-white_paper_c11_595485.pdf

[17] http://movistarmas.telefonica.com.co:8787/Orion - Herramienta Monitoreo Movistar Mas – SolarWinds

[18] Pablo Scaniello y Gonzalo Sosa, "Curso de Evaluación de performance de Redes", Uruguay.

15. Anexos

15.1. Configuración Router sedes

Plantilla SOPO PPAL.txt

Plantilla CALERA.txt

Plantilla TOCANCIPA.txt

Plantilla TOCANCIPA URG.txt

15.2. Simulación de la red en GNS3

HSRP_Rate_limit.7z

15.3. Propuesta comercial

Cuadro_de_Gestion_de_Proyectos___ET_V1_(

15.4. Prueba RFC 2544

INFORME PRUEBAS CENTRO MEDICO.pdf

15.5. Graficas Actuales monitorio MOVISTAR MAS

NODE_DETAILS_MOVISTARMAS_NETWORK]

15.6. Pruebas IP accounting

IP accounting SOPO Agosto 2018.txt

IP accounting SOPO JULIO 2019.txt